IS315
IS Risk Management and Intrusion Detection
[Onsite]

Course Description:

This course addresses concepts of risk management and intrusion detection. Areas of instruction include how to assess and manage risks to information security and identifying the activities involved in the process of information security risk management for an organization. The role of intrusion detection in information security and different tools used to detect intrusion will also be discussed.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IS311 Internetworking Infrastructure and Operations or equivalent, IS312 Information Security Essentials or equivalent

Credit hours: 4

Contact hours: 50 (30 Theory Hours, 20 Lab Hours)

SYLLABUS: IS Risk Management and Intrusion Detection

Instructor: _____

Office hours: _____

Class hours: _____

MAJOR INSTRUCTIONAL AREAS

1. Need for Information Security (IS) risk management
2. Risks in a project
3. Perform risk analysis
4. Threat and vulnerability analysis
5. Various security controls
6. Disaster recovery plan
7. Need for an Intrusion Detection or Prevention System (IDS/IPS)
8. Strengths and limitations of IDS/IPS
9. Types of IDS/IPS
10. Identification of the appropriate IDS/IPS for an organization
11. Deployment of an IDS/IPS on the network and on a host computer

©ITT Educational Services, Inc.

COURSE OBJECTIVES

After successful completion of this course, the student will have the opportunity to:

1. Explain the concepts of risk, threat, and vulnerability as they apply to information systems.
2. Appraise the value of organizational assets.
3. Examine the effect of threats and vulnerabilities on information systems.
4. Perform risk and impact analysis to determine the probable cost of risk exposure.
5. Perform a risk assessment and examine common risk management strategies.
6. Recommend appropriate IS security controls to secure an IS.
7. Analyze best practices to develop a proactive disaster recovery plan for an IS.
8. Describe various aspects of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
9. Examine the operation of common host-based IDS and IPS systems.
10. Apply system hardening techniques to provide host-based intrusion prevention.
11. Examine the need for a layered security solution.
12. Using the ITT Tech Virtual Library, research common security practices as they apply to information system risk management, business continuity, and IDS/IPS.

Related SCANS Objectives

1. Acquires security related data and evaluates it for the purpose of implementing risk management and intrusion detection for an organization.
2. Classifies risks in an orderly manner so that it can be processed further according to the specific requirements of the organization.
3. Interprets risks and effectively communicates the related information.

©ITT Educational Services, Inc.

4. Evaluates the risk information using computers.
5. Solves risk-related issues as a member of the team.
6. Evaluates a decision regarding security risks of the organization and other related problems through negotiation with others.
7. Identifies the knowledge of security requirements of the organization with the different tools used to detect intrusion.
8. Troubleshoots the problems related to the activities involved in the process of information security risk management for an organization.

TEACHING STRATEGIES

The curriculum is designed to promote a variety of teaching strategies that support the outcomes described in the course objectives and that foster higher cognitive skills. Delivery makes use of various media and delivery tools in the classroom.

COURSE RESOURCES

Student Textbook Package

- Panko, Raymond R., Kim, Gregg, M. Bishop, and Todd King, *IS Risk Management and Intrusion Detection, Indianapolis: Pearson Learning Solutions, 2006*

References and Resources

ITT Tech Virtual Library

Login to the ITT Tech Virtual Library (http://www.library.itt-tech.edu/) to access online books, journals, and other reference resources selected to support ITT Tech curricula.

- **General References**
  - **>Reference Resources>** National Vulnerability Database

- >**Program Links>** Information Systems Security (ISS)> Information Systems Security Association (ISSA)
- >**Program Links>** Information Systems Security (ISS)> Computer Security Institute
- >**Program Links>** Information Systems Security (ISS)> **Recommended Links >** CERT Coordination Center
- >**Program Links>** Information Systems Security (ISS)> **Recommended Links >** Common Vulnerabilities and Exposures
- >**Program Links>** Information Systems Security (ISS)> **Recommended Links >** SANS Institute Reading Room

- **Books**

The following books are related to this course and are available through the ITT Tech virtual Library:

- Books > Books 24x7 > CISSP: Certified Information Systems Security Professional Study Guide, Second Edition > Chapter 2: Attacks and Monitoring
- Books > Books 24x7 > CISSP: Certified Information Systems Security Professional Study Guide, Second Edition > Chapter 6: Asset Value, Policies, and Roles > Risk Management
- Books > Books 24x7 > CISSP: Certified Information Systems Security Professional Study Guide, Second Edition > Chapter 16: Disaster Recovery Planning
- Books > Books 24x7 > CIW Security Professional Certification Bible > Chapter 15: Intrusion Detection Systems
- Books > Books 24x7 > Intrusion Detection & Prevention > Chapter 1: Understanding Intrusion Detection
- Books > Books 24x7 > Intrusion Detection & Prevention > Chapter 6: IDS and IPS Architecture
- Books > Books 24x7 > PMP Project Management Professional Study Guide > Chapter 11: Introducing Project Risk Management
- Books > Books 24x7 > Proactive Risk Management

©ITT Educational Services, Inc.

- Books > Books 24x7 > Protect Your Information with Intrusion Detection > Chapter 8: The Life Cycle, Deployment, and Implementation of an IDS
- Books > Books 24x7 > Risk and Decision Analysis in Projects, Second Edition > Chapter 1: Risk and Decision Analysis
- Books > Books 24x7 > Security+ Study Guide, Second Edition (SYO-101) > Chapter 2: Identifying Potential Risks
- Books > Books 24x7 > Software Testing Fundamentals: Methods and Metrics > Chapter 9: Risk Analysis> Benefits of Risk Analysis
- Books > Books 24x7 > The Fundamentals of Risk Measurement

- Periodicals
  - **Periodicals>** INFORMATION SECURITY Magazine
  - **Periodicals>** IT Architect
  - **Periodicals >** IT Architect > The Threat From Within (August 01 2005 Issue)
  - **Periodicals >** IT Architect > Anomaly Detection On the Rise (June 01 2005 Issue)

- Other Resources
  - SecurityFocus Vulnerabilities List – (Offers user the ability to search for vulnerabilities by vendor, title, and version.) http://www.securityfocus.com/vulnerabilities
  - SecurityFocus BugTraq – (BugTraq is perhaps the most comprehensive list of vulnerabilities in existence. As soon as a vulnerability becomes public knowledge, it will be posted to BugTraq.) http://www.securityfocus.com/archive/1
  - SecurityFocus Focus on IDS - This is focused discussion Web forum for IDS. The majority of posters are industry professionals exchanging tips, tricks, and advise. http://www.securityfocus.com/archive/96

- CERT Vulnerabilities, Incidents, and Fixes – (CERT is now operated by the US department of Homeland security, making it a primary resource for advisory information about critical vulnerabilities.) http://www.cert.org/nav/index_red.html

- http://www.microsoft.com/security/

All links to web references outside of the virtual library are always subject to change without prior notice

---

EVALUATION & GRADING

COURSE REQUIREMENTS

1. **Attendance and Participation**

   Regular attendance and participation are essential for satisfactory progress in this course.

2. **Completed Assignments**

   Each student is responsible for completing all assignments on time.

3. **Team Participation (if applicable)**

   Each student is responsible for participating in team assignments and for completing the delegated task. Each team member must honestly evaluate the contributions by all members of their respective teams.

Evaluation Criteria Table

The final grade will be based on the following weighted categories:

CATEGORY	WEIGHT
Writing Assignments	10%
Participation	10%
Lab Assignments	15%
Quizzes	10%
Project 1	15%
Project 2	15%
Course Project	25%
Total	**100%**

Grade Conversion Table

Final grades will be calculated from the percentages earned in class as follows:

A	90 - 100%	4.0
B+	85 - 89%	3.5
B	80 - 84%	3.0
C+	75 - 79%	2.5
C	70 - 74%	2.0
D+	65 - 69%	1.5
D	60 - 64%	1.0

©ITT Educational Services, Inc.

F	<60%	0.0

COURSE OUTLINE

Readings:

- For all weeks, except unit 1, it is recommended that you complete the assigned readings before attending the class.
- **Unit 1**: All the concepts will be covered in the class, therefore, the specified readings are **merely for** your **reference**.

Unit #	Activities for the week

1	• **Read**
	  ○ **Chapter 1:** A Framework-(about 43 pages)
	  ○ **Chapter 1a:** Examples of Security Problems-(about 10 pages)
	• **In Class Discussion(s) #1 and #2**

2	• **Read** ○ **Chapter 1:** Understanding Firewalls (about 15-20 Pages) at ITT Tech Virtual Library>Books>Books 24x7>Firewalls 24Seven, Second Edition • **Lab #1** • **Quiz #1**
3	• **Read** ○ **Chapter 6:** Asset Value, Policies, and Roles-Risk Management > Risk Management (about 10 pages) at ITT Tech Virtual Library>Books>Books 24x7> CISSP: Certified Information Systems Security Professional Study Guide, Second Edition • **Start Project #1 and Submit Project #1 Part I**

4	• **Read** ○ **Chapter 4:** Vulnerability Analysis-(about 30 pages) ○ **Chapter 19**: Security Patching (About 10 Pages) at ITT Tech Virtual Library> Books>Books 24x7> Hardening Network Security • **In Class Discussion #1** • **Lab #1**
5	• **Read** ○ **Chapter 15:** Budget Acquisition and Corporate Commitment to Security-Perform a Risk Assessment (about 2 pages) at ITT Tech Virtual Library>Books>Books 24x7> Hardening Linux ○ **Chapter 3:** Risk Assessment Methodologies-(about 16 pages) ○ **Chapter 2:** Why Risk Assessment>Risk Assessment Best Practices-(about 10 pages) • **In Class Discussion #1** • **Continue Project #1 and Submit Project #1 Part II**
6	• **Read** ○ **Chapter 7:** Access Control and Site Security-(about 36 pages) ○ **Chapter 3:** Risk Assessment Methodologies-(about 3 pages) • **In Class Discussion #1** • **Writing Assignment #1**
7	• **Read** ○ **Chapter 15:** Business Continuity Planning-(about 15 pages) at ITT Tech Virtual Library>Books>Books 24x7> CISSP: Certified Information Systems Security Professional Study Guide, Second Edition ○ **Chapter 8:** Incident and Disaster Response-(about 9 pages) ○ **Chapter 16:** Disaster Recovery Planning-(about 15 pages) at ITT Tech Virtual Library>Books>Books 24x7> CISSP: Certified Information Systems Security Professional Study Guide, Second Edition • **In Class Discussion #1**

©ITT Educational Services, Inc.

	• **Writing Assignment #1** • **Lab #1** • **Start Project #2 and Submit Project #2**
8	• **Read** ○ **Chapter 9:** Intrusion Detection-(about 30 pages) ○ **Chapter 20:** Introduction to Intrusion Detection and Protection>IDS Evasive Techniques (About 3 Pages) at ITT Tech Virtual Library>Books>Books24x7> CISSP: Certified Information Systems Security Professional Study Guide, Second Edition ○ **Chapter 5:** Implementing and Maintaining a Secure Network-Hardening the OS and NOS, Hardening Network Devices, Hardening Applications (About 15 Pages) at ITT Tech Virtual Library>Books>Books24x7>Security+ Study Guide, Second Edition (SYO-101) • **In Class Discussion #1** • **Lab #1**
9	• **Read** ○ **Chapter 17:** The Future of Intrusion Detection and Prevention (about 9 pages) at ITT Tech Virtual Library>Books> Books24x7>Intrusion Detection & Prevention • **Quiz #1** • **Lab #1**
10	• **Read** ○ **Chapter 2:** Break the Network into Common Areas of Functionality for Security(About 25-30 Pages) at ITT Tech Virtual Library>Books>Books24x7>Hardening Network Security • **In Class Discussion #1** • **Lab #1 (Ungraded)**
11	**Course Project**

INTENT/INTERFACE

This course builds on the topics covered in the previous courses by providing students with a comprehensive understanding of risks pertaining to Information Systems (IS). Students will learn how to assess risks by measuring organizational assets and evaluating threats and vulnerabilities. This course provides students with the skills and real world knowledge to evaluate, install, and configure Intrusion Detection Systems (IDS). The inclusion of additional topics such as business and security controls will help the students to develop methodologies to manage and mitigate risk. These topics are critical for students to continue studies in the areas of security policy development and forensic investigation.

The purpose of this course is to provide students with an in-depth understanding about the concepts of risk management and the application of intrusion detection. Risk assessment and intruder detection are foundational IS security concepts, which are required to support advanced topics such as incident handling, security policy development, and forensic investigation. Students taking this course are expected to possess a rudimentary understanding of internetworking and essential information about security concepts.

©ITT Educational Services, Inc.