

CIS 8.1 Assessment

COMPLIANCE AND BEST PRACTICES

Safe Computing Center for Internet Security Framework

Safe Computing follows the CIS 8.1 framework for cybersecurity implementation.

PURPOSE / INSTRUCTIONS

From small businesses to large multi-national enterprises, the CIS 8.1 framework can be followed to tailor best-practice security controls. Selection of which controls to implement are based on your company size, number of information technology assets and sensitivity of your data.

The **CIS Controls v8.1 framework** is a prioritized set of **153 cybersecurity safeguards** organized into **18 controls**, maintained by the **Center for Internet Security (CIS)**. Its purpose is to give organizations a practical, evidence-based blueprint for reducing cyber risk by focusing on the defensive actions that stop the most common real-world attacks.

CIS v8.1 (released June 2024) updates the prior version by adding:

- **Alignment with NIST CSF 2.0**, including a new **Govern** security function that strengthens program oversight and compliance mapping.
- **Refined asset classes and clearer safeguard definitions** to better fit modern cloud, hybrid, and remote environments.

The framework is widely used because it is:

- **Prescriptive and measurable** — it tells organizations *how* to implement security, not just what to protect.
- **Prioritized** — controls are grouped into **Implementation Groups (IG1, IG2, IG3)** so organizations can adopt safeguards based on their size, resources, and risk level.
- **Highly effective** — full implementation defends against a large percentage of MITRE ATT&CK techniques, making it one of the highest-ROI security frameworks available.

If you want, I can also break down the 18 controls, explain the Implementation Groups, or compare CIS v8.1 to NIST CSF or ISO 27001.

Take the [Small and Medium Business Self-Assessment Survey](#) today. It takes less than five minutes to complete and gives you an understanding of your current situation.