SmartSuite

Framework / Cybersecurity / CIS Controls

CIS Critical Security Controls v8.1 – IG1

CIS Controls v8.1 IG1 is the 56-Safeguard essential cyber hygiene baseline for small and medium-sized enterprises with limited security expertise.



What it is

CIS Controls v8.1 Implementation Group 1 (IG1) is the foundational set of 56 Safeguards, out of 153 in the CIS Critical Security Controls, that the Center for Internet Security calls essential cyber hygiene. It is written for small to medium-sized enterprises with limited IT and cybersecurity expertise, and CIS describes it as an on-ramp to implementing the Controls.

CIS, a nonprofit organization, publishes IG1 within CIS Controls v8.1, released on June 24, 2024. It is voluntary guidance with no certification and no legal force of its own. CIS says an IG1 enterprise has limited tolerance for downtime and protects data of low sensitivity, mainly employee and financial information, and that every enterprise should start here.

At a glance

PUBLISHER Center for Internet Security (CIS)	TYPE Control Framework	VERSION v8.1, Implementation Group 1 (56 Safeguards)
EFFECTIVE June 24, 2024	DOMAIN Cybersecurity	FAMILY CIS Controls
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Low

Source: cisecurity.org/controls/v8-1

Why it matters

- **A finite starting point** Fifty-six Safeguards give a small organization a concrete list instead of the full 153.
- **Built for limited resources** The Safeguards are meant to be implementable with limited cybersecurity expertise and ordinary commercial products.
- **Aimed at common attacks** IG1 defends against the most common attacks, which is the goal of essential cyber hygiene.
- **Cumulative path forward** IG2 adds 74 Safeguards and IG3 adds 23 more, so work done for IG1 is not repeated.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CIS Controls v8.1 IG1

IG1 Safeguard List

Load the 56 IG1 Safeguards with their Control, owner and status, so the whole baseline fits on one board.

Asset and Software Inventories

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

Account and Access Review

Schedule account reviews and access checks (Controls 5 and 6) with due dates and sign-off.

Backup and Recovery Tests

Record data recovery tests and results (Control 11) and track fixes to completion.

Incident Response Basics

Hold the incident contacts, procedure and incident log (Control 17) for a small team.

Progress Reporting

Show percent complete by Control and what is left before moving on to IG2.

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 Controls IG1?

Implementation Group 1 is the foundational set of 56 Safeguards in the CIS Controls, described by CIS as essential cyber hygiene. It is designed for small to medium-sized enterprises with limited IT and cybersecurity expertise.

Who should use IG1?

CIS describes an IG1 enterprise as small to medium-sized with limited IT and cybersecurity expertise, limited tolerance for downtime and data that is low in sensitivity, mainly employee and financial information. CIS recommends that all enterprises begin with IG1.

How many Safeguards are in IG1, IG2 and IG3?

IG1 has 56 Safeguards. IG2 adds 74 for a total of 130, and IG3 adds 23 for all 153 in CIS Controls v8 and v8.1. The groups are cumulative.

Is IG1 a certification?

No. It is voluntary guidance from the Center for Internet Security. Organizations use it as a documented baseline, and it has no certification of its own.

What should an organization do first under IG1?

Start with inventories of enterprise assets and software (Controls 1 and 2), because the other Safeguards depend on knowing what is in the environment. Then work through data protection, secure configuration, account management, recovery and incident response using products the organization already has.

 © 2026 SmartSuite Inc. All rights reserved.

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-v81-implementation-group-1-ig1