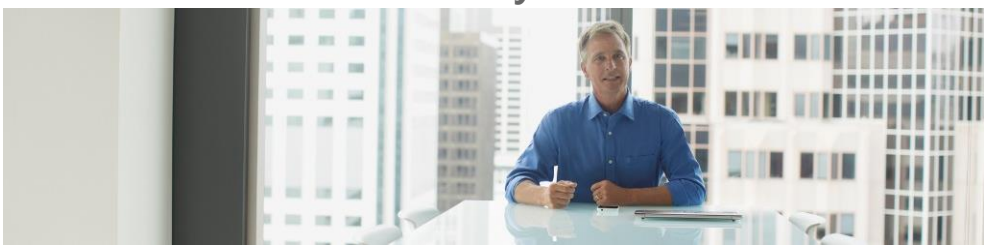
SIGNATURE CONSULTANCY

Cyber Resilience: Assessment

Assess and Validate your Current Cyber Security Controls against CIS Controls V 7

(CIS: Center of Internet Security)

For Organizations looking to improve their security posture and harden their defenses against the various attack vectors, the Cyber Resilience Assessment along with the associated recommendations provides a solid starting ground to reduce risk and exposure, build risk mitigation for most of the severe Cyber attack types against world class security standard: **CIS 20 Critical Security Controls**.



Organization protection

- Don't just protect the network, protect all critical assets
- Implement the right security policies, processes and procedures
- Improve defenses against known attack vectors
- Improve global security posture
- Reduce Risk Exposure
- Mitigate Threat Security Risks

Basic Controls

- **As-is-Analysis** Against Basic Security Controls.
- **Gap** Analysis
- **In-Person** Interviews
- **Review** Implemented Policies & Procedures (documented/ad-hoc)
- **Covers** Network, Hardware, Software, Administrative Privileges, Vulnerability Scanning
- **Findings & Recommendations** Report

Foundational Controls

- **As-is-Analysis** Against Foundational Security Controls.
- **Gap** Analysis
- **In-Person** Interviews
- **Review** Implemented Policies & Procedures (documented/add hoc)
- **Covers Basic Controls** + Email Analysis, Web Application Scanning, Malware Defense Analysis, Protocols & Network Analysis, Data Recovery & Protection Analysis, Boundary Defense Scanning, Access Analysis, Wireless Scanning, account & Monitoring Analysis.
- **Findings & Recommendations** Report

Organizational Controls

- **As-is-Analysis** for the organizational Security Controls.
- **Gap** Analysis
- **In-Person** Interviews
- **Review** Implemented Policies & Procedures (documented/add hoc)
- **Covers Foundational Controls +** Security Training Analysis, Application Analysis, Incident Response Analysis, Penetration Tests & Red Team Exercise Analysis
- **Findings & Recommendations** Report

 | www.signatureconsultancy.com | +961 4 916 307

Cyber Resilience: Assessment

How does it work and what to expect?

Planning & Data Collection

- Define engagement Goals and Scope
- Gather in-scope Information
- Discover in-scope Assets and Data
- Interview Stakeholders

Data Analysis

- Inventory and Control of Hardware and Software
- Analysis of Security Policies
- Analysis of Security Processes & Procedures
- Business Priority Mapping

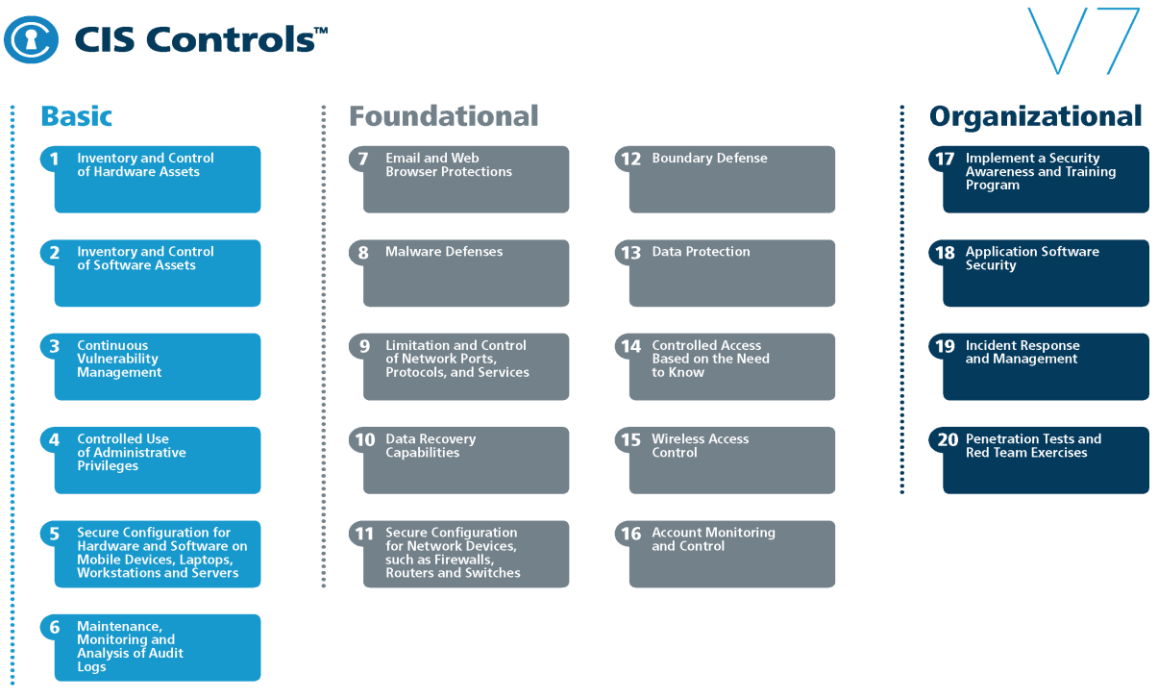
Findings & Recommendations

- Document and share the findings and related recommendations based on CIS Security Controls
- Present and Discuss Findings and Recommendations

Benefits

- Ensure effective defense controls
- Increase resiliency to Cyber attacks
- Increase recovery efficiency
- Minimize potential data loss
- Improve asset Security measures
- Reduce Cybersecurity incidents cost
- Improve awareness and reduce insider threat risk

The Center for Internet Security Critical Security Controls for effective Cyber Defense is a publication of standards for computer security following a prioritized set of actions to protect your organization and data from known cyber attack vectors.



 | www.signatureconsultancy.com

CR:A-int-v2