Overview

Threats to information security continue to grow making it almost commonplace to hear of breaches in the news almost weekly. No longer can an organization maintain the status quo with regards to information security but must work to evolve the defenses put into place to keep pace with the ever-growing threats. In most cases this will be a requirement for doing business with other organizations. In addition, more and more organizations are requiring proof that a certain level of information security has been, and will continue to be, addressed.

One of the first things an organization can do is to determine at what level the organization is at with regards to information security. Using this information along with the unique characteristics of the organization, it will be clear what an organization can do to reduce their risk today and how to maintain that risk level tomorrow.

This proposal outlines what goes into performing a technology risk assessment along with outcomes. TechMD works in conjunction with MAP Cybersecure, LLP to provide the items outlined in this proposal.

Scope of Work

This assessment includes Information Security Controls from the following standards, regulations and certifications:

- ISO 27001 and 27002
- NIST:800-171
- PCI-DSS 3.2.1
- CIS20 Version 7.1 • CCPA

NIST/ISO/CSC/CIS Security Risk and Capability Maturity Level – Manual Assessment

Scope of Work:

- Security Capability Maturity Level rating
- Executive summary
- Full Detail Report and Risk Report
- 12-month roadmap to improve at least two Security Maturity Levels

The outcome of this Risk Assessment will be a 0 to 5 rating on the Security Capability Maturity Level based on requirements for NIST SP:800-171 CSF, PCI-DSS 3.2.1 ,CIS20 v7.1, and ISO 27001 and 2. The score will help assess how statistically likely the organization is to have a Security, Confidentiality or Integrity incident based on the root cause of actual breaches reported to the US Computer Emergency Response Team (US-CERT) in previous years.

1. Selection of Criteria and Checklist Creation
    a. Select & Recommend Specific Security Control
    b. CIS20, reference: https://www.sans.org/critical-security-controls/
2. Gap Assessment for in-scope requirements
    a. Written and Approved Information Security Policy
    b. Assess Certification Readiness

c. Data Governance and Classification
d. Asset Inventory and Device Management
e. Access Controls and Identity Management
f. Business Continuity and Disaster Recovery Planning and Resources
g. Systems Operations and Availability Concerns
h. Systems and Network Security
i. Systems and Network Monitoring
j. Systems and Application Development and Quality Assurance
k. Physical Security and Environmental Controls
l. Customer Data Privacy
m. VendorandThird-PartyServiceProviderQualificationandManagementProcedure
n. Risk Assessment
o. Incident Response and Change Management Procedures

3. Discovery and Review
    a. Review all Data from Section 2
    b. Apply Appropriate Security Capability Maturity Level to all In-Scope Controls
    c. Determine the Organization's Security Capability Maturity Level
4. Summary Report
    a. Summarize Scope & Findings
    b. Highlight Risks According to Priority
    c. Report the Organization's Security Capability Maturity Level
    d. Recommend Remediation Roadmap for Highlighted Risks

Assumptions & Notes

In performing these services, the following scope specific assumptions listed below will apply:

- Organization will make available the appropriate personnel required by the assessment process. This includes someone from each of the following areas:
    - Executive
    - Human Resources (HR)
    - Information Technology (IT)

Payment Terms

Upon acceptance, 50% of the total is due. The remaining 50% will be due upon the delivery of the Summary Reports.

Timeline

Upon acceptance of this proposal, the assessment can be scheduled to start two to four weeks out and will take approximately six to eight weeks to complete.