

CIS Controls v8.1 – IG2

CIS Controls IG2 is an intermediate cybersecurity framework guiding organizations with moderate risk to implement prioritized controls against common threats.



What it is

CIS Critical Security Controls v8.1 — Implementation Group 2 (IG2) is a prescriptive cybersecurity framework that guides organizations in implementing prioritized security controls to mitigate common cyber threats and reduce risk exposure. IG2 represents an intermediate level of security readiness, intended for organizations with moderate risk profiles and regulatory obligations.

Developed and maintained by the Center for Internet Security (CIS), the CIS Controls are widely adopted across sectors for establishing baseline security measures. IG2 focuses on enhancing security for organizations with increased sensitivity around data protection, operational activities, and compliance requirements, covering domains such as asset management, access control, continuous monitoring, 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 Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

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

Why it matters

- **Strengthen cybersecurity governance** Support clear policies, roles, and responsibility assignments that drive effective security management across diverse systems and team
- **Enhance operational resilience** Bolster defenses against common cyberattacks, minimizing the impact of incidents and supporting faster recovery of critical services.
- **Improve regulatory compliance** Align security processes with widely recognized standards, helping meet industry obligations and pass regulatory or customer audits.
- **Increase audit readiness** Prepare documentation and evidence of control implementation, simplifying internal reviews and supporting third-party assurance activities.

How SmartSuite supports CIS Controls v8.1 IG2

Expanded Control Library Management

Track CIS safeguards, assign control owners, and manage implementation tasks across the organization.

Vulnerability and Remediation Tracking

Monitor vulnerability assessments, remediation tasks, and patch management activities.

Identity and Privileged Access Governance

Manage user roles, privileged access approvals, and authentication policies.

Security Incident Response Workflows

Track incident detection, response actions, and remediation activities across security teams.

Vendor and Third-Party Risk Oversight

Evaluate third-party cybersecurity posture and track remediation actions for supplier risks.

Security Program Reporting and Metrics

Generate dashboards and reports showing CIS control adoption and cybersecurity risk posture.

Common framework mappings

FedRAMP Rev. 5

ISO 27001:2022

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 Document

Provides official documentation of CIS Critical Security Controls version 8.1.

cisecurity.org/controls/v8

CIS Implementation Groups Overview

Describes the structure and purpose of CIS Implementation Groups.

cisecurity.org/controls/v8#overview

CIS Control Assessments Guide

Defines assessment guidance for implementing CIS Controls in various environments.

cisecurity.org/controls/v8#assessment-guide

Frequently asked questions

What is CIS Critical Security Controls v8.1 Implementation Group 2 (IG2) used for?

CIS Critical Security Controls v8.1 IG2 provides a prioritized set of cybersecurity safeguards designed to help organizations with moderate risk profiles protect sensitive data and meet regulatory requirements. Organizations use IG2 to strengthen their security posture against common threats by implementing practical, effective security controls.

Is CIS Critical Security Controls v8.1 IG2 mandatory or certifiable?

CIS Controls, including IG2, are not mandatory or certifiable by regulatory authorities but are widely recognized as best practices. Organizations may choose to adopt IG2 controls to enhance their security and demonstrate due diligence to regulators, clients, or auditors.

What organizations should use CIS Controls IG2?

IG2 is intended for organizations with moderate exposure to risk and increased sensitivity around data privacy, regulatory compliance, and operational resilience. It is suitable for entities that manage regulated data, have supply chain obligations, or need to demonstrate a stronger security baseline than the basic IG1 level.

What are the key concepts and artifacts required for IG2 compliance?

Key concepts for IG2 compliance include asset management, user access control, continuous security monitoring, and documented incident response plans. Artifacts commonly required are risk assessments, control implementation evidence, inventories, and audit logs that demonstrate adherence to IG2 safeguards.

How do organizations implement CIS Controls v8.1 IG2?

Implementation begins with a gap assessment against the IG2 safeguard set, integration of these controls into organizational policies and risk management processes, and deployment of technical measures. Ongoing monitoring, vulnerability management, and evidence collection are also essential for sustaining compliance.

How does CIS Controls v8.1 IG2 relate to other cybersecurity frameworks?

CIS Controls IG2 aligns with and complements major frameworks such as NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and SOC 2. It provides a practical set of controls that organizations can map to broader governance, risk, and compliance requirements defined in these frameworks.

What is required for ongoing compliance with CIS Controls IG2?

Maintaining IG2 compliance involves regular monitoring of security controls, continuous vulnerability assessment, updating control implementations, collecting audit evidence, and reviewing policies. Periodic reassessment and documentation help ensure controls remain effective and aligned with evolving threats and business requirements.

How would SmartSuite support CIS Critical Security Controls v8.1 IG2?

SmartSuite enables organizations to manage CIS Controls IG2 by importing control libraries, assigning safeguards, and tracking associated risks. It facilitates centralized control management, evidence collection, and compliance tracking, supports automated remediation workflows, and provides comprehensive dashboards for audit readiness and regulatory reporting.

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

Full framework page and mappings: smartsuite.com/frameworks/cis-critical-security-controls-v81-implementation-group-2-ig2