Protect your network against the most common cyber threats.
A CIS Controls Assessment is an excellent option for organizations that are not required to be compliant to a specified cybersecurity framework but need to secure sensitive data and feel confident in the controls they have implemented.

The CIS Controls standard focuses on defending networks and systems against the most likely and exploitable threats. Your assigned SecurityMetrics CIS Assessor will analyze your network to discover weaknesses and help you strengthen your security posture. SecurityMetrics CIS Assessors have performed similar assessments for over 20 years and will use their experience to implement industry best practices on your network.

Reduce your chances of a compromise and protect your network against common attacks with a SecurityMetrics CIS Assessment.
A SecurityMetrics CIS Audit includes three phases that cover the scope of your network, fixing your vulnerabilities, and reporting your validation. Your assessment will include:

- **A Gap Assessment and Initial Remediation Steps** - Your initial or gap assessment will begin with a phone interview that goes over the scope of your network and sensitive data environment. You will also be introduced to the CIS Controls requirements. At the same time, your SecurityMetrics CIS Assessor gets a preliminary feel for security areas you may need to improve. During this phase, any initial remediation work can take place before the onsite assessment.

- **An Onsite Validation** - When you have completed your initial remediation steps and feel ready for a validation assessment, your SecurityMetrics CIS Assessor will come onsite to validate your compliance to the CIS Controls. This phase typically lasts less than a week. Your assessor will visit your facility and begin collecting evidence that demonstrates you meet the CIS Controls and safeguards. If any additional weaknesses are found, a post-assessment report is generated, highlighting areas that need final remediation.

- **Final Remediation and Reporting** - This phase lasts 45 days and begins after your onsite validation. During this phase you should fix gaps discovered while your assessor begins a report detailing your results and post-onsite remediation efforts. A final report that documents your compliance to the CIS Controls is issued approximately 60 days after the on-site visit.

A SecurityMetrics CIS Assessment can be customized to your unique situation and time constraints, so you can protect your organization and remain operable. Your SecurityMetrics Assessor will work with you to meet requirements in a manageable way.
TAKE ADVANTAGE OF ASSESSOR EXPERTISE

SecurityMetrics CIS Assessors have performed cybersecurity assessments for over 20 years. SecurityMetrics CIS Assessors have experience with many cybersecurity and privacy frameworks, including PCI DSS, HIPAA, HITRUST, and GDPR. SecurityMetrics also has dedicated professional services staff for forensic incident response, vulnerability scanning, security operations monitoring, and penetration testing.

WHY CHOOSE SECURITYMETRICS?

We help customers close data security and compliance gaps to avoid data breaches. We provide managed data security services and are certified to help customers achieve the highest data security and compliance standards. We help local shops as well as some of the world’s largest brands achieve data security through managed services and compliance mandates (PCI, HIPAA, HITRUST, GDPR).
Interested in learning more?

Request a Quote