

Syllabus for IFSM431 (Policy Planning for Security Architects)

Course Description

Prerequisites: IFSM 300 and an upper-level writing course (such as COMM 393 or WRTG 393). A study of various aspects of information assurance (IA) policy planning in an organizational context. Topics include the impact of current legislation and government regulations directing the focus of policy formulation. Key analysis procedures, such as security requirements analysis and risk assessments, are examined to determine their role in policy formation. Projects include generating an information security program for an organization.

Course Goals/Objectives

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

- identify the business and organizational issues involving information assurance (IA) and other related considerations
- understand what information systems means, and why the security and protection of these systems is important
- identify and discuss the fundamental reasons why information systems' security is a critical element in today's business, government, education, and home technology-based environments
- identify and discuss key information systems' security legislative and policy documents that guide development of an information system security program for an organization
- review and develop the key elements of an information systems' security management program
- perform and document a risk-based analysis of information systems' security for an organization, to include identification of threats, vulnerabilities, and countermeasures
- develop a security plan to address the results of the risk assessment
- identify and discuss the ethical and societal issues related to implementing information systems' security programs

Course Materials

Volonino, Principles and Practice of Information Security: Protecting Computers from Hackers and Lawyers. Prentice Hall (ISBN 0131840274)

Course Introduction

Businesses in today's global economy are dependent on network communication and electronic data. The complexity of information technology and the breadth of the systems required to do business in global economies make it difficult to evaluate and protect digital assets from cyber threats, including hackers. There are compelling

business and legal reasons why organizations can no longer ignore cyber risks or their consequences. There are legislative, legal, and ethical issues that have become inseparable from information protection. A defensive infrastructure includes an information security program that supports strict policies, secure practices, and updated technology.

Execution of the security program requires a clear and visible mandate from senior management.

The goals of the organization and information security must be aligned with people, practices, and technology issues. Well-documented policies must be in place, updated, and communicated frequently.

A company's digital assets create liability exposure. This course serves as the foundation for understanding how to identify, qualify, and quantify risk of exposure to hackers who seek to invade systems to do damage and/or for fun, and lawyers, who seek to recover damages on behalf of those perceived to have been wronged by security breaches. There are no infallible security systems, but there are cost-effective methods and policies that can significantly reduce exposure to cyber risks. Failure to implement stringent cyber security effectively leaves corporate assets vulnerable to both hackers and lawyers.

Security needs are managed in the context of the business. Information security is a business problem that can be assessed with the same analytic methods that are used for other business-related risks and consequences (outcomes). Risk analysis can be used to fully identify and assess risk factors, then balance the expected costs (damages) of incidents with the cost of defenses. This course introduces the taxonomy of threats and vulnerabilities and discusses how vulnerabilities may lead to financial loss or to legal problems. You will learn to examine intruders, their exploits, tools and methods of intrusion. You will also learn the reasons for their high success rate.

This course discusses the quantitative methods routinely used for assessing risk. Security investments can be justified by funding them based on the anticipated economic return and a cost-benefit analysis. A risk-based approach can optimize the return of security investments. Security depends on balancing cost and risk with the appropriate use of both technology and policy. Risk analysis methods show business partners and customers that the company has identified and assessed its risk exposure and made prudent security investments.

Businesses are vulnerable to disgruntled and corrupt employees, careless administrators, and hostile managers. Internal security breaches often occur from loyal employees acting carelessly or out of ignorance. Threats often defy technological safeguards and must be addressed by changing users' practices. In this course, you will explore technologies that validate and enforce compliance with policies, secure-use practices, and other business and legal requirements. The course explores defining and writing security policies and the implementation and maintenance of these policies that

focus on accountability by all users. Policy training and documentation are also essential to provide evidence that policies have been in force.

Grading Criteria

Section removed.

Academic Policies and Procedures

Section removed.

Project Descriptions

Article Summary

Find an article on Information Technology from any academic journal or trade journal. Summarize the article in your own words, and then describe how the article supports or differs from course material on the topic. The length will vary depending on the size of the article you choose; it will range from one to three pages. Article summaries should not exceed three pages and be doubled-spaced.

Web Site Analysis

Using the online resources posted in the conference area, you will select one of the reference sites and analyze the content of the Web material. The paper will include a discussion of:

1. Academic credibility of the site material
2. Applicability of the site material to a business organization
3. One item of interest to the student and the reason why
4. Will you use this site for reference? Why?

E-mail Policy Definition

Write an e-mail policy for your workplace, Beach's Trinkets (the hypothetical company in the modules or a university).

Course Schedule

Week	Readings/Assignments	Due Date
1	Volonino, chapter 1: Security in a Globally Connected Economy	
2	Volonino, chapter 2: Sources of Digital Liability	
3	Volonino, chapter 3: Threats, Vulnerabilities, and Risk Exposure Article Summary Due	
4	Volonino, chapter 4: An Affirmative Model of Defense: Digital Liability Management	
5	Volonino, chapter 5: Models for Estimating Risk and Optimizing the Return on Security Investment	
6	Volonino, chapter 5: Models for Estimating Risk and Optimizing the Return on Security Investment (continued)	
7	Midterm Exam	
8	Volonino, chapter 6: Acceptable Use Policies: Human Defense	
9	Volonino, chapter 7: Secure-Use Practices: Defensive Best Practices	
10	Volonino, chapter 7: Secure-Use Practices: Defensive Best Practices (continued) E-mail Policy Due	
11	Volonino, chapter 8: Technology and Auditing Systems: Hardware and Software Defenses	
12	Volonino, chapter 9: Electronic Evidence, Electronic Records Management, and Computer Forensics Web Site Analysis Due	
13	Volonino, chapter 10: Computer Crime, Computer Fraud, and Cyber Terrorism	
14	Volonino, chapter 11: Privacy and Data Protections	
15	Final Examination	