[ISO/IEC 17025:2017
RISK MANAGEMENT

By :

SIRIM STS Sdn Bhd

AGENDA

TIME	ACTIVITIES	
0900 – 1015	Introduction to Risk Management Risk Based Thinking in ISO/IEC 17025:2017	Risk Management Process : - Risk Identification - (Exercise 2)
1015 – 1030	**Break**	**Break**
1030 - 1300	Risk Management Based on ISO 31000:2018 Principles and Framework	Risk Management Process : - Risk Analysis and Evaluation -(Exercise 3)
1300 – 1400	**Lunch Break**	**Lunch Break**
1400 – 1530	Risk Management Process : - Establish context - Exercise 1	Risk Management Process : -Risk Treatment -(Exercise 4) - Presentation
1530 – 1545	**Break**	**Break**
1545 – 1700	Presentation	Procedure Risk Management - Risk management procedure

COURSE OBJECTIVE

- to explain on risk-based thinking in ISO/IEC 17025
- to explain the risk management process
    - Establish context
    - Risk Identification
    - Risk Analysis and Evaluation
    - Risk Treatment
    - Monitoring and Review

What do we know about RM?

- RM is part of our every day lives:

• Crossing the road	- Risk of getting run-over
• Managing our finances	– Risk of going broke
• Purchase of insurance	– Risk of fire, theft, storm
• Choosing to smoke	– Risk of cancer
• Going for a swim	– Risk of drowning

- The choices we make in choosing to accept these risks is part of who we are

Understanding Risk Management

Risk is around us…

- Risk arises from uncertainties that can deviate our goals
- Risk are to be managed – "no risk, no gain"

DEFINITION OF RISK

3.1 Risk – Effect of uncertainty on objectives

Note 1 An effect is a deviation from expected – positive and / or negative, and can be address, result in opportunities and threats

Note 2 Objective can have difference aspects and categories (such as financial, health and safety, and environmental goal) and can apply at different levels (such as strategic, organization-wide, project, product and process)

Note 3 Risk is usually expressed in term of risk sources (3.4), potential events (3.5), their consequences (3.6) and their likelihood (3.7).

(Source ISO 31000)

DEFINITION OF RISK MANAGEMENT

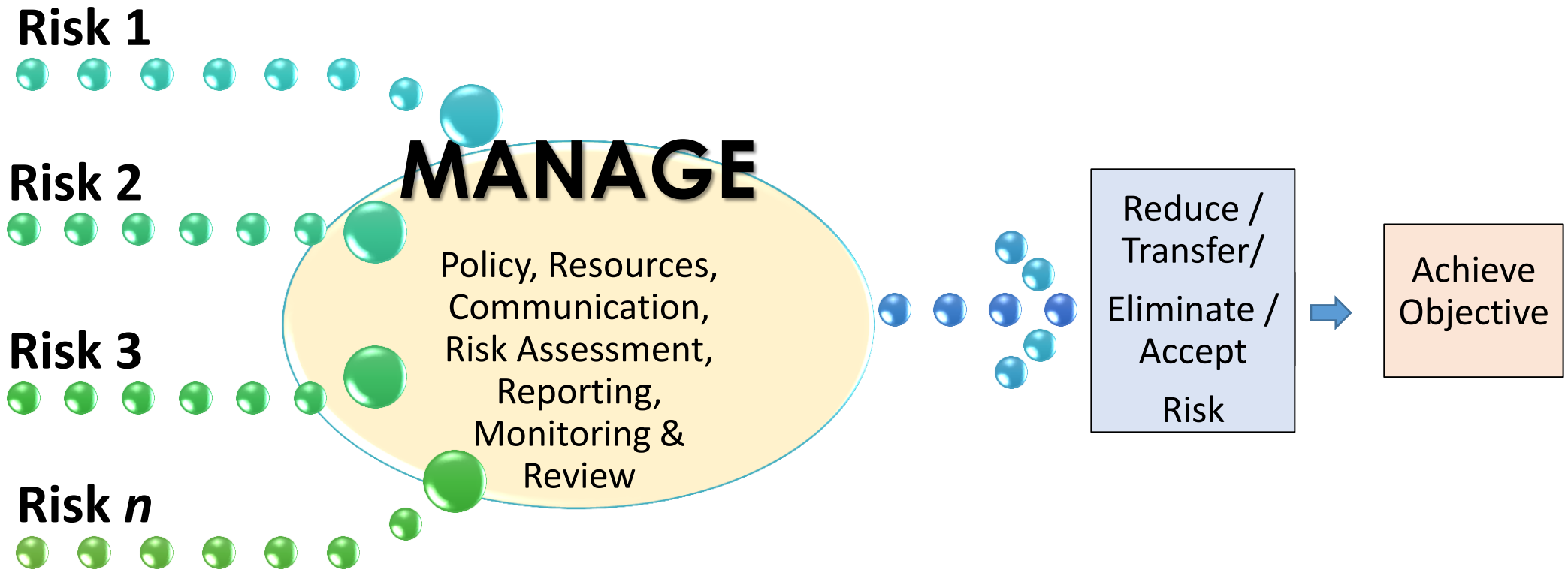
- coordinated activities to direct and control an organization with regards to risk.

  (Adaptation From ISO 31000:2018 Risk Management - Principles And Guidelines)

- Risk Management Comprises **a framework and process** that enable an organization to **manage uncertainty** in a systemic, effective, efficient and systematic way from **strategic, programme, project and operational** perspectives, as well as **supporting continual improvement**

  (BSI British Standard Risk Management - Code of practice BS31100:2008)

What is risk management?



RISK ASSESSMENT PROCESS

Identify

Analyze

Evaluate

BUT there is no requirement for a formal risk management or a documented risk management process in ISO/IEC 17025:2017

A COHERENT SET STANDARDS

- ISO 31000:2018 "Risk management – Principles and guidelines"
- ISO Guide 73 "Risk management – Vocabulary"
- ISO/IEC 31010 "Risk management – Risk assessment techniques"
- HB 327:2010 – Communicating and consulting about risk
- AS/NZS 5050:2010 Business Continuity – Managing disruption-related risk
- HB 266:2010 – Guide for managing risk in not-for-profit organization
- ISO/IEC 27005 – ISMS – RISK MANAGEMENT

Why RISKS MANAGEMENT?

LIFE IS FULL OF UNCERTAINTIES

Risk Management is to reduce the uncertainties in order to

- **Increase the likelihood of achieving the objectives**
- **Improve the identification of opportunities and threats, and**
- **Effectively allocate and use resources for risk treatment**

Understanding Risk Management

Why Manage Risk

Compliance:

In compliance with ISO ISO/IEC 17025 :2017

- Minimize threat and maximize opportunity
- Reduce operational surprises and losses
- Resources are rationalized
- Less management time on fire fighting

Understanding Risk Management

Consequences of Improper Risk Management

In today's world, organisations cannot afford to be caught "off guard" by unexpected events that can cause:

Physical Damage

Loss of Reputation

Potential Legal Suit

Fatality & Major Injuries

Operational Losses

Non Compliance To Regulatory Requirements

What is “Risk-Based Thinking

- Risk-based thinking is something we all do automatically and often sub-consciously
- The concept of risk has always been implicit in ISO 9001 – the 2015 revision makes it more explicit and builds it into the whole management system
- Risk-based thinking is already part of the *process approach*
- Risk-based thinking makes *preventive action* part of the routine

- *Risk is often thought of only in the negative sense. Risk-based thinking can also help to identify opportunities. This can be considered to be the positive side of risk*

Risk Management FOR ISO/IEC 17025:2017 Based On ISO 31000:2018

Understanding Risk Management

ISO/IEC 17025:2017

WHAT TO COMPLY

OBJECTIVES

8.5 Action to address risk and opportunities (Option A)

8.5.1 The organization shall consider the risks and opportunities associated with the laboratories activities in order to:

a) Give **assurance** that management system can achieve its intended result
b) **Enhance** opportunities to achieve the purpose and objectives of the laboratory
c) **Prevent/reduce** undesirable effects and potential failures in the laboratory activities
d) **Achieve improvements**

8.5.2 The laboratory shall plan:

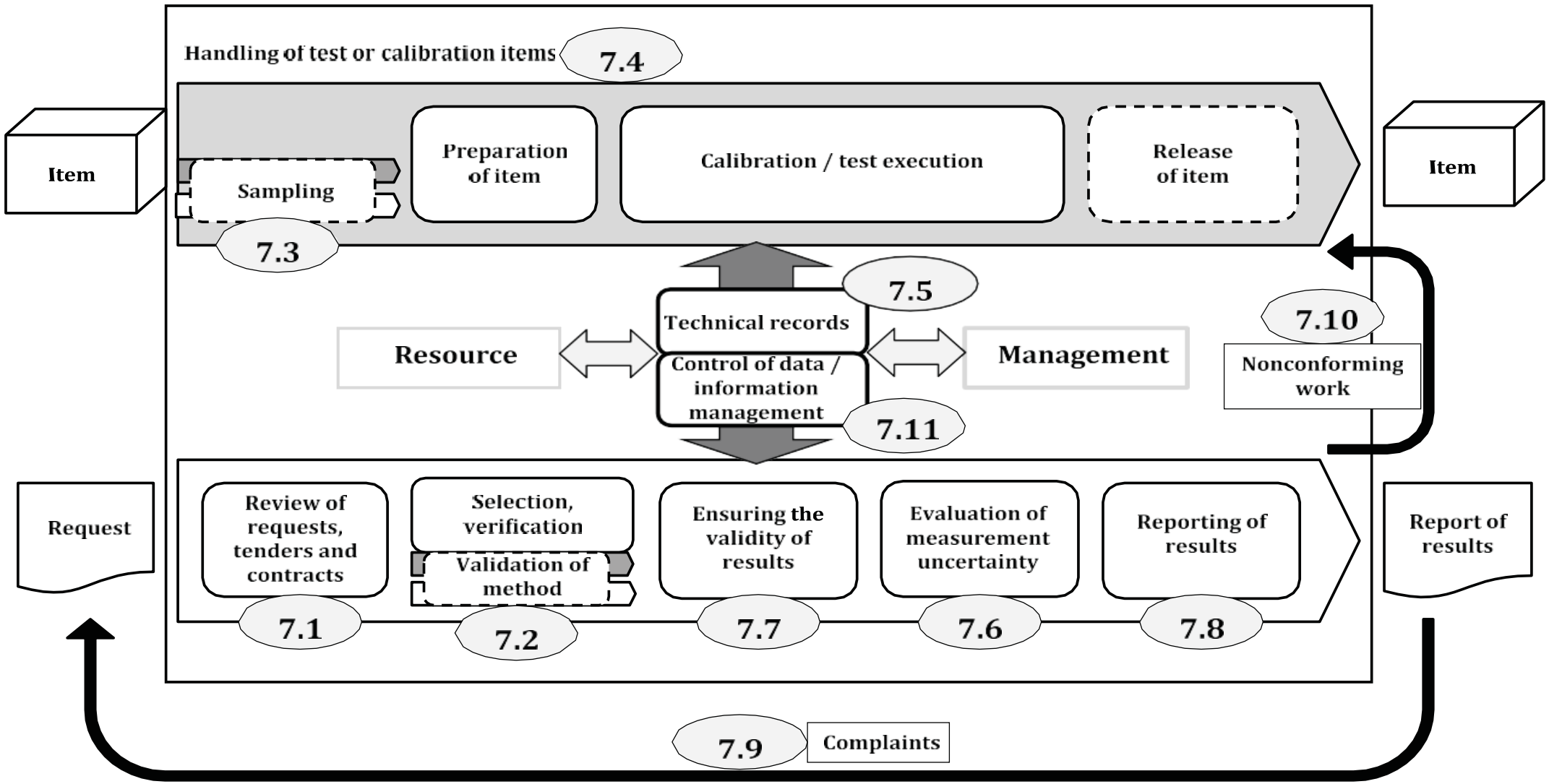
a) Actions to address risks and opportunities;
b) How to:
    1) Integrate & implement actions into its management system;
    2) Evaluate the effectiveness of these actions.

8.5.3 Actions taken to address risks and opportunities shall be proportionate to the potential impact on the validity of laboratory result.

Source: ISO/IEC 17025

RISK IN ISO/IEC 17025:2017 CLAUSES

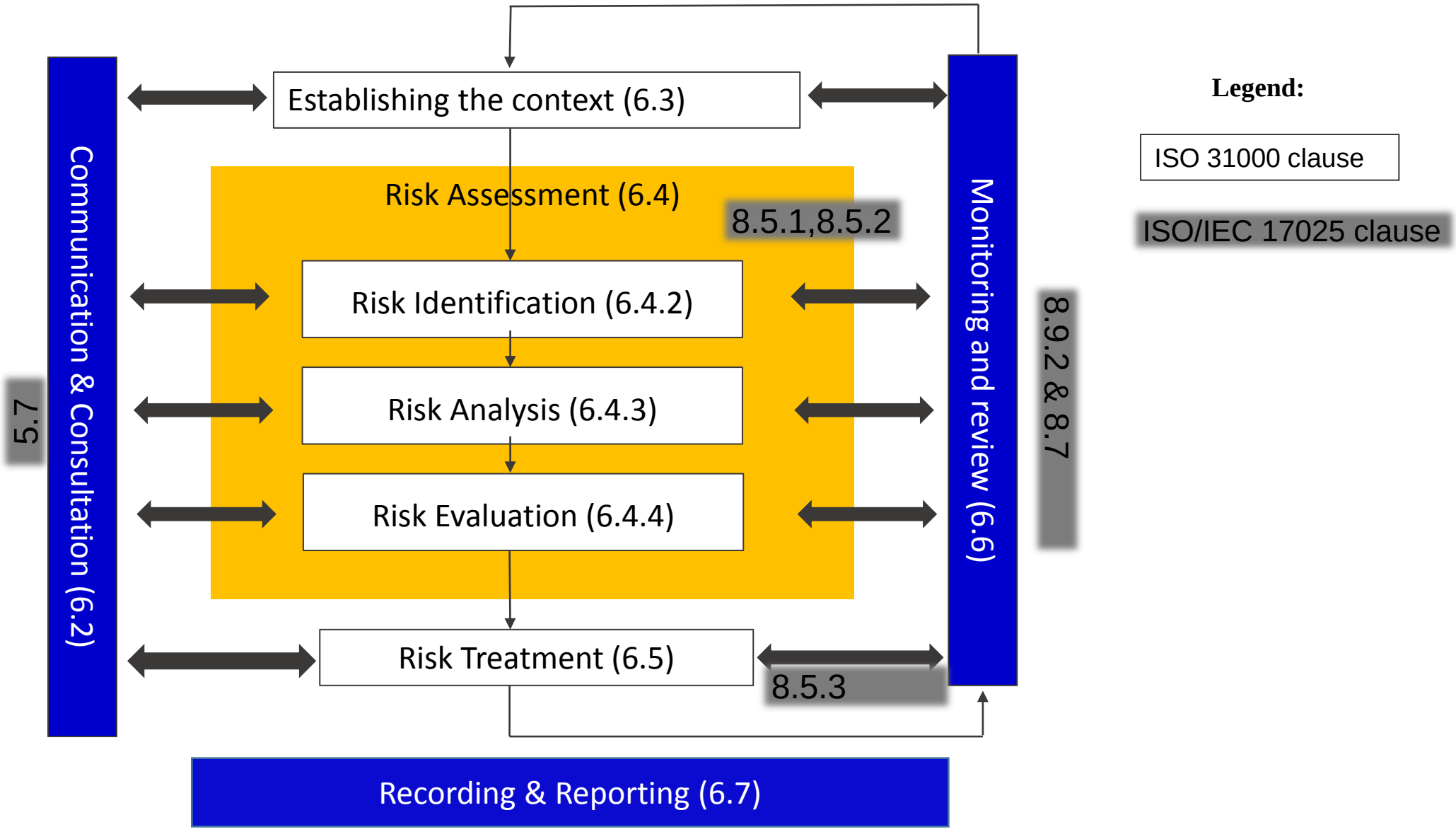
Clause	Details
4.1.4	The laboratory shall identify risks to its impartiality on an on-going basis. This shall include those risks that arise from its activities, or from its relationships, or from the relationships of its personnel. However, such relationships do not necessarily present a laboratory with a risk to impartiality
4.1.5	If a risk to impartiality is identified, the laboratory shall be able to demonstrate how it eliminates or minimizes such risk.
7.8.6.1	When a statement of conformity to a specification or standard is provided, 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.
7.10b	Take actions based upon the risk levels (including halting or repeating of work and withholding of reports, as necessary)
8.7 e	update risks and opportunities determined during planning, if necessary;
8.9.2a	changes in internal and external issues that are relevant to the laboratory
8.9.2m	results of risk identification;



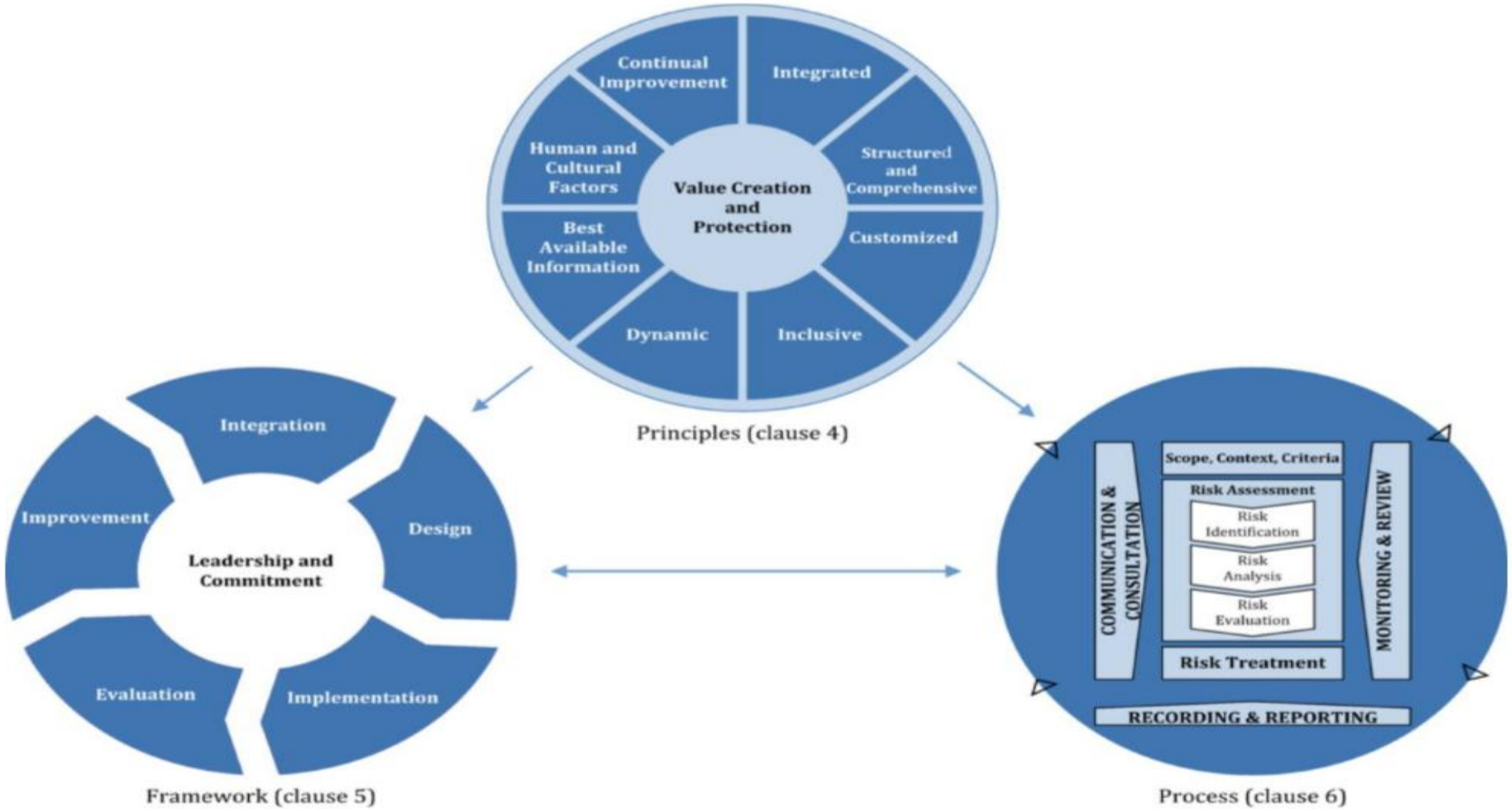
Operational processes of a laboratory

18

ISO 31000:2018 AND ISO/IEC 17025:2017 INTEGRATION



ISO 31000:2018 - STRUCTURE



RISK MANAGEMENT FRAMEWORK

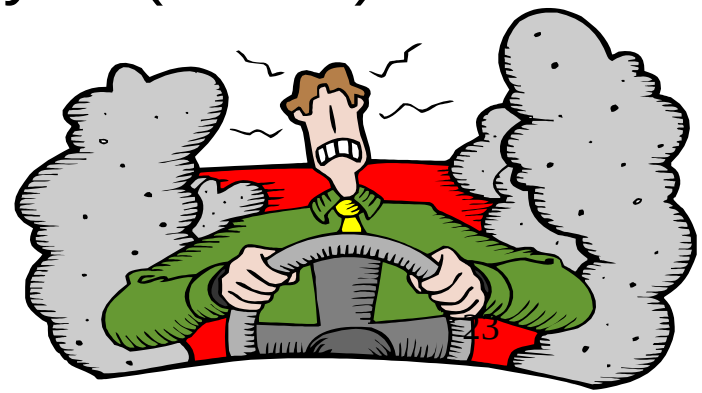
- To esure the organization in integrating risk management into significant activities and functions.
- The effectiveness of risk management will depend on its intergration into governance of organization, including decision making.
- Required support from stakeholder- top management

INTEGRATION INTO ORGANIZATIONAL PROCESSES

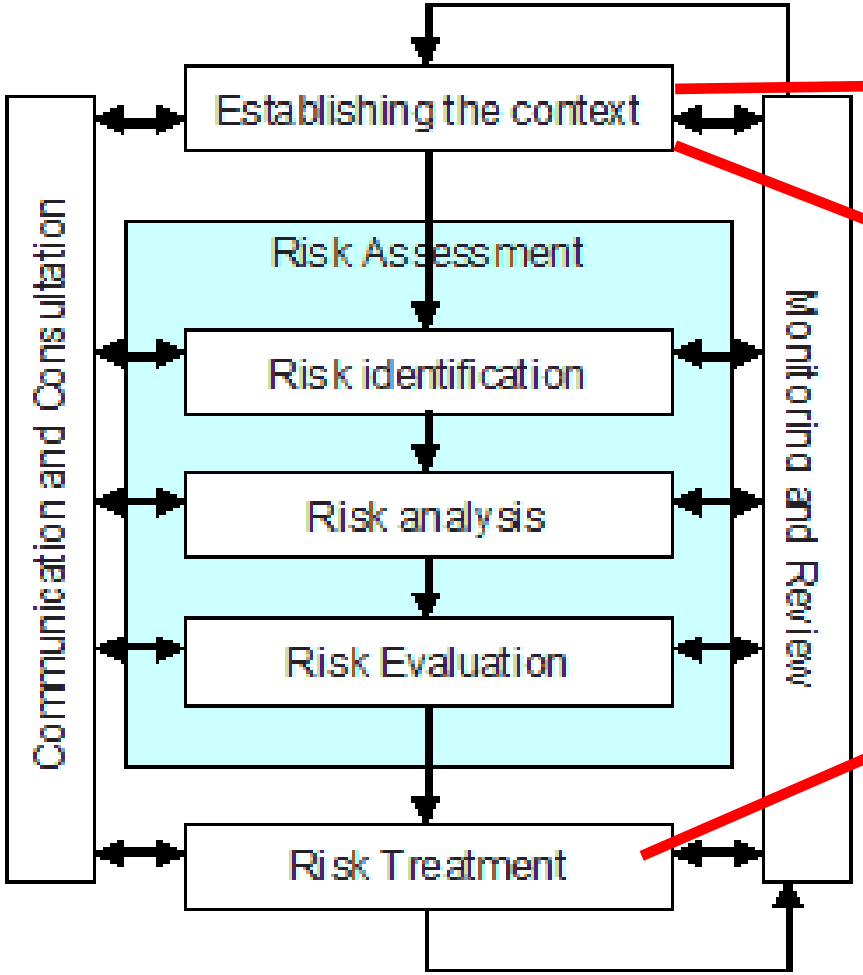
- Risk management should be embedded in and not be separated from organizational practices and processes
- Especially policy development, strategic planning and change management
- Risk management plan to ensure:
  - Implementation of Risk Management policy
  - Risk Management is embedded in all practices and processes

EXAMPLE OF TECHNIQUE

- Hazard Identification, Risk Assessment and Determining Control (HIRADC)
- Hazard and Operability Study (HAZOP).
- Hazard Analysis Critical Control Points (HACCP)
- Aspect And Impact - ISO 14001
- Hazard Analysis - OHSAS 18001
- Fault Tree Analysis (FTA)
- Failure Mode and Effect Analysis (FMEA)



Risk Management Process



Understanding the organisation and its context

Understanding the needs and expectations of interested parties

8.5 Action to address risk and opportunities

RISK FORMAT

- Document used for recording risk management process for identified risks.
- The risk register will cover the significant risks facing the organization or project.
- It will record the results of the risk assessment related to the process, operation, location, business unit or project under consideration.

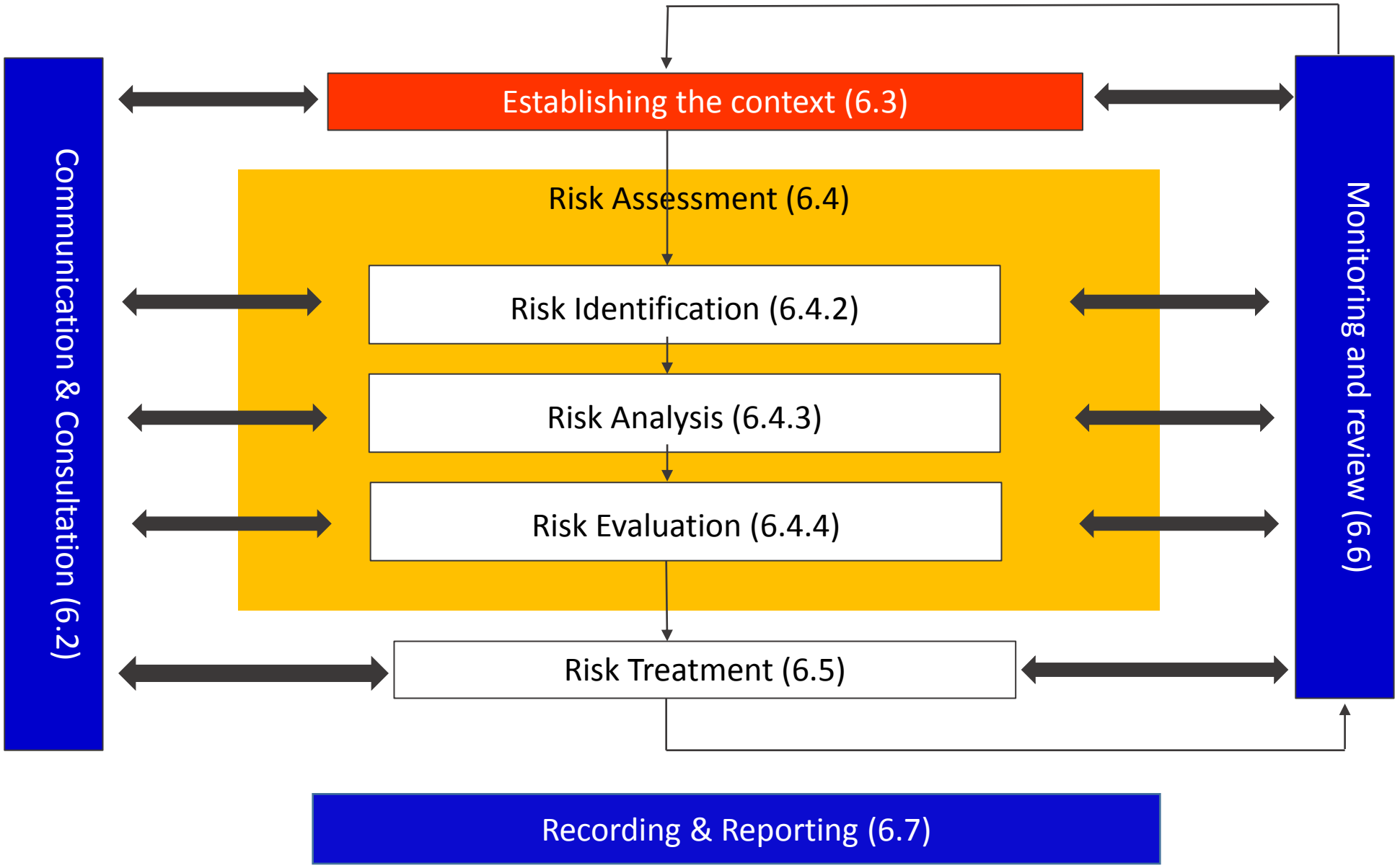
RISK ASSESSMENT FORMAT

Location:	Dept.	Prepared by: Date:	Checked by: Date:	Approved by: Date:
		Review Date:	1.	2.

Risk category	1. Risk Identification				2. Risk Analysis and Evaluation				3. Risk Control		Status
	Process	Risks	Cause	Effect	Current Risk Control	Likelihood	Severity	Risk Rating	Recommended Action /Additional Control	PIC (Due Date/Status)	

Risk Management Process

RISK MANAGEMENT PROCESS



Establish Context

Establish context means defining the ***external and internal*** parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy

Source: ISO 31000

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and its **strategic direction and that affect its ability to achieve intended result of its quality management system**

i. **Issues can include positive and negative** factors or conditions for consideration
ii. **Understanding the external context can be facilitated by considering issues arising** from legal, technological, competitive, market, cultural, social and economic environments, whether international, national, regional or local
iii. **Understanding the internal context can be facilitated by considering issues** related to values, culture, knowledge and performance of the organization

4.2 Understanding the needs and expectations of interested parties

Due to their effect or potential effect on the organization's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, the organization shall determine

i. The interested parties that are relevant to the quality management system
ii. The requirements of these interested parties that are relevant to the quality management system

The organization shall monitor and review information about these interested parties and their relevant requirements.

Source: MS ISO 9001:2015

SOURCES of RISKS

INTERNAL

Resources

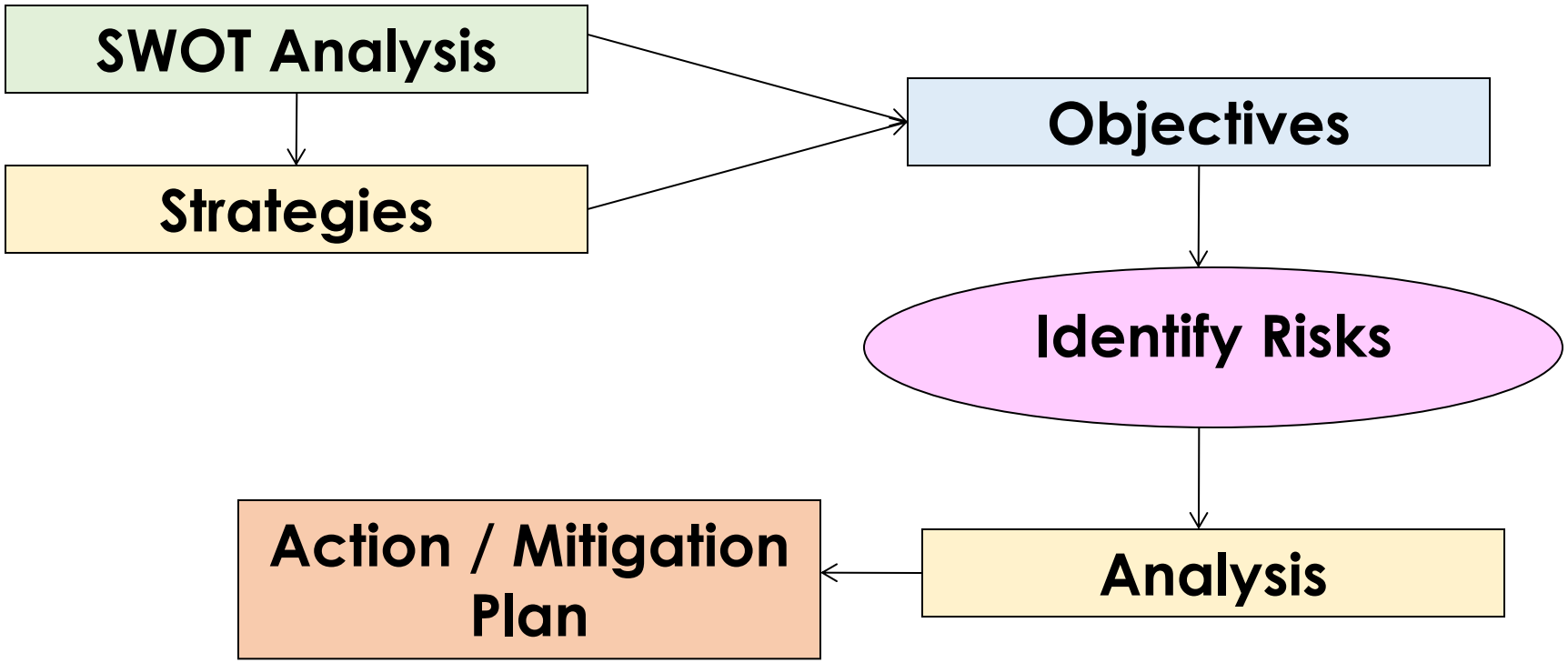
Processes

Inadequate internal controls,
Human errors (incompetence, inexperienced, corruption)
IT failure
Inadequate human resources
Operational Risks
Legal Risks??

EXTERNAL

Political risk
Country Risk
Market Risk
Currency Risk
Interest Rate Risk
Counter-part Risk
Credit or default Risk
Environmental Risk

RELATION BETWEEN STRATEGY, OBJECTIVES AND RISK MANAGEMENT



Risk & Strategic Issues

RISK AND STRATEGIC ISSUES

Division / Region /Dept. : _____ Date: _____

NO.	STRATEGIC DIRECTION	CATEGORY OF ISSUES (INTERNAL / EXTERNAL)	STRATEGIC ISSUES	INTERESTED PARTIES INVOLVED	RISK	OPPORTUNITIES
0	**[KPI 2018]**	**P.E.S.T.E.L**	**[Issues impacted organization's strategic direction]**	**[Issues may affect or potential affect requirements from interested parties]**	**[Specific Risk] (*Specific risk shall register in Risk Management Template; It can be Enterprise Risk Management or Operational Risk Management)**	**[Specific Opportunities]**
1.	Revenue and New Project launched (Project LINAS on testing of waste water analysis)	ECONOMIC	Loosing potential no. of businesses for full commercialization due to obsolete testing method and not marketable.	1. Material Testing Lab & Microbiological Lab 2. Customer 3. Rating Agency of Malaysia	Decreasing & fluctuating of revenue	Maximize Testing Scope and Competitive Pricing
2.	1. Land Matters 2. Timely & completion of Divisional Risks program (New Laboratory legislation requirements) 3. OSHE Compliances	LEGAL	1. Non-compliance to applicable statutory bodies, government agencies, local authorities. 2. Potential breach of contract between parties.	1. Solicitor / Government agencies 2. Customer (External) 3. External Provider 4. Own Management committee 5. Own group & subsidiaries	Potential penalty or Lawsuit.	100% compliance to applicable statutory requirements.

External Issue

Category	Issue	Interested Party	Risk	Opportunities
Legal/Regulatory	New Standard for ISO17025:2017	SFM lab Top management Lab client Lab employee Standard Malaysia	Delay in accreditation	✓ Improve our management system ✓ Gain knowledge
Technology	SmartiLab	Staff Customer IT Department	Delay in registering and reporting the result	✓ More systematic ✓ Traceability
	New equipment for Protein Distillation 8400 Analyzer	Chemist Supplier	High maintenance cost Chemist unfamiliar with the equipment	✓ Expose to up to date technology ✓ Save the working time ✓ Submit testing report to customer on time
Economic	Minimum wage	PCR officer Worker HR department Labor supply agency	Increase of minimum wage for cleaner	✓ Not shortage of manpower ✓ Satisfaction on routine work

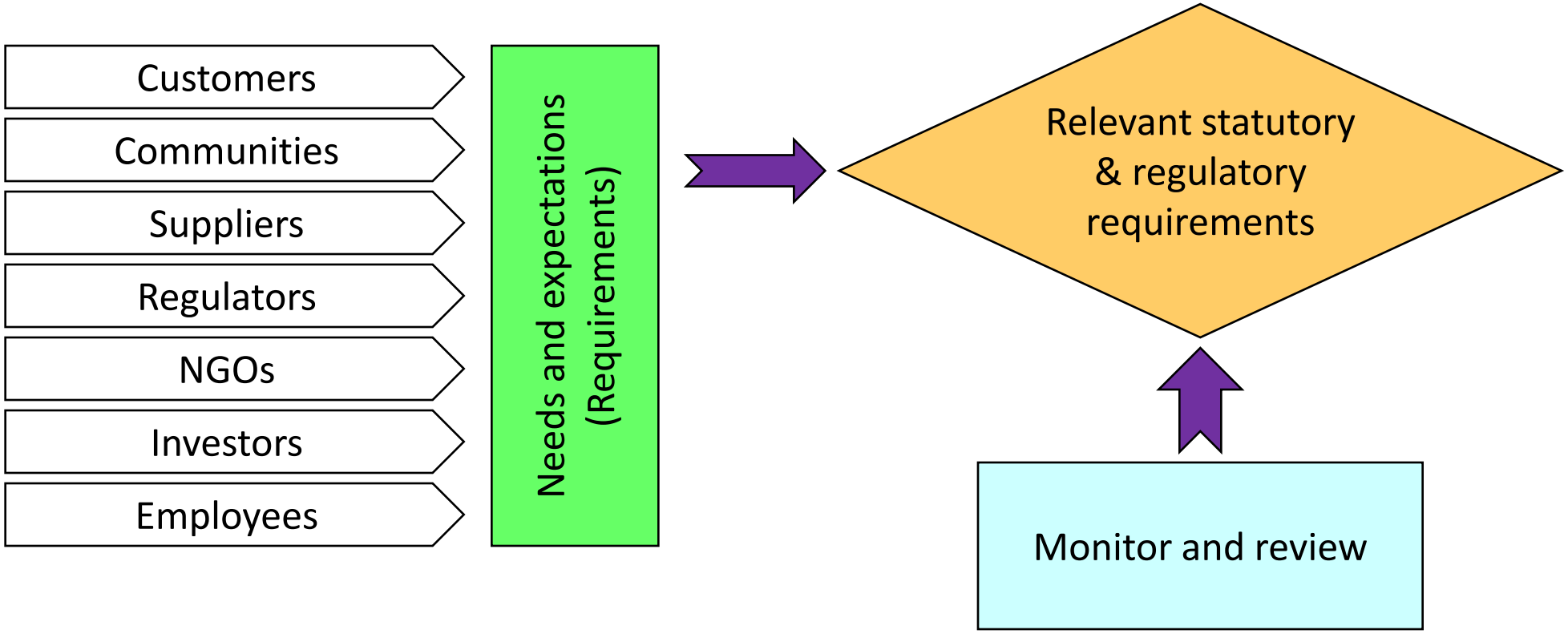
Group Exercise

Establish Context

1. External context includes all external environment parameters and factors that influence how an organization manages risk and tries to achieve its objectives. What are the examples of external context?

2. Internal context includes all internal environment parameters and factors that influence how an organization manages risk and tries to achieve its objectives. What are the examples of internal context?

4.2 Understanding the needs and expectations of interested parties (ISO 9001:2015)

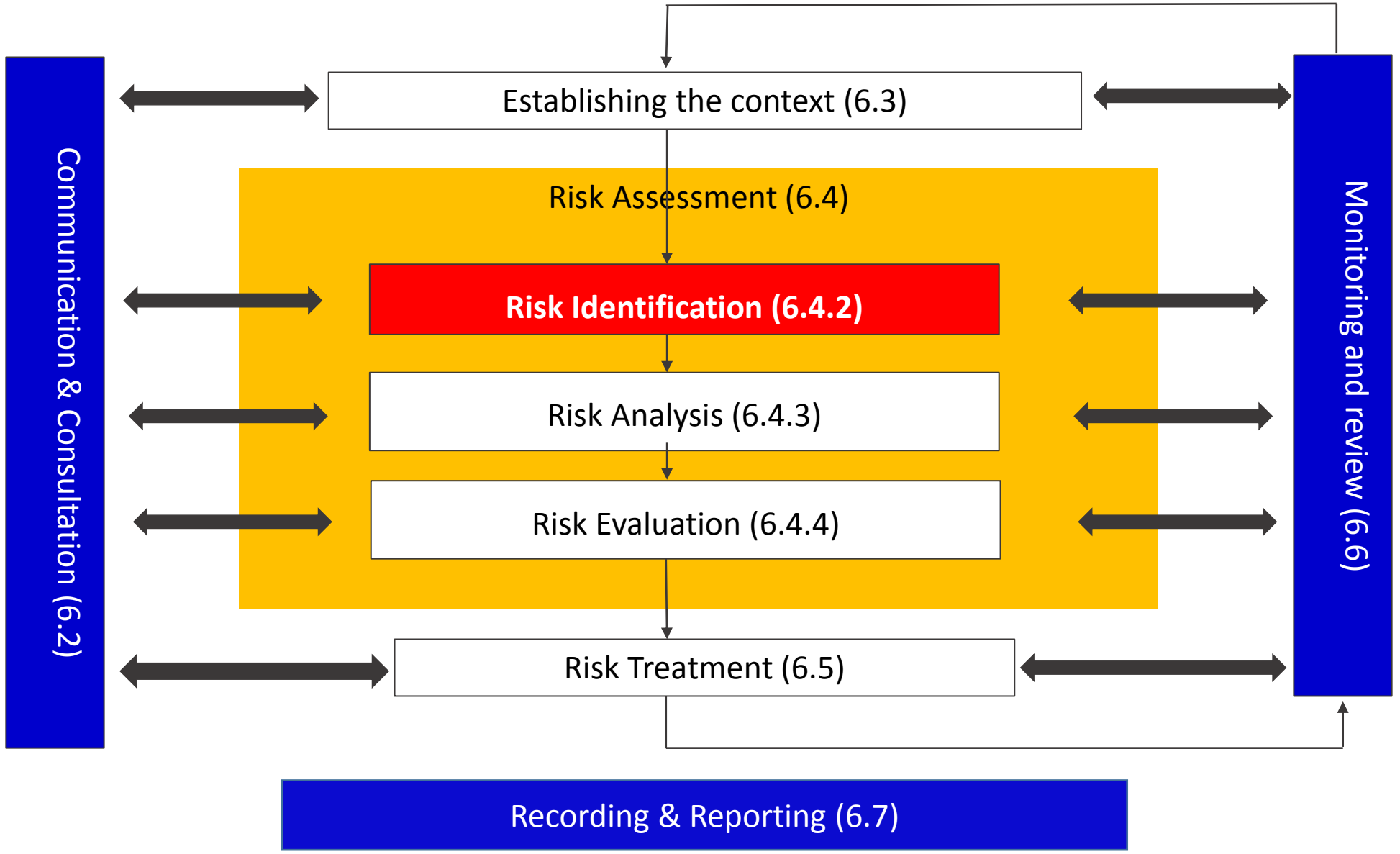


4.2 Understanding the needs and expectations of interested parties (ISO 9001:2015)

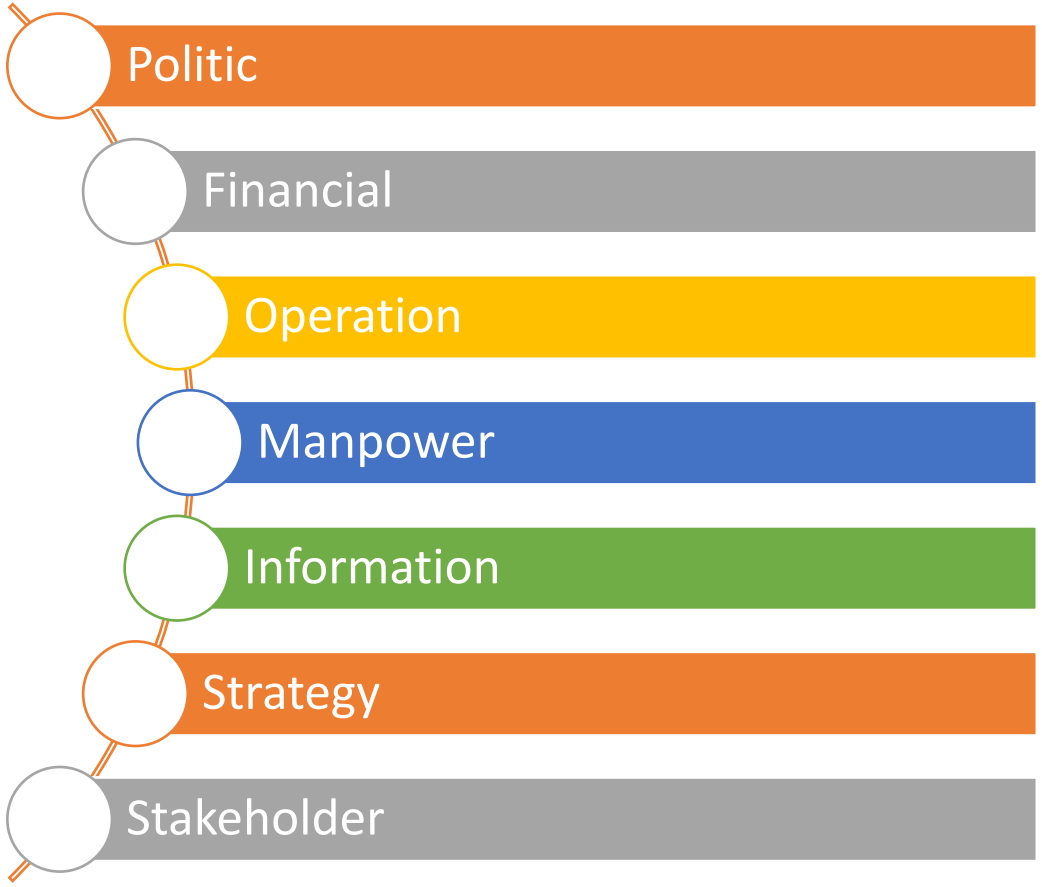
No	Interested Parties	Need and Expectations
1.	Local government authority such as • Ministry of Human resource : Department of occupation safety and health, Human resource development fund • Feed Act 2009- Federal Government Gazette - Feed (Prohibited antibiotics, hormones and other chemicals) Regulation 2012 • Ministry of health Food Act 1983 and Food regulations, Malaysia	Compliance to statutory and regulatory Employee welfares Conductive of safe work environment No fine and penalty
2.	Product and system certification body and accreditation body eg. SIRIM, SGS (Thailand) , SGS (Malaysia), DOF, DVS SAMM etc.	Assess conformity of te company against the

Risk Identification

RISK MANAGEMENT PROCESS



TYPES OF RISKS (RISK CATEGORY)



Selection of risk category as input for risk identification parameter must consider established context that influence objective achievement !!!

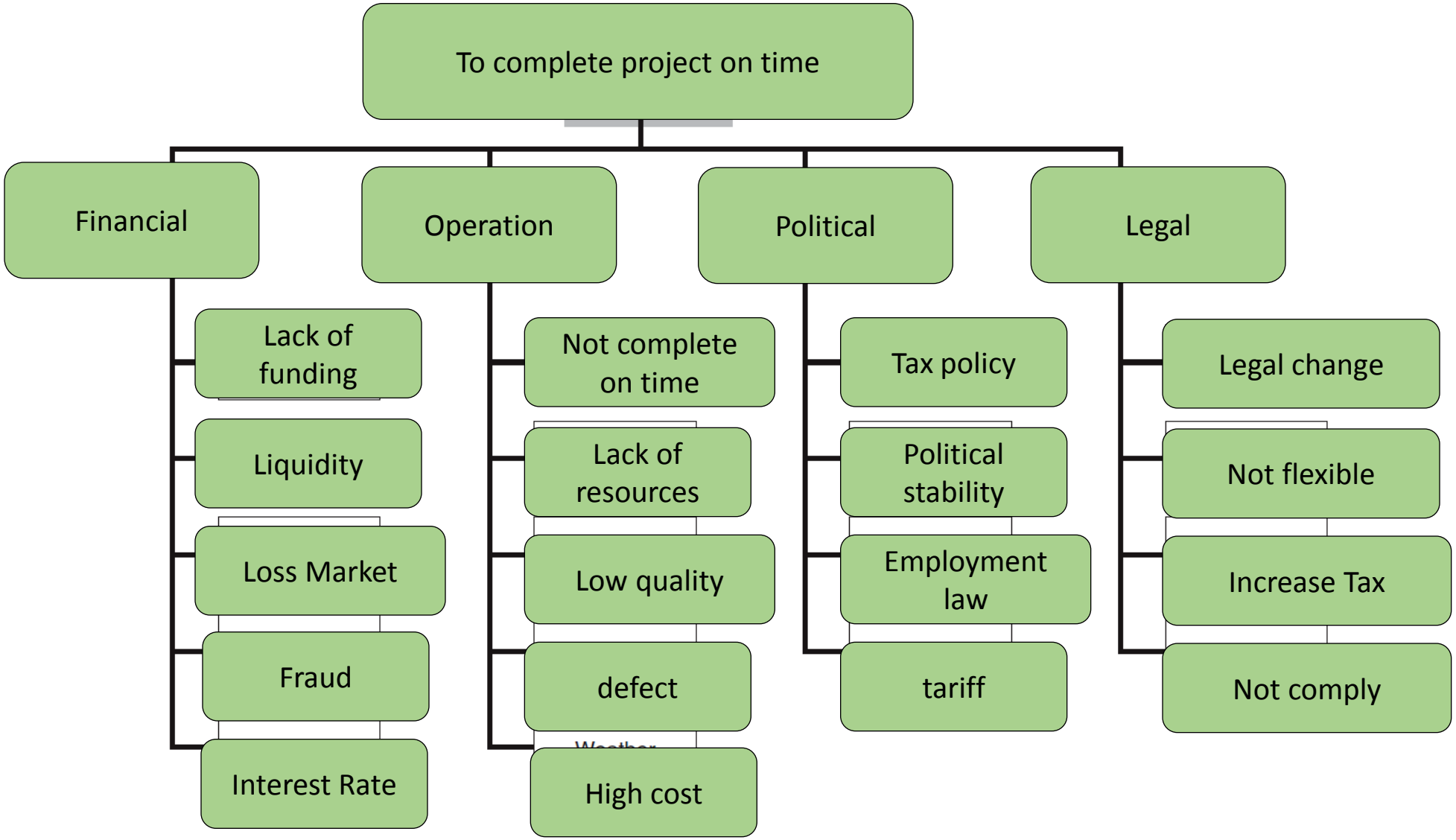
EXAMPLES OF RISKS

Categories	Definition
Politic	Risks associated with changes in national leadership, stability and change leadership
Legal	Risks related to national legislation, contracts, MOU, procedures and policies.
Operation	Risks associated with the work can not be completed on time.
Financial	Risk associated with financial management, transfers, fraud, etc
Manpower	Risks associated with the ability of the workforce, motivation to perform work, high labour turnover, skills shortages, high costs, injury.

EXAMPLES OF RISKS

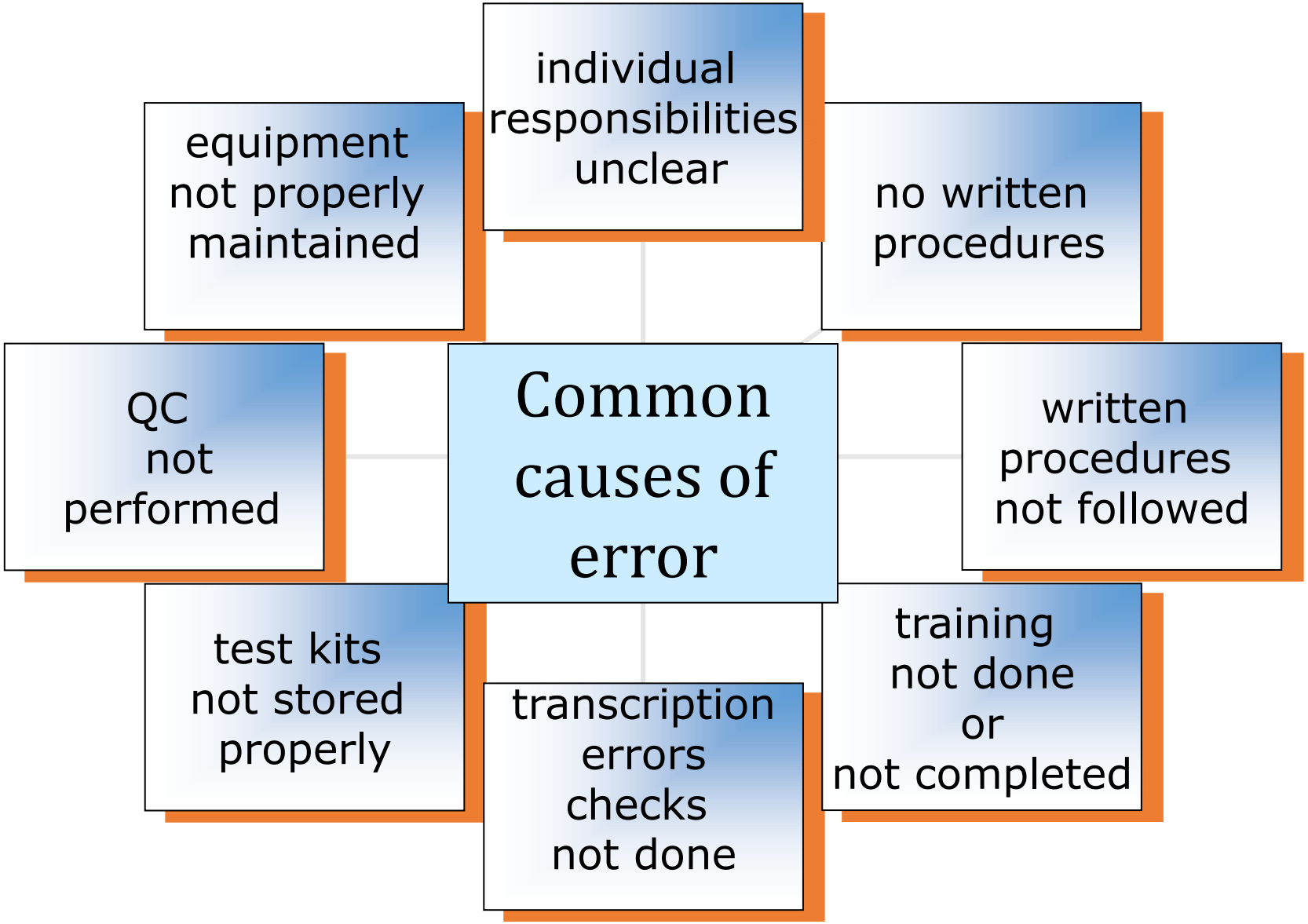
Category	Definition
Information	Risks associated with the resulting information being inaccurate, incomplete, inappropriate, out dated.
Strategy	Risks associated with the strategy or policy failures or mistaken.
Stakeholder	Risks related to failure to achieve the requirements of stakeholders.
Technology	Risks associated with technology infrastructure which is incompatible with the objectives of the business, integrity, relevance, data security and business continuity.
Organization	Risks associated with the organizational structure, accountability, responsibility, which will disturb communication to achieve business objectives.

Structure of Risk (Example)



Some common laboratory errors

- label error
- lost sample
- sample delayed in transit
- contaminated samples
- wrong test performed
- test performed inconsistent with the written procedure
- proficiency testing error
- no action on out of range controls
- false negative result
- late reports
- missing reports
- Complaints
- laboratory accident
- “near miss”


individual responsibilities unclear
equipment not properly maintained
no written procedures
QC not performed
Common causes of error
written procedures not followed
test kits not stored properly
transcription errors checks not done
training not done or not completed

44

Process Risk Management

Risk Identification

Do you know your risk?

Describe the risk!

Identify key process

Identify objective of the key process

What is the risk and how it affects the process?

Who owns the risk?

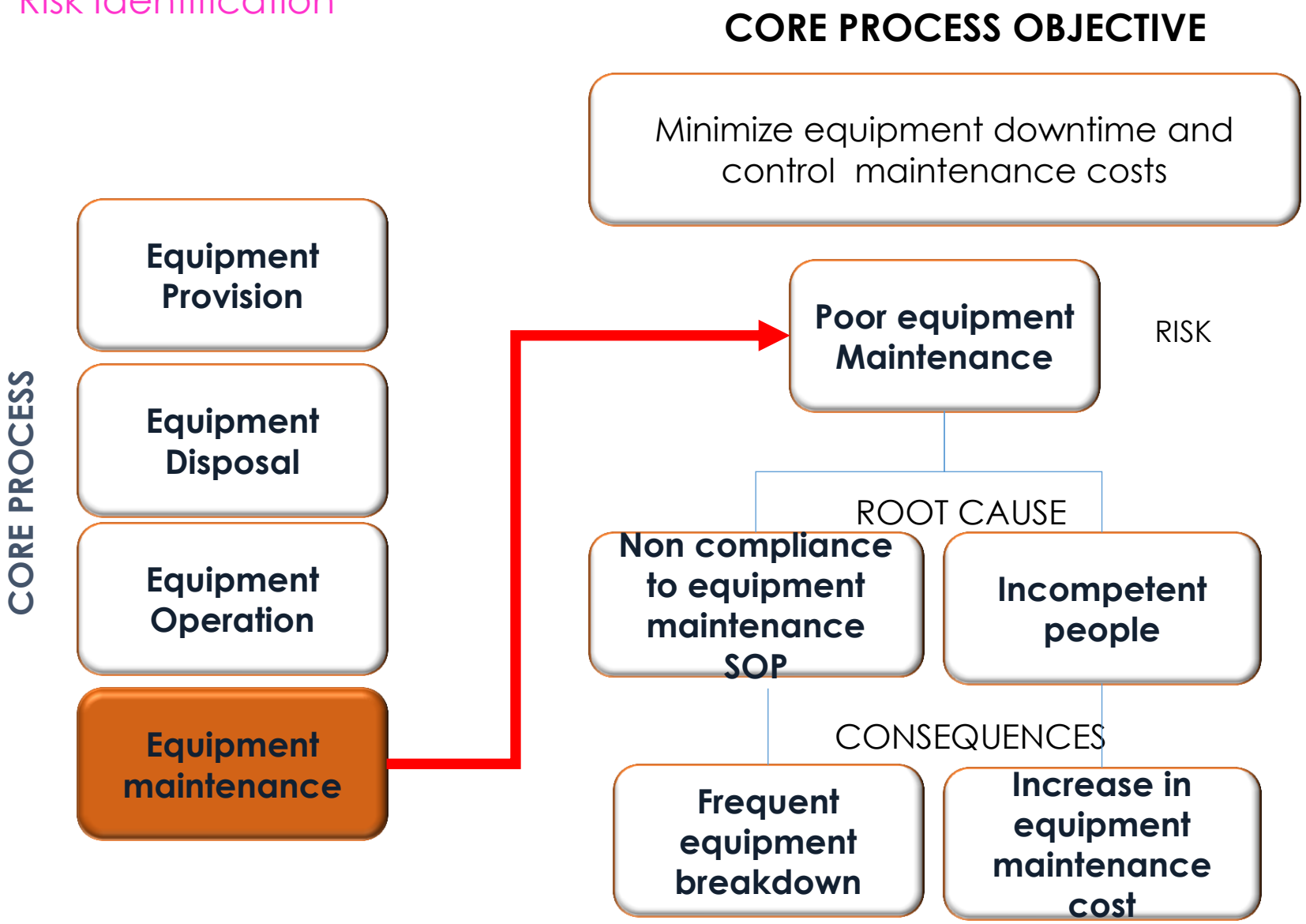
What are the root cause of the risk?

What is the consequences of the risk?

Process Risk Management

Risk Identification

For Illustration Only



Process Risk Management

Risk Identification

Examples of Process Risk

PROCESS	Equipment Maintenance 
PROCESS OBJECTIVE	Minimize equipment downtime, increase operator / user / analyst satisfaction and control fleet maintenance costs
RISK	Poor Equipment Maintenance
ROOT CAUSE	RC1 Non compliance to Equipment maintenance SOP RC 2 Incompetent people
CONSE-QUENCES	C 1 Frequent Equipment breakdown C2 Increase in Equipment maintenance costs

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name / Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

Risk Identification					Risk Analysis & Evaluation				Risk Treatment		Status
Category	Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
[Enter the risk category]	[Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Operation	Confidentiality of information										

Identify Process Function Requirements

- Identify a description of the process or operation being analyzed.
- Process function requirement describes the purpose of the process step / operation.
- Determine the purpose of each process step or process function. May have multiple requirements.

Describe Process Step/ Function/Objective/ Requirements

- Enter a simple description of the process or operation being analyzed.
  - (e.g. Receiving purchasing item, Inspection, Storage, Specimen checking, Waste disposal, etc.)
- Determine the function of each process step
- Indicate as concisely as possible the purpose of the operation being analyzed.

- ***" You cannot identify a failure unless the process characteristic and its requirement have been identified"***

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name/ Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

Risk Identification					Risk Analysis & Evaluation				Risk Treatment		Status
Category	Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
[Enter the risk category]	[Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Operation	Confidentiality of information	Leak of customer information	Unauthorized release confide informa		Policy Statement				Notification to the customer on the information released	Technical Manager	

Describe the manner in which the process could potentially fail to meet the intended process function (s) /requirement (s) described in the previous column.
What could possibly go wrong?

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name/ Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

	Risk Identification				Risk Analysis & Evaluation				Risk Treatment		Status
Category	Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
[Enter the risk category]	1. 1. [Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Operation	Confidentiality of information	Leak of customer information	Unauthorized release of confidential information	Compl custon	Policy Statement on				Notification to the on the n released	Technical Manager	

Root Cause Of risk
Defined as how the risk could occur, described in terms of something that can be corrected and controlled.

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name/ Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

	Risk Identification				Risk Analysis & Evaluation				Risk Treatment		Status
Category	Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
[Enter the risk category]	1. [Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Operation	Confidentiality of information	Leak of customer information	Unauthorized release of confidential information	Complaint by customer	Policy Statement on Quality, Confidentiality and Impartiality				Notification to the customer	Technical	

Effect of risk
Identify potential effects/impact of the risk as perceived by customers.
Should be described as what customer might notice or experience.

Effect(s) of risk

- Brainstorming the "effect of risk" - How does the risk effect the customer.
- Describe the effects of the risk in terms of what the customer might notice or experience.
- State clearly if the risk could impact safety or cause noncompliance to regulations.
- Customer may be external and internal.

Group Exercise

Risk Identification

Know Your Process Risk?

1. Identify Key Process Name, Process Objective & Process Owner
2. Identify risk/ root cause & consequences based on your respective key processes
3. Complete the form given for this activity.

Do not complete Existing Controls & Control Type & Risk Rating section as this will addressed in Risk Analysis & Evaluation session

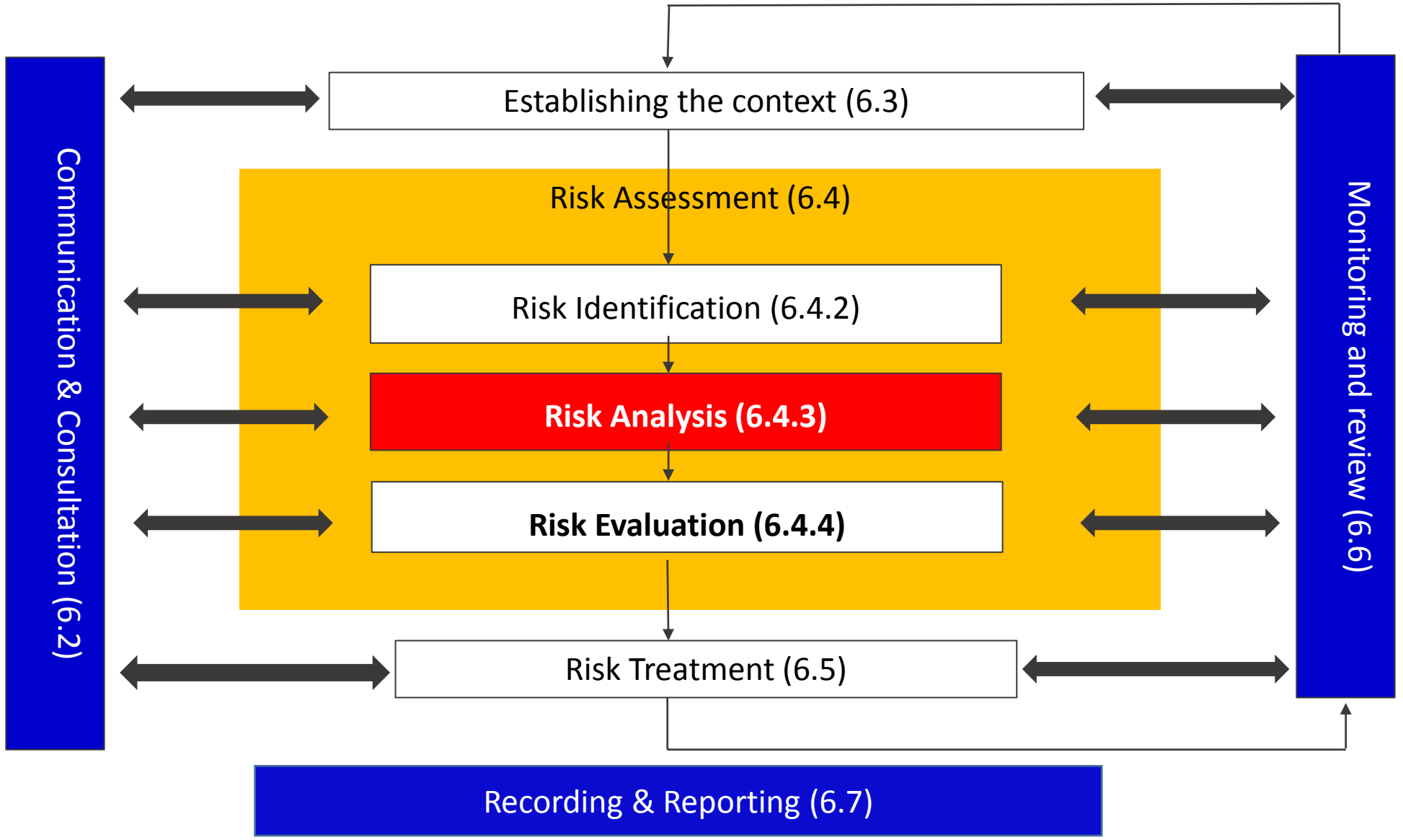
RISK ASSESSMENT FORMAT

Location:	Dept.	Prepared by: Date:	Checked by: Date:	Approved by: Date:
		Review Date:	1.	2.

Risk category	1. Risk Identification				2. Risk Analysis and Evaluation				3. Risk Control		Status
	Process	Specific Risks	Root Cause	consequences	Current Risk Control	Likelihood	Severity	Risk Rating	Recommended Action /Additional Control	PIC (Due Date/Status)	
Operation	Review of request, tenders, and contracts	Incomplete information on analytical form	Lack of cooperation from Customer	Wrong test performed , Waste of resource	Control of record procedure; QSP013						

Risk Analysis & Risk Evaluation

RISK MANAGEMENT PROCESS



Process Risk Management

Risk Analysis & Evaluation

Process to determine

EXISTING CONTROLS TO MITIGATE RISK

LIKELIHOOD OF THE RISK

- Evaluation regarding the chances of risk happening

IMPACT OF THE RISK

- Outcome of the risk (Consequences)
- Financial or Non financial

RISK RATING

- Level or position of risk

Categories of control

Type of Control	Description	Example
Preventive	These controls are designed to limit the possibility of an undesirable outcome being realised	• Elimination or removal of the source of the hazard • Substitution of the hazard with something less risky
Corrective	These controls are designed to limit the scope for loss and reduce undesirable outcomes that have been realized	• Exposure reduction by job rotation or limitation on hours worked • Post implementation review
Detective	These controls are designed to identify occasions of undesirable outcomes having been realized (or example Audit, Inspection & Testing)	• Medical check up (inspection) to seek early symptoms

Current risk control

Safety	PPE, emergency stop button, relief valve, sop
Financial	3rd party financial audit, deposit, Level of authority
Operational	SOP, Quality control inspection
Legal	Contract

But most important, the current risk control must be effective, otherwise it is considered none

RISK ANALYSIS METHODOLOGY

1) Using qualitative or quantitative methods
2) Developing the likelihood scale (e.g: 1-low (Impossible), 5-high (Almost Certain))
3) Developing risk consequences scale (e.g: 1-low (Negligible), 5-high (Critical))
4) Develop risk assessment format (template)

RISK ASSESSMENT FORMAT

Location:	Dept.	Prepared by: Date:	Checked by: Date:	Approved by: Date:
		Review Date:	1.	2.

Risk category	1. Risk Identification				2. Risk Analysis and Evaluation				3. Risk Treatment		Status
	Process	Risks	Cause	Effect/consequences	Current Risk Control	Likelihood	Severity	Risk Rating	Recommended Action /Additional Control	PIC (Due Date/Status)	

Process Risk Management

Risk Analysis - Likelihood (Assessing Probabilities)

- **For actual or recurring events, we use the quantitative method to calculate the probability of risk happening.**
- **For potential event, we use the qualitative method to determine the probability of risk happening based on expert opinion or experience in other companies.**

Level	Level Of Likelihood	Description
1	Rare	The event may occur only in exceptional circumstances – e.g. once in every 3 years or chances of probability is 10% and below
2	Unlikely	The event could occur at some time – e.g. once in every 2 years or chances of probability is above 10% to 25%
3	Possible	The event might occur at some time – e.g. once in every 1 year or chances of probability is more than 25% to 50%
4	Likely	The event will probably occur in most circumstances – e.g. once in 6 months or chances of probability is beyond 50% to 75%
5	Almost Certain	The event is expected to occur in most circumstances – e.g. on a monthly basis or chances of probability is above 75%

Process Risk Management

Risk Analysis – Example of likelihood measurement

	Example of Risk	Likelihood measurement
1	Fall from height (Accident)	Occurrence of incidents involving fall from height

Jan	Feb	Mac	April	Mei	Jun	Julai	Ogos	Sept	Okt	Nov	Dis
-	-	2	1	-	-	-	-	-	-	-	4

The statistics indicate that incidents took place in 3 months (March, April and December).
Therefore, risk likelihood is Unlikely (3 months/ 12 months x 100 = 25%)

UNLIKELY: The event could occur at some time – e.g. once in every 2 years or chances of probability is above 10% to 25%

Process Risk Management

Risk Analysis – Example of financial impact measurement

Variance against targets / budget on financial indicators, e.g. EBITDA, PATAMI , OPEX or REVENUE

LEVEL	LEVEL OF IMPACT	MEASUREMENT
1	INSIGNIFICANT	< 2% variance *
2	MINOR	< 3% variance *
3	MODERATE	< 4% variance *
4	MAJOR	< 5% variance *
5	CATASTROPHIC	> 5% variance *

Process Risk Management

Risk Analysis – Example of non - financial impact measurement

LEVEL	DESCRIPTOR	DESCRIPTION
1	Insignificant	Service disruption involving state level or emergency services below 1 hour
		Recovery period up to 1 week for reputation
		No bodily injuries
		The project is not greatly affected by the event
		Not reported in any media
2	Minor	Service disruption involving state level or emergency services between 1 - 3 hours
		Recovery period up to 3 months for reputation
		Bodily injuries require first aid treatment
		The project may need to be replanned to remain on track
		Reported in local formal media

LEVEL	DESCRIPTOR	DESCRIPTION
3	Moderate	Service disruption involving state level or emergency services between 3-6 hours
		Recovery period up to 1 year for reputation
		Bodily injuries requires medical treatment
		The project will not meet its primary target
		Reported in local formal media & new media
4	Major	Service disruption involving state level or emergency services exceeding 6 hours
		Recovery period of more than 1 year for reputation
		Extensive bodily injuries/permanent disability
		The project will not meet all its objectives
		Reported & criticized in new media and formal media (local & foreign)
5	Catastrophic	Nationwide Service Disruption
		Permanent reputation damage
		Injuries results in death
		The project is stopped
		Highlighted & criticized heavily in new media, formal media (local & foreign) & parliament

- Each key risk owner may suggest the appropriate impact measurement based on the type of risk

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name/ Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

Risk Identification				Risk Analysis & Evaluation				Risk Treatment		Status
Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
1. [Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Confidentiality of information	Leak of customer information	Unauthorized release of confidential information	Complaint by customer	Policy Statement on Quality, Confidentiality and Impartiality	Ra	High	Significant	Notification to the customer on the	Technical	

Current Control (Prevention, Detection) Descriptions of the controls that either prevent the cause of risk from occurring or detect the risk if it occur.

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name/ Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

Risk Identification				Risk Analysis & Evaluation				Risk Treatment		Status
Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
1. [Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Confidentiality of information	Leak of customer information	Unauthorized release of confidential information	Complaint by customer	Policy Statement on Quality, Confidentiality and Impartiality	Rare	High	Significant	Notification to the customer on the information released	Technical Manager	

Likelihood
Likelihood of specific cause of risk will occur.

	Form : Process Risk Assessment	GF/GBA-RCCM/PRA/FM	
		Version 2.0	Date : 01/11/16

Division/Unit : [Division Name/ Unit Name]

Core Process Name : [Core Process Name]

Process Owner : [Process Owner Name]

Date Created : [DD/MM/YYYY]

Date Review : [DD/MM/YYYY]

Reviewed By : [Control Owner Name]

Risk Identification				Risk Analysis & Evaluation				Risk Treatment		Status
Activity	Specific Risk	Root Causes	Consequences	Existing Control	Likelihood & Justification	Impact & Justification	Risk Rating	Additional Control	Control Owner/ Due Date	
1. [Determine activity in the core process address the risk & opportunities]	[Type of risk]	[Detection of risk trigger in core processes]	[Effect of risk occurred]	[Determine action already implemented to control the risk]	[Level of probability risk occur & provide justification] *Refer to Risk Appetite	[Level of consequences risk occurred & provide justification) *Refer to Risk Appetite	[Level of Risk] *Refer to Risk Appetite	[To list down additional key control require to control the risk/for improvement] * If needed	[Responsible person to conduct monitoring and evaluate the effectiveness of these actions & Date to review]	i.e – In Progress / Completed
Confidentiality of information	Leak of customer information	Unauthorized release of confidential information	Complaint by customer	Policy Statement on Quality, Confidentiality and Impartiality	Rare	High		Notification to the		

Impact
Rank associated with the most serious effect for a given risk mode.

Process Risk Management

Risk Analysis – Determining Impact

	Example of Risk	Impact
1	Road Accident	The effects of the risk injury or death (Non-financial) Cases that occurred did not cause death, only serious injury. Thus, the impact is MAJOR

MAJOR - Extensive bodily injuries/ permanent disability

Group Exercise

Risk Analysis & Evaluation

Analyse risk based on the risk that

was identified during previous group exercise

What is Risk Appetite?

Risk appetite should always be within the risk tolerance

- **Amount and type of risk** that an organisation is **prepared to seek, accept and tolerate.**

(Source: British Standard 31100)

- Amount and type of risk that an organisation is **willing to pursue or retain**

(Source: ISO 31000 (Guide 73)

Risk Tolerance (Limit)

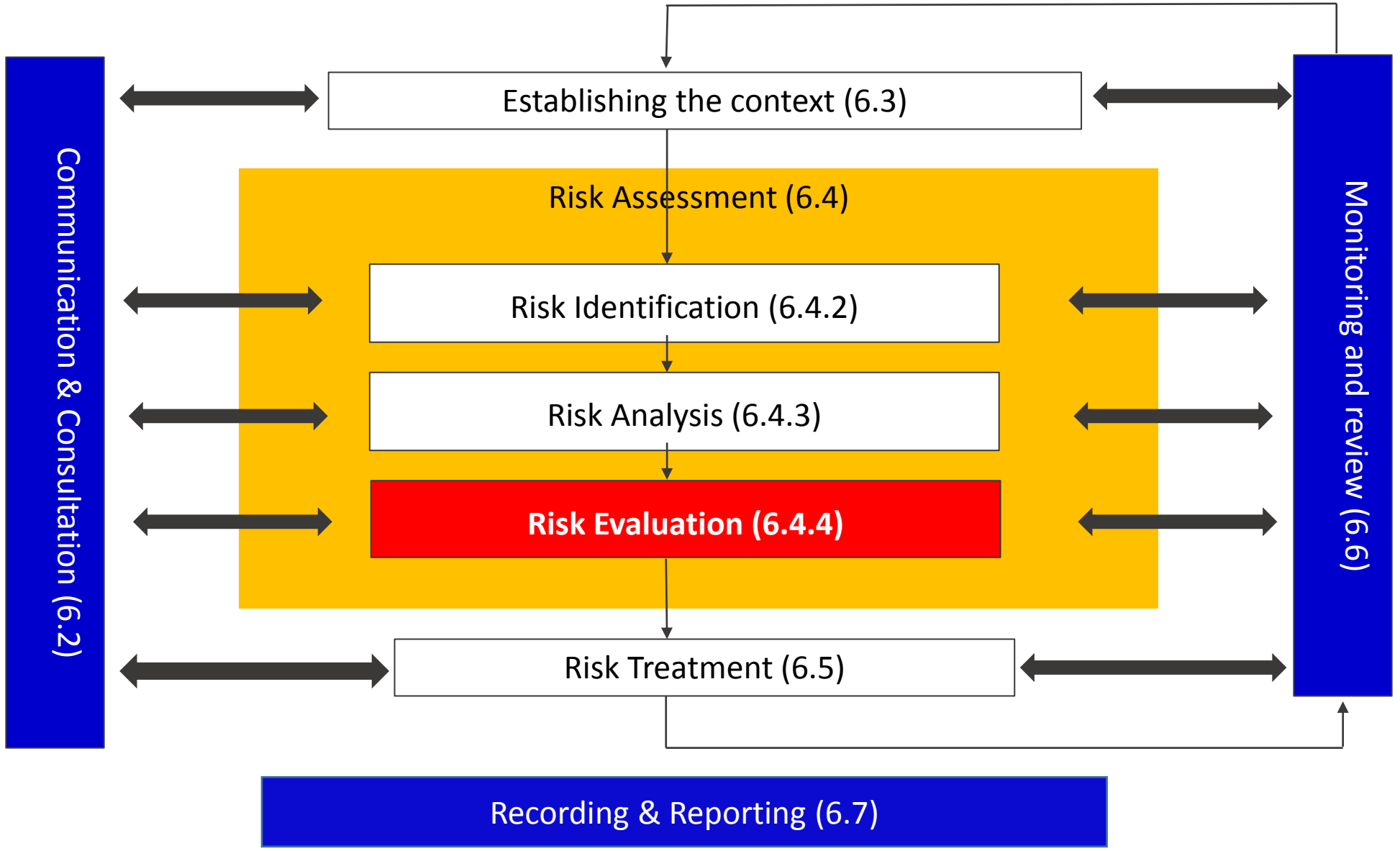
- Organization's or stakeholder's **readiness to bear the risk** after risk treatment in order to achieve its objectives

(Source: ISO 31000 (Guide 73)

- The **maximum amount of risk** that the company can bear despite controls

(Source : European Confederation on Institutes of Internal auditing ECIIA and Federation of European Risk Management Associations FERMA)

RISK MANAGEMENT PROCESS



Process Risk Management

Risk Analysis– Coming with a risk rating

Once the likelihood and impact of the risk have been established, we can then combine them to determine the level of risk. In arriving at this level, the risk rating matrix is used.

Level Of Likelihood	Level Of Impact				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Significant	Significant	High	High	Extreme
Likely	Moderate	Significant	Significant	High	High
Possible	Low	Moderate	Significant	High	High
Unlikely	Low	Low	Moderate	Significant	High
Rare	Low	Low	Moderate	Significant	Significant

Risk rating is calculated using the following formula

LIKELIHOOD × IMPACT

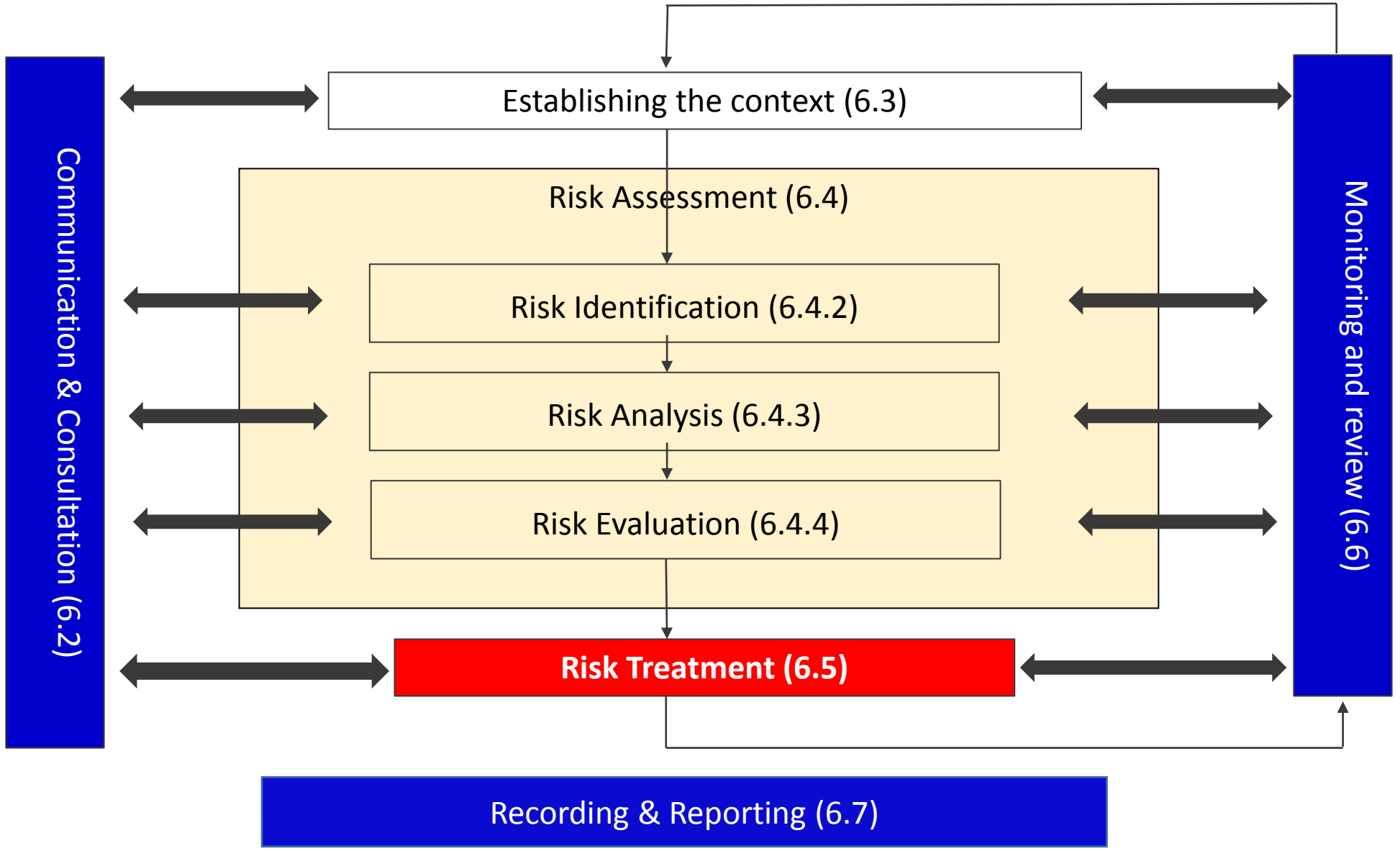
Example: UNLIKELY × MAJOR = SIGNIFICANT

RISK ACTION PLAN TABLE

RISK LEVEL	ACTION AND TIMESCALE
ACCEPTABLE **1-4**	No additional controls are required. Consideration may be given to a more cost effective solution or improvement that imposes no additional cost burden. Monitoring is required to ensure that the controls are maintained.
MODERATE **5-12**	Efforts should be made to reduce the risk, but the costs or prevention should be carefully measured and limited. Risk reduction measures should be implemented within a defined time period. Where the moderate risk is associated with extremely harmful consequences, further assessment may be necessary to establish more precisely the likelihood of harm as a basis for determining the need for improved control measures.
UNACCEPTABLE **15-25**	Work should not be started or continued until the risk has been reduced. If it is possible to reduce risk even with unlimited resources, work has to remain prohibited

Risk Treatment

RISK MANAGEMENT PROCESS



ULTIMATELY, WE NEED TO DECIDE WHETHER…

RISK TREATMENT

AVOID	REDUCE	TRANSFER	ACCEPT
• **not taking or continuing** the activities	• Likelihood and Impact by training, testing, control, improve the management system.	• Involves **another party** to share in whole or in part through contracts, insurance, MOU.	• Identified risks **can not be eliminated** or avoided or no treatment process that can be done.

TRANSFER AND AVOID THE RISK

- When the **likelihood of a risk** is **low** but the **consequences is high**, the organization will wish to **transfer** that risk.

- When a risk is **both of high** likelihood and high **consequences**, the organization will wish to **avoid or eliminate** the risk.

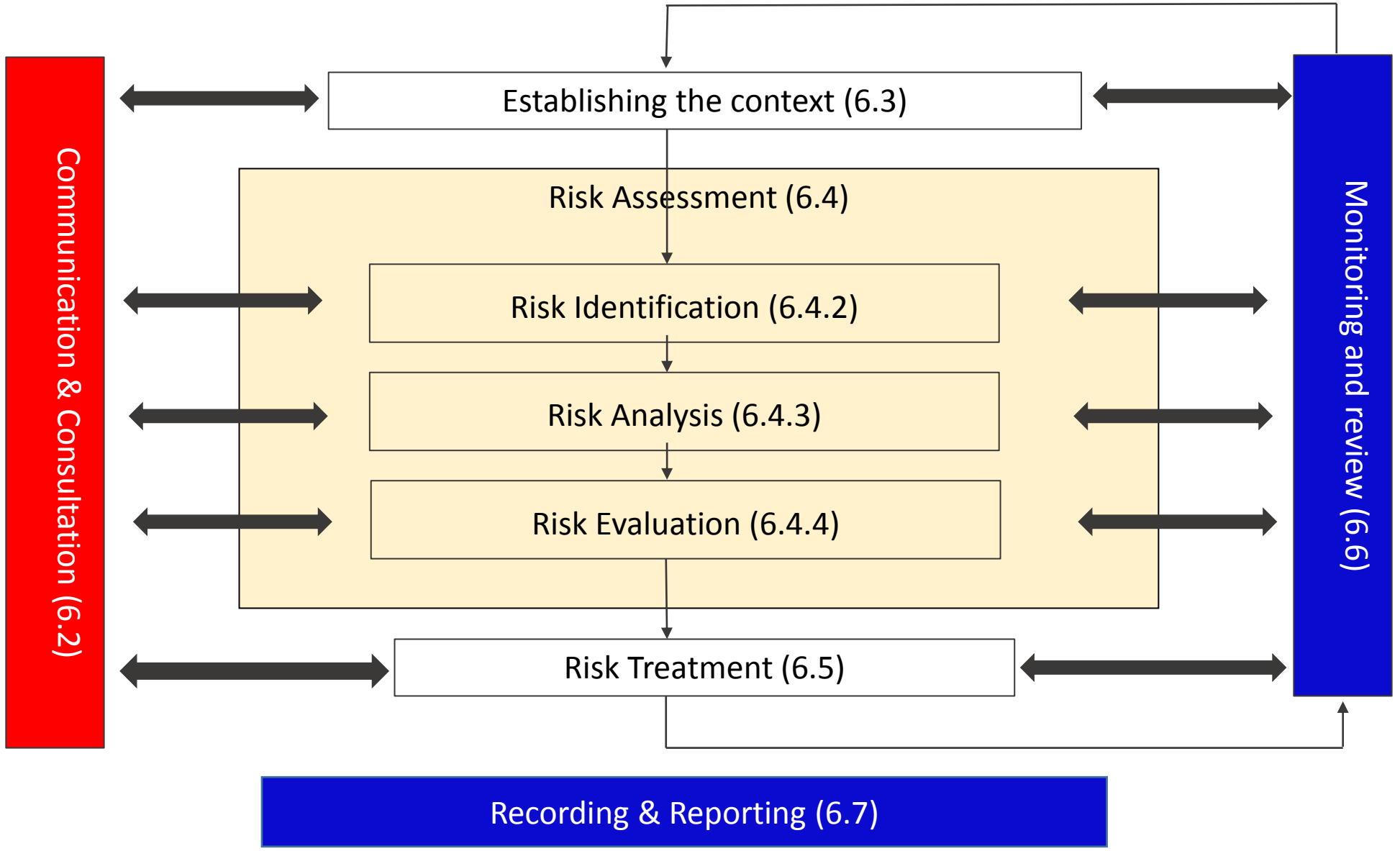
ACCEPT AND REDUCE THE RISK

- When the risk is considered to be **within the risk appetite** of the organization, the organization will **accept** that risk.

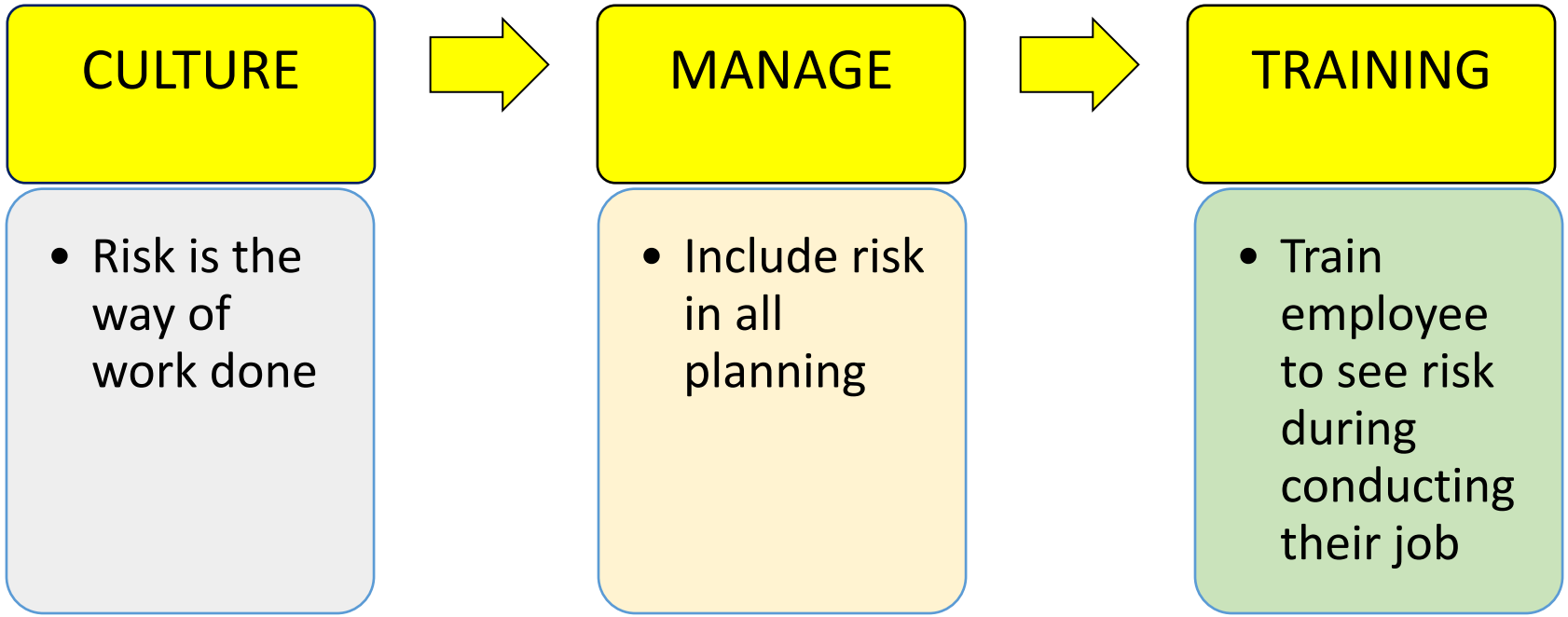
- When the level of **risk exposure** (likelihood) is **high** but the **potential loss (impact)** associated with it is **low**, the organization will wish to treat to **reduce** the risk.

Communication, Monitoring & Review

RISK MANAGEMENT PROCESS



DEVELOPMENT OF RISK MANAGEMENT CULTURE

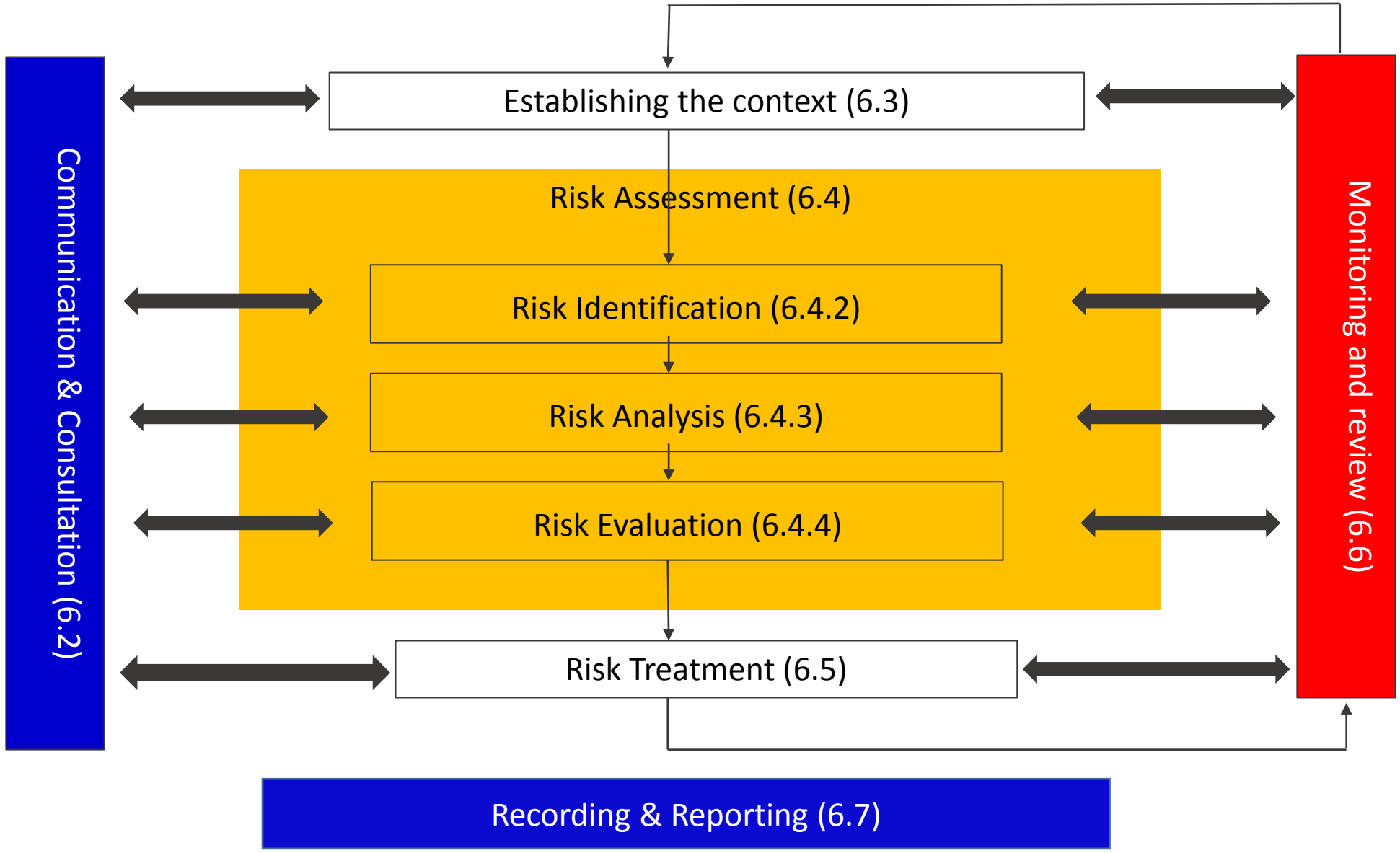


COMMUNICATION AND REPORTING

RISK LEVEL	COMMUNICATION
Critical	• Notify to top management • Immediate action to be taken
High	• Notify to top management • Refer to strategic planner
Medium	• Action to be taken without notifying to top management
Low	• Accept risk but need monitoring

85

RISK MANAGEMENT PROCESS



MONITORING & REVIEW

Always monitoring and conduct strategy evaluation as the context or risk may change or other factors that might arise such as:

1) New risks
2) Existing risk assessment result might be change
3) The risk may be lost
4) Treatment may not be effective

MONITORING & REVIEW

Effectiveness	Details
Excellent	Monitoring conducted at planned interval, audit and review has been conducted to measure the effectiveness of the system.
Good	Monitoring conducted. Action has been taken
Moderate	Monitoring conducted but no action taken
Weak	No monitoring been done

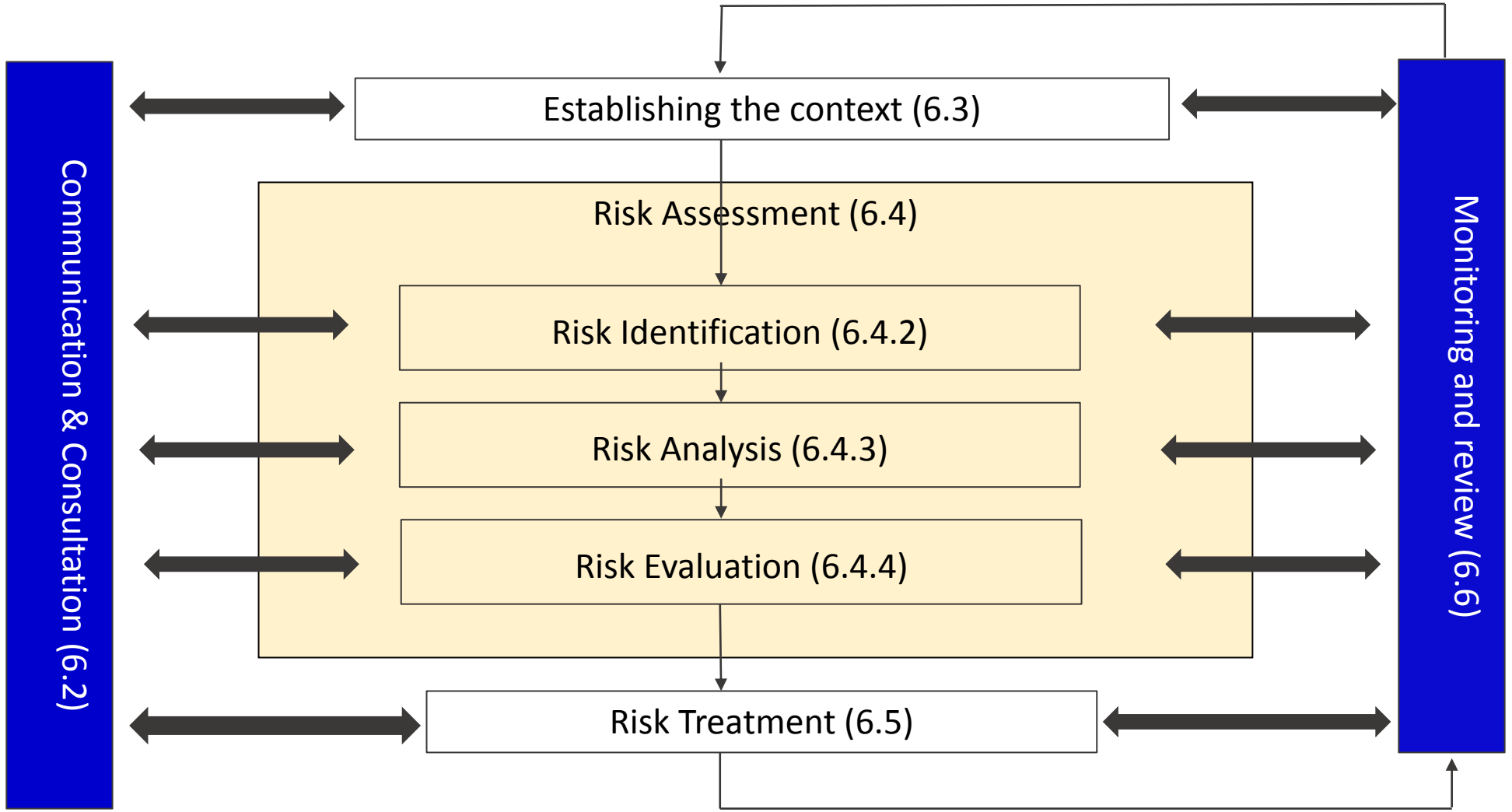
AUDIT

- See the involvement of management
- See the methodology used
- See the members of the group involved
- See what kind of risks are taken into account
- See how the marks given
- View the data used
- See Actions treatment
- See follow-up actions

EFFECTIVE RISK MANAGEMENT

- Maintain global perspective
- Initiate open communication
- Integration of Risk Management in daily operation
- Continual improvement in risk management
- Team cooperation
- To avoid loss business / profit / company image

RISK MANAGEMENT PROCESS



Recording & Reporting (6.7)

Thank you

sarimah@sirim.my
Tel 03-55446237
H/P :012-2348594