

CIS Controls v8.1

CIS Controls v8.1 provides prioritized, practical security actions to help organizations mitigate common cyber threats and strengthen defenses.



What it is

CIS Critical Security Controls v8.1 is a cybersecurity framework that provides a prioritized set of actions to help organizations mitigate the most prevalent cyber threats and improve overall security posture. The framework focuses on practical, implementable safeguards to protect systems and sensitive information against common attack vectors.

Developed and maintained by the Center for Internet Security (CIS), this framework is widely adopted by public and private sector organizations, IT professionals, and compliance teams. It covers key areas such as access control, asset management, incident response, and vulnerability management, aligning with other standards like NIST and ISO to enhance cybersecurity resilience and risk management.

At a glance

PUBLISHER Center for Internet Security	TYPE Standard	VERSION v8.1
EFFECTIVE 2023	DOMAIN Cybersecurity	FAMILY CIS Controls
REGION United States	ADOPTION MODEL Security Baseline	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.cisecurity.org/controls/v8-1>

Why it matters

- **Strengthen security governance** Enable leadership to oversee the implementation of effective controls and maintain accountability across information systems and processes.
- **Enhance regulatory compliance** Support alignment with established standards such as NIST and ISO, helping organizations meet regulatory requirements more efficiently.
- **Increase audit readiness** Provide a documented baseline for security practices, streamlining internal and external audit processes and demonstrating due diligence.
- **Improve threat detection capabilities** Facilitate prompt identification and response to cyber incidents through structured controls and incident management practices.

How SmartSuite supports CIS Controls v8.1

CIS Control Library by IG Organize safeguards by Control family and Implementation Group (IG1-IG3) for phased adoption.	Remediation Workstreams and Owners Assign owners to each safeguard and drive closure with clear due dates and accountability.	Evidence and Configuration Proof Capture scan outputs, configuration baselines, and policy evidence tied to each safeguard.
Continuous Monitoring Cadence Schedule recurring reviews for patching, access, logging, and vulnerability management activities.	Risk-Based Prioritization Link safeguards to risks and assets to focus effort on what reduces exposure fastest.	Executive and Audit Reporting Report progress by Control, IG level, business unit, and open exceptions.

Common framework mappings

ISO 27001:2022

ISO 27002:2022

ISO 27701

MITRE ATT&CK

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

CIS Critical Security Controls v8.1 Provides the official set of controls to improve cybersecurity defenses. cisecurity.org/controls/v8-1	CIS Controls Implementation Guide Outlines detailed steps for implementing each of the CIS Controls effectively. cisecurity.org/cis-benchmarks
CIS Controls Assessment Specification Describes methods for assessing an organization's adherence to the CIS Controls. cisecurity.org/controls/v8-1	CIS Controls Ecosystem Overview Defines the relationship and integration of CIS Controls within broader cybersecurity frameworks. cisecurity.org/controls/cis-controls-navigator

Frequently asked questions

- What is CIS Critical Security Controls v8.1 used for?**
CIS Critical Security Controls v8.1 is used to help organizations identify, prioritize, and implement cybersecurity best practices to reduce risk from common cyber threats. The framework provides a practical roadmap of security safeguards to protect systems, networks, and sensitive data.
- Is implementation of CIS Controls v8.1 mandatory or certifiable?**
CIS Controls v8.1 is not legally required nor certifiable in the way some standards are, such as ISO 27001. However, organizations often adopt it as a recognized best practice to improve their security posture and demonstrate risk management to stakeholders and regulators.
- What types of organizations should use CIS Critical Security Controls v8.1?**
CIS Controls v8.1 is applicable to organizations of all sizes and industries, including both public and private sectors. Its flexible structure allows organizations to tailor implementation based on size, regulatory requirements, and risk tolerance.
- What are the key components and artifacts of the CIS Controls v8.1 framework?**
Key components include 18 control families, each with detailed security safeguards and sub-controls. Organizations use Implementation Groups (IG1, IG2, IG3) to align control deployment with their maturity and risk profile, and create documentation to support audit and compliance processes.

How do organizations implement CIS Critical Security Controls v8.1?

Organizations implement CIS Controls by conducting risk assessments, mapping controls to relevant assets and processes, and selecting appropriate Implementation Groups. Effective deployment involves continuous monitoring, documentation of control effectiveness, and reviewing controls as part of security governance.

How does CIS Controls v8.1 align with other security frameworks?

CIS Controls v8.1 is designed to map to major frameworks like NIST Cybersecurity Framework and ISO 27001, enabling organizations to align controls, demonstrate compliance, and streamline regulatory reporting across multiple standards.

What are the ongoing compliance requirements for CIS Controls v8.1?

Maintaining compliance involves regularly assessing control effectiveness, updating safeguards based on changing threats, and retaining evidence of control operation. Organizations should periodically review risk assessments and update documentation to ensure ongoing alignment with framework requirements.

How would SmartSuite support CIS Critical Security Controls v8.1?

SmartSuite supports CIS Controls v8.1 by offering pre-built control libraries, risk registers, and policy management tools. Users can map controls, collect and manage evidence, track progress toward implementation, and generate audit-ready reports to facilitate compliance monitoring and remediation workflows.

License included / downloadable: Yes The CIS Critical Security Controls are publicly available through the Center for Internet Security.

Full framework page and mappings: smartsuite.com/frameworks/cis-critical-security-controls-v8-1