ISEC 300 FUPE Study Guide

Format

The exam consists of 11 pages of T/F, multiple choice, short answer, essay, and problems for 200 points. Passing is 80%. It is two hours in length and is closed book, and notes. For those students where English is a second language, a translation dictionary may be used.

Notes

This is a thorough exam, comparable to a final exam for the course. You will be expected to do to know a broad overview of security principles and practices as well as terminology, acronyms, examples, etc. Topics include intrusion detection and prevention, authentication, cryptography, physical security, security implementation, personnel, maintenance, policy and planning, and the CIA triad.

Recommended textbook

Whitman, M., & Mattord, H. (2011). Principles of Information Security. (4th ed.). Boston, MA: Course Technology. ISBN: 978-1-1111-3821-9.

Course Description

In a highly connected, data intensive, and cost-focused business environment, the practice of information security not a business advantage; it is a customer requirement. Viruses, malware, trojans, denial of service attacks, phishing, and even WikiLeaks have become headline news. Failure to ensure the confidentiality, integrity, and availability of data costs companies millions, if not billions, of dollars in legal settlements, lost business, and trade secrets. In this breadth-based course, you will get an overview of information security principles and practices, including security models, risk management, access controls, intrusion detection and prevention, cryptography, software vulnerabilities, and ethical issues. Subsequent courses expand on this foundational material in much greater depth.

Course Outcomes

1. Describe how availability, integrity, and confidentiality requirements affect a typical IT infrastructure.
2. Identify common sources of security breaches and their associated countermeasures.
3. Identify, manage, and mitigate risk as part of a security plan.
4. Describe, develop, and maintain appropriate access controls.
5. Create, maintain, and promote suitable security policies.
6. Apply auditing and monitoring techniques to assess security compliance.
7. Employ a business continuity plan to reduce risk.

8. Describe the key components of cryptographic systems.
9. Explore network security risks and layered defense mechanisms.
10. Identify key U.S. security standards and compliance laws.

Weekly Outcomes

Week 1

1. Define information security.
2. Define key terms and critical concepts of information security.
3. Enumerate the phases of the security systems development lifecycle.

Week 2

1. Demonstrate that organizations have a business need for information security.
2. Explain why a successful information security program is the responsibility of both general management and IT management.
3. Distinguish between threats and attacks.
4. Identify threats posed to information security and the more common attacks associated with those threats.

Week 3

1. Describe the functions of and relationships among laws, regulations, and professional organizations in information security.
2. Differentiate between laws and ethics.
3. Identify major national laws that affect the practice of information security.

Week 4

1. Define risk management, risk identification, and risk control.
2. Assess risk based on probability of occurrence and likely impact.
3. Describe the various risk mitigation strategy options.

Week 5

1. Define risk management, risk identification, and risk control.
2. Assess risk based on probability of occurrence and likely impact.
3. Describe the various risk mitigation strategy options.

Week 6

1. Define risk management, risk identification, and risk control.
2. Assess risk based on probability of occurrence and likely impact.
3. Describe the various risk mitigation strategy options.

Week 7

1. Exam week.

Week 8

1. Identify and describe the categories and operating models of intrusion detection and prevention systems.
2. Define and describe honeypots, honeynets, and padded cell systems.
3. List and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories

Week 9

1. Explain the basic principles of cryptography.
2. Describe the operating principles of the most popular cryptographic tools.
3. List and explicate the major protocols used for secure communications.
4. Discuss the nature and execution of the dominant methods of attack used against cryptosystems.

Week 10

1. Discuss the relationship between information security and physical security.
2. Describe key physical security considerations.
3. Identify critical physical environment considerations for computing facilities.

Week 11

1. Explain how an organization's information security blueprint becomes a project plan.
2. Enumerate the many organizational considerations that a project plan must address.
3. Describe technical strategies and models for implementing a project plan.

Week 12

1. Enumerate the credentials that information security professionals can earn to gain recognition in the field.
2. Identify the special security precautions that must be taken when using contract workers.
3. Explain the need for the separation of duties.

Week 13

1. List the recommended security management models.
2. Define a model for a full maintenance program.
3. Describe how planning, risk assessment, vulnerability assessment and remediation tie into information security maintenance.
4. Define digital forensics, and describe the management of the digital forensics function.

Week 14

1. Exam review.

Week 15

1. Exam week.