



Objective and Frameworks

- Current security posture Assessment
- Gap Analysis
- Threat profile Creation
- Security protection and Control Implementation

Security Frameworks:

- NIST, ISO 27001, CIS, CSA etc.



Scope Identification

- Identification of devices and applications
- Organizational communication
- Cybersecurity roles and responsibilities
- Critical functions, services, applications
- Cyber Security Policies, procedures
- Incident response Process
- Cyber threat intelligence feeds
- Threat identification
- Patch management Process
- Vulnerability Assessment reports
- Penetration testing reports Assessment



Assessment and gap analysis

- Define Security Assessment Methodology
- Review existing security policies and Control
- Understand threats and vulnerabilities
- Gap Analyses



Security Controls Implementation

- Identification of applicable security controls
- Preventive Control
- Detective Control
- Responsive Control

Applicable Controls:

- NIST Control
- CIS benchmarking
- SANS Procedural Control

Outcomes & Deliverables

Stakeholder Notes (Daily)
 Kickoff Presentation (Week 1 Only)
 Business Driver Presentation (Week 1 Only)
 Findings, Themes (Weekly)
 Checkpoint Meeting Summary (Weekly)

Architecture Scorecard/Index (Final)
 Gap Summary and Analysis (Final)
 Current State & Future State Summary (Final)
 Impact Analysis (Final)
 Recommendation Report & Execution Plan (Final)