SmartSuite

Framework / Cybersecurity / CIS Controls

CIS Critical Security Controls v8.1 – IG1

CIS Controls v8.1 IG1 provides prioritized basic cybersecurity controls to help resource-limited organizations defend against common threats.

What it is

CIS Critical Security Controls v8.1 — Implementation Group 1 (IG1) is a cybersecurity framework that provides a prioritized set of fundamental security controls specifically tailored for organizations with limited resources and cybersecurity expertise. It focuses on essential defense mechanisms to protect sensitive data and defend against the most prevalent cyber threats.

Developed and published by the Center for Internet Security (CIS), the framework is used by organizations of all sizes as a starting point for implementing basic safeguards. The IG1 controls are recognized as foundational requirements, particularly for small and medium-sized enterprises (SMEs), and cover key areas such as asset management, access control, vulnerability management, and incident response.

At a glance

PUBLISHER Center for Internet Security (CIS)	TYPE Control Framework	VERSION v8.1
EFFECTIVE 2024	DOMAIN Cybersecurity	FAMILY CIS Controls
REGION United States	ADOPTION MODEL Security Baseline	IMPLEMENTATION COMPLEXITY Low

Source: https://www.cisecurity.org/controls/v8

Why it matters

- **Improve security governance** Enable organizations to establish clear oversight and responsibility for essential cybersecurity practices across internal and external environments.
- **Enhance regulatory support** Support compliance by aligning fundamental security measures with regulatory and industry standards, easing preparation for assessments and audits.
- **Strengthen data protection** Improve the safeguarding of sensitive and personal information, reducing exposure to unauthorized access and data breaches.
- **Promote operational resilience** Reduce business disruption risks through effective asset tracking, vulnerability management, and basic incident response capabilities.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CIS Controls v8.1 IG1

Asset Inventory and System Visibility

Track hardware, software, and cloud assets to maintain visibility into systems requiring protection.

Security Control Implementation Tracking

Map CIS safeguards to tasks, owners, and due dates to ensure consistent execution.

Vulnerability and Patch Management

Track vulnerabilities, remediation actions, and patch status across systems and endpoints.

Identity and Access Governance

Manage user access, permissions, and authentication controls to reduce unauthorized access risk.

Security Awareness and Training Programs

Manage employee cybersecurity training initiatives and track participation and completion.

Security Program Monitoring and Reporting

Report on control adoption, open risks, and overall cybersecurity posture.

Common framework mappings

CIS Controls v8.1 IG2 | CIS Controls v8.1 IG3 | ISO 27001:2022 | ISO 27002:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5 | 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 for IG1

Provides detailed guidance for implementing CIS Controls tailored for organizations with limited resources.

cisecurity.org/controls/v8-1

CIS Critical Security Controls Overview

Describes the structure and purpose of the CIS Controls framework.

cisecurity.org/controls

Frequently asked questions

What is CIS Critical Security Controls v8.1 IG1 used for?

CIS Controls v8.1 Implementation Group 1 (IG1) is designed to provide organizations with a prioritized set of fundamental cybersecurity practices, focusing on essential defensive measures. It is primarily used by organizations with limited cybersecurity resources or expertise to improve their baseline security posture and protect against widespread cyber threats.

Is CIS Controls v8.1 IG1 a mandatory or certifiable framework?

The CIS Controls v8.1 IG1 is a voluntary guidance framework and is not itself a certifiable or legally required standard. However, organizations may use its controls to demonstrate due diligence, complement regulatory compliance, or satisfy contractual security requirements.

Who should use CIS Controls v8.1 IG1?

CIS Controls v8.1 IG1 is best suited for small to medium-sized organizations, or any organization seeking to establish essential security controls with limited resources. It offers a pragmatic starting point for implementing cyber hygiene and is applicable across industries.

What security controls are required by CIS Controls v8.1 IG1?

Implementation Group 1 includes foundational controls such as asset inventory, user access management, secure system configurations, vulnerability management, and basic incident response readiness. Each control within IG1 has specific sub-controls that define minimum requirements to reduce common risks.

 © 2026 SmartSuite Inc. All rights reserved.

How does an organization implement CIS Controls v8.1 IG1?

To implement IG1, organizations should assess their current security state, identify and map relevant assets, and deploy the controls as outlined. Documentation, staff awareness training, and basic vulnerability patching are central, with controls applied in a prioritized, risk-based sequence.

How does CIS Controls v8.1 IG1 relate to frameworks like NIST CSF or ISO 27001?

CIS Controls v8.1 IG1 aligns with many requirements in NIST Cybersecurity Framework and ISO 27001, acting as a practical guide for implementing basic measures. Organizations frequently map IG1 controls to these broader frameworks to support a comprehensive compliance or risk management strategy.

What are the ongoing compliance requirements for CIS Controls v8.1 IG1?

Ongoing compliance with IG1 involves continuous monitoring of assets, access, configurations, and vulnerabilities. Organizations should regularly review control effectiveness, gather evidence for audits, update documentation, and perform periodic risk assessments and incident response exercises.

How would SmartSuite support CIS Critical Security Controls v8.1 IG1?

SmartSuite can help manage CIS Controls v8.1 IG1 by centralizing risk tracking, control implementation, and policy documentation. The platform supports evidence collection, automates remediation workflows, enables audit readiness, and provides real-time reporting dashboards to monitor compliance and demonstrate governance.

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-v81-implementation-group-1-ig1