IS20 Security Controls

Modality: On Demand

Duration: 3 Hours

About this course:

We know that what Security Controls is. Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. This intermediate level course covers proven general controls and methodologies that are used to execute and analyze the Top Twenty Most Critical Security Controls. This course allows the security professional to see how to implement controls in their existing network(s) through highly effective and economical automation. For management, this training is the best way to distinguish how you'll assess whether these security controls are effectively being administered. Nearly all organizations containing sensitive information are adopting and implementing the most critical security controls as the highest priority list. These controls were chosen by leading government and private organizations who are experts on how compromised networks/systems evolve and how to mitigate and prevent them from happening. This course helps the students in the preparation for IS20 Certification Exam.

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

Course Objective:

After completing this course, students will be able to:

- Implement the top 20 most critical controls in the work place.

Audience:

This course is intended for:

- Information assurance managers/auditors
- Network security engineers
- IT administrators

Prerequisites:

- A basic understanding of networking 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