Risk Management

Seminar – June 2017

Compiled by:

Raaghieb Najjaar, Yaeesh Yasseen & Rashied Small

SOUTH AFRICAN INSTITUTE OF
PROFESSIONAL ACCOUNTANTS™
YOUR WEALTH

Defining Risk

- **Risk reflects the chance that the actual event may be different than the planned / expected event.**
- **The effect of an uncertainty that could have a negative impact on achieving the business objectives.**
- **Upside risk – the uncertainty of the possibility of making gains (potential opportunities)**
- **Downside risk - the probability that losses or negative outcomes will occur (mitigate negative outcomes)**

Brain Teaser #1

Discuss whether the following represents a risk to the organisation:

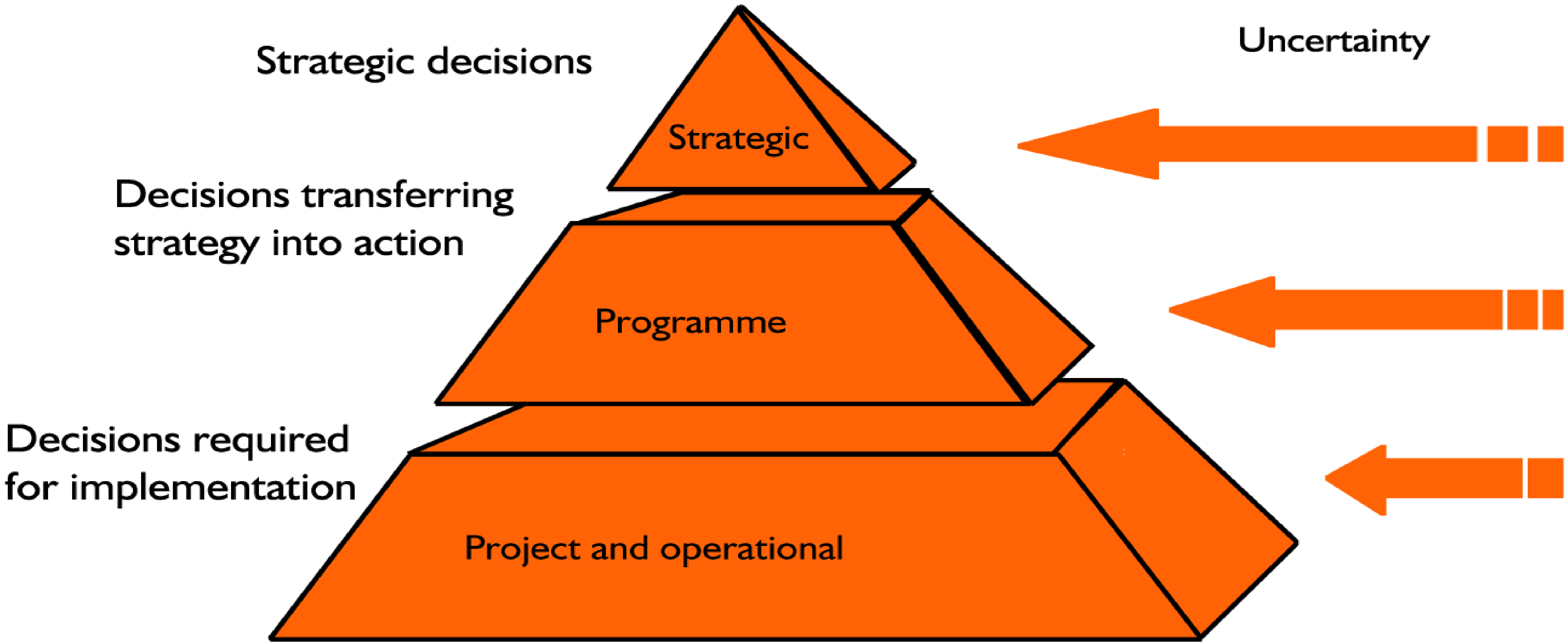
1. **The organisation budgeted an annual amount of R 3.7 million for salaries and wages. The actual expenses incurred amounted to R 4 million.**

2. **The organisation budgeted and amount of R 26 million for revenue. The accounting recorded reflected an annual revenue of R 31,2 million.**

3. **The business owner is prepared to take any income generating opportunity irrespective of the potential losses.**

4. **The business organisation strategic objectives is to maximise profit.**

Hierarchy of Risk



Brain Teaser #2

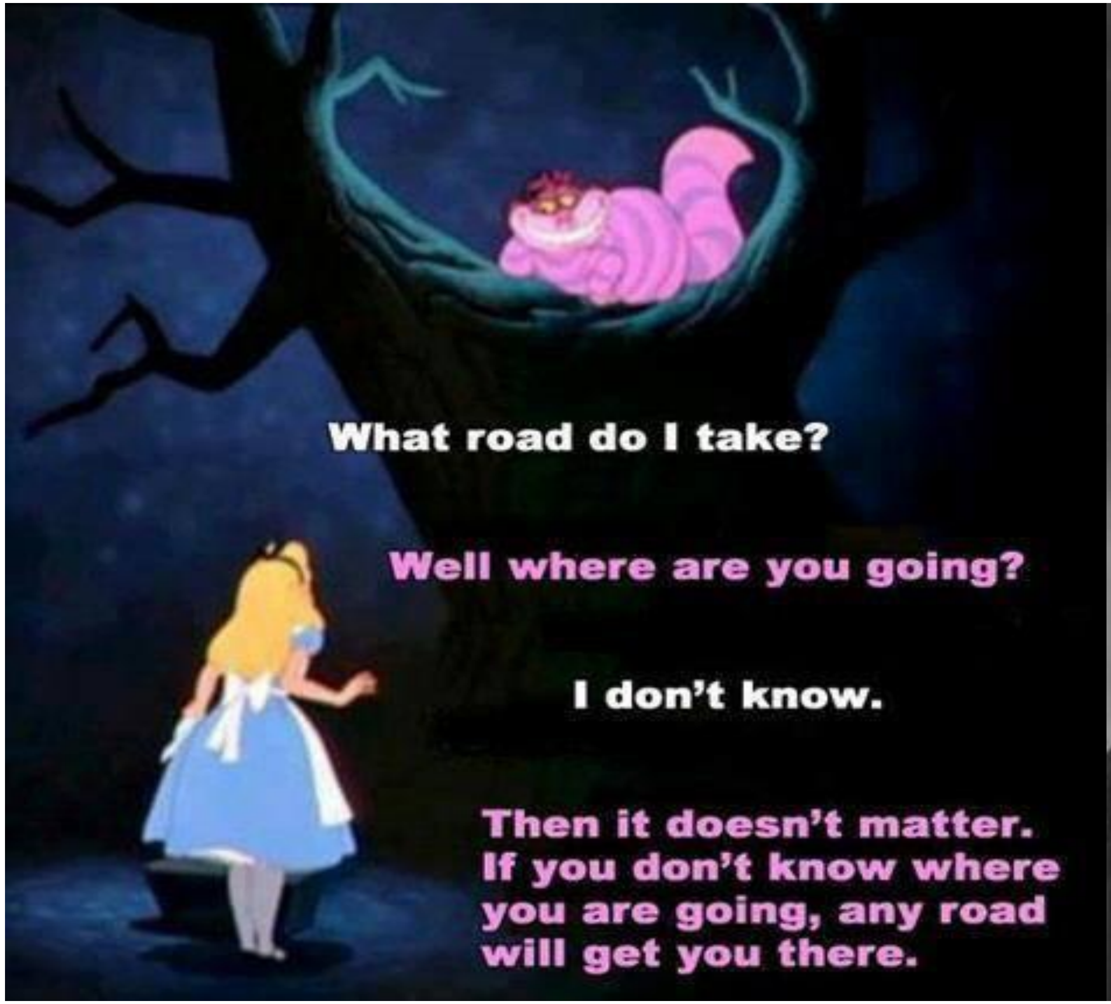
Discuss whether the following statements are True / False:

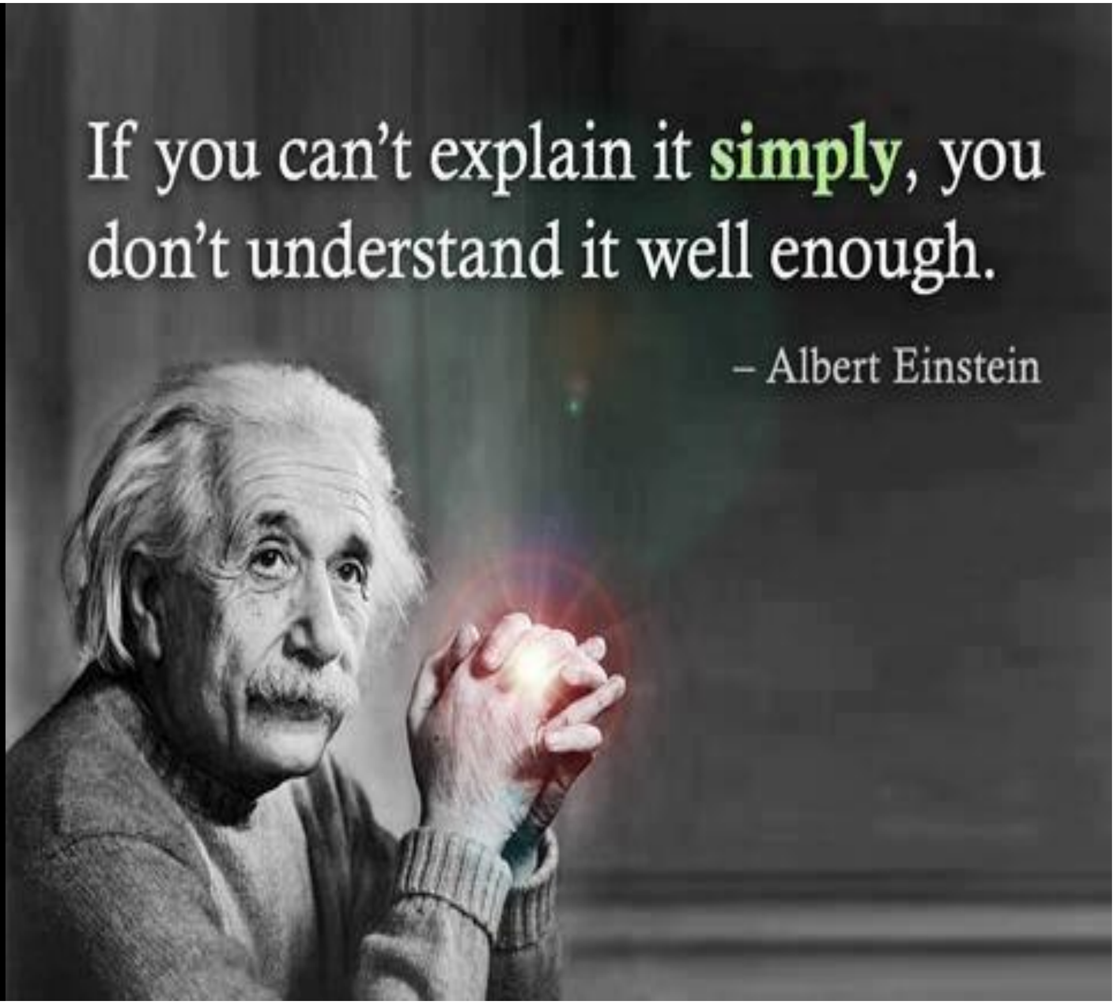
1. **An organisation with no strategic objective or goal seldom encounters risk in its business activities.**

2. **An organisation with a clearly defined strategic objective is more likely to manage potential risk.**

3. **The potential for risk occurring at operational level is often attributed that managers do not take accountability.**

Understanding Risk





Brain Teaser #3

Discuss whether the potential risks and/or challenges encountered in:

1. **An accounting practice**

2. **An organisation conducting business locally and internationally**

Types of Risks

Business/Operational Risk:

- Strategy risk
- Product risk
- Operating risk

Financial Risk:

- Cash flow risk
- Credit risk
- Liquidity risk
- Interest rate risk
- Currency risk

Environmental Risk:

- Political risk
- Economical risk
- Social risk
- Technological risk

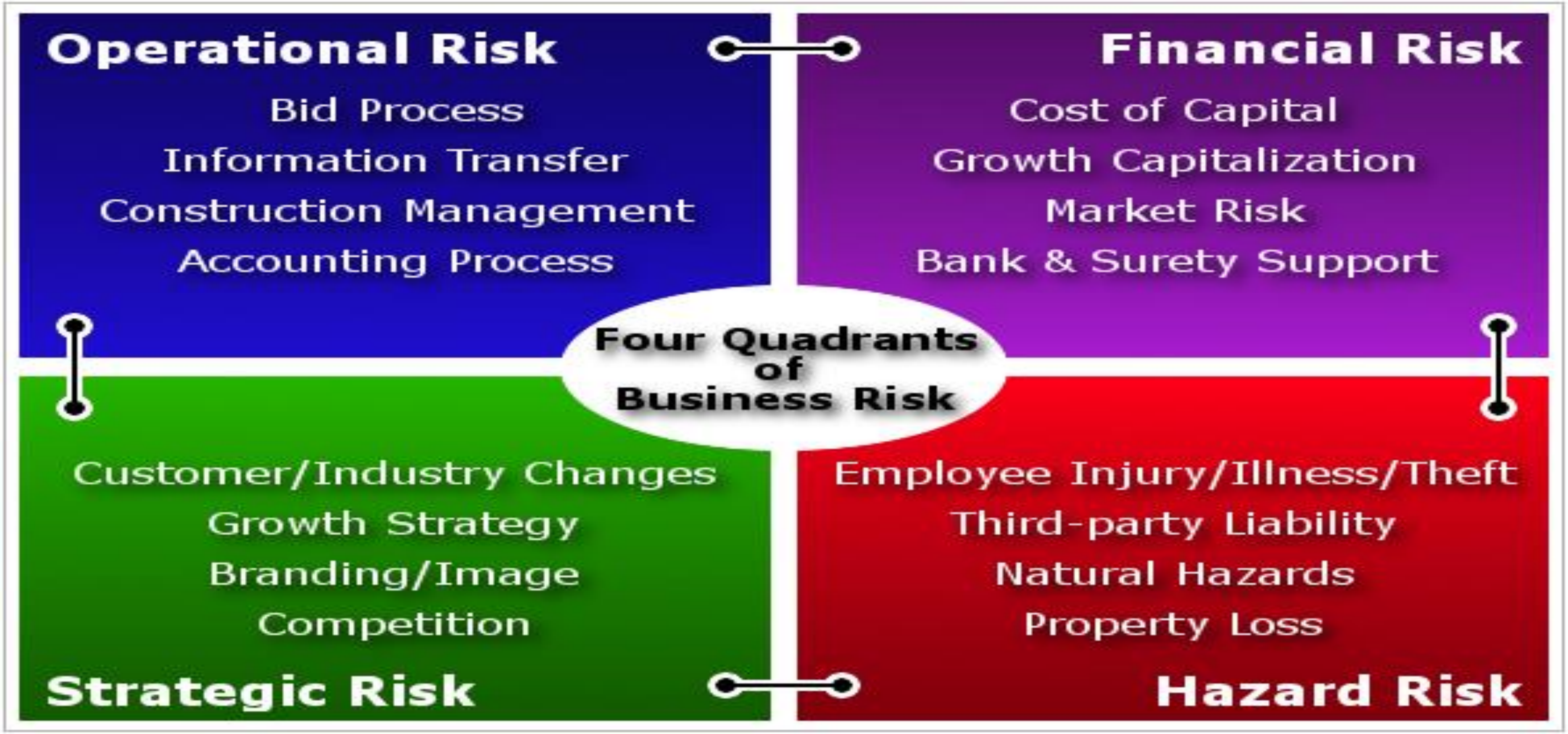
Reputational Risk:

Enterprise Risk

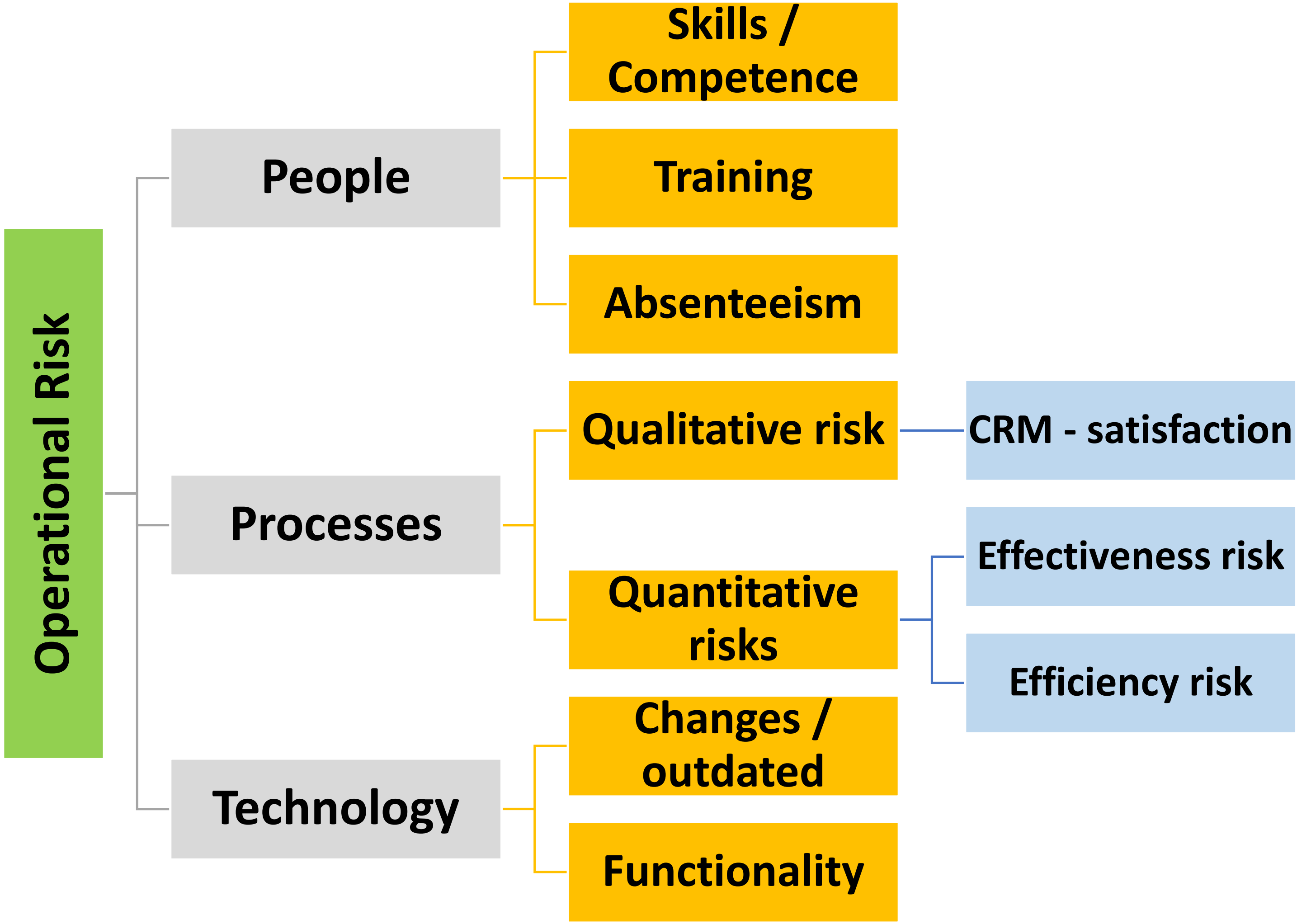
Types of Business Risks

Figure 2 Risks to business

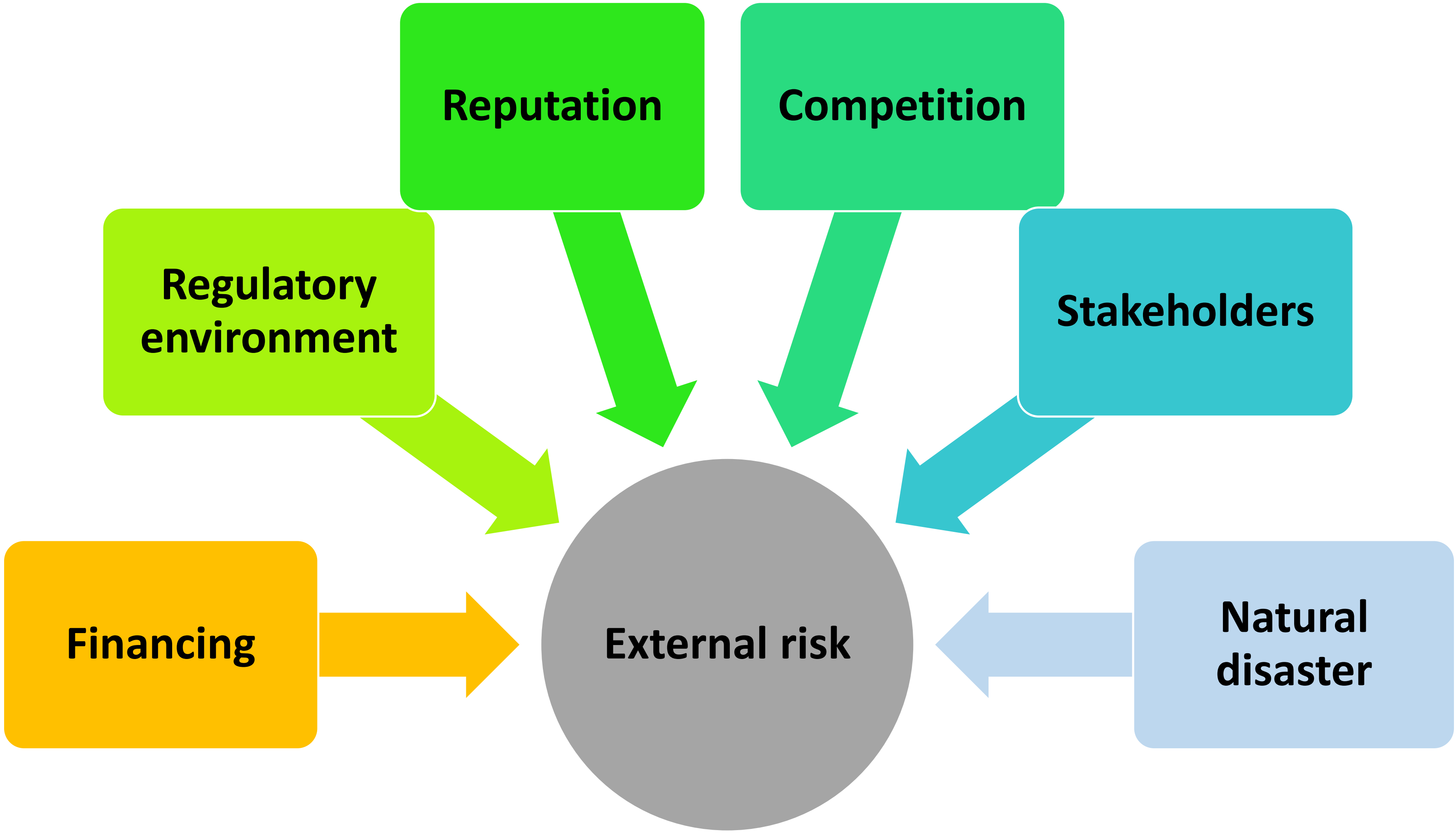
Business Risks



Internal Operational Risks

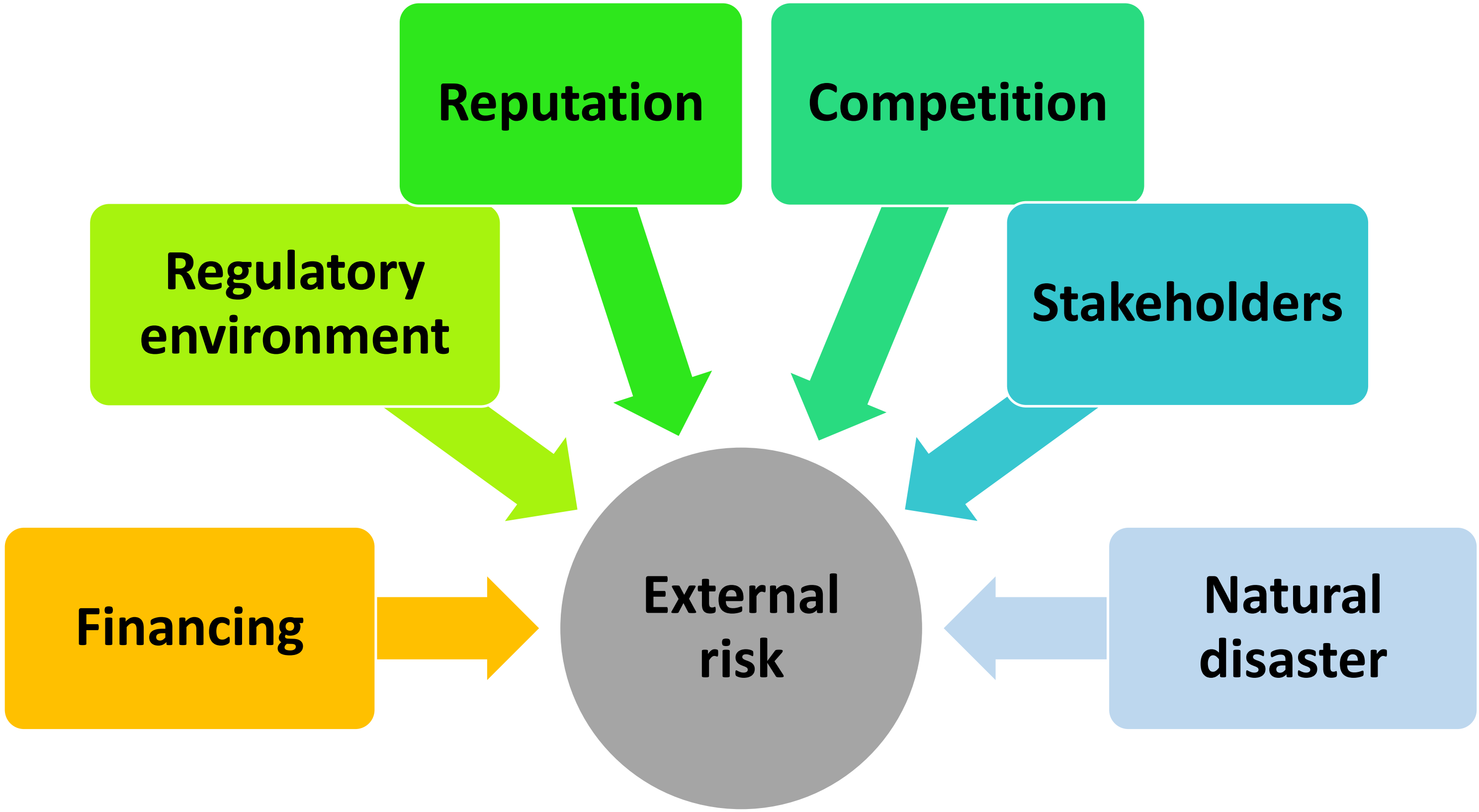


External Risks



Brain Teaser #4

Discuss and rate (scale of 1 – 10) the external risks encountered by the Professional Accountant:

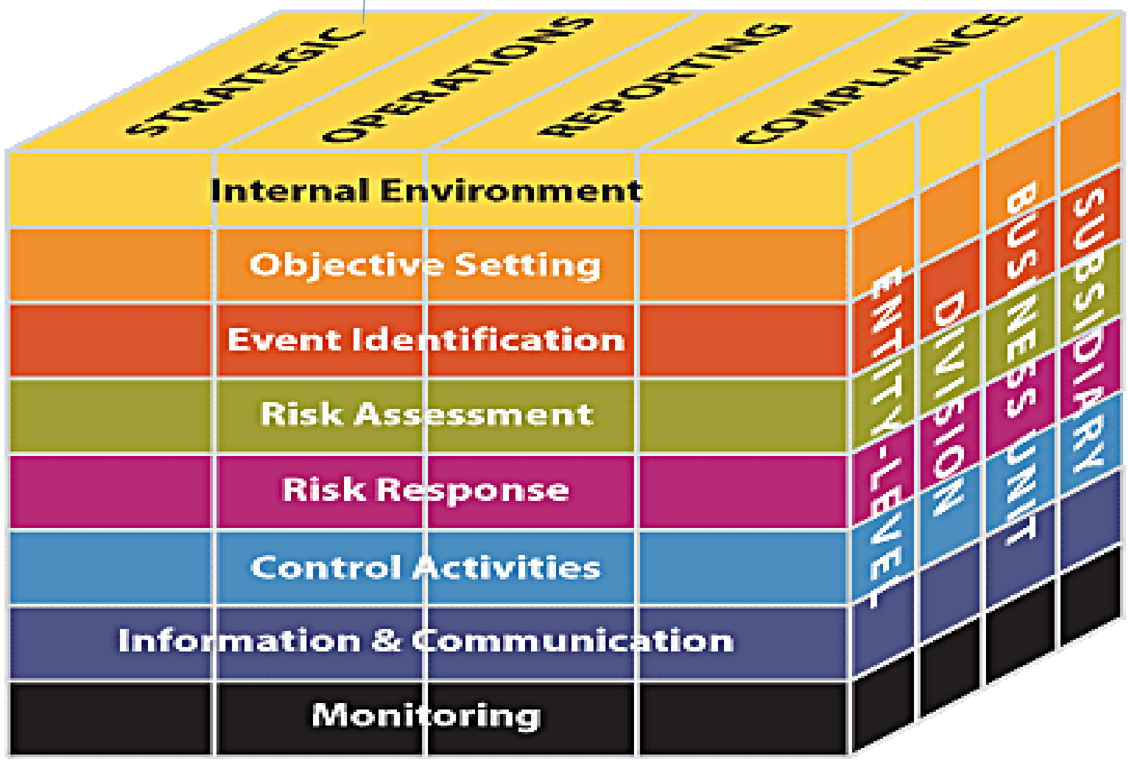


Risk Management

- **Risk management refers to the process designed to reduce or eliminate the risk of certain kinds of events happening or having an impact on the business - process for identifying, assessing and prioritizing risks.**

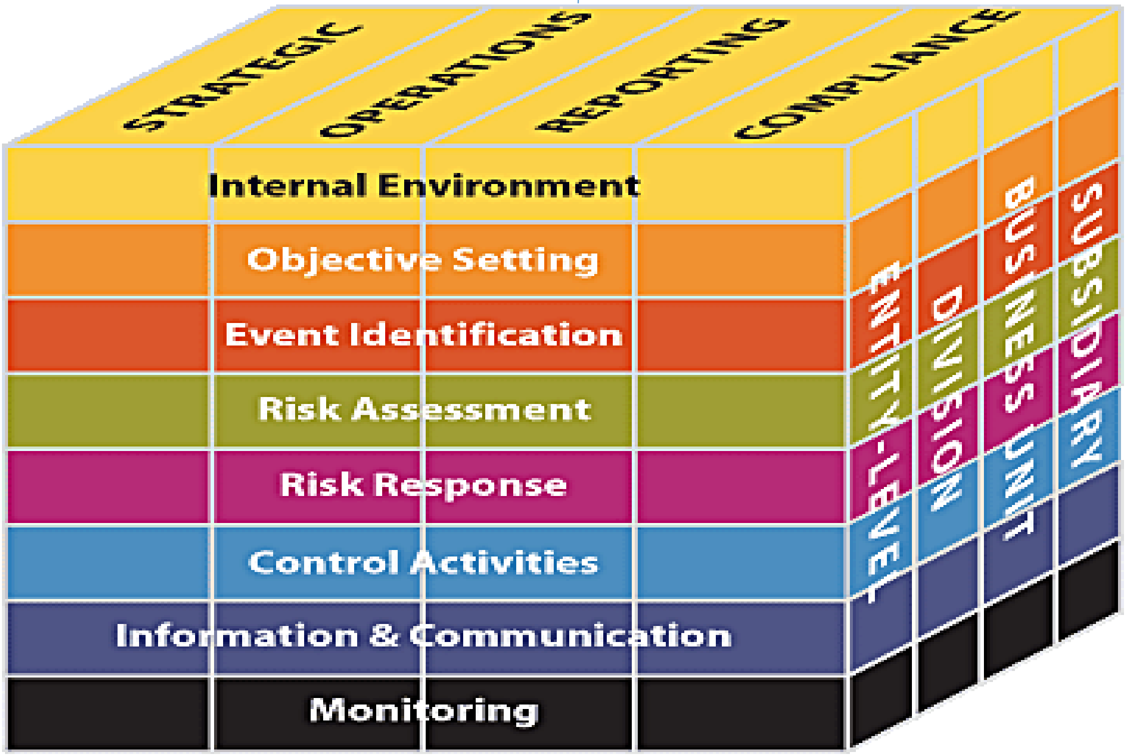
- **Enterprise Risk Management is defined as “a process, effected by an entity’s board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” - COSO**

ERM – Strategic Level



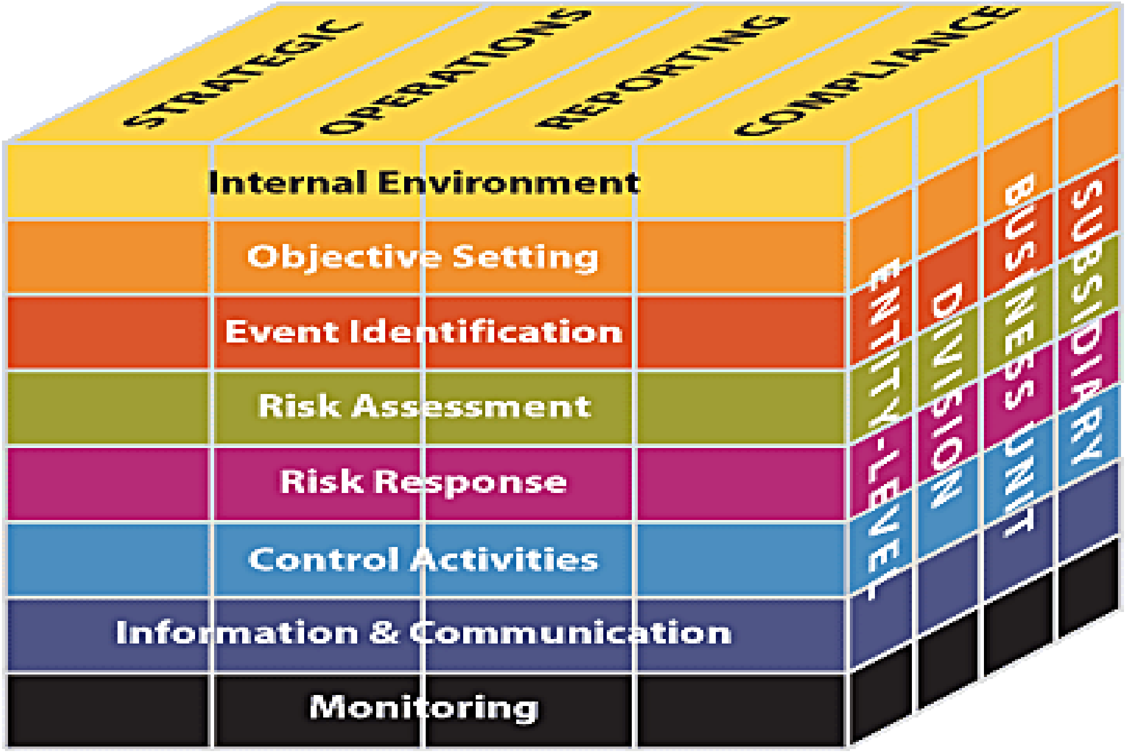
These are the high level goals that are aligned with and support the institution's mission.

ERM – Operations Level



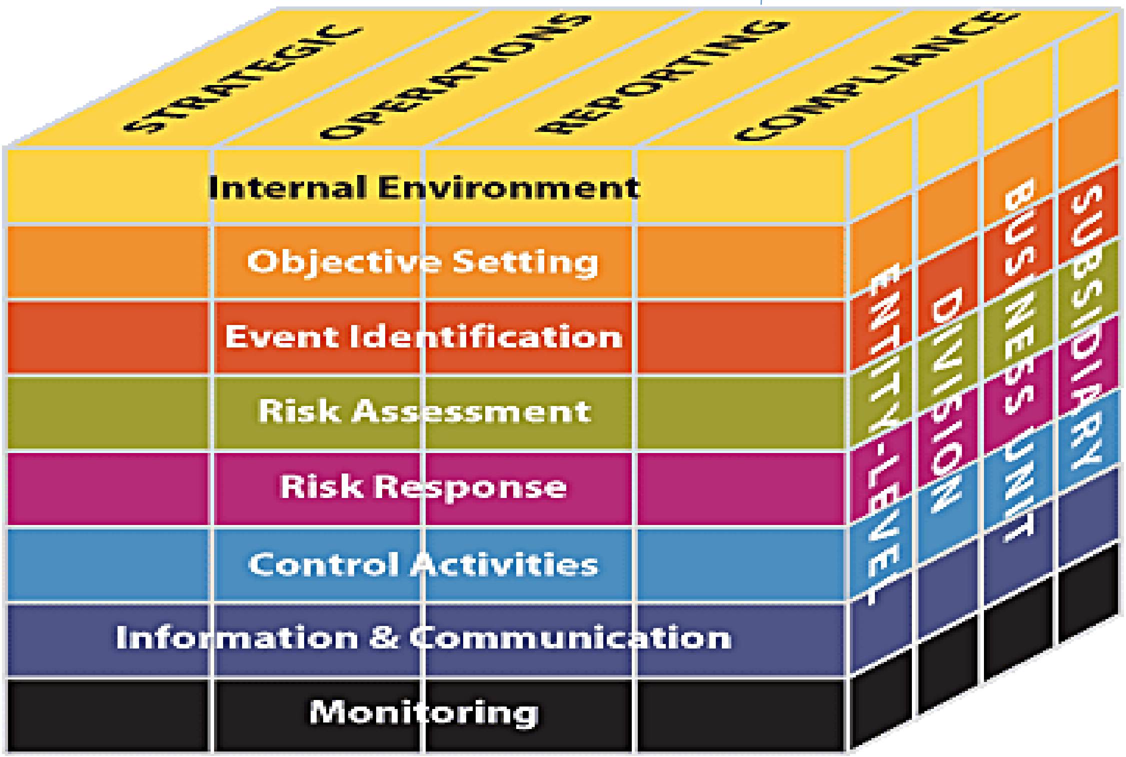
Relate to the ongoing management process and daily activities of the organization.

ERM – Reporting Level



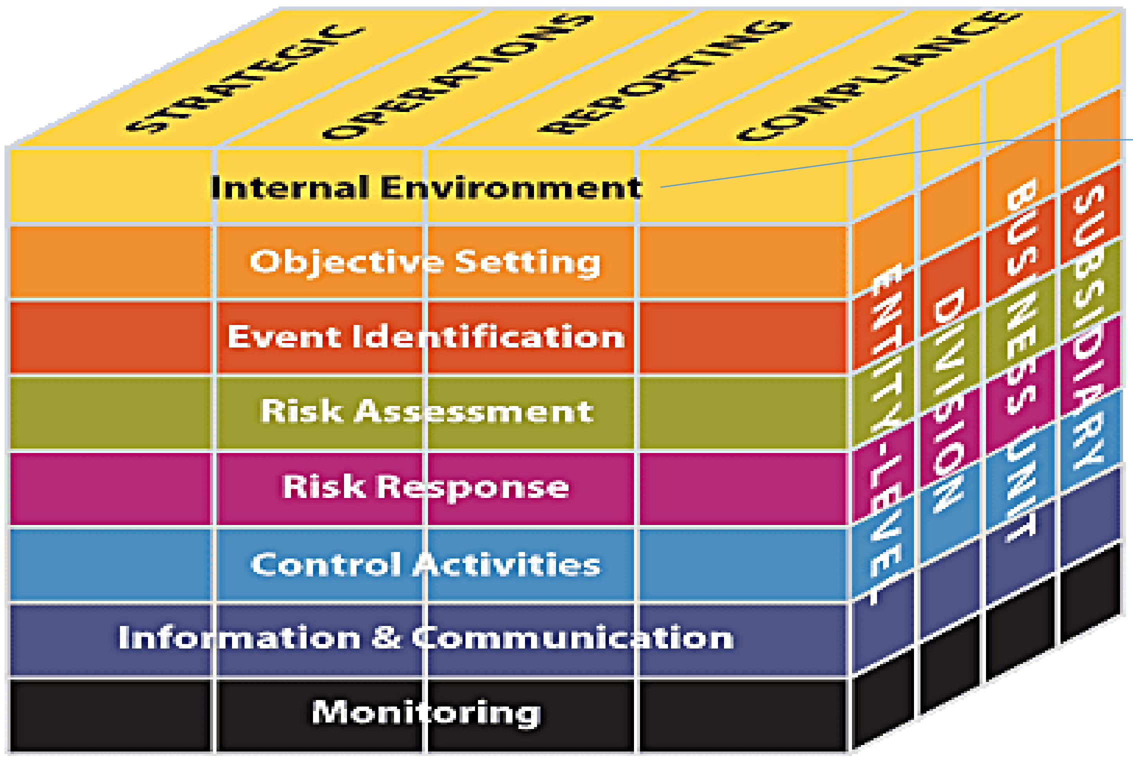
Relates to the organization's adherence to applicable laws and regulations.

ERM – Compliance Level



Relates to the protection of the organization's assets and quality of financial reporting.

ERM – Operations Level



The Internal Environment relates to the general culture, values and environment in which an organization or entity operates (e.g. tone at the top)

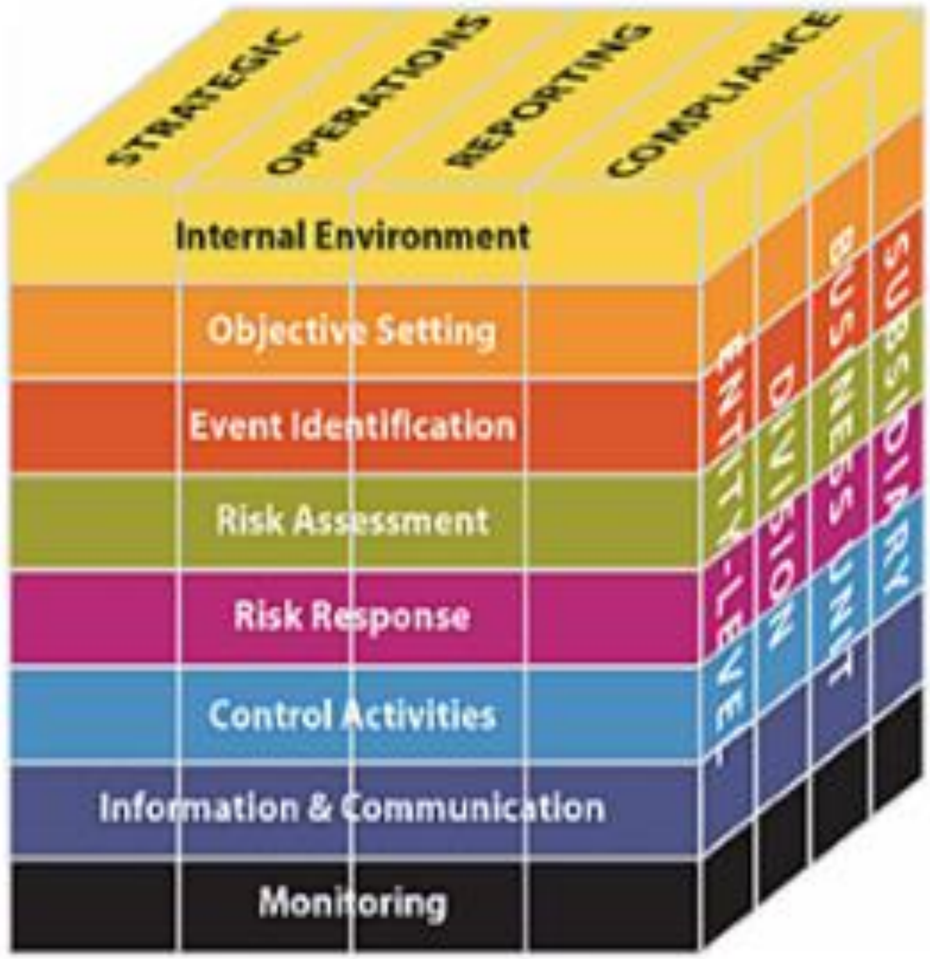
Risk Management Model

Risk Management Process

Establishing the Risk Context

- **Establish the context by identifying the objectives of the project, event or relationship and then consider the internal and external parameters within which the risk must be managed.**

- **Establishing the context sets the framework within which the risk assessment should be undertaken, ensures the reasons for carrying out the risk assessment are clearly known, and provides the backdrop of circumstances against which risks can be identified and assessed.**



Establishing the Risk Context

- **Set the scope for the risk assessment by identifying what you are assessing**

- **Define the broad objectives and identify the reason for the risk assessment**

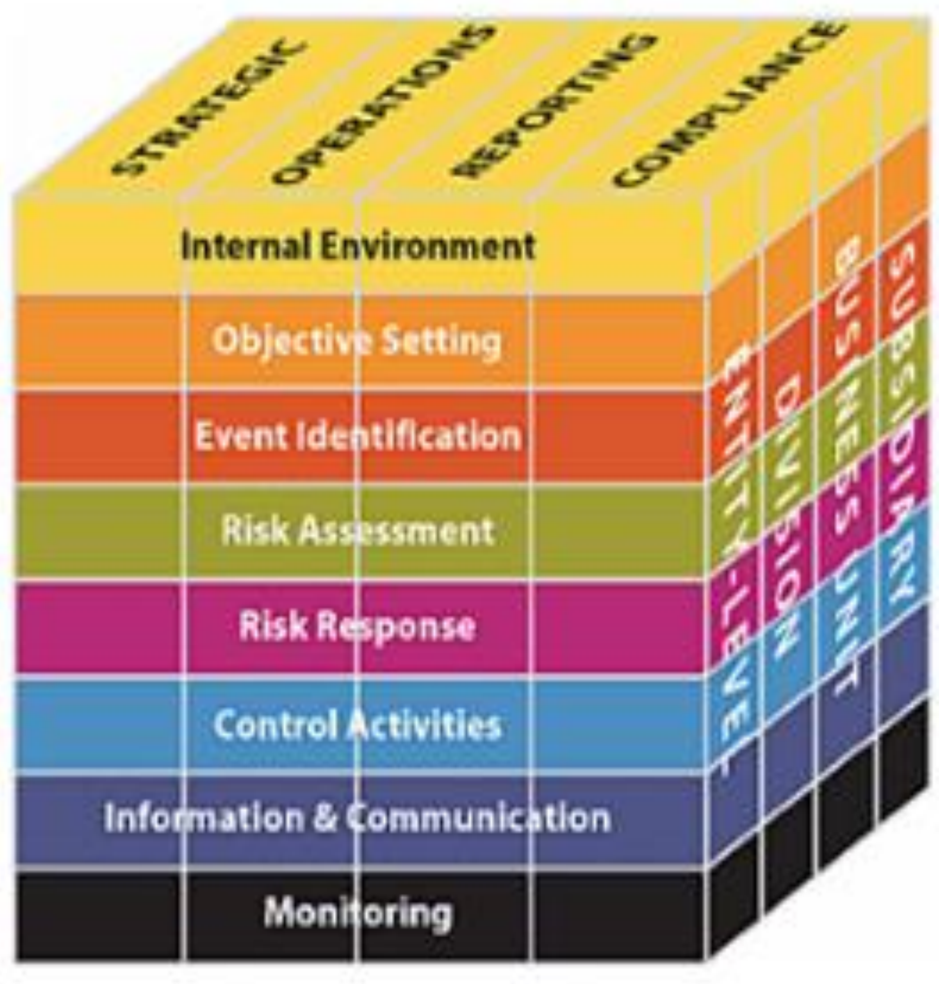
- **Identify the relevant stakeholders, the areas that might be impacted and seek their input - inclusive process**

- **Gather background information by ask the right people and identify the information that is available as well as information that is not available (immediately) but may be necessary**

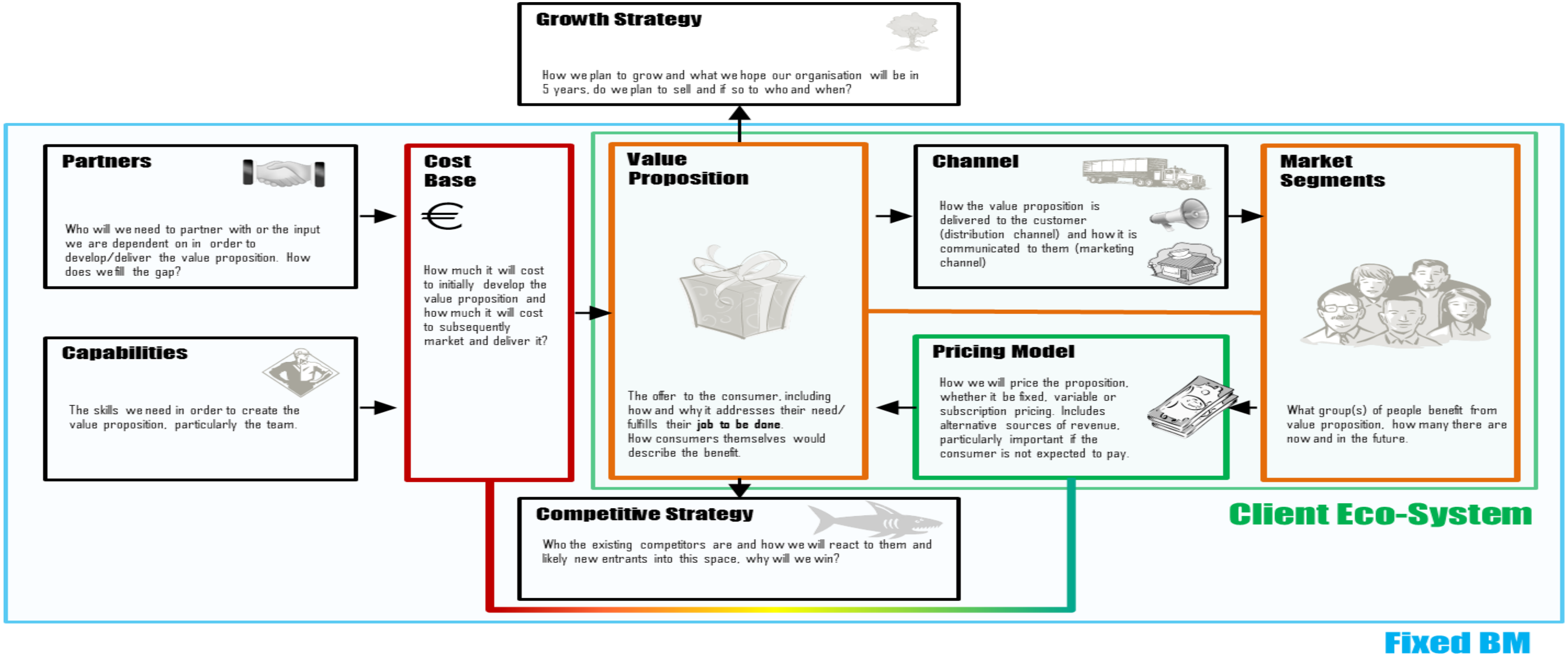
Establishing the Risk Context

When gathering information consider:

- **Strategic & business plans**
- **Reports such as financial statement, inspections, site visit**
- **Personal experience of staff**
- **Corporate knowledge & ‘institutional memory’**
- **Previous event investigations or reports**
- **Surveys, questionnaires and checklists**
- **Insurance claim reports**
- **Business experience (local or international)**
- **Structured interviews or Focus group discussion**
- **Historical records**

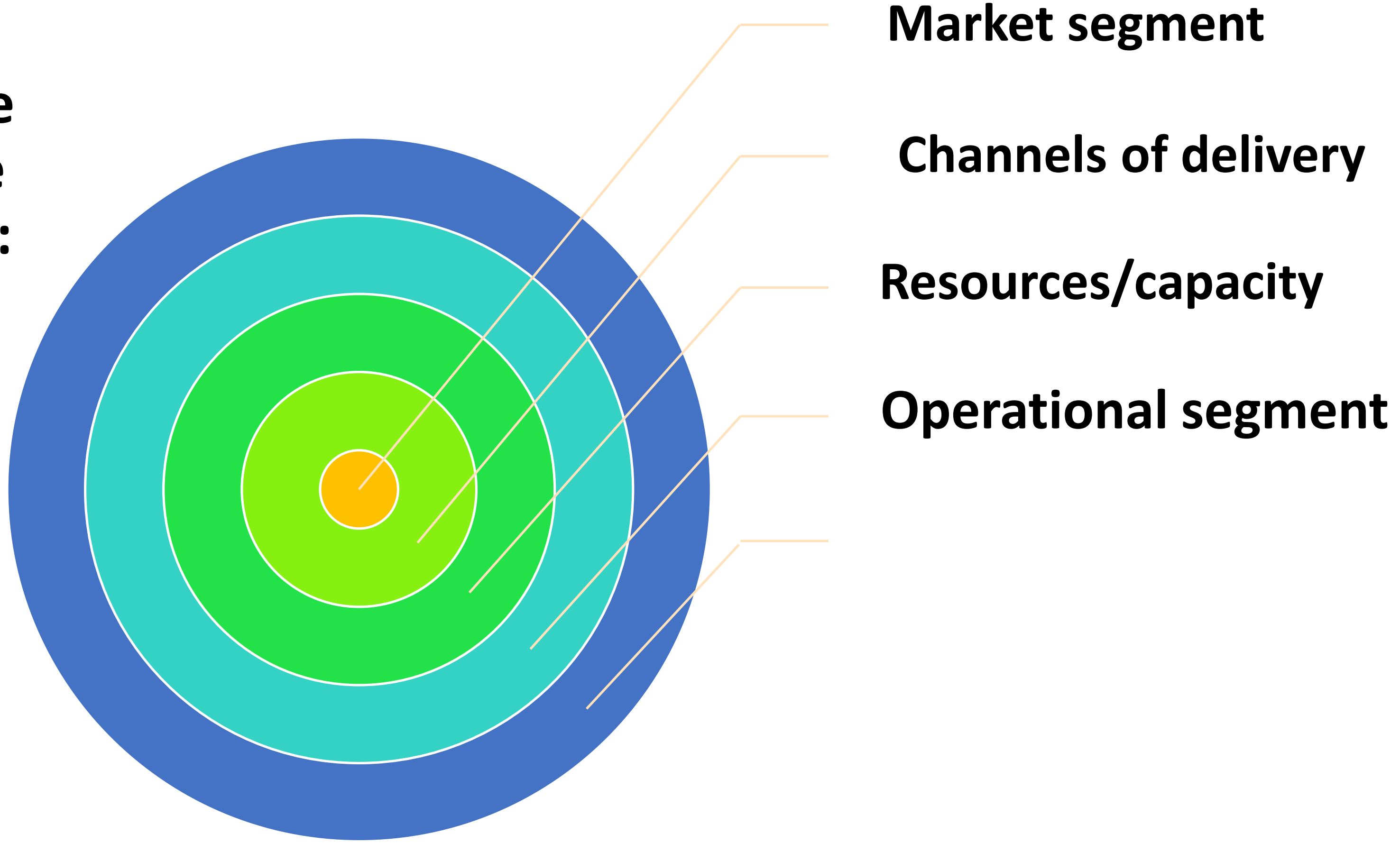


Context of Risk - Business Model

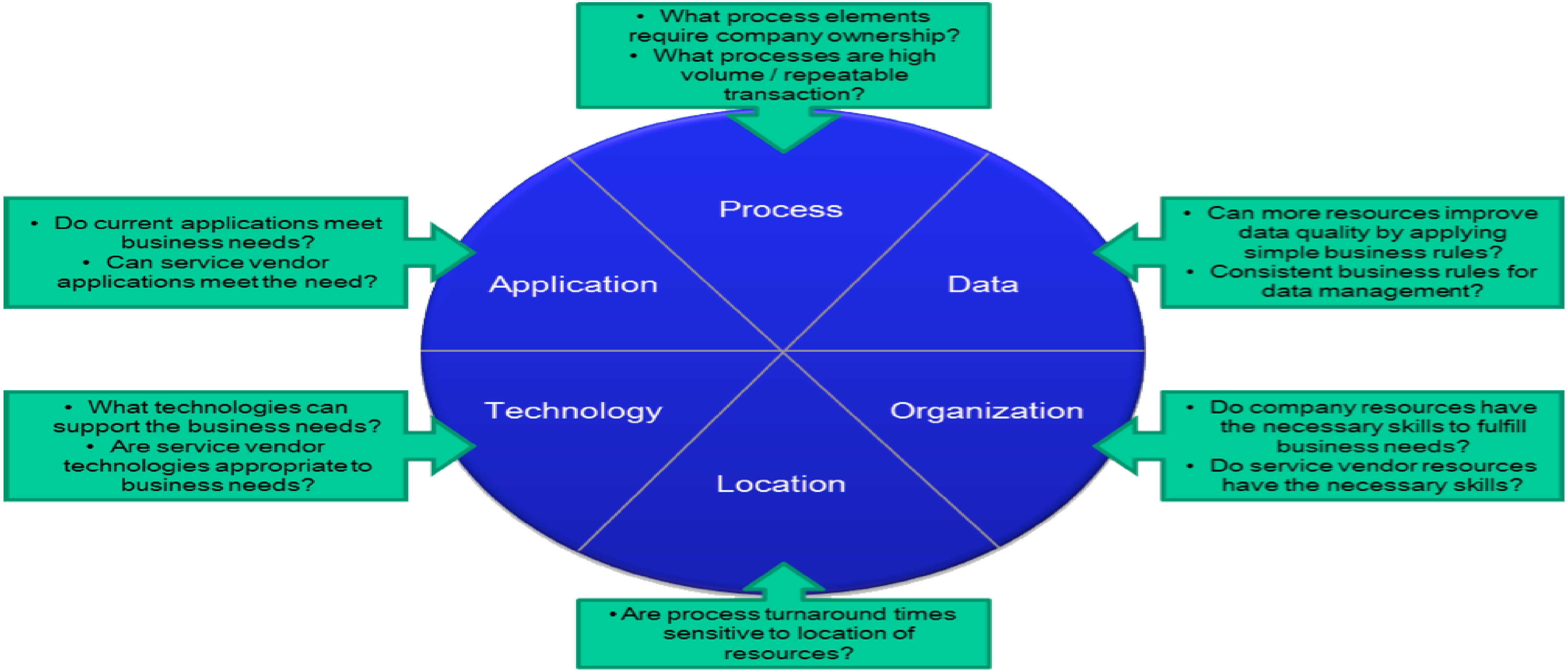


Brain Teaser #5

Identify possible risks associated with each of the segments in the business model:



Risk Assessment – Business Model



Porter’s 5 Forces

Establishing the Risk Context

Identification of Risk

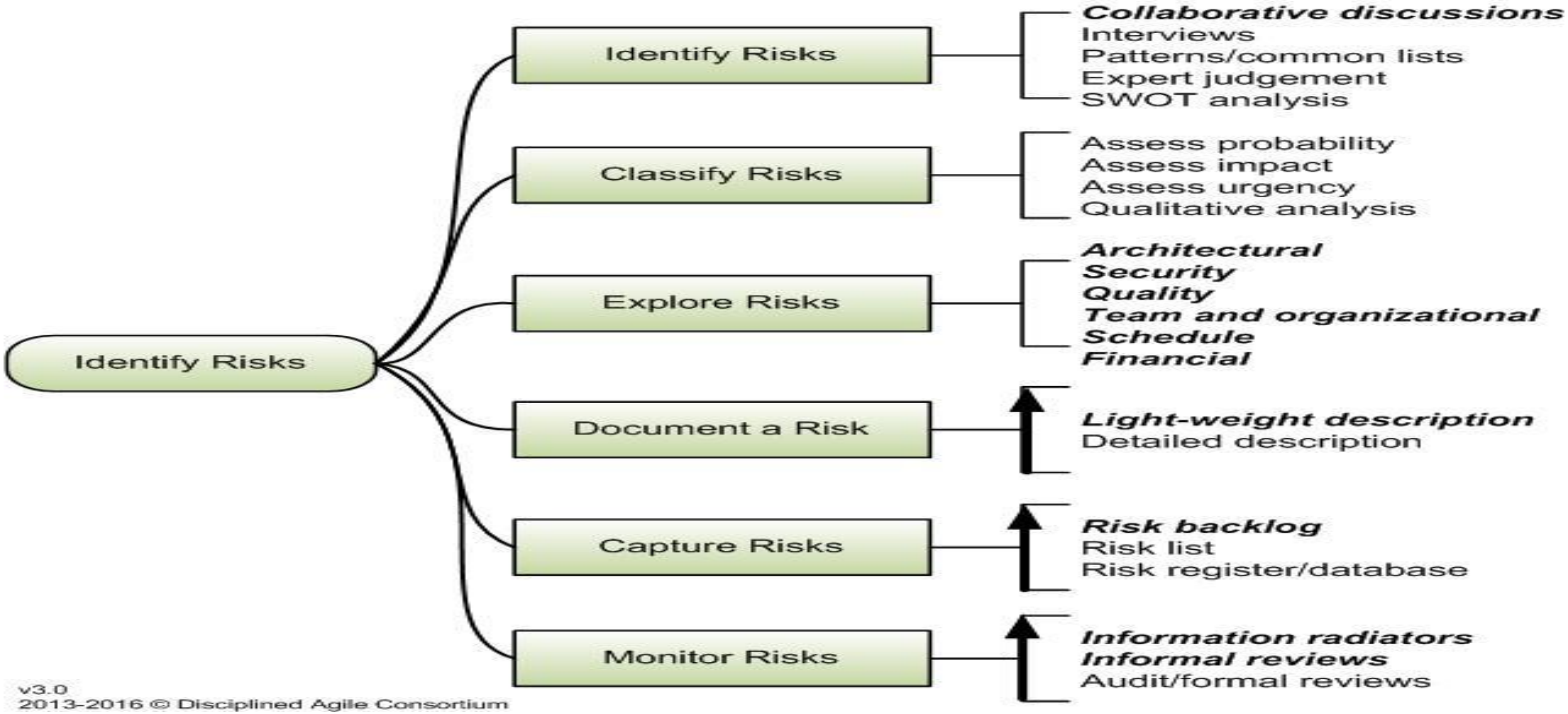
- **Risk identification involves identifying sources of risk, areas of impact, events and their causes and consequences - risk of doing nothing and missing an opportunity**

- **Identify sources of the risk, areas of impact, events (including changes in circumstances) and their causes and potential consequences**

- **Describe those factors that might create, enhance, prevent, degrade, accelerate or delay the achievement of your objectives.**

Identification of Risk

Identification of Risks

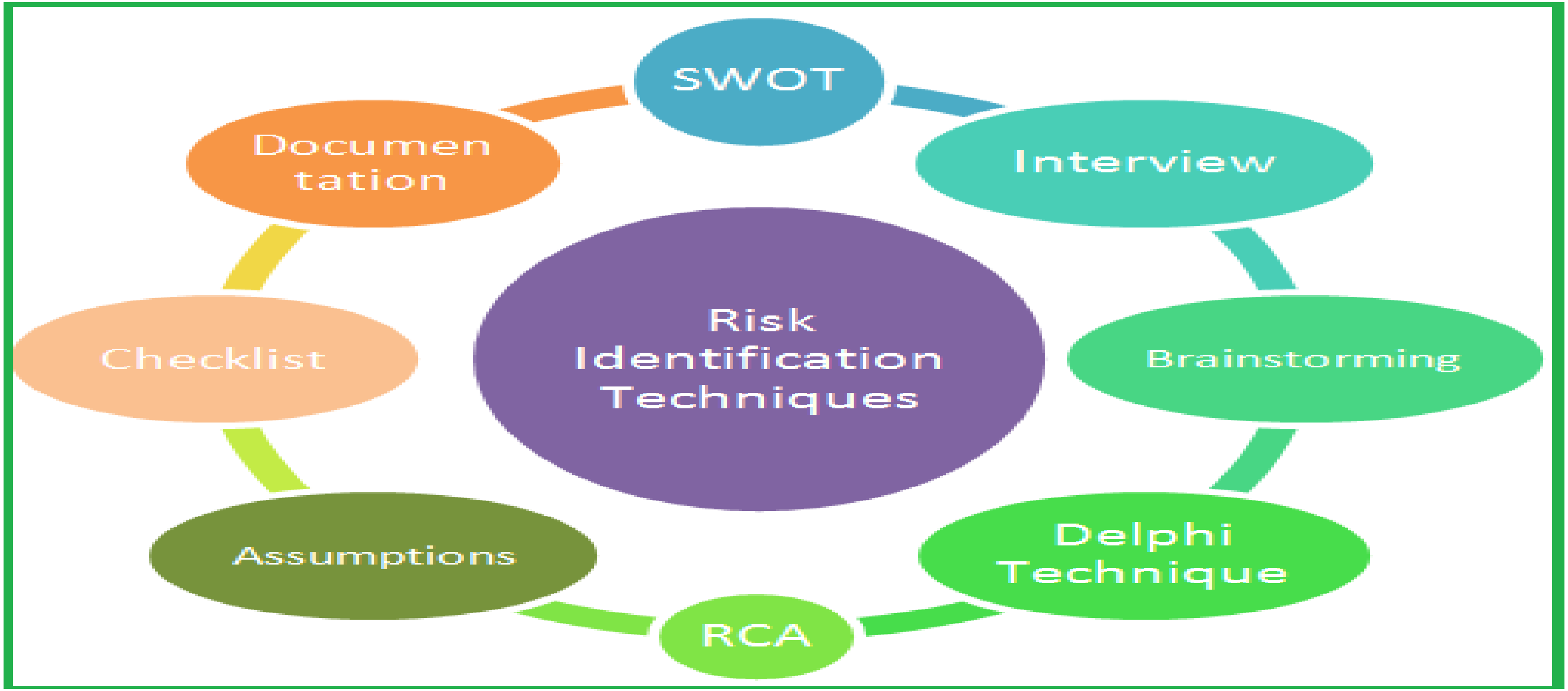


Identification of Risk

- **Identify risks early in the process or project**
- **Identify risks in an iterative and holistic manner**
- **Identify risks with a consistent frequency – ongoing and regularly**
- **Identify risks when change control is performed**
- **Identify risks when major milestones are achieved**

Identifying Risks

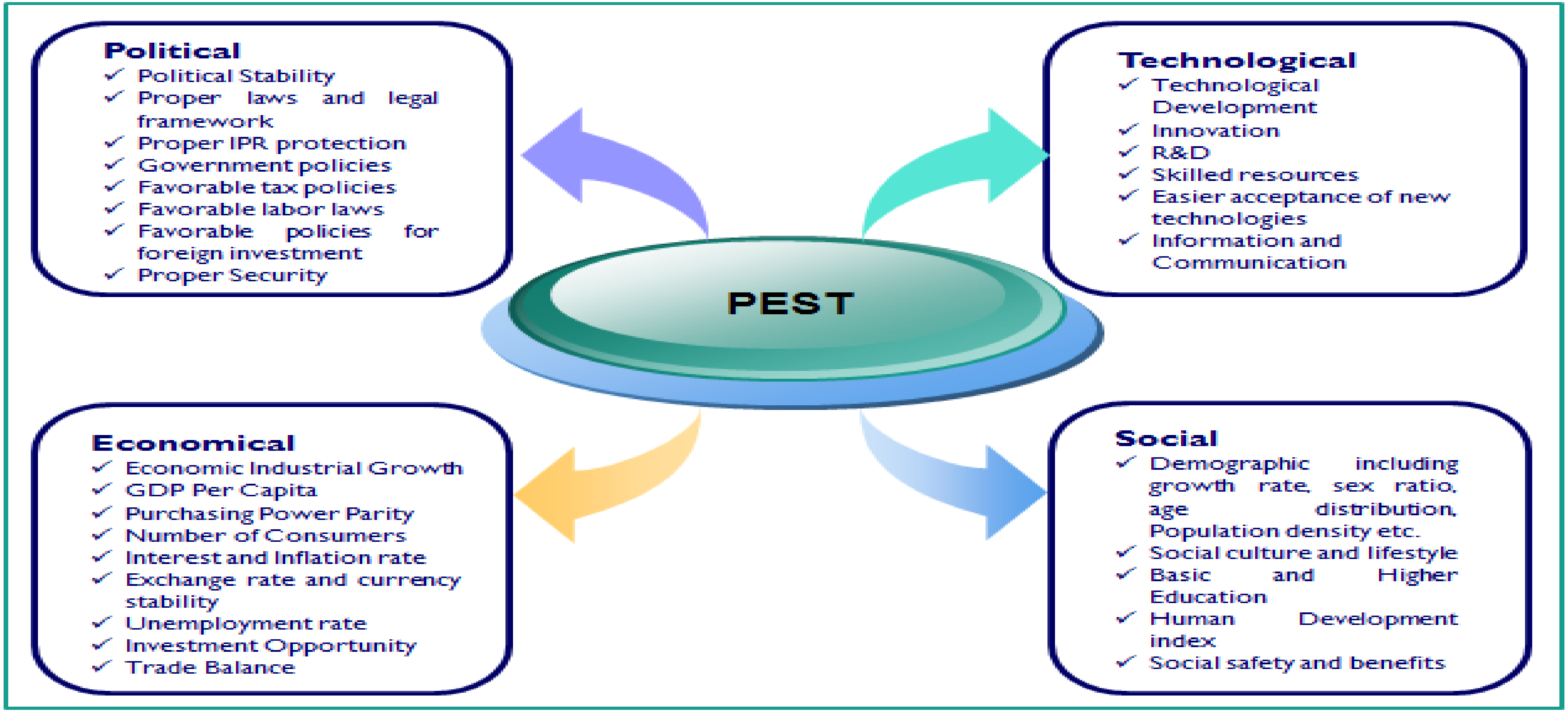
Identification of Risk



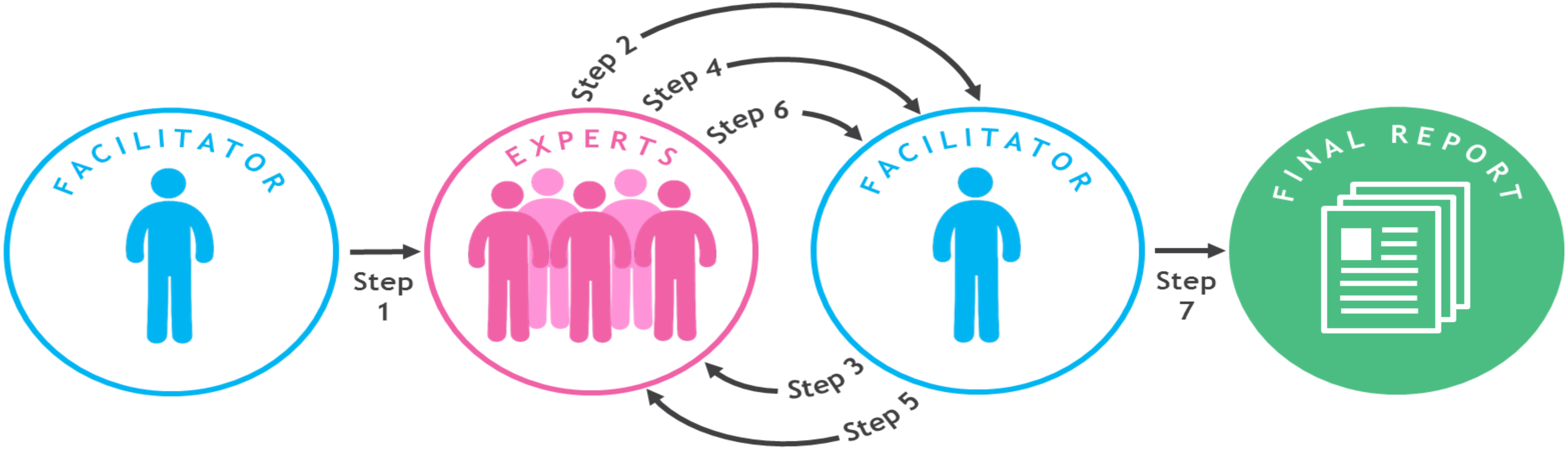
SWOT Analysis

	Favourable	Unfavourable
Internal	**Strengths** • { What are your strengths? } • { What do you do better than • others? } • { What unique capabilites and • resources do you possess? } • { What do others percieve as • your strengths?}	**Weaknesses** • { What are your weaknesses? } • { What do your competitors do • better than you? } • { What can you inprove given the • current situation? } • { What do others percieve as your • weaknesses? }
External	**Opportunities** • { What trends or conditions may • positively impact you? } • { What opportunities are available • to you? }	**Threats** • { What trends or conditions may • negatively impact you? } • { What are your competitors doing • that may impact you? } • { Do you have solid financial • support? } • { What impact do you weaknesses • have on the threats to you? }

PEST Analysis



Delphi Method



Facilitator seeks individual assessments from a pool of experts.

Experts respond to the request, receive feedback and revise their responses.

Facilitator compiles the responses and sends a revised set of questions to each expert. Several cycles of feedback may be needed.

Facilitator produces report on experts' responses, noting key outliers.

Brain Teaser #6

Professional Accountants performing the compilation, review or audit of financial statements use the following statement extracted from the relevant report included in the financial statements to limit their risks when business faces financial and business risk:

"The preparation of the financial statements set out on pages 3 to 13 are the responsibility of the member. We have ascertained that the financial statements are in agreement with the accounting records, summarized in the manner required by section 58(2)(d) of the Act, and have done so by adopting such procedures and conducting such enquiries in relation to the books of accounts and records as considered necessary in the circumstances."

Discuss the possible reasons why the Professional Accountants may be held liable for the financial and business risks faced by organisation.

Identification of Risk - Pitfalls

- **Risks are not identified early when it is less expensive to address**
- **Risks are not identified in an iterative manner**
- **Risk are not identified with appropriate stakeholders**
- **Risk are not identified using a combination of risk identification techniques**
- **Risks are not captured in one location**
- **Risks are not visible and easily accessible.**
- **Risks are not captured in a consistent format (e.g., Cause -> Risk -> Impact).**

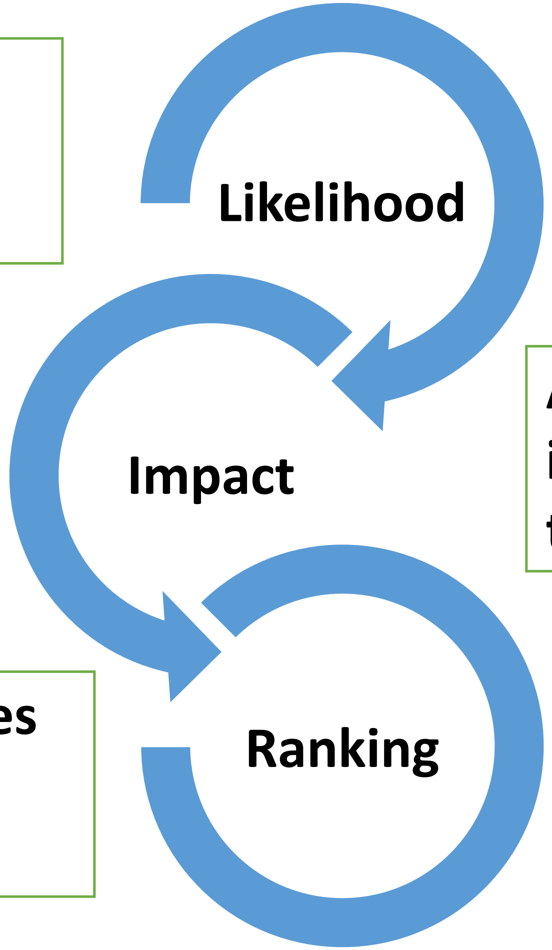
Analysis of Risk

- **Risk analysis is the systematic study of uncertainties and risks encountered in business and many other areas. Risk analysts seek to identify the risks, understand how and when they arise, and estimate the impact (financial or otherwise) of adverse outcomes.**

- **This technique also helps to define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints when they develop to avert possible negative effects on the competitiveness of the company.**

Analysis of Risk

Assess the likelihood of the risk occurring – measuring the probability of occurrence



Assess the consequence/impact if the risk occurred – measuring the frequency or severity

The risk matrix then determines whether the risk rating is low, medium, high or extreme

Types of Risks

Inherent Risk

The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)

Control Risk

Risk of loss arising from internal control systems to lose their effectiveness and thus expose or fail to prevent exposure of the objective they were to protect.

Risks

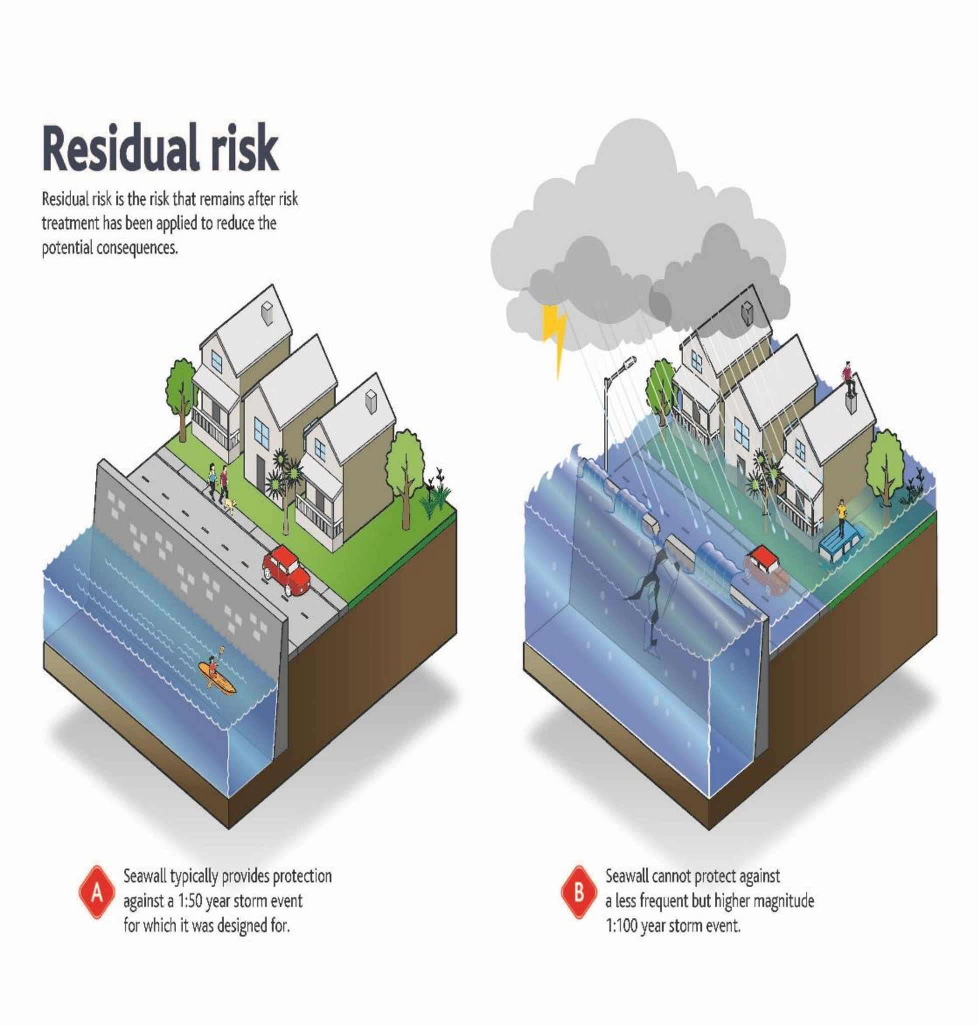
Detection Risk

Risk to detect a material misstatement in the financial statements.

Residual Risk

The risk that remains after controls are taken into account (the net risk or risk after controls).

Residual Risk

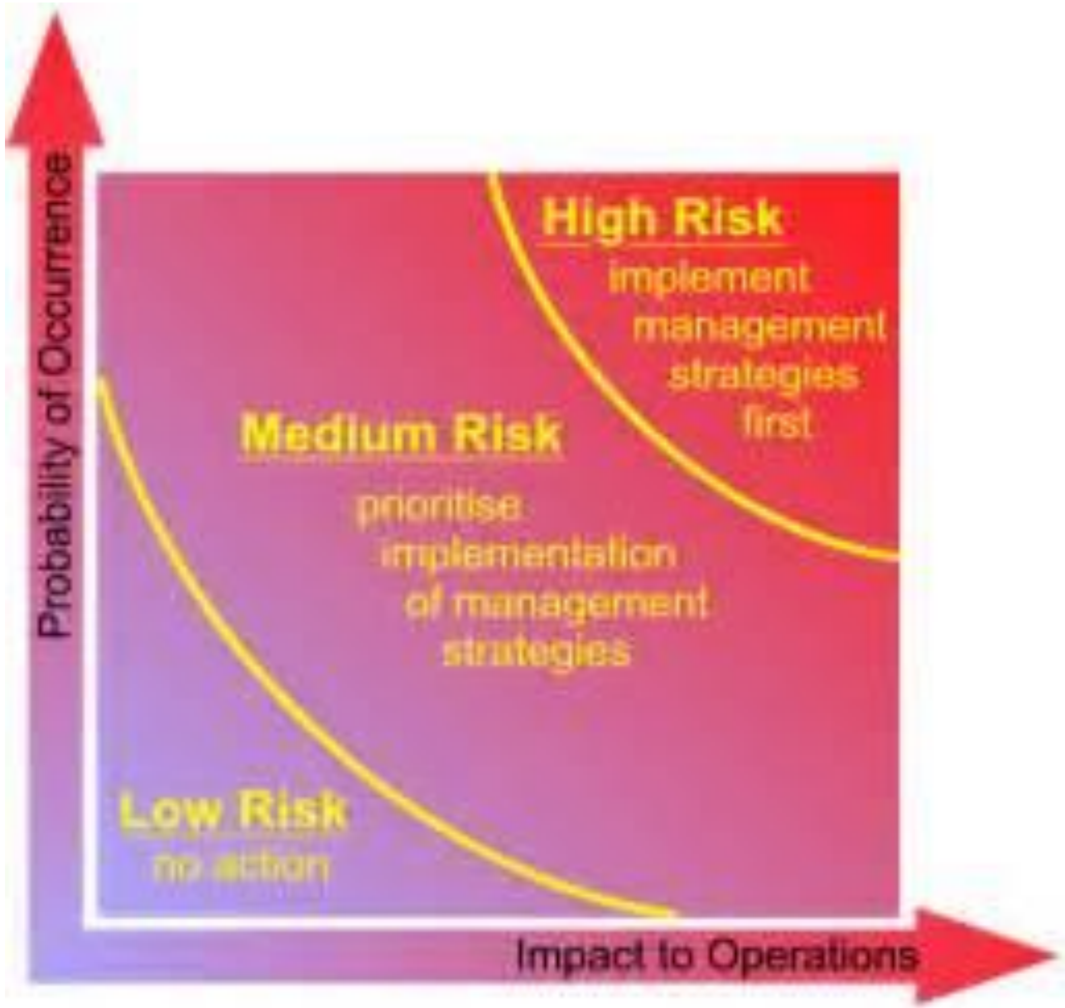


Analysing Risks - Methods

Risk Impact Assessment

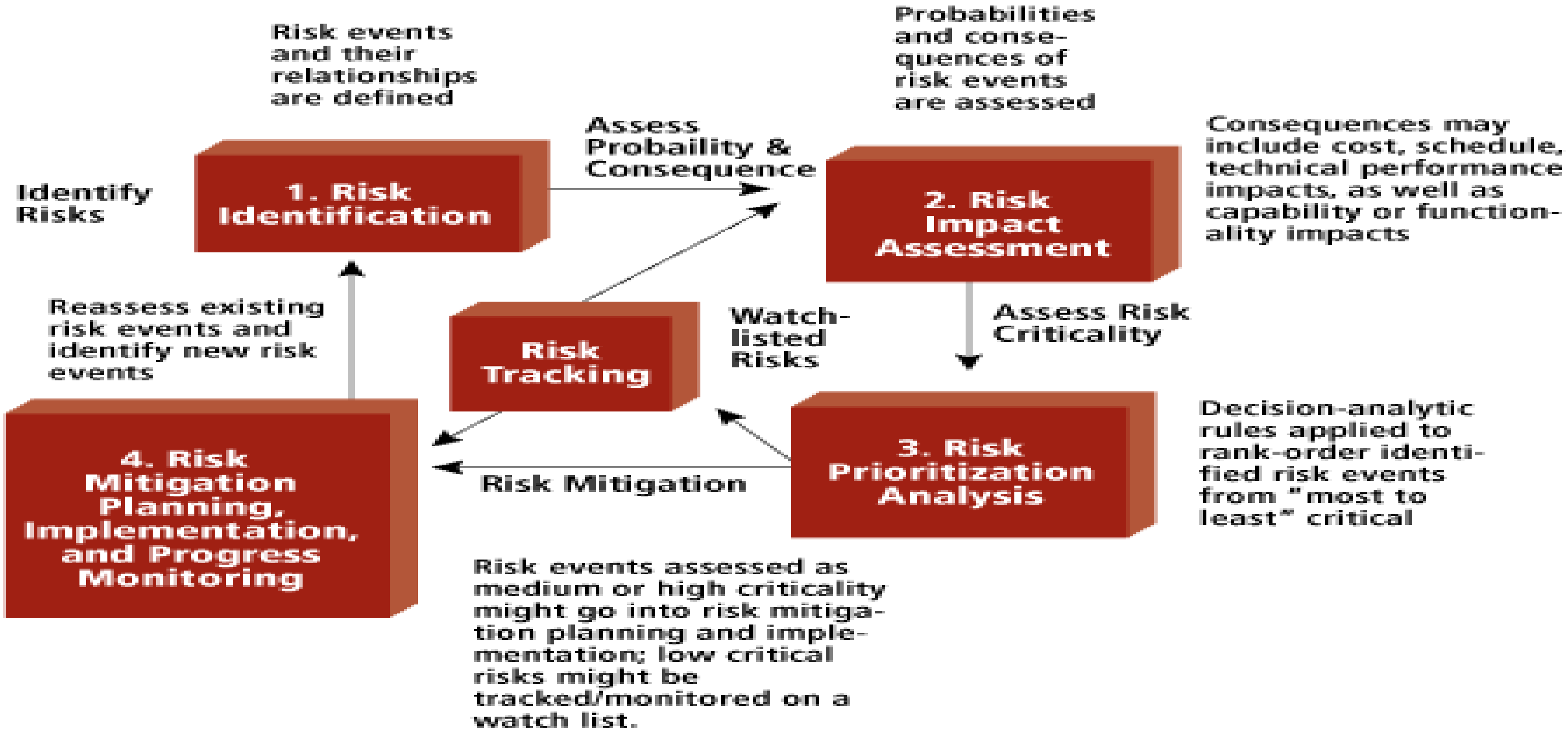
- **Risk impact assessment is the process of assessing the probability (likelihood) and consequences of the events if they are realised.**

- **The results of the assessment are used to prioritise risks to establish a most-to-least critical importance ranking.**

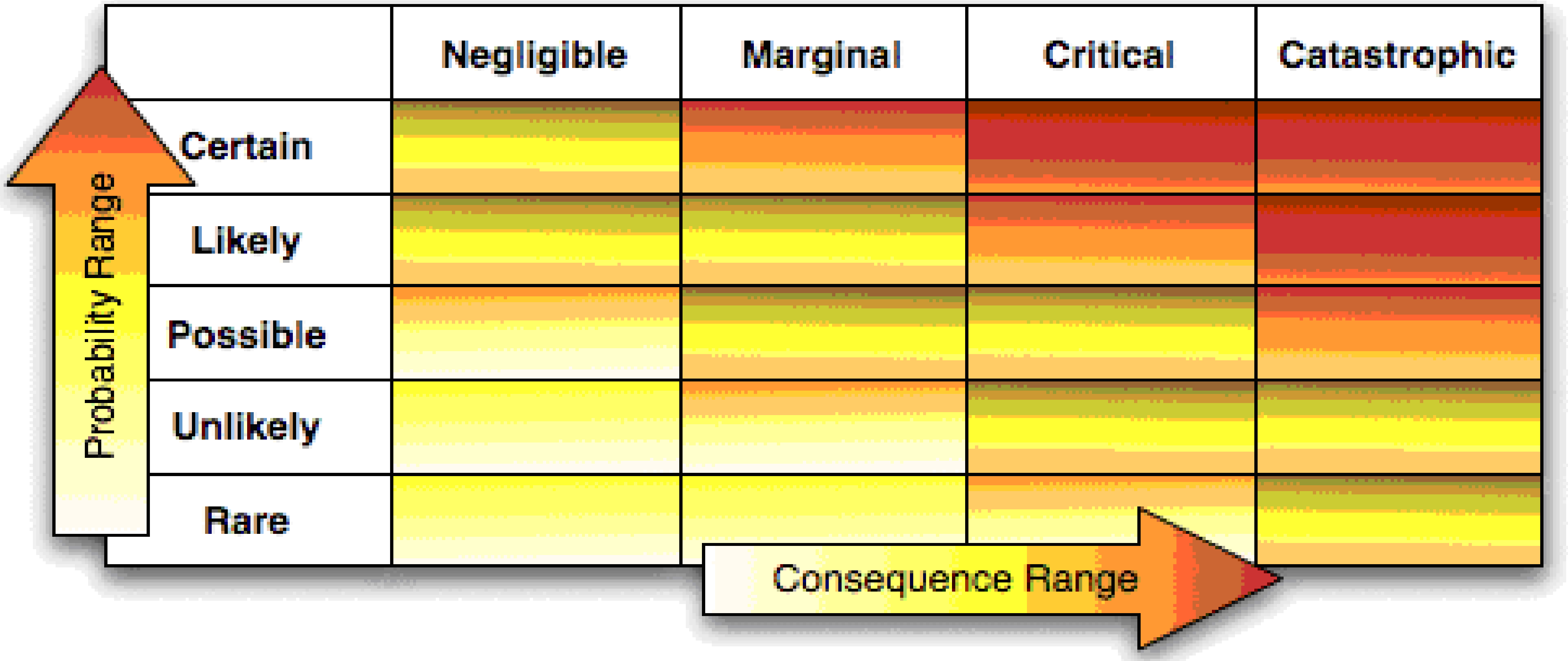


SOUTH AFRICAN INSTITUTE OF PROFESSIONAL ACCOUNTANTS™
YOUR WEALTH

Risk Impact Analysis



Risk Analysis Matrix



Brain Teaser #7

Risk Rating	Description	Likelihood occurrence
1	Rare	
2	Unlikely	
3	Possible	
4	Likely	
5	Certain	

Risk Likelihood Descriptor

Risk Rating	Description	Likelihood occurrence
1	Rare	Highly unlikely, but it may occur in exceptional circumstances, but probably never will
2	Unlikely	Not expected, but there is a slight possibility it may occur at some time
3	Possible	The risk might occur at some time as there is a history of casual occurrence in the business or similar businesses (industry)
4	Likely	There is a strong possibility the risk will occur as there is a history of frequent occurrence in the business or similar businesses (industry)
5	Certain	Very likely as the risk is expected to occur in most circumstances as there is a history of regular occurrence in the business or similar businesses (industry)

Brain Teaser #8

Risk Rating	Description	Financial impact	Business interruption	Reputational impact	Business objective
1	Insignificant				
2	Minor				
3	Moderate				
4	Major				
5	Catastrophic				

Risk Likelihood Descriptor

Risk Rating	Description	Financial impact	Business interruption	Reputational impact	Business objective
1	Insignificant	Minimal financial loss	Negligible as risk does not affect operations	Negligible impact externally	Resolved as part of day-to-day management activities
2	Minor	Limited loss exposure	Inconvenient to function of operations	Adverse effect which may impact on customers	Minor impact which require investigation
3	Moderate	Acceptable loss exposure	Limited disruption to the operations	Directly affecting customer relationships	Significant impact which require management intervention
4	Major	Negative impact of performance	Systems failure which causes temporary disclosure	Negatively affect the reputation of the business	Major impact which require senior management intervention
5	Catastrophic	Financial disaster	Systems failure which require major interventions	Result in regulatory investigations and threaten business closure	Disastrous impact which require strategic decision

Risk Classification

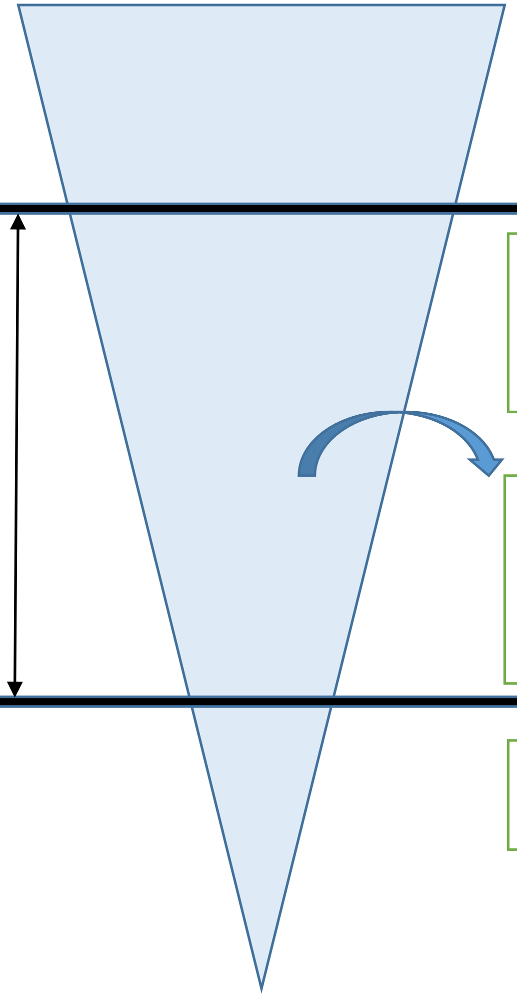
Frequency	Consequence			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	IV	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Risk Class	Interpretation
Class I	Intolerable risk
Class II	Undesirable risk, and tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvements gained
Class III	Tolerable risk if the cost of risk reduction would exceed the improvements gained
Class Iv	Negligible risk

Risk Ranking

IMPACT	ACTIONS		
SIGNIFICANT	Considerable Management Required	Must Manage and Monitor Risks	Extensive Management essential
MODERATE	Risk are bearable to certain extent	Management effort worthwhile	Management effort required
MINOR	Accept Risks	Accept but monitor Risks	Manage and Monitor Risks
	LOW	MEDIUM	HIGH
	LIKELIHOOD		

Risk Classification



Intolerable Region

Risk cannot be justified except in extra-ordinary circumstances

ALARP or tolerability region
(Risk is undertaken only if the benefit is desired)

Tolerable only if further risk reduction is impracticable or if the cost is grossly disproportionate to the improvement gained

As the risk is reduced, the less proportionate it is necessary to spend to reduce it further to satisfy APARP. The concept of diminishing proportion is shown by the triangle

Broadly acceptable region
(No need for detailed working to demonstrate ALARP)

It is necessary to maintain assurance that the risk remains at this level

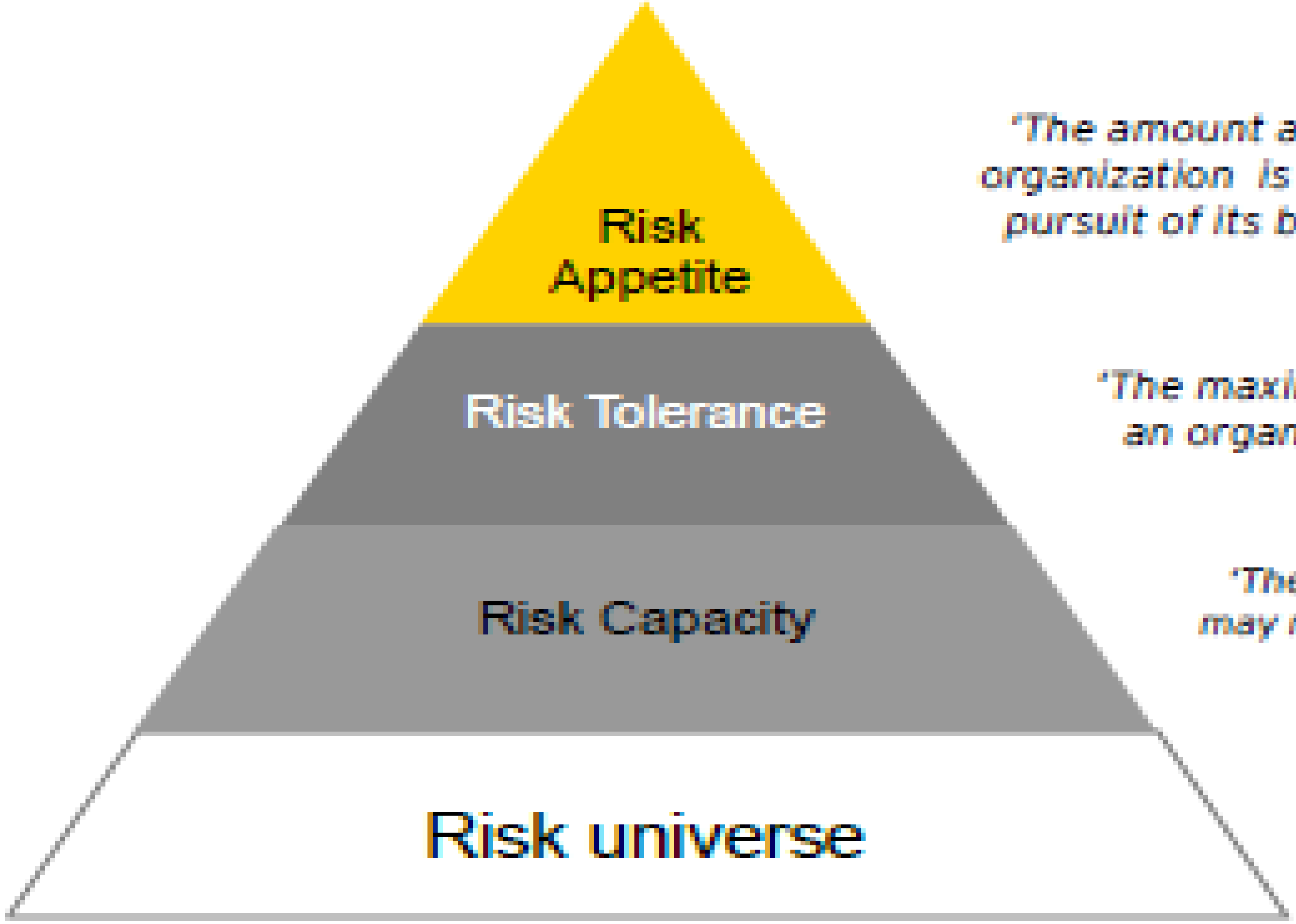
ALARP = As Low As is Reasonably Practical

Evaluation of risk

- **Risk evaluation is a process conducted to decide whether the risk is acceptable or unacceptable with the specific purposes of making decisions about future actions.**

- **Decisions about future actions may include:**
  - **not to undertake or proceed with the event, activity, project or initiative**
  - **actively treat the risk**
  - **prioritising the actions needed, if the risk is complex and treatment is required**
  - **accepting the risk**

Risk Appetite & Risk Tolerance



'The amount and type of risk an organization is willing to accept in pursuit of its business objective'

'The maximum amount and type of risk an organization is willing to tolerate'

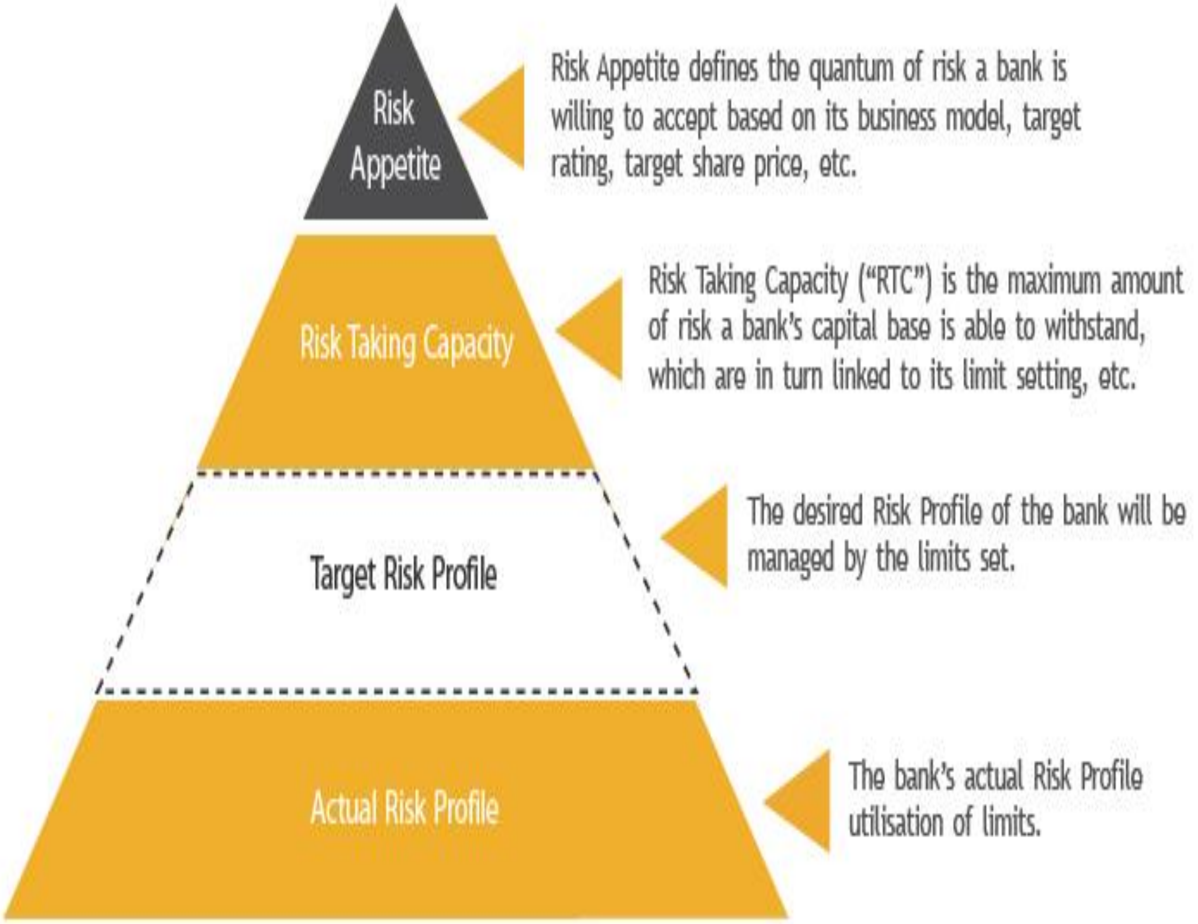
'The maximum level of risk an organisation may run given its capital and liquidity position and other restrictions'.

'All potential risks of the organization'.

Risk Appetite & Risk Tolerance

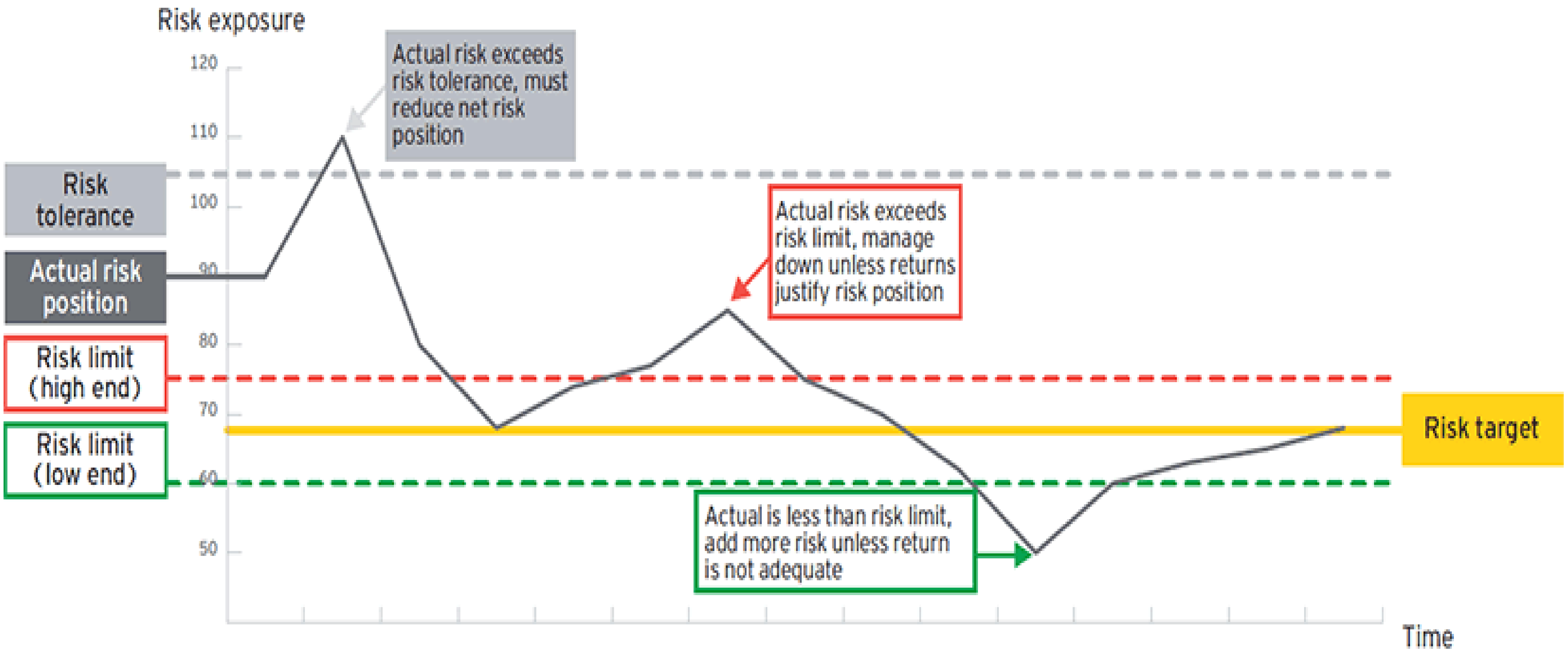
- **Risk appetite is a broad-based description of the desired level of risk that the organisation is willing to take in pursuit of its strategy objective**

- **Risk Tolerance reflects the acceptable variance in the outcomes related to the strategic action taken – ability to tolerate downside risk**



Risk Appetite & Risk Tolerance

Risk appetite/tolerance/target example



Risk Register

RISK REGISTER

Risk ID #	Risk Statement (Description)	Probability of Occurrence	Impact	Score (Probability x Impact)	Risk Trigger	Risk Owner	Planned Response(s) (Description)

Risk Register - Content

When documenting a risk assessment record the following information within the risk register:

- **A description of the risk (setting the context)**
- **Causes or contributing factors**
- **Consequences of the risk – actual or potential**
- **Current controls in place that help manage the risk**
- **An assessment of the likelihood and consequence based on current or existing controls to rate each risk**
- **Actions or treatments needed to address the risk**
- **Progress updates as the treatments are implemented**
- **Results from monitoring and review, including effectiveness of controls**

Risk Register - Value

By formally recording risks the benefits to the organisation are:

- **commit to continuous learning;**
- **obtain benefits for reusing information for management purposes;**
- **minimise costs & efforts of creating & maintaining records;**
- **maximise access & retrieval of information; and**
- **comply with retention periods; and recognise the sensitivity of the information.**

Treatment of Risk

Risk treatment takes place in two distinctive contexts:

- **Proactive context - where an organisation has successfully integrated risk management into a system of management. Risk treatment is integral to and effectively indistinguishable from decision-making. Therefore, at the time a decision is finalised the risk created by the decision will be within the organisation's risk criteria.**

- **Reactive context - the organisation is looking retrospectively at the risk created by decisions taken and implemented previously, and so any risk treatments found necessary will be remedial in nature.**

Treatment of Risk

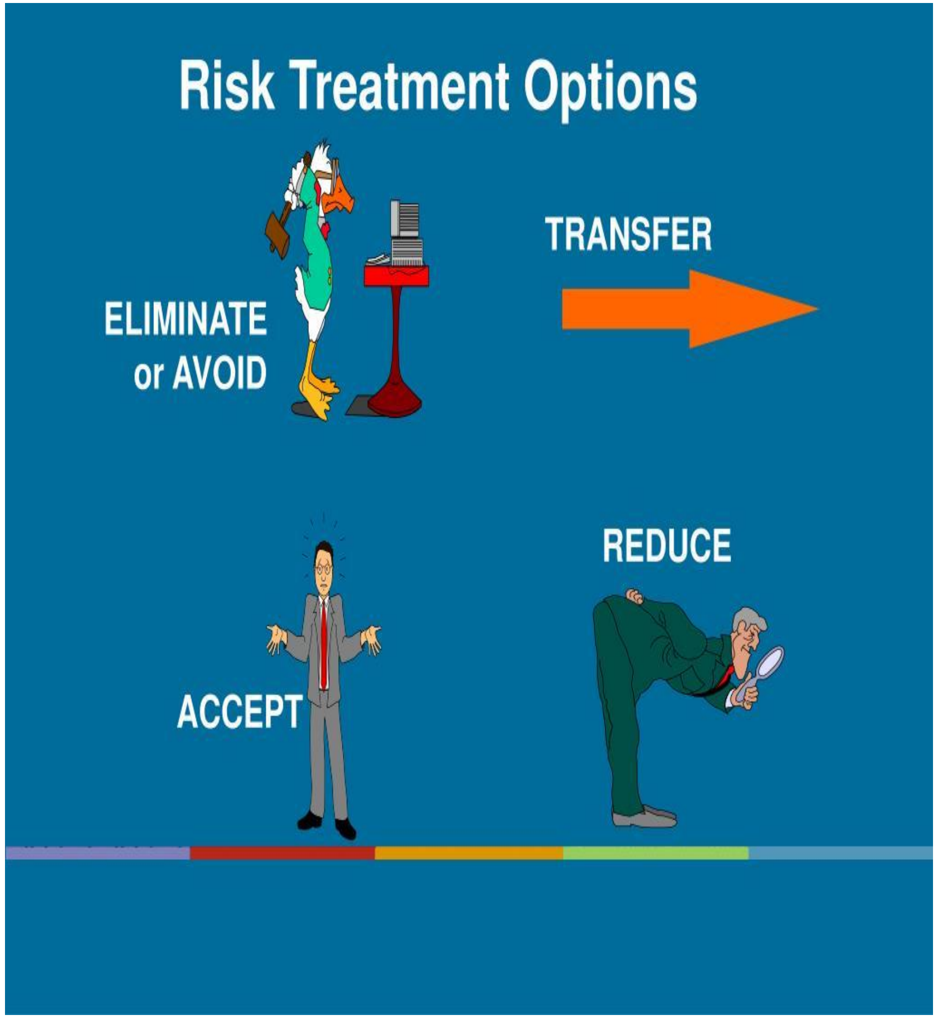
- **Treatment of risk ensures that effective strategies are in place to minimise the frequency and severity of the identified risk - develop actions and implement treatments that aim to manage, control or mitigate the risk.**

- **Treatment options not applied to the source or root cause of a risk are likely to be ineffective and promote a false belief within the organisation that the risk is controlled.**

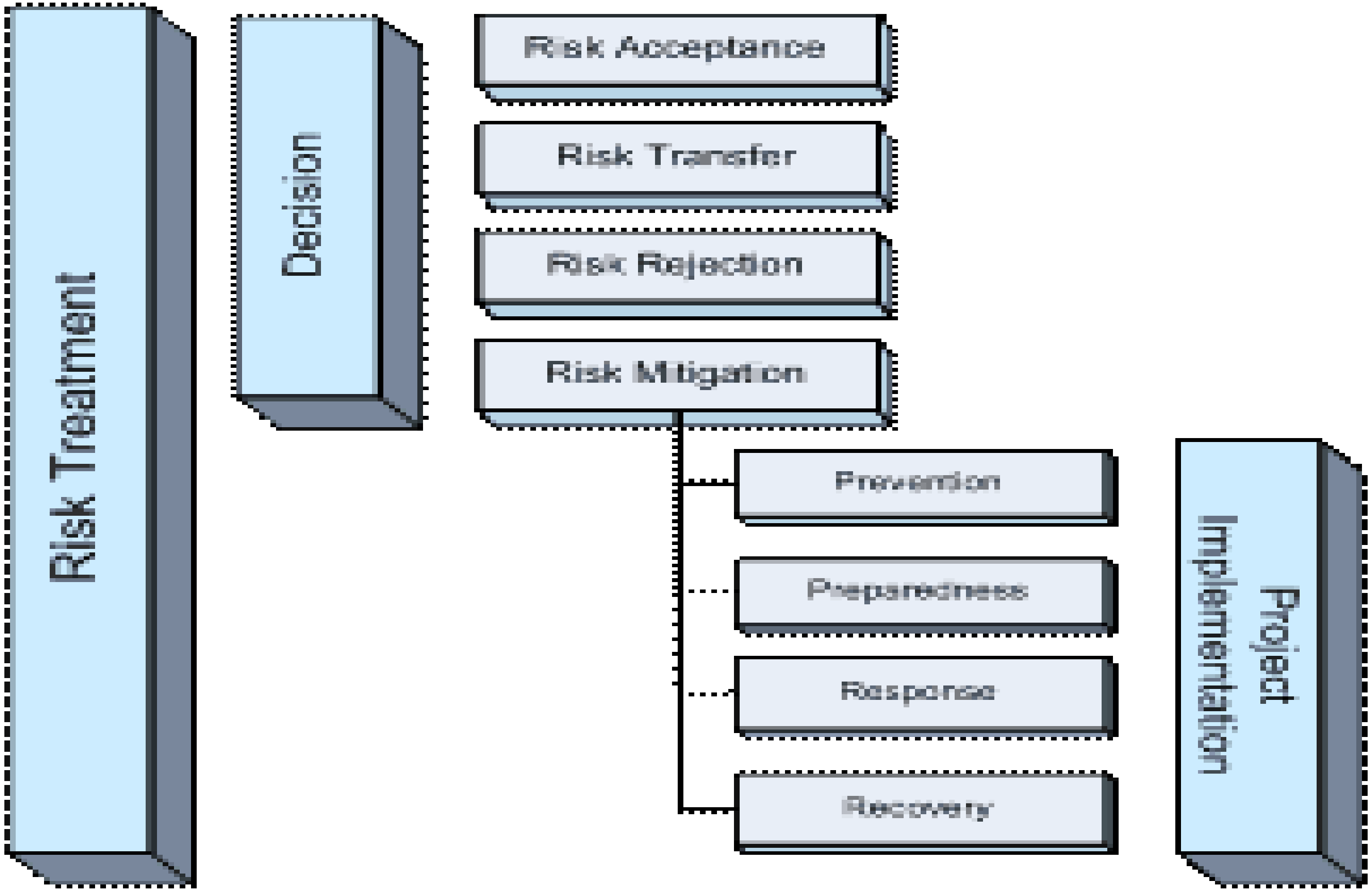
Treatment of Risks

Risk treatment options:

- **Avoid the risk by not starting or continuing an activity**
- **Take or increase risk in order to pursue an opportunity**
- **Remove the risk source**
- **Change the likelihood**
- **Change the consequence**
- **Share the risk e.g. through Insurance, contracts, financing**
- **Retain the risk by informed decision**



Treatment of Risk



Brain Teaser #9

SME owners usually conclude that it is often to cost to mitigate risks and are therefore willing to accept risks and deal with the consequences.

Discuss the circumstances under which risks may be accepted.

Treatment of Risks

A risk may be acceptable or tolerable in the following circumstances:

- **No treatment is available**
- **Treatment costs are prohibitive (particularly relevant with lower ranked risks)**
- **The level of risk is low and does not warrant using resources to treat it**
- **The opportunities involved significantly outweigh the threats**

A risk is regarded as acceptable or tolerable if the decision has been made not to treat - does not imply that the risk is insignificant.

Throw off the bowlines,
Sail away from the safe harbor,
Catch the tradewinds in your sails.

Explore. Dream. Discover.

-- Mark Twain

Treatment of Risks

Treatment of Risks

Risk Treatment

Acceptance/Retention

If, after controls are put in place, the residual risk is deemed acceptable. However, plans should be put in place to manage/fund the consequences of the risk should it occur.

Reduction

Implement a strategy that is designed to reduce the likelihood or consequence of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense.

Share/Transfer

Implement a strategy that shares or transfers the risk to another party, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk.

Avoidance

Deciding not to proceed with the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process.

Treatment of Risk – Developing a Plan

Determine the level of treatment plans required for each risk level that have improvement opportunities. Effective risk treatment relies on attaining commitment from key stakeholders and developing realistic objectives and timelines for implementation.

For each risk identified in the risk assessment, detail the following:

- **Specify the treatment option agreed - avoid, reduce, share/transfer or accept.**
- **Document the treatment plan - outline the approach to treat the risk. Any relationships or interdependencies with other risks should also be highlighted.**
- **Assign an appropriate owner - who is accountable for monitoring and reporting on progress of the treatment plan. Where the plan owner and the risk owner are different, the risk owner has ultimate accountability for implementing he plan.**
- **Specify a target resolution date - where risk treatments have long lead times, consider the development of interim measures.**

Treatment of Risk - Implementation

The treatment plan owner is responsible for coordinating activities that ensure risk treatments are implemented. The owner may not be directly responsible for implementing the risk treatment plans, however, they are responsible for ensuring that plans are completed within the expected timeframe.

When implementing a treatment plan, consider how the initiatives will be supported:

- **Firm structure – Is there a need for any change to structure or delegations of responsibilities to support the risk treatment plan?**
- **Financing - If the budget for control improvement is constrained, should there be a process to prioritise controls with the greatest need or cost benefit?**
- **Resource availability - Does the firm have sufficient physical, human or financial resources to implement the risk treatment plan?**
- **Communication with stakeholders - Does the firm need to commence briefing sessions to inform stakeholders as to what changes are required and why?**

Treatment of Risk - Implementation

For each risk identified in the risk assessment, detail the following:

- **Monitoring mechanisms and review points - The treatment plan owner should specify the mechanisms by which implementation will be monitored. This may include indicators to determine if the risk is increasing or decreasing. Successful implementation will usually be linked to business planning activities and will be reviewed regularly at meetings.**

- **Status of the treatment plan - the status of the treatment plan is either ‘open' for in progress or ‘closed' when implementation has been completed. If the status is closed and the risk has been eliminated, it may be removed from the current risk register into a closed items register. Where a risk is not eliminated, it should be retained in the current register and if another treatment plan is required this should be agreed or, if no other action is possible, the treatment agreed could be to accept and monitor the risk.**

RISK IDENTIFICATION		RISK TREATMENT		
Event	Action	Plan	Risk Owner	Resolve by
Failure to meet compliance obligations	AVOID	Implement formal compliance monitoring process: 1. Identification of compliance requirements 2. Identification of system or tool to manage compliance requirements 3. Monthly review of compliance requirements to ensure there have been no material compliance breaches.	Practitioner	30-Sep-12
Loss of Risk Practitioner	REDUCE	Implement succession plan: 1. Put in place power of attorney arrangements 2. Document key processes 3. Put in place a key client management system to ensure adequate documentation is maintained for key clients 4. Adequately train a secondary level of management and/or identify a potential candidate for partner.	Practitioner	31-Oct-12
Failure to collect receivables in a timely manner	REDUCE	Implement receivables tracking and debtor follow-up process: 1. Identify requirements to track receivables, consider such things as payment terms and conditions 2. Develop process to track aged debtors/receivables and supporting requirements including system reports 3. Consider monitoring requirements including frequency.	Office Manager	15-Sep-12

Monitoring & Evaluation of Risks

- **Monitor changes to the source and context of risks, the tolerance for certain risks and the adequacy of controls. Ensure processes are in place to review and report on risks regularly.**

- **To ensure structured reviews and regular reporting occurs and each area is encouraged to identify a process that allows key risks within their area to be monitored.**

- **Given the diverse and dynamic nature of the business environment, it is important to be alert to emerging risks as well as monitoring known risks.**

Monitoring & Evaluation of Risks

Continuous monitoring:

Once risks have been identified, recorded, analysed, and the agreed treatments have been implemented, an appropriate monitoring and reporting regime needs to be established to provide assurance that the treatment has been effective and now helps to control the risk. Some risk treatments will of course become embedded into daily practices and methods of work. The frequency of review will depend on the risk rating, the strength of controls and the ability to effectively treat the risk.

Monitoring & Evaluation of Risks

Departmental / Entity Management review:

Managers need to ensure there is a process for reviewing risk profiles and activities in their area of responsibility. Wherever possible, risk management should become an agenda item on management meetings or committees and avoid the need for separate processes. The aim of regular review is to identify when new risks arise, and to monitor existing risks to ensure that treatments or controls are still effective and appropriate. How frequently a review process and reporting cycle occurs will depend on the risk appetite and level of risk tolerance but local management review is required.

Monitoring & Evaluation of Risks

Internal audit:

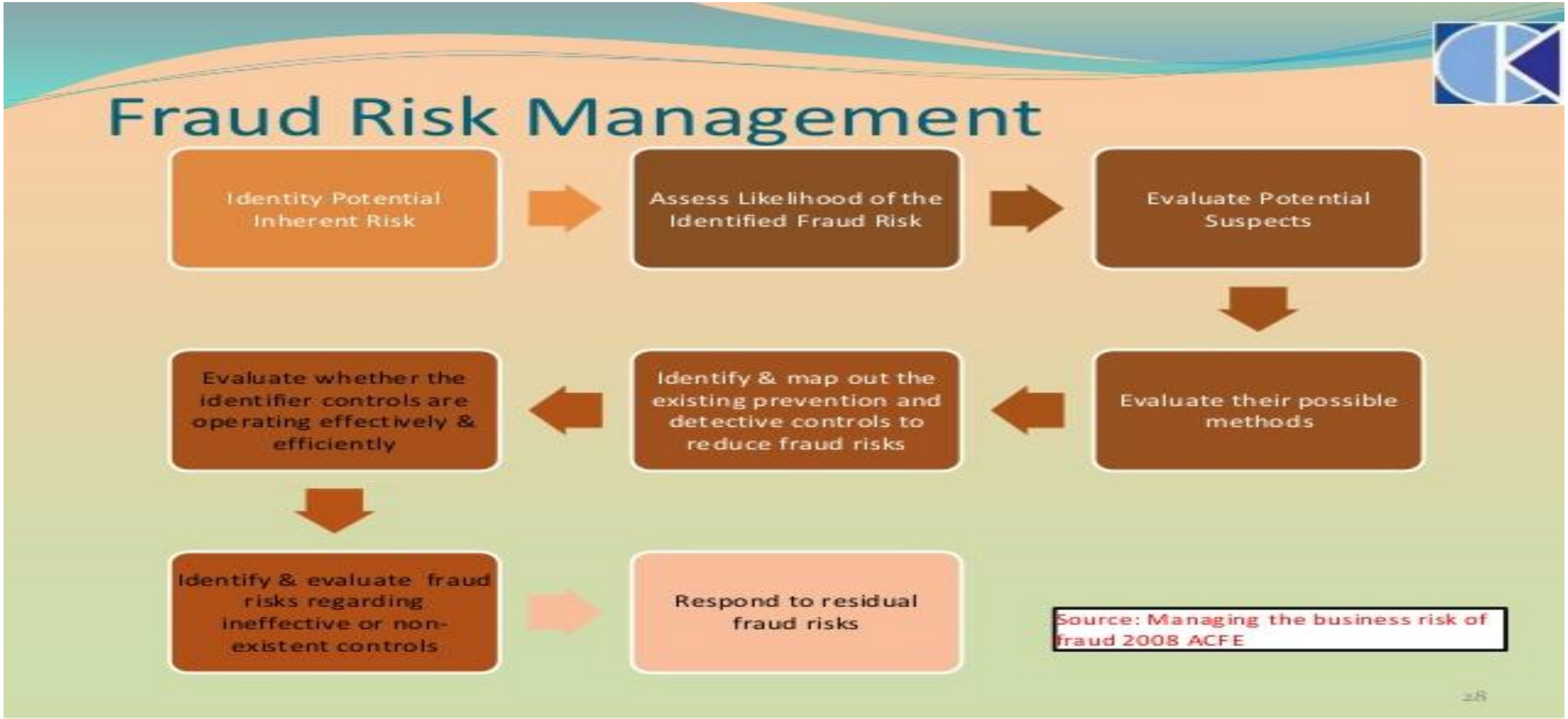
The organisation's internal audit program provides for a review of systems, policies and process assurance and compliance. The auditors apply a risk-based approach to the audit program and help bring a measure of independence and external perspective to the organisation Risk Management Framework.

External audit:

That external audit covers financial, governance, contracting, IT and risk management systems and processes. Management and staff may be required to respond to the risk management activities involved with these audits. Other audits occur from time to time and are imposed through contracts, compacts, and regulation.

Corruption & Fraud Risk Management

Corruption & Fraud Risk Management

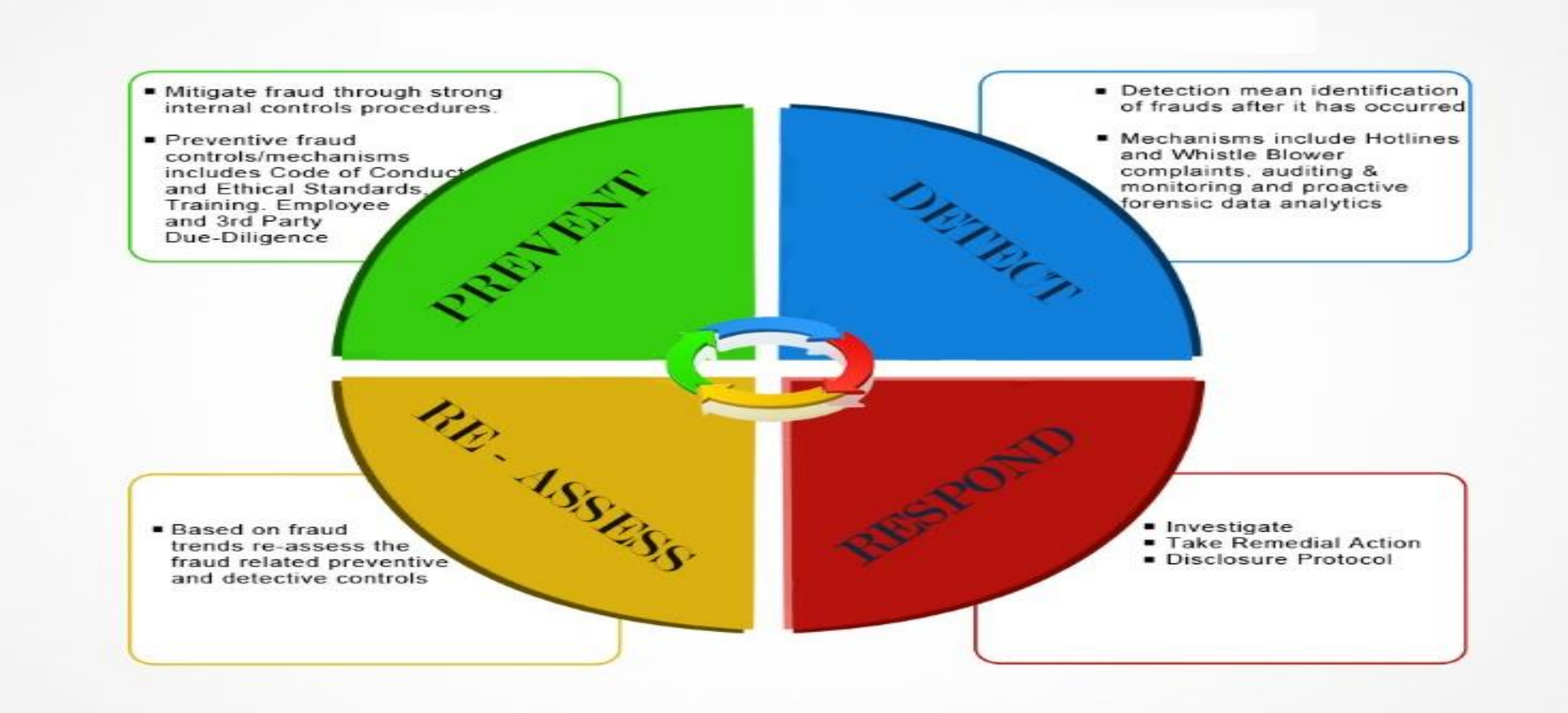


Corruption & Fraud Risk Management

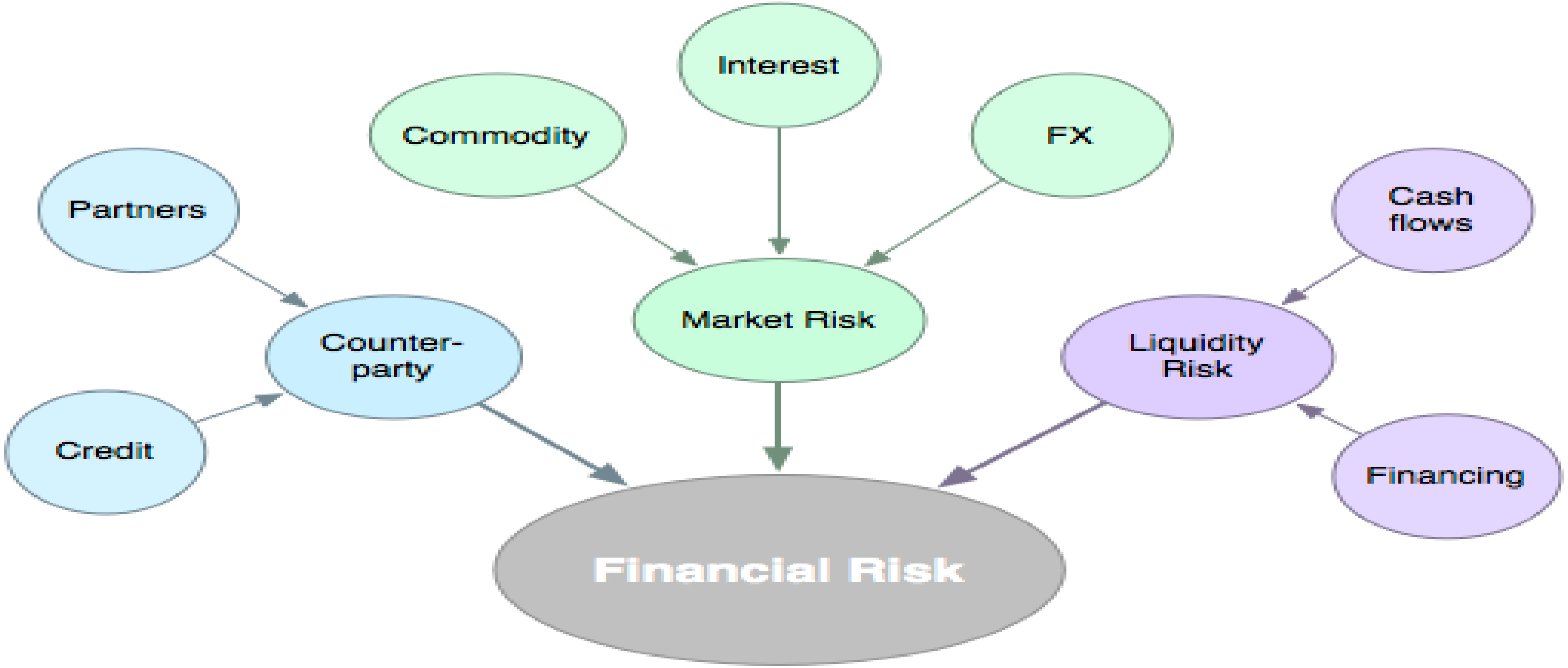
An Approach to Fraud Risk Management – The Anti-fraud Roadmap

Evaluate	Identify	Action Plan	Mitigate	Monitor	Respond
Evaluate current status and effectiveness of an organization's approach to implementing antifraud programs and controls	Assess, define, and document fraud risks and control effectiveness Establish fraud risk profile by analysis of risk against controls	Develop a fraud action plan based on findings and identify activities that defines next steps to address an organization's antifraud program activities	Enhance, implement, and maintain preventative and detective control activities, which mitigate fraud risks identified during assessment	Enable continuous monitoring activities through technology and ongoing review activities to alert management of potential fraud Incorporate findings into annual fraud risk assessment process	Assist in responding to potential occurrences of fraud
Internal Survey	Fraud Risk Assessment	Fraud Risk Action Plan	Fraud Awareness Training	Continuous Monitoring Tools	Fraud Case Management Tools
Diagnosis of Current Position			Mitigate Deficiencies	Data Analytics	Fraud Response

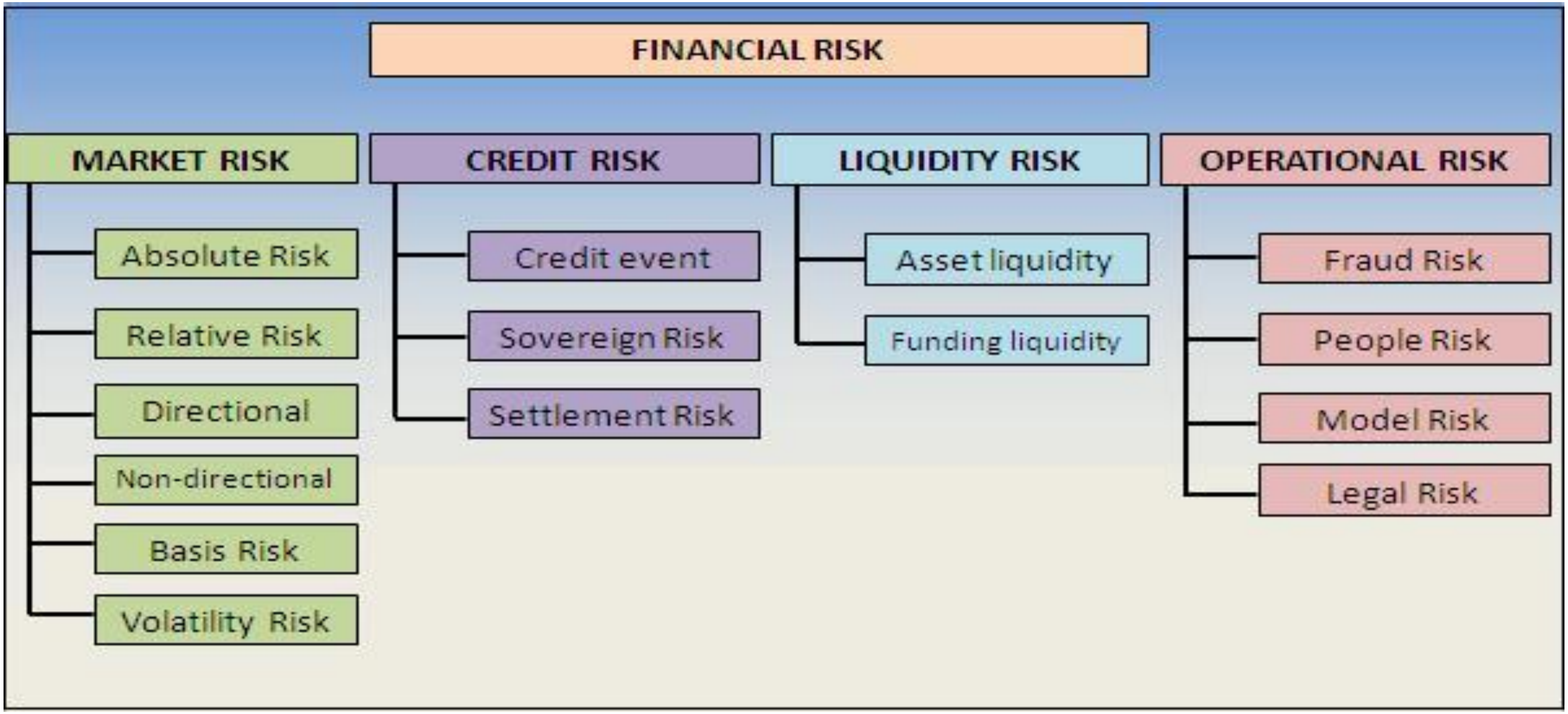
Corruption & Fraud Risk Management



Financial Risk



Financial Risk



Types of Risks

Inherent Risk

The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)

Control Risk

Risk of loss arising from internal control systems to lose their effectiveness and thus expose or fail to prevent exposure of the objective they were to protect.

Risks

Detection Risk

Risk to detect a material misstatement in the financial statements.

Residual Risk

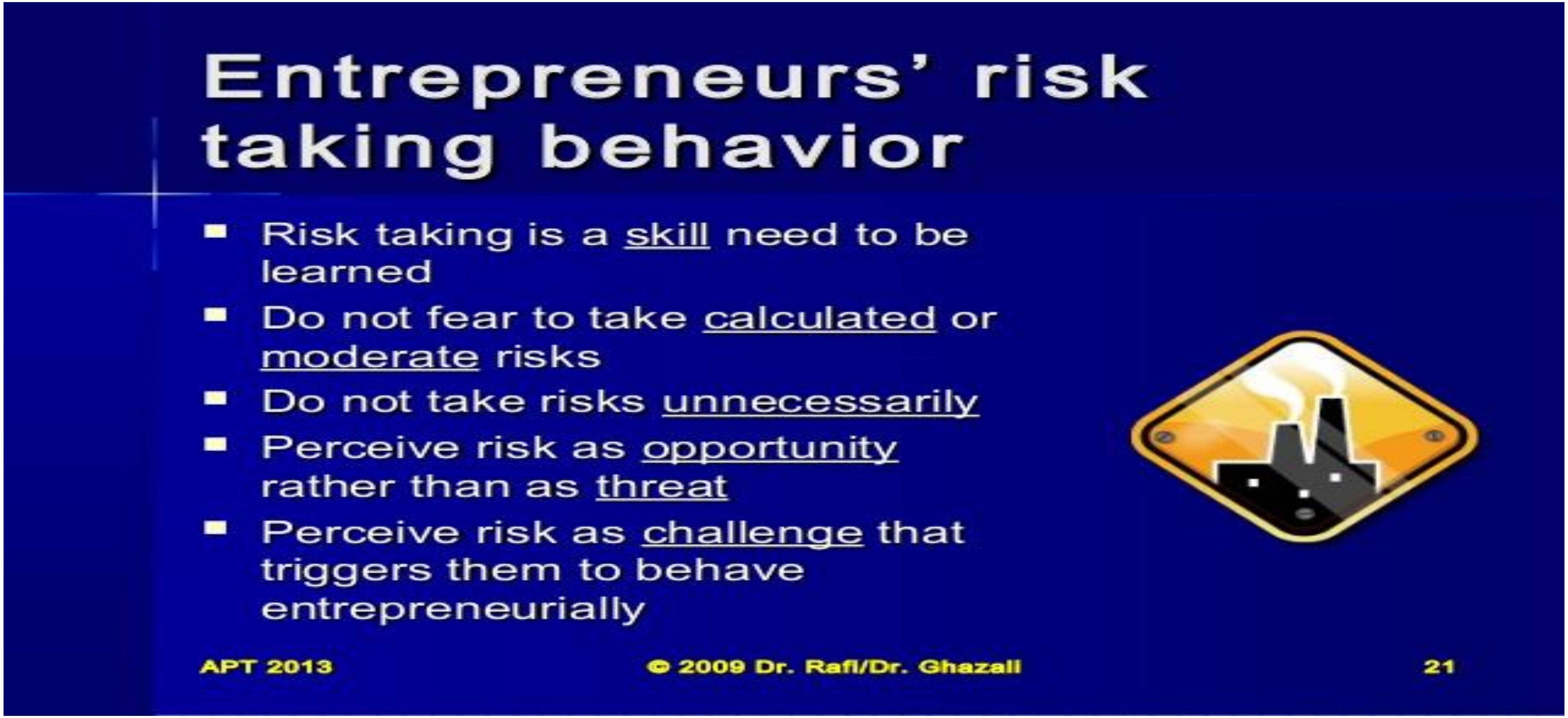
The risk that remains after controls are taken into account (the net risk or risk after controls).

Financial Statement - Risk

- **Financial statement risk is defined as the risk that financial statements may be materially misstated and thus does not satisfy the qualitative characteristics of financial statements as per the Accounting Framework standard.**

- **Financial statement risk implies that the financial statements may not in whole or part fairly represent the financial performance and position of the business and therefore may not be considered to be reliable.**

Some Advice on Risk



Summary – Risk Management

- **Risk Assessment**
  - Identification
  - Measurement
  - Prioritization
- **Risk Management**
  - Control It
  - Share or Transfer It
  - Diversify or Avoid It
- **Risk Monitoring**
  - Process Level
  - Activity Level
  - Entity Level


time for questions

Risk Management- References

1. The University of Adelaide RISK MANAGEMENT HANDBOOK
   *docplayer.net/4489777-The-**university-of-adelaide-risk-management**...*

2. Project Risk Management Handbook: A Scalable Approach
   ***www.dot.ca.gov**/hq/projmgmt/documents/prmhb/PRM_**Handbook**.pdf*

3. Eurojuris Risk management Manual | EUROJURIS International
   *www.**eurojuris**.net/en/node/41583*

4. Caltrans Project Risk Management Handbook
   ***www.dot.ca.gov**/hq/projmgmt/documents/prmhb/archive/caltrans...*


Thank You!