CIS CRITICAL SECURITY CONTROLS.

The Center for Internet Security's Critical Security Controls v8.1, released June 2024, are a prioritized, prescriptive set of 18 Controls and 153 Safeguards built from attack data. Three Implementation Groups set the order of work: **every enterprise starts with the 56 Safeguards of IG1, essential cyber hygiene.**

START AT IG1 | FREE TO USE, NOT CERTIFIED | BUILT FROM ATTACK DATA | GOVERN ADDED IN V8.1

01 THE MECHANISM

Prescriptive by Design

CIS calls the Controls a prescriptive, prioritized and simplified set of best practices. Version 8.1, released June 2024, is an iterative update to v8, built to minimize disruption to Controls users. **The spirit of every Safeguard stayed the same.** [01] [02] [10]

Implementation Groups

Three cumulative groups turn 153 Safeguards into an order of work. IG1 holds 56 Safeguards, the essential cyber hygiene every enterprise starts with; IG2 adds 74 for 130; IG3 adds the last 23 and holds all 153. **CIS calls IG1 the on-ramp and an emerging minimum standard.** [04] [05] [06]

Every Safeguard Is Tagged

The v8.1 assessment specification labels each Safeguard with one asset class (Devices, Software, Data, Users, Network or Documentation) and one security function (Govern, Identify, Protect, Detect, Respond or Recover). **Govern is new in v8.1, realigned to NIST CSF 2.0.** [09] [01]

02 THE FLOW

How an Enterprise Adopts It — PRIORITIZE

1. **Pick your Implementation Group:** IG1 for small to medium enterprises with limited IT and security expertise and low data sensitivity; IG2 where staff manage IT across departments and hold sensitive data; IG3 where security experts face targeted attacks. [04] [05] [06]
2. **Finish IG1 first:** its 56 Safeguards include an asset inventory (1.1), a data management process (3.1), a secure configuration process (4.1), unique passwords (5.2) and automated backups (11.2), all designed for off-the-shelf hardware and software. [04] [09]
3. **Grow into IG2 and IG3:** IG2 adds Safeguards such as software allowlisting (2.5), encryption in transit (3.10), architecture diagrams (12.4) and an incident response process (17.4); IG3 adds passive asset discovery (1.5) and data loss prevention (3.13). [05] [06] [09]

How CIS Keeps It Honest — MEASURE

1. **Offense informs defense:** the Community Defense Model v2.0 (2021) maps Safeguards to ATT&CK techniques for the five top attack types. IG1 alone defends against 77% of malware, 78% of ransomware and 83% of targeted intrusion techniques. [08]
2. **One assessment, thirty mappings:** the CIS Controls Navigator relates v8.1 Safeguards to 30 frameworks, among them NIST CSF 2.0, SP 800-53 Rev. 5, ISO/IEC 27001:2022, PCI DSS v4.0, CMMC 2.0 and SOC 2, filters by Implementation Group and exports a spreadsheet. [03]
3. **Measure, then revise:** the Controls Assessment Specification for v8.1 states what to measure for each Safeguard, and CIS CSAT tracks implementation. The Controls are updated by an informal community process; CIS says it is already working on ideas for Version 9. [09] [07] [10]

03 THE 18 CONTROLS IN SIX GROUPS

GROUP	CONTROLS IT HOLDS
Inventory	Controls 1 and 2 (12 Safeguards): inventories of enterprise assets and software; unauthorized items get removed.
Data	Controls 3 and 11 (19 Safeguards): data protection from classification to encryption and disposal; data recovery.
Configure	Controls 4, 7 and 12 (27 Safeguards): secure configuration, vulnerability management, network infrastructure.
Identities	Controls 5 and 6 (14 Safeguards): user, administrator and service accounts; access and credential lifecycle.
Defend	Controls 8, 9, 10, 13 (37 Safeguards): logging, email and browser protection, malware defense, network monitoring.
Program	Controls 14 to 18 (44 Safeguards): training, service providers, app security, incident response, pen testing.

04 IMPLEMENTATION GROUPS COMPARED

GROUP	SECURITY SPECIALISTS ASSUMED?	WHO IT FITS
CIS Benchmarks	No	Not a group. Hardening guides for specific operating systems, cloud platforms and network devices; Safeguard 4.1 points to them.
IG1 (56)	No	Small and medium firms with limited IT and security expertise and low data sensitivity; the concern is keeping the business running.
IG2 (130)	Yes	Staff manage and protect IT infrastructure across departments with differing risk profiles; holds sensitive client or enterprise data.
IG3 (153)	Yes	Security experts in risk management, penetration testing and application security; regulated sensitive data; faces targeted attacks.

CIS CONTROLS V8.1.

INVENTORY · PRIORITIZE · MEASURE

05 PROGRAM OPERATIONS

Finish IG1 before buying anything new. Its Safeguards are meant for limited cybersecurity expertise and off-the-shelf tools, so inventories, a written secure configuration process, unique passwords, dormant-account cleanup and isolated backups come before enterprise tooling or IG2 work. [04] [09]

Use the asset classes as a coverage checklist. The Documentation class exposes governance gaps: Safeguards 4.1, 4.2, 11.1, 17.2 and 17.3 are written processes that IG1 already expects, and 12.4 and 17.4 follow in IG2. A Safeguard that exists only in someone's head fails the measure. [09] [01]

Assess once, report many ways. Record implementation per Safeguard, then use the Navigator's mappings to show coverage against NIST CSF 2.0, SP 800-53, ISO/IEC 27001, PCI DSS or CMMC from the same evidence, and use the Community Defense Model to explain why IG1 came first. [03] [08]

Mind the license and the safe harbors. Anyone may use the Controls to improve their own cybersecurity; vendors and consultants building them into products or services need SecureSuite or Supporter status. Ohio, Utah, Connecticut and Iowa name the Controls in safe harbor statutes. [07] [02]

06 CONTROL MAPPING

`NIST CSF 2.0`

Version 8.1 realigned its security function mappings to NIST CSF 2.0 and added the Govern function, so each Safeguard now sits under one of six functions. The Navigator carries the Safeguard-to-CSF 2.0 mapping, and the CIS FAQ describes the Controls as a CSF informative reference. [01] [03] [07]

`NIST SP 800-53 & 800-171`

Navigator mappings cover NIST SP 800-53 Rev. 5 across all baselines, SP 800-171 Rev. 2 and Rev. 3, SP 800-172 Rev. 3 and CMMC 2.0. The Controls are the shorter, prioritized list; the NIST catalogs supply the depth when a federal or defense contract requires them. [03]

`CIS BENCHMARKS & CIS-CAT`

CIS keeps the two apart: the Controls are general recommended practices, the Benchmarks harden specific operating systems and products. Safeguard 4.1 is the linchpin across all five attack types in the Community Defense Model, and CIS-CAT shows some alignment between Benchmark settings and the Controls. [07] [08]

`REGULATORY MAPPINGS`

The same Navigator also maps v8.1 to ISO/IEC 27001:2022, PCI DSS v4.0, AICPA SOC 2, NYDFS 23 NYCRR Part 500, DORA, NIS2, HIPAA, CISA Cross-Sector CPGs v2.0 and the NERC CIP standards, among others. The FAQ is explicit that the Controls replace no regulatory, compliance or authorization scheme. [03] [07]

07 WHAT THIS DOES NOT SOLVE

Not a Certification

Accreditation is for member firms that assess others. **CIS issues no enterprise certificate.** [07]

Not Exhaustive

There is no magic to the number 18, CIS says. **It targets the most prevalent attacks**, not every risk. [07] [01]

Not Config Detail

Safeguard 4.1 asks for a secure configuration process; **the Benchmarks say which setting to set.** [07] [09]

Not Frozen

Current in late 2026, v8.1 is revised by community process; **CIS is working on Version 9 ideas.** [10] [07]

08 MYTHS VS. REALITY

MYTH	REALITY
"CIS certifies our organization as compliant."	CIS accredits member service firms; **it offers no enterprise certificate** and replaces no compliance scheme. [07]
"A small firm must implement all 153 Safeguards."	IG1 is 56 Safeguards, **essential cyber hygiene for limited expertise and off-the-shelf tools**; the rest follow. [04]
"Version 8.1 rewrote the Controls."	Iterative update: **no Implementation Group changed**; it added Govern, revised asset classes and a glossary. [01] [10]
"Basic hygiene barely dents real attacks."	The Community Defense Model finds IG1 **defends against 78% of ransomware techniques** and 77% of malware techniques. [08]
"You have to pay CIS to use the Controls."	**Free for anyone to use** on their own security; vendors and consultants need SecureSuite membership. [07]

09 SPEAK THE PROGRAM — KEY TERMS

SAFEGUARD

Unit of the Controls (ex Sub-Control); **each requires you to do one thing**; 153 in v8.1.

IMPLEMENTATION GROUP

One of three cumulative Safeguard sets **chosen by risk profile and resources**: IG1 to IG3.

ESSENTIAL CYBER HYGIENE

CIS's name for IG1: **56 foundational Safeguards every enterprise should apply** first.

ASSET CLASS

The v8.1 tag on a Safeguard: **Devices, Software, Data, Users, Network or Documentation**.

SECURITY FUNCTION

Govern, Identify, Protect, Detect, Respond, Recover; **Govern arrived in v8.1** via CSF 2.0.

CIS RAM

CIS's risk assessment method for the Controls; **v2.2 for v8.1 published December 5, 2025**.