IS 20
Security Controls

Overview
Mile2®'s vendor-neutral IS20 Controls certification 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 or if they are falling short of industry standards. Nearly all organizations containing sensitive information are adopting and implementing the most critical security controls as the highest priority list.

Upon Completion
Upon completion, the IS20 Security Controls candidate will be able to not only competently take the IS20 Controls exam but will also have an understanding of how to implement the top 20 most critical controls in the workplace.

Course Length
3 days

Format
- Instructor-led classroom
- Instructor-led Online Training

Prerequisites
- A basic understanding of networking and security technologies

Student Materials
- Student Workbook
- Exam Prep Exam Guide

Who Should Attend?

- Information assurance managers/auditors
- System implementers/administrators
- Network security engineers
- IT administrators
- Auditors/auditees
- DoD personnel/contractors
- Federal agencies/clients
- Security vendors and consulting groups looking to stay current with frameworks for information assurance

Course Contents

- 0.Course Introduction
- I.Critical Control 1: Inventory of Authorized and Unauthorized Devices
- II. Critical Control 2: Inventory of Authorized and Unauthorized Software
- III. Critical Control 3: Secure Configurations for Hardware and Software on
- IV. Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- V. Critical Control 5: Boundary Defense
- VI. Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs Network Ports, Protocols, and Services
- VII. Critical Control 7: Application Software Security
- VII. Critical Control 8: Controlled Use of Administrative Privileges
- IX. Critical Control 9: Controlled Access Based on Need to KNow
- X. Critical Control 10: Continuous Vulnerability Assessment and Remediation
- XI. Critical Control 11: Account Monitoring and Control
- XII. Critical Control 12: Malware Defenses
- XIII. Critical Control 13: Limitation and Control of
- XIV. Critical Control 14: Wireless Device Control
- XV. Critical Control 15: Data Loss Prevention
- XVI. Critical Control 16: Secure Network Engineering

- XVII. Critical Control 17: Penetration Tests and Red Team Exercises
- XVIII. Critical Control 18: Incident Response Capability
- XIX. Critical Control 19: Data Recovery Capability
- XX. Critical Control 20: Security Skills Assesment and Appropriate Training to Fill Gaps
- Gaps