### Security Impact Assessment (SIA)

To ensure the template aligns with industry standards, let's incorporate additional elements and structure it more clearly:

#### **1. Introduction**

Purpose: To evaluate the potential security impacts of proposed changes to the information system or its environment and to identify measures to mitigate associated risks.

Scope: This assessment covers all aspects of the proposed changes, including technical, operational, and management controls.

Audience: IT staff, security officers, system administrators, risk management personnel, and other stakeholders involved in the change management process.

#### **2. System Overview**

System Name: [System Name]

System Description:

* Function: [Brief description of the system's function and purpose]
* Components: [List of major components and their roles]
* Data: [Description of the types of data processed and stored]

System Owner: [Name and contact information of the system owner]

#### **3. Change Description**

Change Request ID: [ID Number]

Proposed Change:

* Description: [Detailed description of the proposed change]
* Reason for Change: [Explanation of why the change is necessary]
* Impact on Operations: [Potential effects on system operations]

Implementation Plan:

* Schedule: [Timeline for implementing the change]
* Resources Required: [List of resources needed for the implementation]
* Dependencies: [Any dependencies on other systems or processes]

#### **4. Security Impact Analysis**

Impact on Confidentiality:

* Potential Risks: [Identify potential risks to data confidentiality]
* Mitigation Measures: [Measures to mitigate these risks]

Impact on Integrity:

* Potential Risks: [Identify potential risks to data integrity]
* Mitigation Measures: [Measures to mitigate these risks]

Impact on Availability:

* Potential Risks: [Identify potential risks to system availability]
* Mitigation Measures: [Measures to mitigate these risks]

Impact on Authentication and Authorization:

* Potential Risks: [Identify potential risks related to authentication and authorization]
* Mitigation Measures: [Measures to mitigate these risks]

Impact on Audit and Monitoring:

* Potential Risks: [Identify potential risks related to audit and monitoring capabilities]
* Mitigation Measures: [Measures to mitigate these risks]

#### **5. Risk Assessment**

Risk Identification:

* Risk 1: [Description of the first identified risk]
* Risk 2: [Description of the second identified risk]
* [Continue as needed]

Risk Analysis:

* Likelihood: [Likelihood of each risk occurring]
* Impact: [Potential impact of each risk]
* Risk Rating: [Overall risk rating for each risk]

Risk Mitigation Strategy:

* Mitigation for Risk 1: [Strategy for mitigating the first identified risk]
* Mitigation for Risk 2: [Strategy for mitigating the second identified risk]
* [Continue as needed]

#### **6. Recommendations**

Security Enhancements:

* Recommendation 1: [First recommended security enhancement]
* Recommendation 2: [Second recommended security enhancement]
* [Continue as needed]

Policy and Procedure Updates:

* Recommendation 1: [First recommended update to policies/procedures]
* Recommendation 2: [Second recommended update to policies/procedures]
* [Continue as needed]

Training and Awareness:

* Recommendation 1: [First recommended training/awareness program]
* Recommendation 2: [Second recommended training/awareness program]
* [Continue as needed]

#### **7. Approval**

Review and Approval:

* Reviewed by: [Name and title of the reviewer]
* Date: [Date of the review]
* Approved by: [Name and title of the approver]
* Date: [Date of the approval]

#### **8. Appendices**

A. Glossary of Terms:

* Definitions of key terms and acronyms used in the assessment.

B. Supporting Documents:

* List of documents referenced in the assessment.

C. Contact Information:

* List of key contacts involved in the assessment