How Do I

Perform a Risk Assessment

Prepared by:

Robin Nozick

MT(ASCP)

ISBT WPIT Traceability Task Force Co-Chair

Michael Breard

MS, MT(ASCP)SBB, CQA(ASQ), PMP(PMI),LSSGB,MPM(AAPM)

Chair ISBT Working Party on Information Technology (WPIT)

Chair ISBT WPIT Traceability Task Force

Steps To Risk Management

How do I

Risk Management is a continuous cycle composed of:

- Risk Assessment
- Risk Minimization (Will be addressed in Part 2)

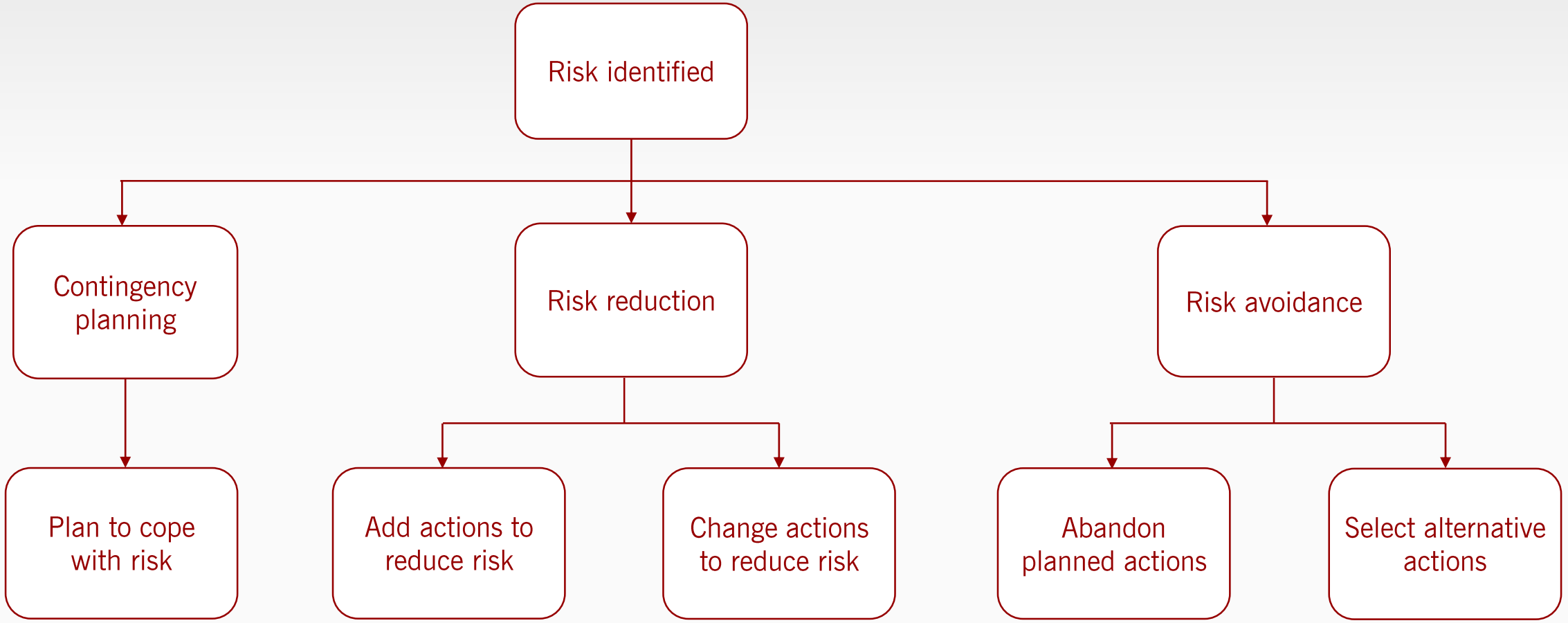
Risk Management Process

Risk Assessment:

- Analysis that identifies critical control points in software where, if there is a failure or malfunction, harm to a patient, donor or business may occur

- Tools that allow validation resources to focus on critical areas of an automated system

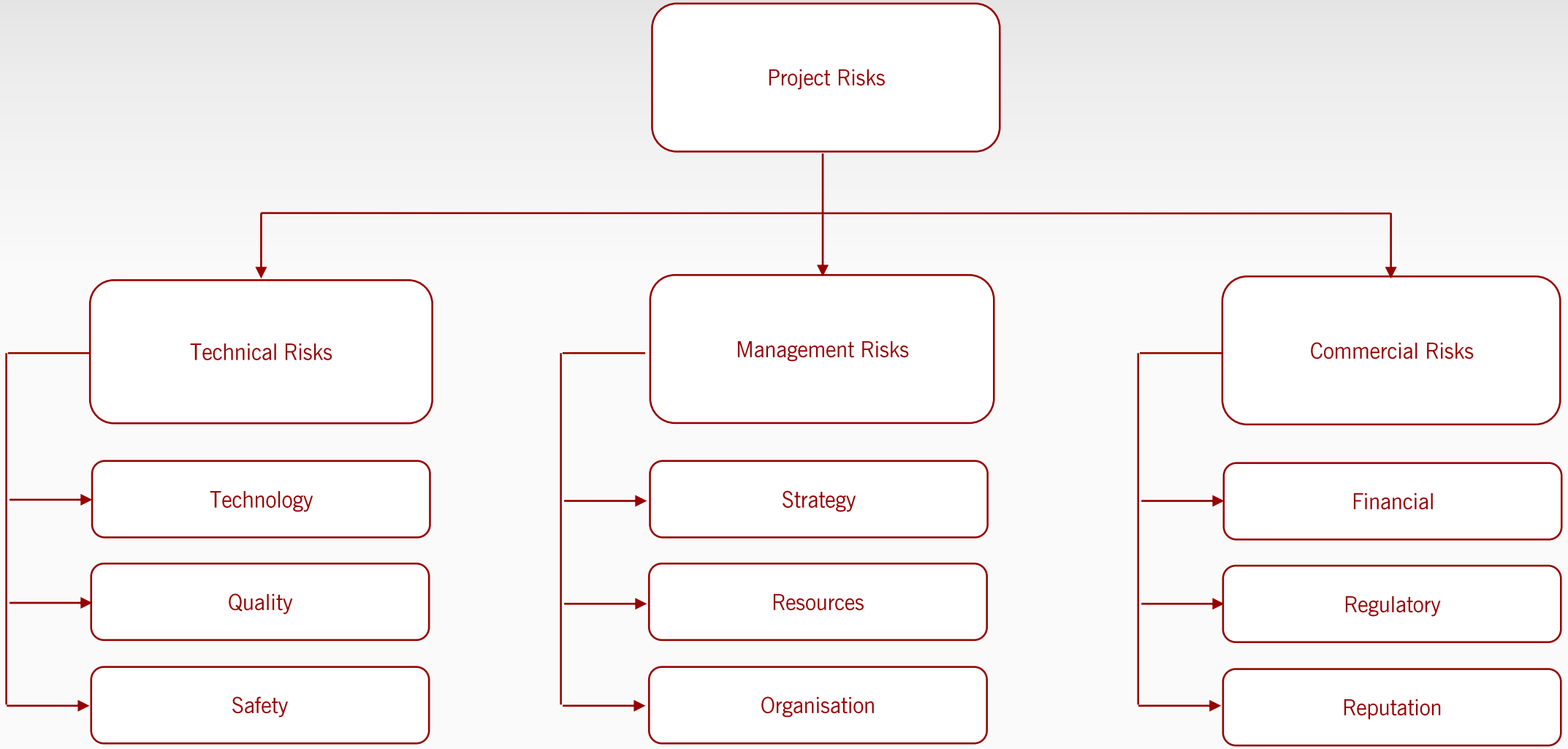
Risk Management



What is Risk Assessment?

- A comprehensive evaluation of the risk and its associated impact, which can be financial and/or operational
- The process of determining acceptable levels of risk
- Risk is typically a function of ‘probability of occurrence’ and ‘severity of the consequence’

Risk Breakdown



Three Steps To Determine Levels Of Risk

How do I

1. Identify risks and create a Risk Document
2. Apply empirical techniques to analyze the situation in terms of consequences and likelihood
3. Estimate likelihood/consequences and develop mechanism to apply category

Risk Assessment: Step 1

- Identify Risks
  - For your Operational Qualification (OQ) Validation, take your (User Requirement Specifications (URS) document which describes your needs and assess the risk if each one did not function in the system as documented.
  - For your Performance Qualification (PQ) Validation, identify the less critical items not covered in your OQ process such as data on reports, labels, ordering documents, processes between departments etc. and don't forget business continuity items.
  - If a decision is made TO DO or NOT TO DO something – what is the risk?

Risk Identification Example

How do I

Req #	Requirement	Probability/Likelihood	Severity
1	The system shall permit the user to access specific functionality based on defined security permissions.		
2	The system shall have the ability to mark or indicate that a specific unit or product has been recalled by a Donor center		
3	The system shall provide a method to identify and quarantine all in dated products from all prior donations dating back 5 years if the result of the anti-HIV-1/2 EIA screen is reactive.		
4	The system shall print a call list by club/blood type report		

Risk Assessment: Step 2

How do I

- Apply sensible, practical, realistic techniques to identify and trace back to the trigger, event, or cause:
  - Look for things that could harm or kill a patient
  - Look for things that could harm your business and/or personnel
  - Read the automated system's documentation and include the things the vendor says are critical control points
  - Validate that messages display appropriately since these usually warn of a critical control point
  - You don't have to use any particular marketed tool to do this. Just be sensible.

Empirical Thinking

ISBT How do I

- Thinking based on YOUR Experience or Observation:
  - What is the outcome if this requirement is not handled correctly? Could someone get severely hurt or die? Will the business fail?
  - What is the probability of it happening?
  - Will it be detected in normal use of system? Will it be detected in Performance Qualification or does it need to be tested in Operational Qualification?
  - What is the cost associated with mitigating vs the cost of accepting the risk?

Risk Assessment: Step 3

- Develop a logical approach to estimate Likelihood/Probability/Consequences:
  - For processes look at:
    - Probability of detection during normal functionality
    - Likelihood of situation occurring
  - Likelihood/Probability has minimal benefit for OQ validation since you are already dealing with worst cases. Consequences are more realistic and valuable for determining what to include in your OQ.

Risk Identification Example with Probability/Severity

How do I

Req. No.	Requirement	Probability/ Likelihood	Severity
1	The system shall permit the user to access specific functionality based on defined security permissions.	Frequent	High
2	The system shall have the ability to mark or indicate that a specific unit or product has been recalled by a Donor center	Probable	Mod
3	The system shall provide a method to identify and quarantine all in-dated products from all prior donations dating back 5 years if the result of the anti-HIV-1/2 EIA screen is reactive	Occasional	Mod
4	The system shall print a call list by club/blood type report	Frequent	Low

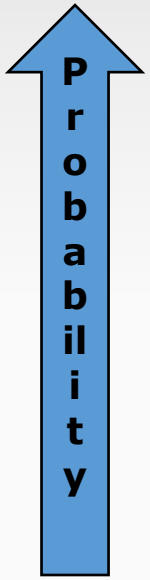
Example Risk Matrix 1

How do I

Likelihood/ Severity	High	Mod.	Low	Negligible
Frequent	1	1	1	3
Probable	1	1	2	3
Occasional	1	2	2	4
Remote	2	2	3	4
Improbable	3	3	3	4

Risk Assessment Matrix

How do I



Low	Medium	High
Low	Medium	Medium
Low	Low	Low

Impact

Follow Through

- Green:
  - Ensure:
    - Adequate Investigation
    - Adequate Product or Service Containment
    - Adequate Correction
  - Set Up A Monitoring Plan
  - Re-Visit

- Yellow or Red:
  - Ensure:
    - Adequate Investigation
    - Adequate Product or Service Containment
    - **IMMEDIATE** Correction
  - Root Cause Analysis
  - Implement Corrective Action
  - Monitor Success

Example Risk Matrix 2

Code	Outcome	Definition
1	Unacceptable	High Priority
2	Undesirable	Moderate Priority
3	Acceptable with Review	Low Priority
4	Acceptable without Review	No Priority

Risk Identification Example with Level of Scrutiny/Priority Assignment

How do I

Req #	Requirement	Probability/Likelihood	Severity	Level of Scrutiny/ Priority
1	The system shall permit the user to access specific functionality based on defined security permissions.	Frequent	High	1
2	The system shall have the ability to mark or indicate that a specific unit or product has been recalled by a Donor center	Probable	Moderate	1
3	The system shall provide a method to identify and quarantine all in dated products from all prior donations dating back 5 years if the result of the anti-HIV-1/2 EIA screen is reactive.	Occasional	Moderate	2
4	The system shall print a call list by club/blood type report	Improbable	Low	3

How to Use ‘Likelihood’ in Your Assessment

How do I

- In OQ validation likelihood is not valued highly because of the nature of the validation, ie. Worse Case Testing
- In PQ validation you will most frequently be validating processes that are very likely to occur.
- Blood bankers would consider a failure that could kill or severely injure a patient, no matter how likely it is to occur, a High Risk.

Risk Assessment As A Factor In Determining Extent of Validation

- The greater the degree of risk, the greater the level of validation required.
- When determining the level of risk the main consideration shall be what the severity of harm the device could inflict or permit as a result of its failure.

Risk Management Process

Risk Minimization/Mitigation:
Will be discussed in Part 2