

Syllabus for IFSM433 (Information Security Needs Assessment Planning)

Course Description

Prerequisite: IFSM 300. Recommended: IFSM 430. In-depth practice in gathering security requirements to generate a security plan. Topics include the collection and analysis of functional security requirements, risk analysis, requirements traceability matrices and the collection of metrics, the investigation of physical security, operational procedures and legal issues related to information security, and the identification of education and training requirements. Projects include generating a site security plan based on site-specific or case-study requirements.

Course Goals/Objectives

After successful completion of this course, you should be able to:

- collect and analyze security requirements
- perform and document a risk assessment
- develop a requirements traceability matrix with metrics
- examine physical and operational security procedures
- explain the security legal issues that impact this area of risk assessment
- develop security education and training materials
- develop a site security plan from requirements
- test security plan implementation against security requirements
- validate and certify security plan
- identify the activities involved in security administration
- define the role of the Information Assurance Officer (IAO)

Course Materials

Kairab. A Practical Guide to Security Assessments. CRC Press. (ISBN: 0849317061)

Course Introduction

Security requirements are introduced as vital requirements for an enterprise. Additionally, the domains of the Certified Information Systems Security Professional (CISSP) are introduced for capturing security requirements leading to a security plan.

Risk assessment is identified as the first process in the risk management methodology. Threats, vulnerabilities, and impact on assets are identified to perform risk assessments associated with an information system throughout its development life cycle. Quantitative versus qualitative approaches are examined. Total risk versus residual risk is considered.

Security metrics are defined. Security downward and upward traceability matrices are described. Security models and modes are introduced. Security evaluation methods are explored. The Capability Maturity Model (CMM) is defined.

Security awareness comes about through training, education, certification and forums. Security incident organizations and the Department of Homeland Security are discussed. Emphasis is on keeping up with security in parallel with advancing technologies.

Security plans are developed comparing the NIST, Pipken, and OCTAVE security planning methodologies. The roles of system administrator (SA), database administrator (DBA), and system security manager (SSM) are differentiated. The roles of Information Assurance Officer (IAO) and/or Information Systems Security Officer (ISSO) (they maintain and manage the living security plan) are also introduced.

Grading Criteria

Section removed.

Academic Policies and Procedures

Section removed.

Project Descriptions

Risk assessment activity: A case study will be used to perform a risk assessment that will be initially derived from analyzing assets, vulnerabilities, threats, and countermeasures. Then total risk will be weighed against the residual risk that the case study's accreditor is willing to accept.

Homework Assignments: Various homework assignments will be given throughout the semester. These assignments will include (but not limited to) the following:

Requirements traceability matrix: A case study will be used to develop a requirements traceability matrix describing and following the life of requirements in both the forward and backward direction.

Security education/training materials: Security awareness and education training materials will be gathered and organized into a proposed security training program for management.

Encryption Exercise: This exercise will focus on different types of encryption. You need to require that you demonstrate your understanding of encryption concepts.

Security Product Report: In this report, you will provide a report on a security product (software, hardware, or service) that is commercially available.

Security plan: A living security plan will be developed from case study security requirements that incorporate inspection, protection, detection, reaction, and reflection phases.

Extra Credit: One extra credit assignment will be given about halfway through the course. Look for information about this assignment at about midterm. Points earned on extra credit can be applied to the Homework portion of the class.

All writing assignments should comply with UMUC policies. In particular, considerable focus will be on documenting your research.

Course Schedule

Week	Readings/Assignments	Due Date
1		
2	Pipken, pages 19-25,55-79 Security Requirements Case Study Due	
3	Pipken, chapters 7-9 Assign Risk Assessment Activity	
4	Pipken, chapters 10 and 11	
5	Pipken, chapters 12 and 13 Risk Assessment Activity Due	
6	Pipken, chapters 14 and 15 Assign Requirements Traceability Matrix	
7	Pipken, chapters 16 and 17	
8	Pipken, chapters 18 and 19 Requirements Traceability Matrix Due	
9	Pipken, chapters 20 and 21 Assign Security Training and Education Activity	
10	Pipken, chapters 22 and 23	
11	Pipken, chapters 24 and 25 Security Training and Education Activity Due	
12	Pipken, chapters 26 and 27 Assign Security Plan	
13	Pipken, chapters 28 and 29	
14	Pipken, chapters 30 and 31 Security Plan Due	
15	FINAL EXAMINATION	