DATA SHEET

CIS SANS 20

Compliance Consulting Services

AT A GLANCE

Si works with its clients to implement SANS 20 controls to enforce technical safeguards and operational procedures that strengthen defences against cyber threats.

The SANS 20 Critical Security Controls are a prioritised list designed to provide maximum benefits towards improving risk posture against real-world threats. This list of 20 control areas grew out of an international consortium of U.S and international agencies and experts, sharing from actual incidents and helping to keep it current against evolving global cyber security threats. Additionally, the SANS Top 20 CSC are mapped to NIST controls as well as NSA priorities.

KEY ADVANTAGES OF SANS 20

BENEFITS OF IMPLEMENTING SANS 20 CONTROLS

- Compared to other international security standards the number of controls to implement are very few
- Correctly implementing SANS20 controls helps mitigate all major risks
- Follows a thorough yet common sense approach to identify risks which is easy to understand

WHY SI?

1. Certified, expert consultants with significant experience in this domain
2. Our no-nonsense approach that focuses purely on achieving client objectives
3. In depth industry knowledge through subject matter experts allowing us to offer not just technical but very business oriented advice

SANS TOP 20 CONTROLS

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices such as Firewall Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

IMPLEMENTATION THE 7 STEPS

1. Take inventory of your assets
2. Measure asset control
3. Evaluate the most critical gaps
4. Plan and implement your controls
5. Test your controls
6. Train and monitor users
7. Respond to incidents