KPMG

cutting through complexity™

ERM identification, analysis, mitigation, tracking, and monitoring

ICPAK Conference

Disclaimer

This presentation is made by KPMG Kenya, a member firm of the KPMG network of independent firms affiliated with KPMG International, a Swiss cooperative. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

This presentation has been prepared solely and exclusively for the benefit, information and use by the participants of the Enterprise Risk Management Conference and for the sole and exclusive purposes of communicating material related to the workshop. These slides cannot be used by the participants of the workshop for any purposes other than as expressly stated herein; neither can these slides be disclosed to, referred to, or used by, any other third party. KPMG accepts no liability or responsibility whatsoever, resulting directly or indirectly from the disclosure of the presentation contents to any third party and/or the reliance of any third party on the contents of the presentation, either in whole or in part, and the participants of the workshop agrees to indemnify KPMG in this respect.

This presentation is based on, and should be considered only in the context of the full text of our report.

When Tony Hayward became CEO of BP,2007 he vowed to make safety his top priority. Among the new rules he instituted were the requirements that all employees use lids on coffee cups while walking and refrain from texting while driving. Three years later, on Hayward's watch, the Deepwater Horizon oil rig exploded in the Gulf of Mexico, causing one of the worst man-made disasters in history. A U.S investigation commission attributed the disaster to management failures that crippled "the ability of individuals involved to identify the risks they faced and to properly evaluate, communicate and address them."

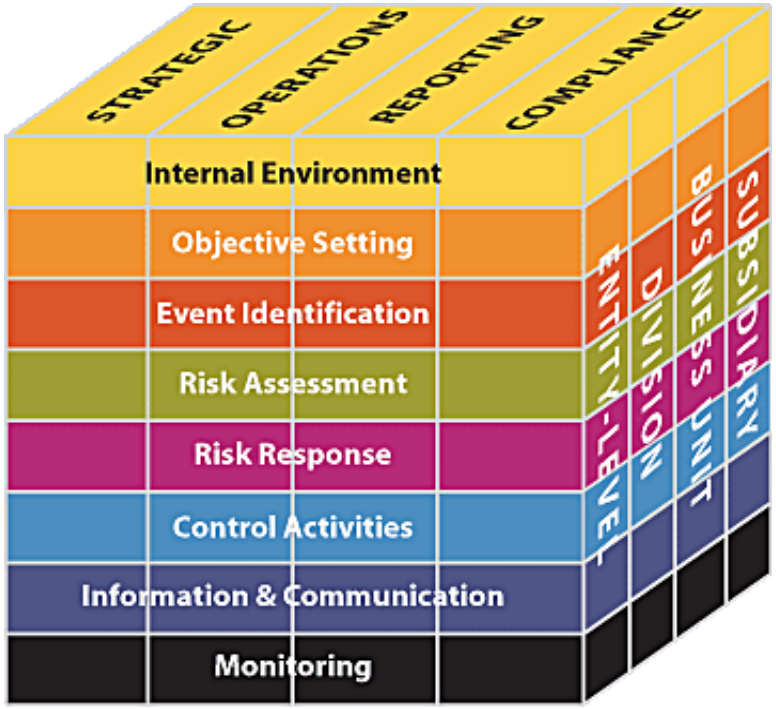
Course Objectives

- How to carry out an enterprise risk assessment.
- How to respond to risks.
- Monitoring of risks.

What is a risk assessment?

Risk Assessment

This is the **identification** and **analysis of risks** that have an impact on the ability of an organization to **achieve its objectives**.



It forms a basis for **determining** how risks should be **managed**.

Allows an entity to **understand the extent** to which potential events might **impact** objectives.

What are the risk assessment techniques?

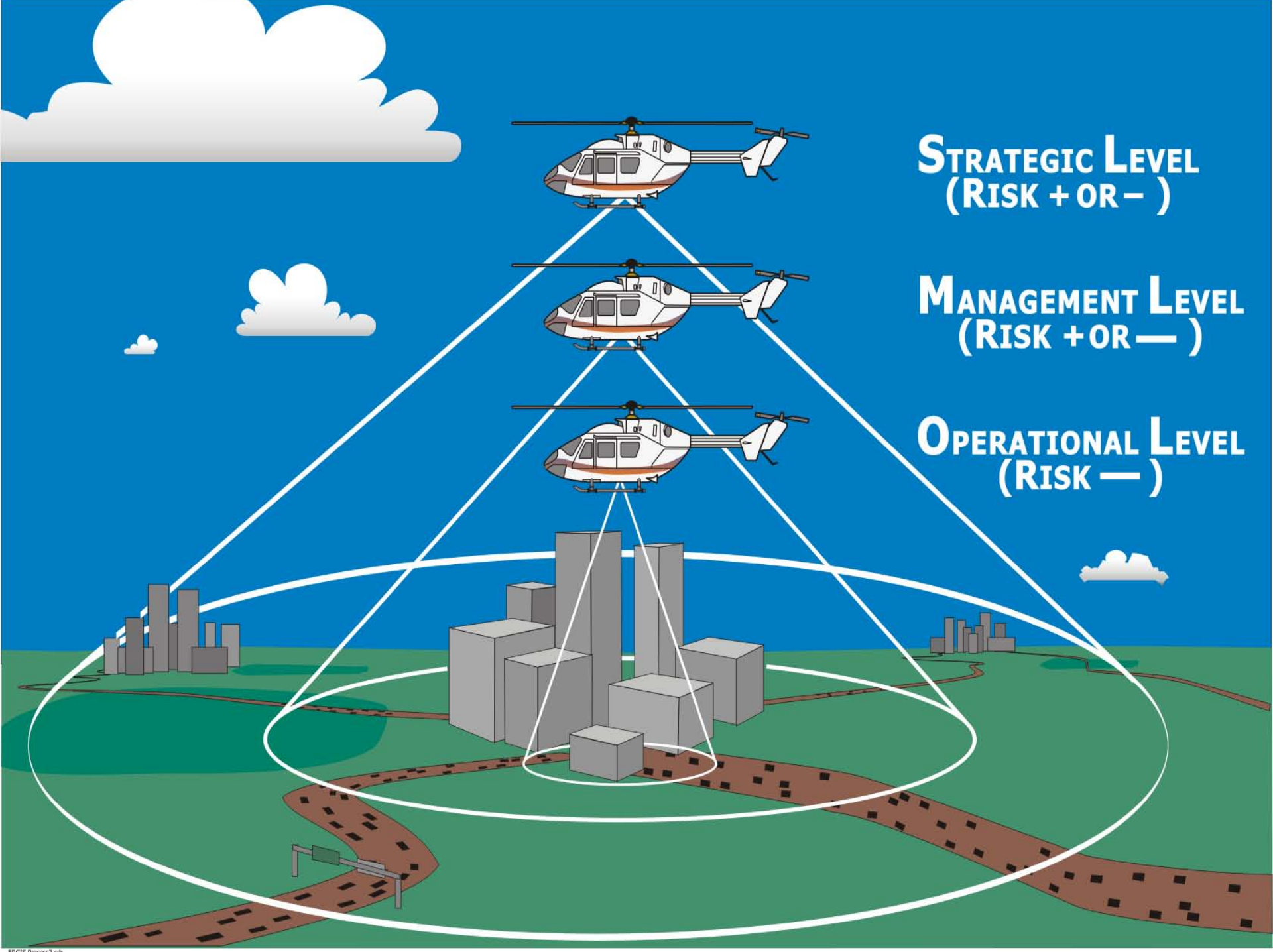
- Risk assessment questionnaire
- Interviews
- Workshops

Levels of Risk Assessment

Risk assessments are done at mainly two levels;

- Strategic level risk assessment- Focuses on risks that can affect the current business model, survival of the organization and the ability of the organization to achieve its strategic objectives.
- Process level risk assessment – Focuses on risks that affect the ability of an organization to achieve its process objectives.

The risk assessment process is however similar in both scenarios.



ERGIS Process2.cdr

Risk Assessment Process

Step 1: Identify the Strategic/process objectives of the organisation

Step 2: Identify the possible events (Risks) that could affect the organisation's strategy and process objectives

Step 3: Categorise the Risks

Risk Assessment Process

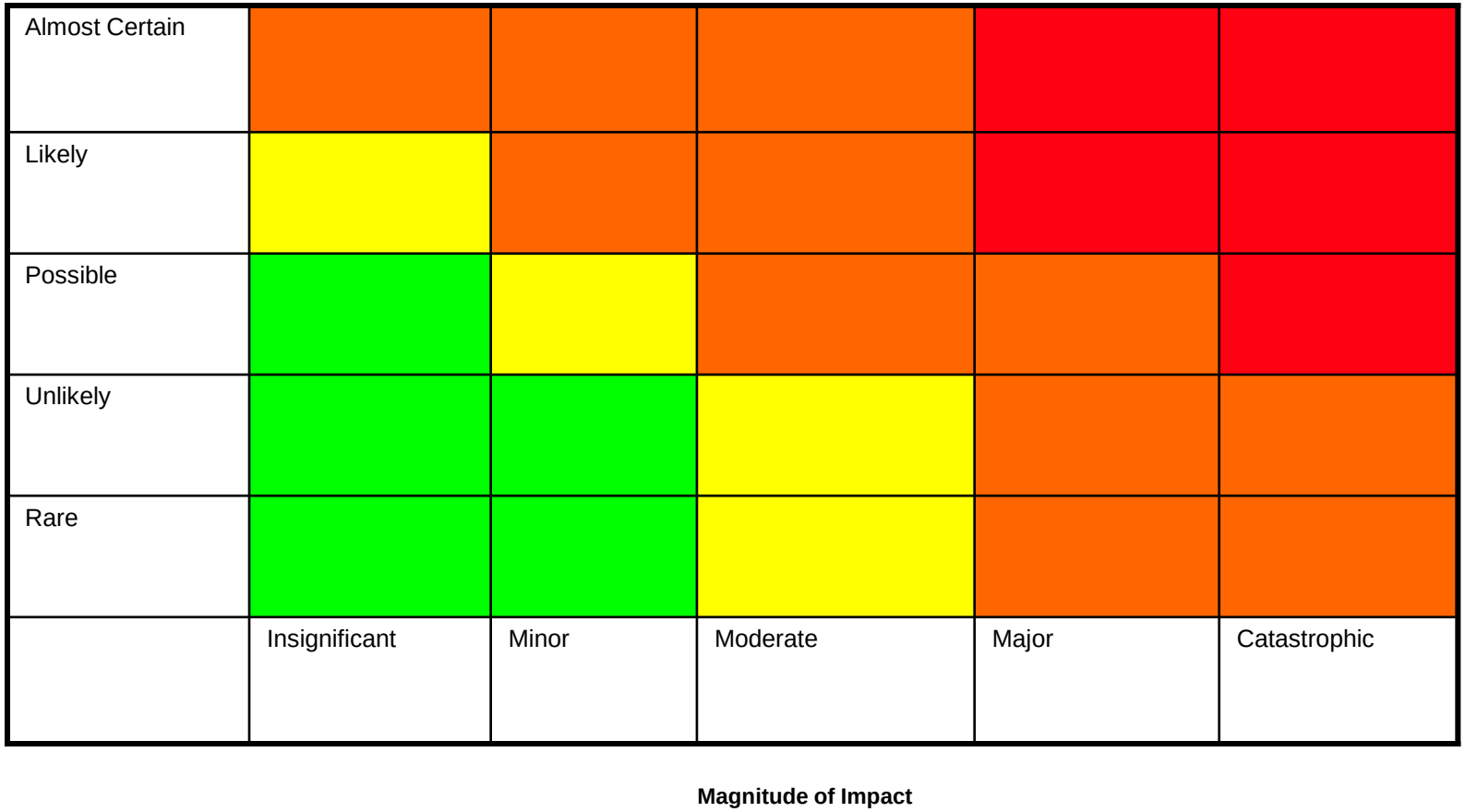
Step 4: Nominate responsible owners for each Risk

Step 5: Root cause analysis

Step 6: Consequences of Risk – qualitative and quantitative

Step 7: Gross risk rating

Example of a risk heat map



Risk Assessment

Assesses risks from two perspectives:

- Likelihood
- Impact

Likelihood – Will it occur? What are the chances?

Impact - What are the consequences? How much?

Risk criteria

- **Impact**
  - Insignificant
  - Minor,
  - Moderate,
  - Major
  - Catastrophic
- **Likelihood**
  - Rare
  - Unlikely
  - Possible
  - Likely
  - Certain

Classification criteria

	Description	Examples of likelihood
1	Certain	The event will occur in most circumstances; There is a history of regular/predictable occurrences; Very high likelihood of 50% and above.
2	Likely	The event will probably occur in most circumstances; There may be a history of frequent occurrences; High likelihood of 20%-49%.
3	Possible	The event might occur at some time; There could be a history of occurrence; Medium likelihood of 10%-19%.

Classification criteria

	Description	Examples of likelihood
4	Unlikely	Not expected, but there's a slight possibility the event could occur at some time; Some of the team consider this a risk that might occur; Low likelihood of 5% -9%.
5	Rare	Highly unlikely, the event may occur in exceptional circumstances; No experience of a similar failure or sufficient controls now in place; Very low likelihood of 2% -4%.

Classification criteria

	Description	Examples of impact
1	Catastrophic	Failure to deliver on corporate objectives Impact on revenue is more than 40% Board of Directors & CEO required to resign Significant national and international reputation damage
2	Major	Partial failure to deliver corporate objectives Impact on revenue is between 25% to 39% Adverse local publicity

Classification criteria

	Description	Examples of impact
3	Moderate	Moderate impact on the organization's strategic objectives/operation activities 15%-29% Impact on revenue is between 15%-24% Short term disruption of service capability
4	Minor	Minor impact on the organization’s strategic objectives Impact on revenue is between 1%-5% Impact on the organizations strategic objectives/ operation activities between 5% - 15%.

Classification criteria

	Description	Examples of impact
5	Insignificant	Financial impact on the organization is below 1% of total annual revenue. Impact on the organizations strategic objectives/ operation activities below 5%.

Enterprise Risk Management

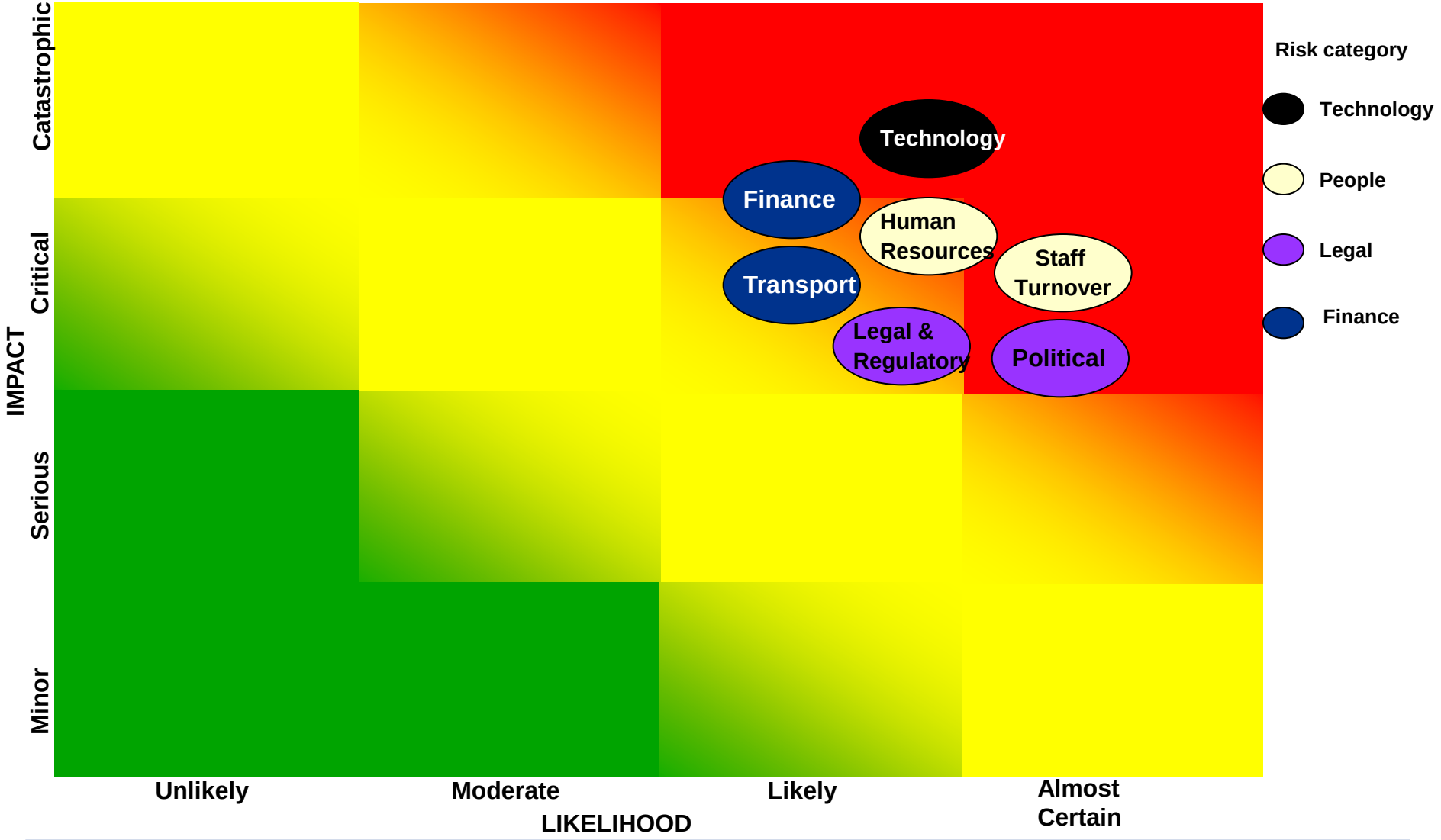
- Assess risk on both an inherent/gross and a residual basis.

Inherent (gross) risk – is the risk to an organization before any management actions

Residual risk – is the risk that remains after management's response to the risk (The unmitigated risk)

- Risk assessment is applied first to inherent risk – once risk responses have been developed – management then considers residual risk

Example – Gross/ Inherent Risk profile



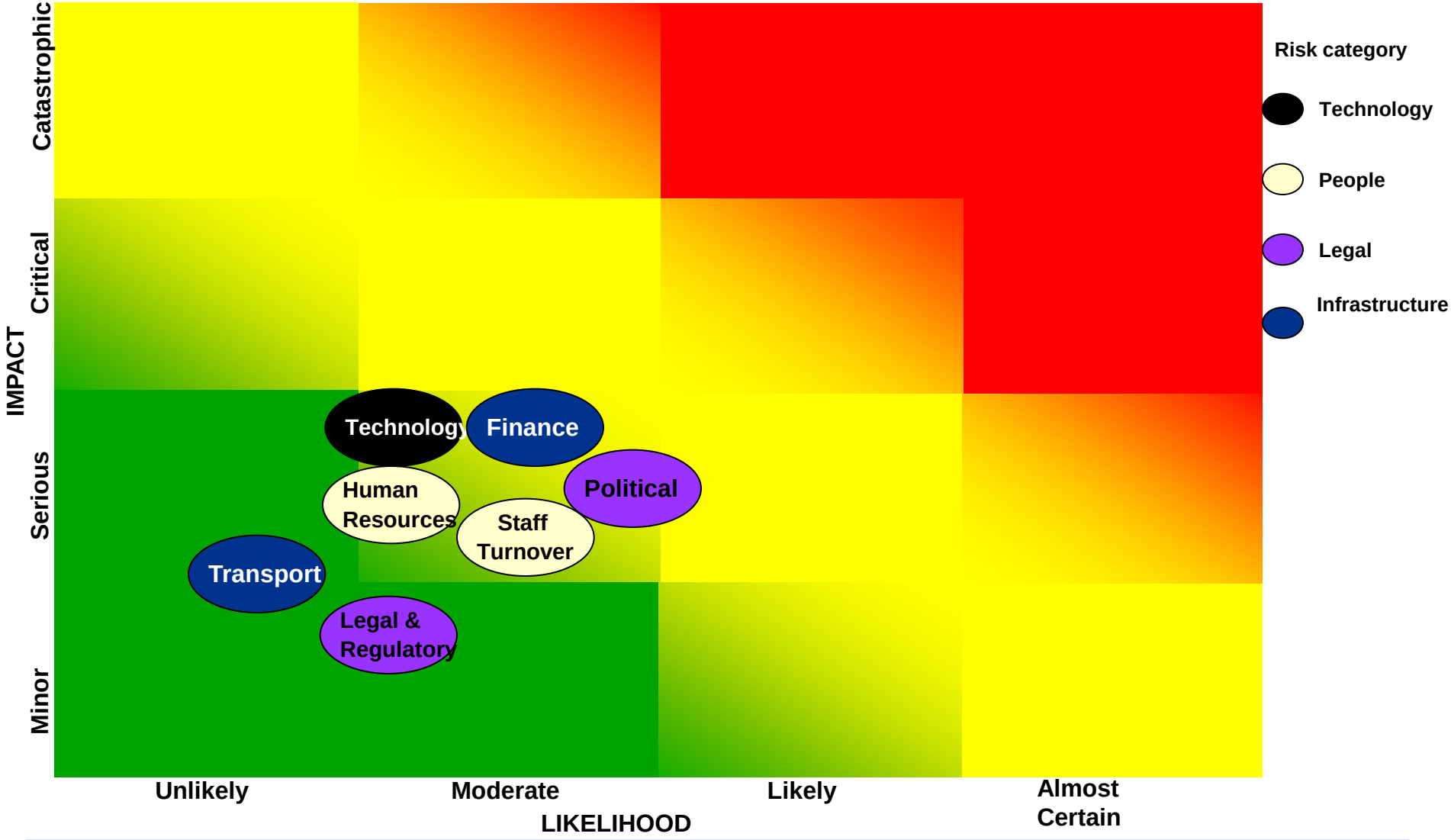
Risk Assessment Process

Step 8: Controls Identification

Step 9: Controls assessment

Step 10: Driving risk assessment from Gross to Residual Risk

Example – Residual/Net Risk profile



Risk Assessment Process

Step11:Developing actions to respond to risk occurrence and manage risk consequence

Step 12: Decide upon a Risk response for each Risk

Step 13: Defining Key risk indicators

Step 14: Performing periodic monitoring

KPMG

cutting through complexity™

Risk Response

March 2013

Enterprise Risk Management
Risk Response

Just as evidenced in Hayward's story, risk management is too often treated as a compliance issue that can be solved by drawing up lots of rules and making sure that all employees follow them. Such rules are sensible but could severely damage a company!

Enterprise Risk Management
Categories of Risk Response

1. Avoidance

Exiting the activities giving rise to risk e.g. exiting a product line, declining expansion to a new geographic market, or selling a division.

Examples of direct avoidance responses

- clarifying requirements
- defining objectives
- obtaining information
- improving communication
- undertaking research, prototyping or development

Enterprise Risk Management
Categories of Risk Response

Examples of indirect avoidance responses

- Changing the scope of the project to exclude risky elements
- Adopting a familiar approach instead of an innovative one
- Using proven technology and/or methodology instead of leading edge
- Building redundancy into the project design

Enterprise Risk Management
Categories of Risk Response

2. Reduction/mitigation

Action is taken to reduce risk likelihood or impact, or both to below a threshold of “risk acceptability”.

This is the strategy used most often.

Preventative responses are better than curative ones, since they are more proactive, and if fully successful can lead to risk avoidance.

Enterprise Risk Management
Categories of Risk Response

3. Sharing

Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk.

Examples

- Hedging
- Insurance
- Performance bonds
- Guarantees and contracts.

4. Acceptance

No action is taken to affect risk likelihood or impact.

Residual risks - those which remain after avoidance, transfer or mitigation responses. Also include those minor risks where any response is not likely to be cost-effective compared to the possible cost of bearing the risk impact.

Management must recognize and accept these risks, and adopt responses to protect against their occurrence.

KPMG

cutting through complexity™

Risk monitoring

March 2013

Enterprise Risk Management
Risk monitoring

Context for activities:

- Risk management framework and principles

- Governance principles

- Organizational design

- Management control systems

Effective Risk Management = Proactive Implementation of Appropriate Responses to Identified Risks

Minimum standards – four key activities:

1. Registering changes to risk registers

2. Reacting to early warning indicators

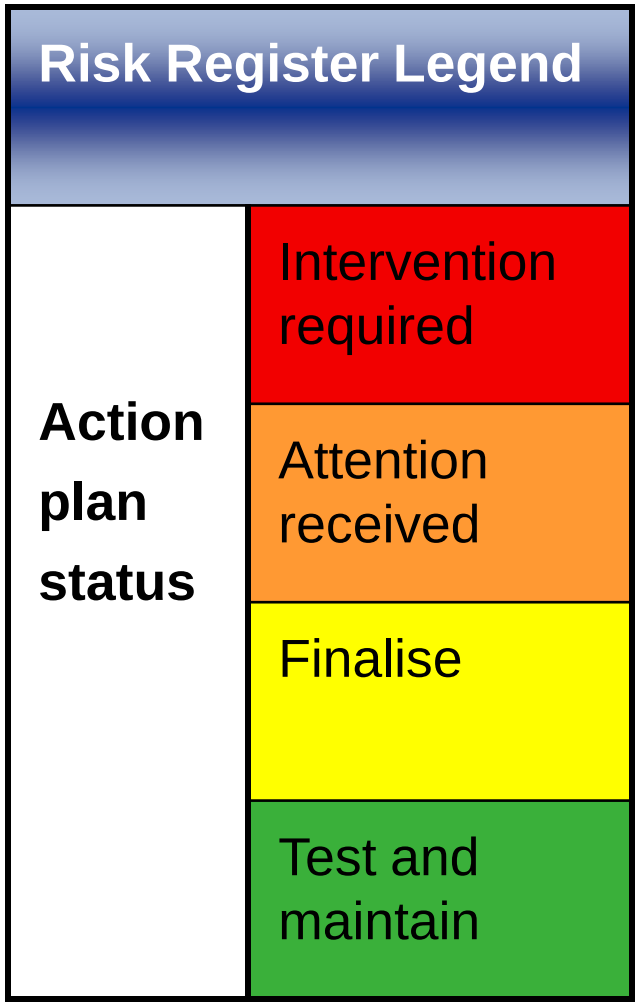
3. Reviewing implementation of risk responses

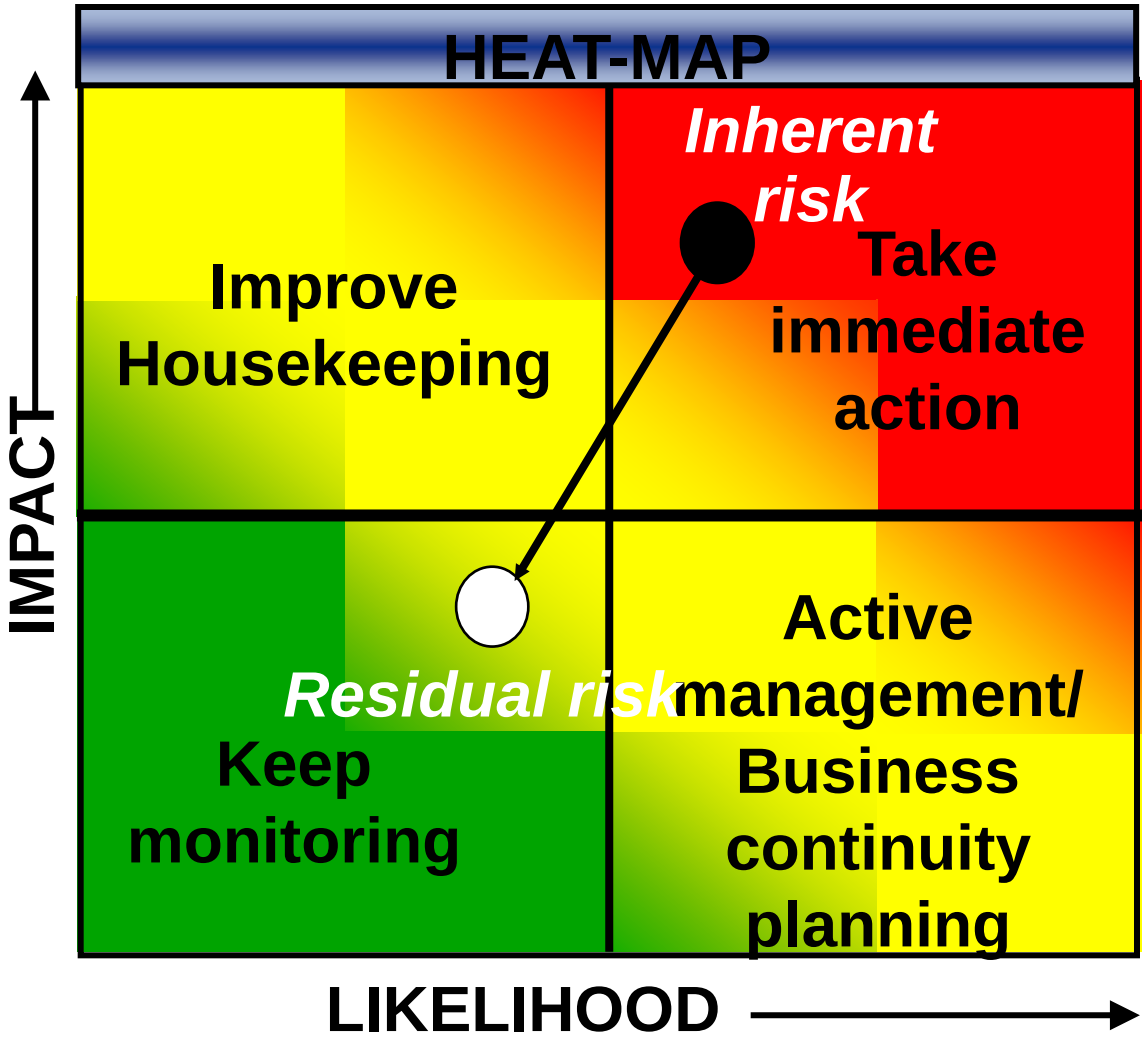
4. Reporting on success of implementation and changes in overall risk profile

Enterprise Risk Management
Risk monitoring

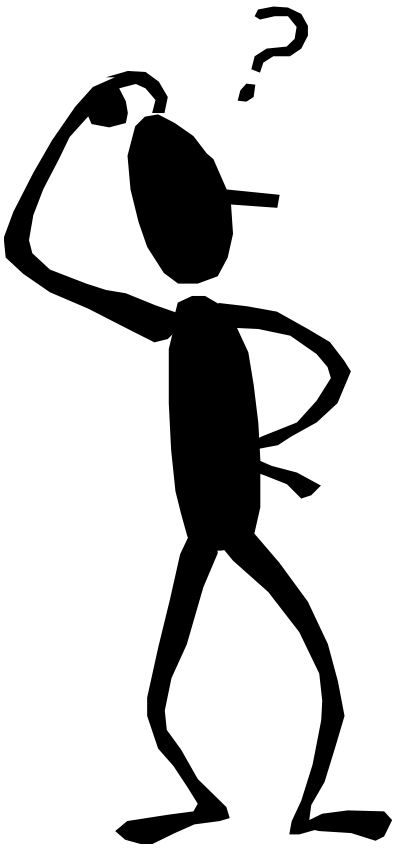
Risk monitoring should be done everyday, however it is important for organizations to developed structured ways of ensuring that key risks are well monitored.

Monitoring Heat maps





Questions?



Thank you

Benson Kamunya

Manager, Risk Consulting

KPMG Kenya

+254 20 2806000

bkamunya@kpmg.co.ke