CS-105 · Compliance & Frameworks

# CIS Controls

A prioritized set of practical safeguards for building a defensible security baseline.

## Executive Summary

The CIS Controls are a prioritized set of practical safeguards published by the Center for Internet Security to help organizations defend against the most common and damaging attacks. They are organized so that a team with limited resources can start with the highest-value basics and grow from there. Implementation groups let organizations pick a scope that matches their size, risk, and capability.

## What It Is

The CIS Controls are a community-developed, prioritized list of defensive actions, called safeguards, grouped into a manageable number of top-level controls. Rather than describing broad outcomes, they focus on concrete, testable measures such as maintaining an inventory of hardware and software, controlling administrative privileges, and managing configurations. The set is intentionally ordered so the earliest controls deliver the most protection per unit of effort. To make adoption realistic, the safeguards are sorted into implementation groups (commonly referred to as IG1, IG2, and IG3), where the first group represents essential cyber hygiene for smaller organizations and each higher group adds safeguards for organizations with greater risk and resources.

## Why It Matters

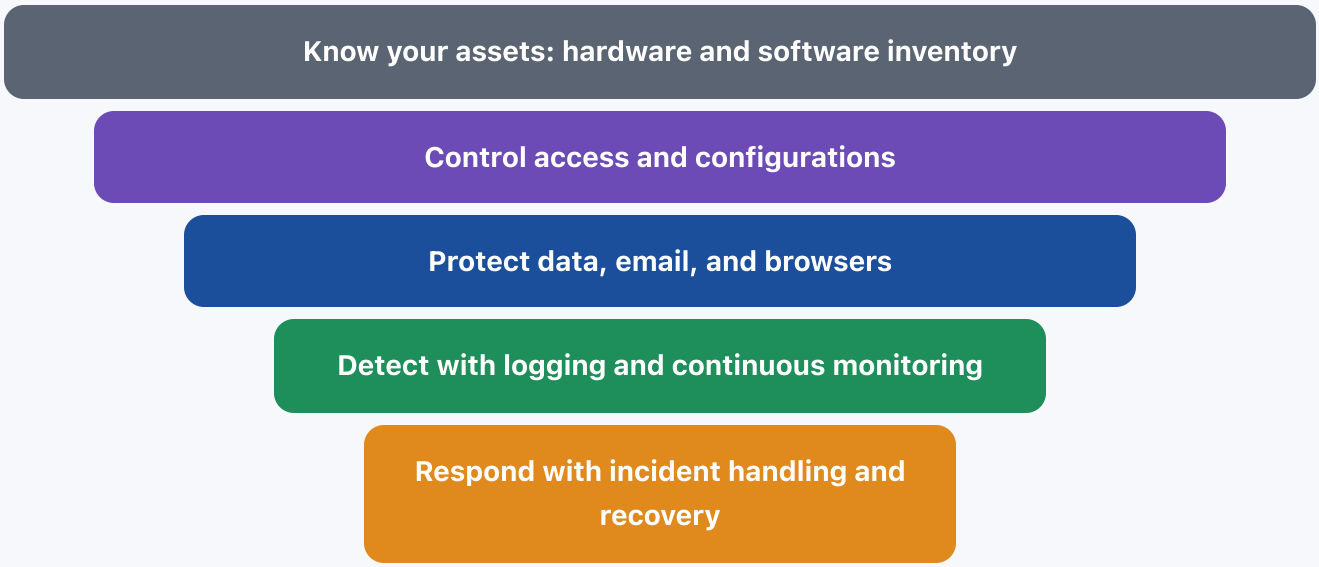
Many organizations know they should improve security but do not know where to begin. The CIS Controls answer that question by giving a defensible starting order grounded in how real attacks actually unfold. Because the safeguards are specific and measurable, they are easy to audit and to translate into projects, budgets, and metrics. They also map to broader frameworks, so effort spent implementing CIS Controls supports compliance with other requirements at the same

time. For professionals, the controls provide a practical bridge between high-level frameworks and the day-to-day technical work of reducing risk.

## How It Works

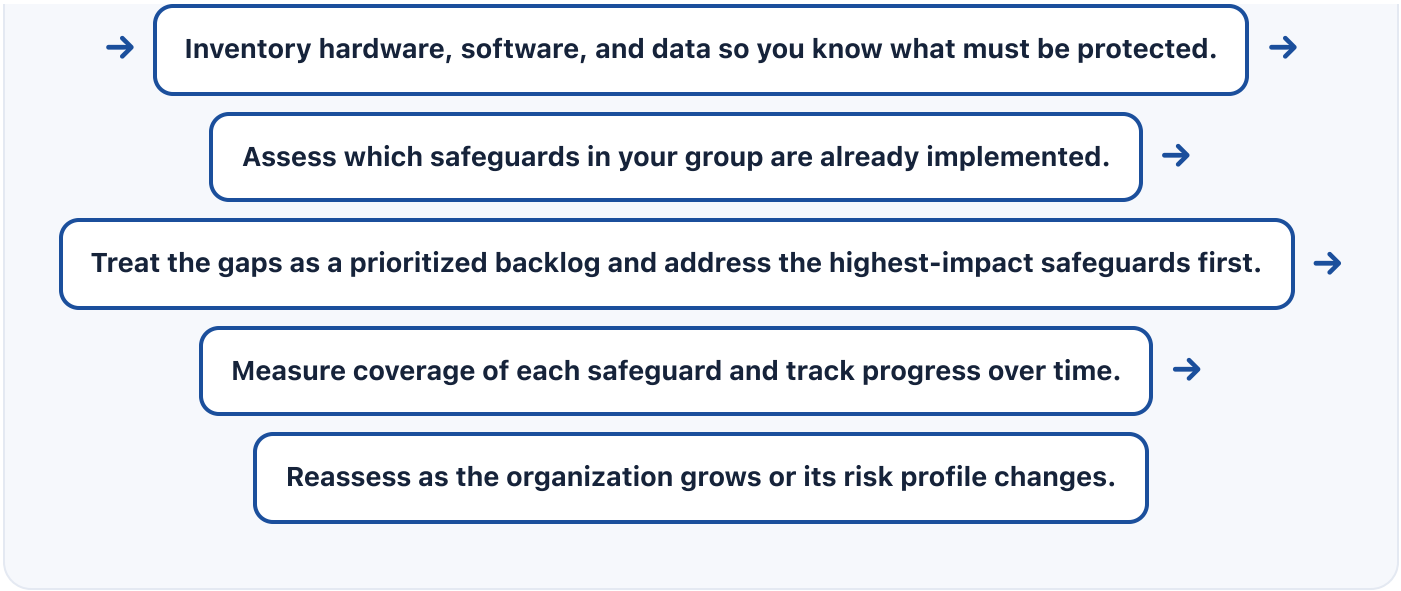
An organization first selects the implementation group that fits its size, risk profile, and resources. It then assesses which safeguards in that group are already in place, treats the gaps as a prioritized backlog, and works down the list. Because the controls are ordered by impact, early wins such as building an accurate asset inventory and enforcing multi-factor authentication tend to reduce risk quickly. Each safeguard is written to be measurable, which lets teams track coverage over time and demonstrate progress. Many organizations map the CIS Controls to a broader framework like the NIST CSF so that improving the controls also advances their overall program.

## Architecture Diagram




Safeguards build upward: essential hygiene first, then broader coverage, then advanced defenses as risk and resources grow.

## Visual Workflow




## Common Attacks

- Skipping asset inventory, which leaves unknown devices and software unprotected
- Choosing an implementation group beyond the team's capacity and stalling
- Implementing later safeguards while foundational hygiene remains incomplete
- Treating safeguards as one-time projects instead of maintained practices
- Failing to measure coverage, so progress and gaps stay invisible

## Common Mistakes

- Buying tools before establishing an accurate inventory of what exists
- Assuming a small organization must attempt every advanced safeguard
- Ignoring the built-in prioritization and tackling safeguards in random order
- Documenting a safeguard as complete without verifying it actually works
- Leaving safeguards unmapped to broader frameworks and duplicating compliance effort

## Best Practices

- Select the right implementation group before starting, not the most ambitious one
- Build and maintain an accurate hardware, software, and data inventory first
- Follow the built-in prioritization so early effort delivers the most risk reduction
- Make each safeguard measurable and review coverage on a regular cadence

- Map the CIS Controls to the NIST CSF or another framework to reuse the effort
- Assign an owner to each control area so maintenance does not lapse

## Quick Checklist

- [x] Implementation group chosen and documented with rationale
- [x] Current, owned inventory of hardware, software, and sensitive data
- [x] Multi-factor authentication enforced on important accounts
- [x] Administrative privileges limited and reviewed
- [x] Secure configurations applied and monitored for drift
- [x] Coverage of each safeguard measured and reported over time

## Recommended Tools

**Asset inventory tool**
Discovers and tracks hardware and software so nothing is unmanaged

**Configuration management tool**
Applies secure baselines and detects drift

**Vulnerability scanner**
Finds weaknesses to prioritize against the safeguards

**GRC platform**
Tracks safeguard coverage, evidence, and framework mappings

## Industry Standards

**CIS Critical Security Controls**
The prioritized safeguards themselves, grouped into implementation groups

**CIS Benchmarks**
Secure configuration baselines that support several safeguards

**NIST Cybersecurity Framework (CSF) 2.0**
Broader framework the CIS Controls commonly map to

## Career Relevance

The CIS Controls are widely used by GRC analysts, compliance analysts, security auditors, and CISOs to set a defensible baseline and to translate frameworks into concrete work. Security engineers and IT staff often implement the safeguards directly, while auditors and risk professionals use their measurable nature as evidence. For the privacy and AI governance professionals AI-Governance-Jobs.com serves, the controls offer a practical way to show that governance decisions are backed by real safeguards.

## Interview Questions

- What are the CIS Controls and how do they differ from a framework like the NIST CSF?
- Explain implementation groups and how you would choose the right one.
- Why is asset inventory treated as a foundational safeguard?
- How would you prioritize safeguards for an organization just starting out?
- How do the CIS Controls support compliance with broader requirements?

## Related Certifications

CompTIA Security+ | ISC2 CISSP | ISACA CISM

## Further Reading

- CIS Critical Security Controls
- CIS Controls Implementation Groups
- CIS Benchmarks

## Key Takeaways

- The CIS Controls are prioritized, practical safeguards for building a defensible baseline.
- Implementation groups let organizations scope effort to their size and risk.
- Foundational hygiene, starting with asset inventory, delivers the most early risk reduction.

- Safeguards are specific and measurable, which makes them easy to audit and track.
- The controls map to broader frameworks, so the work supports wider compliance.

## FAQ



## Related Careers

### RELATED ROLES

Grc Analyst | Compliance Analyst | Security Auditor | Ciso

### RELATED CERTIFICATIONS

CompTIA Security+ | ISC2 CISSP | ISACA CISM

### CURRENT OPENINGS

Live roles are on the job board.

**Browse all jobs**

### GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

### SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **CIS Controls**
3. Go deeper: NIST Cybersecurity Framework (CSF)
4. Go deeper: ISO/IEC 27001
5. Validate it: work toward **CompTIA Security+**

6. Find the role: browse current openings

## RELATED SHEETS

CS-104 NIST Cybersecurity Framework (CSF) | CS-106 ISO/IEC 27001 | CS-001 Cybersecurity | CS-085 Risk Ratings | CS-009 Core Security Principles