INFORMATION SYSTEMS RISK ASSESSMENT

System Name: _____

(System Vendor and System Name)

Instructions

✓ Determine the **Impact Type** *(Direct/Indirect/Minimal)* based on **Daily Operations, Customer Information/Personal Information,** and **Data Integrity**. Provide a **Description/Justification** for the chosen **Impact Type** in the *Risk Form.*

✓ In Table 1, based on the **Impact Type** selected, if there are different risk levels, apply the **HIGHEST** of the risk in the *Overall System Risk portion* of this assessment.

✓ Table 2 includes sample risk factors to determine the chosen level of system risk.

Risk Form

Risk Factors	Impact Type *(Choose One for Each Impact)*	Description/Justification:
Is there direct or indirect impact to Daily Operations?	☐ Low ☐ Medium ☐ High	
Is there direct or indirect impact to Customer/Personal Information?	☐ Low ☐ Medium ☐ High	
Is there direct or indirect impact to Data Integrity?	☐ Low ☐ Medium ☐ High	

Table 1: Risk Level Determination

Impact Types based on Daily Operations, Customer/Personal Information, and/or Data Integrity	Implementation Method & Risk Level		
	Out of the Box *(GAMP Category 3)*	Configured *(GAMP Category 4)*	Custom *(GAMP Category 5)*
Direct	Medium	High	High
Indirect	Low	Medium	High
Minimal	Low	Low	Low

Table 2: Examples of Risk Factors

Risk Factors	Description/Justification:
Direct Impacts to Daily Operations, Customer/Personal Information, and/or Data Integrity	Functionality/technology that has immediate or direct effect on daily operations; customer/personal information; data integrity and the state of data criteria being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available.
Indirect Impacts to Daily Operations, Customer/Personal Information, and/or Data Integrity	Functionality/technology that has a downstream effect after a series of failures, on daily operations; customer/personal information; data integrity and the state of data criteria being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available.
Minimal Impacts to Daily Operations, Customer/Personal Information, and/or Data Integrity	Functionality/technology that has minimal effect on daily operations; customer/personal information; data integrity experiencing a failure.

Overall System Risk Classification

✓ It has been determined that the overall System Risk Classification as:

☐ *Low*
☐ *Medium*
☐ *High*

✓ Please provide reasoning and/or justification for the chosen System Risk Classification below. Include any pictures, screenshots, and/or other graphics as needed as part of the evidence needed to apply the classification chosen:

[Insert reasoning/justification text here; Form will expand from this point]

Information System Security Risk Assessment Notice

It is understood that security risk assessments are a continuous activity to preserve the integrity and strength of our systems and networks. Risk assessments for all systems are recommended to be done every two (2) calendar years or more often should an incident take place. Records will be kept at a minimum of five (5) calendar years from the time the assessment has taken place. By signing below, you certify the results of the assessment is accurate and is correctly classified as of the date furnished below.

Approvals

Role/Department	Printed Name & Title	Signature	Date
Business Owner			
System Owner (IT)			
[Others As Required; Delete Row if Not Needed]			

Revision History

The following is the content change control history for this form:

Date	Version	Change(s) Applied	Personnel Applying Change(s)
01/01/2023	1.0	Creation of Information System Risk Assessment Form	Bob Bomabob
03/29/2023	1.01	Modification of Form to align with new template and document formatting guidelines	Doug Trovinger
03/30/2023	1.1	Added Section *Information Security Assessment Notice* to enhance quality of document and provide timeline for assessment records once completed.	Doug Trovinger