cavirin

Compliance Solution Brief

THE CHALLENGE

Reputation is the new target for cyber attacks

- Criminals value information – financial, health, critical infrastructure
- When assessing and documenting Cyber risk it's hard to know if we've got it right
- The pace of technology increases unknown dependency on third parties
- IT cannot trace or control our data – exfiltration occurs
- The role of government and information custody is often misunderstood
- External auditors share how well your systems, software, and procedures worked with actual data collected across a specified timeframe.
- Findings in audit reports become barriers to business.
- In today's cloud economy, customer due diligence has gone from *nice to have* to **mandate.**

Center for Internet Security

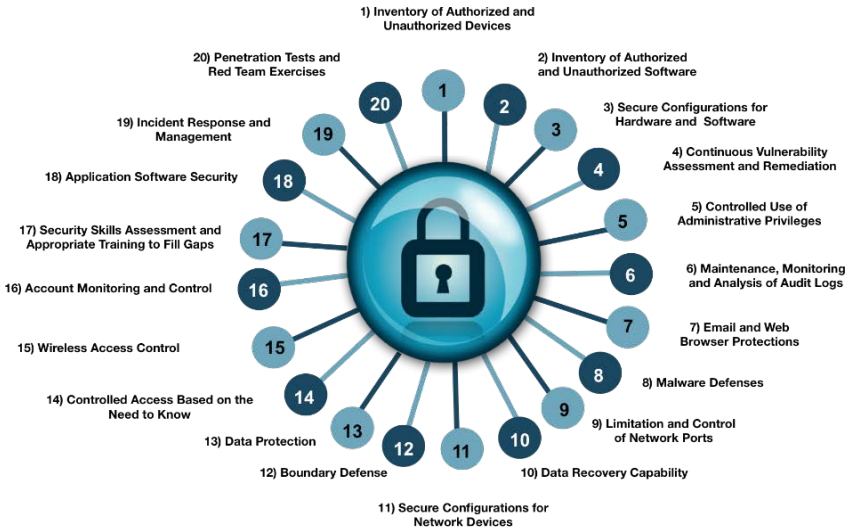
Center for Internet Security Critical Security Controls v.6.0

CIS Critical Security Controls™ SUPPORTER

Why comply with CIS CSC v.6.0?

The Center for Internet Security's Critical Security Controls are especially relevant because they are updated by cyber experts based on actual attack data pulled from a variety of public and private threat sources. Organizations that implement CIS Controls are likely to prevent majority of cyber-attacks. The CIS Critical Security Controls™ (CIS Controls) are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber-attacks. CIS CSC v6.0 contains important components that make-up an effective cyber defense system, allowing companies to prioritize controls that protect against the greatest threats, provide metrics for IT personnel to understand, continuously diagnose and mitigate risks, and automate defenses to ensure compliance with the controls.

> With regard to Critical Security Controls, CSC "*…failure to implement all of the controls that apply to an organization's environment constitutes a lack of reasonable security.*"
>
> Kamala Harris, Attorney General, CA



Cavirin Security and Compliance offers system based mapping of CIS Benchmark rules according to their most relevant CIS CSC 6.0 risks, making failure and success in IT controls continuously available to risk management reporting process.

CIS CSC is the right choice

- Referenced by the U.S. Federal Government in the NIST Cybersecurity Framework and other guidelines, and validated by the Australian government
- Recommended by the U.S. National Governor's Association, the UK's Centre for the Protection of National Infrastructure (CPNI), Symantec, Zurich Insurance, and others

cavirin

Compliance Solution Brief

Leveraging CIS CSC risk findings to optimize environments and pass audits faster

Facing multiple forms of external controls assessment, organizations often fail due to improper security settings, incorrect configurations, low levels of encryption, or poor policies and procedures. Continuous testing over those controls could have prevented costs in business disruption, time consuming client discussion, or lost business opportunities.

Cavirin's ARAP™ solution automatically checks system configuration settings across all target environments, reporting against expected system based SOC 2 Illustrative criteria. Review and response to address recommended fix actions allows timely remediation to found problems, and further rewards the business by rapid completion of unnecessarily disruptive SOC 2 audit events.

THE SOLUTION

Cavirin's Automated Risk Analysis Platform (ARAP™) assists Chief Risk & Security, as well as IT and DevOps leadership in gathering configuration data used to address their top security and compliance challenges:

- Settings that indicate missing patches for operating systems and applications.
- Monitoring and detecting sensitive data loss (data exfiltration)
- Locating policies that enable weak passwords.
- Lack of logs and audit trails necessary to conduct forensics
- Security validation for new systems
- Missing or outdated anti-malware technology
- Settings that enable encryption of sensitive information in transit
- The information necessary to remediate deficiencies that would otherwise be impossible to manage due to the lack of trained staff maintaining security controls.

Compliance in any environment

- Cloud Native platform supporting 12-factor patterns (things like port binding, logs, concurrency…)
- A "hyper plane" of integrated "risk assessment" amongst segmented vulnerability domains
- Works with Private, Hybrid, and Public Clouds and Support **AWS**, **Azure**, **GCP** (Google Cloud Platform)
- Manages thousands of out-of-box policies, well curated and certified (SCAP, XCCDF, OVAL)
- Supports most compliance authorities (PCI, HIPAA, NIST, SOC2, FedRamp, CIS Benchmark, DISA, CIS CSC, CSF)
- Is CIS Certified security content (Multiple OS, Docker, AWS Cloud)
- Complies with DISA standards in all aspects of delivery and reported results

Center for Internet Security and Cavirin

Cavirin Security and Compliance actively contributes to CSC mapping with NIST Cyber Security Framework (CSF) and NIST 800-53 r4 and Appendix J for Privacy, making this contribution publically available through the Champion contribution. In fact, Cavirin Security and Compliance actively contributes to all major standards and organizations responsible for the mapping of regulatory requirements and the most highly leveraged national and international standards. In addition to organic CIS Benchmarks and DISA STIG NIST based configuration management, Cavirin has implemented all assessments with NIST Cyber Security Framework (CSF) and NIST 800-53 r4 and Appendix J for Privacy. Clients who elect to use multiple policy packs, including ISO27002:2013, will benefit by the extended use of multiple frameworks to align Information Security Programs and Policy.