

# ISSC – Top 20 Information Systems Security Controls

## KEY DATA

**Course Name:** General Security – Top 20 Information Systems Security Controls

Maps to SANS Security 440 & ISC2 CAP (Certification and Accreditation Professional)

**Certification Track:**  
Mile2's ISSC (Information Systems Security Controls) & ICS2 CAP

**Duration:** 2-3 days

**Language:** English

**Format:**

Instructor-led  
Live Virtual Training

**Prerequisites:**

- A basic understanding of networking and security technologies

**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 OVERVIEW

This course covers proven tools and methodologies needed to execute and analyze the Top Twenty Most Critical Security Controls. Nearly all organizations containing sensitive information are adopting these Security Controls, listed below, as the highest priority list of what must be substantiated before anything else.

These controls were chosen by leading government and private organizations who are experts on how attacks work and what can be done to prevent them from happening. The controls were selected as the best way to block known attacks as well as help search for and alleviate any damage from the attacks that are successful. This course allows the security professional to see how to implement controls in your existing network through highly effective and economical automation. For management, this training is the best way to distinguish how you will assess whether these security controls are effectively being administered.

## UPON COMPLETION

Upon completion, students will be able to confidently undertake the ISC2 CAP and SANS Security 440 certification examination. Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security environment. This course offers up-to-date proprietary laboratories and case studies that have been researched and developed by leading security professionals from around the world.

**Also available as:**

### LIVE ON-LINE REMOTE TRAINING

**Attend live class from anywhere in the world!**

- Live Presentations with Powerful functionality that delivers easy viewing of slides and other documents, shared Internet access, virtual whiteboard, and a media center all through an easy-to-use toolbar.
- Application, file, and desktop sharing enable you to view live demonstrations.
- Dedicated high spec remote PC per student with full access as if you are sitting in-front of the PC in the classroom.
- Instructor views each students session when you perform your hands on labs, the instructor can access your remote system to demonstrate and assist while you sit back to absorb the classroom style mentoring you expect.
- Public and private text chat allows for increased interactivity between students and instructor

## DETAILED MODULE DESCRIPTION

- I. Course Introduction
- II. Critical Control 1: Inventory of Authorized and Unauthorized Devices
- III. Critical Control 2: Inventory of Authorized and Unauthorized Software
- IV. Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- V. Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- VI. Critical Control 5: Boundary Defense
- VII. Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
- VIII. Critical Control 7: Application Software Security
- IX. Critical Control 8: Controlled Use of Administrative Privileges
- X. Critical Control 9: Controlled Access Based on Need to Know
- XI. Critical Control 10: Continuous Vulnerability Assessment and Remediation
- XII. Critical Control 11: Account Monitoring and Control
- XIII. Critical Control 12: Malware Defenses
- XIV. Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services
- XV. Critical Control 14: Wireless Device Control
- XVI. Critical Control 15: Data Loss Prevention
- XVII. Critical Control 16: Secure Network Engineering
- XVIII. Critical Control 17: Penetration Tests and Red Team Exercises
- XIX. Critical Control 18: Incident Response Capability
- XX. Critical Control 19: Data Recovery Capability
- XXI. Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps