CIS Controls

Welcome to Version 8 of the CIS Critical Security Controls

Thanks to our volunteer community, the CIS Critical Security Controls (CIS Controls) continue to grow in influence and impact across a world-wide community of adopters, vendors, and supporters. What started over ten years ago as a simple grassroots activity to help enterprises focus on the most important steps to defend themselves against real-world cyber-attacks has become a world-wide movement.

Version 8 is the most effective, best-researched version of the Controls. We addressed emerging technologies, new business and operational challenges (such as work from home), and done more work than ever to study attacks and translate that into prioritized actions. At the same time, we simplified the document by combining like activities and using consistent language.

We've also matured our ability to bring data, rigor and transparency to our recommendations to give you confidence in our work, created cross-mappings to numerous other security frameworks and recommendations, and worked closely with the marketplace to ensure that you are supported with high-quality tools and other resources to help you measure your CIS Controls implementation.

Thanks to everyone for making v8 great!

Phyllis Lee

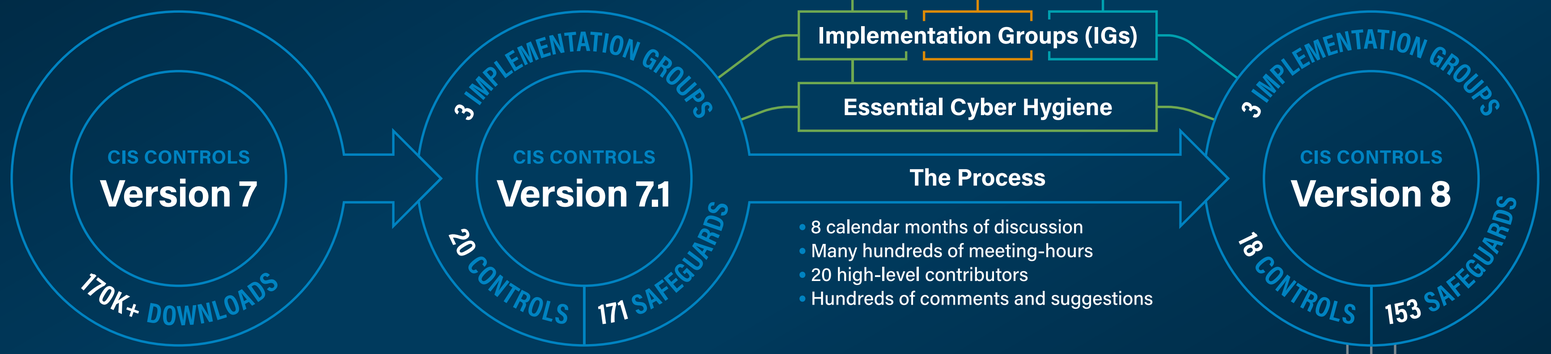
153
TOTAL SAFEGUARDS

The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

IG1
56 SAFEGUARDS
IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

IG2
74 SAFEGUARDS
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

IG3
23 SAFEGUARDS
IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.



Guides Cloud • Mobile • Microsoft Windows 10 • Telework & Small Medium Businesses (SMB) • Community Defense Model (CDM)

Tools CIS Controls Assessment Specification • CIS Controls Self Assessment Tool (CSAT) • CIS Controls Navigator • CIS Risk Assessment Method (RAM)

Mappings NIST • CMMC • PCI • MITRE ATT&CK v8.2

CIS Center for Internet Security®

Creating Confidence in the Connected World.™

Critical Security Controls v8

01 Inventory and Control of Enterprise Assets
02 Inventory and Control of Software Assets
03 Data Protection
04 Secure Configuration of Enterprise Assets and Software
05 Account Management
06 Access Control Management
07 Continuous Vulnerability Management
08 Audit Log Management
09 Email and Web Browser Protection
10 Malware Defenses
11 Data Recovery
12 Network Infrastructure Management
13 Network Monitoring and Defense
14 Security Awareness and Skills Training
15 Service Provider Management
16 Applications Software Security
17 Incident Response Management
18 Penetration Testing

SANS Security Frameworks and CIS Controls Training Courses

SEC566: Implementing and Auditing Security Frameworks & Controls

5 Day Program | 30 CPEs | Laptop Required

GCCC
GIAC Critical Controls Certification
giac.org/gccc

THIS COURSE WILL PREPARE YOU 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

NOTICE TO STUDENTS

The CIS released version 8 of the Controls in May 2021. This course content is updated to reflect the changes in the CIS Controls, as well as the most recent versions of the NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC).

Building and Auditing Critical Security Controls

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?

In addition to defending their information systems, many organizations have to comply with a number of cybersecurity standards and requirements as a prerequisite for doing business. Dozens of cybersecurity standards exist throughout the world and most organizations must comply with more than one such standard. Is your organization prepared to comply and remain in compliance?

In February of 2016, then California Attorney General, Vice President Kamala Harris stated that "the 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

The Center for Internet Security (CIS) Critical Controls are specific security controls 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.

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

SEC566 will enable you to master the specific and proven techniques and tools needed to implement and audit Version 8 of the CIS Controls as documented by the Center for Internet Security (CIS), as well as those defined by NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC). Students will learn how to merge these various standards into a cohesive strategy to defend their organization and comply with industry standards.

SANS' in-depth, hands-on 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 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 whether the Controls and other standards are effectively implemented.

"The course overall was excellent! I do feel like I can put together a plan to begin implementing these controls at our organization right away! I have a feeling I will be referencing these books often. We most definitely will be having at least one person from my team attending this class next year."
—Sarah Kroeplien, Acuity

SANS CYBERSECURITY LEADERSHIP

Version 8 of the CIS Critical Security Controls

AND

SANS Security Frameworks and CIS Controls Training Courses

For Cyber Leaders of Today and Tomorrow

sans.org/cybersecurity-leadership

sans.org/cybersecurity-leadership

@secleadership | SANS Security Leadership

MGTPS_CISCC_v1.3_0521

SEC440: CIS Critical Controls: A Practical Introduction

2 Day Course | 12 CPEs | Laptop Required

Introduction to Critical Security Controls

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? Does your organization need an on-ramp to implementing a prioritized list of technical protections?

In February of 2016, then California Attorney General, Vice President Kamala Harris recommended that "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

SANS has designed SEC440 as an introduction to the CIS Critical Controls, in order to provide students with an understanding of the underpinnings of a prioritized, risk-based approach to security. The technical and procedural controls explained in the CIS Controls were proposed, debated and consolidated by various private and public sector experts from around the world. Previous versions of the CIS Controls were prioritized with the first six CIS Critical Controls labeled as "cyber hygiene" and now the CIS Controls are now organized into Implementation Groups for prioritization purposes.

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 course introduces security and compliance professionals to approaches for implementing 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.

"SEC440 is a great course that immerses the auditor with critical controls—provides focus on what really matters."
—Louis Guion, Mohawk Industries

AUTHORS OF BOTH COURSES: James Tarala & Kelli K. Tarala of Enclave Security | **enclavesecurity.com**

It's not just about the list...

We listened to your questions and responded with guidance for implementing the CIS Controls, showing compliance against other frameworks and tools to measure your Controls implementation. It's not just about a list of best cybersecurity practices—it's about the ecosystem around the Controls to help all enterprises, regardless of size, successfully implement a cybersecurity program.

CIS Controls Tools

CIS CSAT Pro CONTROLS SELF ASSESSMENT TOOL
Helps teams track and document their progress in implementing the CIS Controls. Progress can be compared to industry averages.

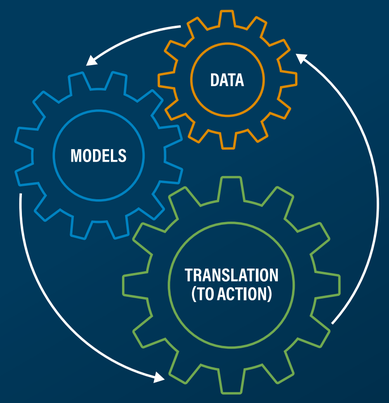
CIS RAM RISK ASSESSMENT METHOD
A method and tool to let enterprises of varying security capabilities navigate the balance between implementing security controls, risks, and organizational needs.

CIS Controls Assessment Specification
Identifies specific tests for Safeguards that can be automated, and provides a specification for vendors to implement them.

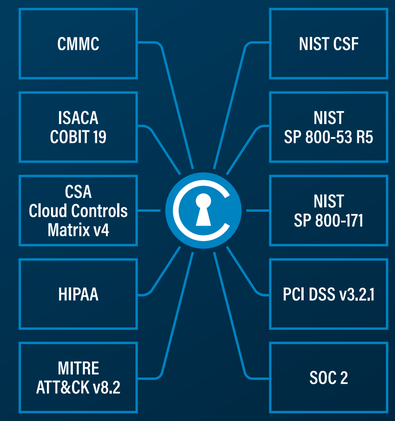
CIS Controls Navigator
Online tool to compare CIS Safeguards with recommendations found in other security frameworks.

CIS WorkBench
CIS collaboration platform for volunteers and CIS staff to share ideas, develop content, and learn from each other.

CIS Community Defense Model
Identifies the security value of CIS Safeguards against specific attacks identified by open data sources, and described using the MITRE ATT&CK Framework.



Navigating an Ocean of Cyber Frameworks
Authoritative and vetted cross-mappings from our security best practices applied to well-known target frameworks or standards. For current versions and information on mappings, go to www.cisecurity.org/controls/v8/



CIS Benchmarks™

CIS Controls Version 8 (and all prior versions) calls out secure configuration of enterprise assets and software as an essential part of any cyber defense program. We believe in the value of this activity so strongly that we founded the company on this idea over 20 years ago! We are the world's largest independent producer of consensus-based configuration guides, bringing together experts from all across the industry and the world to create, share, and support this essential security content—the CIS Benchmarks.

The CIS Benchmarks include more than 100 configuration guidelines across 25+ vendor product families. Benchmarks for top technologies are updated within 90 days of the vendor release date. CIS Benchmarks are consumable in different forms. For example, CIS Hardened Images, virtual machine images configured to the CIS Benchmarks, are available in the major cloud solution marketplaces. We provide mappings to the CIS Controls and MITRE ATT&CK Framework. We also provide CIS STIG Benchmarks.

We are proud to have collaborated on CIS Controls v8 with these fellow nonprofits, who serve the common good by developing and sharing essential cybersecurity best practices.

For all of us, "collaborate" is a verb, not a bumper sticker.

cloud security alliance℠

The Cloud Security Alliance participated on the Controls v8 team, making sure that it reflected the best available information on cloud security. We also mapped CIS Controls v8 Safeguards with CSA's Cloud Controls Matrix.

https://cloudsecurityalliance.org/

SAFECode

SAFECode brought their expertise to lead the drafting of CIS Control #16, Application Software Security. They issued a companion SAFECode document "Application Software Security and the CIS Controls," to provide amplifying guidance on this foundational topic.

https://safecode.org/

Special thanks to our industry partners:

aws, Black Hills Information Security, Ethical Hat, Halock, Microsoft, panaseer, RSA, SANS, tenable