>_ CIS Controls v8.1 on One Page

null-packet · free cheat sheet · independent guidance, not affiliated with the Center for Internet Security · authoritative text: cisecurity.org/controls

The idea: **18 Controls, 153 Safeguards, 3 Implementation Groups.** Prioritised so you know what to do first. Start with IG1, in control-number order.

IMPLEMENTATION GROUPS

IG1 · 56	Essential cyber hygiene. Every organisation. The floor you are judged against.
IG2 · +74	Process depth, central management. Sensitive or regulated data.
IG3 · +23	Adversary-grade. Data whose loss causes public harm.

If you have to ask, you are IG1. Do all 56 properly before anything above.

THE 18 CONTROLS, AND THE ONE THING TO GET RIGHT ON EACH

1	**Enterprise Assets**	A living inventory with a last-seen date. You cannot protect what you cannot see.
2	**Software Assets**	Know what is installed and flag anything end-of-life.
3	**Data Protection**	Classify it, control access, and encrypt laptops with escrowed keys.
4	**Secure Configuration**	Harden to a CIS/Microsoft baseline, enforced by GPO/Intune, not by hand.
5	**Account Management**	Dedicated admin accounts. No daily-driver Domain Admins.
6	**Access Control**	MFA on admin, remote and external access. Least privilege.
7	**Vulnerability Mgmt**	Automate OS and app patching. Patch KEV-listed CVEs first.
8	**Audit Log Mgmt**	Collect the logs, keep them long enough, be able to search them.
9	**Email & Web**	DNS filtering (cheapest big win) and DMARC to reject.
10	**Malware Defenses**	Modern anti-malware on everything, servers too; autorun off.
11	**Data Recovery**	3-2-1 with an immutable/offline copy, and test the restore.
12	**Network Infrastructure**	Supported firmware; segment the flat network; encrypted management.
13	**Network Monitoring**	Centralise alerts; filter between segments. (IG2+)
14	**Awareness Training**	A tracked programme, not an annual video. Phishing sims.
15	**Service Providers**	An inventory first; then classify and contract the critical ones.
16	**Application Security**	Build software? Shift security left. If not, scope it N/A.
17	**Incident Response**	Know who to call; write the plan; exercise it. (IG2)
18	**Penetration Testing**	Validate the lot, after the basics are done. (IG2+)

THE FOUR THAT SAVE YOU

Whatever else you do, get these right, they prevent the two disasters that close smaller organisations (ransomware, credential theft): **1. MFA on admin accounts (6.5) 2. Dedicated admin accounts (5.4) 3. Immutable/offline backup (11.4) 4. Tested restore (11.5).**

ORDER OF OPERATIONS

See everything (1, 2) → lock the doors (5, 6, 4) → keep current (7) → protect data (3, 11) → shut common doors (9, 10) → see events (8, 13) → people & suppliers (14, 15) → mature (12, 16, 17, 18).

IT MAPS TO WHAT YOU ALREADY REPORT

Every control cross-walks to ISO 27001:2022, NIST CSF 2.0, NIST 800-53 and NIS2 Article 21. Implement once; answer many audits, and most cyber-insurance questionnaires, with the same evidence.