

# **Risk Management in Projects.**

(The Art of Saving Time, Money, and Creating Value)



**Nairobi, March 2020**



# House Keeping

- Facilities
- Planned Fire alarms/drills
- Planned Breaks
- Health & Safety Moment



# Lead Tutor



**Cass Business School**  
CITY UNIVERSITY LONDON



**Glasgow Caledonian University**  
Glasgow School for Business and Society



Leading the risk profession



- Actuarial Training: BSc & PGD
- Masters in Enterprise Risk Management: MSc
- Certified Fellow & Former Director: Institute of Risk Management (IRM) UK
- Chartered Insurer UK : ACII (UK)
- Specialty: Enterprise Risk, Reward, Strategy & Performance Management
- Professional Awards: The UK Risk Manager of the Year 2009/10; EU Strategic Risk Awards 2007 & 08
- Certified Risk trainer - IRM & Chartered Insurance Institute (CII) UK
- Chief Risk Officer (CRO) - Public, Private , Financial Services, Health Sector & Oil and Gas
- PhD – Risk Management, Leadership and Performance Outcomes





**5 mins**

# Introduction & Ice Breaker

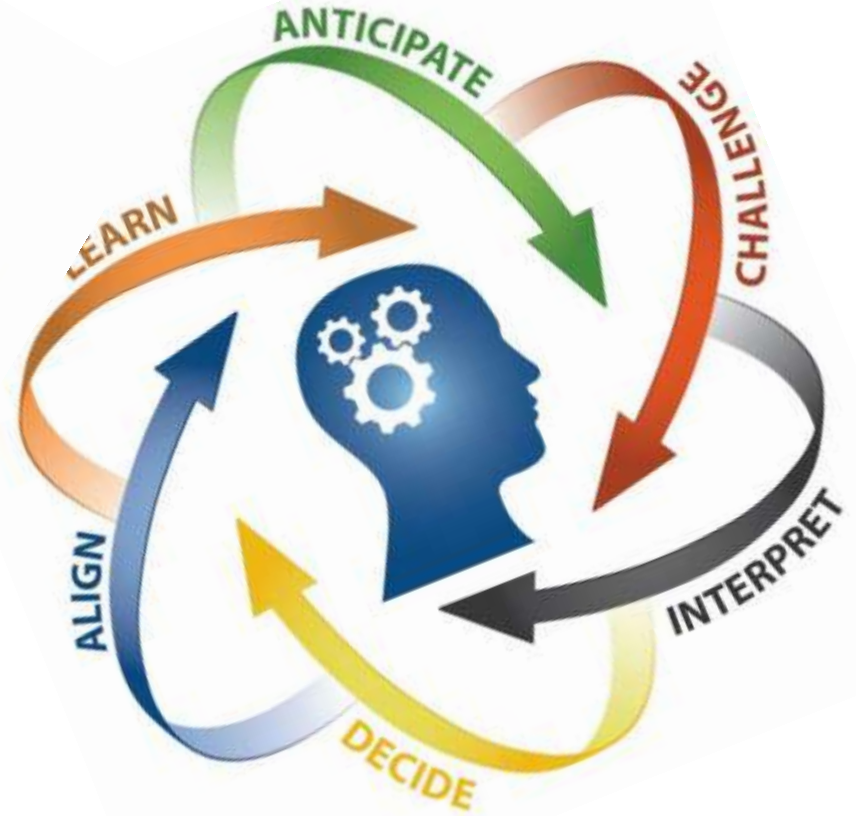
Get up and pair up with someone in the room who you've not met before or don't know very well

Find out:

- Who they are, and their role
  - What their experience is of risk management
  - What their objectives are for the session
- 
- Take it in turns to introduce your new acquaintance to the group



# Learning Agenda



# Introduction

Habits of highly effective people.



- They take initiative. (“Be Proactive”)
- They focus on goals. (“Begin with the End in Mind”)
- They set priorities. (“Put First Things First”)
- They only win when others win. (“Think Win/Win”)
- They communicate. (“Seek First to Understand, Then to Be Understood”)
- They cooperate. (“Synergize”)
- They reflect on and repair their deficiencies. (“Sharpen the Saw”)
- They find their voice and help others find theirs.

*Based on the work of Stephen Covey: The seven habits of highly effective people - The 8th habit*

# Day 1: Session 1



## Introduction - Project Management

- What is a project? What is a programme?
- Project types; Criteria to define project type
- Principles of good project management
- Designing structures to fit the project;
- Governance - roles and responsibilities

# What is a Project/Programme ?



“Unique process consisting of a set of coordinated and controlled activities with start and finish dates, undertaken to achieve an objective conforming to specific requirements, including constraints of time, cost, quality and resources”

- A Project is a planned set of activities
- A Project has a scope
- A Project has time, cost, quality and resource constraints



# What is...



A project consists of a temporary endeavour undertaken to create a unique product, service or result. Another definition is a management environment that is created for the purpose of delivering one or more business products according to a specified business case....

**“Projects deliver outputs, discrete parcels or "chunks" of change”**

A program is a group of related projects managed in a coordinated manner to obtain benefits and control NOT available from managing them individually.

**“Programs create outcomes”**



# Characteristics of a Project

- A finite and defined lifecycle, i.e. a clear start and an end
- Defined and measurable business products
- A corresponding set of activities to create (and quality check) the business products
- A defined amount of resources, e.g. cash, people, equipment
- An organisation structure, with defined responsibilities, to manage the project
- Is unique
- Loads of risks



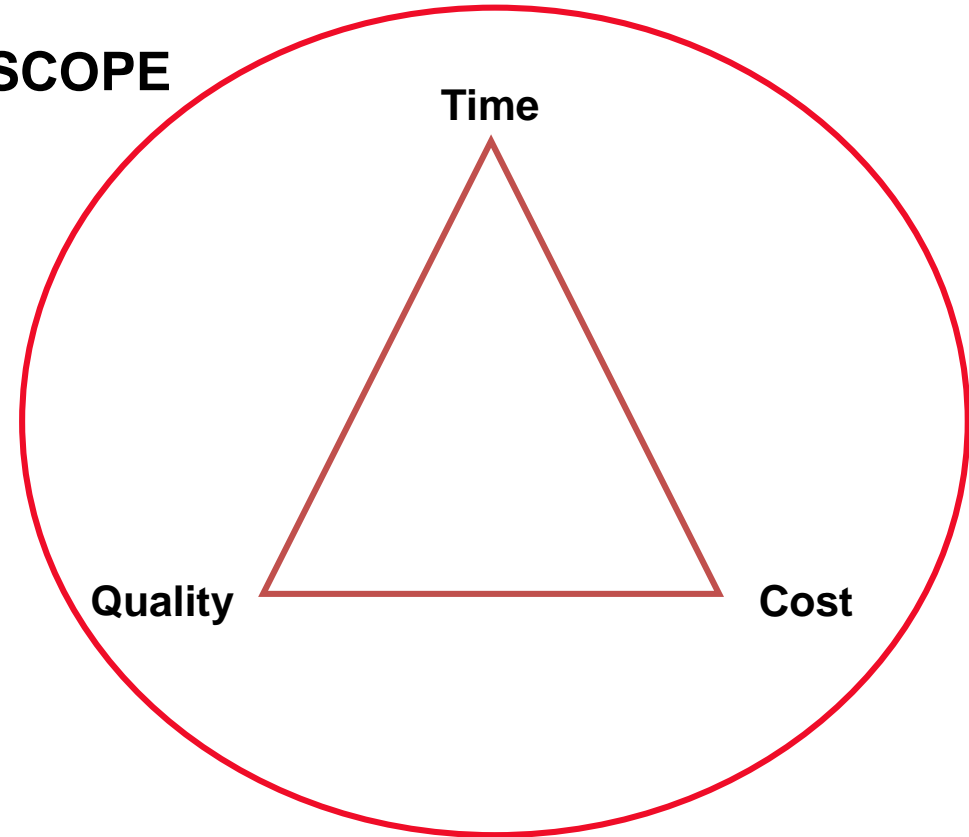
# Every project has a...



## Types of Projects:

- Manufacturing Projects
- Construction Projects
- Management Projects
- Research Projects

**SCOPE**



Increased **Scope** = increased time + increased cost

Tight **Time** = increased costs + reduced scope

Tight **Budget** = increased time + reduced scope.



# Common Problem Areas

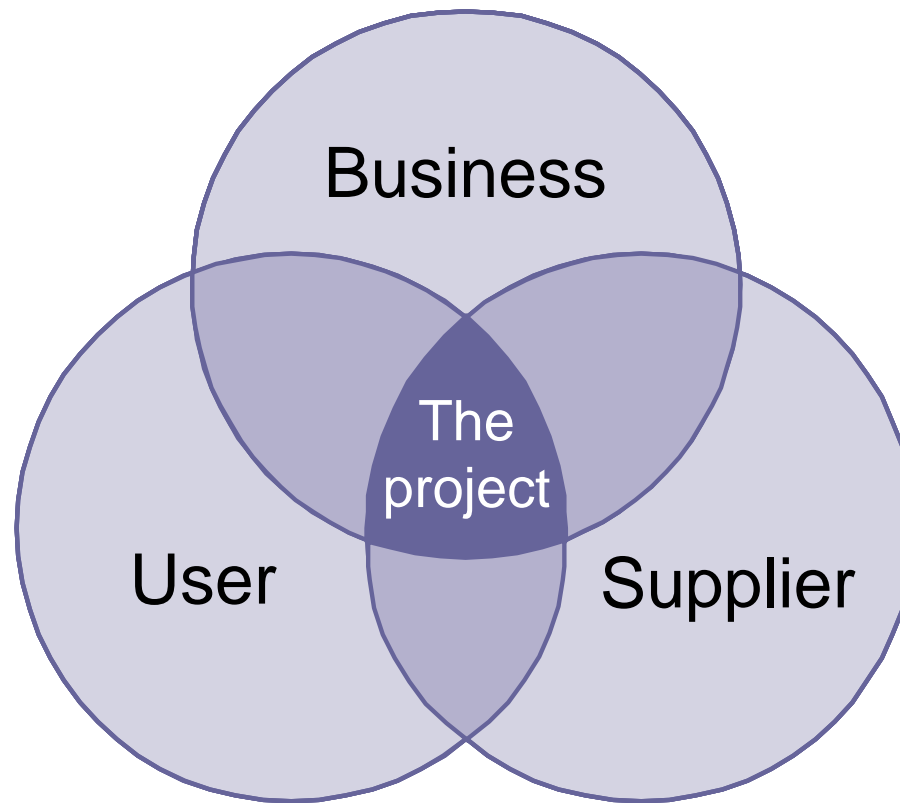
- Lack of clear objectives
  - Little or no customer/user involvement
  - Required deliverables not fully described
  - Poor management of changes
  - Too few resources
- 
- No effective project plan
  - Inability to track progress effectively
  - Poor communication
  - Lack of buy-in/commitment
  - **Poor Risk Management**





# The Project Organisation...

The 3 main areas of any project which must be satisfied if a project is to be successful



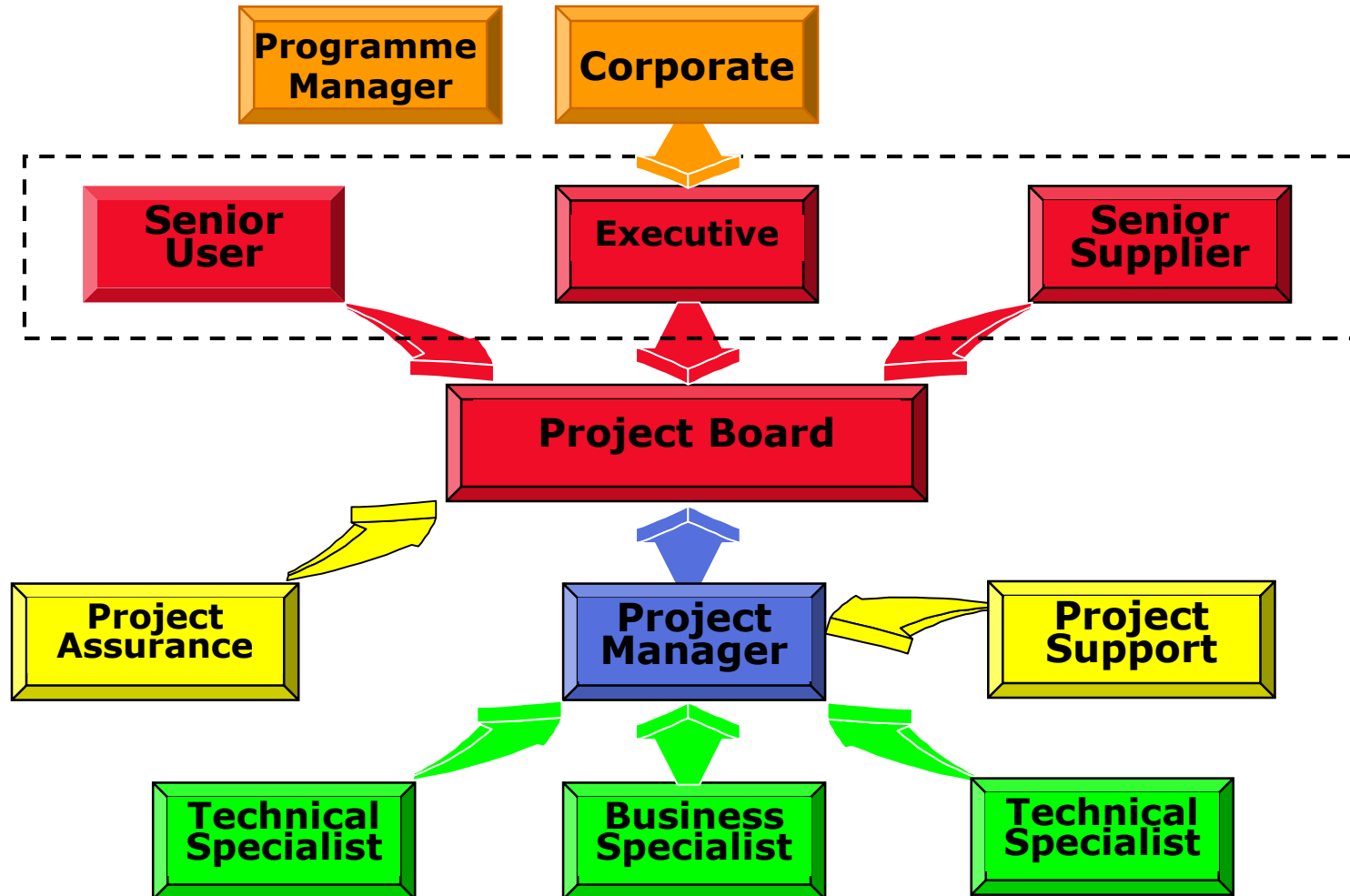
# Project Governance...



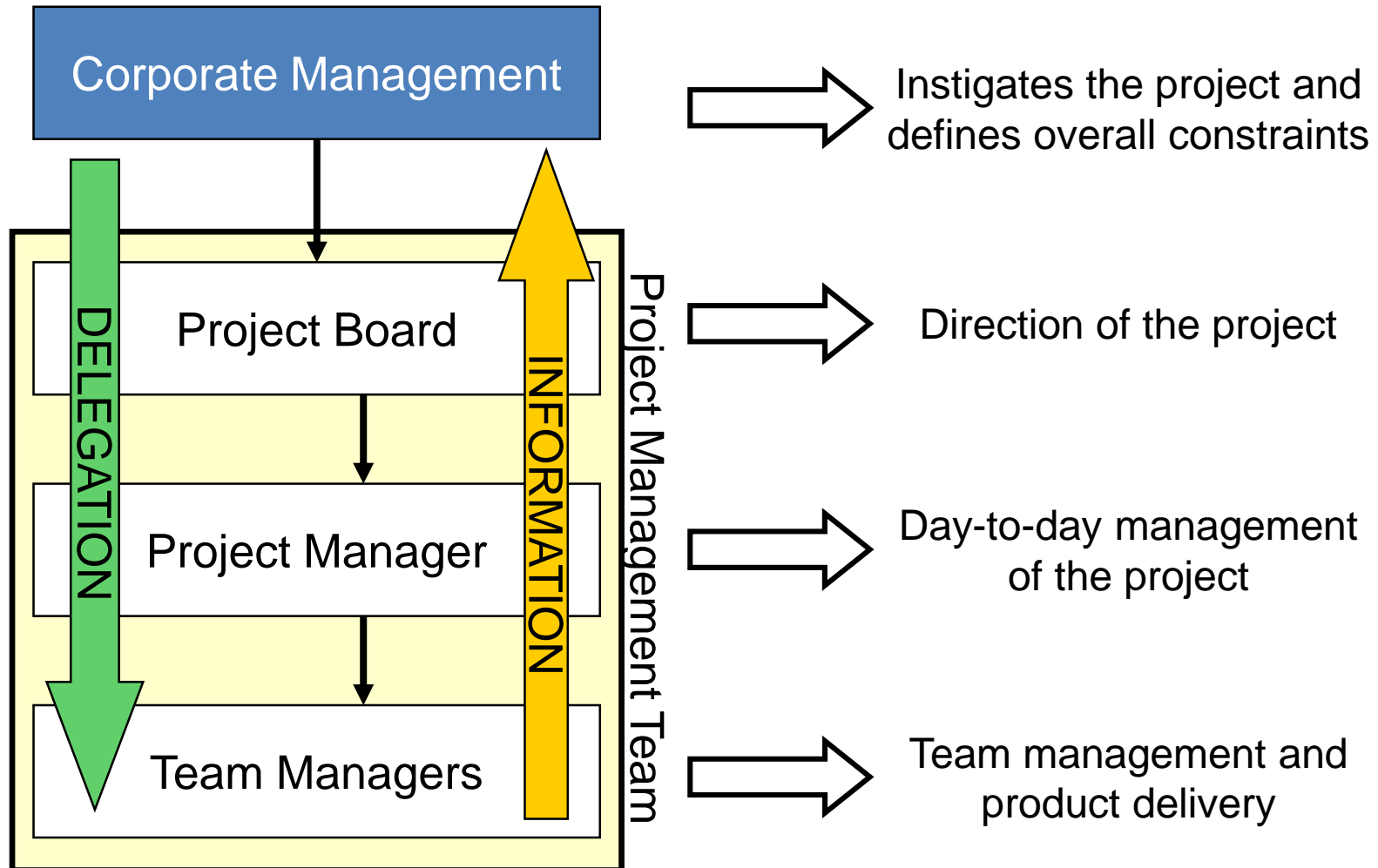
- How do you determine who owns the project ?
- How do you determine who drives the project ?
- How do you determine who the team members are ?
  
- Project team is made up of two parts
  - The authority part
  - The members who do the work

“The purpose of the Governance Structure is to define and establish the project’s structure of accountability and responsibilities”

# Risk Roles and Responsibilities



# 4 Management Levels





# Day 1: Session 2



## Project Management (Recap)

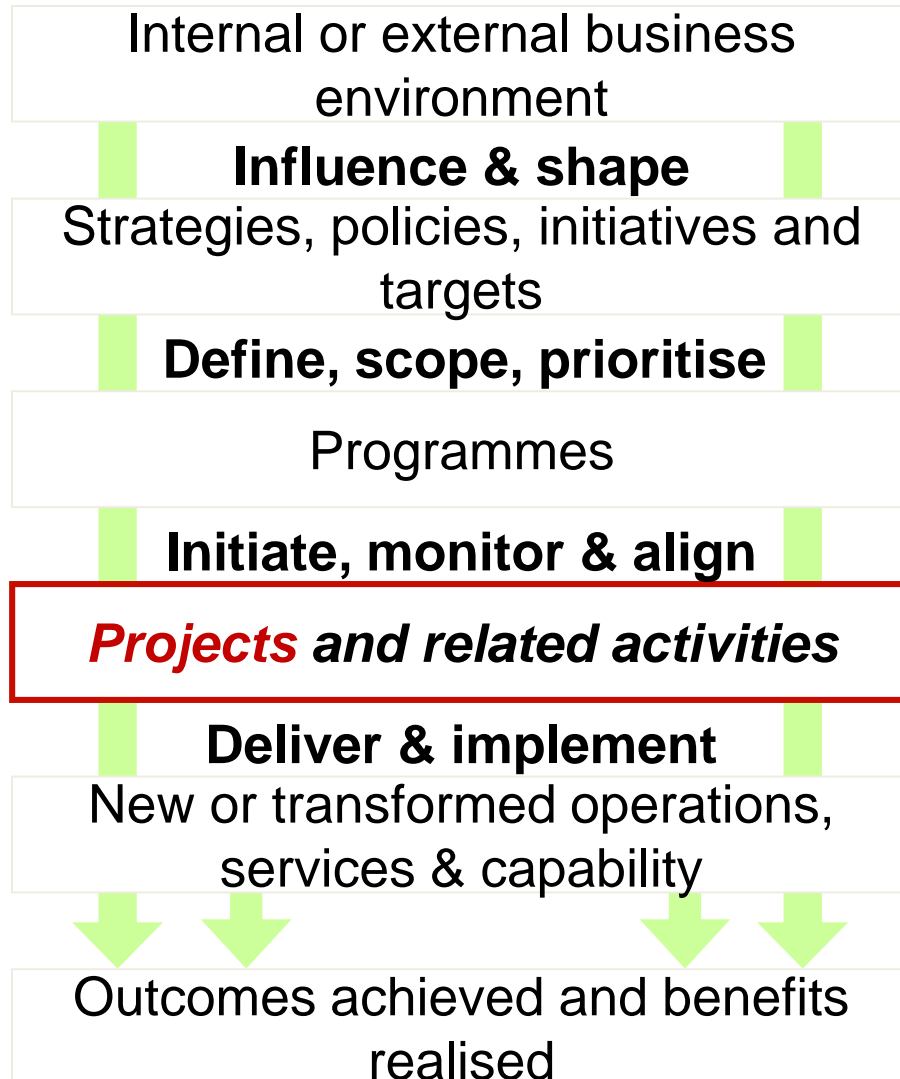
- Project lifecycle and validation;
- Project Design; Implementation, and benefit realization
- Types of project reports; team building and team working
- Close out and close down
- Post Implementation reviews – business learning

# Key Components of a Project



- Business Case
- Project Organisation
- Planning
- Controls
- Risk and Issue Management
- Quality Management
- Change Control
- Stakeholder Management

# Project Management Environment



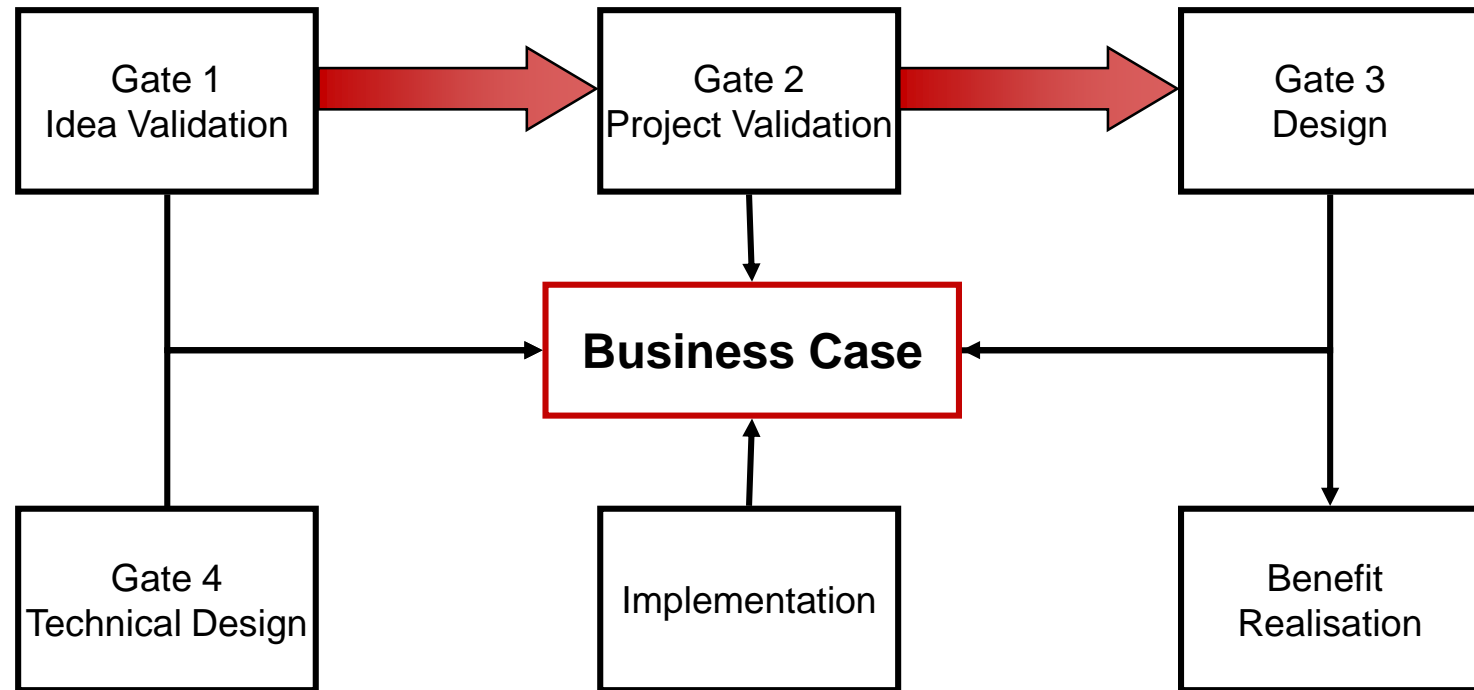
## Considerations:

- Resources
- Impact of change
- Inter-dependencies
- Order and sequence
- Risk

# Project Life Cycle



A living document...



- Focus should be on the totality of business change
- If a satisfactory Business Case does not exist, the project should not be started
- If justification for the project disappears, the project should be stopped





# Idea Validation

- Justification of whether an idea is a viable project
- Provide a baseline against which the future viability of the project can be assessed
- Purpose
  - Why the project is worthwhile and what is intended to achieve
- Where the initial idea is first defined i.e. from
  - Management board meeting
  - Strategic/business planning
  - Team level workshop

# Project Validation

- Develop the idea into a fully viable project to allow decision makers to proceed
- More research into the Business Case with supporting evidence that goals are SMART

(Specific, Measurable, Achievable, Realistic, Timely)



# Project Design

- Design of the Project Deliverables
- Impact on resources
  - Finance
  - People
  - Processes

## Technical Design

- Normally applicable where External Contractors or Service Providers
- Normal Procurement and formal tendering process will take place

## Implementation

- Mobilisation of resources to start the work
- For change projects the roll out of new systems, services or restructuring etc

## Outputs

- Progress Reports
- Product

## Benefit Realisation

- Benefit Realisation Plan defines how and when a measurement of the achievement of the project benefits can be made
  - The handover process to the end user
  - The closure of the project
  - The tracking of benefits
  - The benefits profile

# Project Life Cycle





How the customer explained it



How the Project Leader understood it



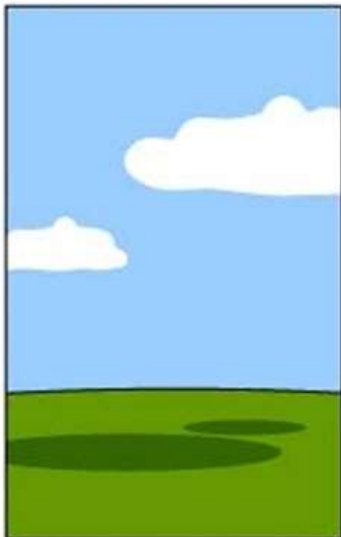
How the Analyst designed it



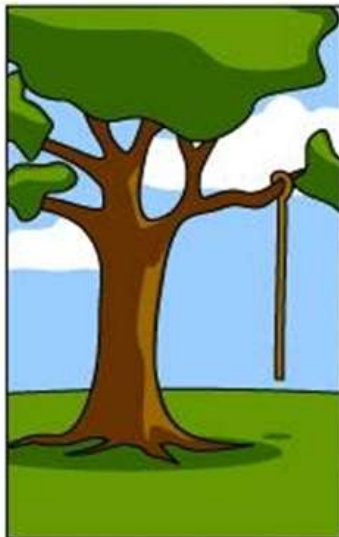
How the Programmer wrote it



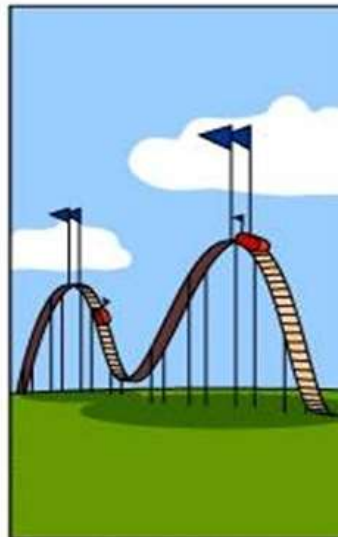
How the Business Consultant described it



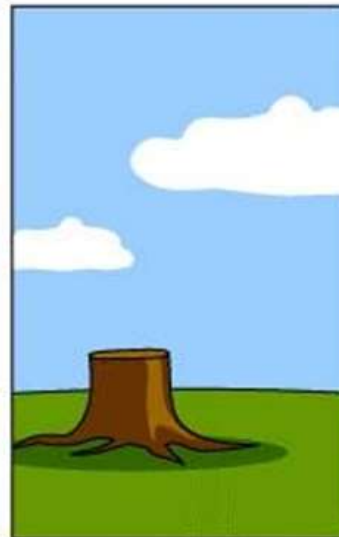
How the project was documented



What operations installed



How the customer was billed



How it was supported



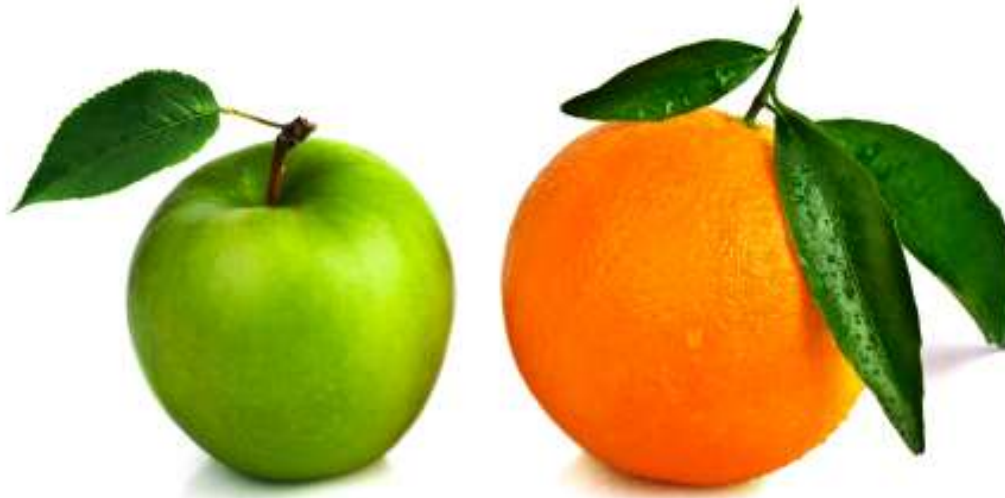
What the customer really needed





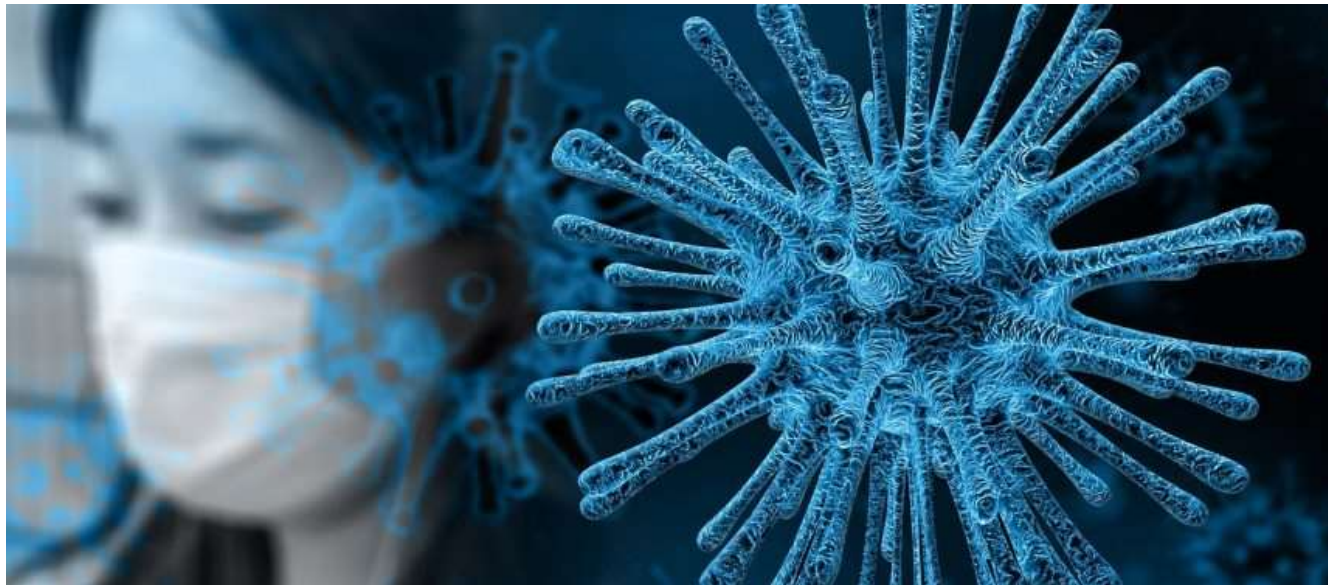
# Day 1: Session 3

Introductions, key principles & definitions



- Strategy, Goals and Objectives
- Why performance measurement and management?
- Governance - Roles & Responsibilities
- What is risk and why manage risk?
- Risk management principles
- Attributes of effective risk management

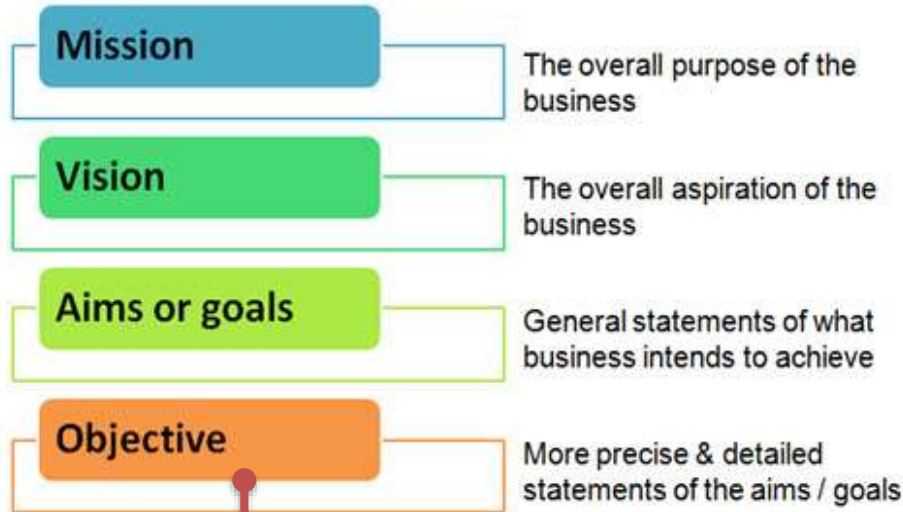
# Recent Issues





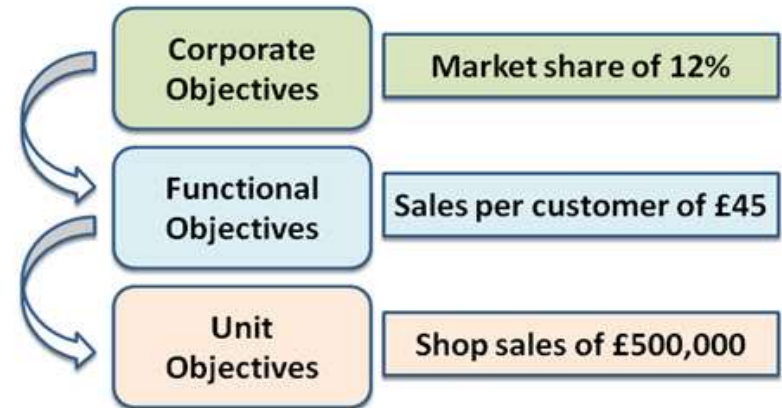
# Introduction

## Goals & Objectives



“Objectives are statements of specific outcomes that are to be achieved”

Issues, Problems vs.  
Performance



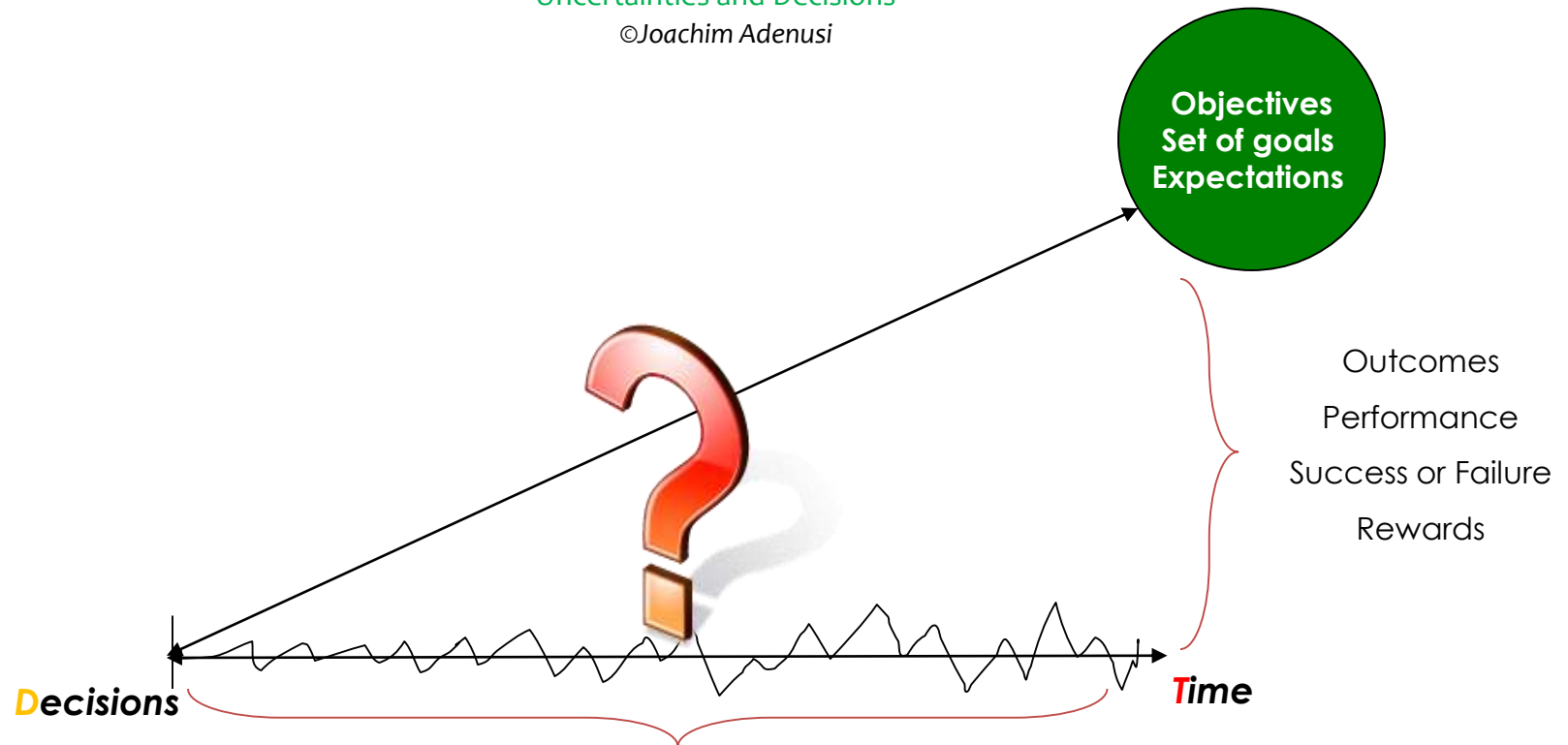
“The trouble with not having a goal is that you can spend your life running up and down the field and never score.” – Bill Copeland



# Dot principle

Uncertainties and Decisions

©Joachim Adenusi



“**Decisions** + **Objectives** + **Time** (Dot) = Uncertainties ”

©Joachim Adenusi

*“Even a correct decision is wrong when it is taken too late” - Lee Lacocca*



# Introduction

Performance Measurement and Management

- What is performance?
- Performance Management?
- Performance Measurement?
- Effectiveness and efficiency ?

Q

# What is governance?

A

The system by which organisations are directed and controlled.

Generic aspects of governance include:

- the rights and duties of owners/shareholders and other stakeholders
- how powers are shared and exercised by directors
- how the holders of power are held accountable for what they do





# Corporate Governance Principles

## 1 Accountability

Responsibility for one's own decisions and actions, and ensuring they can be explained and clarified.

## 2 Responsibility

Efficient performance of duties and to the best of one's abilities.

## 3 Equitable Treatment

Fair and equitable treatment of all stakeholders.

## 4 Transparency

Ensuring corporate operations can be examined and information is disclosed to relevant parties.

## 5 Vision to Create Long-term Value

Looking towards the future to create long-term added value and sustainable growth.

## 6 Ethics

Existence of business ethics and code of conduct.





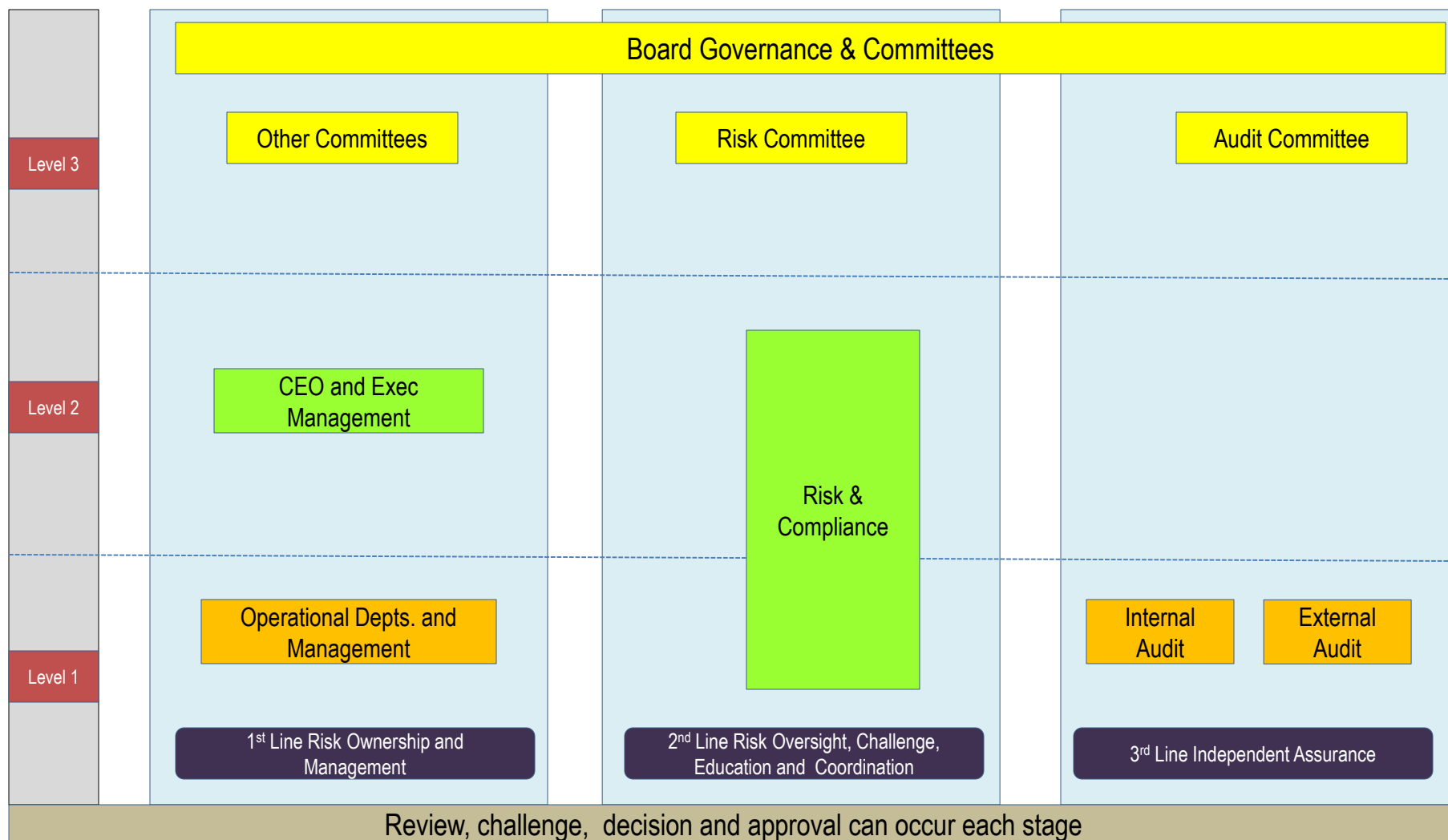


# Corporate Governance – Issues © IFC

- Risk 1: The Company and its shareholders have not demonstrated a commitment to implementing high quality CG policies and practices.
- Risk 2: The Board of Directors is not up to the task of overseeing the strategy, management and performance of the company.
- Risk 3: The Company's risk management and controls are insufficient to ensure sound stewardship of the company's assets and compliance with relevant regulations.
- Risk 4: The Company's financial disclosures are not relevant, faithful, and timely representation of its economic transactions and resources.
- Risk 5: The Company's minority shareholders' rights are inadequate or abused.



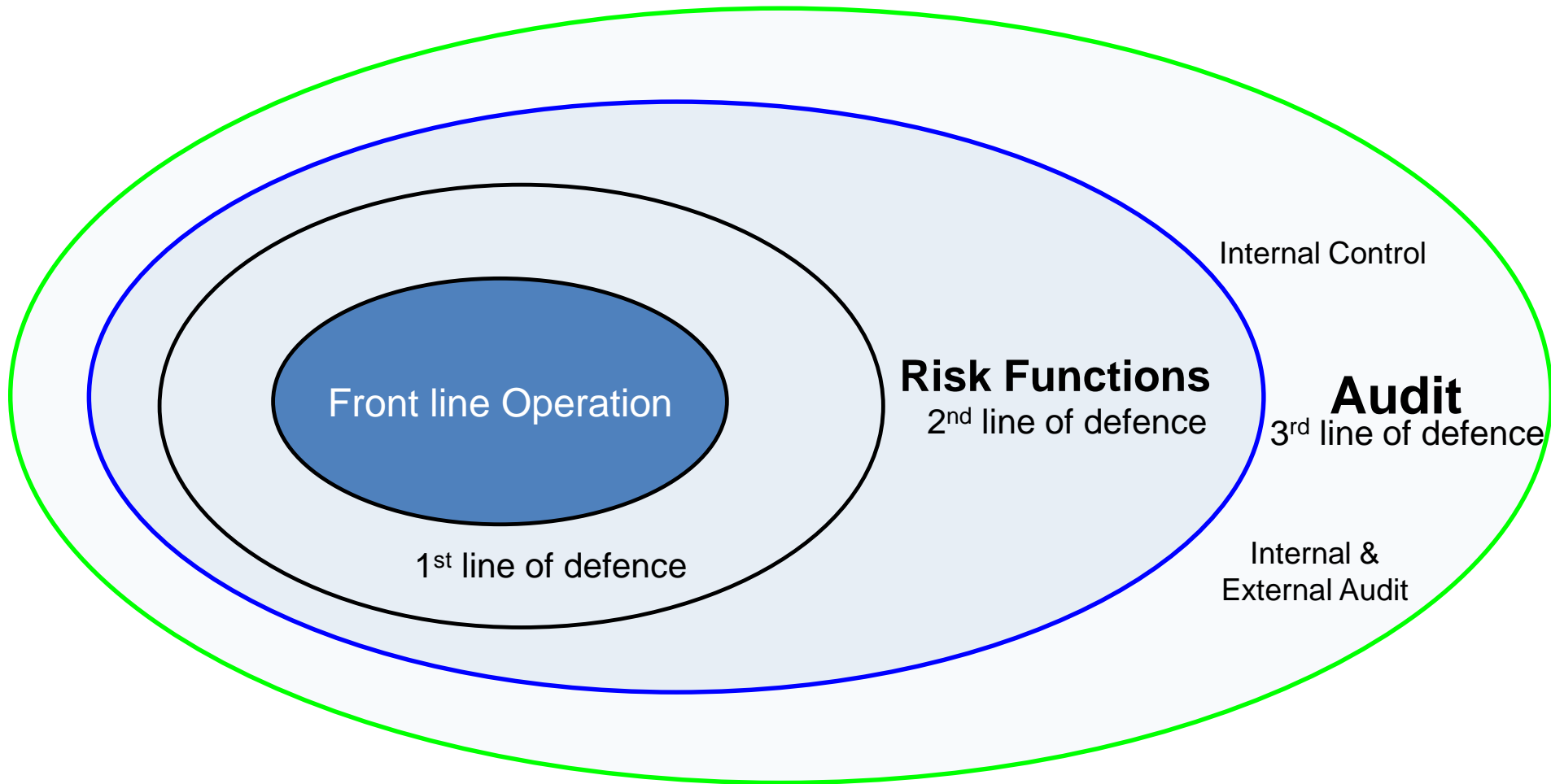
# Risk Governance...3 lines of defence



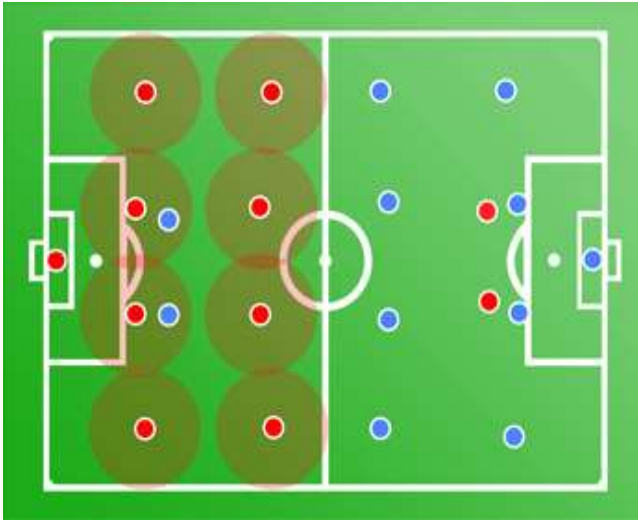
# Lines of defence



- The basis for a sound risk governance structure is a clear separation of roles



# Lines of defence



## First Line of Defence

Responsible for execution and decision making in line with the business objectives and strategy;

- Board
- Management Team
- Branches
- Staff

## Second Line of Defence

Responsible for independent oversight of risk taking activities and to quantify risks;

- The Risk Committee(RC)
- Chief Risk Officer (CRO)
- Risk Manager
- legal & Compliance

## Third Line of Defence

Responsible for giving independent assurance

- Audit (Internal & External)
- Internal Control



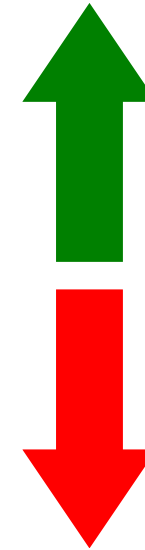
# Governance of an organisation



# What is risk and risk management?



“Effect of uncertainty on objectives”



Positive

Negative



Management is the process of reaching organizational goals by working with and through people and other organizational resources.



# What is the best definition of risk?

Organisation	Definition of risk
ISO Guide 73 ISO 31000	Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence
Institute of Risk Management (IRM)	Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative
COSO – ERM Integrated Framework	The possibility that an event will occur and adversely affect the achievements of objectives
From <i>old</i> AS/NZ 4360:2004	The chance of something happening that will have an impact on objectives





# Definitions of risk management

Organisation	Definition of risk management
ISO Guide 73 ISO 31000	Coordinated activities to direct and control an organisation with regard to risk
Institute of Risk Management (IRM)	Process which aims to help organisations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure
COSO – ERM Integrated Framework	A process affected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.



# Why manage risk?

- Achievement

- Safeguarding



What events can you recall that support the need for a structured and systematic approach to risk management?

# Risk Categorisation (Taxonomy)



Market risk

Liquidity risk

Group risk

Strategic risk



Insurance Risk

Credit risk

Operational risk

Reputational risk

## Why categorised risk?

Why?

Working through practical example...



# Risk Standards

- Australian New Zealand Risk Management Standard – AS/NZ 4360:1999, 2004, 2009
- A Risk Management Standard; Published by the UK AIRMIC, ALARM, IRM: 2002
- COSO Enterprise Risk Management -- Integrated Framework (2017)
- The UK Orange Book Management of Risk - Principles and Concepts (Government 2004)
- The UK Green Book – for programmes and projects
- Risk management. Code of practice BS 31100:2008, 2011 complying with ISO 31000
- ISO 31000:2018 provides principles and generic guidelines on risk management.
- Basel Banking Guidance – No integrated risk management guidance. Liquidity, Operational, Market, Electronic Banking, Capital Risks etc
- European Solvency II – Risk & Capital Management Requirements



# ISO 31000 – 2018 overview

Throughout the course we will use ISO 31000 as our core framework

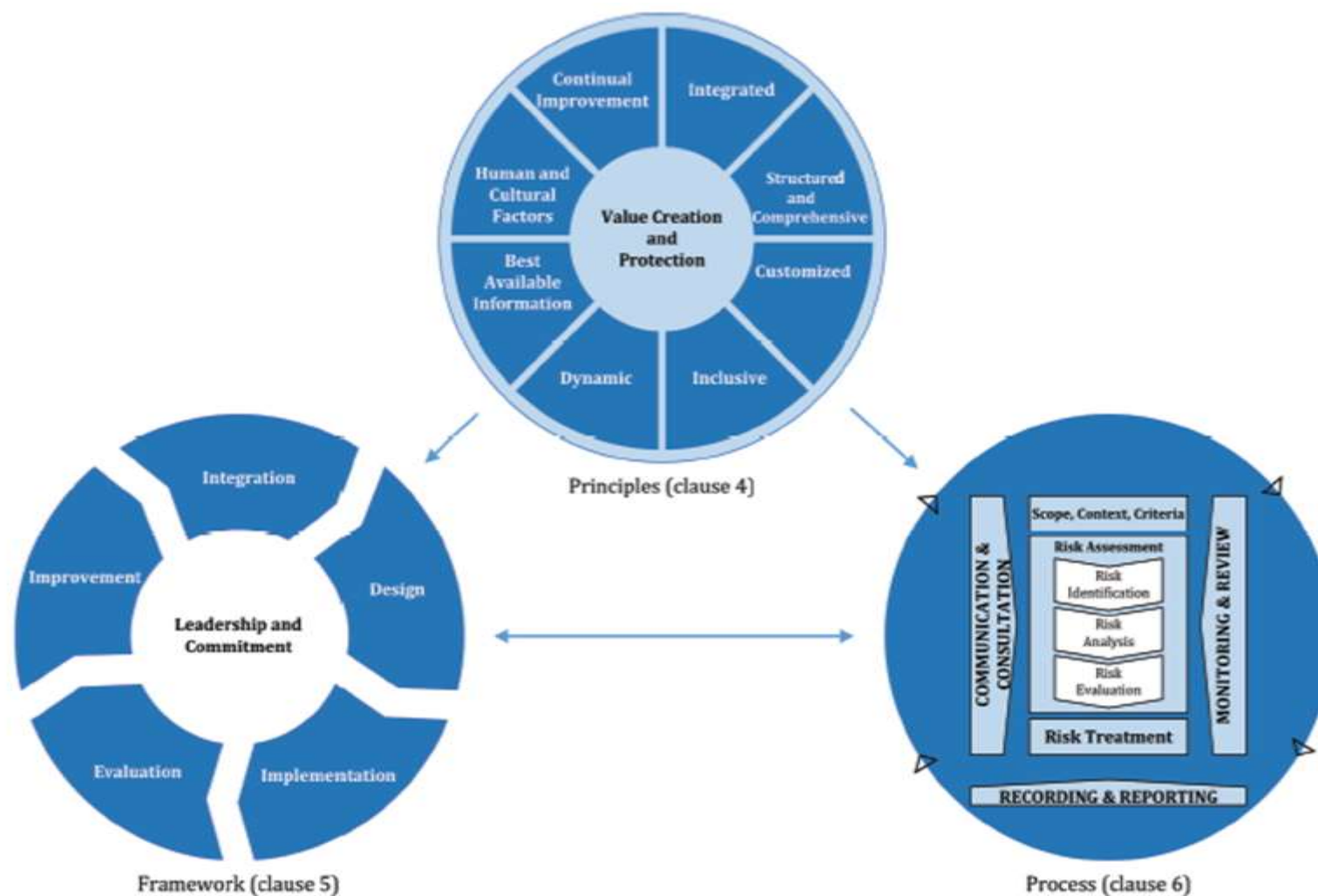
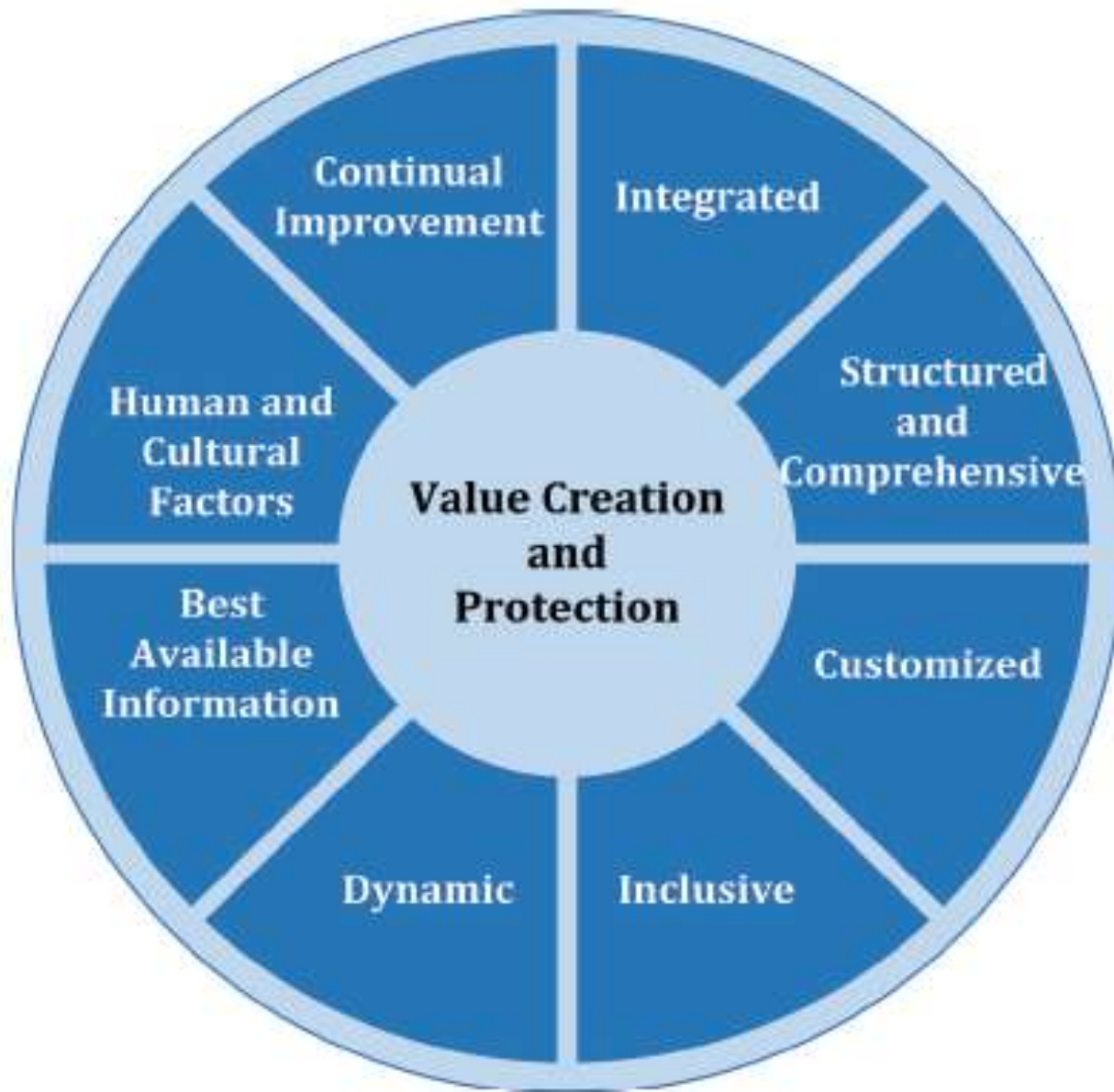


Figure 1 — Principles, framework and process



**Figure 2 — Principles**

# Designing a Risk Programme

## Risk Framework, Strategy, Policies and Process



**Figure 3 — Framework**



# What we know



## Risk



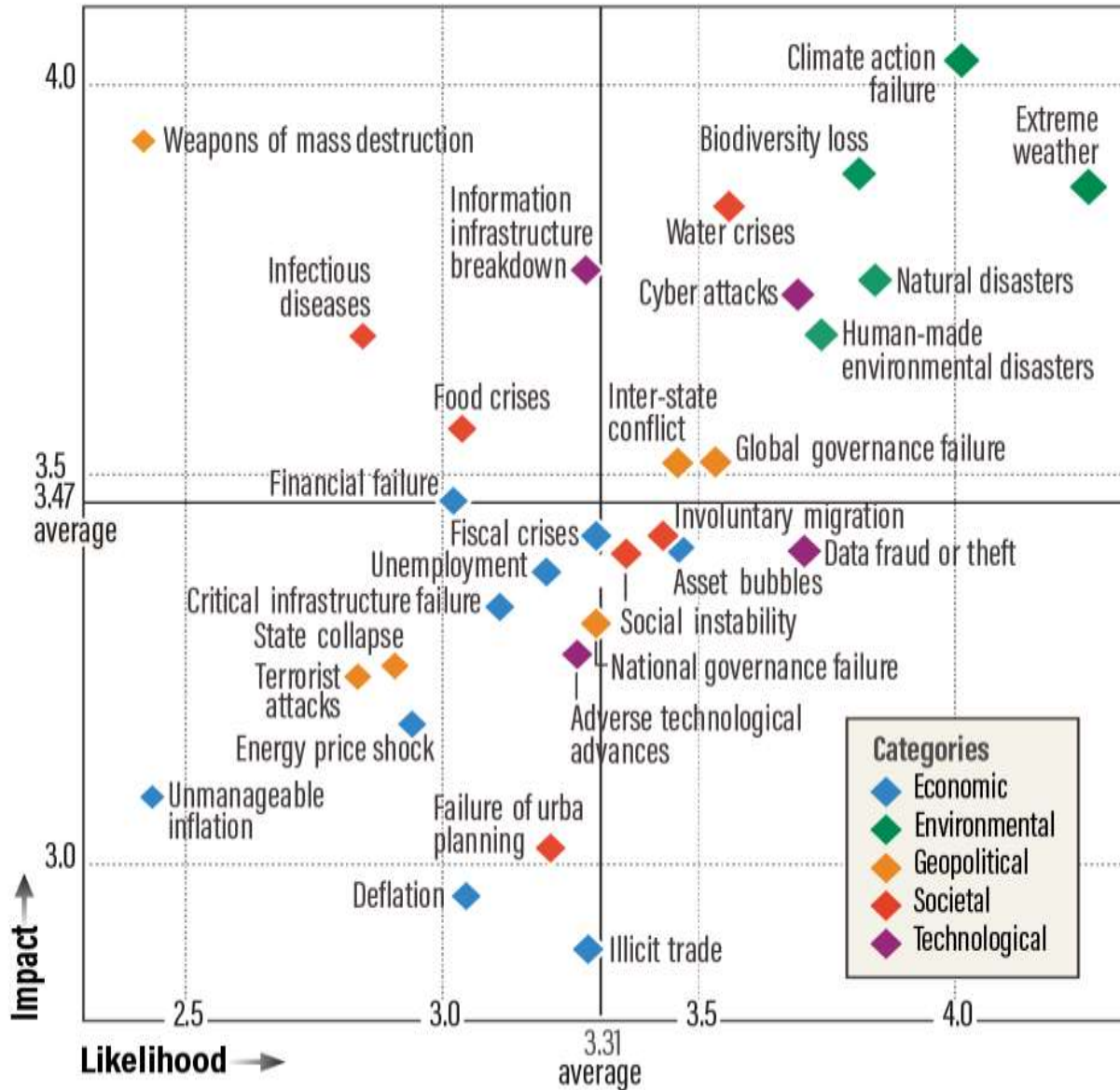
“Effect of uncertainty on objectives”

## Performance Management



a process by which managers and employees work together to plan, monitor and review an employee's work objectives and overall contribution to the organization.

# LONG-TERM GLOBAL RISKS LANDSCAPE (2020)



Source: Weforum.org

**Exercise:** 2020 Global Risk Report

# Risks in the news

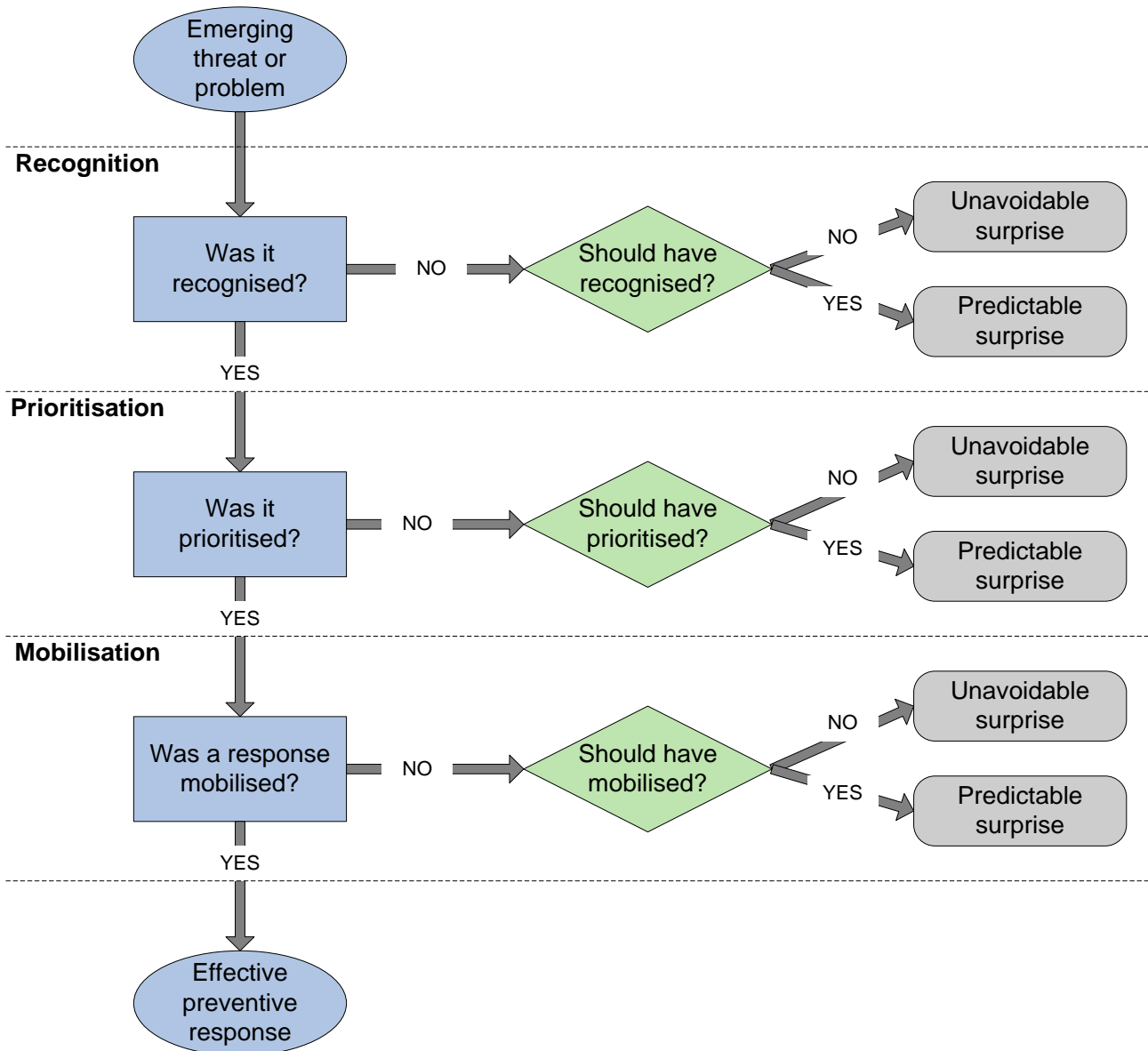


## Exercise:

What risks can you identify in today's media?

Which Sector? Who will it affect? Who should know about it? Why it is important? What could be done and when (how soon)?

# Does foresight make a difference?



Consider the list of disasters identified.  
Was this a failure of:

- prediction?
- prioritisation?
- mobilising resources?

Harvard Business Review, March 2003



# Break

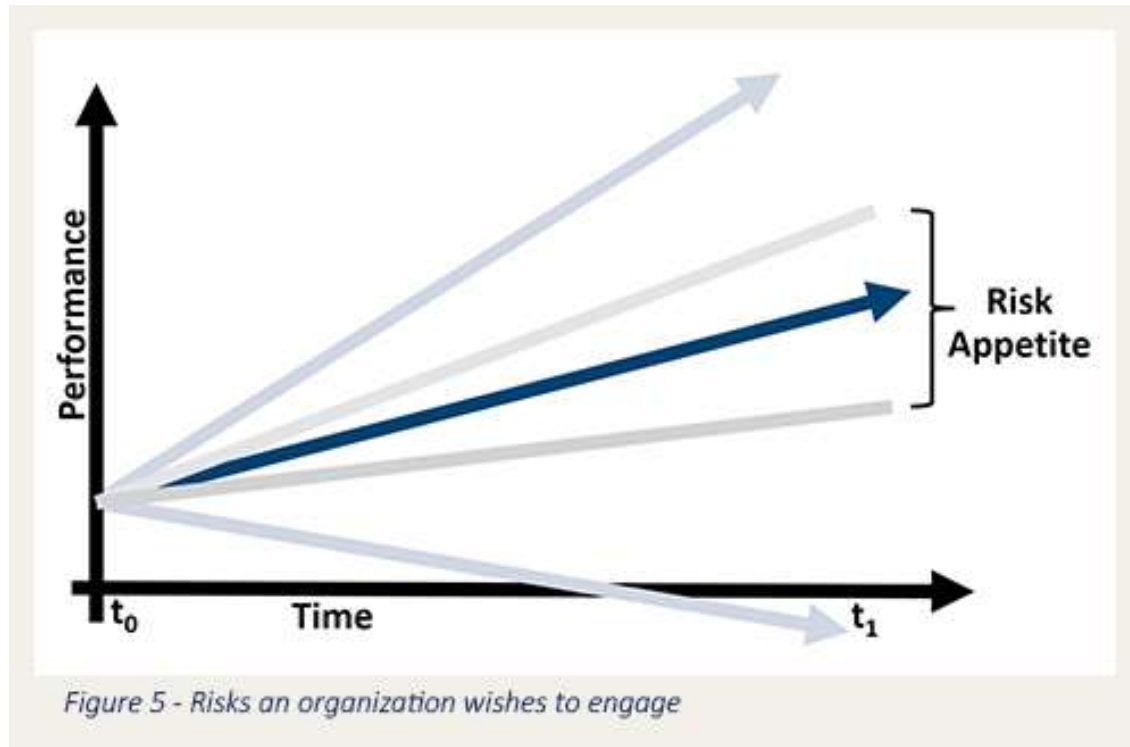


# Tea Break...!



# Day 1: Session 4

## Risk Appetite & Strategic Plans

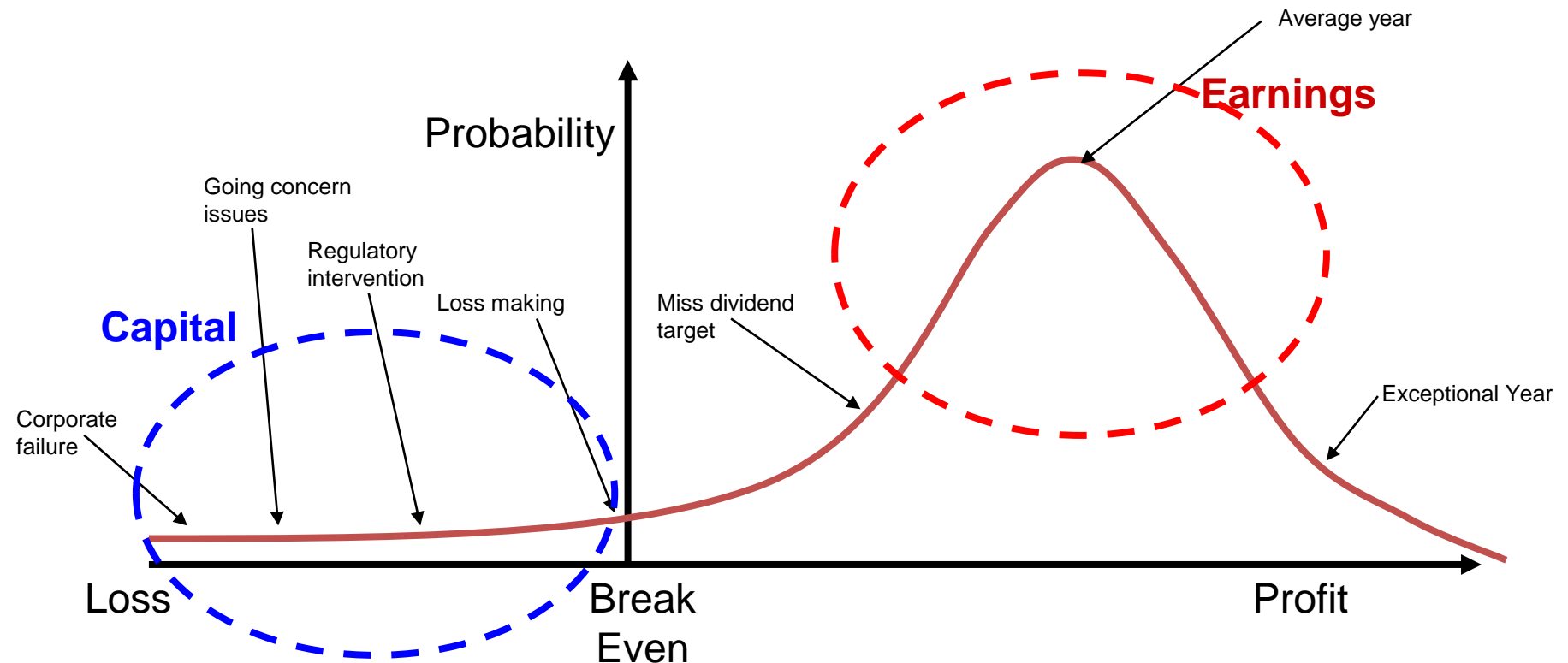


- Risk Appetite: importance & uses
- Practical application: Risk Statements, limits/tolerances
- Emending risk appetite: KPIs, KRIs and KCIs
- Using risk to drive performance and appraisals (Rewards)



# Earnings vs. Capital

- Earnings – focused on what we expect to happen
- Capital – focused on extreme downside



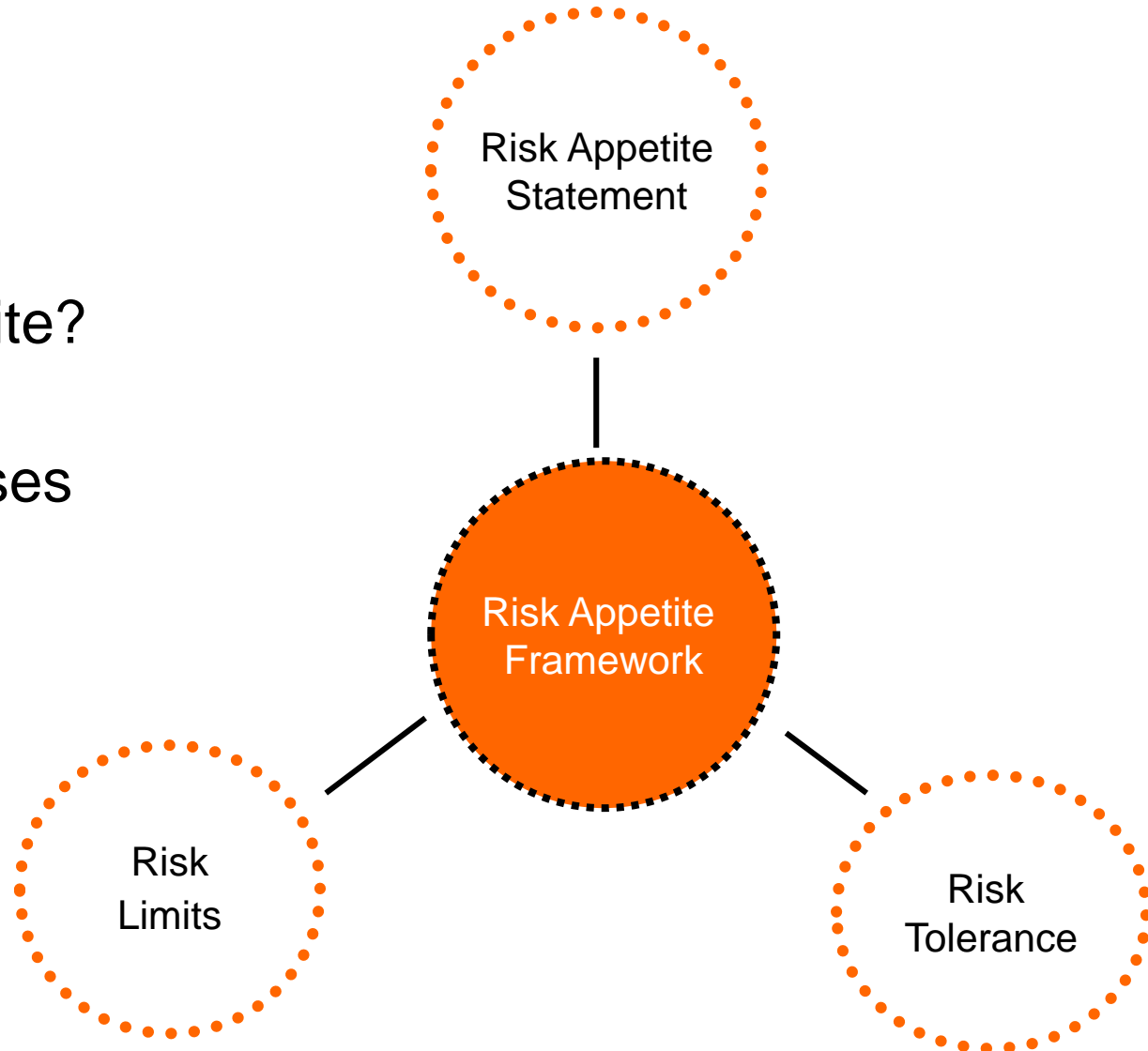


# Risk Appetite: importance & uses



What is Risk Appetite?

Importance and Uses



# Purpose of RA statements



Clarity for investors  
and stakeholders

Alignment of teams to  
risk strategy

Clear goals for staff and  
management

Regulation

Embedding the  
business strategy

Forward looking

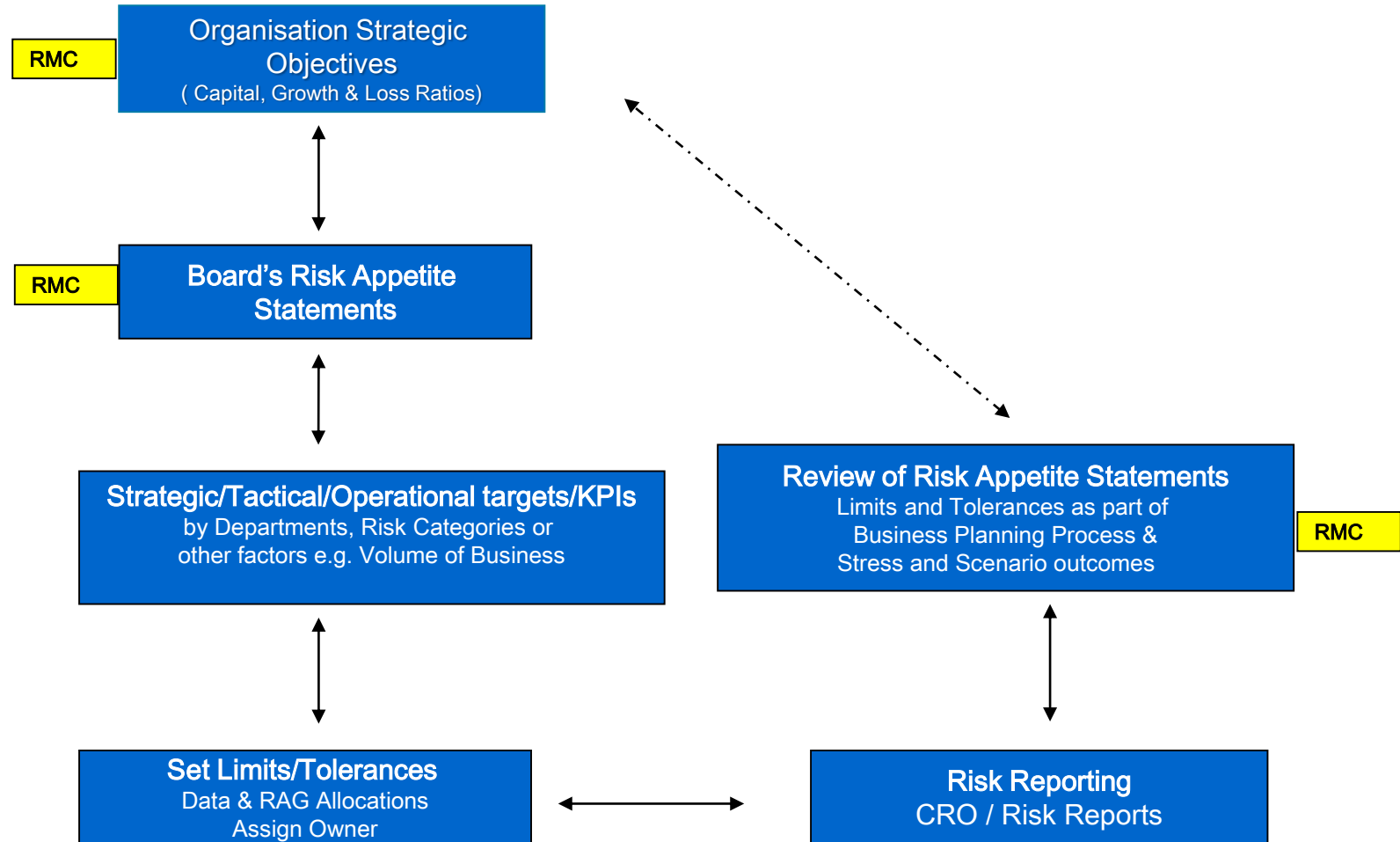
Drive down unintended  
risk types

Improve ability to  
respond to risks

Focus understanding  
around value of risk

Other thoughts?

# Risk Appetite Setting Process



**RMC** Risk Management Committee

# Key Risk Appetite KPI's



## Action & Escalation Process

Parameters	Indicators	Justification(s) /Basis	Owner	Frequency of monitoring & data collection
<b>Quantitative Indicators</b>				
1. Return On Capital – not less than 18% (asset under custody + shareholder funds). <i>(Discussion to be had how to deliver on this return rate)</i>	If actual < 4.5% , then <b>Red</b> If actual is ≥ 4.5% but < 5%, then <b>Amber</b> If actual is ≥ 5%, then <b>Green</b>	▪ <i>Proposed figure also in line with best industry standards, which says..." returns shall be set at a level more conservative higher than rate of inflation"</i>		
2. Interest Income <b>Not less than 6.25% per quarter</b>	If actual < 6.25% , then <b>Red</b> If actual is ≥ 6.25% but < 7%, then <b>Amber</b> If actual is ≥ 7%, then <b>Green</b>	▪ <i>ERM would monitor and trigger deviations if's market share possession falls below 1%.</i>		M – Quarterly
3. Cost of funds <b>Not more than 14% pa or 3.5% per quarter</b>	If actual > 3.5%, then <b>Red</b> , If actual is >3% but ≤ 3.5%, then <b>Amber</b> If actual is ≤ 3%, then <b>Green</b>	▪		M - Quarterly
4. Liquidity ratio	If actual > 50%, then <b>Red</b> if actual > 45% but ≤ 50%, then <b>Amber</b> If actual ≤ 45%, then <b>Green</b>	▪ <i>Data to be collated on a monthly basis and analyzed quarterly</i>		M - Quarterly DC – Monthly
5. Portfolio at Risk (PaR)	If actual > 25% , then <b>Red</b> If actual > 20% but ≤ 25% then <b>Amber</b> If actual ≤ 20% , then <b>Green</b>	▪ <i>Regulatory limit is not more than 10%. Exy currently has a PaR of 48% as at Q2 2015. Selected staff will meet and decide on what the tolerance limits should be</i>		M - Quarterly DC – Monthly

**Red**

KPI clearly exceeding tolerance limit, urgent actions & decisions required immediately with effective monitoring & follow up

**Amber**

KPI close to tolerance limit, actions & decisions required with effective monitoring & follow up

**Green**

KPI on track (nothing to report) for information only



# Five tests for risk appetite frameworks

- Do the managers making decisions understand the degree to which they (individually) are permitted to expose the organisation to the consequences of an event or situation? Any risk appetite statement needs to be practical, guiding managers to make risk-intelligent decisions.
- Do the executives understand their aggregated and interlinked level of risk so they can determine whether it is acceptable or not?
- Do the board and executive leadership understand the aggregated and interlinked level of risk for the organisation as a whole?
- Are both managers and executives clear that risk appetite is not constant? It changes as the environment and business conditions change. Anything approved by the board must have some flexibility built in.
- Are risk decisions made with full consideration of reward? The risk appetite framework needs to help managers and executives take an appropriate level of risk for the business, given the potential for reward.
- Source – [www.theirm.org/riskappetite](http://www.theirm.org/riskappetite)



# Day 2: Sessions 5 - 8

## Risk Management Process



- Establishing the context
- Risk identification, description, analysis and evaluation
- Qualitative analysis & evaluation
- Risk treatment (also called risk response/plan)
- Risk reporting and assurance



# Communication and consultation

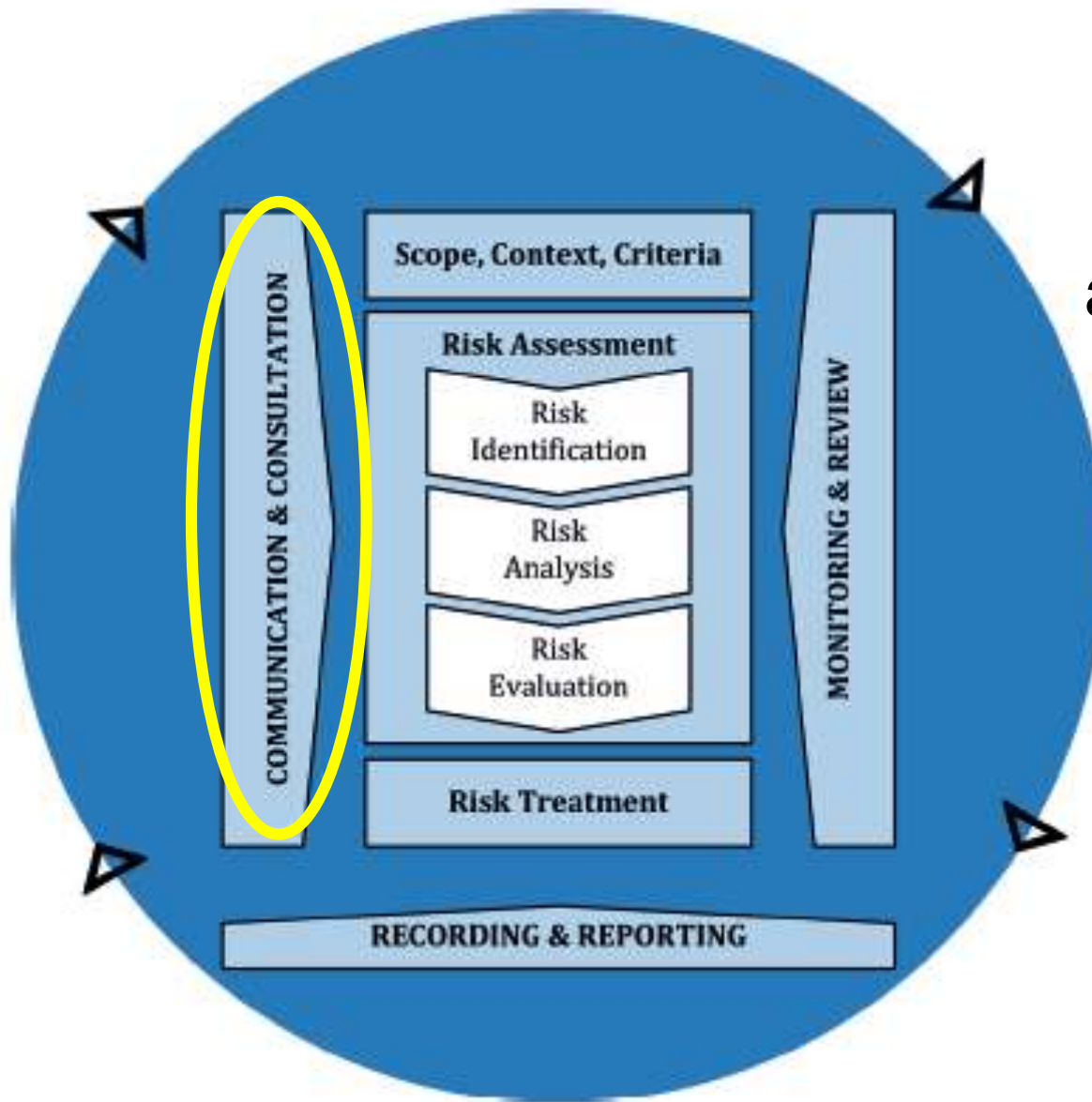


Figure 4 — Process





# Communication and consultation

## Communication

- a continual and iterative process that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders

## Consultation

- a two-way process of informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue

## Stakeholders

- a person or organisation that can affect, be affected or perceive themselves to be affected by a decision or activity



## Establishing the context

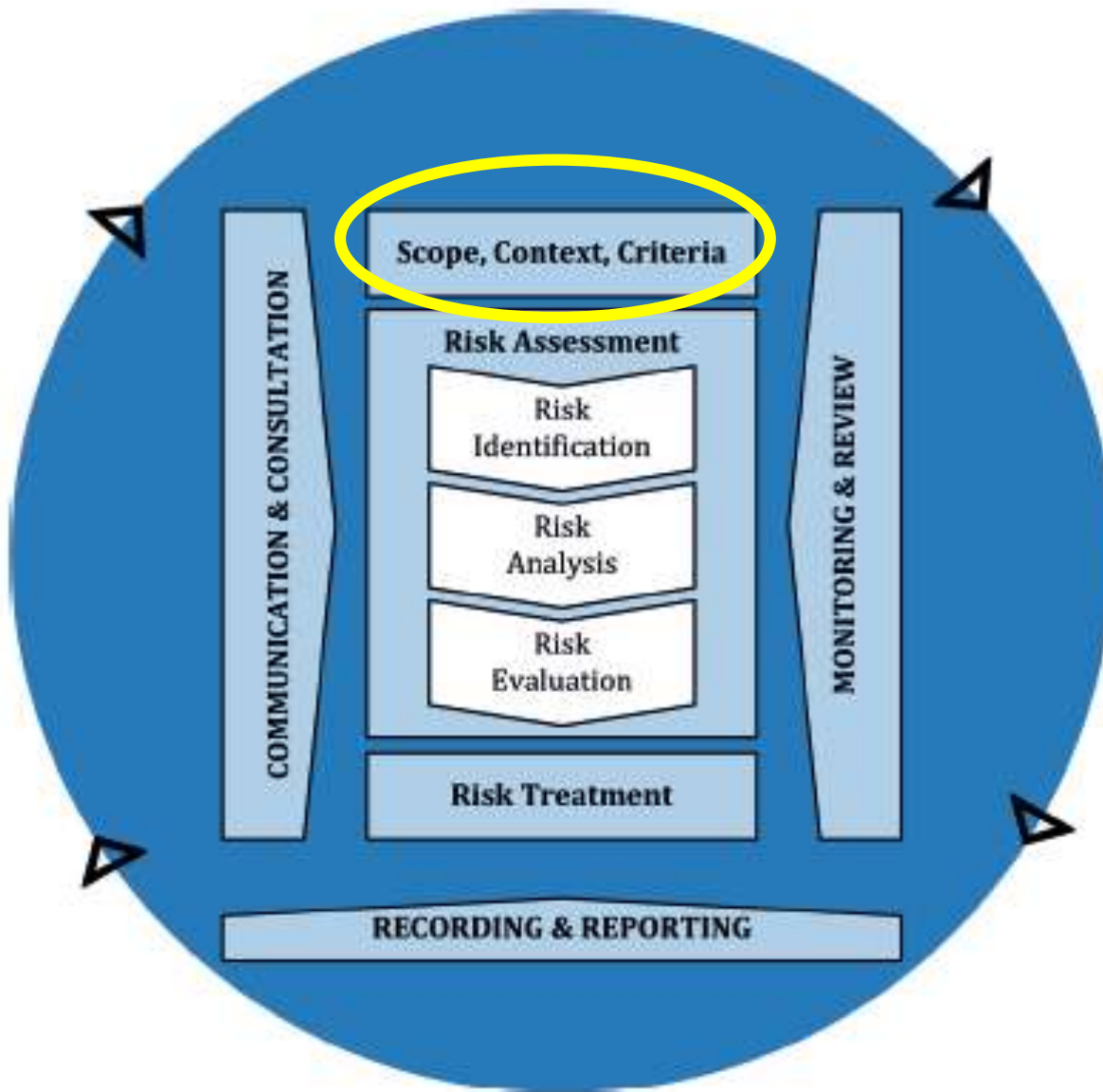
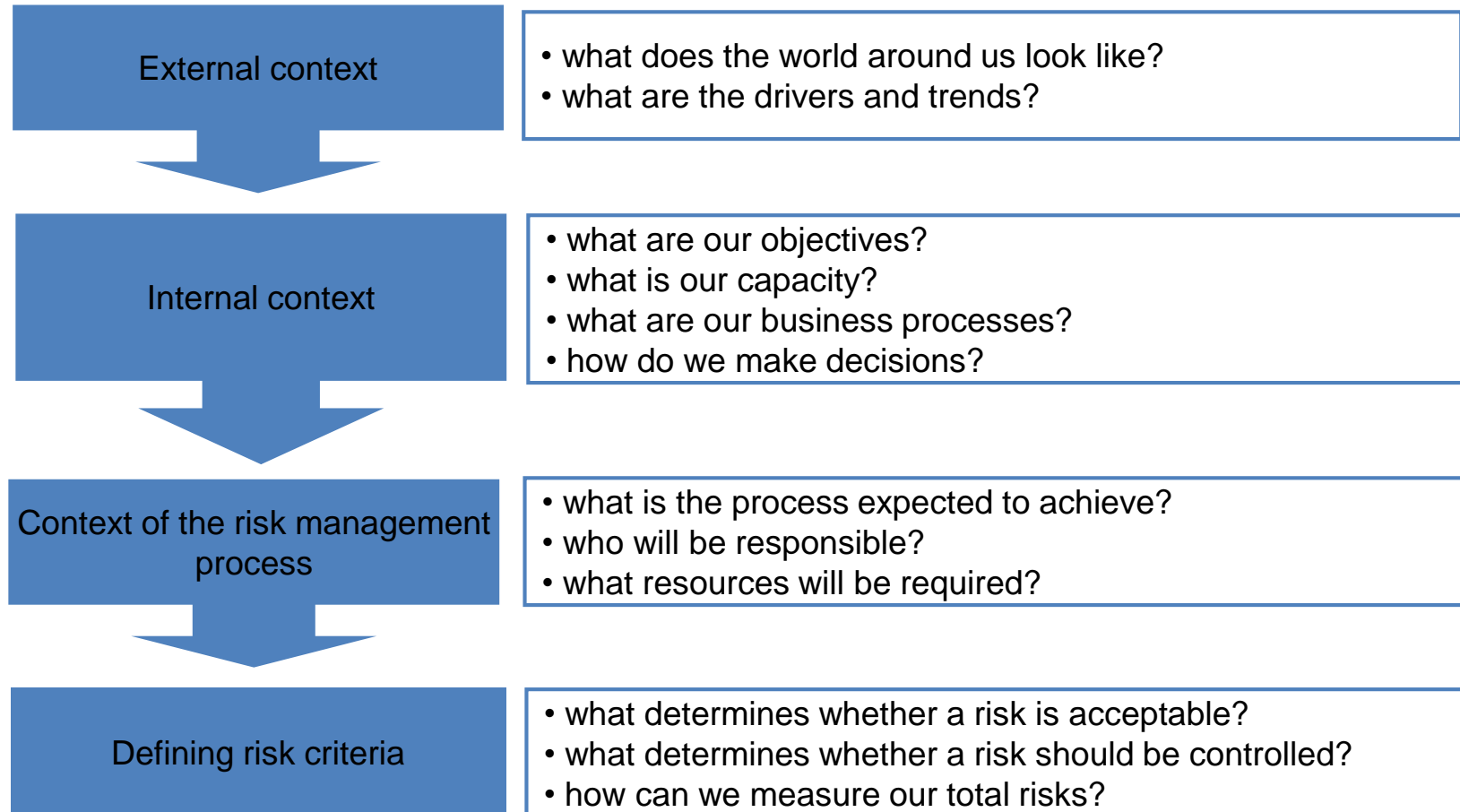


Figure 4 — Process



# Establishing the context





Interview your neighbour about the context of their organisation. For example find out about -

- the size, geographic location and spread, scale of operations
- type of product/market/customers/ competitors/funding
- do they operate in a regulated environment?
- ownership and management structure
- type of employee (specialized skills base)
- are they risk seeking or risk averse



# Risk Assessment

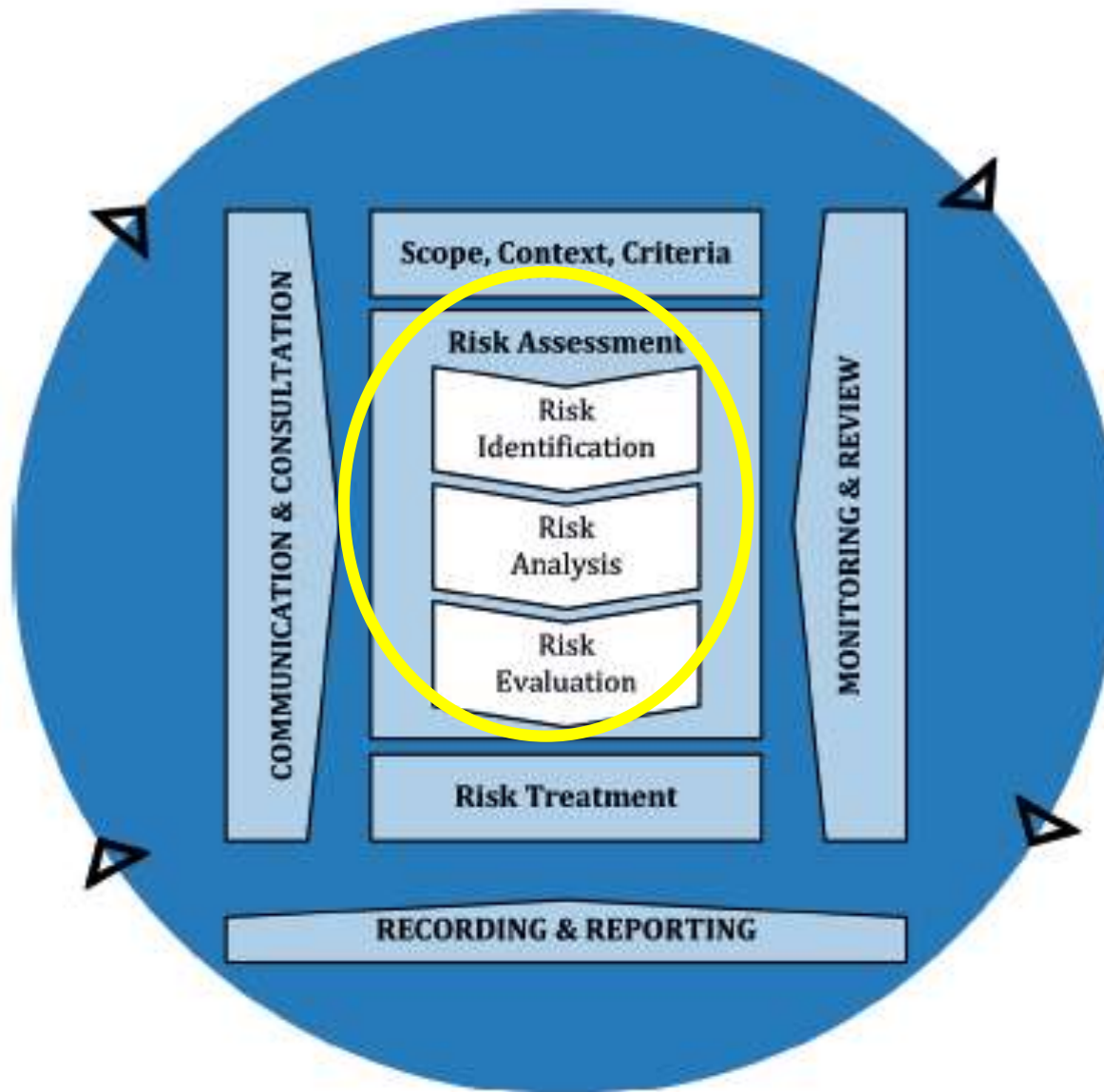


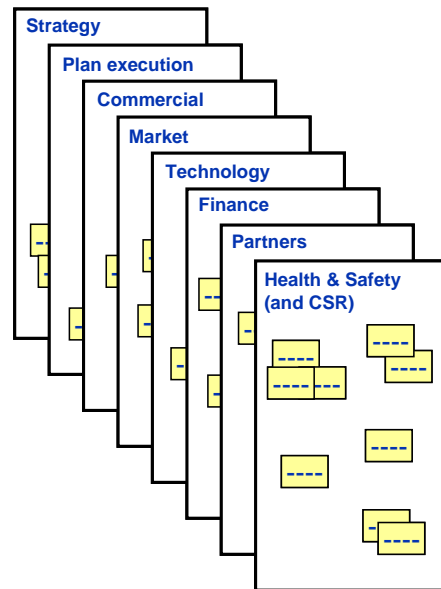
Figure 4 — Process



# Two main types of identification techniques

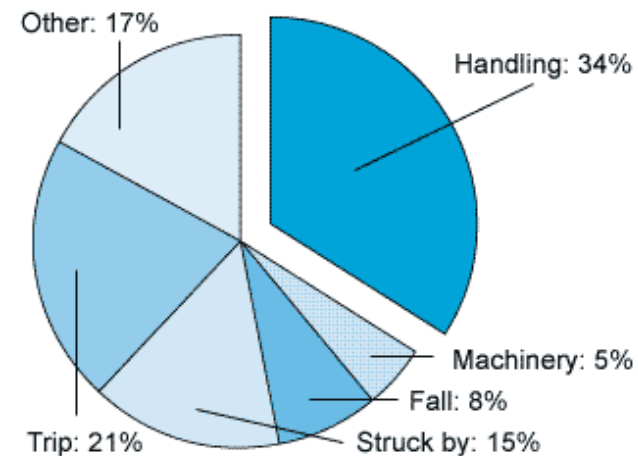
## Forward looking

- brainstorming workshops
- surveys
- expert knowledge



## Historic

- statistical analysis
- trend analysis



Injury statistics



# Qualitative versus quantitative

## Qualitative

- simple to understand
- capitalises on judgement of user
- quick and inexpensive
- appropriate for use where there is little statistical evidence

## Quantitative

- competence in using the technique is required
- can be expensive to use
- stronger evidence base to analysis
- less prone to user bias
- can only be used where there is a volume of data about the type of event





# Risk identification and assessment tools (1)

Technique	Brief description
Questionnaires and checklists	Use of structured questionnaires and checklists to collect information to assist with the recognition of the significant risks
Workshops and brainstorming	<p>Collection and sharing of ideas and discussion of the events that could impact on objectives, stakeholder expectations or key dependencies.</p> <p>Use of headings or categories commonly used to provide a structured approach, for example -</p> <ul style="list-style-type: none"><li>IRM risk wheel,</li><li>Strengths, Weaknesses, Opportunities, Threats (SWOT)</li><li>PESTLE – Political, Economic, Social, Technological, Legal, Environmental (PESTLE)</li></ul>



## Risk identification and assessment tools (2)

Technique	Brief description
Risk profiling/risk registers	Use of consequence and probability assessments plotted on a risk matrix or heat map to describe the risk.
Inspections and audits	Physical inspections of premises/activities and audits of compliance with established systems and procedures
Flowcharts and dependency analysis	Analysis of processes and operations within the organisation to identify critical components that are key to success
HAZOP and SWIFT	Team-based studies using sets of prompt words to identify risks in a structured 'what if' manner.



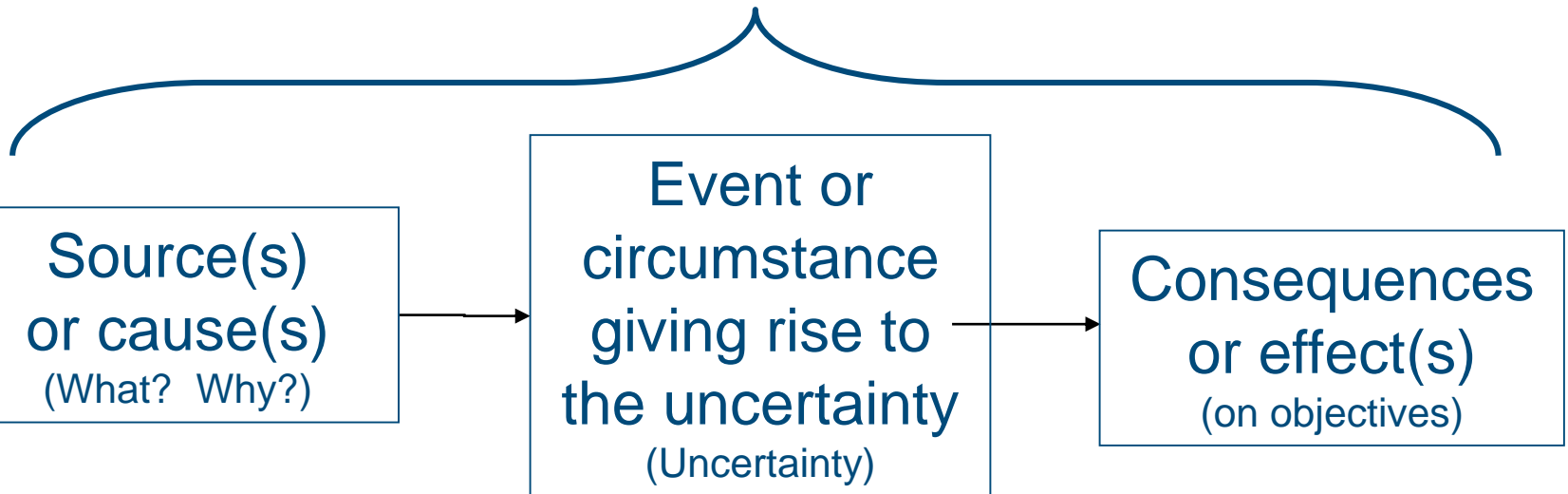
## Risk identification & assessment tools (3)

Technique	Brief description
Event trees Fault trees	Visual technique for exploring the sequence of events that must occur in order for a top event to happen (fault trees) or the sequence of events that may follow a top event (event trees). Can be qualitative or quantitative in nature.
Risk modelling techniques	A range of techniques involving the development of computer models to help explore complex systems with multiple inputs with numerous potential outcomes.
Risk bow-ties	Placing the risk event in the middle of the bow-tie analysis helps to explore both potential causes and consequences in depth.



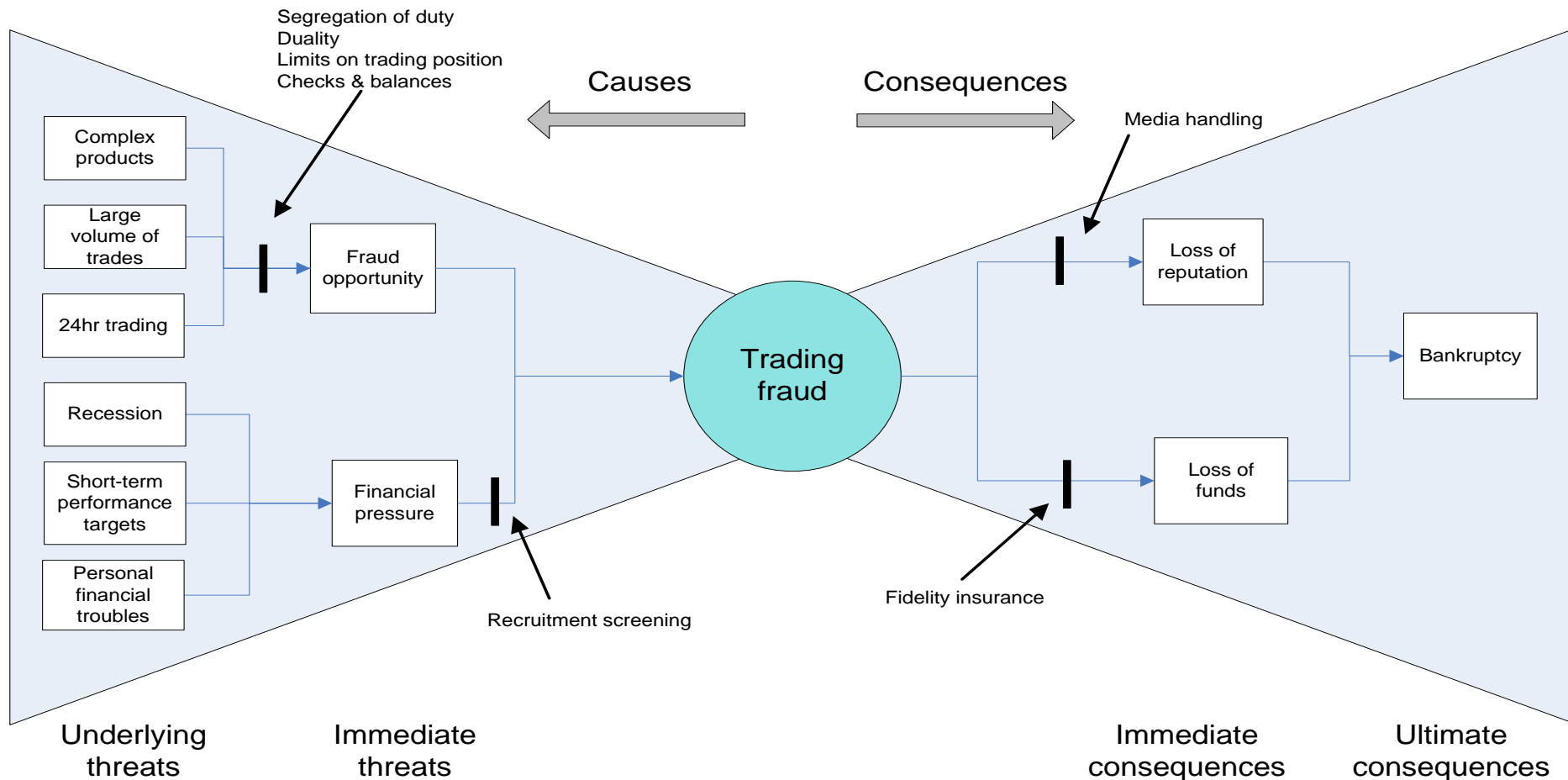
# Describing a risk

Combines the cause(s), the event(s) and the effect(s)





# Example – trading fraud



## Bow tie exercise

# Risk matrix



Likelihood	Probable			
	Possible			
	Remote			
		Low	Medium	High

Impact



# Likelihood

Estimation	Descriptors	Indicators
<b>Probable</b>	Likely to occur each year or more than a 25% chance of occurrence	Potential of it occurring several times within the time period (e.g. ten years). Has occurred recently
<b>Possible</b>	Likely to occur in a ten-year time period or less than a 25% chance of occurrence	Could occur more than once within the time period (e.g. ten years). Is there a history of occurrence?
<b>Remote</b>	Not likely to occur in a ten-year period or less than a 2% chance of occurrence	Has not occurred. Unlikely to occur





# Estimating likelihood - criteria

Within the next 12 months the event is:

## **Almost certain**

- Frequent occurrence > 90% chance

## **Likely**

- Regular occurrence > 60% chance

## **Possible**

- Occasional occurrence > 10% chance

## **Unlikely**

- Has never occurred < 10% chance



# Estimating impact – criteria

	REPUTATION	FINANCE	SERVICE DELIVERY	COMPLIANCE	SAFETY
EXTREME	Loss of credibility key stakeholders; extensive adverse media; external intervention	Financial loss exceeding £/\$ ???	Total sustained disruption to critical services	Intervention by regulator; serious breach of legal or contractual obligation	Fatality (multiple)
HIGH	Significant loss of trust; significant adverse media	Financial loss exceeding £/\$???	Significant sustained disruption to critical services	Censure by regulator; breach of legal or contractual obligation	Serious injury or ill-health (disabling)
MEDIUM	Significant complaints	Financial loss exceeding £/\$???	Some short-term disruption to services	Failure to meet recommended best practice	Injury or ill-health resulting in lost time
LOW	Isolated complaints	Low-level or no financial loss	Minor disruption to services	Failure to meet internal standards or SLA	Minor injury (no lost time)



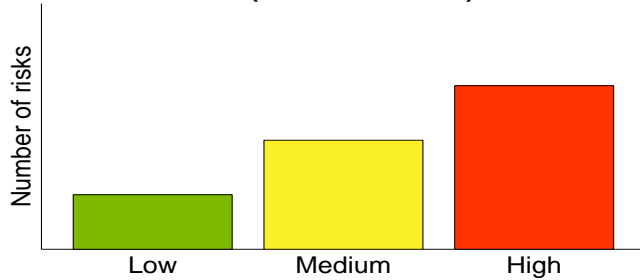
# Putting it all together

LIKELIHOOD	<b>PROBABLE</b> Likely to occur each year or more than a 25% chance of occurrence	3	3	6	9
	<b>POSSIBLE</b> Likely to occur in a ten year time period or less than a 25% chance of occurrence	2	2	4	6
	<b>REMOTE</b> Not likely to occur in a ten year period or less than a 2% chance of occurrence	1	1	2	3
			1	2	3
			LOW	MEDIUM	HIGH
			•financial impact on the organisation is likely to be less than £x  •low impact on delivery of the organisation's strategic or operational activities  •low stakeholder concern	•financial impact on the organisation is likely to be between £x and £x  •moderate impact on delivery of the organisation's strategic or operational activities  •moderate stakeholder concern	•financial impact on the organisation is likely to exceed £x  •significant impact on delivery of the organisation's strategic or operational activities  •significant stakeholder concern
			IMPACT		

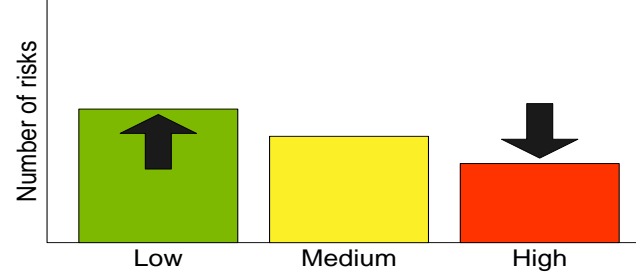


# Three points of risk assessment

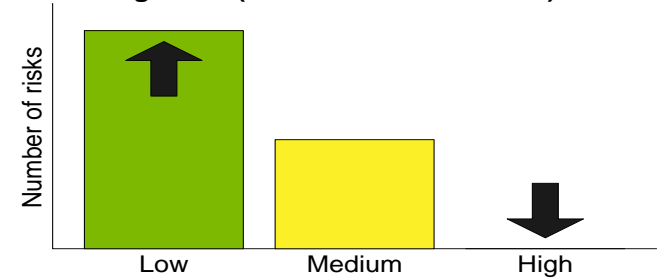
## 1. Inherent risk (with no controls)



## 2. Residual risk (with existing controls)



## 3. Target risk (with additional controls)





# Opportunity and threat matrix

Upside Risk			Likelihood	Downside Risk		
High	High	Medium	1:2 Probable	Medium	High	High
High	Medium	Low	1:10 Possible	Low	Medium	High
Medium	Low	Low	1:100 Unlikely	Low	Low	Medium
Major	Moderate	Minor		Minor	Moderate	Major
Consequence						
Multiple objectives exceeded beneficially.	Objective delivered significantly early, better, or cheaper.	Objective delivered slightly early, better or cheaper.	Objective-driven (Customer, people, society or key performance)	Slippage and minor deviation.	Failure to meet an objective.	Extinction of organisation.

# Establish Risk Provision



- MUST be relative to the estimate
- MUST be relative to the scope
- MUST be relative to the job (not just say 10%)
- Approach can be dependent on project type and business maturity
- Not always about Monte Carlo

## Risk Estimating Techniques (Project)

- % on cost
  - Benchmarking (Historic data)
  - Optimism Bias (International 'Benchmarks')
- Three-Point Estimate
- Expected Monetary Value ( $\% \times \text{Ave. Cost}$ )
- Quantitative Risk Assessment (QRA) – Monte Carlo
  - Cost (QCRA)
  - Schedule (QSRA)
  - Integrated Cost and Schedule

# Three Point Estimating



- Three Point on Base Cost Estimates
  - Uncertainty around measure – Level of design detail
  - Unit Rate – Sensitivity e.g. market tested
- Three Point Estimate of risk impacts should it occur

## Estimate of potential risk impact

- Three 'scenarios' e.g. Unforeseen ground conditions
  - Most Likely (dependent on knowledge)
  - Minimum (Non-Hazardous material rate x Min additional volume)
  - Maximum (100% Hazardous material rate x 'Reasonable' Max volume)
- Minimum – Most Likely – Maximum range of impacts when the risk occurs
- Therefore avoid a minimum impact = 0
  - If the risk is 10% likely, 90% of the time the impact is already zero

## What about 100% likelihood risks?

- Include 'Known' element in base cost
- Identify 'Extra over' risk for uncertain impact





# Risk Treatment

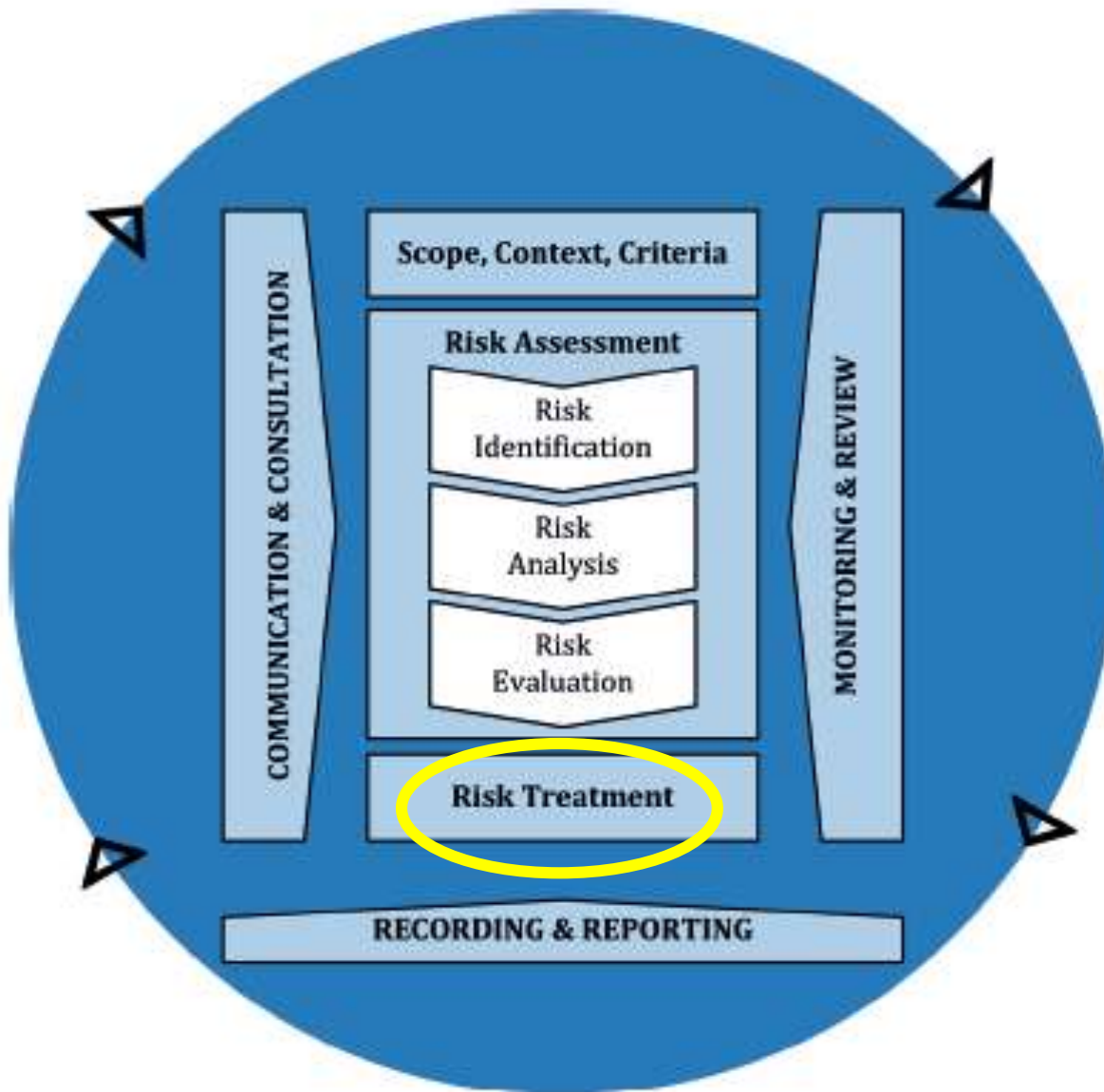


Figure 4 — Process



# What is risk treatment?

A process to modify risk (ISO 31000)

Risk treatment (or response) involves:

- the selection of one or more options for modifying risks
- implementing those options
- the treatments then provide controls or modify current controls

*Treatments or Controls include any process, policy, device, practice or other actions which modify the risk*

# Risk treatment plans (action plans)



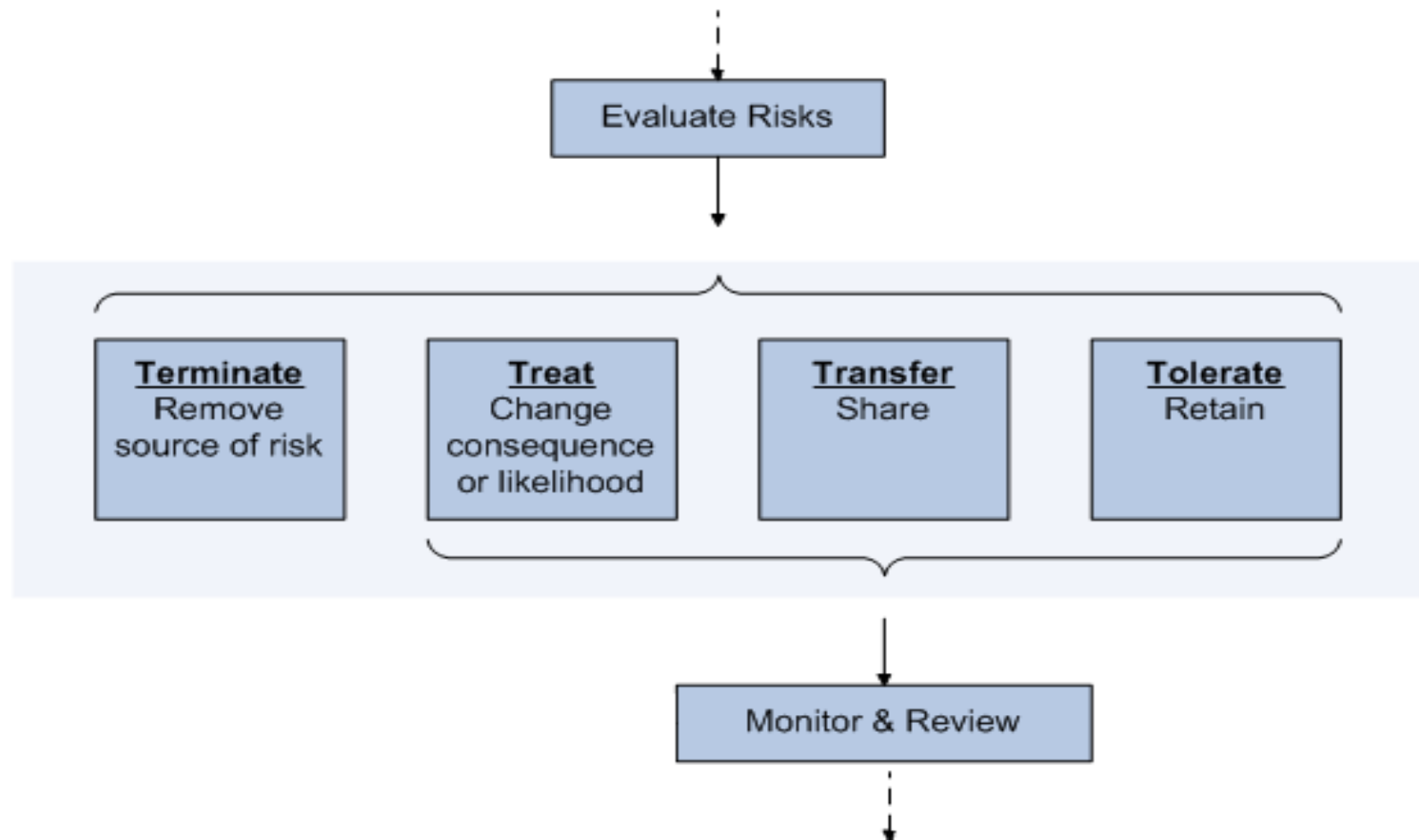
The purpose of risk treatment plans is to document how the chosen treatment options will be implemented.

Information should include:

- a description of what the planned action is
- expected benefit(s) to be gained
- performance measurements and constraints
- accountabilities (risk owners and control owners)
- reporting and monitoring requirements
- resourcing requirements
- timing and scheduling



# Risk response options

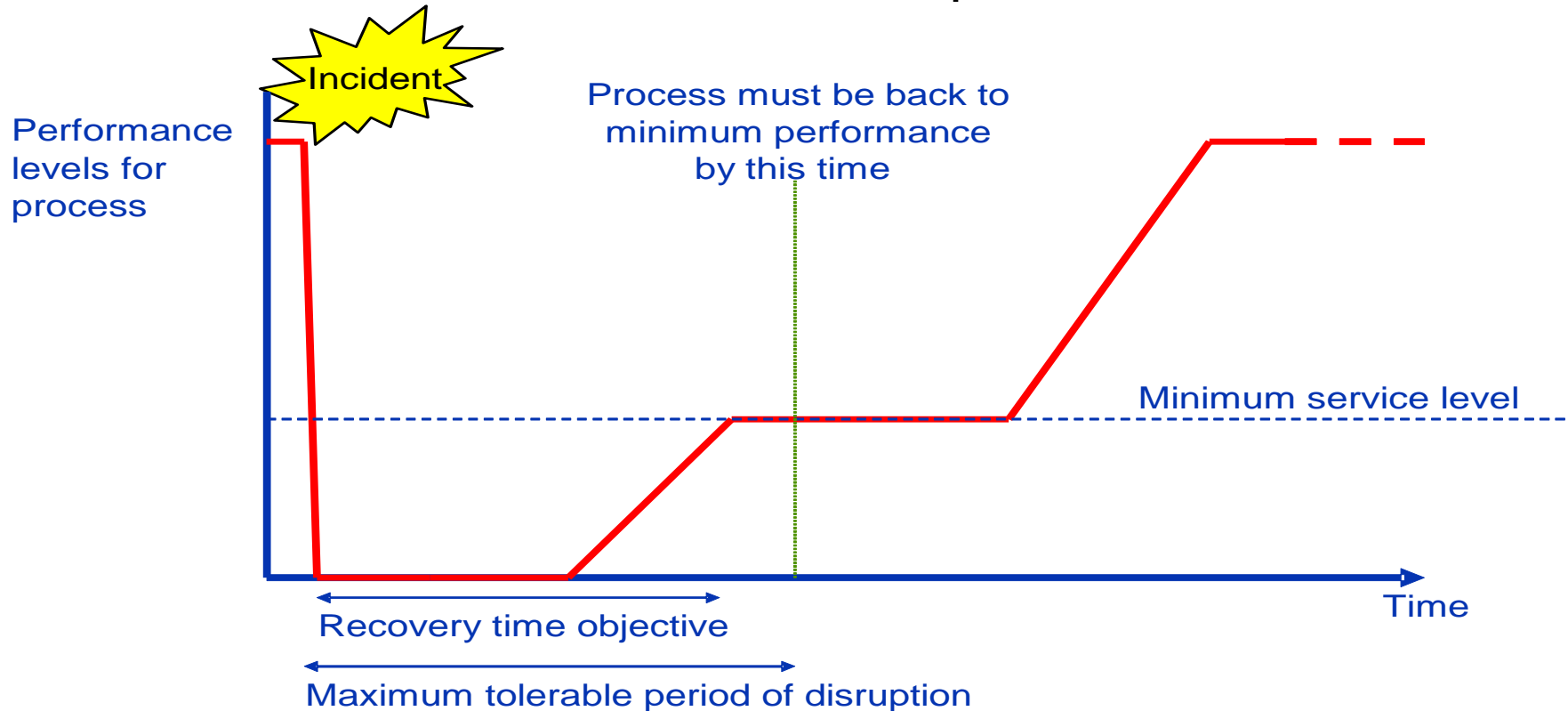


# Business continuity management



Business continuity management (BCM) provides a framework for business resilience.

The focus of BCM is on managing the impact of risks to mission and time-critical processes





# Key activities in business continuity planning

1. assess company activities to identify critical people, processes and equipment
2. identify critical customers and suppliers
3. plan what to do if any important buildings, plant or store were to become inaccessible
4. identify necessary actions to ensure continuity of critical business functions
5. decide who should be involved in the planning process
6. define and prepare procedures, identifying individual responsibilities in crisis management and recovery activities
7. coordinate with others including neighbours, utility suppliers, suppliers, shippers and key customers
8. review the plan annually and when the business changes



# Monitoring and review

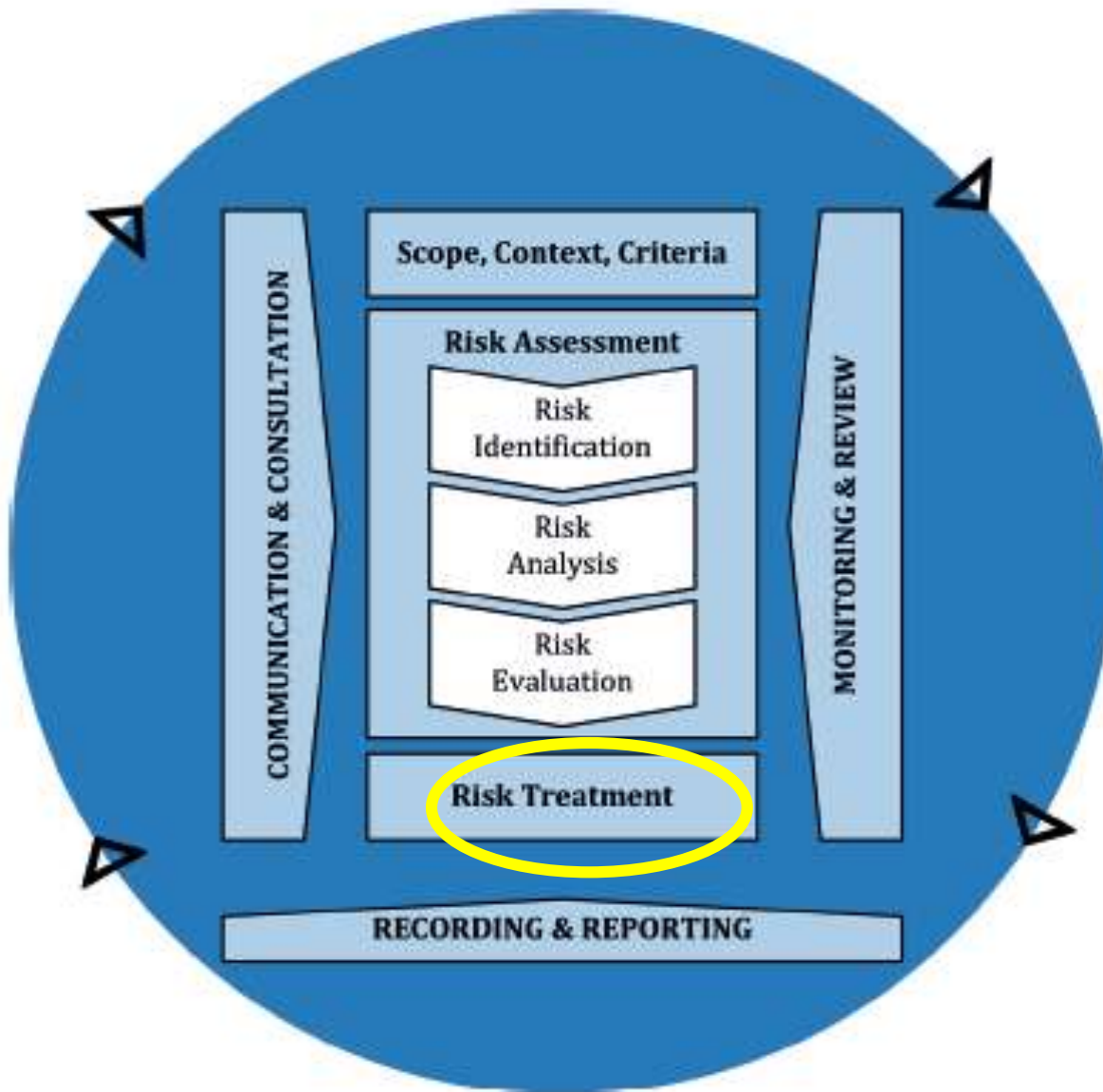


Figure 4 — Process





# Purpose of monitoring and review

- ensure controls effective and efficient
- obtain information to improve risk assessment
- learn the lessons from events
  - changes, trends, successes and failures
- detect change to internal or external context or to the risk itself
- identify emerging risks

# Risk Register – Risk Details



Updated	12/02/2014
Next risk ref	102
Version	v1.0

Project Manager	
Project Number	

Capture Document  
Control information

Risk Owner and ID		Risk Details			
Owner	Risk ID	Risk Status	Risk Description	Risk Cause	Risk Impact
Employer	101	Open	Risk that the your house may flood	Extreme Weather; Poor Insulation; Insufficient Heating	Delayed departure; reduced time on holiday; costs incurred while waiting in the airport (possibly accommodation)

Unique Risk Identifier

Clear description of the uncertainty affecting the project

Potential effects on the scheme objectives should the risk occur

Contractual Owner of the risk exposure

Current status of the risk on the scheme:  
Open, Closed, Escalated, etc.

Potential cause(s) of the risk occurring

# Risk Register – Risk Assessment



Assessment – based on the controls in place

Assessment – based on the anticipated effects of the **Identified** response actions

Current Risk Assessment					Post-mitigation Risk Assessment					Risk Proximity	
Likelihood	Cost	Time	Safety Security Legal & Reputational	Score	Likelihood	Cost	Time	Safety Security Legal & Reputational	Score	Risk Start Date	Risk Stop Date
2	3	1		9	1	2	0		3	Nov-14	Mar-15
				0					0		
				0					0		

Likelihood / Probability of the risk **Occurring**

Cost Impact **on / attributable to the scheme**

Time impact on scheme deliverables

Assessment of other impacts caused by the scheme

Calculated from Likelihood and Maximum Impact – **Allows Prioritisation**

Time period when The risk may impact on the scheme

# Risk Register – Risk Responses



Risk Response					
Risk Response Owner	Risk Treatment	Mitigation Action(s) Description(s)	Action Owner	Action Close Date	Notes
Contractor	Treat	Ensure appropriate fitout including: frost Stat installed; Ensure sufficient insulation installed; Maintenance of central heating system.	Contractor	Jul-14	

Risk response approach (discussed later)

For capture of risk change commentary, Assessment backup, Assumptions, etc.

Owner responsible for development and delivery of **the actions** (not risk exposure)

Responsible for **implementation** of the identified actions

Date for closeout of the identified **Response Action(s)** (not risk itself)

Description of activities identified to mitigate, monitor or control the identified risk



# Risk reporting

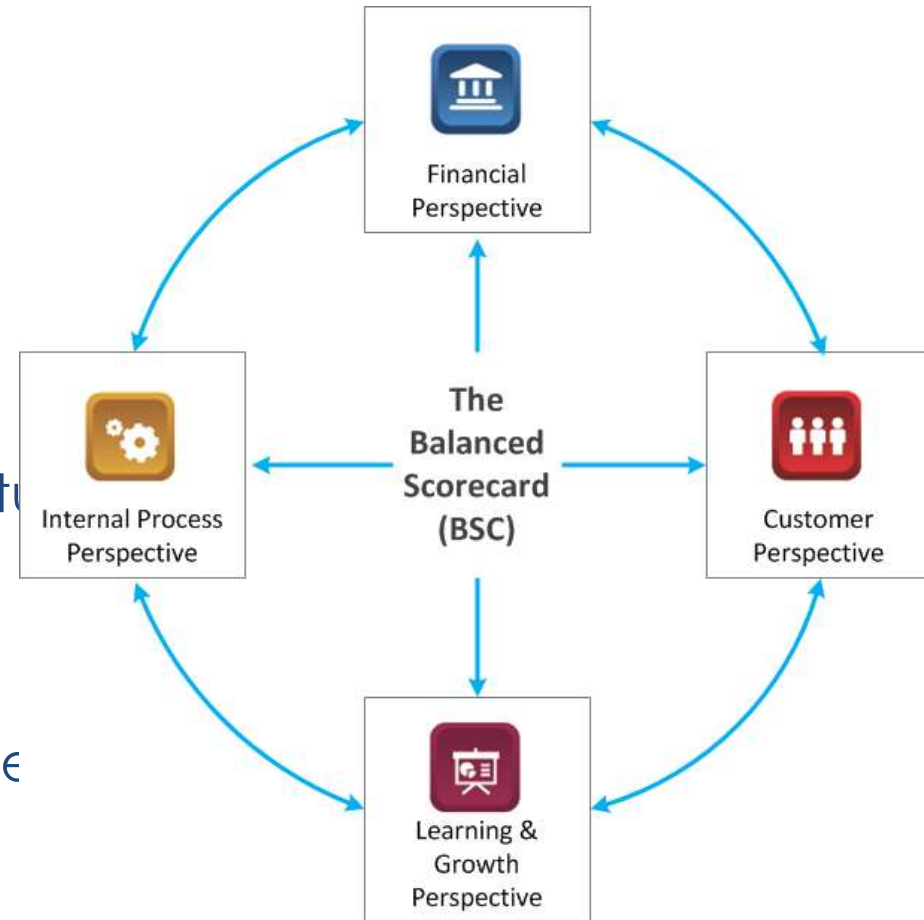
- Efficiently meet data requests
- Provide targeted formatting
- Build a scalable solution
- Reduce time and costs





# What is a dashboard?

- A dashboard is a .....
- Key characteristics:
  - Provides a real-time user interface
  - A snapshot or graphical presentation of the current state of indices
  - Shows *historical trends and comparison* of an organization's key performance indicators to enable informed decision making





# Benefits of risk dashboard



- Move quickly





# Creating a risk reporting dashboard

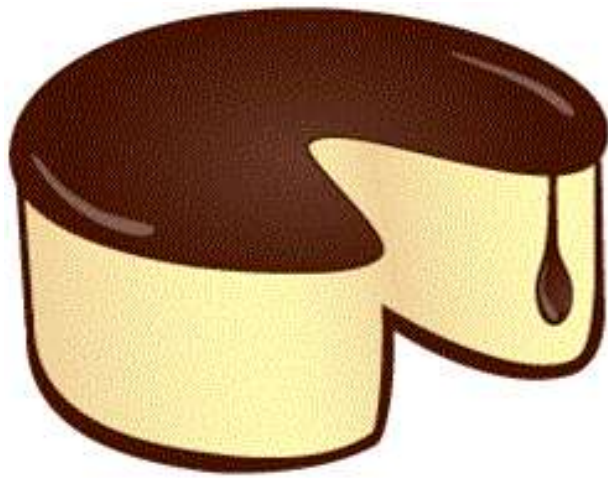
## Considerations:

- What is the reason for the dashboard?
- Specific KPI's?
- Data source
- How often will it be updated?
- Who will receive the report and in what format?





# *Sweet things Ltd*



- Report prepared for potential buyer for 'Sweet things' bakery.
- 'Sweet things' is a family owned business and is being sold because owner is retiring.

# Sweet things Ltd



## Risk Reporting Dashboard for Sweet things bakery ltd, 2014

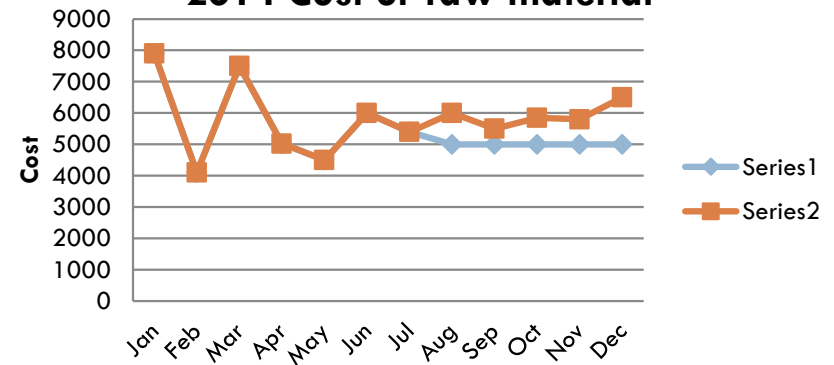
### Key Risks

Risk name	Description	Impact/Residual risk				Trend
		Q1	Q2	Q3	Q4	
Volatile cost of raw materials	Prices of wheat and vegetable oil can vary more than 40% during a one-year period, along with this natural gas prices can fluctuate by more than 25%	High	Med	Low	Low	↓
Loss of customers	The supermarket industry has been consolidating, and as that has happened, some have formed their own bakeries. Larger chains have the resources to take some of their baking operations in-house, including "fresh-baked" goods resulting in loss of customers	Med	Med	Med	Med	→
Health & Safety	Contamination with allergens resulting in loss of reputation	High	High	Med	Med	↘
Changing trends in taste	Changing consumer preferences as it relates to changing tastes and dietary trends	Low	Low	Low	Low	→
Automation	Risk that lack of automation makes business unable to compete profitably	High	High	Med	Med	↘

### Risk Heat Map



### 2014 Cost of raw material





# Things to consider

## Define monitoring and review responsibilities

- risk owners
- control owners
- responsibility for the review of the whole process

## How frequently should

- risks and their control measures be reviewed?
- the effectiveness of the ERM process be reviewed?

## Benchmarking and maturity models



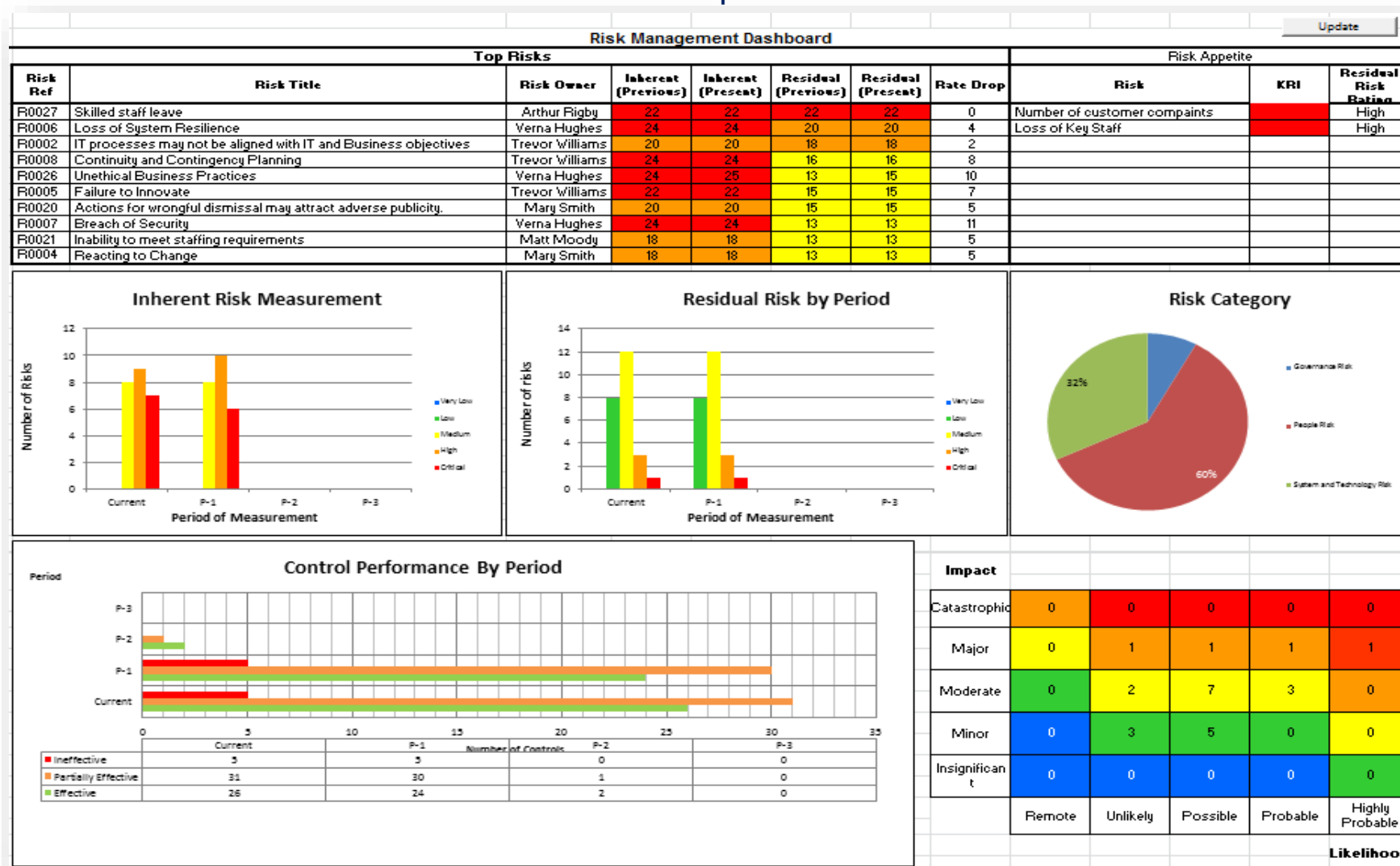
## Rating Scale For Effective Reporting

Rating	Status	Description for Effective Reporting
1	Very Poor (Ineffective)	The report is not accurate and consistent within the organisation; lacks formal approval or review process and/or not delivered on time to reflect the true position of the business; not fit to inform effective decision-making
2	Poor (Ineffective)	The report is not accurate but consistent within the organisation; gone through informal approval or review process and/or not delivered on time to reflect the true position of the business; not fit to inform effective decision-making
3	Good (Average)	The report is accurate and consistent within the organisation; gone through formal approval or review process and delivered on time to reflect the true position of the business; fit to inform effective decision-making
4	Very Good (Best-Practice)	As 3, we can demonstrate active management engagement/feedback from each report and the effectiveness could be measured and the value of presenting each report to each governing body is clear?



# Risk Management reporting

## 'Dashboard reports'





*practice*  
makes *better*



# Overview of ISO and COSO Framework

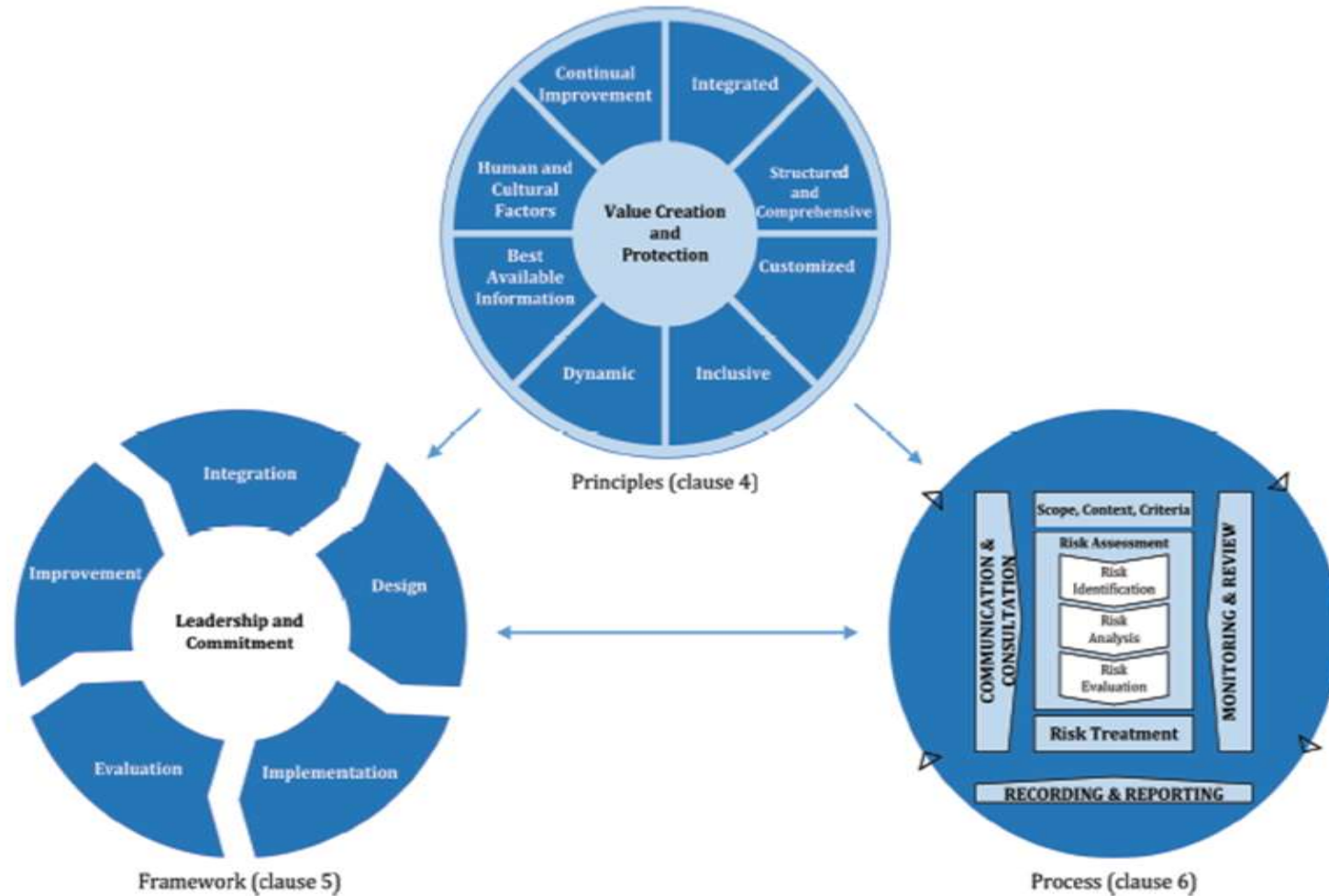
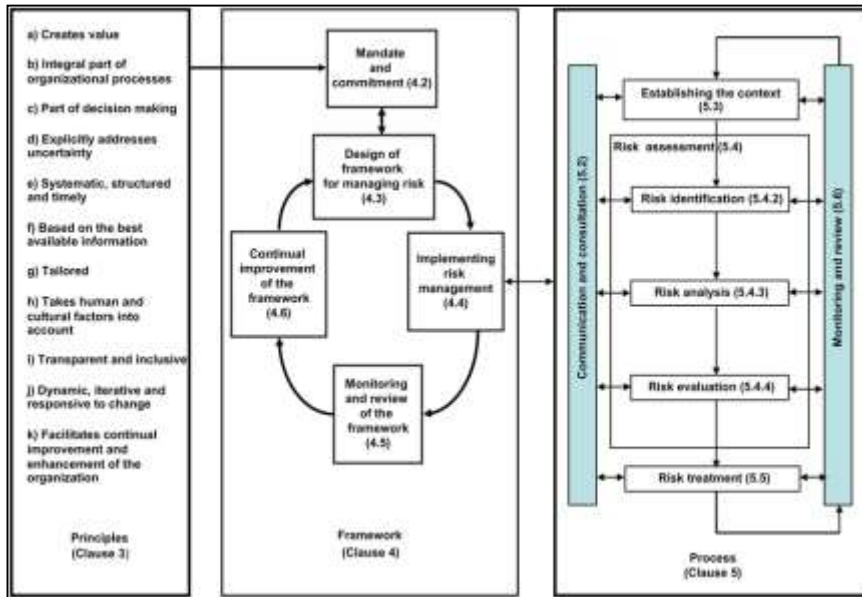


Figure 1 — Principles, framework and process

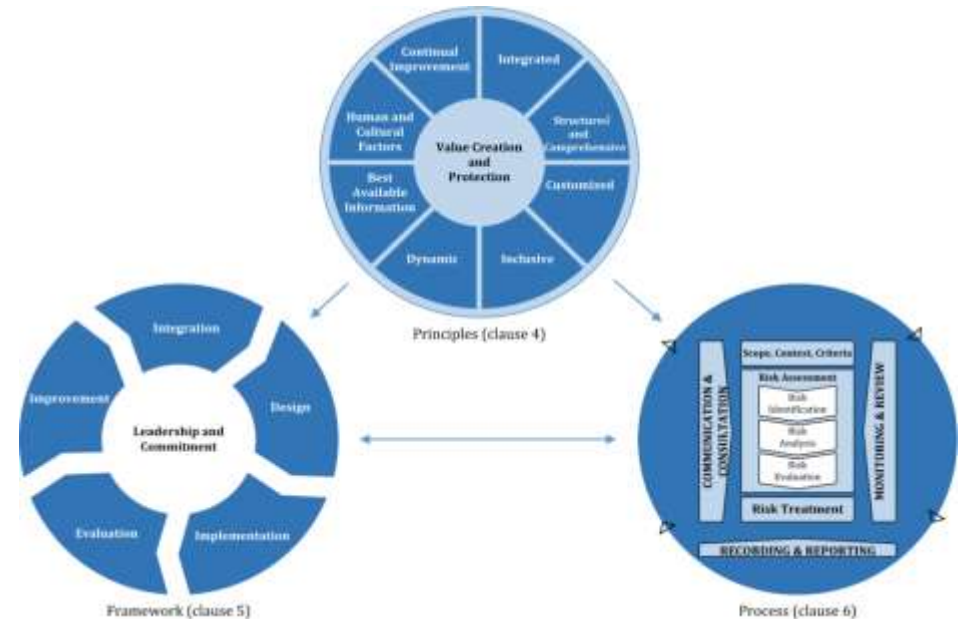


- Throughout the course we will use ISO 31000 as our core framework

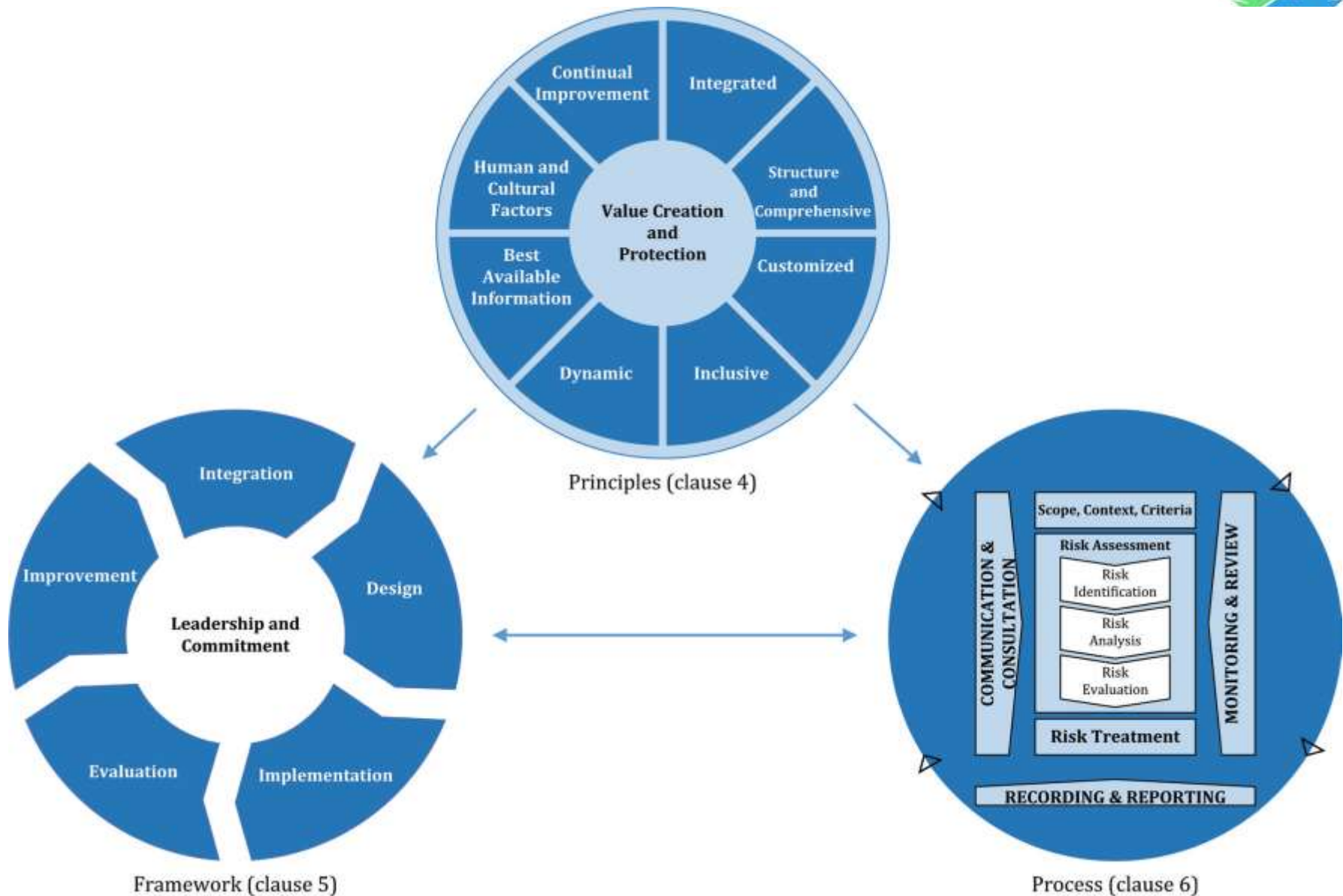
## ISO 31000:2009



## ISO 31000:2018



- Framework: Centred on leadership and commitment, includes integration as additional step
- Principles: Focus on Value creation and protection.
  - 8 principles instead of 10;
  - Summarized as PACED – Proportionate, Aligned, Comprehensive, Embedded, Dynamic
- Process: Risk assessment & risk treatment are central to risk management process





# ISO 31000:2018

- ISO 31000:2018 is focused on keeping risk management simple
- Reinforces definition of risk as the “*effect of uncertainty on objectives*”
- Shorter, leaner and more precise
- Focus on leadership by top management and integration
- Greater emphasis on the iterative nature of risk management
- Streamlining of the content with a greater focus on customization
- Additional step in the Process – recording and reporting

# COSO ERM Framework



New framework:

- More clearly connects enterprise risk management with a multitude of stakeholder expectations.
- Positions risk in the context of an organization's performance, rather than as the subject of an isolated exercise.
- Enables organisations to better anticipate risk so they can get ahead of it, with an understanding that change creates opportunities, not simply the potential for crises.
- Clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organisation

# COSO ERM Framework



- Introduces new structure and new principles
  - Five components across framework; 20 new principles supported by a set of principles, covering everything from governance to monitoring



- Focuses on Integration
- Emphasizes value
- Links to strategy
- Links to performance
- Recognizes the importance of culture
- Focuses on decision-making
- Links to internal controls



# COSO vs ISO 31000:2018



## COSO ERM Framework

vs

## ISO 31000:2018

1. Longer document
2. Focused on Enterprise Risk Management
3. Risks and opportunities
4. Emphasis on integration
5. Emphasis on the importance of leadership buy-in
6. Links risk with strategy and performance
7. Brings more to the table with the ERM approach that can be applied at any level of an organisation

1. Short and concise
2. General approach to Risk Management
3. Opportunities can give rise to threats
4. Risks tied to objectives
5. Emphasis on integration
6. Emphasis on the importance of leadership buy-in
7. Does not link risk with strategy and performance

# Break



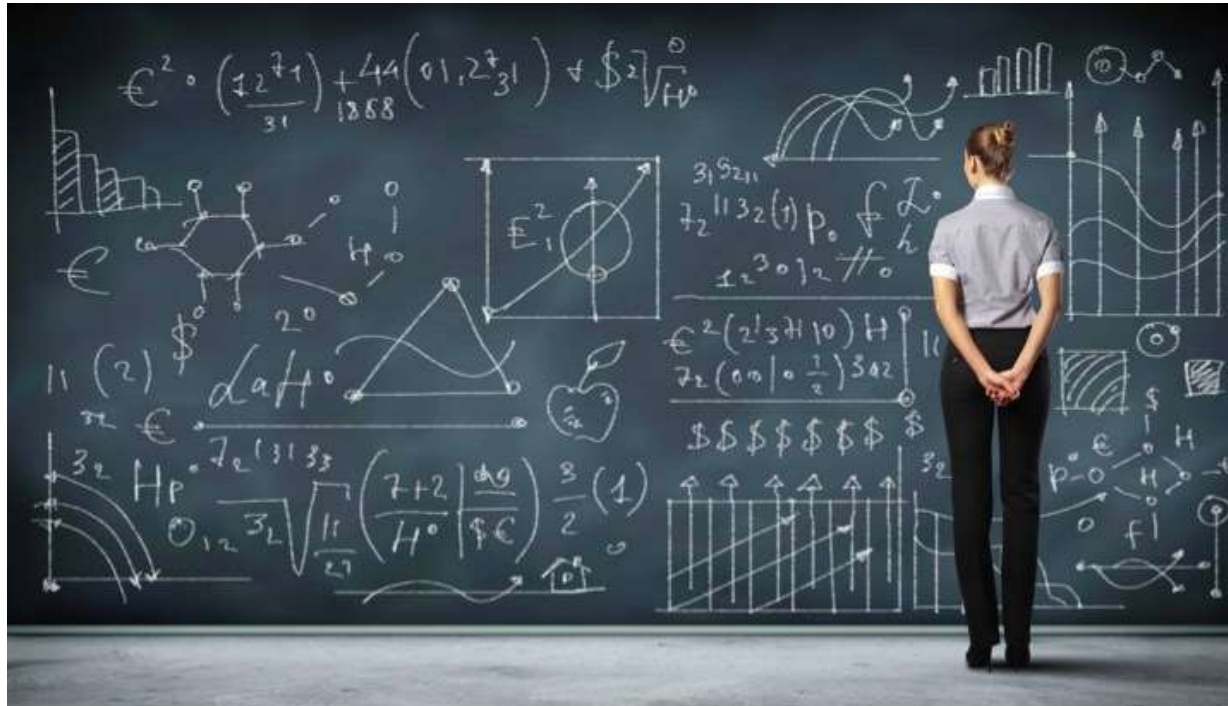
# Tea Break...!





# Day 3: Sessions 9 - 11

## Practical tips



- How to run an ERM risk assessment workshop
- Risk assessment meeting
- When to run risk workshops
- Good risk management



# Introducing Facilitation

This section will discuss the principles and background of Facilitation:

- What Facilitation is
- What Facilitation involves
- The benefits of Facilitation and using a trained Facilitator

## What is facilitation?

- The art of managing a group so that the quality and quantity of work achieved is greater than the contributions of the individuals within it
- The group works more efficiently and productively under the guidance and suggestions of the facilitator

## How does a facilitator achieve this?

- Agreement that the group want to work in a co-operative way
- Have an overall aim and method in mind
- Be able to adjust flexibly to the dynamic that builds up within the group
- Maintaining commitment of the group
- Be able to deal with negative reactions or situation



# Why should you use a facilitator?

- Organisation - preparation & support allows the team to focus on the subject matter
- Challenging - able to ask the difficult / 'daft' questions
- Always keeps a focus on the end objective - output thinking
- Keeps control (*people and process*) to ensure the workshop doesn't drift off track (*wasting time and money*)

## When should you use a facilitator

- Running a major review/workshop
  - Creating your initial risk register
  - Prior to key stage gates, or key dates within your project
  - Prior to a quantitative risk analysis
- When the Risk Management culture needs a boost
- To set up an effective Risk Management process on your project/programme
- Large number of participants and hence a large number of outputs to be managed
- When you have "personalities" that need to be managed



# What do you think makes a good facilitator?



5 mins

## Qualities of a facilitator

### ■ What makes a good facilitator?

- Communicates clearly and expressively
- Strong interpersonal Skills
- Ability to think quickly on ones feet
- Logical
- Strong active listening skills
- Self confidence
- Leadership skills
- Strong motivator
- Client empathy
- Energetic
- Understands team dynamics



### ■ What doesn't make a good facilitator?

- Someone naturally introvert
- More comfortable following set processes rather than the pressure of thinking on ones feet
- Not comfortable presenting to people
- Not comfortable multi-tasking -reading body language, leading, and recording at the same time
- Someone who is heavily involved in the project
- Not happy dealing with / turning around uncomfortable situations





# The Six Dimensions of Facilitation

1. **The planning dimension.** Goal-oriented / output thinking. Understanding aims and setting up process to achieve it.
  2. **The meaning dimension.** Managing participants' understanding. Making sense of the information.
  3. **The confronting dimension.** Challenging. Highlighting areas of resistance and avoidance. Asking the “daft” questions.
  4. **The feeling dimension.** Managing feelings and emotions within the group.
  5. **The structuring dimension.** Using methods and techniques to provide structure around the facilitation process.
  6. **The valuing dimension.** Creating a supportive, inclusive, empowering climate. Honoring the individuality within the group. Encouraging open honest communication.
- *From Heron J (1999), The Complete Facilitator's Handbook, Kogan Page*

# Time, People and Information Management



## ■ ***Prior to the workshop***

- Identifies the time available
- Clarifies outputs required
- Confirms the time available for each section
- Creates a workshop handbook – Agenda, housekeeping, behaviours, context setting.

## ■ ***During the workshop***

- Manages 'disruptive' behaviours
- Takes executive decisions where required to keep on track
- Uses tools and techniques to optimise the time spent
- Parks issues out of context for later discussion

## ■ ***Following the workshop***

- Collates and circulates information
- Captures comments and undertakes follow-up required
- Reports on findings



# Ice Breakers

- Useful way to for the group to get to know each other
- Energising – try one after lunch / after a difficult exercise
- Injects a little fun into the workshop

## More Ice Breakers

- **Two truths and a lie** – Each person tells 2 facts and one lie about themselves and the group have to guess the lie
- **The year of the coin** – Hand out a coin to each participant, they then have to share what they were doing in that year
- **Fabulous Flags** – Each participant creates a flag depicting in images what they want to get out of the workshop, and presents to the group
- **Signatures** – Each participant has a sheet with a number of different descriptions e.g. Cat lover, plays an instrument etc. They need to mingle with the group and get a signature from people who match those descriptions. No one to sign the same sheet twice!
- **Human knot** – Stand in a circle and put your hands in the middle to join hands with 2 different people across the circle. Then have fun untangling yourselves!

# Embedding risk management



## Visible commitment from the top

- articulated and endorsed through a policy and framework for managing risk
- lead through actions – risk-based decision making, aligned with strategic objectives

## An organisational framework to ensure

- clearly defined responsibility and accountability
- training for all relevant stakeholder groups to raise awareness of benefits, establish responsibilities and improve skills in management of risk

## Integration into management processes

- ensure the benefits for business and resource planning are clearly established through integration with the 'normal' business planning processes
- integrate into performance management system and establish KPI's



# KPIs etc



# Key Performance and Risk Indicators





# Key risk and control indicators

## KRIs

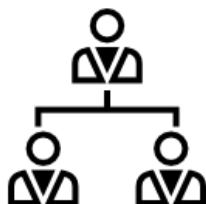
Metrics to help identify changes that could alter the overall assessment of key risk events

## KCIs

Metrics to help assess the effectiveness of key controls

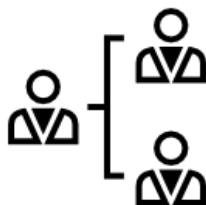
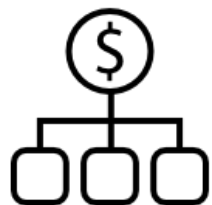


# Financial Risk Management (P&L)



- Reducing cash flow and earnings volatility.

- Managing the costs of financing costs (e.g. through the use of derivatives).



- Increasing the value of a company's shares. By reducing financial volatility, it can lower the cost of capital which can increase profits and value of a company.



- Management of operating costs by managing fluctuations.

# Health and Safety management



## The costs of failure

Health and safety law is Criminal Law

Failure to manage health and safety can result in:

- ❖ prosecution, fines and imprisonment
- ❖ compensation claims
- ❖ loss of output or service
- ❖ replacement costs
- ❖ loss of reputation
- ❖ Death, injury,





# Security Risk Management



## Five-level national alert system

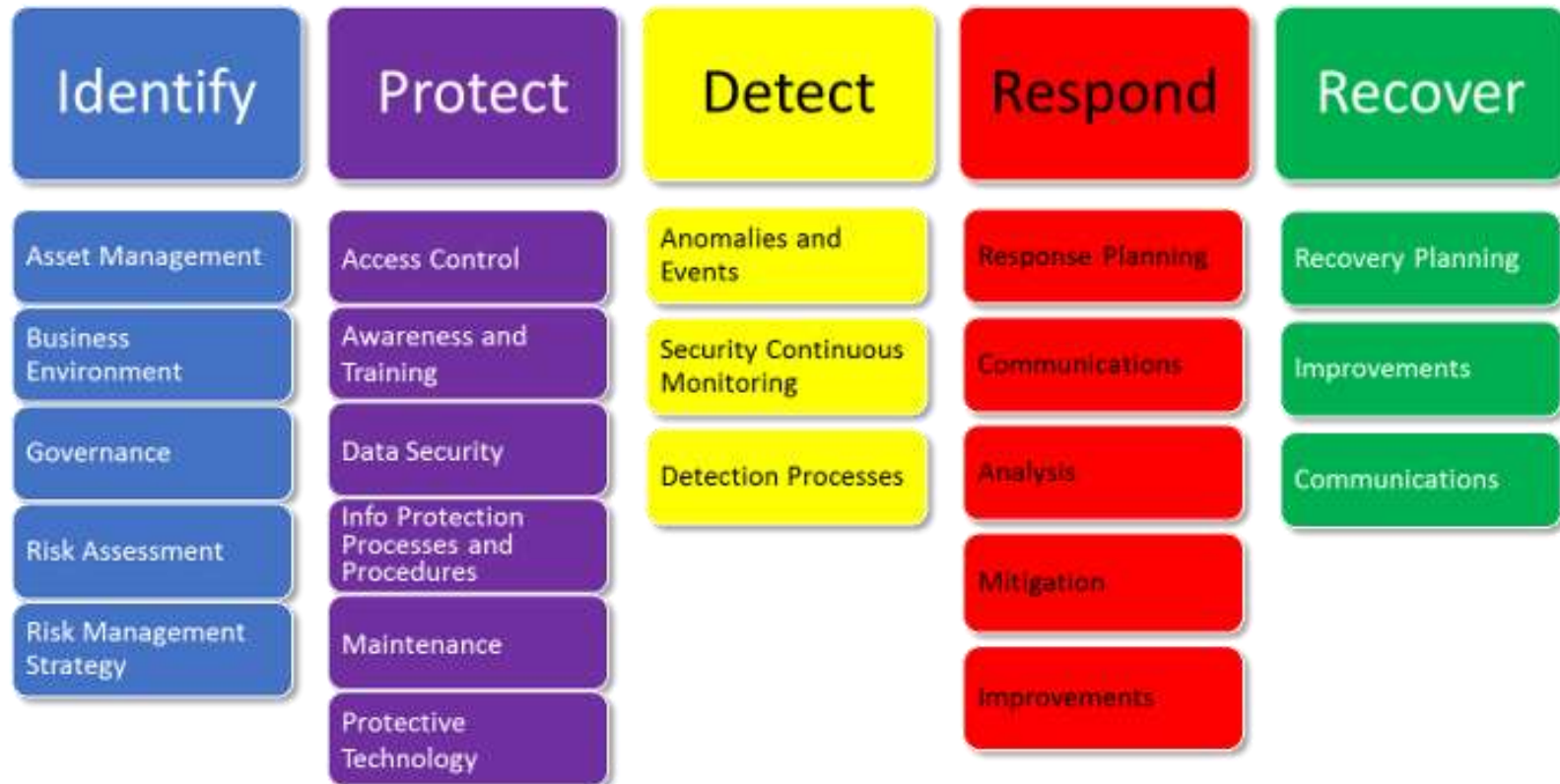
COLOR CODE	CONDITION LEVEL	RECOMMENDED PROTECTIVE MEASURES
<b>GREEN</b>	<b>LOW</b> <i>Low risk of terrorist attacks</i>	<ul style="list-style-type: none"><li>- Refine security plans</li><li>- Assess facilities for vulnerabilities</li></ul>
<b>BLUE</b>	<b>GUARDED</b> <i>General risk of terrorist attacks</i>	<ul style="list-style-type: none"><li>- Check emergency communications</li><li>- Review and update emergency-response plans</li></ul>
<b>YELLOW</b>	<b>ELEVATED</b> <i>Significant risk of terrorist attacks</i>	<ul style="list-style-type: none"><li>- Increase surveillance of critical locations</li><li>- Coordinate emergency plans with nearby towns</li></ul>
<b>ORANGE</b>	<b>HIGH</b> <i>High risk of terrorist attacks</i>	<ul style="list-style-type: none"><li>- Take precautions at public events</li><li>- Restrict access to essential personnel</li></ul>
<b>RED</b>	<b>SEVERE</b> <i>Severe risk of terrorist attacks</i>	<ul style="list-style-type: none"><li>- Monitor or redirect transportation systems</li><li>- Close public and government facilities</li></ul>



# Cyber Risk Management



## NIST Cyber Security Framework



# Leadership...







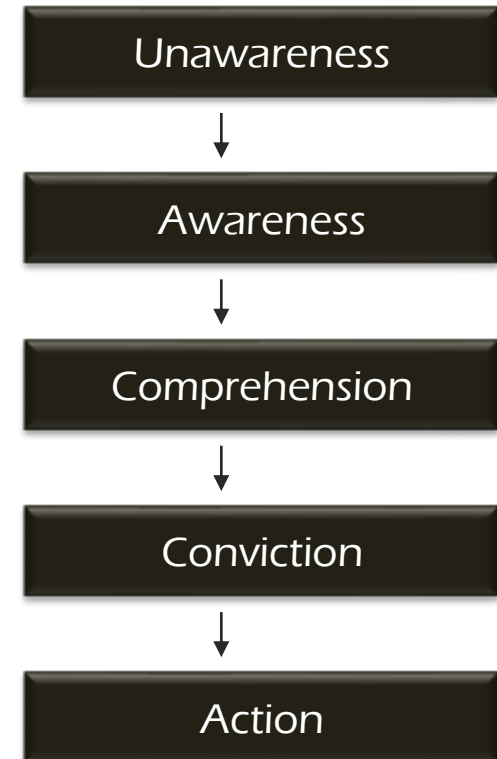
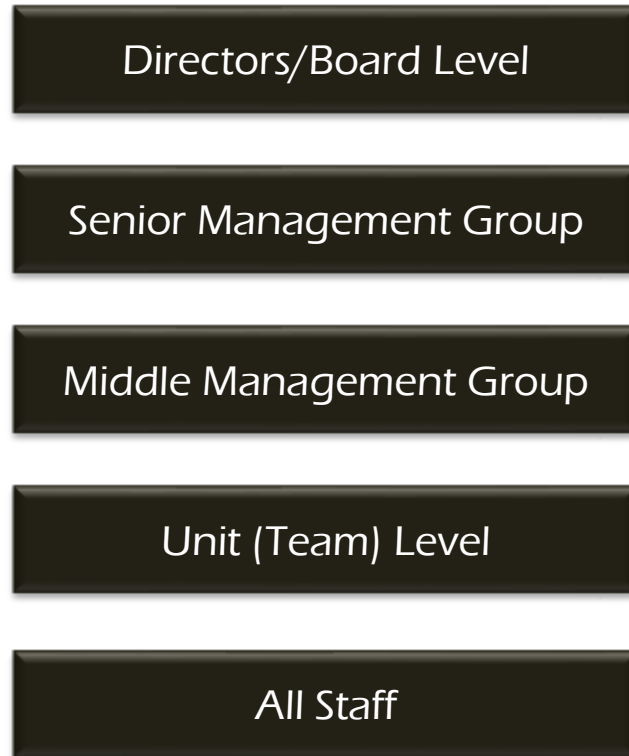
## Embedding ERM Culture – Challenges!

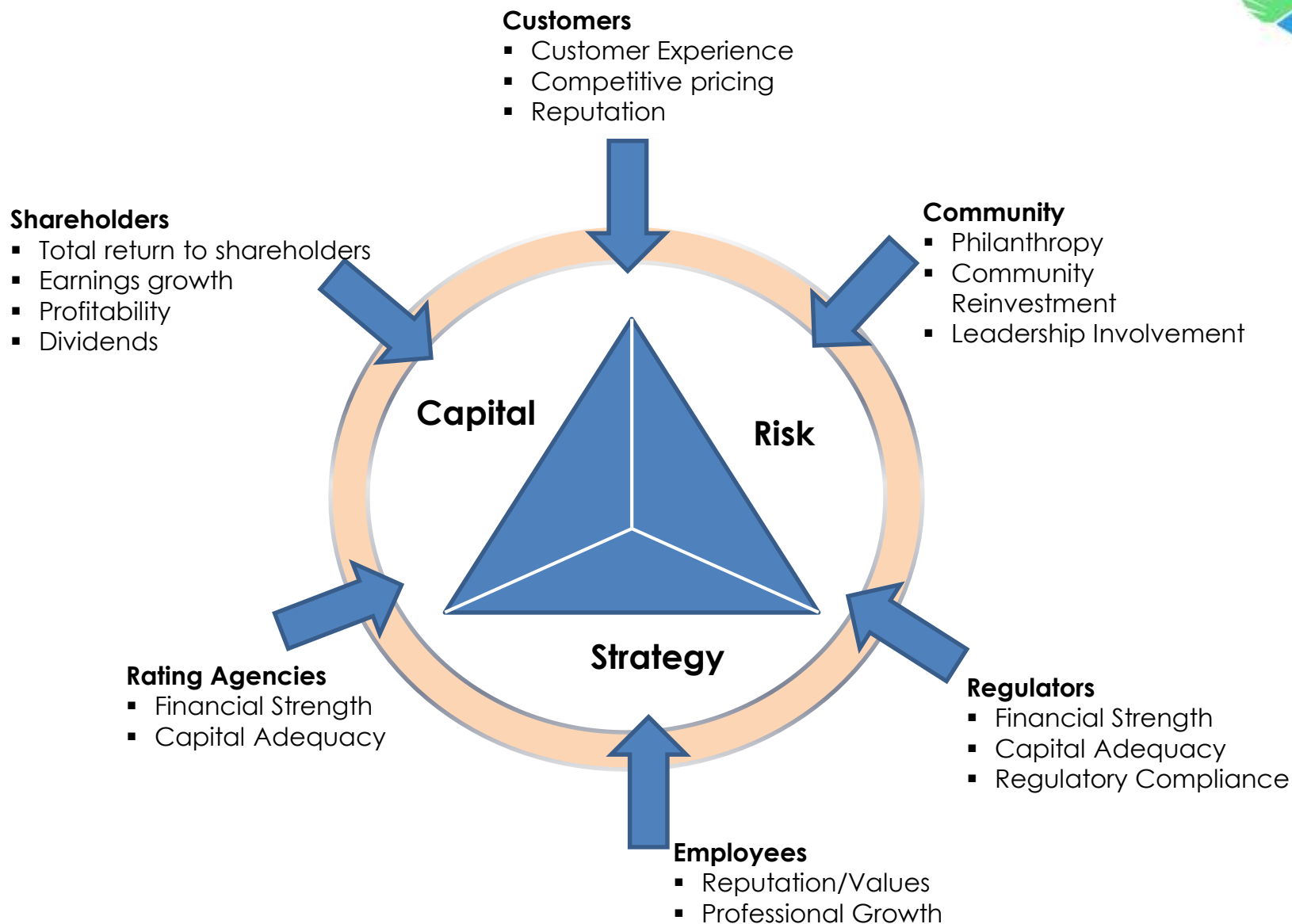
- Lack of real commitment from the top
- Insufficient or lack of continuous evidence of the value added benefits of ERM
- Not effectively integrated into business models/processes
- Assumptions (Risk Measurement vs. Management)
- “Risk Champion” lacks the ability to communicate the benefits of RM in a creative or inspirational manner



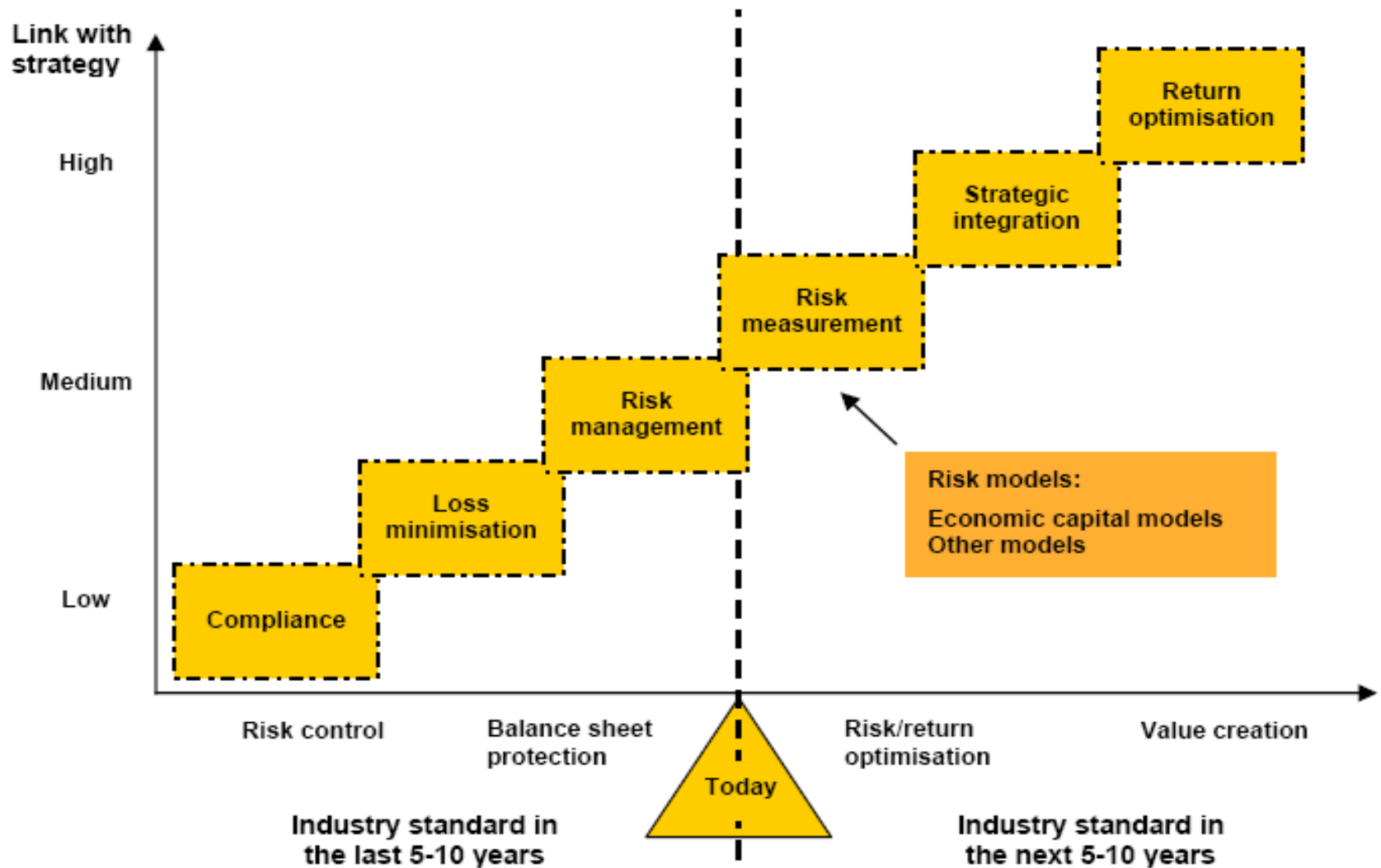
# Risk Communication Maturity Model

- a journey of change





# Evolution of Enterprise Risk Management



*'The Role of ERM in Ratings', Mark Puccia, Managing Director, Standard & Poor's  
March 30, 2007*



# Questions & Contact



## **Joachim A Adenusi**

Partner – Inspirational Risk

Tel no: +44 7947 182 934 (m)

E-mail: [jadenusi@inspirationalrisk.com](mailto:jadenusi@inspirationalrisk.com)

Web: [www.inspirationalrisk.com](http://www.inspirationalrisk.com)

Twitter: @Joachim\_Adenusi

@inspired\_risk