CIS Controls

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.

Basic

1. Inventory and Control of Hardware Assets
   - Physical and logical security controls should be in place for all hardware assets.
2. Inventory and Control of Software Assets
   - Software inventory and controls should be in place to manage software risks.
3. Continuous Vulnerability Management
   - Vulnerability scans and patches should be performed regularly.
4. Controlled Use of Administrative Privileges
   - Administrative privileges should be limited to the smallest possible scope.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
   - Devices should be configured securely to prevent vulnerabilities.
6. Maintenance, Monitoring, and Analysis of Audit Logs
   - Audit logs should be monitored and analyzed to detect security incidents.

Foundational

7. Email and Web Browser Protections
   - Protection against web-based attacks should be in place.
8. Malware Defenses
   - Malware should be detected and removed to prevent it from spreading.
9. Limitation and Control of Network Ports, Protocols, and Services
   - Unnecessary network services should be disabled.
10. Data Recovery Capabilities
    - Data recovery plans should be in place to protect against data loss.
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
    - Network devices should be configured securely.

Organizational

12. Boundary Defense
    - Physical and logical controls should be in place to protect boundaries.
13. Data Protection
    - Data should be protected to prevent unauthorized access.
14. Controlled Access Based on the Need to Know
    - Access should be based on the principle of least privilege.
15. Wireless Access Control
    - Wireless access should be controlled to prevent unauthorized access.
16. Account Monitoring and Control
    - User accounts should be monitored and controlled to prevent misuse.

Cybersecurity + Community

CIS RAM

CIS RAM (Risk Management and Assumption) is a framework designed to help organizations understand and manage the risks associated with their IT systems. It includes a set of guidelines for identifying, evaluating, and responding to risks.
Find Frameworks that Fit

Choose frameworks that guide the work of your cybersecurity program and, ultimately, simplify the complex world of cybersecurity in a way that can be more easily understood by business leaders.

- Control frameworks describe the security controls that are the foundation of every security program.
- Program frameworks help structure the security program, establish a basis for evaluating program activities, and simplify communication about the program.
- Risk frameworks provide a consistent approach for managing and assessing risk in a way that provides value to the business.

Choose a framework from each of these three categories to mature your program over time. Examples of common frameworks include:

**Control Frameworks**
- NIST 800-53
- NIST CSF

**Program Frameworks**
- ISO 27001
- FAIR

**Risk Frameworks**
- NIST 800-37
- NIST 800-30

Map Controls to the Framework

Security frameworks can be used together. This diagram shows how the CIS Controls can map to the Categories and Functions of the NIST Cybersecurity Framework (CSF).

- **CIS Controls #1**: Identify
  - **CIS Control 1**: Asset Management
  - **CIS Control 8**: Software and Configuration Management
- **CIS Controls #2**: Protect
  - **CIS Control 3**: Update and Patch Management
  - **CIS Control 4**: Access Control
- **CIS Controls #3**: Detect
  - **CIS Control 5**: Monitor and Control
  - **CIS Control 6**: Incident Response
- **CIS Controls #4**: Respond
  - **CIS Control 7**: Communication and Coordination
  - **CIS Control 8**: Physical and Environmental Protection
- **CIS Controls #5**: Recover
  - **CIS Control 9**: Mitigation and Contingency Planning
  - **CIS Control 10**: Risk Management

Monitor and Measure Security

To continuously improve security effectiveness:

- Establish and measure meaningful security metrics.
- Monitor those metrics frequently enough to minimize incident impact.
- Take action rapidly and efficiently to effectively improve overall security.

The CIS Controls have proven to be an effective starting point for selecting key security metrics.

Establish continuous monitoring guidelines that define which controls should be monitored on a weekly, monthly, or an ongoing basis.

**C U R R I C U L U M**

To implement security frameworks and build technically valid, business-driven security programs, engagement from all levels of leadership is required.

- Executive
  - Mission Statements
  - Board, CIO, CEO, CFO, COO, CSO, COIT, CSO

- Technology Knowledge Base
  - Network
  - Technical
  - Physical Security
  - Security Engineering

- Security Leadership
  - SANS Security Leadership
  - FOCUS
  - Critical Security Controls – In-Depth

- Technical
  - Technology Leadership
  - Technical Skills
  - Databases
  - Tools

- Business knowledge increases as you move up

- New Technology
- Technical Skills

- Risk Management

- Critical Security Controls – In-Depth

- Security Awareness

- ISO 27001

- Risk Management

- Business Environment

- Supply Chain Risk Management

- Information Protection Processes

- Identity Management,
  - Information Protection Processes
  - Supply Chain Risk Management

- Business Objectives

- Empowerment

- Negotiation

- Communications

- Risk Acceptance

- Monitor and Measure Security

- **CIS Controls #19**: Business Environment
  - **CIS Control 19**: Establish and Leverage Metrics

- **CIS Controls #10**: Communications
  - **CIS Control 10**: Mitigation and Contingency Planning

- **CIS Controls #15**: Physical Security
  - **CIS Control 15**: Physical and Environmental Protection

- **CIS Controls #7**: Incident Response
  - **CIS Control 7**: Monitoring and Control

- **CIS Controls #9**: Risk Management
  - **CIS Control 9**: Risk Management Frameworks

- **CIS Controls #6**: Control Frameworks
  - **CIS Control 6**: Control Frameworks

- **CIS Controls #5**: Incident Response
  - **CIS Control 5**: Incident Response

- **CIS Controls #4**: Access Control
  - **CIS Control 4**: Access Control

- **CIS Controls #3**: Monitoring and Control
  - **CIS Control 3**: Monitor and Control

- **CIS Controls #2**: Update and Patch Management
  - **CIS Control 2**: Update and Patch Management

5 Keys for Building a Cybersecurity Program

- **Control Frameworks**
  - **NIST 800-53**: Controls are described in a standardized, modular format.
  - **NIST CSF**: Framework provides a high-level view of the security landscape.

- **Program Frameworks**
  - **ISO 27001**: Framework provides a comprehensive approach to information security.
  - **FAIR**: Framework provides a structured approach to risk management.

- **Risk Frameworks**
  - **NIST 800-37**: Framework outlines risk management practices.
  - **FAIR**: Framework provides a structured approach to risk management.

SANS Training to Implement the CIS Controls and Build a Security Program

**SEC66**: Implementing and Auditor the Critical Security Controls – In-Depth

This course gives security professionals the tools they need to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to lead, inspire, and motivate your teams.

**MG514**: Security Strategic Planning, Policy, and Leadership

This course shows you the tools you need to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to lead, inspire, and motivate your teams.

- “I moved into management a few years ago and am currently working on a new security strategy roadmap and this class just condensed the past two months of my life into a one week course and I still learned a lot!”

- “This training sets the stage for executive level success. If you are interested in ever becoming a CISO, this course is a must.”

sans.org/curricula/management

sans.org/sec66

sans.org/mg514