CSXF: ISACA Cybersecurity Fundamentals Certificate

Course Code: CSXF
Duration: 3 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Learn, train and grow with Cybersecurity Fundamentals.

As the cyber landscape continues to evolve rapidly, it is not enough to rely solely on knowledge and theory. Cybersecurity Fundamentals training is a performance-based testament to your real-life skills and experience and proclaims that your commitment, tenacity, and abilities exceed expectations. This course is a comprehensive understanding of Cybersecurity's key concepts, the impacts on your business, and the integral role of a cybersecurity professional in protecting enterprise data and infrastructure.

Cybersecurity 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 Cybersecurity. These skills are in high demand as threats continue to plague enterprises around the world. This knowledge-based certificate can enable you to:

- Demonstrate your understanding of the principles that frame and define Cybersecurity and the integral role of cybersecurity professionals in protecting enterprise data.
- Add a credential to your resume/CV that will distinguish you from other candidates for advancement or a new job.
- Stay ahead of the curve on your current career path or start your new cybersecurity career strong.

The purpose of the ISACA® Cybersecurity Fundamentals qualification is to measure whether a candidate has sufficient knowledge and understanding of the key concept principles by defining Cybersecurity and the integral role of cybersecurity professionals in protecting cyber assets in the modern world.

SKILLS COVERED

The Cybersecurity Fundamentals training provides a dynamic learning experience where you'll learn to:

- Explain cybersecurity concepts.
- Define enterprise cybersecurity roles and responsibilities.
- Identify the main components of telecommunications technologies.
- Identify differences between information technology systems and specialized systems.
- Explain defense in depth.
- Describe common causes of enterprise service disruption.
- Identify the key components of security architecture.
- Describe risk management processes and practices.
- Appraise cybersecurity incidents to apply appropriate responses.
- Recognize system life cycle management principles, including software security and usability.
- Analyze threats and risks within the context of the cybersecurity architecture.
- Evaluate decision-making outcomes of cybersecurity scenarios.

WHO SHOULD ATTEND?

The Cybersecurity Fundamentals Certificate is intended for a wide-range of individuals, including:

- Those new to IT, students, recent graduates and career changers.
- Audit, risk, security and governance professionals looking to gain base-line IT knowledge and skills.
- Current IT Professionals looking to reskill or upskill to broaden their IT knowledge and skills or keep up-to-date.

PREREQUISITES

There are no prerequisites required to attend this course.

MODULES

Module 1: Introduction to Cybersecurity

Learning Objectives

- Identify and explain cybersecurity concepts.
- Identify main components of telecommunications technologies.
- Differentiate types of security.

Topics

- Overview
- What is Security?
- Types of Security

Module 2: Cybersecurity and Privacy

Learning Objectives

- Identify differences between information technology systems and specialized systems.
- Discuss enterprise cybersecurity roles and responsibilities.
- Define governance, risk management and compliance (GRC).
- Distinguish between privacy and security.

Topics

- Specialized Systems
- Roles and Responsibilities
- Governance, Risk Management and Compliance
- Cybersecurity Governance
- Privacy
- Privacy vs. Security

Module 3: Service Disruption and Cybersecurity

Learning Objectives

- Identify and discuss common causes of enterprise service disruption.
- Explain business continuity planning.
- Describe the relationship between business continuity planning (BCP) and disaster recovery (DR).

Topics

- Resilience

- Business Continuity and Disaster Recovery
- Business Impact Analysis
- Recovery Concepts

Module 4: Threat Landscape

Learning Objectives

- Identify and discuss common causes of enterprise service disruption.
- Explain business continuity planning.
- Describe the relationship between business continuity planning (BCP) and disaster recovery (DR).

Topics

- Specialized Systems
- Roles and Responsibilities
- Governance, Risk Management and Compliance
- Cybersecurity Governance
- Privacy
- Privacy vs. Security

Module 5: Cyberattacks

Learning Objectives

- Identify and explain cybersecurity concepts.
- Identify main components of telecommunications technologies.
- Differentiate types of security.

Topics

- Attack Attributes
- Attack Process
- Malware and Attacks

Module 6: Risk Mitigation

Learning Objectives

- Identify differences between information technology systems and specialized systems.
- Discuss enterprise cybersecurity roles and responsibilities.
- Define governance, risk management and compliance (GRC).
- Distinguish between privacy and security

Topics

- Risk Assessment
- Supply Chain Considerations
- Risk Management Life Cycle
- Managing Risk
- Using the Results of Risk Assessments

Module 7: Securing Assets

Learning Objectives

- Identify differences between information technology systems and specialized systems.
- Discuss enterprise cybersecurity roles and responsibilities.
- Define governance, risk management and compliance (GRC).
- Distinguish between privacy and security.

Topics

- Risk Identification, Standards, Frameworks and Industry Guidance
- Endpoint Security
- System Hardening
- Logging, Monitoring and Detection
- Data Security

Module 8: Security Architecture

Learning Objectives

- Identify components of a security architecture.
- Compare security models.

Topics

- Architecture, Models, and Frameworks

Module 9: Security Controls

Learning Objectives

- Explain defense in depth.
- Compare traditional security and assume-breach philosophies.
- Identify three main types of security controls.
- Distinguish types of logical access controls.
- Identify and explain types of administrative controls.
- Explain each component of authentication, authorization and accounting (AAA).

Topics

- Security Controls

Module 10: Network Security

Learning Objectives

- Explain methods to achieve isolation and segmentation.
- Identify network security hardware.
- Distinguish types of firewalls.

Topics

- Network Security

Module 11: Application and Cloud Security

Learning Objectives

- Recognize system life cycle management principles, including software security and usability.
- Identify and analyze cloud service models.
- Discuss risk associated with cloud computing.

Topics

- Application Security
- Cloud Security

Module 12: Software Management and Encryption

Learning Objectives

- Identify elements of cryptographic systems.
- Identify and discuss key systems.

Topics

- Configuration Management
- Change Management
- Patch Management
- Encryption Fundamentals, Techniques and Applications

Module 13: Introducing Security Operations

Learning Objectives

- Discuss security operations center (SOC) deployment models.
- Identify common SOC functions, roles and responsibilities.
- Identify vulnerability assessment tools, including open source tools and their capabilities.

Topics

- Security Operations

Module 14: Testing Technologies and Security Tools

Learning Objectives

- Differentiate vulnerability scanning and penetration testing.
- Discuss common phases of penetration testing.
- Identify and use common cybersecurity tools.
- Discuss components that aid cybersecurity monitoring and detection.

Topics

- Tool and Technologies (Monitoring, Detection, Correlation)
- Forensics

Module 15: Handling Security Incidents

Learning Objectives

- Understand incident response and handling methodologies.
- Distinguish between an event and an incident.
- Discuss the elements of an incident response plan (IRP).

Topics

- Incident Handling

Practice Labs

- SQL Injection
- Windows Event Monitoring & Defender
- Threat Removal
- Threat Detection
- File Permissions on Windows and Linux
- Forensics: File Recovery, Baselining with Lynis
- Scanning Ports and Utilizing SSH
- Windows and Linux OS Firewalls

END OF PAGE