

CYBER SECURITY FUNDAMENTALS (CSX)

By ISACA®

Course: ISACA-CSXF | Instructor-led

Duration: 2 days

HRDF SBL Claimable

CSXF is an excellent way to gain foundational knowledge in cyber security and begin to build your knowledge and kick-start your career in this crucial area. CSX is designed to help fortify and advance the industry by educating, training and certifying a stronger, more informed workforce—from recent college graduates to C-suite level executives.

The entry point into our cyber security program, Cyber Security Fundamentals offers a certificate in the introductory concepts that frame and define the standards, guidelines and practices of the industry. The certificate and related training are an ideal way to get started on a career in cyber security. These skills are in high demand, as threats continue to plague enterprises around the world.

The Certificate is aligned with the National Institute of Standards and Technology (NIST) National Initiative for Cyber Security Education (NICE), which is compatible with global cyber security issues, activities and job roles. The Certificate is also aligned with the Skills Framework for the Information Age (SFIA).

AUDIENCE

- ▶ College/university students and recent graduates, those new to the field, as well as those looking to change careers.
- ▶ C-suite level executives.
- ▶ Professionals in related Information technology roles needing to understand more about cyber security concepts.
- ▶ It is also an excellent resource for professionals in the field looking for a cyber security refresher course.

PREREQUISITES

- ▶ College/university graduates.

LEARNING OBJECTIVES

- ▶ 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 information technology and information security 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.

Copyright @ LGMS Academy 2018 | 191118

COURSE OUTLINE

Module 1: Introduction to Cyber Security

- ▼ Cyber security objectives
- ▼ Cyber security roles
- ▼ Differences between information security & cyber security

Module 2: Cyber Security Principles

- ▼ Confidentiality, integrity, availability
- ▼ Authentication & non-repudiation

Module 3: Information Security (IS) within Lifecycle Management

- ▼ Lifecycle management landscape
- ▼ Security architecture processes
- ▼ Security architecture tools
- ▼ Intermediate lifecycle management concepts

Module 4: Risk & Vulnerabilities

- ▼ Basics of risk management
- ▼ Operational threat environments
- ▼ Classes of attacks

Module 5: Incident Response

- ▼ Incident categories
- ▼ Incident response
- ▼ Incident recovery

Module 6: Future Implications & Evolving Technologies

- ▼ New & emerging information technology & information security technologies
- ▼ Mobile security issues, risks & vulnerabilities
- ▼ Cloud concepts around data & collaboration

General Information

- ▼ Instructor Led-Workshop
- ▼ One (1) Examination Token
- ▼ Course Material

CSXF Examination

- ▼ Online
- ▼ Closed-book
- ▼ Remotely-proctored exam
- ▼ Results are immediate
- ▼ 75 MCQs
- ▼ Duration: 2 hours
- ▼ Passing score: 65%

It covers 5 domains:

1. Cyber Security Concepts
2. Cyber Security Architecture Principles
3. Security of networks, systems, applications and data
4. Incident Response
5. Security Implications and Adoption of Evolving Technology

The Cyber Security Fundamentals Certificate does not have an expiration date.

You may purchase the exam again if you do not pass the exam. There is no limit on number of times you can take the exam. Each exam fee is 150 USD.

For details regarding the exam, including hardware and software requirements, download the complimentary exam guide; http://www.isaca.org/cyber/Documents/CSX-Exam-Guide_bro_Eng_1014.pdf