SEC566: Implementing and Auditing the Critical Security Controls – In-Depth

GCCC
Critical Controls
giac.org/gccc

5	30	Laptop
Day Program	CPEs	Required

You Will Be Able To

- Apply a security framework based on actual threats that is measurable, scalable, and reliable in stopping known attacks and protecting organizations' important information and systems
- Understand the importance of each control and how it is compromised if ignored, and explain the defensive goals that result in quick wins and increased visibility of networks and systems
- Identify and utilize tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Understand how the Critical Controls map to standards such as NIST 800-53, ISO 27002, the Australian Top 35, and more
- Audit each of the Critical Security Controls, with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS).

As threats evolve, an organization's security should too. To enable your organization to stay on top of this ever-changing threat scenario, SANS has designed a comprehensive course that teaches students the Critical Security Controls, a prioritized, risk-based approach to security. Designed by private and public sector experts from around the world, the Controls are the best way to block known attacks and mitigate damage from successful attacks. They have been adopted by the U.S. Department of Homeland Security, state governments, universities, and numerous private firms.

The Controls are specific guidelines that CISOs, CIOs, IGs, systems administrators, and information security personnel can use to manage and measure the effectiveness of their defenses. They are designed to complement existing standards, frameworks, and compliance schemes by prioritizing the most critical threat and highest payoff defenses, while providing a common baseline for action against risks that we all face.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle. The British government's Center for the Protection of National Infrastructure describes the Controls as the "baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence."

SANS' in-depth, hands-on training will teach you how to master the specific techniques and tools needed to implement and audit the Critical Controls. It will help security practitioners understand not only how to stop a threat, but why the threat exists, and how to ensure that security measures deployed today will be effective against the next generation of threats.

The course shows security professionals how to implement the Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

> **"SEC566 provides great tools, explanation, and insight!"**
>
> — Ryan LeVan, **Trex Company, Inc.**

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast

Section Descriptions

SECTION 1: Introduction and Overview of the 20 Critical Controls

Section 1 will introduce you to all of the Critical Controls, laying the foundation for the rest of the class. For each Control, we will follow the same outline covering the following information:

- Overview of the Control
- How It Is Compromised
- Defensive Goals
- Quick Wins
- Visibility & Attribution
- Configuration & Hygiene
- Advanced
- Overview of Evaluating the Control
- Core Evaluation Test(s)
- Testing/Reporting Metrics
- Steps for Root Cause Analysis of Failures
- Audit/Evaluation Methodologies
- Evaluation Tools
- Exercise to Illustrate Implementation or Steps for Auditing a Control

In addition, Critical Controls 1 and 2 will be covered in depth.

TOPICS: Critical Control 1: Inventory of Authorized and Unauthorized Devices; Critical Control 2: Inventory of Authorized and Unauthorized Software

SECTION 2: Critical Controls 3, 4, 5, and 6

TOPICS: Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers; Critical Control 4: Continuous Vulnerability Assessment and Remediation; Critical Control 5: Controlled Use of Administrative Privileges; Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs

SECTION 3: Critical Controls 7, 8, 9, 10, and 11

TOPICS: Critical Control 7: Email and Web Browser Protections; Critical Control 8: Malware Defenses; Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services; Critical Control 10: Data Recovery Capability (validated manually); Critical Control 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

SECTION 4: Critical Controls 12, 13, 14, and 15

TOPICS: Critical Control 12: Boundary Defense; Critical Control 13: Data Protection; Critical Control 14: Controlled Access Based on the Need to Know; Critical Control 15: Wireless Device Control

SECTION 5: Critical Controls 16, 17, 18, 19, and 20

TOPICS: Critical Control 16: Account Monitoring and Control; Critical Control 17: Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually); Critical Control 18: Application Software Security; Critical Control 19: Incident Response and Management (validated manually); Critical Control 20: Penetration Tests and Red Team Exercises (validated manually)

Who Should Attend

- Information assurance auditors
- System implementers or administrators
- Network security engineers
- IT administrators
- Department of Defense personnel and contractors
- Staff and clients of federal agencies
- Private sector organizations looking to improve information assurance processes and secure their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC/AUD440, SEC401, SEC501, SANS Audit classes, and MGT512

> **"This course is providing me with the necessary context to understand the Critical Security Controls in depth, and further helping me understand how to present recommendations to our business owners."**
>
> — Chris Harper, **Centrus Energy**

Course Preview
available at: **sans.org/demo**