CIS (Center for Internet Security) Overview

Summary

The **Center for Internet Security (CIS)** is a non-profit organization founded in 2000 to promote global cybersecurity by providing actionable resources for organizations to defend against cyber threats. It develops and maintains the **CIS Controls** (a prioritized set of 18 cybersecurity best practices, version 8 in 2021) and **CIS Benchmarks** (over 100 configuration guidelines for securing specific technologies, updated regularly). CIS also operates Information Sharing and Analysis Centers (ISACs) like MS-ISAC (for state/local governments) and EI-ISAC (for elections infrastructure). The framework emphasizes practical, high-impact measures to mitigate common attacks, serving as an on-ramp for compliance with regulations like NIST, HIPAA, and GDPR. As of October 2025, CIS focuses on AI risks, cloud security, and supply chain threats, with no direct penalties but enabling regulatory alignment.

Key Requirements

CIS resources are voluntary best practices, not mandates, but are structured for implementation. Key elements include:

1. **CIS Controls (v8)**:
    - **18 Prioritized Controls** grouped into **Implementation Groups (IGs)**:
        - **IG1 (Basic)**: 6 foundational controls for small organizations (e.g., asset inventory, access control basics).
        - IG2 (Foundational): 56 safeguards across the 18 CIS Controls for medium-sized entities (e.g., continuous vulnerability management, secure configuration for hardware/software).
        - IG3 (Organizational): 56 safeguards across the 18 CIS Controls for large/high-risk entities (e.g., penetration testing, supply chain risk management).
    - **Core Focus Areas**:
        - Inventory and control of hardware/software assets.
        - Secure configuration and continuous monitoring.
        - Incident response, training, and third-party risk management.
        - Data protection (e.g., encryption, backup testing).
2. **CIS Benchmarks**:
    - Technology-specific hardening guides (e.g., for AWS, Microsoft Azure, Windows Server).
    - Require implementing recommended configurations (e.g., disabling unnecessary services, enabling MFA).
    - Updated quarterly; community-vetted via Consensus Assessments Initiative.
3. **Implementation Guidance**:
    - Conduct risk assessments (e.g., using CIS RAM v2.1 for prioritization).
    - Maintain policies, training, and monitoring; map to regulations via CIS Mappings.
    - Use tools like CIS-CAT Pro for automated assessments.

Compliance Process:

- Self-assessment via CIS Controls tools; no formal certification but supports audits (e.g., for NIST 800-171).
- Regular reviews (e.g., annual for IG1, continuous for IG3).

Who Is Affected

- **Organizations**:
  - Businesses, governments, and non-profits of all sizes seeking to improve cybersecurity (e.g., small firms using IG1, enterprises using IG3).
  - Particularly those aligning with regulations (e.g., DoD contractors via NIST mappings) or in critical sectors (e.g., elections via EI-ISAC).
- **Governments**:
  - U.S. state/local/tribal entities via MS-ISAC; election offices via EI-ISAC.
- **Employees and Vendors**:
  - IT/security teams implementing controls; third-party providers monitored under supply chain requirements.
- **Regulators/Partners**:
  - Indirectly influenced (e.g., NIST references CIS); no direct enforcement.
- **Impact of Non-Implementation**:
  - No penalties from CIS, but increased vulnerability to breaches; aids avoidance of fines under aligned regs (e.g., HIPAA up to $1.9M). (Clarification: This is the annual cap per violation type, not per individual violation.)

Informational Resources

- **CIS Official Website**: cisecurity.org (free downloads of CIS Controls v8, Benchmarks, mappings, and tools like CIS-CAT Pro trial).
- **CIS Controls Page**: cisecurity.org/controls (v8 guide, IG breakdowns, FAQs).
- **CIS Benchmarks**: cisecurity.org/benchmark (downloadable PDFs for 25+ vendors; requires free registration).
- **Training and Tools**:
  - CIS RAM v2.1: cisecurity.org/cis-ram (free risk assessment method).
  - CIS Community: cisecurity.org/community (forums, webinars).
  - SANS CIS Training: sans.org (paid courses on implementation).
- **Industry Resources**:
  - NIST Mappings: cisecurity.org/controls/mapping (free alignments to NIST 800-53, HIPAA).
  - "CIS Controls Guide" (free PDFs from Splunk or Tenfold Security).
- **Community Support**:
  - MS-ISAC/EI-ISAC: msisac.cisecurity.org and ei-isac.org (threat sharing for governments).