MEMORANDUM FOR <AO Name>
Authorizing Official
<Company Name>

FROM: Steven Senz
Certified Information System Auditor
Your Cybersecurity Matters

SUBJECT: Accreditation Statement

Reference:
1. NIST SP 800-171
2. Risk Management Framework – NIST guidance
3. System Security Plan <Insert Name>

Background

Between <Start Date> and <End Date>, a Security Test and Evaluation (ST&E) was conducted on the <System Name> operated by the <Organization/Office> located at <Location>. The ST&E was performed by <Name> under the direction of the undersigned Certifying Agent under the authority of <Name> Authorizing Official (AO), <Company Name>, and was conducted in accordance with the Risk Management Framework. The purpose of the ST&E was to demonstrate, through selected verification techniques and verification procedures documented in the <System Name> ST&E Plan (dated <Date>) and ST&E Report (dated <Date>), that necessary security controls that are identified in the <System Name> Security Plan (dated <Date>) are implemented correctly, meet minimum security requirements, are effective in their application, and that the controls adequately mitigate risks described in the <System Name> Risk Assessment Report (dated <Date>). The certification effort provides the Approving Official with important information necessary to make an informed, risk-based decision regarding the operation of <System Name>.

Summary of Findings

The results of the certification effort are summarized in the following two figures:

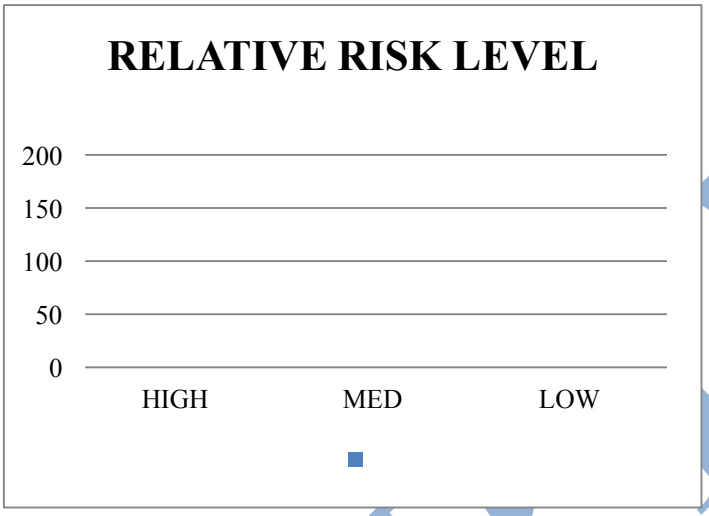

Figure 1

<Number> vulnerabilities found in <System Name> controls are ranked as <Low, Moderate, or High> risk as determined by risk assessment engine of ASCERTIS and tailored to account for compensating controls. Therefore, <System Name> is categorized as having a <Low, Moderate, or High> level of risk.

The results of the risk assessment of <System Name> indicated that the primary risks to system resources related to <appropriate risk e.g. unlawful/unauthorized acts committed by hackers, computer criminals, and insiders related to system intrusion, fraud, and spoofing>. <Unintentional user errors and omissions> are additional critical risks to system data and operations.

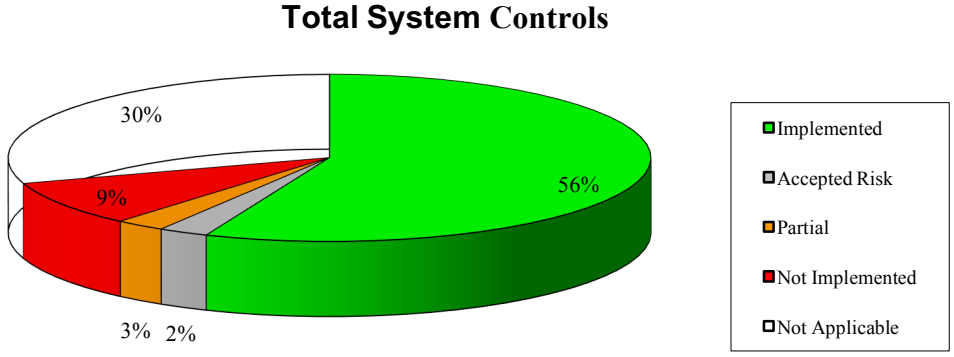

Figure 2