SANS The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SEC566: **Implementing and Auditing CIS Controls**

GCCC
Critical Controls
giac.org/gccc

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Apply security controls based on actual threats that are measurable, scalable, and reliable in stopping known attacks and protecting your organization's important information and systems
- Understand the importance of each control and how it is compromised if ignored
- Explain the defensive goals that result in quick wins and increased visibility of network and systems
- Identify and use tools that implement controls through automation
- Create a scoring tool to measure the effectiveness of each control
- Employ specific metrics to establish a baseline and measure the effectiveness of security controls
- Competently map CIS Controls to compliance and standards such as PCI-DSS, the NIST Cybersecurity Framework (CSF), ISO 27000, and more
- Audit each of the CIS Controls with specific, proven templates, checklists, and scripts provided to facilitate the audit process

Business Takeaways

- Efficiently reduce the most important cyber-related risks
- Align compliance requirements with security and business goals and solutions
- Report the status of cybersecurity defense efforts to senior leadership in clear, business terms
- Enjoy peace of mind that your organization has a comprehensive strategy for defense and compliance

What are CIS Controls?

The CIS Controls (formerly known as Critical Security Controls) are a recommended set of prioritized cyber defense best practices. They provide specific and actionable ways to protect against today's most pervasive and dangerous attacks. SANS provides CIS Controls v8 training, research, and certification. Version 8, released in May 2021, is a Change to the Entire Controls Ecosystem and provides backwards compatibility with previous versions and a migration path for users of prior versions to move to v8. Whether you use the CIS Controls or another control framework to guide your security improvement program, it is critical to understand that a controls list is simply a starting point. With the release of version 8, CIS added new tools and guides to the CIS controls ecosystem to help organizations:

- Implement, track, measure, and assess controls
- Prioritize controls based on evolving threats
- Justify investment in CIS Controls implementation
- Implement CIS Controls best practices for mobile devices and applications
- Apply CIS Controls best practices to cloud environments
- Comply with multiple frameworks by providing a map of regulatory frameworks

Organizations need to defend their information systems and there are many solutions, requirements and tools to navigate. Which solutions should be implemented first? What will reduce the most risk and defend against the most common attacks? SANS and CIS have mapped the most common and likely threats and attacks to a prioritized list of mitigations called the CIS Controls. These controls are regularly reviewed to ensure they continue to mitigate the the ever-evolving threat and surface-area landscape. By following the CIS Controls, organizations will reduce cyber risk, measure, and report on residual risk.

SEC566 will enable you to master the specific and proven techniques and tools needed to implement and audit the controls defined in the Center for Internet Security's (CIS) Controls. Students will gain direct knowledge of the CIS Controls and ecosystem of tools to implement CIS controls across organizations complex networks, including cloud assets and third-party risk. Additional tools to measure both CIS Control coverage as well as assess risk throughout the program will be provided. This in-depth, hands-on critical security controls training will teach security practitioners to 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. SEC566 shows security professionals how to implement the CIS Controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, this course is the best way to understand how you will measure cybersecurity control effectiveness. In addition, CIS Controls are mapped to other frameworks to ensure compliance as well as security leveraging the CIS Controls.

> **"All week long I have been noting the topics and items I want to bring back to my team to improve various operations. This content is perfectly aligned with the work I am doing. So yes, this was an excellent course."**
>
> —Thad Zeitler, **Athena Health**

sans.org/sec566

- Watch a preview of this course
- Discover how to take this course: Online, In-Person

Section Descriptions

SECTION 1: Introduction and Overview of the CIS Controls

Students will learn the background and context for Version 8 of the CIS Controls. In addition, students will learn about the ecosystem of tools and resources to implement, measure, assess and report on the security program. These foundational concepts are key to prioritizing implementation of controls to address the ever-changing threat landscape. Focus will be placed on the evolving network landscape and how to apply the CIS Controls in modern environments, including cloud and IoT technologies. Students will learn how to prioritize control implementation based on CIS Implementation Groups.

In this first course section we will establish baseline knowledge of key terms used in the defensive domains. In addition, we will take a deep dive into cover Control #1, the Inventory and Control of Enterprise Assets. Any time a new device is installed on a network, there are risks of exposing the network to unknown vulnerabilities or hampering its operation. Malicious code can take advantage of new hardware that is not configured and patched with appropriate security updates at the time of installation. Attackers can use these vulnerable systems to install backdoors before they are hardened. In automating CIS Control #1, it is critical that all devices be included in an accurate and up-to-date inventory control system. Any device not in the database should not be allowed to be connected to the network. Some organizations maintain asset inventories by using specific large-scale enterprise commercial products or by using free solutions to periodically track and sweep the network.

TOPICS:

- Understanding the CIS Critical Controls
- Understanding the resources and tools related to the CIS Controls
- Understand control effectiveness against common threats leveraging Mitre ATT&CK
- Understanding and practicing control assessments
- CIS Control #1: Inventory and Control of Enterprise Assets

SECTION 2: Data Protection, Identity and Authentication, Access Control Management, Audit Log Management

During Section 2, the course will begin to cover the defensive domains of software control, data protection, identification and authentication, and access control management. Students will learn how identity and access control promotes data protection.

TOPICS:

- CIS Control #2: Inventory and Control of Software Assets
- CIS Control #3: Data Protection
- CIS Control #5: Account Management
- CIS Control #6: Access Control Management

SECTION 3: Server, Workstation, Network Device Protections (Part 1)

During Section 3 , the course will cover the defensive domains of configuration management, email and web browser integrity, vulnerability management, and audit and accountability.

TOPICS:

- CIS Control #7: Continuous Vulnerability Management
- CIS Control #4: Secure Configuration of Enterprise Assets and Software
- CIS Control #8: Audit Log Management
- CIS Control #9: Email and Web Browser Protections

SECTION 4: Server, Workstation, Network Device Protections (Part 2)

Section 4 will cover the defensive domains of system integrity, system and communications protection, configuration management, and media protection.

TOPICS:

- CIS Control #10: Malware Defenses
- CIS Control #11: Data Recovery
- CIS Control #12: Network Infrastructure Management
- CIS Control #13: Network Monitoring and Defense

SECTION 5: Governance and Operational Security

Section 5 will cover the defensive domains of security awareness , service provider management, application development security, incident management, and penetration testing.

TOPICS:

- CIS Control #14: Security Awareness and Skills Training
- CIS Control #15: Service Provider Management
- CIS Control #16: Application Software Security
- CIS Control #17: Incident Response Management
- CIS Control #18: Penetration Testing

> **"I would recommend this course to anyone that is going to be a ISSO or ISSM or CISO."**
>
> —Matthew S., **US Military**

> **"A comprehensive walk-through of the Critical Security Controls, not just focusing on the 'what' but, more importantly, the 'why.' It has been an invaluable learning experience for me."**
>
> —Justin Cornell, **LOM (UK) Limited**

Who Should Attend

- Information Assurance Auditors
- System Implementers or Administrators
- Compliance Analysts
- IT Administrators
- Department of Defense (DoD) personnel or contractors
- Federal agencies or clients
- 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

NICE Framework Work Roles

- Security Control Assessor (SP-RSK-002)

GCCC
Critical Controls
giac.org/gccc

GIAC Critical Controls Certification

The GIAC Critical Controls Certification is the only certification based on the Critical Security Controls, a prioritized, risk-based approach to security. This certification ensures that candidates have the knowledge and skills to implement and execute the Critical Security Controls recommended by the Council on Cybersecurity, and perform audits based on the standard.

- Background, purpose, and implementation of the CIS Critical Controls
- Account monitoring, application software security, boundary defense, and controlled use of administrative privileges and need-to-know access
- Data protection and data recovery capability; email and web browser protections; inventory and control of hardware and software assets; and limitation and control of network ports
- Maintenance, monitoring, and analysis of audit logs; secure configurations for hardware, software, and network devices; and wireless access control