SmartSuite

Framework / Cybersecurity / CIS Controls

CIS Controls v8.1

CIS Controls v8.1 is a prioritized set of 18 Controls and 153 Safeguards, in three Implementation Groups, with a new Govern function.



What it is

The CIS Critical Security Controls (CIS Controls) v8.1 is a prioritized set of 18 Controls and 153 Safeguards that tell an organization which security actions to take first to defend against common attacks. Version 8.1, released on June 24, 2024, is an iterative update to v8 that adds the Govern security function from NIST CSF 2.0, revises asset classes and expands the glossary, and it did not change the Implementation Groups.

The Center for Internet Security (CIS), a nonprofit organization, develops the Controls with a community of volunteer experts. They are voluntary guidance, not a regulation or certification. Three cumulative Implementation Groups, IG1 with 56 Safeguards, IG2 adding 74 and IG3 adding 23, tell an organization where to start based on its size, data and risk.

At a glance

PUBLISHER Center for Internet Security	TYPE Standard	VERSION v8.1 (18 Controls, 153 Safeguards)
EFFECTIVE June 24, 2024	DOMAIN Cybersecurity	FAMILY CIS Controls
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: cisecurity.org/controls/v8-1

Why it matters

- **A short, ordered list** Eighteen Controls start with asset inventories and run to incident response and penetration testing, so the first steps are about knowing what is in the environment.
- **Implementation Groups set priority** IG1 is essential cyber hygiene with 56 Safeguards, IG2 adds 74 for 130 in total, and IG3 adds 23 for all 153.
- **Governance is explicit in v8.1** The new Govern function from NIST CSF 2.0 identifies Safeguards that support governing a cybersecurity program, and CIS counts 26 of them.
- **Works with cloud and supply chain** The v8.1 page highlights hybrid and fully cloud environments and supply chain security.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CIS Controls v8.1

Control and Safeguard Library

Load the 18 Controls and 153 Safeguards with their Implementation Group, asset class and security function.

Implementation Group Selection

Record the chosen group for each business unit and the Safeguards in scope, so IG1 work comes before IG2 and IG3.

Asset Inventories

Keep enterprise asset and software inventories as linked records that feed Controls 1 and 2.

Safeguard Evidence and Testing

Attach evidence and test results to each Safeguard and track pass, fail and exceptions.

Gaps and Roadmap

Turn failed Safeguards into prioritized tasks with owners and due dates, and show progress by Control.

Governance Reporting

Report coverage by Implementation Group and by security function, including Govern, for leadership.

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 Benchmarks FAQ

Answers common questions about what the Benchmarks cover, how Level 1 and Level 2 profiles differ, and how to assess against them.

cisecurity.org/cis-benchmarks/cis-benchmarks-faq

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 are the CIS Critical Security Controls?

A prioritized set of 18 Controls and 153 Safeguards from the Center for Internet Security that tells organizations which security actions to take first against common attacks. Version 8.1 was released on June 24, 2024.

What changed in CIS Controls v8.1?

It added the Govern security function from NIST CSF 2.0, realigned function mappings to CSF 2.0, revised asset classes with new mappings to Safeguards, expanded glossary definitions and clarified some Safeguard text. The Implementation Groups were not modified.

What are Implementation Groups?

Cumulative sets of Safeguards that help organizations prioritize: IG1 has 56 Safeguards (essential cyber hygiene), IG2 adds 74 for 130 in total, and IG3 adds 23 for all 153. They are based on an enterprise's risk profile and available resources.

What are the 18 CIS Controls?

Asset inventory, software inventory, data protection, secure configuration, account management, access control management, continuous vulnerability management, audit log management, email and web browser protections, malware defenses, data recovery, network infrastructure management, network monitoring and defense, security awareness and training, service provider management, application software security, incident response management, and penetration testing.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Are the CIS Controls mandatory or certifiable?

No. They are voluntary guidance published by CIS. Organizations use them as a baseline and for evidence, and they can map them to frameworks such as NIST CSF 2.0 and ISO/IEC 27001.

License included / downloadable: No CIS publishes the CIS Controls v8.1 for download in PDF and Excel on cisecurity.org. The text is not included with the platform.

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

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.