Cyber Security Audit Certificate Training

Duration: **2 Day**

BILGINC IT Academy
info@bilginc.com
bilginc.com

ISACA's Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits. It provides security professionals with an understanding of the audit process, and IT risk professionals with an understanding of cyber-related risk and mitigating controls.

The Cybersecurity Audit Certificate is a comprehensive course designed to help individuals prepare for the Cybersecurity Audit Certificate exam and to understand risk and implement controls to better protect against cyber threats.

The Cybersecurity Audit Certificate exam and manual are organised within four high-level domains:

Cybersecurity and Audit's Role

Cybersecurity Governance

Cybersecurity Operations

Cybersecurity Technology Topics

These domains are the result of extensive research and feedback from subject matter experts from around the world.

Prerequisites

You do not need any prerequisites for this accelerated course. However, ISACA recommends that you have a basic understanding of cyber security concepts and previous experience within the industry.

Cyber Security Audit Certificate Training

Duration: **2 Day**

BILGINC
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

With the increasing number of cyberthreats, it is becoming critical for audit plans to include cybersecurity. ISACA's Cybersecurity Audit Certificate Program provides audit/assurance professionals with the knowledge needed to excel in cybersecurity audits, and IT risk professionals with an understanding of cyber-related risk and mitigating controls.

- Understand Security Frameworks to Identify Best Practices
- Define threat and vulnerability management
- Assess threats with the help of vulnerability management tools
- Build and deploy secure authorization processes
- Explain all aspects of cybersecurity governance
- Distinguish between firewall and network security technologies
- Enhance asset, configuration, change and patch management practices
- Manage enterprise identity and information access
- Identify application security control
- Identify cyber and legal regulatory requirements to aid in compliance assessments
- Identify weaknesses in cloud strategies and controls
- Perform cybersecurity and third-party risk assessments
- Identify the benefits and risks of containerization