Syllabus and Course Outline

MIS 315 Information System Security & Risk Management

Professor: ***Dr. Bob Folden***

Office Number: ***BA 336A***

Phone: ***Office (903) 468-6053 (email is the best way to contact me)***

E-mail: ***Bob.Folden@tamuc.edu***

Office Hours: ***Tuesday and Thursday 11:00 am to 12:00 pm, Tuesday 1:00 pm to 5:00 pm and other times by special appointment.***

Course Description:

This is an introduction to the various technical and administrative aspects of Information Security and Assurance. This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features.
The purpose of the course is to provide the student with an overview of the field of Information Security and Assurance. Students will be exposed to the spectrum of Security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of the Information Security Planning and Staffing functions.

Course Objectives:

1. Identify and prioritize information assets.
2. Identify and prioritize threats to information assets.
3. Define an information security strategy and architecture.
4. Plan for and respond to intruders in an information system
5. Describe legal and public relations implications of security and privacy issues.
6. Present a disaster recovery plan for recovery of information assets after an incident.

Accommodations

Students with Disabilities:

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services
Texas A&M University-Commerce
Gee Library
Room 132
Phone (903) 886-5150 or (903) 886-5835
Fax (903) 468-8148
StudentDisabilityServices@tamu-commerce.edu

Conduct

"All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (See Guidebook, p. 42-45)

Academic Integrity

Academic integrity is the pursuit of scholarly activity free from fraud and deception and is an educational objective of this institution. Academic dishonesty includes, but is not limited to, cheating, plagiarizing, fabricating of information or citations, facilitating acts of academic dishonesty by others, having unauthorized possession of examinations, submitting work of another person or work previously used without informing the instructor, or tampering with the academic work of other students

All work submitted to this Instructor may be submitted to an academic integrity verification service such as Turnitin.com.

You are responsible for authenticating any assignment submitted to this instructor. If asked, you must be able to produce proof that the assignment submitted is actually your own work. Therefore, it is recommended that you engage in a verifiable working process on assignments. Keep copies of all drafts of your work, make photocopies or digital copies of research materials, keep logs or journals of your work on assignments, and papers, learn to save a version of assignments under individual filenames on computers or diskettes, etc.

The inability to authenticate your work, should it be requested, is sufficient grounds for failing an assignment.

Appeals Process:

Students taking online classes at Texas A&M University-Commerce have the same rights as students enrolled in face-to-face classes. The A&M-Commerce Student *Guidebook* (page 55) details those rights and explains complaint and grievance procedures, as well as the Student Code of Conduct. Students have the right to appeal course grades, *Guidebook* (page 35), admissions committee decisions, or any adverse action taken by any *online* faculty against any student. The appeal process is the same for all types of appeals.

Requests from students with disabilities for reasonable accommodations must go through the Academic Support Committee. For more information, please contact the Office of Student Disability Resources and Services, Gee Library, Room 132 Phone (903) 886-5150 or (903) 886-5835."

Projects:

1. **Identify and prioritize information assets. Identify and prioritize threats to information assets.** Choose a company (any company that interests you) to use as your company (You may also use your personal system as your company). You will assume the role of the Chief Security Officer of the company. You will identify all of your security assets. You will then identify and prioritize the threats to those assets. **See NIST Special Publication 800-26** for guidance in doing the self-assessment. You will also find help in the textbook.

   Sample Risk Assessment Report Outline

   EXECUTIVE SUMMARY
   I. Introduction
   • Purpose
   • Scope of this risk assessment
   Describe the system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment.
   II. Risk Assessment Approach
   Briefly describe the approach used to conduct the risk assessment, such as—
   • The participants (e.g., risk assessment team members)
   • The technique used to gather information (e.g., the use of tools, questionnaires)
   • The development and description of risk scale (e.g., a 3 x 3, 4 x 4, or 5 x 5 risk-level matrix).
   III. System Characterization
   Characterize the system, including hardware (server, router, switch), software (e.g., application, operating system, protocol), system interfaces (e.g., communication link), data, and users.
   Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort.
   IV. Threat Statement
   Compile and list the potential threat-sources and associated threat actions applicable to the system assessed.
   V. Risk Assessment Results
   List the observations (vulnerability/threat pairs). Each observation must include—
   • Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
   • A discussion of the threat-source and vulnerability pair
   • Identification of existing mitigating security controls
   • Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
   • Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
   • Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)

• Recommended controls or alternative options for reducing the risk.

VI. Summary

Total the number of observations. Summarize the observations, the associated risk levels, the SP 800-30 Page B-2 recommendations, and any comments in a table format to facilitate

2. **Define an information security strategy and architecture.**
   You will develop a security strategy for your selected company that identifies the information assets and the security risks. Support your choices from the information security literature (you may use white papers or NIST documents). Treat this as if it would be the document that will guide the development of the security plan for the company. You will probably want to include a diagram of the physical layout of the system, as well as, the logical system design. Thoroughness is a critical factor. Remember that you need to address the needs of various users and systems in the company. Use the following table (or something similar) to summarize your plan.

SAMPLE SAFEGUARD IMPLEMENTATION PLAN SUMMARY TABLE

(1) Risk (Vulnerability/ Threat Pair)	(2) Risk Level	(3) Recommended Controls	(4) Action Priority	(5) Selected Planned Controls	(6) Required Resources	(7) Responsible Team/Persons	(8) Start Date/ End Date	(9) Maintenance Requirement/ Comments

(1) The risks (vulnerability/threat pairs) are output from the risk assessment process
(2) The associated risk level of each identified risk (vulnerability/threat pair) is the output from the risk assessment process
(3) Recommended controls are output from the risk assessment process
(4) Action priority is determined based on the risk levels and available resources (e.g., funds, people, technology)
(5) Planned controls selected from the recommended controls for implementation
(6) Resources required for implementing the selected planned controls
(7) List of team(s) and persons who will be responsible for implementing the new or enhanced controls
(8) Start date and projected end date for implementing the new or enhanced controls
(9) Maintenance requirement for the new or enhanced controls after implementation.

3. **Describe legal and public relations implications of security and privacy issues.**
   Construct a short paper identifying the legal and public relations implications of security and privacy issues for your chosen company. You will need to document your contentions from relevant scholarly literature. This should address both national and state

laws that impact security and privacy. Provide as much information on the various laws that would need to be complied with as possible. Identify the specific legislation by name and number so that it would be possible to locate the appropriate law.

4. **Present an incident response plan.**
   Use the information in Section 2.6 of the NIST SP 800-61. This should be a thorough document that covers policies and procedures for all types of incidents and your proposed response to them. Be sure to support your decisions from the literature.

Discussions:

In this course, you will be expected to participate in Discussions weekly. Professional communication is always expected. In order to achieve the maximum number of points for your Discussion grade, please answer each thread on three separate levels:

1) Answer the posted question (10 points);
2) Respond to another's posted answers (6 points);
3) Reply to any persons who have responded to you (4 points).

Discussion questions and topics may be added to the discussion area throughout the Semester. You will need to visit the area regularly. You are to consider the question or topic and post an appropriate response. You should support your response with external sources (**not course textbooks**) whenever appropriate. I will grade your responses based upon the quality of the response, including whether it is supported from external sources. All support should include all of the appropriate elements as identified in the APA Style Manual.

This is to be an attempt to create a seminar environment where you will be able to increase one another's knowledge of the subject. You should visit this area at least once a week to read the material and respond appropriately. You may add information at a later time as you would in a regular discussion.

Textbook(s) and Other Materials:

Required:

Smith, Richard E. *Elementary Information Security*.
ISBN 978-0-7637-6141-7 (Jones & Bartlett Learning, 2013).

Recommended:

Grading:

Project 1	300
Project 2	300
Project 3	300
Project 4	400
Labs	100
Discussions	340
Total Points Possible	**2,540**

Grading Percentages

A =	90= percent of total points
B =	80-89 percent of total points
C =	70-79 percent of total points
D =	60-69 percent of the total points
F =	59- or less percent of the total

Requests from students with disabilities for reasonable accommodations must go through the Academic Support Committee. For more information, please contact the Office of Student Disability Resources and Services, Gee Library, Room 132 Phone (903) 886-5150 or (903) 886-5835."

Course Outline and Assignments: This is only a proposal to guide you in your efforts to stay up with the course.

Unit	Due Date	Reading Assignment	Projects or Exams
Personal Security	**2/11/14**	Chapter 1	Discussion 1
		Chapter 2	Discussion 2 **Lab #1**
		Chapter 3	Discussion 3 **Project 1**
		Chapter 4	Discussion 4
		Chapter 5	Discussion 5 **Lab #2**
Cryptographic Security	**3/18/14**	Chapter 6	Discussion 6
		Chapter 7	Discussion 7 **Lab #3**
		Chapter 8	Discussion 8 **Lab #4**
		Chapter 9	Discussion 9 **Lab #5**
Network Security	**4/8/14**	Chapter 10	Discussion 10
		Chapter 11	Discussion 11 **Lab #6**
		Chapter 12	Discussion 12 **Lab #7**
Internet Security	**5/6/14**	Chapter 13	Discussion 13 **Project 2**
		Chapter 14	Discussion 14 **Lab #8**
		Chapter 15	Discussion 15 **Lab #9**
		Chapter 16	Discussion 16 **Project 3**
		Chapter 17	Discussion 17 **Lab #10** **Project 4** **Drop Dead Date: Everything due at this time.**

[+] Assignments are due 2400 hours (midnight) of the date that they are assigned.

Requests from students with disabilities for reasonable accommodations must go through the Academic Support Committee. For more information, please contact the Office of Student Disability Resources and Services, Gee Library, Room 132 Phone (903) 886-5150 or (903) 886-5835."