SEC566: **Implementing and Auditing CIS Controls™**

GCCC Critical Controls
giac.org/gccc

5 Day Program | 30 CPEs | Laptop Required

You Will Be Able To

- Design and implement CIS Controls across IT, cloud, hybrid, and AI environments
- Build metrics and risk scores to measure effectiveness and communicate residual risk
- Streamline configuration, coverage, and compliance with automation and orchestration
- Apply strong identity and access controls to secure users, services, and AI workflows
- Enforce endpoint, network, and cloud defenses and extend to AI pipelines and training data
- Establish a culture of continuous improvement through vulnerability management, secure configurations, and forward-looking defense

Business Takeaways

- Reduce attack surface with a prioritized set of CIS Controls
- Maximize ROI by focusing on safeguards with the highest risk reduction
- Create a consistent, measurable security posture across systems, partners, and AI workflows
- Demonstrate regulatory compliance and industry standard alignment through CIS mappings and measurable reporting
- Strengthen detection and response against real-world and AI-enabled threats
- Show measurable improvements with metrics, scoring, and automation
- Build a sustainable, business-aligned program that earns executive support

What are CIS Controls?

The CIS Critical Security Controls are a prioritized set of actions that collectively form a defense-in-depth approach to cybersecurity. They were developed by a community of IT security experts to address the most common attack patterns and provide organizations with concrete steps to improve their security posture.

Implementing and Auditing CIS Critical Controls

Cyber threats are constantly evolving, but the fundamentals of defense remain the same: organizations need a practical roadmap that cuts through complexity and prioritizes the actions that reduce the most risk. The CIS Controls provide exactly that—a proven, prioritized set of safeguards designed to stop the attacks that matter most and build lasting resilience.

SEC566™ gives practitioners, auditors, and risk leaders the knowledge and hands-on experience to put the CIS Controls into practice with confidence. You will learn to design, implement, and audit safeguards across traditional IT, cloud, hybrid, and third-party ecosystems, with expanded coverage for AI-related technologies and workflows. We must keep our skills sharp as organizations adopt machine learning, automation, and intelligent decision-making systems—SEC566™ provides a controls-focused foundation for securing AI models, protecting data, applying guardrails, and ensuring accountability to advanced and merging technology adoptions.

Students will learn how to apply the CIS Controls to AI model development and deployment, ensuring that security is integrated throughout the lifecycle of AI systems. You will learn through practical use cases how to safeguard training data, protect against model tampering, and maintain accountability in AI-driven decisions. This AI coverage builds on the core strengths of the course, giving students a holistic view of how the Controls defend both established systems and next-generation technologies. Through hands-on labs, practical tools, and Cyber42 leadership simulations, you will practice not only implementing the Controls but also measuring their effectiveness, automating coverage, and reporting outcomes in ways that resonate with executives and regulators. Learning mappings to frameworks such as NIST, ISO, and PCI-DSS ensures your work strengthens both compliance and security.

"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**

Section Descriptions

SECTION 1: Introduction and Overview of the CIS Critical Controls

Learn the foundations of the CIS Controls framework, its evolution, and implementation strategies. Focus on enterprise asset inventory as the cornerstone of security, exploring tools and techniques to maintain accurate device tracking across complex networks.

TOPICS: CIS Critical Controls; Resources and Tools of the CIS Controls; Mitre ATT&CK for Common Threats; Control Assessments Practice; CIS Control #1

SECTION 2: Data Protection, Identity, and Authentication

Become proficient in the defensive domains of software control, data protection, and identity management. Learn implementation techniques for secure configurations, privileged access controls, and effective account management systems.

TOPICS: Software Asset Management; Data Protection Strategies; Identity and Access Management (IAM) Best Practices; Secure Access Control Implementation

SECTION 3: Server, Workstation, and Network Protections

Discover the inner workings of vulnerability management, secure configurations, and audit logging implementation. Gain proficiency in techniques to protect email and web browsing while maintaining comprehensive security baselines.

TOPICS: CIS Controls 4, 7, 8, and 9; Secure Configuration Frameworks; Vulnerability Management Systems; Audit Logging Implementation; Email Protections

SECTION 4: Network Infrastructure and Defense

Delve into advanced system protections: malware defenses, data recovery, and network infrastructure security. Learn to monitor network traffic and detect malicious activities using practical tools.

TOPICS: Malware Defense Implementation and Automation; Applying CIS Controls to AI Workflows; Data Recovery Strategies and Testing; Network Infrastructure Hardening and Management; Network Monitoring and Intrusion Detection

SECTION 5: Governance and Operational Security

Develop skills in governance domains including security awareness, service provider management, and incident response. Discover techniques for app security, effective security management, and penetration testing.

TOPICS: Security Awareness Training; Service Provider Management; Application Security Implementation; Incident Response Frameworks; Penetration Testing

"I would recommend this course to anyone that is going to be an ISSO, ISSM, or CISO."

—Matthew S., **U.S. 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 (OPM 612)

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