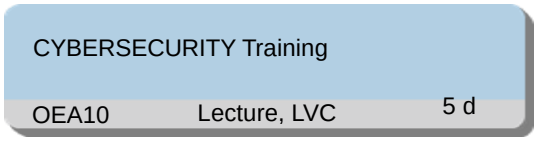
CYBER SECURITY TRAINING

Training Path



Target Audience

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

Objectives

On completion of this program, the participants will be able to:

- Explain the core information assurance (IA) principles
- Identify the key components of cyber security network architecture
- Apply cyber security 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 cyber security architecture
- Appraise cyber security incidents to apply appropriate response
- Evaluate decision making outcomes of cyber security scenarios
- Access additional external resources to supplement knowledge of cyber security

Training Content

1. Introduction to Cyber security
   - a. Cyber security objectives
   - b. Cyber security roles c. Differences between Information Security & Cyber security
2. Cyber security Principles
   - a. Confidentiality, integrity, & availability b. Authentication & non-repudiation
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