ISACA® Cybersecurity Fundamentals

Duration: 2 Days
Method: Instructor-Led Training (ILT) | Live Online Training

Certification: ISACA® Cybersecurity Fundamentals Certificate
NOTE: This certificate awards approximately ONE (1) hour of
CPE for every ONE (1) hour of instructor-led training.

Course Description

This course offers participants an introduction to cybersecurity, a rapidly evolving field that is becoming crucial for business continuity, job security, and national safety. It provides a foundational overview of cybersecurity, focusing on essential topics such as network security, risk management, cryptography, and incident response. Through hands-on labs and real-world scenarios, participants will learn to identify threats, implement defence strategies, and respond to security incidents. The course aims to build a strong base for further cybersecurity studies or certifications.

Target Audience

This course 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

To attend this course, candidates must have:
- Basic Computer Literacy such as:
  o Navigating common operating systems like Windows and macOS, with a basic understanding of Linux.
  o Browsing the internet, use email, and grasp basic knowledge of networking concepts such as IP addresses, Wi-Fi, and firewalls.
  o Proficiency in using common applications, and basic file management.
  o General awareness of security concepts like malware, and phishing.

Tel: 876-978-1107 / 876-978-1486
WhatsApp: 876-978-9353
E-Mail: training@RWTTS.com | **Website:** www.RWTTS.com

Microsoft Partner

Exam Details

Length of Exam:	• 2 Hours
Number of Questions:	• 48
Passing Score:	• 65%
Question Format:	• Multiple Choice and Performance-Based
Exam Format:	• Online Via Remote Proctoring

Course Objectives

Upon successful completion of this course, attendees will be able 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 defence 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 response.
- Recognize system life cycle management principles, including software security and usability.
- Analyse threats and risks within context of the cybersecurity architecture.
- Evaluate decision-making outcomes of cybersecurity scenarios.

Course Topics

Module 1: Introduction to Cybersecurity
- Overview
- What is Security?
- Types of Security

Module 2: Cybersecurity and Privacy
- Specialized Systems
- Roles and Responsibilities
- Governance, Risk Management and Compliance
- Cybersecurity Governance
- Privacy
- Privacy vs. Security

Module 3: Service Disruption and Cybersecurity
- Resilience
- Business Continuity and Disaster Recovery
- Business Impact Analysis
- Recovery Concepts

Module 4: Threat Landscape
- Specialized Systems
- Roles and Responsibilities
- Governance, Risk Management and Compliance
- Cybersecurity Governance
- Privacy
- Privacy vs. Security

Module 5: Cyberattacks
- Attack Attributes
- Attack Process
- Malware and Attacks

Module 6: Risk Mitigation
- Risk Assessment
- Supply Chain Considerations
- Risk Management Life Cycle
- Managing Risk
- Using the Results of Risk Assessments

Module 7: Securing Assets
- Risk Identification, Standards, Frameworks and Industry Guidance
- Endpoint Security
- System Hardening
- Logging, Monitoring and Detection
- Data Security

Module 8: Security Architecture
- Architecture, Models, and Frameworks

Module 9: Security Controls
- Security Controls

Module 10: Network Security
- Network Security

Module 11: Application and Cloud Security
- Application Security
- Cloud Security

Module 12: Software Management and Encryption
- Configuration Management
- Change Management
- Patch Management
- Encryption Fundamentals, Techniques and Applications

Tel: 876-978-1107 / 876-978-1486
WhatsApp: 876-978-9353
E-Mail: training@RWTTS.com | **Website:** www.RWTTS.com

Microsoft Partner

Course Topics *Continued*

Module 13: Introducing Security Operations
- Security Operations

Module 14: Testing Technologies and Security Tools
- Tool and Technologies (Monitoring, Detection, Correlation)
- Forensics

Module 15: Handling Security Incidents
- Incident Handling

LABS INCLUDED