

Sponsors



Unified Security for Threat Detection, Incident Response, and Compliance



CyberPosture Intelligence for the Hybrid Cloud



Prioritizing your CIS Controls and meeting Duty of Care



Delivering Controls with CIS-Certified "Security through System Integrity"



Continuous Security



# SANS Security Leadership

POSTER



## Five Keys for Building a Cybersecurity Program

and



Knowledge and skills to build a world-class cybersecurity program

[sans.org/curricula/management](https://sans.org/curricula/management)



# CIS Controls™

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.



## Basic

CIS Controls V7 separates the controls into three distinct categories:

**Basic:** Key controls which should be implemented in every organization for essential cyber defense readiness.

**Foundational:** Technical best practices provide clear security benefits and are a smart move for any organization to implement.

**Organizational:** These controls are more focused on people and processes involved in cybersecurity.

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

## Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

“Start by taking care of the basics: build a solid cybersecurity foundation by implementing the [CIS Controls], especially application white-listing, standard secure configurations, reduction of administrative privileges and a quick patching process.”

Zurich Insurance Group  
Risk Nexus: Overcome by cyber risks?  
Economic benefits and costs  
of alternate cyber futures  
Switzerland

## CIS Benchmarks™

A single operating system can have over 200 configuration settings and studies of cyber attacks and security incidents invariably reach the same conclusion: poor configuration choices and management are major contributors to the success of attackers. Moreover, every reasonable security framework requires secure configurations as part of ensuring suitable endpoint posture.

CIS Benchmarks are best practices for the secure configuration of a target system.

Available for more than 100 technologies, CIS Benchmarks are developed through a unique consensus-based process comprised

of cybersecurity professionals and subject matter experts around the world. CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry and academia. CIS Benchmarks are free to download in PDF format, with additional file formats (XCCDF, Word, etc.) available to CIS SecureSuite Members.

To further help you with your adoption of the CIS Controls within your organization, each benchmark recommendation is also annotated with the relevant CIS Control.

→ <https://www.cisecurity.org/cis-benchmarks/>

## CIS SecureSuite® Membership

Used worldwide, CIS SecureSuite Membership provides integrated cybersecurity resources to help businesses, nonprofits, governmental entities and IT experts start secure and stay secure. Security-minded IT professionals can significantly improve their organization's cybersecurity posture by investing in a CIS SecureSuite Membership. CIS SecureSuite is used to defend against cyber attacks because it provides access to a host of integrated cybersecurity tools and resources that automate configuration assessment, remediation and enhanced insight to

improve overall cybersecurity posture. CIS SecureSuite delivers integration of the CIS Benchmarks (the only consensus-based, best practice security configuration guides both developed and accepted by government, business, industry and academia) and the CIS Controls. Over 90% of members report that they're satisfied with the value of their CIS SecureSuite membership. In addition, the majority of members say that CIS membership has directly made their organization more secure.

→ <https://www.cisecurity.org/cis-securesuite/>

## The NIST Framework & The CIS Controls: Unifying Your Cyberdefense Program

**NIST** **CIS Controls™**  
The National Institute of Standards and Technology – or NIST – Cybersecurity Framework, provides a means for organizations to describe and make risk-based decisions regarding their cybersecurity program, which aligns and supports an organization's adoption of the CIS Controls. The CIS Controls by design are a prioritized set of technical controls aimed at helping organizations address the most common and pervasive attack methodologies that most organizations are facing. As such, the CIS Controls can provide a starting direction for organizations to seek to achieve and track through the NIST Framework by using

pre-existing cross references. In addition, by leveraging the CIS Controls, you'll also have cross mappings to various other best practices, regulations and frameworks. Alternatively, organizations can use the CIS Controls to help them implement their target profile by providing technical security guidance on how to achieve the different sub-categories of the framework.

Together with the NIST Framework, the CIS Controls can drive the creation a target profile based on preventing the most prevalent attacks or help you implement the objectives of the sub-categories of your established target profile.

## Cybersecurity + Community

When designing the latest version of the CIS Controls, our community relied on key principles to guide the development to simplify, focus, and align them to address the current cybersecurity threat environment. Version 7 of the CIS Controls was developed to align with the latest cyber threat data, security technology, as well as increasing business demands for information technology. We recognize that the cybersecurity world is constantly shifting and reacting to new threats and vulnerabilities, which often results in chaos and confusion about which steps to take in order to harden systems and data.

In order to cut through the confusion, we collaborated on CIS Controls V7 with a global community of cybersecurity experts – leaders in academia, industry and government – to secure input from volunteers at every level that included feedback from a community of over 300 individuals dedicated to improving cybersecurity for all.

Thanks to people like you, the CIS Controls continue to grow in influence and impact across a world-wide community of adopters, vendors and supporters. The idea that started with a small group of friends has become an international movement of volunteers across the entire cyber ecosystem developing, sharing and supporting best practices that can help every enterprise defend itself. CIS is here to help support, evolve and bring together expertise and energy like yours to create, support and sustain best practices in defense.

CIS appreciates the many security experts who volunteer their time and talent to support the CIS Controls and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

## CIS RAM

CIS Risk Assessment Method (CIS RAM) helps us address questions like, "How much security is enough?" and "What constitutes 'due care' or 'reasonableness'?" CIS RAM is a powerful tool to guide the prioritization and implementation of CIS Controls, and to complement their technical credibility with a sound business risk-decision process. It is also designed to be consistent with more formal security frameworks and their associated risk assessment methods. The CIS RAM lets organizations of varying security maturity navigate the balance between implementing security controls, risks and organizational needs. The core of the CIS RAM is the Duty of

Care Risk Analysis (DoCRA) methodology that allows organizations to weigh the risks of not implementing the controls and its potential burden on the organization.

CIS RAM was developed by HALOCK Security Labs in partnership with CIS. HALOCK provided CIS RAM methods for several years with positive response from legal authorities, regulators, attorneys, business executives and technical leaders. HALOCK and CIS collaborated to bring the methods to the public as CIS RAM in 2018. CIS is a founding member of the non-profit DoCRA Council that maintains the risk analysis standard that CIS RAM is built upon.

→ CIS RAM is about Balance:



Learn more at <https://learn.cisecurity.org/cis-ram>



## Getting Involved



As a non-profit driven by volunteers, CIS is always looking for new topics and assistance in creating cybersecurity guidance. If you're interested in volunteering and/or have questions, comments or have identified ways to improve this guide, please write us at [controlsinfo@cisecurity.org](mailto:controlsinfo@cisecurity.org) and join a CIS Control Community.



CIS® (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines

are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

31 Tech Valley Drive  
East Greenbush, NY 12061

518.266.3460

<https://workbench.cisecurity.org/>

[www.cisecurity.org](http://www.cisecurity.org)

[learn@cisecurity.org](mailto:learn@cisecurity.org)

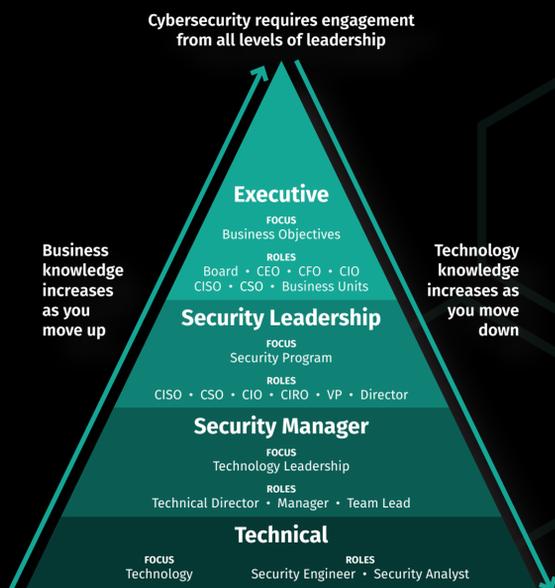
@CISecurity

[/company/the-center-for-internet-security/](https://company/the-center-for-internet-security/)

[/centerforintsec](https://centerforintsec.com)

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

**Knowledge and skills to build a world-class cybersecurity program**



**CURRICULUM**

To implement security frameworks and build technically solid, business-driven security programs, engagement from all levels of leadership is required.

FOUNDATIONAL	CORE	SPECIALIZATION
<b>MGT512</b> SANS Security Leadership Essentials for Managers with Knowledge Compression™ GSLC	<b>MGT514</b> Security Strategic Planning, Policy, and Leadership GSTRT	<b>AUD507</b> Auditing & Monitoring Networks, Perimeters, and Systems GSNA
<b>SEC566</b> Implementing and Auditing the Critical Security Controls – In-Depth GCCC	<b>MGT516</b> Managing Security Vulnerabilities: Enterprise and Cloud NEW	<b>LEG523</b> Law of Data Security and Investigations GLEG
<b>MGT414</b> SANS Training Program for CISSP® Certification GISP	<b>MGT517</b> Managing Security Operations: Detection, Response, and Intelligence	<b>MGT433</b> SANS Security Awareness: How to Build, Maintain, and Measure a Mature Awareness Program
<b>MGT525</b> IT Project Management, Effective Communication, and PMP® Exam Prep GCPM	<b>MGT415</b> A Practical Introduction to Cybersecurity Risk Management	

[sans.org/curricula/management](https://sans.org/curricula/management)

@secleadership

# Five Keys for Building a Cybersecurity Program

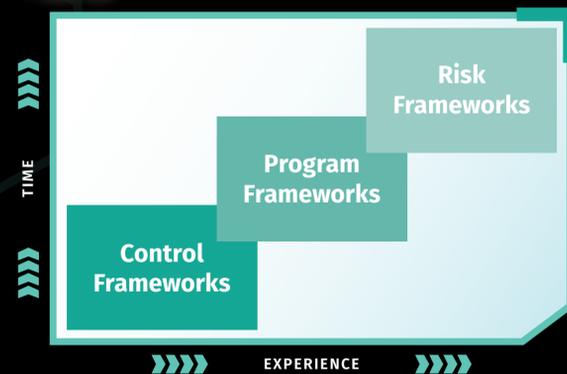
## 1 Find Frameworks that Fit

Choose frameworks that guide the work of your security program and, ultimately, simplify the complex world of cybersecurity in a way that can be more easily understood by business leaders.

- Control frameworks describe the security controls that are the foundation of every security program.
- Program frameworks help structure the security program, establish a basis for evaluating program activities, and simplify communication about the program.
- Risk frameworks provide a consistent approach for managing and assessing risk in a way that provides value to the business.

Choose a framework from each of these three categories to mature your program over time. Examples of common frameworks include:

- Control Frameworks**
  - NIST 800-53
  - CIS Controls
- Program Frameworks**
  - ISO 27001
  - NIST CSF
- Risk Frameworks**
  - NIST 800-39, 800-37, 800-30
  - ISO 27005
  - CIS RAM
  - FAIR



## 2 Map Controls to the Framework

Security frameworks can be used together. This example shows how the CIS Controls can be mapped to the Categories and Functions of the NIST Cybersecurity Framework (CSF).

FUNCTION	CATEGORY	CIS CONTROL
Identify	Asset Management	CIS Control #1, 2
	Business Environment	
	Governance	
	Risk Assessment	CIS Control #3
Protect	Risk Management Strategy	
	Supply Chain Risk Management	
	Identity Management, Authentication, and Access Control	CIS Control #4, 9, 11, 12, 13, 14, 16
	Awareness and Training	CIS Control #4, 17
	Data Security	CIS Control #1, 2, 13, 14, 18
Detect	Information Protection Processes and Procedures	CIS Control #3, 5, 7, 10, 11
	Maintenance	CIS Control #4, 12
	Protective Technology	CIS Control #4, 6, 8, 11, 13, 14, 16
	Anomalies and Events	CIS Control #6, 9, 12, 19
Respond	Security Continuous Monitoring	CIS Control #3, 8, 19
	Detection Processes	CIS Control #6
	Response Planning	CIS Control #19
	Communications	CIS Control #19
Recover	Analysis	CIS Control #3, 19
	Mitigation	CIS Control #3, 19
	Improvements	CIS Control #19
	Recovery Planning	CIS Control #19
	Improvements	CIS Control #19
	Communications	CIS Control #19

## 3 Manage and Assess Risk

Beyond the activities defined in control or program frameworks, you also need to determine which capabilities to prioritize. What do you do first or not at all? How do you make this determination beyond just a checklist of activities?

ISO 27005 is a commonly referenced standard that defines a systematic approach to manage and assess risk for an organization.



## 5 Monitor and Measure Security

To continuously improve security effectiveness:

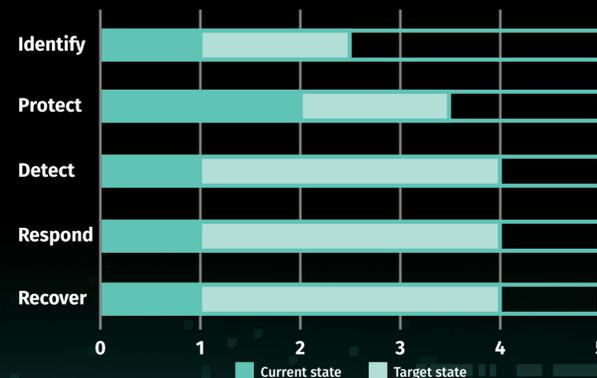
- Establish and measure meaningful security metrics.
- Monitor those metrics frequently enough to minimize incident impact.
- Take action rapidly and efficiently to effectively improve overall security.

The CIS Controls have proven to be an effective starting point for selecting key security metrics.

Establish continuous monitoring guidelines that define which controls should be monitored on a weekly, monthly, or on an ongoing basis.

## 4 Measure Maturity and Progress

Use a risk-based approach to prioritize security controls to reach a desired target state. Developing a roadmap allows you to measure maturity and progress over time.



Frequency	CIS Control	Example Measure
Continuous and Ongoing	(1) Inventory of Devices	Percentage of unauthorized assets that have not been removed from the network, quarantined, or added to the inventory in a timely manner
	(3) Continuous VA and Remediation	Percentage of vulnerabilities that have not been remediated in a timely manner
Weekly	(6) Maintenance, Monitoring, Analysis of Logs	Percentage of assets that are not configured to aggregate appropriate logs to a SIEM or log analytic tools for correlation and analysis
	(9) Limitation/Control of Ports, Services	Percentage of hardware assets that are not configured to require only network ports, protocols, and services with validated business needs
Monthly	(2) Software Inventory	Percentage of high-risk business applications that have not been physically or logically segregated from other business systems
	(5) Secure Configurations	Percentage of assets that do not have a documented, standard security configuration

## SANS Training to Implement the CIS Controls and Build a Security Program

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

This course 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 to measure whether the Controls have been implemented effectively.

*“Provides greater structure to the basic controls. Good methodology provided in implementing controls.”*

[sans.org/sec566](https://sans.org/sec566)

### MGT514 Security Strategic Planning, Policy, and Leadership

This course gives you the tools you need to become a security business leader who can: build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

*“I moved into management a few years ago and am currently working on a new security strategy/roadmap and this class just condensed the past two months of my life into a one week course and I still learned a lot!”*

*“This training sets the stage for executive level success. If you are interested in ever becoming a CISO, this course is a must.”*

[sans.org/mgt514](https://sans.org/mgt514)