Information Security Risk Management
MSIT 3440 - Summer 2009
Course Syllabus

Course Description
Functional, performance, and economic considerations used to dominate the IT environment, however, security criteria have now emerged as another primary concern for decision makers. It is essential for any IT professional to understand the risk management lifecycle and the various frameworks which have evolved to model proper information security management. This course will explore each phase of the risk management lifecycle, focusing on policies and assessment processes that should be used to properly mitigate and assess risk. Students will learn techniques to perform risk assessments for new IT projects, how to measure security ROI, and how to quantify the current risk level for presentation to executive level management. A common case study will be followed throughout the course to provide a holistic view of how to properly use tools to calculate the costs and benefits of any security investment.

Instructor
Evan Wheeler, MS CISSP SSCP GCFA
Phone: (843) 860-4460
Email: ewheeler@clarku.edu

Required Text
T. Peltier, "Information Security Risk Analysis", Auerbach, 2005.

Grading

Class Participation and Attendance:	20%	(40 points)
Assignments:	30%	(60 points)
Take Home Midterm Exam:	20%	(40 points)
Final Project:	30%	(60 points)

Weekly exercises will be assigned to students individually or to be completed in small groups according to the week's topic. The assignments will follow a progression of the typical risk management lifecycle showing students how to complete each step in a real world scenario based on a single case study that will be used throughout the semester. Assignments will be based on an assessment of a fictional government agency and other instructor provided information. The final project will be based on one of three hypothetical scenarios to be assessed using the FRAAP approach.

The midterm exam will consist of several individual exercises to be completed outside of class by students individually based on a fictional government agency case study. Students will receive feedback on individual assignments and should make revisions before turning in the completed midterm deliverable. This deliverable will resemble several sections of a typical risk analysis report.

By the end of the semester, student groups will have completed an entire risk analysis report which is a compilation of the various weekly assignments and midterm exam. This final report will be presented by each group to the class as if they were presenting the results to an executive management group. Students will be graded on the content of the report and the manner in which it is presented.

Schedule
Summer Session I runs from May 18th to June 29th. We will meet on Tuesday and Thursday evenings from 6:00pm to 9:30pm. The following course schedule will be followed:

Session	Topic	Assignment	Reading
1 May 19	Introduction & Definitions	Current Event Summary & Resume	Ten Security Domains *Chapters 1 & 2*
2 May 21	Threat Landscape **Current Event Presentations**	Critical Asset Exercise	HGA Case Study
3 May 26	Risk Profiling	List the Vulnerabilities Exercise	Chapter 3
4 May 28	Risk Exposure Factors	Rate Risks Exercise	Chapter 8
5 June 2	Security Controls & Services	Map Controls to Vulnerabilities Exercise	Chapter 4
6 June 4	Risk Assessment Techniques	Prepare Midterm	Security ROI Articles
7 June 9	Measuring Security ROI **Midterm Due**	No Assignment	NIST SP 800-12
8 June 11	Mitigation Plans and Long-term Strategies	Management Response Exercise	NIST SP 800-30
9 June 16	Introduction to FRAAP Method	Mitigation Plan Exercise Executive Summary Exercise	Chapter 6
10 June 18	Integration into the Design Process	Finish in Class Group FRAAP Exercise	Chapter 7
11 June 23	NIST Method **Final Group Presentations**	Finish Audit Report	OCTAVE Approach Intro
12 June 25	OCTAVE Method **Final Group Presentations**		

The course schedule will not follow the order of the book exactly, but rather will be based on a logical progression of topics based on prerequisite knowledge needed and the topic's phase of the Risk Management Lifecycle.

Course Format

On Tuesdays, the class period will begin with a short quiz for extra credit based on the assigned reading or last week's lecture material. The answers to the quiz will be reviewed after completion.

Lecture will cover topics related to the reading, but will not just review or summarize the reading. When articles are assigned, the lecture will include class discussions. The topics covered in lecture should help the student apply the reading materials to practical situations and advanced topics. The format will vary based on the week's topic.

When available, guest speakers will come in to present their perspective on a special area related to the week's topic and provide real world examples for students. This also provides a great networking opportunity for students to meet active professionals in the field. When speakers are not available, lecture or hands on activities will be substituted.

Hands on activities or demonstrations will be used to illustrate real world applications of the week's topics. This may involve demonstrations of risk assessment tools, interactive group exercises, or instructor lead hands on exercises to illustrate pertinent concepts. Completion of in class activities and participation in discussions on Cicada (http://cicada.clarku.edu) will comprise the participation portion of your grade in addition to participating in class discussions.

Guest Speakers

During the course of the semester, we will bring in industry experts to supplement the lectures and in class assignments with talks on related topics. The following guest speakers have been scheduled for this semester:

Class 5 – *The Relationship Between IT & Security Teams*. Charles Kolodgy, Research Director for IDC

Class 8 – *IT Audit and Risk Management*. Justin Peavey, CISO for Omgeo

Class 9 – *Steps to Ensure a Successful Security Assessment*. Ken Smith, Security Solutions Architect for Forsythe Solutions Group

Class 10 – *Integrating Risk Management into the Software Development Lifecycle*. Jeff Bardin, Director of Risk Management for EMC

Class 11 – *Raising the Bar on Security*. Eben Berry, CISO for Blue Cross Blue Shield of Massachusetts

Please try to especially arrive on time to these sessions as a courtesy to our guest speakers.

Assignments

1. **Extra Credit Quizzes (5 pts. each)** – A short quiz will be provided at the beginning of each class session. The quiz will cover the topics from the last class or from the reading assignment.
2. **Security Current Event (10 pts.)** – Find a current topic in the news related to information assurance, and bring in the article. You will need to summarize the key points of the article for the class. This should take 3 to 5 minutes. Please also post a link to the article or a reference for the article on the designated Cicada discussion thread.
3. **Midterm Assignment (40 pts.)** – Throughout the first three weeks of class, students will complete assignments based on a provided case study for a fictional government agency. Each assignment will cover a different aspect of a typical risk assessment. Students will turn in the individual assignments each session for review and comments by the instructor. Students will then have the opportunity to revise their submissions and compile them for grading as the midterm assignment.
    a. **List Critical Assets Exercise (5 pts.)** – Based on the case study, identify and describe the business value for each of the critical assets for the agency. Rate the overall risk sensitivity for these assets based on the provided scale.
    b. **List Vulnerabilities Exercise (5 pts.)** – Read through the provided case study, and list the vulnerabilities that have been identified. All vulnerabilities are not necessarily technical.
    c. **Rate the Risks Exercise (5 pts.)** – For each vulnerability, describe the threat in addition to the vulnerability, and rate the risk exposure. This rating should take into account all the factors of likelihood of exploitation and the sensitivity of the asset.
    d. **Map Controls to Vulnerabilities Exercise (5 pts.)** – Using the list of vulnerabilities from the case study, recommend controls that could mitigate the particular weaknesses. Controls can be technical or process based.

e. **Midterm Deliverable (20 pts.)** – Revise the previous four assignments based on the instructor's feedback and turn in for grading.

4. **Audit Assignment (50 pts.)** – Students will now use the same case study, but this time treat it as an audit report. Several exercises will be performed from the perspective of the organization being audited.
    a. **Management Response Exercise (10 pts**.) – Based on the risk assessment provided in the case study, students should write a management response to the items as if responding to an audit report. This report should include timelines for completing remediation and a high-level description of the remediation approach chosen.
    b. **Mitigation Plan Exercise (10 pts**.) – Now that management has responded to the audit report, students need to develop a mitigation plan to address each of the audit items. This should include specific steps that will be taken, responsible parties identified, and timeframes for delivery.
    c. **Executive Summary Exercise (10 pts**.) – Students will write an executive summary for the audit report of the case study. The summary should be no longer than one page summarizing the primary findings that would be of interest to the executive level managers.
    d. **Audit Report Deliverable (20 pts.)** – Revise the previous three assignments based on the instructor's feedback and turn in for grading.
5. **Final Project & Presentation (60 pts.)** – Students will work in teams of three during class to complete the FRAAP analysis exercise. The results should be written up for submission by the their assigned presentation date and groups will be expected to present their results to the class in a short presentation (20 minutes). Groups will receive one grade for the written deliverable and students will be graded individually on their presentations. Each presenter will be graded individually for their contribution to the presentation and style (20 pts.) and the deliverable will be given one grade for the group (40 pts.).

Policies, Rules and Other Administrative Stuff

Attendance

You will be graded on class participation as well as participation in online discussions and activities. Therefore, it will help you to actually be in class. Please do not make me start taking official attendance – come to class, come on time, and participate!

Honesty and Plagiarism

1. Please do not take credit for someone else's work. If you use someone else's ideas, cite where you got them from – I will know if you do not, and you will not be given credit for the work!!
2. Please do not cheat on your exam – this will put me in a very bad mood, and will put your grade in a very bad place.

The Clark University honesty policies apply to all Clark classes – please see the university website (www.clarku.edu) for further details.

Other Important Things to Know

You are expected to participate in a good amount of discussion in this course. The rules for this are as follows:

1. You will treat one another, and me, with respect at all times – there are no exceptions to this rule!

2. There are no stupid arguments, just ones you disagree with. Therefore, if you disagree with an argument presented, refer to rule #1 before you respond to it.
3. It is no fun to talk while other people are talking – this goes for me as well as your fellow classmates. Again, please refer to rule #1 before leaning over to speak to your neighbor while someone else is trying to lead class.
4. Discussions are more fun when you actually have an opinion – please come in ready to share yours with the class.
5. Please turn the ringers off on all phones. If you need to take a call during class time, please step outside to be considerate to other students.

You are also expected to do a fair bit of writing over the course of this semester. Please keep in mind that, as I have to read everything you write, correct grammar and spelling are highly appreciated, and, in some cases, will be reflected in your grade. All writing should be typed, in 12 point font, and page requirements are not just a suggestion!

Late work will be accepted, but will be graded down one level for each day past the due date (e.g., an A will be graded A-, a B- will be graded C+, etc.). If there are extenuating circumstances for the work being late, please speak to me as soon as possible so that we can work out a fair extension.

Finally, I am very much hoping that this will be a fun class for all of us, and that we will all learn something new in every session (including me!). This depends a great deal on how you approach the class, however, so I leave it to you – come prepared, come with questions, and come ready to jump head first into the material, and we will all have a great semester!