SmartSuite

Framework / Cybersecurity / CIS Controls

# CIS Controls v8.1 – IG3

CIS Controls v8.1 IG3 is the complete 153-Safeguard set for enterprises with security specialists, regulated data and targeted-attack risk.




## What it is

CIS Controls v8.1 Implementation Group 3 (IG3) is the complete set of 153 Safeguards in the CIS Critical Security Controls, made up of IG1's 56, IG2's 74 and 23 further Safeguards that the Center for Internet Security says an enterprise needs to abate targeted attacks from a sophisticated adversary. It is written for enterprises that employ security specialists and hold sensitive data under regulatory or compliance oversight.

CIS, a nonprofit organization, publishes IG3 within CIS Controls v8.1, released on June 24, 2024. It is voluntary guidance with no certification of its own. CIS says IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight, and that a successful attack could seriously harm the public.

## At a glance

| | | |
|---|---|---|
| PUBLISHER<br>Center for Internet Security (CIS) | TYPE<br>Control Framework | VERSION<br>v8.1, Implementation Group 3 (153 Safeguards) |
| EFFECTIVE<br>June 24, 2024 | DOMAIN<br>Cybersecurity | FAMILY<br>CIS Controls |
| REGION<br>United States | ADOPTION MODEL<br>Voluntary | IMPLEMENTATION COMPLEXITY<br>High |

Source: cisecurity.org/controls/v8-1

## Why it matters

- **Complete coverage** IG3 contains every Control and Safeguard, 153 in total, so an IG3 program covers the whole catalog.
- **Built for specialist teams** An IG3 enterprise commonly employs security experts who specialize in facets such as risk management, penetration testing and application security.
- **Regulated and sensitive data** IG3 applies where assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight.
- **Availability and integrity matter** IG3 protects service availability and the confidentiality and integrity of sensitive data where a successful attack could seriously harm the public.

 © 2026 SmartSuite Inc. All rights reserved. 

## How SmartSuite supports CIS Controls v8.1 IG3

### Full Safeguard Catalog

Load all 153 Safeguards with Control, Implementation Group, asset class and security function, and mark the 23 IG3 additions.

### Specialist Ownership

Assign each Safeguard to a named owner or specialist team, such as penetration testing or application security.

### Control Testing and Evidence

Schedule tests, attach results and record exceptions for each Safeguard, including advanced controls.

### Threat and Risk Linkage

Link Safeguards to the risks and threat scenarios they counter, including targeted attack and zero-day cases.

### Regulatory Mappings

Map Safeguards to the frameworks the organization reports against so one set of evidence serves several audits.

### Executive Reporting

Report coverage by Implementation Group, Control and security function, including Govern, for the board and auditors.

## 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 IG3?

Implementation Group 3 is the complete set of 153 Safeguards in the CIS Critical Security Controls. It adds 23 Safeguards to IG2 and is intended for enterprises that face targeted attacks from sophisticated adversaries.

### Who should implement IG3?

Enterprises that commonly employ security experts who specialize in areas such as risk management, penetration testing and application security, whose assets and data are subject to regulatory and compliance oversight, and where a successful attack could seriously harm the public.

### How does IG3 differ from IG1 and IG2?

The groups are cumulative. IG1 has 56 Safeguards as essential cyber hygiene, IG2 adds 74 for 130, and IG3 adds 23 for all 153. The IG3 additions must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

### Is IG3 a certification?

No. It is voluntary guidance from the Center for Internet Security, and an organization claims alignment through its own documented implementation and evidence.

 © 2026 SmartSuite Inc. All rights reserved. 

### Does IG3 include the Govern function added in v8.1?

Yes. IG3 contains every Safeguard, so it includes the 26 Safeguards that CIS identifies as supporting the Govern security function that v8.1 added from NIST CSF 2.0.

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-controls-v8-1-ig3

 © 2026 SmartSuite Inc. All rights reserved. 