ISACA®
Trust in, and value from, information systems

CSX™
CYBERSECURITY NEXUS

Cybersecurity Fundamentals Online Course

Course Description

The Cybersecurity Fundamentals Online Course will provide learners with principles of data and technology that frame and define cybersecurity. Learners will gain insight into the importance of cybersecurity and the integral role of cybersecurity professionals. The interactive, self-guided format will provide a dynamic learning experience where users can explore foundational cybersecurity principles, security architecture, risk management, attacks, incidents, and emerging IT and IS technologies.

Learning Objectives:

- Explain the core information assurance (IA) principles
- Identify the key components of cybersecurity network architecture
- Apply cybersecurity architecture principles
- Describe risk management processes and practices
- Identify security tools and hardening techniques
- Distinguish system and application security threats and vulnerabilities
- Describe different classes of attacks
- Define types of incidents including categories, responses and timelines for response
- Describe new and emerging IT and IS technologies
- Analyze threats and risks within context of the cybersecurity architecture
- Appraise cybersecurity incidents to apply appropriate response
- Evaluate decision making outcomes of cybersecurity scenarios
- Access additional external resources to supplement knowledge of cybersecurity

Note

This course is not designed to cover all knowledge areas that will be tested in the Cybersecurity Fundamentals Certificate Exam. Therefore, it is recommended that you understand the following concepts prior to taking the exam:

- Security architecture principles and frameworks (i.e. SABSA, Zachman, TOGAF, etc.)

- OSI model

- TCP/IP

- General firewall features, types, issues, and platforms

- Networking (i.e. ports, protocols, VPNs, etc.)

•Application security

•Risk assessments

•Business continuity plans (BCP)

•BYOD

Target Audience

- Zero to three years cybersecurity experience
- Audit, risk, compliance, information security, government and legal professionals with a familiarity of basic IT/IS concepts who:
    - are new to cybersecurity
    - are interested in entering the field of cybersecurity
    - are interested in the ISACA Cybersecurity Fundamentals Certificate
- Students and recent grads

Course Outline

1. Introduction to Cybersecurity
    a. Cybersecurity objectives
    b. Cybersecurity roles
    c. Differences between Information Security & Cybersecurity
2. Cybersecurity Principles
    a. Confidentiality, integrity, & availability
    b. Authentication & nonrepudiation
3. Information Security (IS) within Lifecycle Management
    a. Lifecycle management landscape
    b. Security architecture processes
    c. Security architecture tools
    d. Intermediate lifecycle management concepts
4. Risks & Vulnerabilities
    a. Basics of risk management
    b. Operational threat environments
    c. Classes of attacks
5. Incident Response

   a. Incident categories
   b. Incident response
   c. Incident recovery

6. Future Implications & Evolving Technologies
   a. New & emerging IT & IS technologies
   b. Mobile security issues, risks, & vulnerabilities
   c. Cloud concepts around data & collaboration