SmartSuite

Framework / Cybersecurity / CIS Controls

CIS Controls v8.1 – IG3

CIS Controls IG3 defines advanced prioritized security controls to protect critical assets in high-risk, complex organizations.

What it is

CIS Critical Security Controls v8.1 — Implementation Group 3 (IG3) is a cybersecurity framework that defines an advanced set of prioritized security controls enabling organizations to mitigate complex cyber threats and safeguard critical assets. IG3 represents the most comprehensive level of implementation within the CIS Controls framework, addressing sophisticated risks faced by organizations with large, mature, and complex environments.

Published by the Center for Internet Security (CIS), the CIS Controls are widely adopted by security leaders, risk managers, and compliance professionals to strengthen cybersecurity defenses. IG3 is intended for organizations with significant regulatory obligations or heightened risk profiles, and it covers areas such as access control, vulnerability management, incident response, and data protection.

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 Very High

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

Why it matters

- **Strengthen cybersecurity leadership** Enable organizations to establish comprehensive oversight and governance over security programs in line with evolving cyber threats.
- **Advance regulatory compliance** Support meeting the most demanding legal, regulatory, and industry-specific security requirements through robust control implementation.
- **Increase audit readiness** Facilitate evidence-based security control validation and streamline preparation for audits and assessments across various standards.
- **Enhance incident response capabilities** Improve detection, containment, and response to sophisticated cyber incidents targeting sensitive information or mission-critical assets.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CIS Controls v8.1 IG3

Advanced Control Library Management

Track CIS safeguards, map controls to assets, and assign ownership for advanced security controls.

Threat and Incident Response Workflows

Coordinate detection, investigation, and remediation activities across security teams.

Identity and Privileged Access Governance

Manage privileged access approvals, role-based permissions, and authentication policies.

Threat and Vulnerability Monitoring

Track detected threats, vulnerabilities, and security risks across systems and infrastructure.

Third-Party and Supply Chain Security Oversight

Monitor vendor cybersecurity posture and manage supplier risk assessments.

CIS Control Adoption and Security Program Maturity Reporting

Provide dashboards and reports showing CIS control adoption, risk posture, and security program maturity.

Common framework mappings

ISO 27001:2022 | ISO 27002:2022 | 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

Defines comprehensive best practices for cybersecurity controls by the Center for Internet Security.

cisecurity.org/controls/v8

CIS Controls Implementation Group 3 (IG3) Overview

Outlines advanced security measures tailored for complex environments within CIS Controls v8.

cisecurity.org/controls/v8

CIS SecureSuite Membership Benefits

Outlines offerings and resources available to organizations for implementing CIS Controls.

cisecurity.org/cis-securesuite

CIS Controls Risk Assessment Method

Describes methods to assess and prioritize risk using CIS Controls.

learn.cisecurity.org/cis-ram-v2-2

Frequently asked questions

What is CIS Controls v8.1 IG3 used for?

CIS Controls v8.1 Implementation Group 3 (IG3) is used to provide advanced, prioritized cybersecurity safeguards for organizations facing complex cyber threats and possessing high-value or sensitive assets. It is designed to help large, mature enterprises with heightened risk profiles implement rigorous security controls and reduce exposure to sophisticated attacks.

Is CIS Controls v8.1 IG3 required or certifiable?

CIS Controls v8.1 IG3 is not mandated by law nor is it a certifiable framework. However, it is widely adopted as a best practice benchmark and is often referenced by regulators and auditors to demonstrate a high standard of internal security controls within risk management and compliance programs.

Who should use CIS Controls v8.1 IG3?

IG3 is intended for organizations with substantial regulatory obligations, complex IT environments, or elevated security needs, such as financial institutions, healthcare organizations, or critical infrastructure providers. It is suitable for entities that must address advanced threat actors and require comprehensive risk mitigation.

 © 2026 SmartSuite Inc. All rights reserved.

What are the key concepts and required artifacts for IG3?

Key concepts of IG3 include asset management, threat-informed risk assessments, advanced access controls, continuous vulnerability management, and structured incident response. Required artifacts typically include documented policies, control mappings, risk registers, evidence of technical safeguards, monitoring logs, and reports verifying control effectiveness.

How do organizations implement CIS Controls v8.1 IG3?

Implementation involves mapping IG3 controls to relevant assets, conducting risk assessments to set tailored control baselines, and deploying both technical and administrative security measures. Effective implementation also requires ongoing documentation, continuous testing, incident response processes, and validation of control performance.

How does CIS Controls v8.1 IG3 relate to other frameworks like NIST CSF or ISO 27001?

CIS Controls v8.1 IG3 aligns well with established frameworks such as NIST Cybersecurity Framework and ISO 27001 by providing a granular, actionable set of safeguards that complement broader risk management and governance requirements. Organizations often map IG3 controls to these frameworks to strengthen their overall compliance posture.

What are the ongoing compliance requirements for IG3?

Ongoing compliance with IG3 involves periodic reassessment of risk, continuous monitoring of control performance, regular documentation and evidence collection, and prompt remediation of identified gaps. Audit readiness demands retaining records of security activities, control testing, and incident response actions.

How would SmartSuite support CIS Controls v8.1 IG3?

SmartSuite supports CIS Controls v8.1 IG3 by offering an integrated library of mapped controls, linked risk registers, and automated policy workflows. The platform enables streamlined risk tracking, centralized control management, efficient evidence collection, ongoing audit readiness, and reporting dashboards to monitor implementation and compliance status.

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-controls-v8-1-ig3

 © 2026 SmartSuite Inc. All rights reserved.