

Which specific CIS Benchmark (product and version) should be used? Example naming format: CIS Benchmark –



What it is

CIS Benchmarks are consensus-based cybersecurity standards that enable organizations to strengthen security controls and reduce risk by providing recommended technical configurations for operating systems, applications, and network devices. These benchmarks help ensure consistent implementation of security best practices and support compliance efforts across various IT environments.

Developed and published by the Center for Internet Security (CIS), the CIS Benchmarks are widely used by security professionals, IT administrators, and compliance teams. The framework encompasses a broad range of technologies, covering system hardening, secure configuration, and operational controls to address common threats and vulnerabilities. Organizations often reference CIS Benchmarks alongside standards such as NIST 800-53 or ISO 27001 for comprehensive security and compliance programs.

At a glance

PUBLISHER Center for Internet Security (CIS)	TYPE Guidance	VERSION Continuously updated benchmark releases by platform
EFFECTIVE 2005	DOMAIN Cybersecurity	FAMILY CIS Controls
REGION United States	ADOPTION MODEL Security Baseline	IMPLEMENTATION COMPLEXITY Moderate

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

Why it matters

- Strengthen configuration management** Promote consistent application of secure settings, reducing risks from misconfiguration and unauthorized system changes.
- Enhance regulatory alignment** Support compliance by mapping benchmark controls to industry and governmental security requirements.
- Increase audit preparedness** Enable organizations to demonstrate security best practices and provide documented evidence during compliance audits.
- Improve threat mitigation** Reduce exploitable weaknesses and improve defenses against malware, ransomware, and other cyber threats.

How SmartSuite supports CIS Benchmarks

Benchmark Library and Scope Coverage

Track benchmark requirements by technology with defined asset scope.

Secure Configuration Baselines

Document hardened configurations and approved baselines with version control.

Compliance Scans and Evidence Capture

Attach scan outputs and remediation proof to benchmark requirements.

Exceptions and Compensating Controls

Manage exceptions, approvals, and compensating controls with traceability.

Drift Monitoring and Recurring Reviews

Schedule recurring validation to detect configuration drift over time.

Compliance Reporting Dashboards

Report coverage, exceptions, and remediation status by platform and team.

Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

FedRAMP Rev. 5

HIPAA (NIST SP 800-66 Rev. 2)

Official resources

CIS Benchmarks Overview

Provides a comprehensive introduction to CIS Benchmarks and their application in cybersecurity.
cisecurity.org/cis-benchmarks

CIS Benchmark Level 1 and Level 2 Details

Defines Level 1 and Level 2 benchmark specifications for secure configurations.
cisecurity.org/benchmark

CIS Controls Implementation Guide

Outlines detailed steps for implementing each of the CIS Controls effectively.
cisecurity.org/cis-benchmarks

CIS Benchmark Scoring Tool

Describes the tool for scoring compliance against CIS Benchmarks.
cisecurity.org/cybersecurity-tools/cis-cat-pro

Frequently asked questions

What are CIS Benchmarks used for?

CIS Benchmarks provide consensus-driven security configuration standards to help organizations harden systems, applications, and network devices. They are used to reduce security risks stemming from misconfiguration and to support compliance with industry and regulatory requirements.

Are CIS Benchmarks mandatory or certifiable?

CIS Benchmarks are not legally mandatory and do not provide a formal certification. However, they are widely adopted as best practices and often referenced in audits or as a basis for demonstrating due diligence in security and regulatory compliance programs.

What is the applicability or scope of CIS Benchmarks?

CIS Benchmarks cover a broad scope, including operating systems, databases, applications, cloud services, and networking equipment. Organizations select relevant CIS Benchmarks based on their IT environment, technologies in use, and specific regulatory or operational requirements.

What key concepts or artifacts are required by CIS Benchmarks?

The key concepts include benchmark profiles (Level 1 for essential security and Level 2 for stringent requirements), system hardening guidelines, and prescriptive control catalogs. Artifacts generated include configuration assessment reports, remediation plans, and compliance dashboards.

How do organizations implement CIS Benchmarks?

Organizations begin by assessing current system configurations against CIS Benchmark recommendations, identifying deviations, and remediating gaps. Implementation involves integrating benchmarks into change management, regular configuration reviews, and automated compliance checks.

How do CIS Benchmarks relate to other frameworks like NIST 800-53 or ISO 27001?

CIS Benchmarks often complement broader frameworks such as NIST 800-53 or ISO 27001 by providing technical, control-specific configuration guidance. They can be mapped to controls in these frameworks to help demonstrate detailed implementation and control effectiveness.

What are the ongoing compliance requirements for CIS Benchmarks?

Maintaining compliance with CIS Benchmarks requires continuous monitoring, periodic configuration audits, documented remediation activities, and evidence of alignment to benchmark controls. Regular review and update cycles are necessary to stay in line with evolving security threats and benchmark updates.

How would SmartSuite support CIS Benchmarks?

SmartSuite enables organizations to operationalize CIS Benchmarks by importing control libraries, mapping benchmark requirements to internal policies, tracking risk and remediation, collecting compliance evidence from scans, and generating audit-ready reports and dashboards for ongoing governance.

License included / downloadable: Yes CIS Benchmarks are publicly available through the Center for Internet Security. Some resources and tooling may require CIS membership, but the benchmark guidance itself can generally be accessed through CIS.

Full framework page and mappings: smartsuite.com/frameworks/cis-benchmark