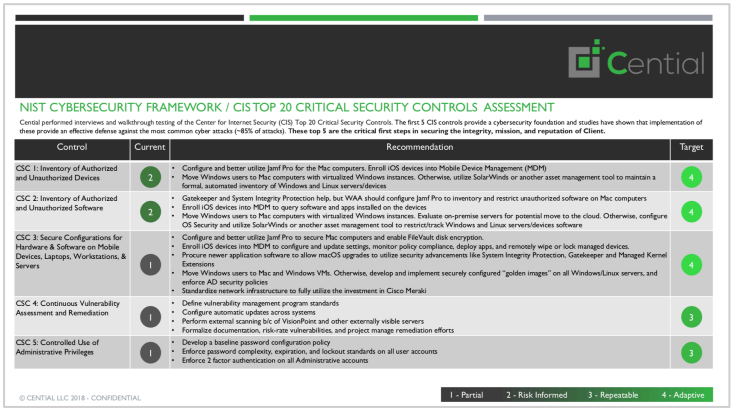
Cybersecurity Assessment

Assess and improve your security posture.

Let Cential experts show you the current status of your cybersecurity program and the best way to improve it to handle tomorrow's threats.

Whether your organization is in the early stages of building their cybersecurity program, or whether you need guidance to ensure you're properly following best practices, Cential's cybersecurity assessments are tailored to your organization's needs. We work closely with your technology teams to create a comprehensive assessment of your technology environment and how it aligns with cybersecurity framework guidance and best practices. This assessment is a critical step in establishing, monitoring, and improving your information security program.



NIST CYBERSECURITY FRAMEWORK / CIS TOP 20 CRITICAL SECURITY CONTROLS ASSESSMENT

Cential performed interviews and walkthrough testing of the Center for Internet Security (CIS) Top 20 Critical Security Controls. The first 5 CIS controls provide a cybersecurity foundation and studies have shown that implementation of these provide an effective defense against the most common cyber attacks (~85% of attacks). **These top 5 are the critical first steps in securing the integrity, mission, and reputation of Client.**

Control	Current	Recommendation	Target
CSC 1: Inventory of Authorized and Unauthorized Devices	2	• Configure and better utilize Jamf Pro for the Mac computers. Enroll iOS devices into Mobile Device Management (MDM) • Move Windows users to Mac computers with virtualized Windows instances. Otherwise, utilize SolarWinds or another asset management tool to maintain a formal, automated inventory of Windows and Linux servers/devices	4
CSC 2: Inventory of Authorized and Unauthorized Software	2	• Gatekeeper and System Integrity Protection help, but WAA should configure Jamf Pro to inventory and restrict unauthorized software on Mac computers • Enroll iOS devices into MDM to query software and apps installed on the devices • Move Windows users to Mac computers with virtualized Windows instances. Evaluate on-premise servers for potential move to the cloud. Otherwise, configure OS Security and utilize SolarWinds or another asset management tool to restrict/track Windows and Linux servers/devices software	4
CSC 3: Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers	1	• Configure and better utilize Jamf Pro to secure Mac computers and enable FileVault disk encryption. • Enroll iOS devices into MDM to configure and update settings, monitor policy compliance, deploy apps, and remotely wipe or lock managed devices. • Procure newer application software to allow macOS upgrades to utilize security advancements like System Integrity Protection, Gatekeeper and Managed Kernel Extensions • Move Windows users to Mac and Windows VMs. Otherwise, develop and implement securely configured "golden images" on all Windows/Linux servers, and enforce AD security policies • Standardize network infrastructure to fully utilize the investment in Cisco Meraki	4
CSC 4: Continuous Vulnerability Assessment and Remediation	1	• Define vulnerability management program standards • Configure automatic updates across systems • Perform external scanning b/c of VisionPoint and other externally visible servers • Formalize documentation, risk-rate vulnerabilities, and project manage remediation efforts	3
CSC 5: Controlled Use of Administrative Privileges	1	• Develop a baseline password configuration policy • Enforce password complexity, expiration, and lockout standards on all user accounts • Enforce 2 factor authentication on all Administrative accounts	3

© CENTIAL LLC 2018 - CONFIDENTIAL

1 - Partial | 2 - Risk Informed | 3 - Repeatable | 4 - Adaptive

Get the most for your cybersecurity spend – fast.

Timing is critical, so we provide immediate feedback while onsite and deliver a detailed report with recommendations within two weeks of the conclusion of our onsite activity. The process includes:

- A formal kick-off meeting with key stakeholders
- Up to five days of hands-on discovery sessions with your technology teams and business process owners
- Our detailed assessment tool showing security areas, security controls, and detailed security standards assessed, qualitative conclusions, and calculated quantitative scoring at each level
- A formal report customized for your organization based on our onsite discovery and our internal processes, tools, and methodologies
- Observations giving insight into key themes and opportunities found
- An in-depth closing meeting covering key findings and actionable recommendations

Benefits

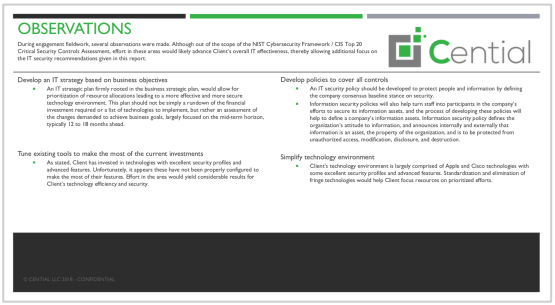
Cential combines onsite and offsite services to:

- Assess your technology environment's security posture
- Provide feedback and suggestions on information security best practices
- Mentor your team
- Provide immediate feedback
- Deliver a clear, focused report with actionable recommendations
- Plan implementation milestones and next steps
- Provide security awareness and training

Assessment Frameworks

Our expert developed assessment programs include:

- NIST CSF
- CIS CSC
- COBIT
- ISO 27001
- GDPR Security Risk
- HIPAA Security Risk



OBSERVATIONS

During engagement fieldwork, several observations were made. Although out of the scope of the NIST Cybersecurity Framework / CIS Top 20 Critical Security Controls Assessment, effort in these areas would likely advance Client's overall IT effectiveness, thereby allowing additional focus on the IT security recommendations given in this report.

Develop an IT strategy based on business objectives

- An IT strategic plan firmly rooted in the business strategic plan, would allow for prioritization of resource allocations leading to a more effective and more secure technology environment. This plan should not be simply a rundown of the financial investment required or a list of technologies to implement, but rather an assessment of the changes demanded to achieve business goals, largely focused on the mid-term horizon, typically 12 to 18 months ahead.

Develop policies to cover all controls

- An IT security policy should be developed to protect people and information by defining the company consensus baseline stance on security.
- Information security policies will also help turn staff into participants in the company's efforts to secure its information assets, and the process of developing these policies will help to define a company's information assets. Information security policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.

Tune existing tools to make the most of the current investments

- As stated, Client has invested in technologies with excellent security profiles and advanced features. Unfortunately, it appears these have not been properly configured to make the most of their features. Effort in the area would yield considerable results for Client's technology efficiency and security.

Simplify technology environment

- Client's technology environment is largely comprised of Apple and Cisco technologies with some excellent security profiles and advanced features. Standardization and elimination of fringe technologies would help Client focus resources on prioritized efforts.

© CENTIAL LLC 2018 - CONFIDENTIAL

Ordering

Contact us today to discuss how Cential can help your cybersecurity program. Email info@cential.co.