

DETAILED SECURITY RISK ASSESSMENT TEMPLATE

Executive Summary

[Briefly summarize the scope and results of the risk assessment. Highlight high risk findings and comment on required management actions]

DETAILED ASSESSMENT

1. Introduction

1.1 Purpose

[Describe the purpose of the risk assessment in context of the organization's overall security program]

1.2. Scope of this risk assessment

[Describe the scope of the risk assessment including system components, elements, users, field site locations (if any), and any other details about the system to be considered in the assessment]

2. Risk Assessment Approach

2.1 Participants

Role	Participant
System Owner	
System Custodian	
Security Administrator	
Database Administrator	
Network Manager	
Risk Assessment Team	

2.2 Techniques Used

Technique	Description
[List techniques used e.g., questionnaires, tools]	[Describe the technique used and how it assisted in performing the risk assessment]

2.3 Risk Model

[Describe the risk model used in performing the risk assessment. For an example risk model refer NIST publication SP-800-30]

3. System Characterization

3.1 Technology components

Component	Description
Applications	[Describe key technology components including commercial software]
Databases	
Operating Systems	
Networks	
Interconnections	
Protocols	

3.2 Physical Location(s)

Location	Description
[Include locations included in scope]	

3.3 Data Used By System

Data	Description
[Detail data elements included in scope]	[Describe characteristics of data elements]

3.4 Users

Users	Description
[Detail categories of users]	[Describe how users access the system and their intended use of the system]

3.5 Flow Diagram

[Provide connectivity diagram or system input and output flowchart to delineate the scope of this risk assessment effort].

4. Vulnerability Statement

[Compile and list potential vulnerabilities applicable to the system assessed].

Vulnerability	Description
[List vulnerabilities]	[Describe vulnerability and its impact]

5. Threat Statement

[Compile and list the potential threat-sources applicable to the system assessed].

Threat-Source	Threat Actions
[List threat sources]	[List and/or describe actions that can be taken by threat source e.g., identity theft, spoofing, system intrusion]

5. Risk Assessment Results

[List the observations (vulnerability/threat-source pairs). Each observation should include—

- Observation number and brief description of observation (e.g., Observation 1: User system passwords can be guessed or cracked)
- A discussion of the threat-source and vulnerability pair
- Identification of existing mitigating security controls
- Likelihood discussion and evaluation (e.g., High, Medium, or Low likelihood)
- Impact analysis discussion and evaluation (e.g., High, Medium, or Low impact)
- Risk rating based on the risk-level matrix (e.g., High, Medium, or Low risk level)
- Recommended controls or alternative options for reducing the risk].

Item Number	Observation	Threat-Source/ Vulnerability	Existing controls	Likelihood	Impact	Risk Rating	Recommended controls