Town of Westlake

Strategic IT and Security Assessment

Scope of Work

Assessment Deliverables:

Executive Summary:

- Assessment Criteria Explanation
- Analysis summary of the current state of IT
- Analysis summary of existing risk
- Analysis summary of strategic, operational and risk mitigation recommendations
- Current state of IT Detail
- Gap analysis against known best practices
- Provide the foundation for the creation of a strategic technology plan
- High-level recommendations for risk mitigation, ranked by risk

Assessment Criteria

1. *Determine Risk to Confidentiality, Integrity and Availability (CIA)*
   a. Perform a manual, mid-level assessment of infrastructure and its configuration
   b. Active Directory – Health and Configuration Discovery
   c. Active Directory – Administrator, User, Security Group and Share Permission Discovery
   d. Active Directory – Group Policy Configuration Discovery (including password policies)
   e. Windows Server and SQL Server Discovery
   f. Windows Workstation and Installed Application Discovery (best effort)
   g. Vulnerability Scan - External, Public IP Address Range(s)
2. *Operational Framework-Servers, cloud, networks, third party and developed applications*
   a. Assess existing Cloud (email and collaboration, cloud servers) and Infrastructure (physical) configuration, IT management practices against industry best practice methodologies and standards-based management
   b. Assess existence of comprehensive documentation platform, populated with all technology, infrastructure, vendor/supplier, software details to ensure CIA and critical knowledge retention over time

c. Existence of and adherence to standard operating procedures for IT management and security, including but not limited to incident response, patching, anti-malware management
d. Existence of and adherence to change management policies and procedures
e. Assess appropriate Role Based Access (RBAC) among the Operations team to ensure access levels are appropriate to their respective roles
f. Assess Data Backup and Restore Capability and Timeframe
    - Diagrams and DR flow documentation, if it exists
g. Assess Disaster Recovery Capability and Timeframe
h. Assess Business Continuity Capability and Timeframe

3. *End User Access, End User Devices, Connectivity, Configuration and Support*
    a. Assess End User Access Management
        - Authentication/Identification
        - Role Based Access Control (RBAC)
    b. Assess Role Based Access Control (RBAC) among the Service Desk team to ensure access levels are appropriate to their respective roles
    c. Assess Active Directory active/inactive user accounts
    d. Assess Active Directory active/inactive computer accounts
4. *Cybersecurity – Information Assurance, Threat Defense, Detection and Response Capability*
    a. Analyze manual external vulnerability scan results
    b. Analyze Active Directory assessment results
    c. Assess existence and level of layered infrastructure and endpoint threat defense, detection and response tools and expertise (anti-malware, web and DNS protection, firewall live security scanning)
    d. Assess existence of cybersecurity incident response policies, procedures, including statutory reporting requirements
    e. Assess critical infrastructure and endpoint configuration against security management best practices
    f. Assess existence of and adherence to end user cybersecurity training protocols