Risk Assessment Document

This document identifies and assesses potential risks in IT infrastructure, including vulnerabilities and threats.

**Template Structure**:

1. **Title Page**
   * Document Title: "Risk Assessment Report"
   * Author: Rick Abraham
   * Date
2. **Introduction**
   * **Purpose**: Brief overview of the document’s purpose (e.g., to assess risks in a specific IT environment).
   * **Scope**: Define the systems or networks included in this assessment.
3. **Methodology**
   * Describe the process for identifying risks (e.g., interviews, system scans, vulnerability testing tools like Nessus).
4. **Risk Identification**
   * List each risk with the following details:
     + **Asset**: Server, network, software application, etc.
     + **Threat**: Description of the threat (e.g., unauthorized access).
     + **Vulnerability**: What makes the asset vulnerable?
     + **Risk Rating**: Rate each risk (Low, Medium, High) based on likelihood and impact.
5. **Risk Mitigation Recommendations**
   * For each identified risk, provide recommended actions:
     + **Mitigation Strategy**: Steps to reduce or eliminate the risk.
     + **Implementation Priority**: Assign a priority level (Immediate, High, Moderate, Low).
6. **Conclusion**
   * Summarize key findings and emphasize critical mitigation actions.