

USE CASE

CRITICALSTART® CIS Critical Security Controls v8 Risk Assessment

KEY BENEFITS

- ✓ Assess current posture
- ✓ Roadmap pragmatic improvements
- ✓ Comply with federal and state requirements
- ✓ Obtain compliance evidence
- ✓ Reduce cyber risk
- ✓ Facilitate simplified audit reporting, meeting multi-framework oversight demands
- ✓ Cost-effective for small to mid-sized businesses (SMBs)

Guidelines to protect your organization from cyber threats

The Center for Internet Security (CIS) Critical Security Controls v8 Risk Assessment template provides a prioritized, prescriptive set of safeguards to help mitigate the most prevalent cyber-attacks against systems and networks. These suggested best practices are mapped to and referenced by multiple legal, regulatory, and policy frameworks to ensure the identification and recommendation of the most effective technical security controls needed to stop attacks.

Ideal use cases

Practical for organizations of all types and sizes, including small to mid-size businesses and contractors needing foundational security guidance, the CIS Critical Security Controls v8 assessment offers a cybersecurity baseline to protect companies from cyber threats.

This risk assessment is applicable for:

- State and local government agencies
- Healthcare providers
- Financial services institutions
- Public school systems
- Small-to-medium retailers

How it works

Critical Start's Cyber Risk Dashboard displays security maturity levels ranked against CIS Critical Security Controls v8 requirements. The Dashboard also contains Risk-Ranked Reduction Recommendations so that organizations can identify, prioritize, and mitigate the gaps that would hinder risk reduction and limit federal and state opportunities. With the information the assessment provides, Critical Start can:

- Catalog deployed safeguards in place and map them back to the 18 control categories outlined in the CIS Critical Security Controls v8
- Pinpoint gaps that leave defenses exposed
- Provide actionable remediation recommendations to achieve compliance
- Detail compliance evidence for audits

Responses to CIS Critical Security Controls v8 facilitate simplified audit reporting and benchmarking against peers compliant with related standards and infosec frameworks, meeting multi-framework oversight demands by correlating to other guidelines and streamlining compliance reporting by fulfilling multiple standards simultaneously.

