STANDARD SUMMARY · CERT.GT

CIS Controls

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: IT and security officers, especially in small and medium-sized organizations.

The CIS Controls are a prioritized list of concrete actions against the most common attacks. Where other frameworks say what to achieve, these say what to do first. They are free and the current version is 8.1: 18 Controls and 153 Safeguards.

The Implementation Groups

The Safeguards are split into three cumulative groups. Start with the first one.

IG1 · Essential Cyber Hygiene	56 Safeguards. The minimum for any organization, designed for small teams with few IT staff.
IG2	IG1 plus 74 Safeguards. For organizations with dedicated IT staff and sensitive data.
IG3	All 153 Safeguards. For organizations with security specialists and a risk of targeted attacks.

The 18 Controls

1	Inventory and Control of Enterprise Assets.
2	Inventory and Control of Software Assets.
3	Data Protection.
4	Secure Configuration of Enterprise Assets and Software.
5	Account Management.
6	Access Control Management.
7	Continuous Vulnerability Management.
8	Audit Log Management.
9	Email and Web Browser Protections.
10	Malware Defenses.
11	Data Recovery.
12	Network Infrastructure Management.
13	Network Monitoring and Defense.
14	Security Awareness and Skills Training.
15	Service Provider Management.
16	Application Software Security.
17	Incident Response Management.
18	Penetration Testing.

Where to start

- Controls 1 and 2: you cannot protect what you do not know you have. Build the inventory of devices and software.
- Control 4: change factory-default passwords, and turn on the screen lock and the firewall on every device.
- Controls 5 and 6: one account per person, two-step verification, and administrator privileges only for those who need them.
- Control 7: turn on automatic updates and check every month what was left unpatched.
- Control 11: automatic backups, with one offline copy and restore tests.
- Control 14: train staff to recognize phishing and report it.

Free tools from CIS

- CIS Benchmarks: secure configuration guides for operating systems, cloud and applications.
- CIS CSAT: a self-assessment tool for measuring progress on each Control.
- Mapping tables to NIST CSF, ISO 27001 and PCI DSS.

Common mistakes

- Jumping to advanced Controls without having finished the inventory.
- Measuring progress by tools purchased rather than by Safeguards that are working.
- Building the inventory once and not maintaining it.

Official text

CIS Critical Security Controls v8.1, free at cisecurity.org/controls.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

Summary prepared by cert.gt for educational purposes; it is not the official text of the standard and does not replace legal or compliance advice. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).