Mini Project 26 Security Assessment

Executive Summary

A security assessment was performed by the Risk Management team in order to:

1) Identify areas of concern within the organization
2) Categorize observations by severity in order to identify priority for remediation
3) Provide recommendations for remediation of risks identified
4) Provide control number references for additional in-depth references for remediation

Risk Register

A Risk Register was created to organize and identify findings. Concerns are identified as observations, from which Risks to business are identified and ranked. Risks are ranked between Low, Medium, High, and Critical. Control Number and Control Description can be used as a reference by remediation teams. Recommendations are brief remediation steps that can be immediately taken to remediate risks.

This assessment specifically references the following documents for security controls:

- CIS Critical Security Controls v7.1
- CIS Password Policy Guide
- NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems

Amongst eight total risk observations, the number of severity ranks are:1

- Critical: 1
- High: 5
- Medium: 2
- Low: 0

The eight total observations and their severity rank are:

1. Too many people have admin access (Critical)
2. Password requirements are misconfigured (High)
3. Unauthorized code changes could be occurring (High)
4. Backup tapes may be inadequate and are not being tested (Medium)
5. Backup power source may be inadequate and is not being tested (High)
6. Improper database access could be occurring (High)
7. Policies and procedures are outdated (Medium)
8. Remote access is performed via RDP (High)

Immediate recommendation is to address 1 Critical and 5 High risks following recommendations on the Risk Register, and then address Medium risks as business needs allow.