

The goal of a security assessment, (also known as a security audit or security review), is to ensure that necessary security controls are integrated into the infrastructure, applications and processes. A properly completed security assessment should provide documentation outlining any security gaps between existing processes and approved corporate security policies. Management can address security gaps in three ways: Management can decide to cancel projects/applications/procedures that do not meet standards, allocate the necessary resources to correct the security gaps, or accept the risk based on an informed risk / reward analysis.

They are looking for a PM to come in to facilitate this program. The PM should have experience planning and overseeing similar Risk Assessment/Mitigation campaigns (ISO 27000, SOX, HIPPA, RedFlag). The PM will be expected to work with various departments to locate, assess, plan mitigation/remediation for IT Security threats and vulnerabilities, and document findings.

Timeframe is a start of early May – duration to be determined.

Requirements: PMI Certification and experience planning and overseeing similar security assessment projects with medium to large scale organizations (500-1000 users).

Subject Matter expertise of Security Assessments and CISSP or CISA certifications would be helpful.

Keywords: There are common vendor-neutral professional certifications for performing security assessment.

- CISSP
- CISA
- BS7799 Lead Auditor - ISO/IEC 27001:2005 Auditor/Lead Auditor

<http://slc-staffing.com/nevada-staffing.html>