RSI | Datasheet

CIS Controls

Advisory Services

The Center for Internet Security (CIS) Controls condense safeguards from various regulatory guides into one manageable framework. These controls were formerly known as the CIS Critical Security Controls—or CIS CSC. CIS Controls are a prioritized set of actions designed to protect your organization from all known threat vectors. Here are some of the key elements involved in the CIS Controls.

Asset Control

The CIS framework requires visibility and governance over all physical and virtual assets, including strict access monitoring controls.

Secure Communication

Services such as email and messaging apps must be secured to prevent social engineering and other related cybercrimes.

Threat Prevention

Your company must safeguard against the rapidly escalating threats of cybercrime. CIS Controls provide up-to-date protections.

Security Benchmarks

Measuring your security practices and staff behaviors against the CIS benchmarks facilitates risk awareness and preparation.

Ongoing Training

Education and training on detecting and preventing threats is required to ensure that all staff members maintain awareness.

Reputation Protection

Implementing CIS Controls bolsters your reputation, prevents cyberattacks, and minimizes your risk profile.

The 18 CIS Controls

The CIS framework comprises 153 safeguards, distributed across 18 distinct Controls:

1. Enterprise Asset Inventory
Management of all physical assets (5 safeguards).

2. Software Asset Inventory
Management of all virtual assets (7 safeguards).

3. Data Protection
Safe handling of sensitive data (14 safeguards).

4. Security Configuration
Security settings across systems (12 safeguards).

5. Account Management
Management of all user accounts (6 safeguards).

6. Access Control
Tight restriction of data access (8 safeguards).

7. Vulnerability Management
Continuous threat tracking (7 safeguards).

8. Audit Log Management
Auditing and careful audit logging (12 safeguards).

9. Email / Browser Safety
Protections for email and web vectors (7 safeguards).

10. Malware Defenses
Maintenance of antivirus software (7 safeguards).

11. Data Recovery
Maintenance of secure data backups (5 safeguards).

12. Network Infrastructure
Management of secure networks (8 safeguards).

13. Network Monitoring
Monitoring of all network traffic (11 safeguards).

14. Security Awareness Training
Maintenance of security training program (9 safeguards).

15. Service Provider Management
Management of third-party risks (7 safeguards).

16. Application Software Security
Maintenance of application security (14 safeguards).

17. Incident Response
Management of security events (9 safeguards).

18. Penetration Testing
Regular execution of pen-testing (5 safeguards).

Optimization of Your CIS Controls Implementation

Flexible Implementation
RSI Security will work seamlessly with your in-house team to implement all of the CIS Controls on your schedule.

Resource Efficiency
Your initial and ongoing implementation will be strategized for maximum efficiency and ROI.

Roadmap Development
A custom roadmap will be developed based on your current posture and present status for all CIS requirements.

Long-Term Optimization
We'll work with you to maintain long-term implementation as the CIS Controls evolve over time with new version releases.

About RSI Security

RSI Security has been working with the Center for Internet Security Controls and all previous versions of CIS CSC since the initial release of them in 2008. As a full-suite cybersecurity and compliance advisory firm, our team is well equipped to expertly handle the management of all CIS requirements. Connect with us to get started on CIS Controls implementation and a consultation on any additional applicable compliance frameworks. We will design a tailored cybersecurity program to minimize your organizational risk and systematize your compliance efficiently.

www.rsisecurity.com • 858.999.3030 • info@rsisecurity.com