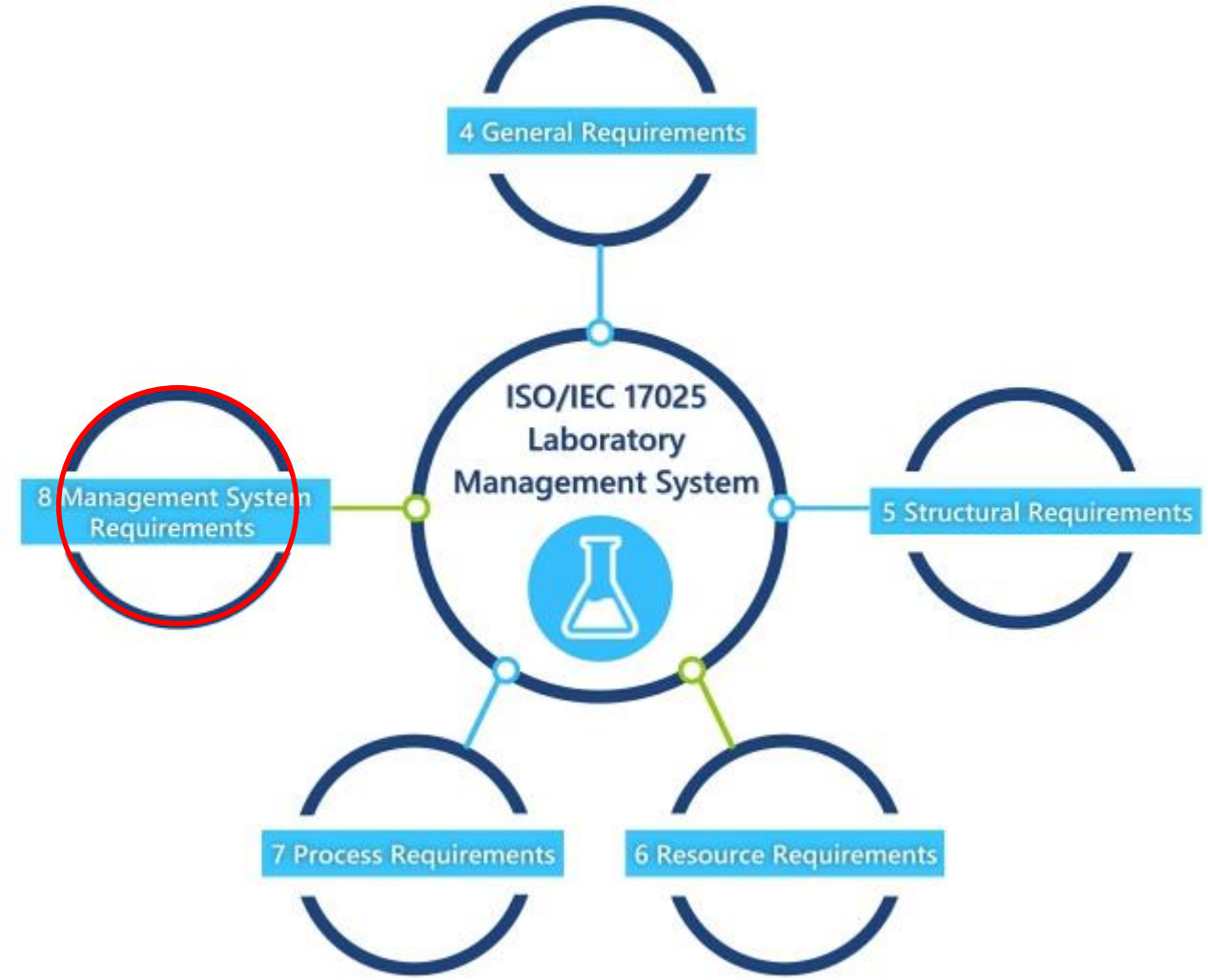
L10 Risk and Opportunity

IAEA

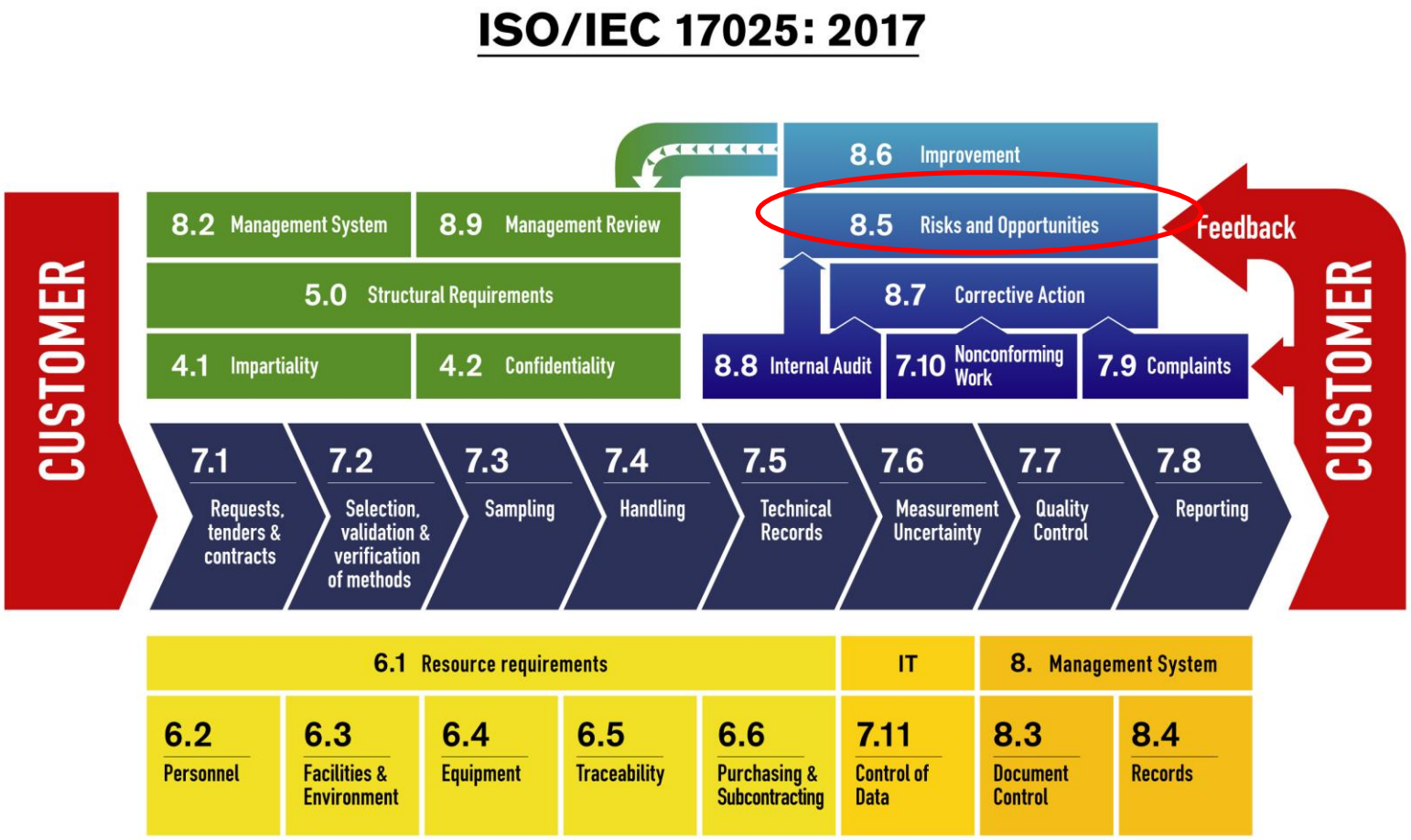
International Atomic Energy Agency

8 Management System Requirements



IAEA

Structure


ISO/IEC 17025: 2017
8.6 Improvement
8.5 Risks and Opportunities
Feedback
8.2 Management System
8.9 Management Review
5.0 Structural Requirements
8.7 Corrective Action
4.1 Impartiality
4.2 Confidentiality
8.8 Internal Audit
7.10 Nonconforming Work
7.9 Complaints
CUSTOMER
CUSTOMER
7.1 Requests, tenders & contracts
7.2 Selection, validation & verification of methods
7.3 Sampling
7.4 Handling
7.5 Technical Records
7.6 Measurement Uncertainty
7.7 Quality Control
7.8 Reporting
6.1 Resource requirements
IT
8. Management System
6.2 Personnel
6.3 Facilities & Environment
6.4 Equipment
6.5 Traceability
6.6 Purchasing & Subcontracting
7.11 Control of Data
8.3 Document Control
8.4 Records

Objectives

In this lecture we will discuss risk and opportunity:

- Risk concept
- Structured risk statements
- Risk and opportunity
- Risk management

What is a Risk?

You've carefully planned in your laboratory

- The customer supplied you the user's requirements
- Estimated 5 testers could perform testing
- Placed subcontractor on contract to perform the task for some parameters where you do not have capability

What could go wrong?

- All 5 testers may not be available
- Laboratory team may not be as productive as expected (and take longer than you expected)
- The subcontractor may deliver later
- The subcontractor may not deliver what you expected
- The requirements may not be complete or consistent
- The customer may not have supplied the real user's requirements
- Many more….

IAEA

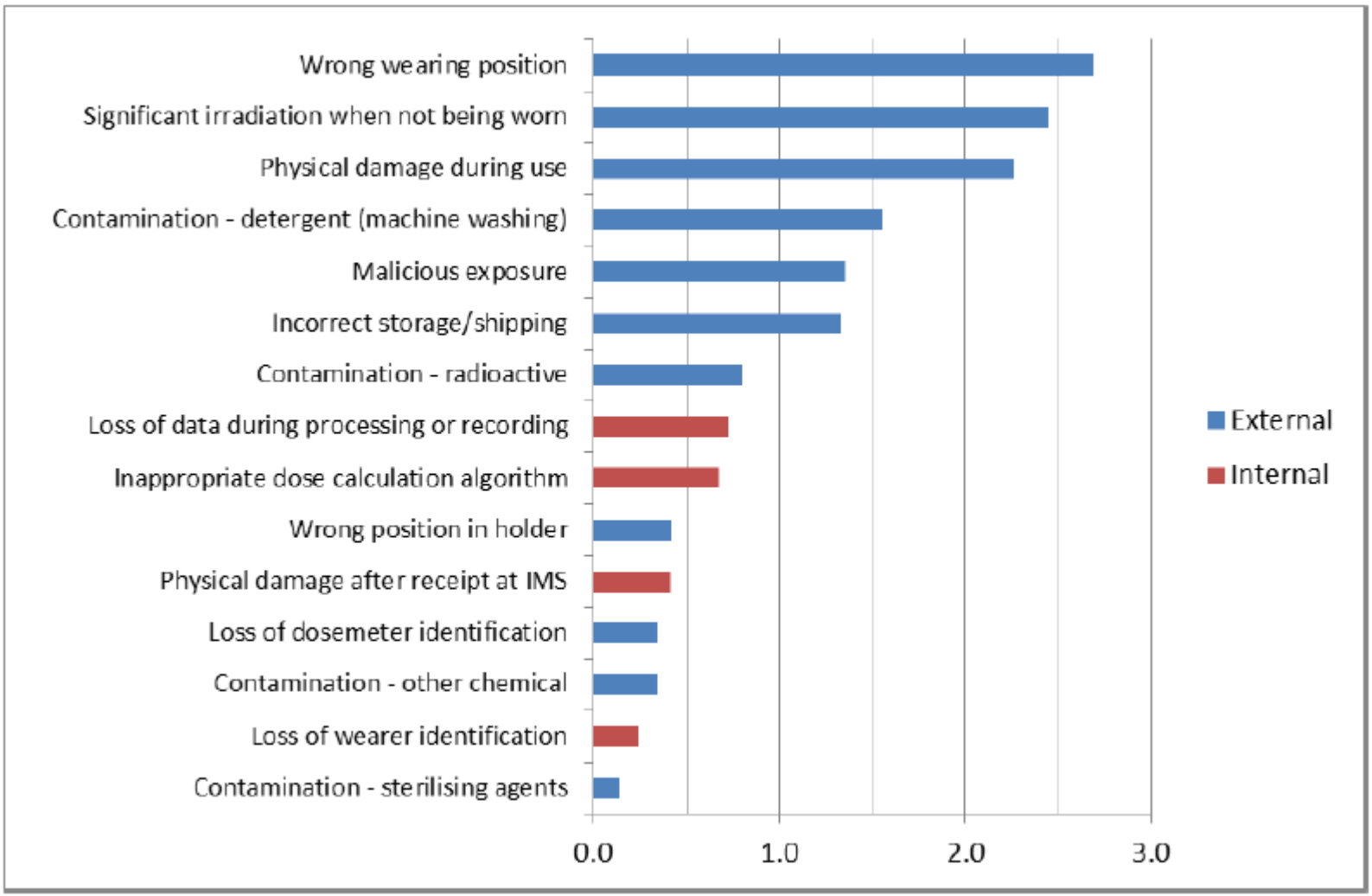
What should be in your risk register budget – example of IMS

- Dosemeters exposed for internal calibration dosemeters wrongly sent to customers
- Confusion between measured values (readings) and dose values. In general, the dose measurement is accredited not the 'dose to the person' value
- Malicious exposures
- Late returned dosemeters: can give bad results, e.g. if stored incorrectly?
- Wrong background subtraction, strongly dependent on how background is evaluated (dosemeters sent to client, mean annual value, raw results without BG subtraction…)
- Instruments 'bad results': transient event during readout, mechanical shock, electronic noise
- Bad identification (dosemeter identification vs attribution to person)
- Data loss during data transfer
- Software problems (shift of dose results)
- Lost data after power shutdown
- Loss of data due to wrong backup
- Wrong instrument settings

IAEA

Source: EURADOS Report 2015-04

Other well known errors in IMS



Source: EURADOS Report 2015-04

Most common analytical errors in TLD

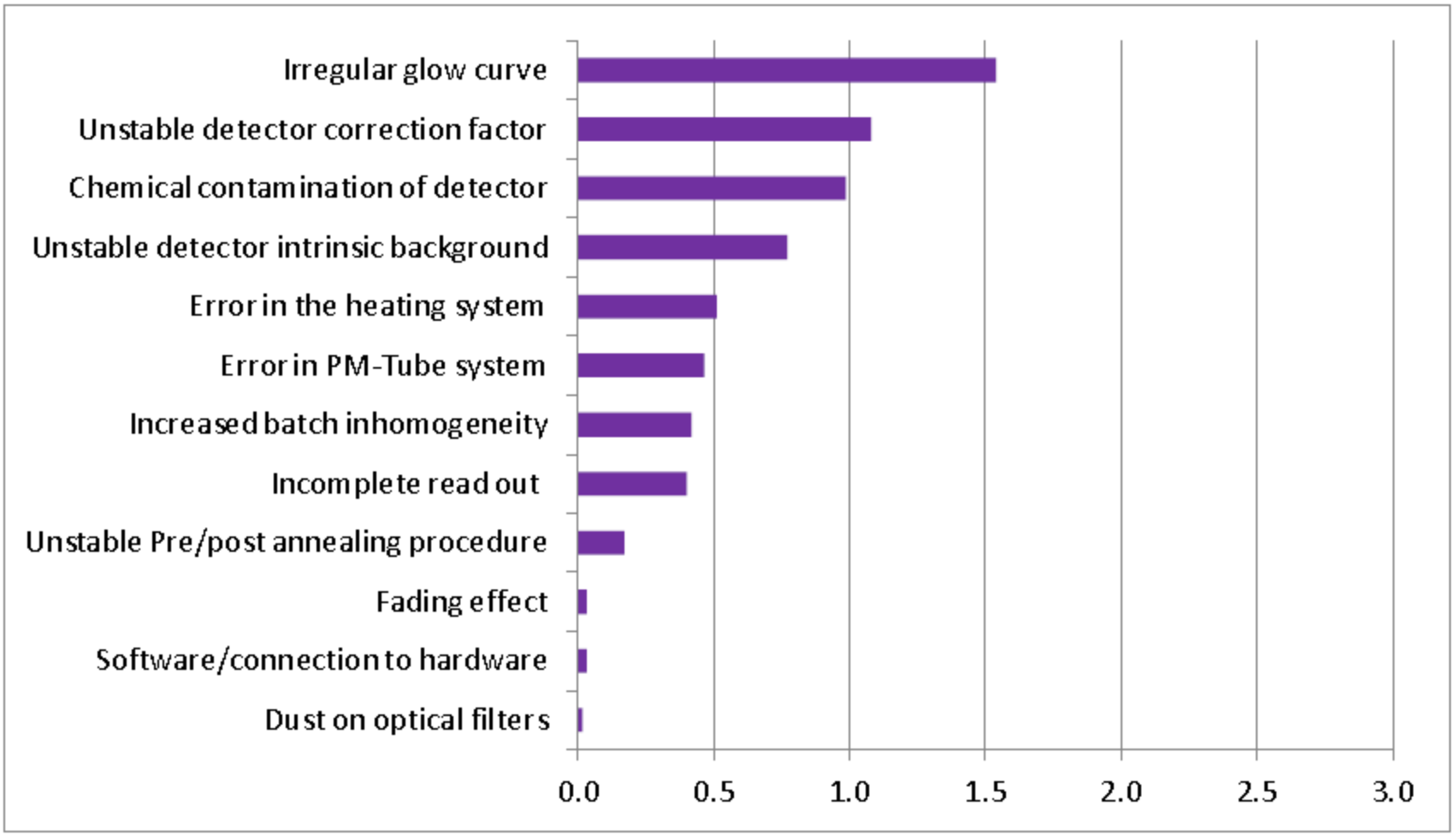


Figure 39. Most important sources of error for thermoluminescence dosemeters (TLDs)

Source: EURADOS Report 2015-04


Risk Management – Identifying and Preventing The Causes before they happen- ISO/IEC 17025:2017 requirements
Business Continuity – Dealing with the Consequences before they happen

IAEA

Structured Risk Statements

- **Risk = Probability/likelihood** of adverse event X **Impact** if the event occurs

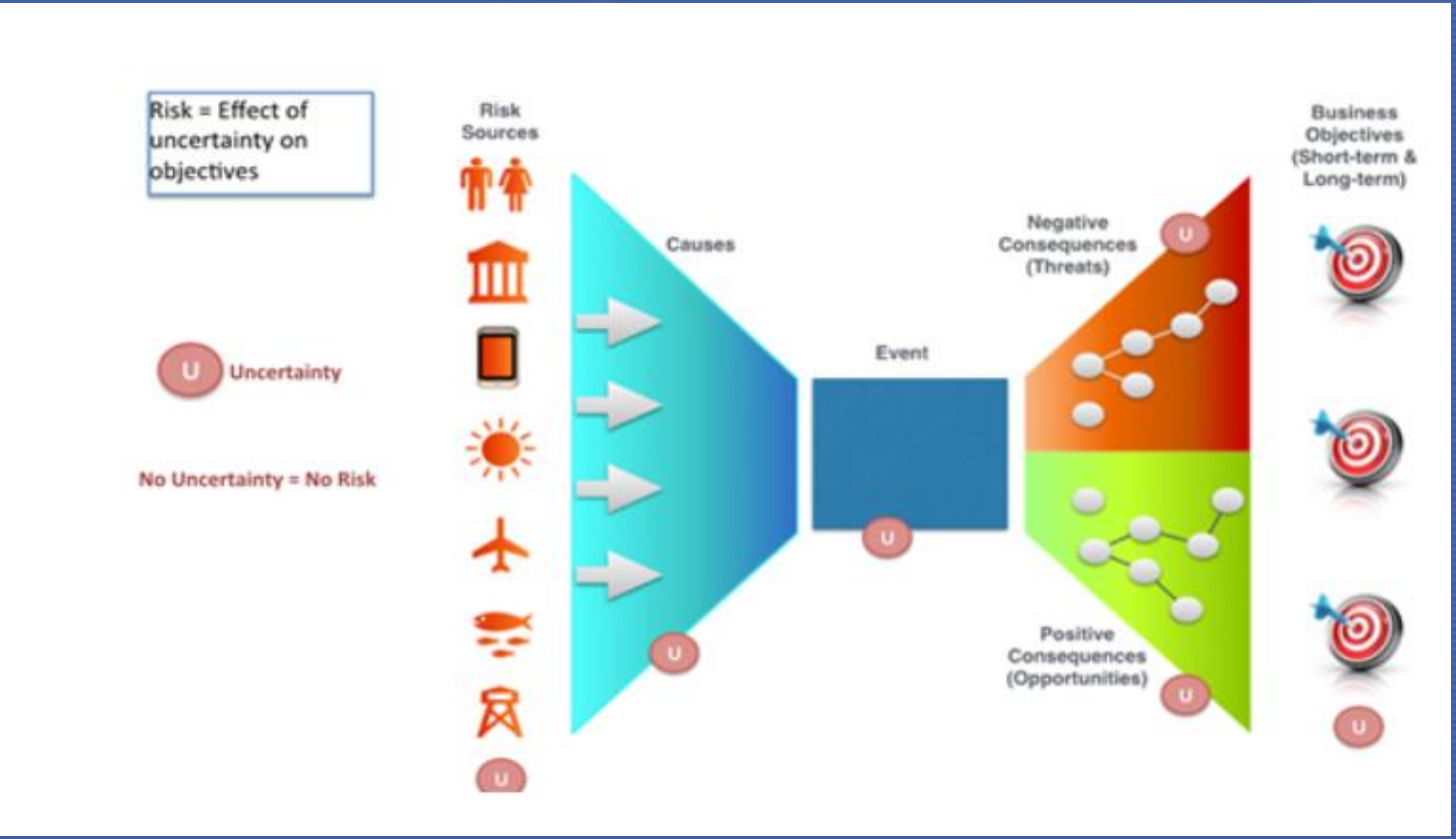
- **Risks should be stated in a structured manner**
  - If adverse event happens, then impact

    e.g. If the vendor is two weeks late with the test environment, then delivery to the customer will be three weeks late
  - If the customer does not identify a key user requirement,
    then the laboratory will not perform as the users desire and customer satisfaction will be diminished by 50%

IAEA

Definition of risk

- Risk focusses on the uncertainty of meeting objectives and therefore could relate to impact on Cost, Schedule, Customer satisfaction, Quality (functionality/usability/technical mistakes/…), Image/Reputation, Safety, Security, Environmental

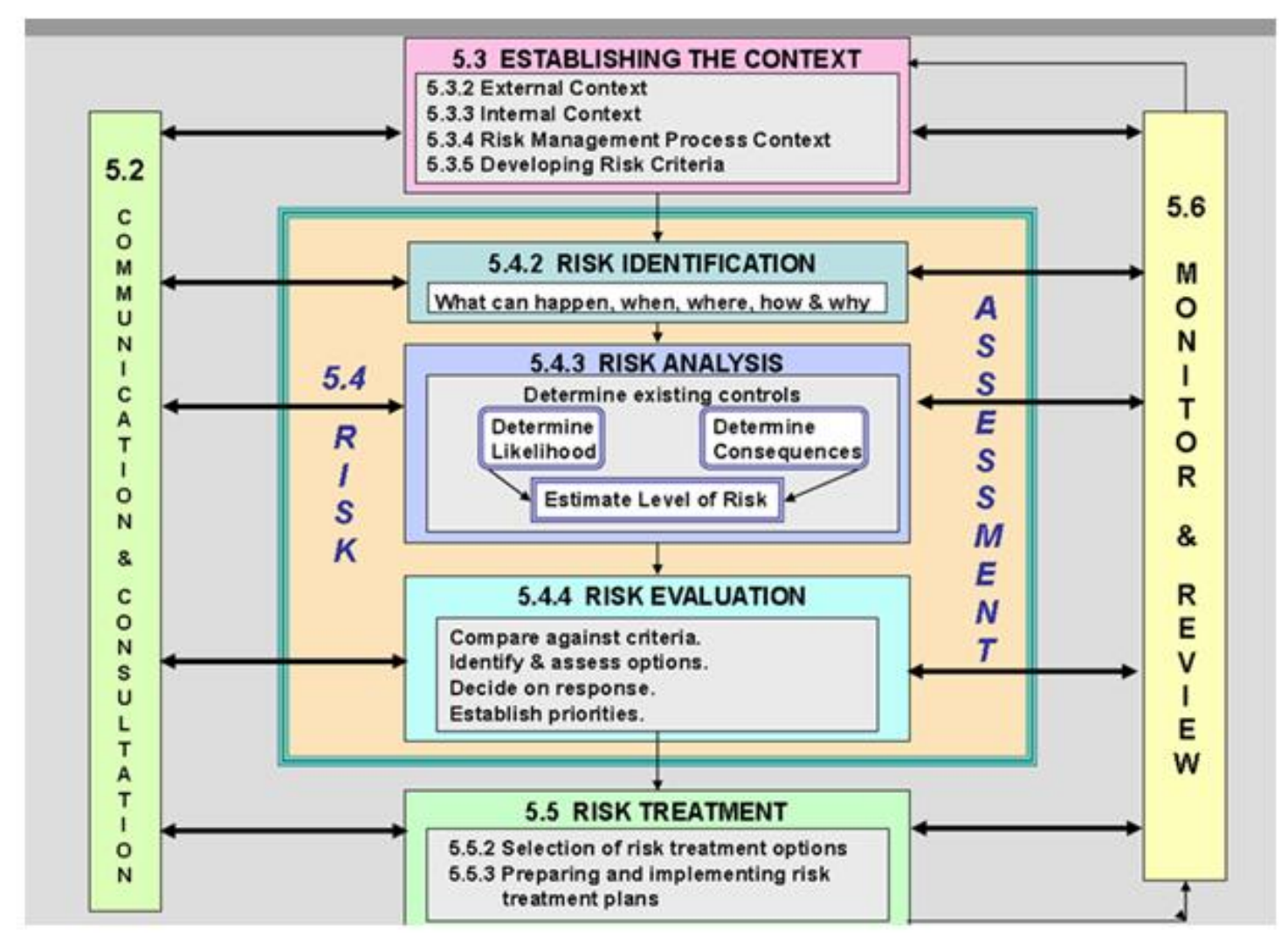


Risk Management

What is Risk Management?

" Process of identifying, controlling and minimizing or eliminating laboratory risks that may affect laboratory management systems, for an acceptable cost "

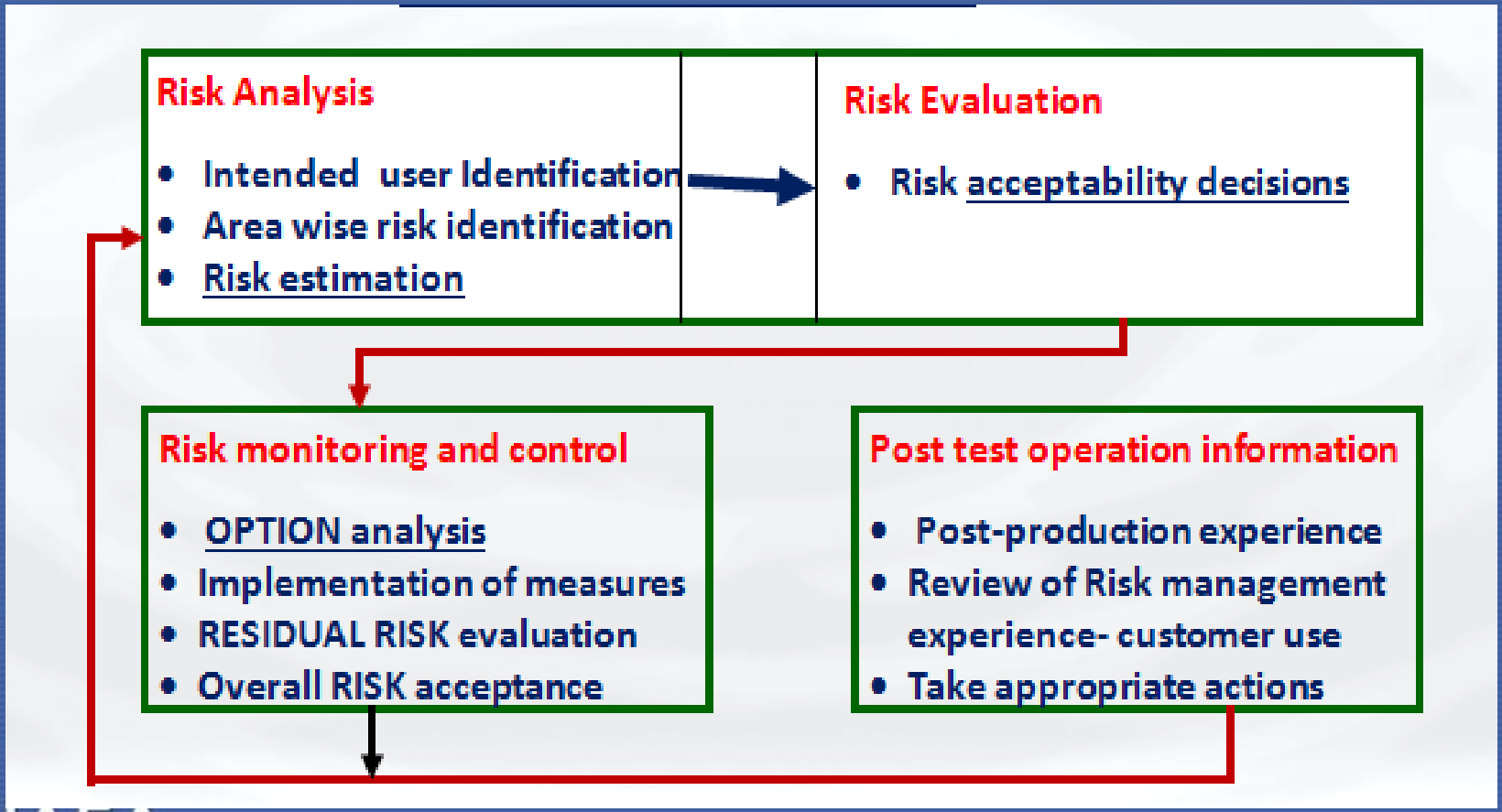
The process of risk management



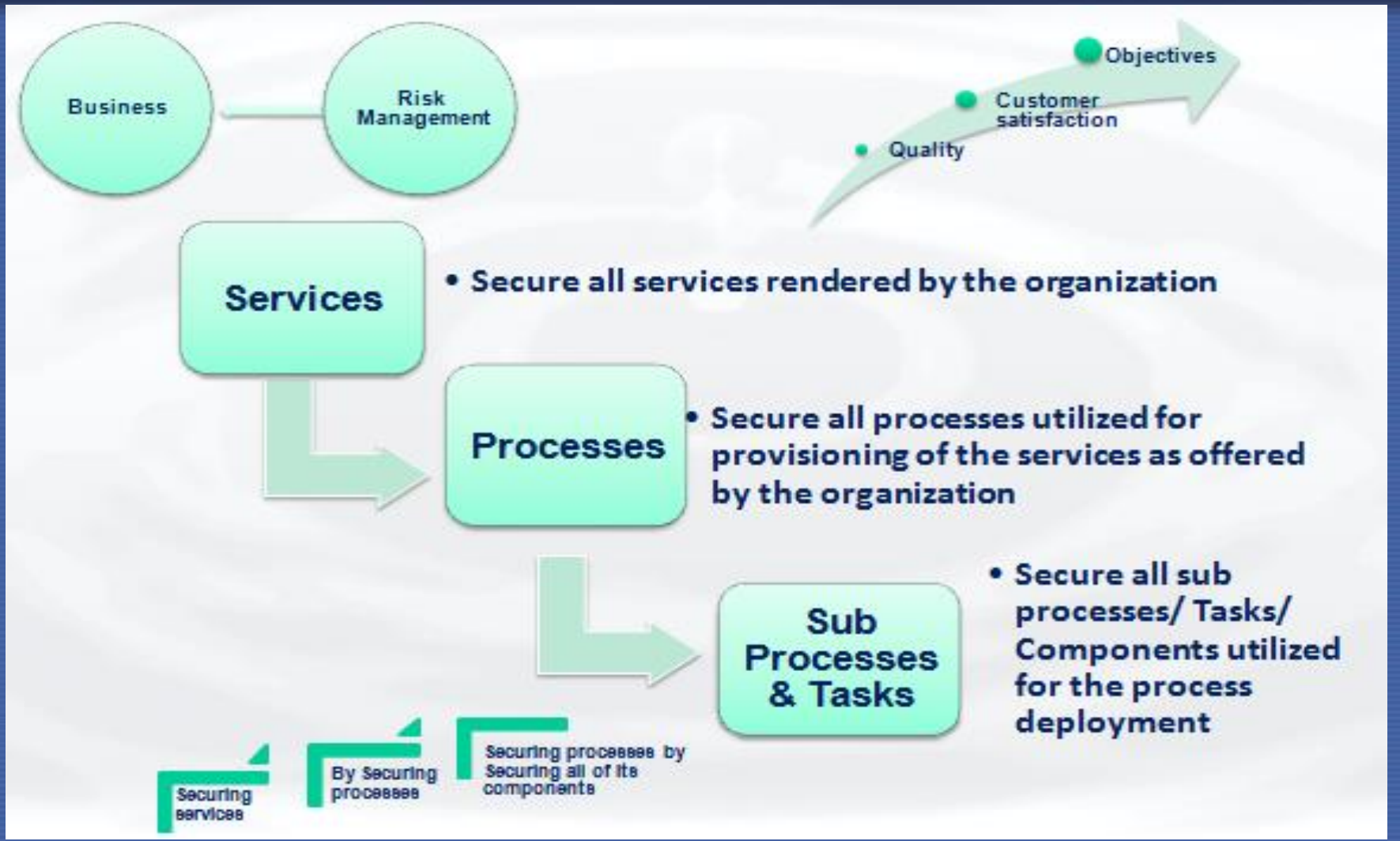
Risk and Opportunity

The objective of this presentation are to appreciate and understand how an QMS is established in terms of:

Four Phases of Risk



Risk assessment process



Risk Management Approach

- Dependent on type of laboratories
- Dependent on type of customers
- Dependent on type of assets and processes
- Management Commitment

Risk Assessment Tools

- Perception based
- History / experience / data based
- Types – Qualitative and Quantitative depends on size / scale and complexity of operations
- **Qualitative model –**
  - Purely perception based;
  - Experience / history can also be added
  - Involvement of all

ISO/IEC 17025:2017 is not suggesting any tools and laboratory can use own methodology for laboratory

IAEA

Risk Assessment Tools

- **Qualitative model –**
  - Impact / Severity (I) e.g. rating 1 – 5
  - Probability/Likelihood (P) e.g. rating 1 – 5
  - Risk factor : I x P (e.g. rating of 1 to 25)

  - Review – periodically based upon feedback of incidents, complaints, objectives

Severity/Impact

- 5 A very high risk band where adverse risks are intolerable whatever benefits the activity may bring. Risk reduction is essential, whatever the cost
- 4 A high risk band where the risk would not be generally acceptable unless there were significant benefits
- 3 A medium risk band where costs and benefits are taken into account and opportunities are balanced with potential adverse consequences.
- 2 A low risk band where positive or negative risks are small and potential benefits can be justified
- 1 A very low risk band where risks are negligible and no risk treatment are necessary.

Risk Assessment in Organization

Risk Assessment Severity Example

Potential Business Impact	Business Operations and Financial Health	Legal and Regulatory Obligations	Impact on customer, reputation and Loss of Goodwill	Personal Information/ Laboratory Human issues
Low	Little or no Disruption/ Financial Loss	No Legal or Regulatory obligation	Minor and Limited embarrassment within the organisation	No distress or Embarrassment caused
Medium	Detrimental to business efficiency or financial health	Technical breach of a legal or regulatory obligation	Adversely affect relations with customers or shareholders	Minor embarrassment or distress to an individual
High	Cause serious disruption/ financial loss	Serious breach of legal or regulatory requirements	Seriously affect relations with customers and shareholders	Serious embarrassment or distress
Very High	Could lead to bankruptcy	Could lead to the organisation being closed down	Threaten the future of the business	Widespread and serious embarrassment or distress

Probability / Likelihood

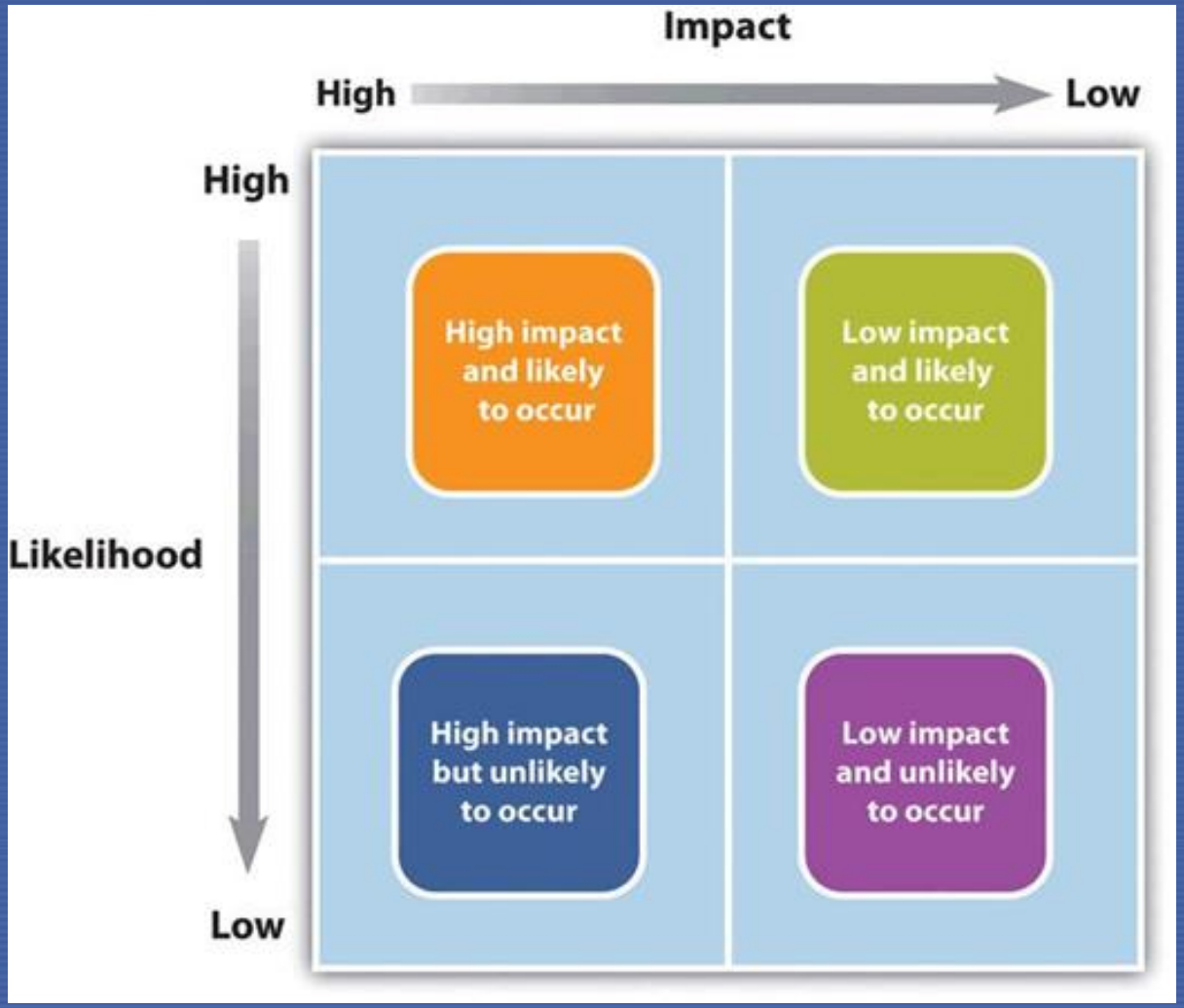
- 5 A very high probability band (continuous, every day, every batch etc.) Risk reduction is essential, whatever the cost
- 4 A high probability band (every supplier change, chemist change weekly, every material unload)
- 3 A medium probability band (monthly, product campaign end, seasonal).
- 2 A low probability band (yearly, equipment change).
- 1 A very low probability band (never happened, once in lifetime).

Risk Assessment Likelihood Example

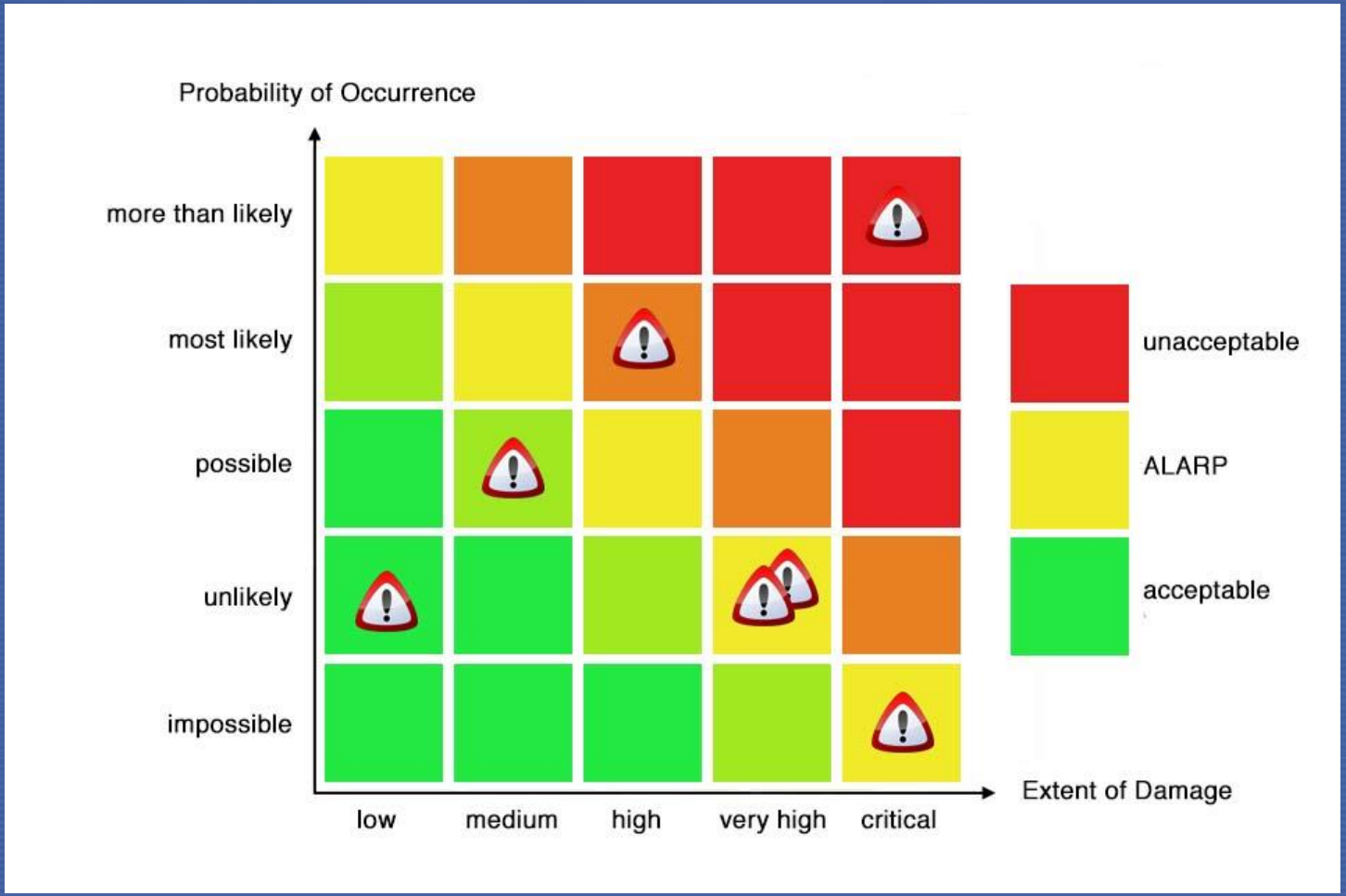
Risk Assessment

Very low -1	An event that is highly unlikely to occur ,if ever
Low- 2	An Event that is unlikely to occur, perhaps once every 3 years
Medium -3	An event likely to occur relatively infrequently
High -4	An event that is fairly probable, and could be expected to occur several times a year
Very High -5	A highly frequent event. This event could reasonably expected to occur at least every month or more frequently

Risk Evaluation – the "risk matrix"

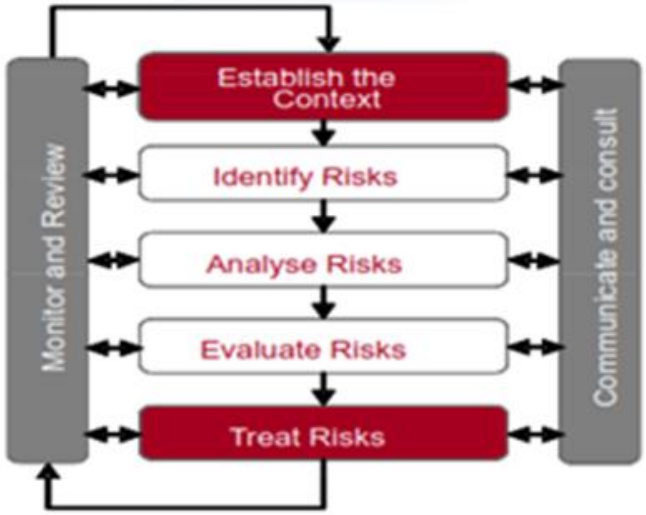


The Decision Table



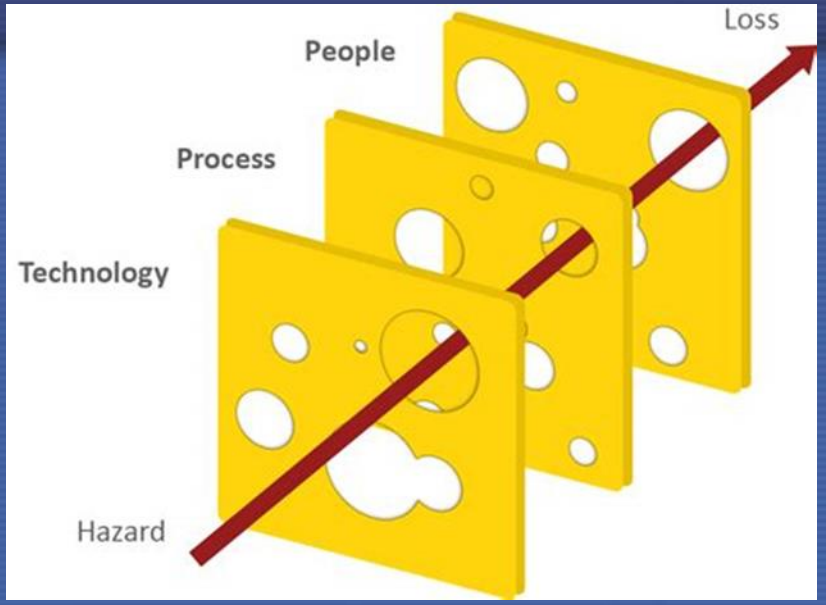
Sample Risk Sheet

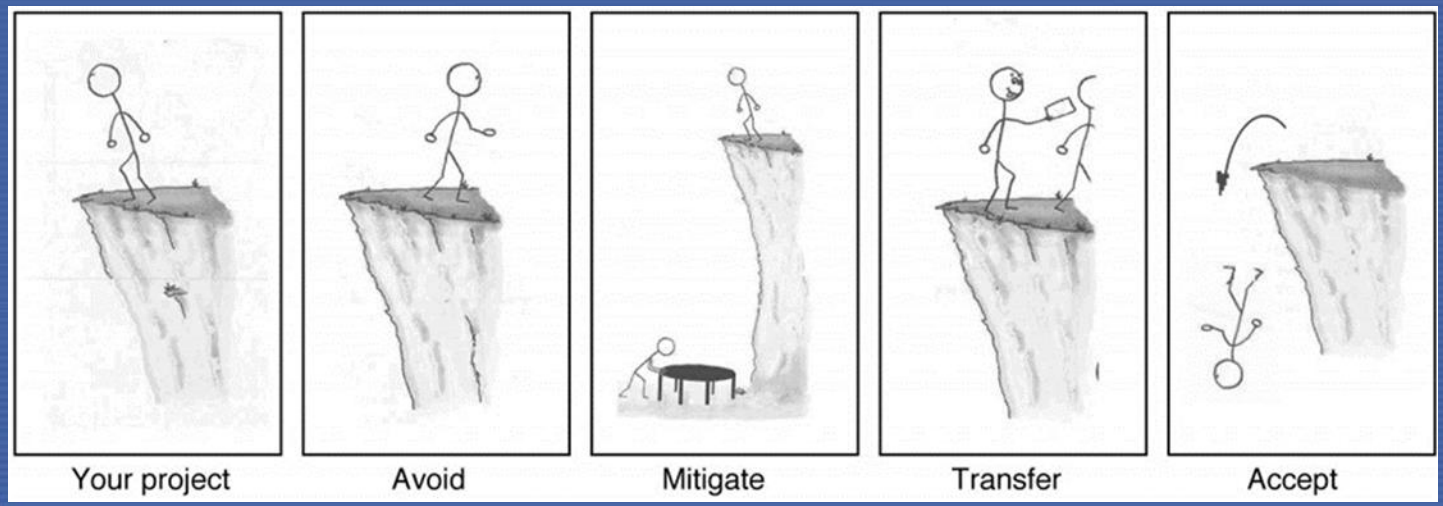
Risk Factor = Likelihood x Severity



Process	Sub Process	Task / Components	RISKS Associated						Likelihood (Po)	Impact	Risk Value
			Tech/Quality	Customer	Env	People	legal	Others			

Risk treatment – Define & Implement Controls/Preventive Actions





IAEA

Risk Treatment – A PDCA cycle

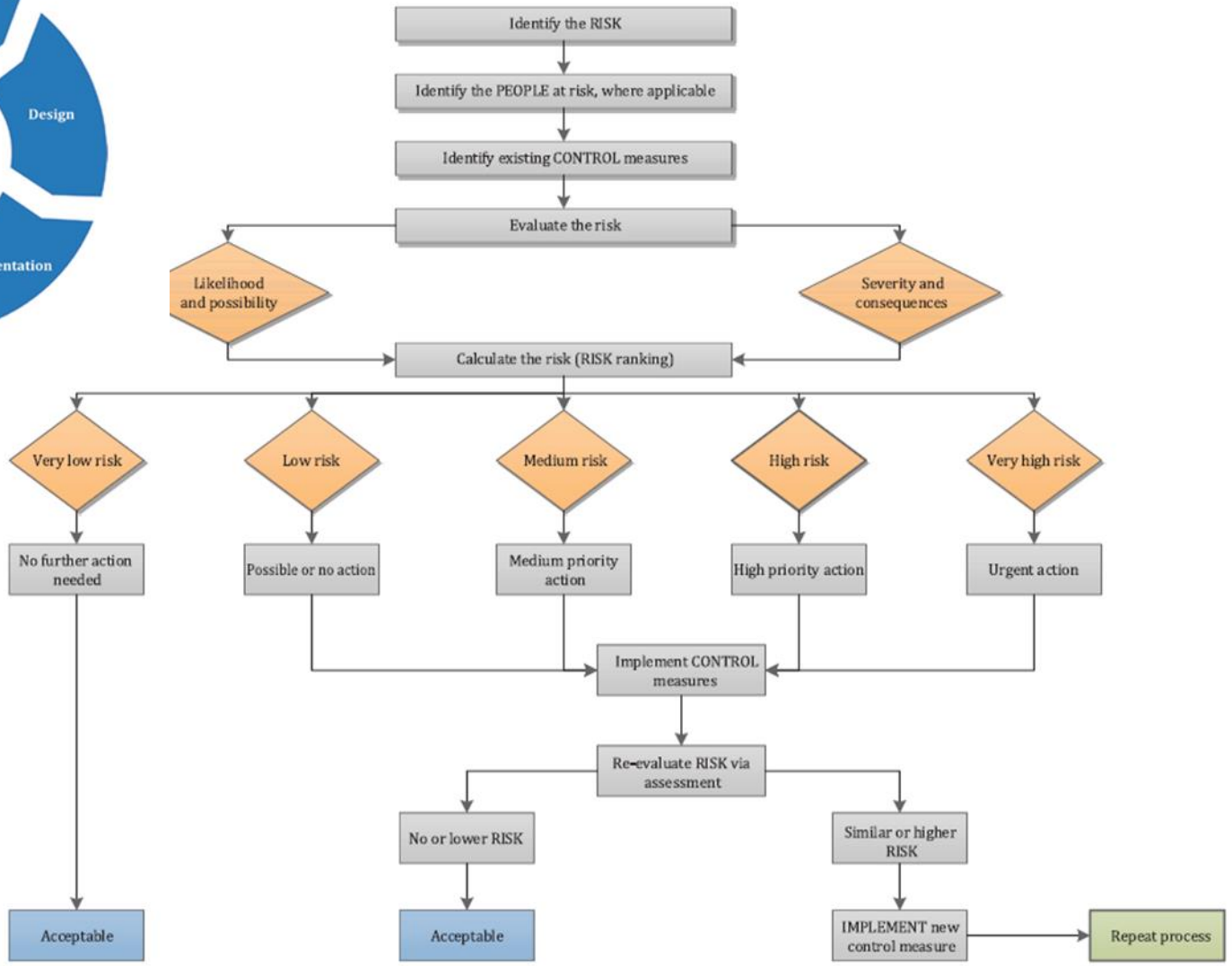


Figure A.1 — Risk assessment flow chart

The PDCA-Cycle – from inherent to residual risk

1. Environment & Objectives → 2. Event Identification → 3. Risk Assessment → 4. Risk Monitoring and Reporting

Inherent Risk Assessment (IR)

Risk Description	Impacts
There is a risk that the company is not in a position to recover its operations in the event of a disaster or major outage.	◻ Financial ◻ Reputation ◻ Regulatory/Legal ◻ Safety ◻ Services

Inherent Risk Assessment	
Consequence	Major (7)
Likelihood	Likely (4)
Overall Risk Rating	Extreme (28)

Consequence	Likelihood				
	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Catastrophic (9)	9	18	27	36	45
Major (7)	7	14	21	28 (IR)	35
Moderate (5)	5	10	15	20	25
Minor (3)	3	6	9	12	15
Insignificant (1)	1	2	3	4	5

Residual Risk Assessment (RR)

Causes	Control Strategy
Cause 1- Service Areas have not identified continuity and recovery requirements.	Undertake a Business Impact Assessment (BIA).
Cause 2- Inadequate or no CMP.	Create and test a CMP to ensure …

Residual Risk Assessment	
Consequence	Minor (3)
Likelihood	Unlikely (2)
Overall Risk Rating	Low (6)

Consequence	Likelihood				
	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Catastrophic (9)	9	18	27	36	45
Major (7)	7	14	21	28 (IR)	35
Moderate (5)	5	10	15	20	25
Minor (3)	3	6 (RR)	9	12	15
Insignificant (1)	1	2	3	4	5

Areas to consider during risk and opportunity identification

- Laboratory Requirement
- Business Requirement
- Contractual Requirement
- Client/customer Requirement
- Process and product requirements
- Legislative Requirement
- Regulatory Requirement
- Technical Requirements
- Human/Staff Requirements

Risk - Examples under ISO/IEC 17025:2017

Risk – Examples:

- **Human**
  - Non availability/long leave
  - Inadequate skill/competence
- **Technical**
  - Product specification not achieved/ Quality issue
  - Process failure or capability utilization
  - Delay in delivery
  - Failure of Network , Poor System performance
- **Customer related**
  - Delay in payment
  - Delay in communication and approval
- **Physical**
  - Theft, Willful Damage
- **Environmental**

  Power failure, Fire, Water, Legal authority notice

IAEA

Example of a template

				Initial Risk Assessment (without any controls in place)				Residual Risk Assessment			
Sr #	Area	Activities / Process	Quality Concerns / Risks	Severity Rating	Likelihood	Risk Rating	Existing Controls in Place	Severity Rating	Likelihood	Risk Rating	Further Controls Required
1	Lab Activities	Sample collection	Misidentification of sample/specimen	3	3	9	Sample receiving person from lab verify name & identification Criteria. Furthermore, as sample received in lab it is entered in Sample Log and batch number/code is also alotted otherwise he will return sample to customer for proper identification	3	1	3	
2	Lab Activities	Sample collection	Samples received in lab is not placed in controlled environment	4	2	8	All sample are stored in designated location of lab and environment conditions of lab is recorded on daily basis. Lab Incharge also verified environment record.	4	1	4	
3	Lab Activities	Sample preparation	Inaccurate process parameters (e.g. Temp. Pressure, weighing error), expire reagents used in preparation	4	2	8	Weighing balance are calibrated and placed on flat surface. Furthermore rubber pad under weighing balance to reduce vibrations and it is place in designated position. Volume measurement is done through calibrated flask. Chemist are properly trained on testing activities. Reagents lists are available used in testing activities, expiry of reagents are recorded in this list. Before using reagents Chemist verify its expiry	4	1	4	

Risk Treatment

1. Actions selected and implemented to reduce the risks to an acceptable level
2. Preventive Detective or Corrective
3. Measures can be physical procedural or product
4. Cost balance with Risks and Potential impacts
5. Accept the risk with management approval
6. Transfer the risk for example insurance taken
7. Taking risk in order to pursue an opportunity,
8. Eliminating the risk source, changing the likelihood or consequences,
9. Sharing the risk, or retaining risk by informed decision and management acceptance

IAEA

Where Risk is Addressed in ISO/IEC 17025:2017 Standard

- **Several places where risk based thinking is identified in revised ISO/IEC 17025:2017 standard**
- **Reference is** ISO 31000, *Risk management - Principles and guidelines*
- Total 31 times the word “risk” is used in the ISO/IEC 17025:2017 standard

IAEA

Where Risk is Addressed in ISO/IEC 17025:2017 Standard (2)

- § 4.1.4 Identify risks to its impartiality on an on-going basis. Include those risks
  - From its activities,
  - From its relationships with supplier, customer
  - From the relationships of its personnel.

- § 4.1.5 If a risk to impartiality is identified, then laboratory has to demonstrate how it eliminates or minimizes such risk.

Where Risk is Addressed in ISO/IEC 17025:2017 Standard (3)

- § 7.8.6 When a statement of conformity to a specification or standard is provided, the laboratory shall document the decision rule employed, taking into account the level of risk (such as false accept and false reject and statistical assumptions) associated with the decision rule employed and apply the decision rule. If the decision rule is prescribed by the customer, regulations or normative documents, a further consideration of the level of risk is not necessary.

- § 7.10.1 b Actions (including halting or repeating of work and withholding of reports, as necessary) are based upon the risk levels established by the laboratory.

IAEA

Where Risk is Addressed in ISO/IEC 17025:2017 Standard (4)

- § 8.5 Actions to address risks and opportunities

- § 8.5.1 The laboratory has to consider the risks and opportunities associated with the laboratory activities in order to:

  a) give assurance that the management system achieves its intended results;

  b) enhance opportunities to achieve the purpose and objectives of the laboratory;

  c) prevent, or reduce, undesired impacts and potential failures in the laboratory activities;

  d) achieve improvement

Where Risk is Addressed in ISO/IEC 17025:2017 Standard (5)

- § 8.5.2 The laboratory shall plan:
  - a) actions to address these risks and opportunities;
  - b) how to:
    - integrate and implement these actions into its management system;
    - evaluate the effectiveness of these actions.

NOTE Although this document specifies that the laboratory plans actions to address risks, there is no requirement for formal methods for risk management or a documented risk management process. Laboratories can decide whether or not to develop a more extensive risk management methodology than is required in ISO/IEC 17025, e.g. through the application of other guidance or standards

Where Risk is Addressed in ISO/IEC 17025:2017 Standard (6)

- § 8.5.3 Actions taken to address risks and opportunities are proportional to the potential impact on the validity of laboratory results. The Options to address risks can include identifying and avoiding threats, taking risk in order to pursue an opportunity, eliminating the risk source, changing the likelihood or consequences, sharing the risk, or retaining risk by informed decision.
  - NOTE 1 Options to address risks can include identifying and avoiding threats, taking risk in order to pursue an opportunity, eliminating the risk source, changing the likelihood or consequences, sharing the risk, or retaining risk by informed decision.
  - NOTE 2 Opportunities can lead to expanding the scope of the laboratory activities, addressing new customers, using new technology and other possibilities to address customer needs.

IAEA

Where Risk is Addressed in ISO/IEC 17025:2017 Standard (7)

- **§ 8.6.1 Improvement:** Opportunities for improvement can be identified through the review risk assessment, analysis of data, and proficiency testing results

- § **8.7.1 e Corrective Action:** Update risks and opportunities determined during planning, if necessary for corrective action.

- **§ 8.9.3 m Input to management review:** results of risk identification to discuss in management review meeting;