Computerized System Risk Assessment Workshop

Dhruw Kumar Jha

Workshop Scope

- This workshop focuses on performing the Requirements Risk Assessments (RRA) for Computerized Systems as defined in SOP-11349, *Risk Assessment* of *Computerized Systems* in order to determine the rigor of validation testing.

- It is not intended to address the Controls and Mitigations required for a computerized system being developed.

Learning Objectives

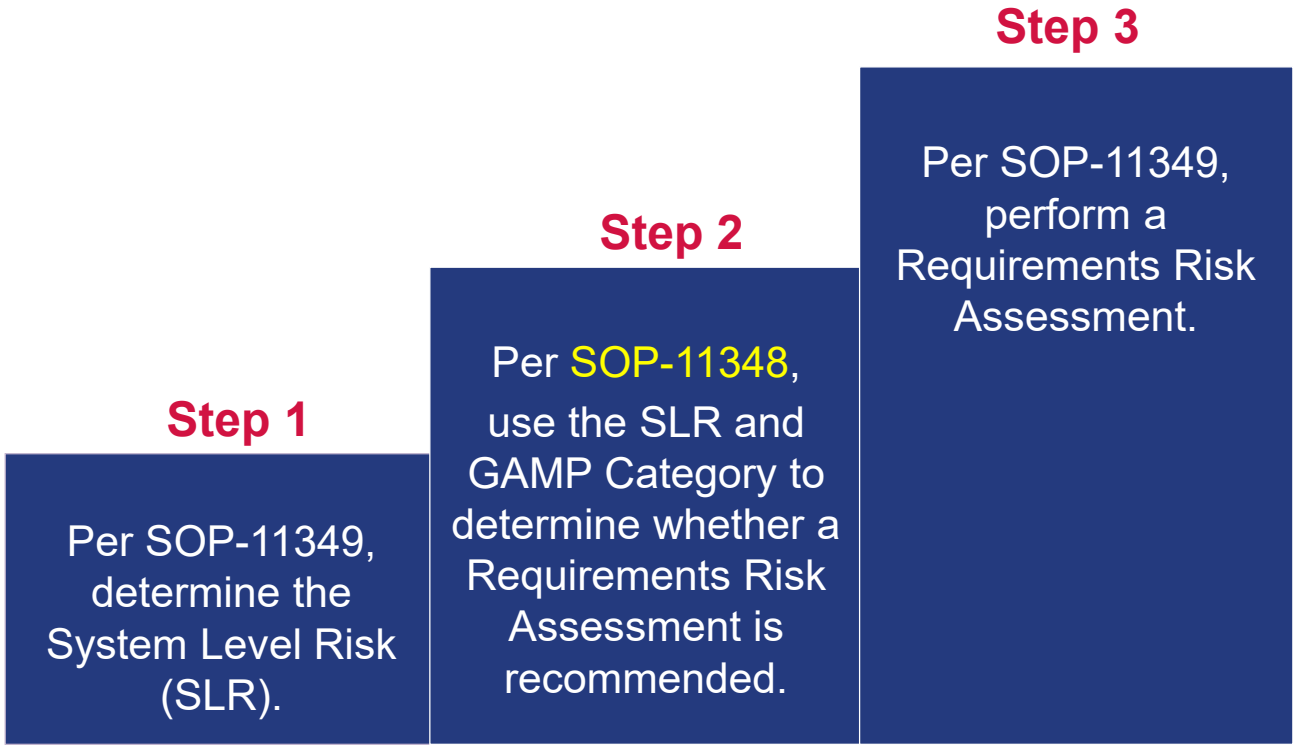
The objectives of this training are to understand:

- The components of the risk assessment process
  - System Level Risk (SLR)
  - Requirements Risk Assessment (RRA)
- The recommended RRA approach
- How to determine Severity, Probability, and Detectability
- When and how to update an existing Risk Assessment

Agenda

- Review of System Level Risk (SLR)
- Requirements Risk Assessment (RRA) Process
- Updating an Existing RRA

Steps to a Requirements Risk Assessment



What determines the need for a Risk Assessment?

SOP-11348 Attachment 1:

Recommended Deliverables By SLR & GAMP Category

	GAMP Category		
Activity/Deliverable	5	4	3
GXP Applicability Assessment	L	L	L
Part 11 and Annex 11 Applicability Assessment	L	L	L
System Criticality Assessment	L	L	L
User Requirements Specification	L	L	L
Validation Plan	L	L	L
Functional Specification	N/A	M	L
Design Specification	H	M	L
Configuration Specification	N/A	L	L
Requirements Risk Assessment	**H**	**M**	**L**

No Risk Assessment?

If SOP-11349 indicates that a Requirements Risk Assessment is “recommended” for your system and the team decides not to perform a Risk Assessment, then all requirements/functions will need to be tested with the highest rigor.

System Level Risk Assessment Review

System Level Risk Assessment Overview

- Governed by SOP-11349, *Risk Assessment* of *Computerized Systems*
- Requires completion of FRM-08654 to assess system for type/criticality of GxP Data & Technology
- Used for new computerized systems and existing computerized systems based on the changes proposed.
- Responsible Roles:
  - Business Process Owner (BPO) – GxP Record Criticality & System Functionality Assessment
  - System Manager (SM) – Categorize Industry Use and GAMP Level
  - Validation Lead (VL) – Facilitates process & does the math
  - Quality Assurance (QA) – Ensure compliance to SOP

FRM-08654 Sections

Section 1: System Criticality Assessment

– Criticality of the GMP, GLP and GCP Records – Business Process Owner

1 SYSTEM CRITICALITY ASSESSMENT		
1.1 Criticality of records: *If the system manages an official source record listed in a column, check the box next to the record and at the top of the column*		
☐ **Low**	☐ **Medium**	☐ **High**
GMP ☐ Validation records except as noted for Medium Risk records ☐ Training records ☐ Facilities records ☐ Report formatting records ☐ Other low risk records (list in Comments)	**GMP** ☐ SOPs ☐ Specifications ☐ Analytical methods ☐ Process validation records ☐ Inventory records ☐ Equipment calibration and maintenance logs ☐ Annual product reviews ☐ Other medium risk records (list in Comments)	**GMP** ☐ Software is regulated as a medical device ☐ Master records, batch production records, control records ☐ Lot release records ☐ Product stability data ☐ Component and labeling records ☐ Equipment cleaning and use logs ☐ Returned drug product or salvaging records ☐ Distribution and inventory records ☐ Calibration certificates ☐ Product complaint records ☐ Other high risk records (list in Comments)
GLP ☐ Validation records ☐ Training records	**GLP** ☐ SOPs ☐ Archive indices	**GLP** ☐ Protocols and amendments ☐ Raw data

Enter “1”, “2”, or “3” based on the highest score checked above.	**GxP Record Criticality Score**	☐ High – 3 ☐ Medium – 2 ☐ Low – 1

FRM-08654 Sections

Section 1: System Criticality Assessment

- Criticality of the GMP, GLP and GCP Records – Business Process Owner

Section 2: Technology Assessment

- Functionality Score - Business Process Owner

2 TECHNOLOGY ASSESSMENT			
2.1 Functionality Score – *Check all boxes that represent functions that the system performs.*			
System Function		**Description**	**Score**
☐	Data creation/modification	System used to capture electronic raw data, create/modify/delete records, or derive new data from existing data.	3
☐	Data analysis and reporting	System used to report, trend, transform or analyze data or used to create electronic regulatory submissions that are not subsequently 100% verified.	2
☐	Data transport/browsing/storage	System used to move electronic records from one platform to another, facilitate storage or to allow read-only access to data.	1
Enter "1", "2", or "3" based on the highest score checked above.		**Functionality Score**	

FRM-08654 Sections

Section 1: System Criticality Assessment

- Criticality of the GMP, GLP and GCP Records – Business Process Owner

Section 2: Technology Assessment

- Functionality Score - Business Process Owner
- Distribution Score - System Manager

2.2 Distribution Score – *Check the box that best represents the system's installed base.*

	System Type	Description	Score
☐	Custom system	System was developed by or for Gilead, or source code was modified for Gilead, or source code is open source.	5
☐	Regulated industry; limited use	System was developed for regulated industry but is NOT widely used.	4
☐	Multi-industry; limited use	System was developed for general purposes across many industries but is NOT widely used.	3
☐	Regulated industry; broad use	System was developed for regulated industry and is widely used.	2
☐	Multi-industry; broad use	System was developed for general purposes across many industries and is widely used.	1
Enter "1", "2", "3", "4", or "5" based on the highest score checked above.		**Distribution Score**	

FRM-08654 Sections

Section 1: System Criticality Assessment

- Criticality of the GMP, GLP and GCP Records – Business Process Owner

Section 2: Technology Assessment

- Functionality Score - Business Process Owner
- Distribution Score - System Manager
- Complexity Score (GAMP Category) - System Manager

2 TECHNOLOGY ASSESSMENT				
2.3 Complexity Score – *Check all boxes that represent functions that the system performs*				
GAMP Category		**Description**	**Typical Examples**	**Score**
☐	Category 5 – Custom Application	Software custom designed and coded to suit the business process	Varies, but includes: • Internally and externally developed IT applications • Internally and externally developed process control applications • Custom ladder logic • Custom firmware • Spreadsheets (macro)	3

FRM-08654 Sections

Section 1: System Criticality Assessment

- Criticality of the GMP, GLP and GCP Records – Business Process Owner

Section 2: Technology Assessment

- Functionality Score - Business Process Owner
- Distribution Score - System Manager
- Complexity Score (GAMP Category) - System Manager

Section 3: Overall Technology Risk Score – Validation Lead

3 OVERALL TECHNOLOGY SCORE			
Overall Score	**Technology Risk**	**Overall Technology Score** *Add functionality, distribution and complexity scores and enter here*	
11 To 10	**High**		
9 To 6	**Medium**	**Technology Risk Score:** *(Determined by table on left)* ☐ High ☐ Medium ☐ Low	
5 To 3	**Low**		

FRM-08654 Sections

Section 1: System Criticality Assessment

- Criticality of the GMP, GLP and GCP Records – Business Process Owner

Section 2: Technology Assessment

- Functionality Score - Business Process Owner
- Distribution Score - System Manager
- Complexity Score (GAMP Category) - System Manage

Section 3: Overall Technology Risk Score – Vali

Section 4: System Level Risk – Validation Lead

Appendix 5 – SYSTEM LEVEL RISK DETERMINATION

GxP Record Criticality Score	Technology Score: Low	Technology Score: Medium	Technology Score: High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

4 SYSTEM LEVEL RISK		
GxP Record Criticality Score	**Technology Score**	**System Level Risk**
☐ High – 3 ☐ Medium – 2 ☐ Low – 1	☐ High ☐ Medium ☐ Low	☐ High ☐ Medium ☐ Low

FRM-08654 Sections

Section 1: System Criticality Assessment

- Criticality of the GMP, GLP and GCP Records – Business Process Owner

Section 2: Technology Assessment

- Functionality Score - Business Process Owner
- Distribution Score - System Manager
- Complexity Score (GAMP Category) - System Manager

Section 3: Overall Technology Risk Score – Validation Lead

Section 4: System Level Risk – Validation Lead

Section 5: System Criticality – Validation Lead

5 SYSTEM CRITICALITY			
Overall Score	**System Criticality**	**Overall System Criticality Score** *Add record criticality, functionality and complexity scores and enter here*	
8 To 9	Critical (High)		
5 To 7	Major (Medium)	**System criticality level Score:** *(Determined by table on left)* ☐ High ☐ Medium ☐ Low	
3 To 4	Minor (Low)		

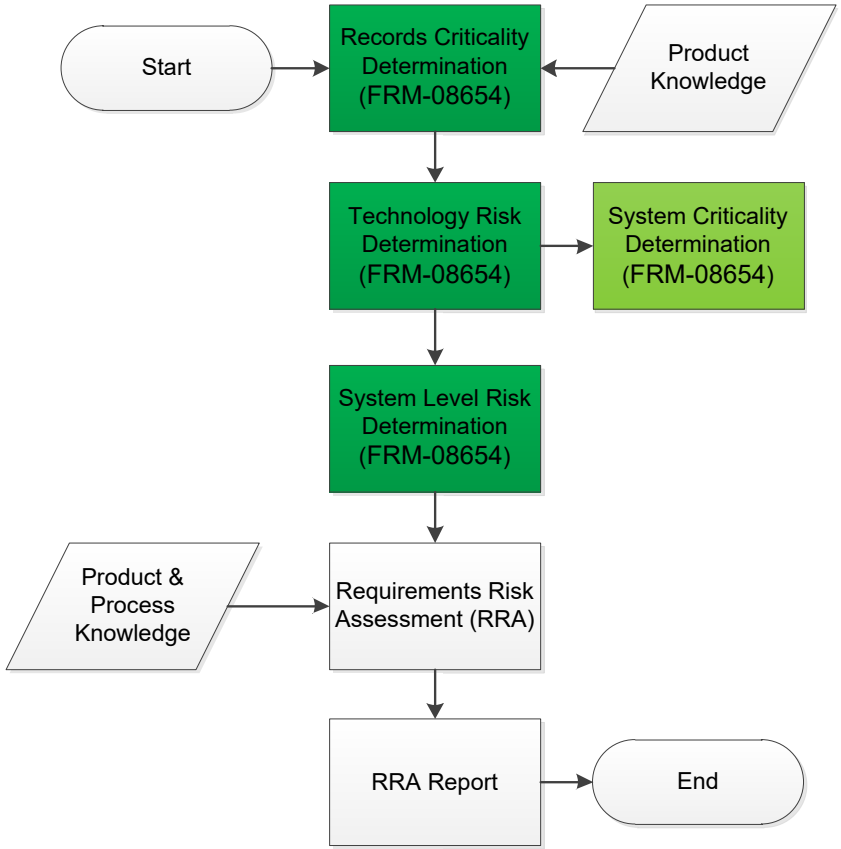
FRM-08654 Roles and Responsibilities Summary

Role	Responsibility
Business Process Owner (BPO)	• Completes **Section 1 System Criticality Assessment**, which identifies the Criticality of the GxP records • Completes **Section 2.1 Functionality Score**, which identifies what the system will do with those records.
System Manager (SM)	Completes **Sections 2.2 and 2.3** of the **System Technology Assessment**, which identify the Industrial Use of the system (i.e., Distribution Score) and GAMP Category (i.e., Complexity Score).
Validation Lead (VL)	Calculates the **Technology Score,** the **System Level Risk,** and **System Criticality** based on the input provided by the BPO and SM.
Quality Assurance (QA)	Reviews and approves the form and ensures compliance to SOP.

FRM-08654 Assessment Outcomes

FRM-08654 Sections	TempTale	GPID	Discoverant	Empower	LabX
GxP Record Criticality Score	3 - High	1 - Low	2 - Medium	3 - High	3 - High
Overall Technology Score	5 – Low	7 - Medium	7 - Medium	6 - Medium	9 - Medium
System Level Risk	Medium	Low	Medium	High	High
System Criticality	7 - Medium	6 - Medium	7 - Medium	8 - High	8 -High

Risk Assessment Process So Far…



Requirements Risk Assessment Process

When to Start a Requirements Risk Assessment

- Following requirements and specification approvals.

- Use to develop OQ or PQ test scripts.
- Approve assessment report before protocol approval(s).

Recommended RRA Options

SOP-11349 is flexible and allows the Risk Assessment Team to determine their Risk Assessment approach based on project size and system complexity.

For new LIS systems, there are two recommended approaches.

The risk assessment team can create a:

Option 1: RA Plan and create a separate Risk Assessment Report.

Option 2: Follow SOP-11349 and create a Risk Assessment Report.

Take-Away: Risk Assessment strategy needs to be approved before you do the assessment. The approach selected needs to be documented in the validation plan.

Option 1: Creating a RRA Plan and Report

- When to select RRA Plan and Report:
  - When the system is complex and the project will occur over a long period of time.
  - When the methodology differs for the SOP-11348 and/or you want to modify the definitions to fit your system.
- Benefits of RRA Plan and Report:
  - There is clarity on the methodology agreement before the start of the RRA.
  - The Risk Assessment meeting(s) become mechanical since the severity, probability, and detectability have been clearly defined.

Option 2: Creating a RRA Report Only

- Following completion of the requirements risk assessment per SOP-11349, the Validation Lead generates a requirements risk assessment report.
- The report must contain, at a minimum, the following information:
  - Purpose
  - Scope
  - Risk Evaluation Methodology (If it differs from the SOP)
  - Summary of Risk Priorities (count by ratings)
  - Risk Level – Derivation of risk priorities (including severity, probability, and detection, as well as justification). This is the risk assessment matrix.

SOP Requirements Risk Assessment Table

System Name *Indicate the name of the system. If subcomponent, include both system and subcomponent name.*							
Assessment Scope / Assumptions Made: *Indicate specifications (Document IDs) and any assumptions made for this assessment.*							
Function or Spec. ID #	Sub-Function Or Child Spec. ID #	Assessment of Risk					Comments (Include measures and controls where applicable)
		Severity	Probability	Risk Class	Detectability	Risk Priority	
Indicates the specification #	*This would indicate a sub-function if assessment is not grouped by functional category.*						*Include comments and justification if risk priority is low or medium. The justification explains the reason for assessment input that contributed to the overall rating.*

Note: The SOP-11349 also allows the Validation Lead to decide to combine RRA report within a specification (e.g., U/FRS) rather than in a RRA Summary Report.

Risk Assessment Table - Comments Column

- The Comments Column of the Risk Assessment Table is intended to provide information that will justify why a requirement has a Risk Priority of “Low” or “Medium”.

- The Comments Column can help explain why:
  - The Severity is Low (e.g., the Severity is Low because there is a back-up paper process).
  - The Probability is Low (e.g., the function is “out of the box” and requires no configuration or custom code).
  - The Detectability is “High” (e.g., the user will know immediately if the function is not working).
- The Comments Column information can also include any system and/or procedural controls that help reduce Severity, reduce Probability, or increase Detectability.

Sample URS-Based Risk Assessment

Empower Risk Assessment Table

Function or Spec. ID #	Sub-Function Or Child Spec. ID #	Assessment of Risk					Comments (Include measures and controls where applicable)
		Severity	Probability	Risk Class	Detectability	Risk Priority	
UR-1	The user must have the ability to separate chromatographic data by project.	High	Low	2	High	Low	Easily detectable and user cannot proceed.
UR-2	The authorized user must have the ability to create new projects.	High	Low	2	High	Low	Easily detectable and user cannot proceed.
UR-3	The user must have the ability to identify the location of users, systems, and nodes (FR3 New feature).	Medium	Low	3	High	Low	Easily detectable through automatic controls.
UR-4	The system must be configured to automatically back up data daily to allow for recovery from a catastrophic system failure.	High	Medium	1	Medium	High	N/A
UR-5	The user must have the ability to archive projects without loss of data.	High	Low	2	High	Low	Easily detectable through automatic controls.
UR-6	The user must have the ability to back up and restore system audit trails without loss of data.	High	Low	2	Medium	Medium	Easily detectable through automatic controls.

Sample URS-FRS Based Risk Assessment

GPLM Risk Assessment Table

This assessment method prevents the need for all the functional requirements to inherit the risk priority of their associated user requirement.

URS #	URS Statement	FRS #	FRS Statement	Severity	Probability	RC (SxP)	Detection	RPR (SxPxD)
URS-4-7.2-18	For new ICNs, inherit Primary UoM, Shipping and Storage Conditions from parent IP item number and assign it to the ICN for integrating with downstream business processes	FRS-4-7.2-18.1	Authorized users will create new ICNs in GPLM, without Primary UoM, Shipping and Storage Conditions. This user will indicate the Parent IP Item Number and then take it through the approval process using GPLM Change Order. Once approved, an event PX "Update Table : Commercial API (ICN) : Validate EBS Item Category, Check Mandatory Attributes' will then take the Primary UoM, Shipping and Storage Conditions values from the Parent IP part and associate them as the ICN attributes, in downstream systems.	H	M	H	M	H
		FRS-4-7.2-18.2	The relationship tab of the ICN will be populated with Parent IP Item Number, when the ICN part is released on a GPLM Change Order using a Clinical Item and ICN Approval (GPLM) workflow, using an event PX "Update Table : Commercial API (ICN) : Validate EBS Item Category, Check Mandatory Attributes.	H	M	H	H	M

Planning the RRA Meeting

Meeting Considerations:

- Who should attend
- What supplies to have at the meeting
- What meeting ground rules to follow
- What questions to ask

RRA Team Members

The “Fab Four” of the Risk Assessment Team include:

- Business Process Owner (Paul)
- System Manager (George)
- Validation Lead (Ringo)
- Quality Assurance (John)

RRA Team Member Roles

Business Process Owner
Uses business process knowledge to describe the **severity** & **detectability** of a system function failure.

System Manager
Uses system functional knowledge to identify the **probability** (i.e., complexity) & **detectability** of a failure.

Validation Lead
Leads the risk assessment process.

Quality Assurance
Provides regulatory / compliance expertise to ensure that the team is asking the right questions and avoiding bias.

RRA Team Recommendations

- The most RRA-experienced member should facilitate the individual requirement assessments.
- All team members need to come to the meeting with an open mind (i.e., No pre-conceived notions about risks, such as all risks being “Low”.)

Recommended RRA Meeting Supplies

Be sure to bring the following to the RRA meeting:

- Approved Requirements Documents:
  - User Requirements Specification (URS)
  - Functional Requirements Specification (FRS)
- Copies of SOP-11349, *Risk Assessment of Computerized Systems* or the Risk Assessment Plan
- A Risk Assessment Template Table in MS Word that contains the User and Functional Requirements
- A Laptop and Projector

Recommended RRA Meeting Ground Rules

1. Listen and don't interrupt (i.e., Let others finish).
2. Ensure that all participate, and responses come from everyone.
3. Be present and avoid electronic distractions (e.g., Phones, Email, Instant Messaging, etc.).
4. Make it a safe, brainstorming, and collegial environment (e.g., Avoid criticizing).
5. Hold an in-person meeting, and avoid having attendees dial-in.
6. When a meeting cannot be in person, use a video conference.
7. Schedule meeting long enough to keep momentum (e.g., 2 hours).

Recommended Questions to Ask

Four fundamental questions to ask in order to clearly define the risk during the RRA meeting:

1. What might go wrong? (Consider what is known or predictable.)
2. What is the complexity of the function? (i.e., Probability)
3. What are the consequences (i.e., Severity)?
4. Can the problem be detected and how easily (i.e., Detectability)?

Determining Severity, Probability, and Detectability

Risk Component	SOP-11349 Appendix 2	Major Contributor	Comments
Severity	Table 1	BPO	• Don't view Severity as a domino effect. • If you use too many degrees, then everything will be severe.
Probability	Table 2	SM	• It's important to understand how the system is built, its components, and their interaction. • The probability levels are based on amount of configuration and customization.
Detectability	Table 4	BPO, SM, & VL	• Based on user's visibility through the UI. • All participants should be able to contribute to the potential detectability.

Severity = High

Per SOP-11349

Severity	Description
High	If a system failure of this type occurs there likely would be a direct impact on data integrity, product quality, or patient safety. The following are examples: • A function that is used to make key decisions, e.g., expiry dates, patient dosing, lot status, product recalls, etc. • A function that directly impacts regulatory requirements. • A function that impacts the accuracy of GxP critical data. • A function that impacts the retrieval of GxP data during retention periods.

Severity = High

Severity Level	Discoverant Functionality Failure Mode
High	If a failure was to occur, there would be significant impact to the patient safety, product quality, and system and data integrity. Effects of failure of the function include, but are not limited to, the following: ▪ Data integrity of a record can be compromised if system fails or if task is incomplete ▪ Interface failure, inaccurate information communicated ▪ Inability to record correct and accurate entries in the audit trail or metadata field values ▪ Failure of functionality that supports or produces information related to 21 CFR Part 11, and Annex 11

Severity = High

Severity Level	LAB-X Functionality Failure Modes
High	If the failure was to occur, there would be significant impact to product quality, product safety, system functionality and/or data integrity. Effects of failure of the function include, but are not limited to, the following: • Data integrity of a record can be compromised if component fails or if component is incomplete • Interface failure, inaccurate information communicated • Inability to record an e-signature and/or audit trail • Failure to functionality that supports or produces information related to 21 CFR Part 11 or Annex 11 • Failure to functionality that supports the safety, purity, potency, identity, effectiveness or quality of a product

Severity = High

Rating	GLIMS Definitions
High	If a failure was to occur, there would be significant impact to the system and/or data integrity. Effects of failure of the function include, but are not limited to, the following: • Data integrity of a record can be compromised if component fails or if component is incomplete • Interface failure, inaccurate information communicated • Improper or incomplete GLIMS records - leading to an unacceptable change being assessed, implemented, or used • Inability to record an e-signature and/or audit trail • Inability to record correct and accurate entries in the audit trail, electronic signatures or metadata field values • Failure of functionality that supports or produces information related to 21 CFR Part 11, 21 CFR Part 211, or Eudralex, Volume 4, Annex 11 • Failure of functionality that supports the safety, purity, potency, identity, effectiveness or quality of a product.

Probability

Per SOP-11349

Probability of Occurrence	Description
High	Custom software or component developed to meet a requirement (e.g., GEM interfaces, custom extensions).
Medium	Custom configuration using complex conditions or complex interactions (e.g., configuration of reports or business rules requires more than a simple checkbox configuration or single parameter input).
Low	Standard non-configured out-of-the-box (OOTB) functionality or simple configuration components (e.g., checkbox configuration for record lock).

Probability

Technical Complexity Level	ELN Technical Design
High	Custom or bespoke code was purposely developed to satisfy user requirements including requirements involving integration to or with other systems.
Medium	Gilead-specific parameter settings were configured to fulfill user requirements.
Low	Out-of-the-box and/or default parameter settings are used to fulfill user requirements; no custom code or Gilead-specific settings are necessary.

ELN is similar to the SOP.

Probability

Probability Level	(Lab-X) Technical Design
High	Failure is very likely to occur The functionality is complex The likelihood of user data entry error is high
Medium	Failure is unlikely, but can reasonably be expected to occur The functionality is moderately complex The likelihood of user data entry error is medium
Low	Failure is unlikely The functionality has low complexity The likelihood of user data entry error is low

Lab-X differs by including likelihood and complexity, and includes user data entry.

Detectability

Per SOP-11349

Detection	Description
High	• System is unavailable. • Functional failure results in alert back to the user (immediate or during user session). • User detection – user cannot perform job function (fields/ screens are restricted).
Medium	• User detection – user may notice the functionality/component stops operating but an alert is not provided on the interface (e.g., job does not complete, screen locks, email notifications).
Low	• User detection – user may notice functionality failure only upon review of data outside of record (e.g., review of admin audit trail data).

Detectability

Rating	Definitions (GTrack)
High	• System is unavailable • User detection - user cannot perform job function (fields/ screens are restricted)
Medium	• User detection - user can notice the functionality/ component stops operating but can verify activity completion from within record
Low	• User detection - user may notice only upon review of data outside of record (e.g., review of admin audit trail data)

GTrack differs by not including the use of notifications.

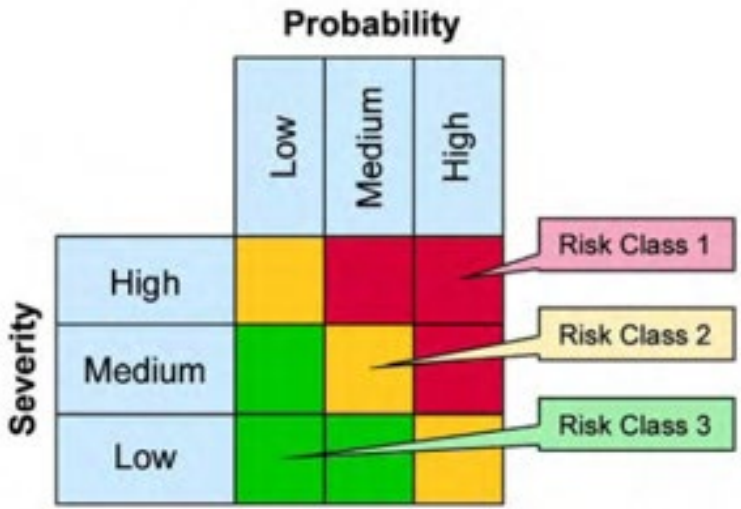
Detectability

Detectability Level	Ease of detection (Lab-X)
High	User is able to easily identify that system functionality is non-operational because he or she is unable to perform assigned task(s). Data integrity, security and system functionality is not adversely impacted by the failure.
Medium	User identifies the functionality failure during the performance of the assigned task(s); however the failure is not severe enough to impede the completion of the assigned task(s).
Low	User is not able to identify the existence of functionality failure(s), or is not able to easily detect functionality failures(s) during the performance of the assigned task(s).

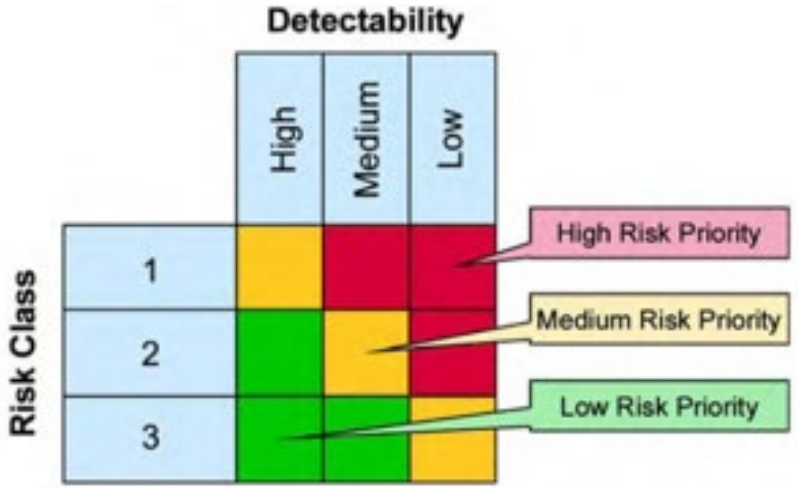
Lab-X differs by defining Medium as a failure where the task can still be completed.

Risk Rubrics

Risk Class



Risk Priority



Exercise

GVault Requirements Exercise

URS Req. #	Requirement Description	Severity	Probability	Risk Class	Detection	Risk Priority
URS-1	The Document Management system prohibits users from deleting a document in any state.					
URS-2	Upon entering the ‘Approved’ state for a DtA document, the Document Management system shall set the previous steady state version to ‘Superseded’ status.					
URS-3	The Document Management system will transition a DtE document in ‘DCC Approved, Pending Release’ status to ‘Prereleased’ status automatically when the Prerelease Date is reached.					
URS-4	A Controlled Issuance & Batch Printing (CIBP) Group user must be able to specify a page range during issuance.					

GVault RRA Exercise Results

URS Req. #	Requirement Description	Severity	Probability	Risk Class	Detection	Risk Priority
URS-1	The Document Management system prohibits users from deleting a document in any state.	High	Low	2	Low	High
URS-2	Upon entering the ‘Approved’ state for a DtA document, the Document Management system shall set the previous steady state version to ‘Superseded’ status.	High	Low	2	Medium	Medium
URS-3	The Document Management system will transition a DtE document in ‘DCC Approved, Pending Release’ status to ‘Prereleased’ status automatically when the Prerelease Date is reached.	High	Medium	1	Low	High
URS-4	A Controlled Issuance & Batch Printing (CIBP) Group user must be able to specify a page range during issuance.	Medium	High	1	High	Medium

Updating an Existing Risk Assessment

Considerations for Adding/Modifying Requirements

A New Section of Requirements

Use the Previous Severity & Detectability Definitions

Use Probability based on SOP-11349

Or

Use Previous Probability Definitions

Requirements Intermixed with Existing Requirements

Use the Previous Severity & Detectability Definitions

Use Previous Probability Definitions

Questions?


danke
謝謝
thank you
gracias
ngiyabonga
teşekkür ederim
рахмат
спасибо
obrigado
dziękuję
bedankt
go raibh maith agat
sukriya
kop khun krap
terima kasih
merci
grazie
arigatô
dakujem
mochchakkeram
dank je
barka
welalin
tack
mersi
vinaka
blagodaram
faafetai lava
kiitos
dankie
dhanyavad
hvala
mauruuru
köszönöm
enkosi
sobodi
dēkuji
mesi
sagolun
najis tuke
kam sah hamnida
তোমাকে ধন্যবাদ
감사합니다
xièxie
ありがとう
tanemirt
rahmet
chnorakaloutioun
gratias ago
gracies
sulpáy
misaotra
matondo
paldies
grazzi
djiere dieuf
дякую
mamnun
tapadh leat
хвала
asante
manana
obrigada
obrigado
trugarez
мерси
shukriya
dhanyavadagalu
diolch
takk
taiku
ευχαριστώ
merci