IS20 Security Controls

Modality: On Demand

Duration: 3 Hours

About this course:

The IS20 Security Controls course covers methodologies and proven general controls that were used in the execution and analysis of the Top Twenty Most Critical Security Controls. This course is intended for security professionals who are looking forward to learning about the implementation of highly competent and economical automation techniques for enhancing controls in the existing systems to make them more secure. Through the IS20 Security Controls course, an individual can learn about assessing security controls and comparing it with industry standards.

The average salary for Information Assurance Manager is **$83,443** per year**.**

Course Objective:

The objectives of the IS20 Security Controls course is to enable individuals to implement the Top 20 Most Critical Security Controls.

Audience:

Following can take up the IS20 Security Controls course.

- Network Security Engineers
- IT Administrators
- Information Assurance Managers/Auditors

Prerequisites:

- Basic Knowledge of network and security technologies.

Suggested prerequisites courses:

- LFS211 - Linux Networking and Administration
- Certified Security Leadership Officer

Course Outline:

- Module 01 - Inventory of Authorized and Unauthorized Devices
- Module 02 - Inventory of Authorized and Unauthorized Software
- Module 03 - Secure Configurations for Hardware and Software on Laptops, Workstations and Servers
- Module 04 - Secure Configurations for Hardware Network Devices such as Firewalls, Routers and Switches
- Module 05 - Boundary Defense
- Module 06 - Maintenance, Monitoring, and Analysis of Audit Logs
- Module 07 - Application Software Security
- Module 08 - Controlled Use of Administrative Privileges
- Module 09 - Controlled Access Based on Need to Know
- Module 10 - Continuous Vulnerability Assessment and Remediation
- Module 11 - Account Monitoring and Control
- Module 12 - Malware Defenses
- Module 13 - Limitation and Control of Network Ports, Protocols and Services
- Module 14 - Wireless Device Control
- Module 15 - Data Loss Prevention
- Module 16 - Secure Network Engineering
- Module 17 - Penetration Tests and Red Team Exercises
- Module 18 - Incident Response Capability
- Module 19 - Data Recovery Capability
- Module 20 - Security Skills Assessment and Appropriate Training to Fill Gaps