Lesson 8: Risk, Response, and Recovery

This Week's Learning Objective(s)

- Describe the principles of risk management, the common response techniques, and the issues related to recovery of IT systems.

Before Class Reading(s)

Prior to this session, students will have read:

- Chapter 8, "Risk, Response, and Recovery", *Fundamentals of Information Systems Security*

Due at the Beginning of Class

Collect the following assignments:

- Testing and Monitoring Security Controls
- Define an Acceptable Use Policy (AUP)

Lecture Topics

TASK	NOTES & DOCUMENTS
Deliver presentation	ppt15_108
Distribute text and worksheet(s)	[illegible] [illegible] mwch [illegible]

Review main concepts	• **Business continuity, disaster recovery, BIA, and incident response**
	  ○ BCP
	  ○ DRP
	  ○ BIA
	  ○ Computer incident response team (CIRT) plan
	• **Risk assessments**
	  ○ Overview of risk management
	  ○ Overview of risk assessment
	  ○ Steps for performing a risk assessment

	○ Principal differences between qualitative and quantitative assessments

In-Class Activities

Facilitate the following In-Class Activities following the lesson lecture. Assignment Sheets, handouts and answer keys can be accessed in the instructor portal where you received your Instructor Guide. The Discussion Rubric is found in appendix in this guide.

Class Discussion Ungraded, ground Graded, online/blended	**Small Group Discussions:** Facilitate small group discussions. Instruct groups to share their findings. • What calculations are needed for quantitative risk assessments? • How are qualitative risk assessments performed?
Role-Play Activity Ungraded, all modalities	**Computer Incident Response Team (CIRT) Roles** Facilitate a role-play activity by dividing students into groups and assigning each group a scenario. • Give students the work sheet "[illegible]". • Each group member should assume a CIRT role and state what actions they would take during outlined scenarios. • Each scenario should address the notification, response, and suggestions for recovery and follow-up.
Individual Project Graded, all modalities	**BCP, DRP, BIA, and Incident Response Plan Mix and Match** • Distribute student worksheet "[illegible]". • Students complete this assignment individually. • Students submit completed handout. **Instructor Answer Key:** [illegible]
In-Class Assignment Graded, all modalities	**Quantitative and Qualitative Risk Assessment Analysis** • Based on the previous assignments about Richman Investments, students should go through scenarios and complete the worksheet "[illegible]". **Instructor Answer Key:** [illegible]
In-class lab Graded, all modalities	**Perform Business Continuity Implementation Planning** • Facilitate the instructor demo and hands-on lab. • **Lab Location:** Instructor's Lab Manual

Quizzes

Advise the students if there is a quiz this week. If so, facilitate the quiz.

Review

Review and emphasize the following with students.

Key Concepts

- Quantitative and qualitative risk assessment approaches
- Business impact analysis (BIA)
- Business continuity plan (BCP)
- Disaster recovery plans (DRP)
- Elements of an incident response plan

Key Words

- Business Continuity Plan
- Business Impact Analysis
- Disaster Recovery Plan
- Incidence Plan
- Incidence Response
- Qualitative Risk Assessment
- Quantitative Risk Assessment
- Risk Assessment
- Risk Management
- Risk Mitigation

Homework Assignment(s): Quantitative and Qualitative Risk Assessment Analysis

- Description:
  - Completed worksheet on the quantitative and qualitative risk assessments for given scenarios.
- Objective(s) Covered:
  - Describe the principles of risk management, the common response techniques, and the issues related to recovery of IT systems.
- Due Date:
  - Beginning of Lesson 9
- Handouts:
  - [illegible]
- Grading Rubric(s):
  - Standard 1.1, 1.2, 1.3, 1.4, 1.5, 1.6 and 1.7 evaluation criteria; Evaluation of Student Learning section in manual

Class Reminders

Before the next session remind students to:

1. Read Chapter 9, "Cryptography"
2. Remind students that Quantitative and Qualitative Risk Assessment Analysis is due at beginning of Lesson 9
3. Remind students that Project Part 1: Multilayered Security Plan is due by the beginning of Lesson 12.

Lesson 14: Information Security Professional Certifications

This Week's Learning Objective(s)

- Describe popular information security certifications and their requirements.

Before Class Reading(s)

Prior to this session, students will have read:

- Chapter 14, "Information Security Professional Certifications", *Fundamentals of Information Systems Security*

Due at the Beginning of Class

Collect the following assignments:

- NA

Lecture Topics

TASK	NOTES & DOCUMENTS
Deliver presentation	ppt15_114

Review main concepts	• **Compliance**
	  ○ Information security certification
	  ○ Vendor-neutral certifications
	  ○ Vendor-specific certifications
	• **Steps to obtain an information security certification**
	  ○ Set goal
	  ○ Get experience
	  ○ Research/study
	  ○ Take test(s)
	  ○ Why some certification bodies require recertification of credentials

In-Class Activities

Facilitate the following In-Class Activities following the lesson lecture. Assignment Sheets, handouts and answer keys can be accessed in the instructor portal where you received your Instructor Guide. The Discussion Rubric is found in appendix in this guide.

Class Discussion Ungraded, ground Graded, online/blended	**Small Group Discussions:** Facilitate small group discussions, then instruct groups to share their findings.
	• Who does the DoD Directive 8570.01 "Information Assurance Training, Certification and Workforce Management" apply to? • In what situations is it required? • How does it differ from the new 8140 Standard? • In what situations is a vendor-neutral certification most applicable? • In what situations is vendor-specific certification most applicable?
In-Class Project Ungraded, all modalities	**The Certification Ladder** • Have students form small groups. • Each group should create a certification plan for a person who wants to become a high-ranking security manager. • The certification plan should include at least one entry-level, one intermediate, and one advanced certification.
Individual Project Graded, all modalities	**Project Part 2: SSCP® Domain Research Paper Work Session** • Refer students to access the online Candidate Information Bulletin • Remind students to consult "funsec_project" • Students should focus on writing a proposal to the senior management of Richman Investments based on the seven tasks provided.
In-class lab Graded, all modalities	• None

Quizzes

Advise the students if there is a quiz this week. If so, facilitate the quiz.

Review

Review and emphasize the following with students.

Key Concepts

- Popular vendor-neutral professional certifications
- Popular vendor-specific professional certifications
- The DoD/Military 8570.01 requirements

Key Words

- Vendor-Neutral Professional Security Certifications
- Vendor-Specific Professional Security Certifications
- DoD/Military 8570.01
- DoD/Military 8140