The role of Boards in setting the risk appetite frameworks and in Enterprise Risk Management implementation programs.

By: CPA Frank Mwiti

Eastern Africa Markets Leader, EY Africa

June 2021

Agenda

1. Risk appetite as performance appetite

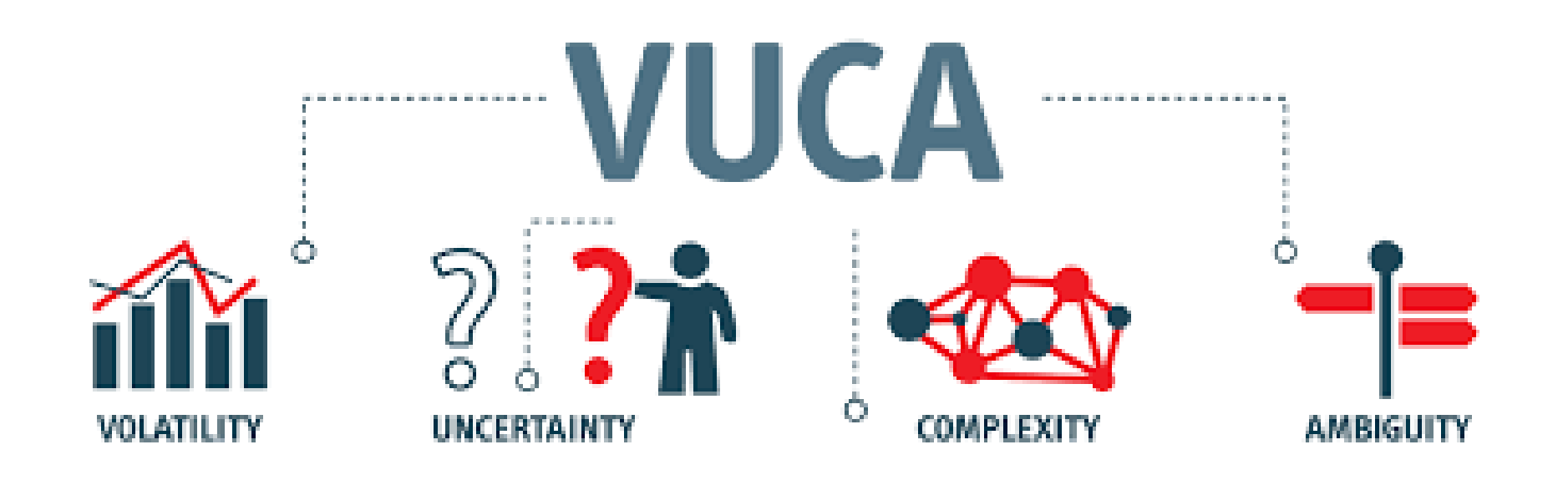
2. Upside, downside and outside risks

3. Alignment with ERM

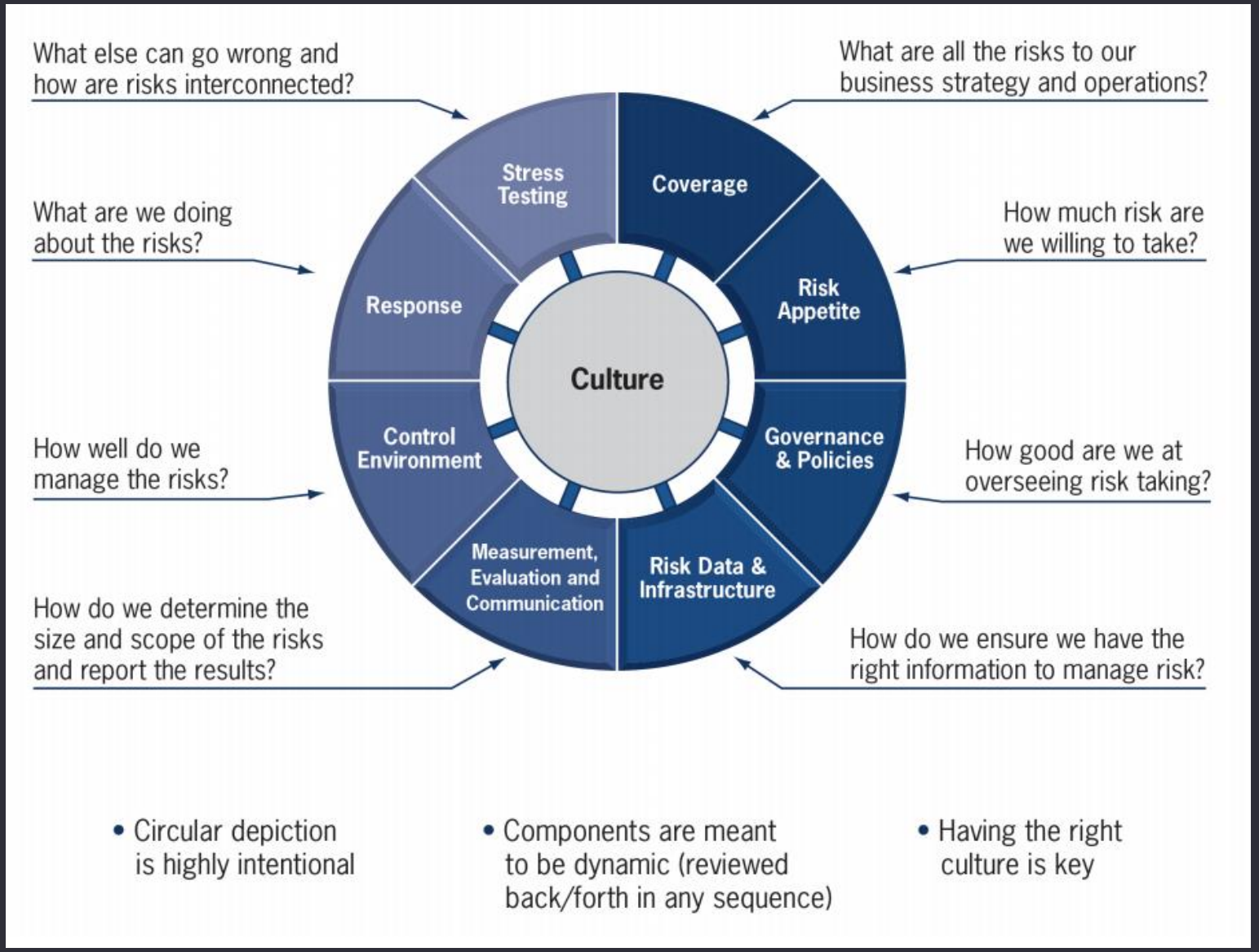
Agenda

1. Risk appetite as performance appetite

"Risk appetite" is a nebulous term and a moving target, which negates effective risk-taking — and the gains it would otherwise make possible.

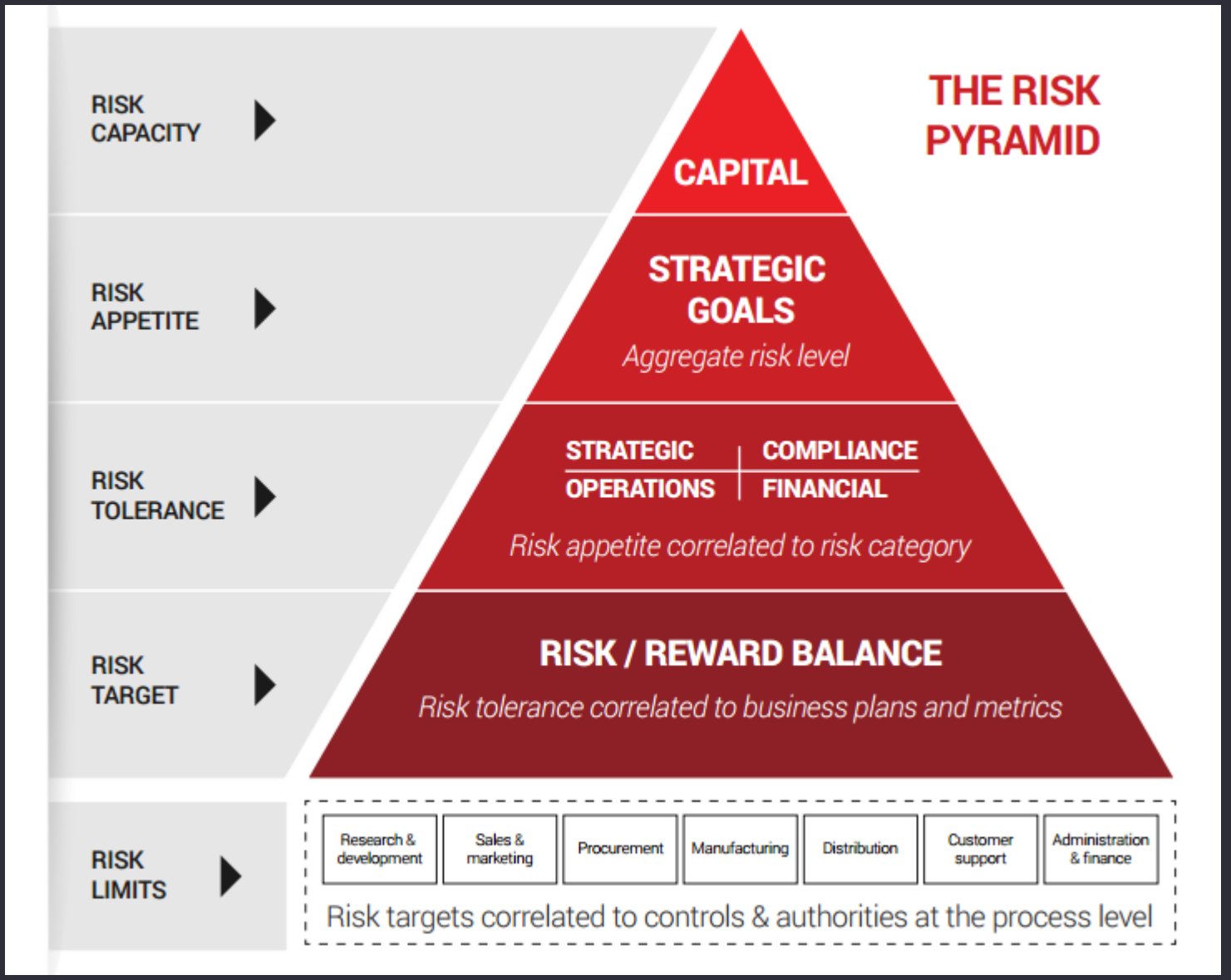


ERM is the capability to effectively answer the following questions

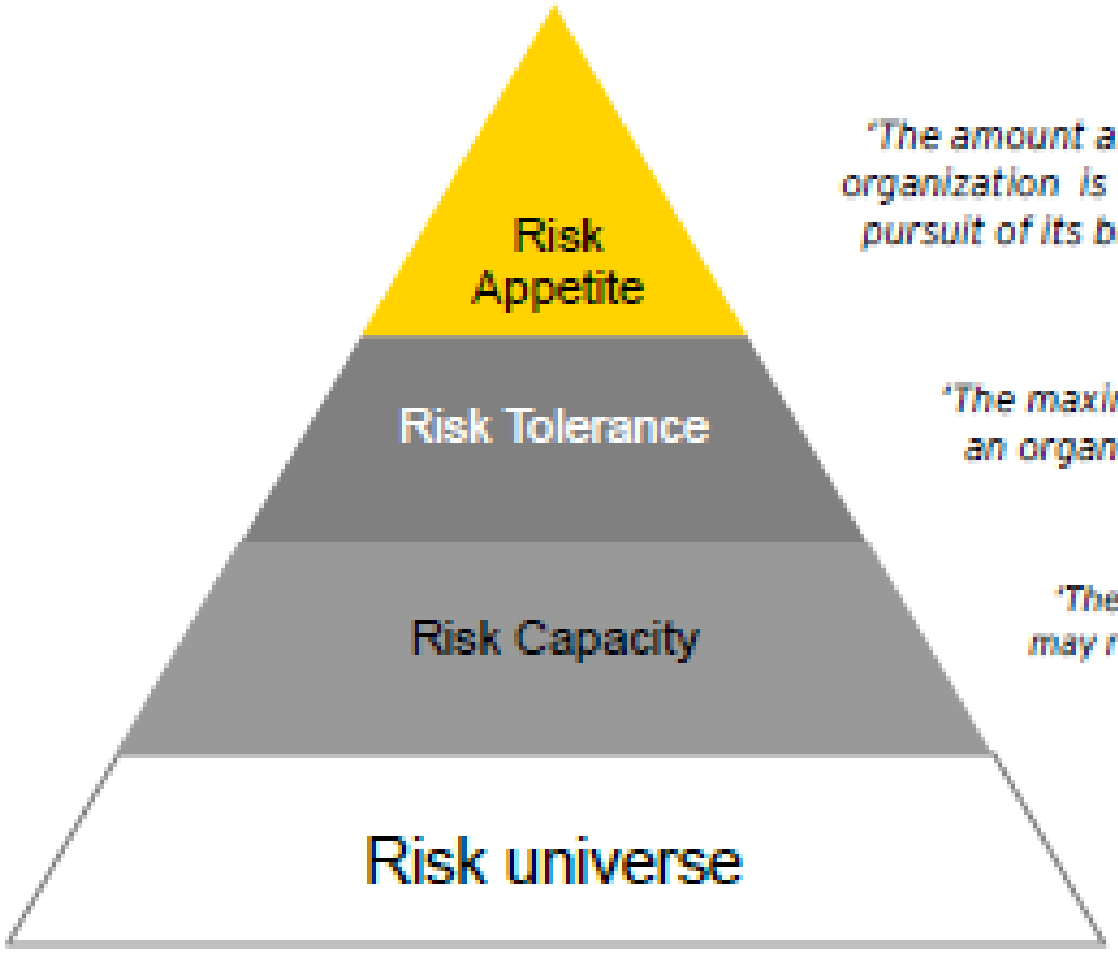


- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

The Risk Pyramid



Risk Appetite



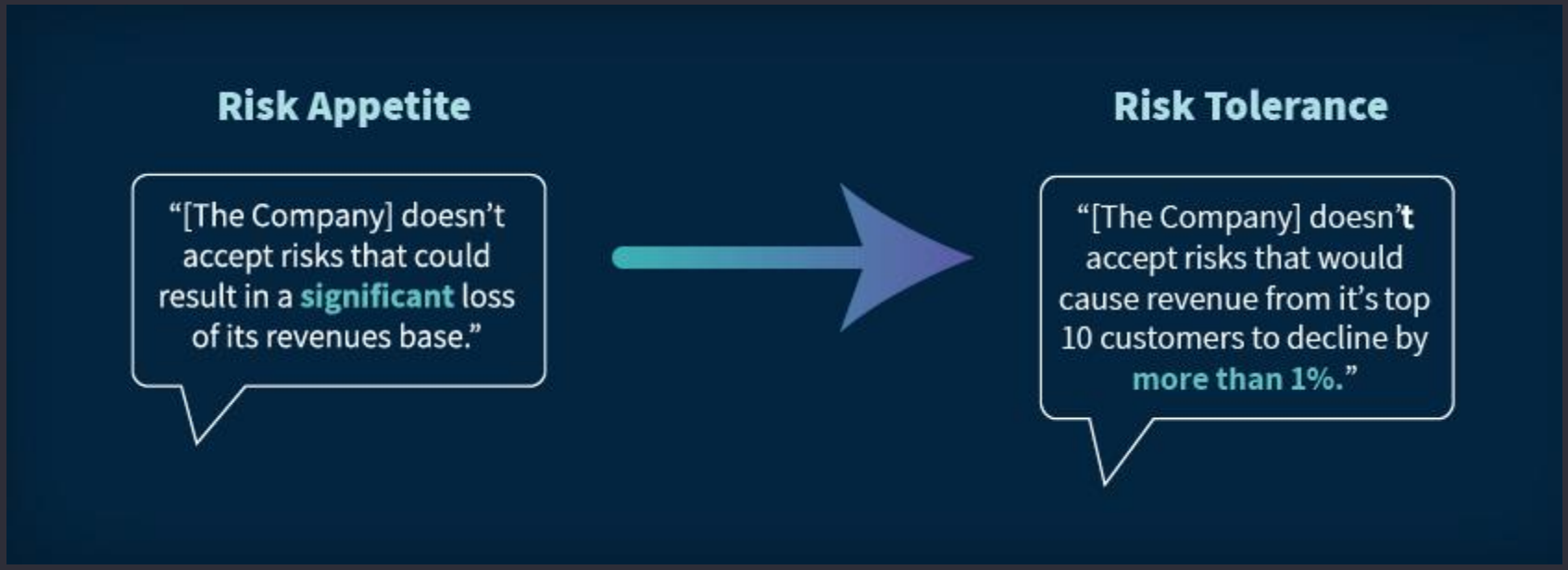
'The amount and type of risk an organization is willing to accept in pursuit of its business objective'

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

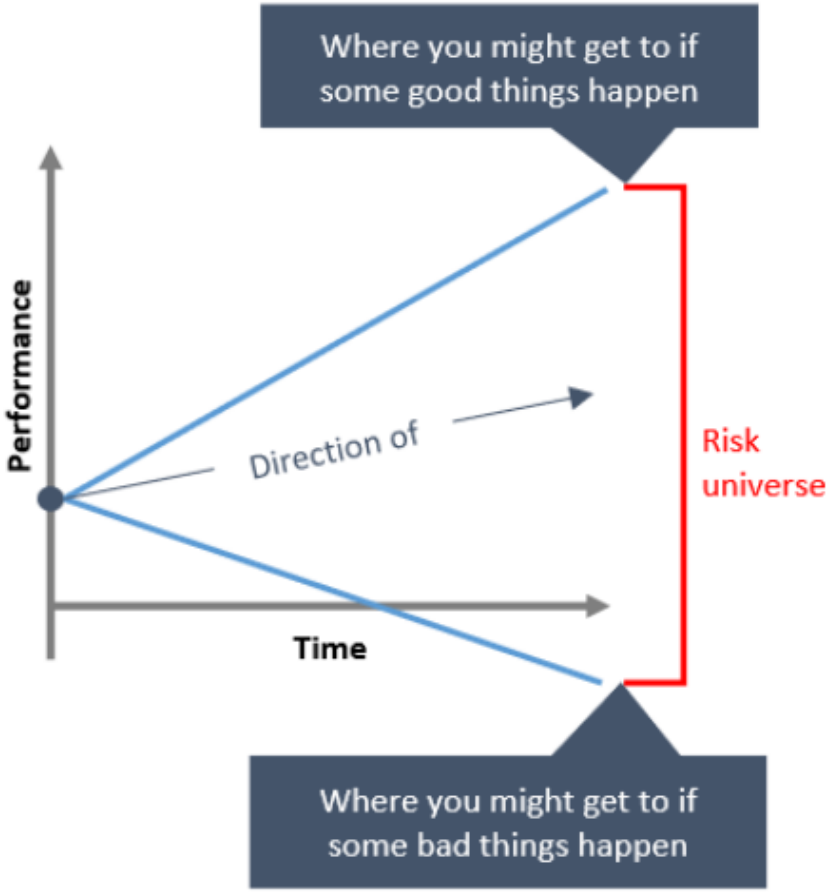
'The maximum level of risk an organisation may run given its capital and liquidity position and other restrictions'.

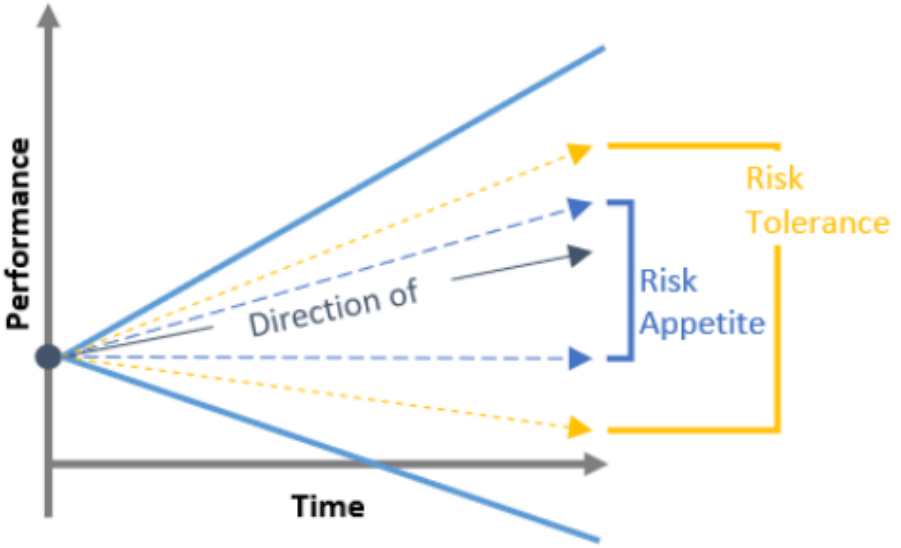
'All potential risks of the organization'.

Risk appetite focuses on the level of risk an organization deems acceptable whereas risk tolerance focuses on the acceptable level of variation around risk objectives.



Understanding the relationship between risk appetite and threshold





To better balance risks to performance, organizations should redefine the way appetite is measured.

We are living in the Transformative Age:

- Shifting organizational models
- Industry convergence
- Technology

One of the few certainties in this VUCA environment is that risks are abundant.

To better understand and balance risks and performance, the definition of appetite needs to be understood and measured from a more performance-centric approach.

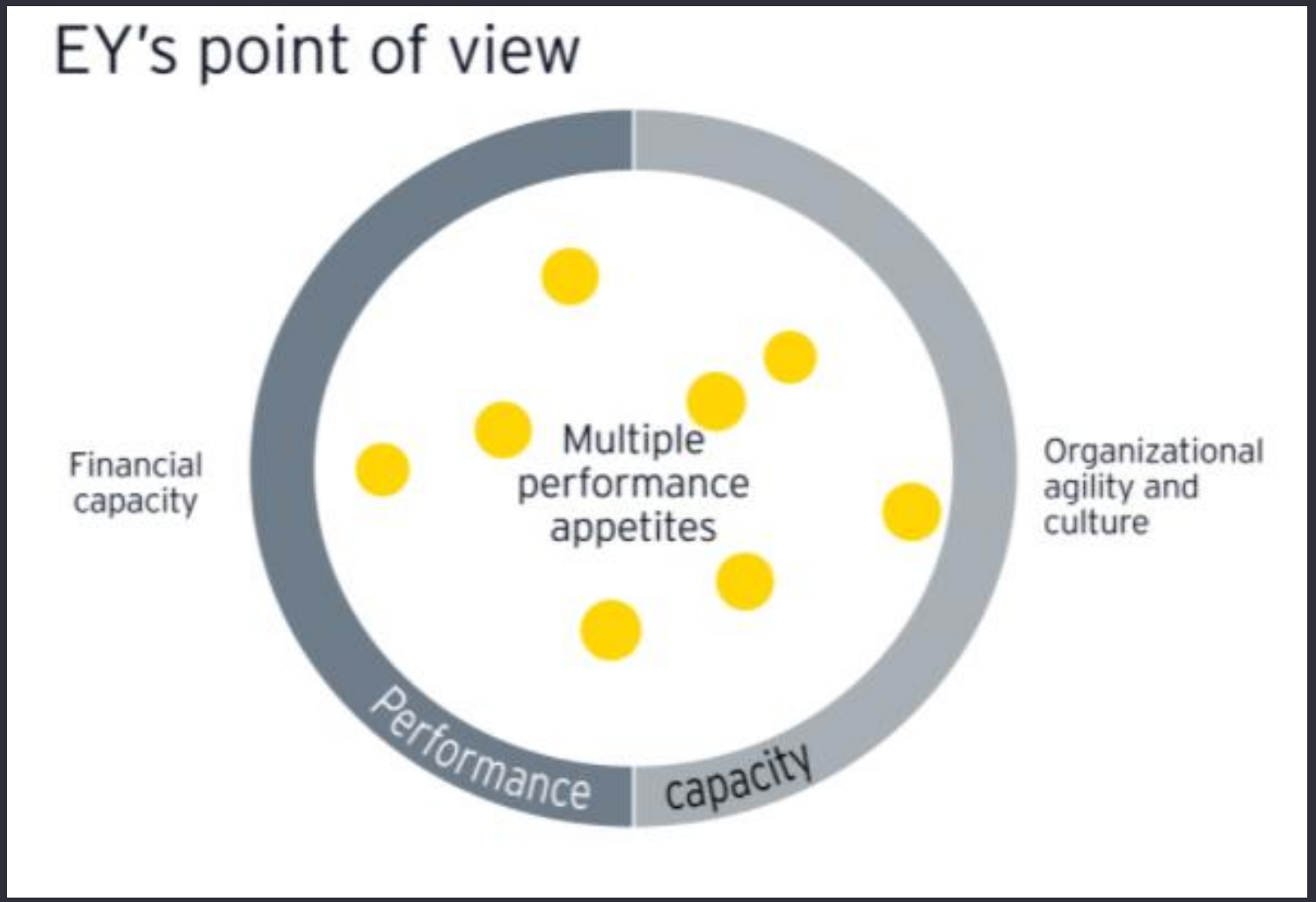
Definition	Standards	Perspective
Risk appetite: amount and type of risk that an organization is willing to pursue or retain	ISO 2002, Guide 73 Risk Management Vocabulary	Downside risk focus only Compliance oriented
Risk Appetite: Amount and type of risk that an organization is prepared to seek, accept or tolerate.	BSI 31100	
Risk Tolerance: organization's readiness to bear the risk after risk treatments in order to achieve its objectives. Note: risk tolerance can be limited by legal or regulatory requirements.		
No standard definition, focus on risk criteria and other risk management concepts	BSI 31100 2008, ISO 31000 2019	
Risk Appetite is a component within the Internal Environment in the COSO ERM cube. amount of risk, on a broad level, an organization is willing to accept in pursuit of value.	COSO ERM 2004	
Tolerance: **Risk Tolerance**: What is the acceptable level of deviation an organization is willing to accept in shooting for its goals?		
References the COSO ERM 2994 definition. The guide as a whole elevates the ERM's role in supporting performance but no explicit redefinition of risk appetite to align with this expanded focus	COSO ERM 2017	Includes upside risk focus Performance Oriented
When considering threats, the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realized. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance.	HM Treasury, Orange Book 2004	
When considering opportunities, the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses mWay be incurred with or without realising the benefits).		
The amount of risk that an organization is willing to seek or accept in the pursuit of its long-term objectives.	Institute of Risk Management, Risk Appetite Guidance Paper 2011	
Risk appetite is about what the Board does want to do and how it goes about it.		
Risk tolerance: The boundaries of risk-taking outside of which the organizsation is not prepared to venture in the pursuit of its long termlong-term objectives.		
In the IRM definition, **risk tolerance** is broader than risk appetite – with risk appetite focused specifically on active risk seeking or acceptance in pursuit of objectives		
Risk appetite is the amount of risk an organization is willing to accept on a broad level in pursuit of its objectives given consideration of costs and benefits.	**Playbook: Enterprise Risk Management for the U.S. Federal Government, 2016** *Aligns with Office of Management and Budget Circular A-123*	

The degree of variation in performance that executive management and the board are willing to accept on an aggregate basis in relation to strategic and business objectives is the organization's "performance appetite."

Why redefine risk appetite as performance appetite?

- Is less subjective or based on respective risk owners' views of the risk
- Enables effective decision-making
- Is easier to understand and helps management relate to day-to-day operations
- Expands focus from downside risk during implementation to a holistic view of upside, downside and outside risks
- Is easier to measure, avoiding confusion and churn on what is acceptable
- Ties into established KPIs
- Aligns with leading practice, COSO ERM 2017
- Intuitive people can relate to it, and most organizations already do it in some way in their day-to-day operations

The Shift = Just as risk appetite raises the question of "risk capacity," performance appetite raises the question of "performance capacity."



"There is no single … appetite, but rather a range of appetites for different types of risk and this range of appetites needs to align under, and be consistent with, an overall … appetite framework" IRM 2011

In simple terms, an organization's performance capacity is driven by two main elements:

1. Financial Capacity - the financial limit of an organization's ability to absorb losses with its own funds or borrowed funds without major disruption.

2. Organizational agility - includes organization's ability to harness other forms of capital in a responsive and rapid way. Other forms of capital may include resources (e.g., infrastructure, assets and people), relationships and knowledge.

Agenda

2. Upside, downside and outside risks

Trust by design: looking at risk identification in the Transformative Age

Efforts to identify and evaluate risks tied to strategic goals and objectives must consider:

- Risks that organizations know well and are capable to prevent or effectively mitigate
- Risks that are recognized as inherent to strategy and demand more focus
- Risks that are not fully recognized and may not be capable to prevent

Trust by Design – expanding consideration of risks that cause variation in performance: upside, downside, outside

Upside risks

Risks that offer benefits – risk that are significant to the organization's ability to execute its business strategy and achieve its objectives

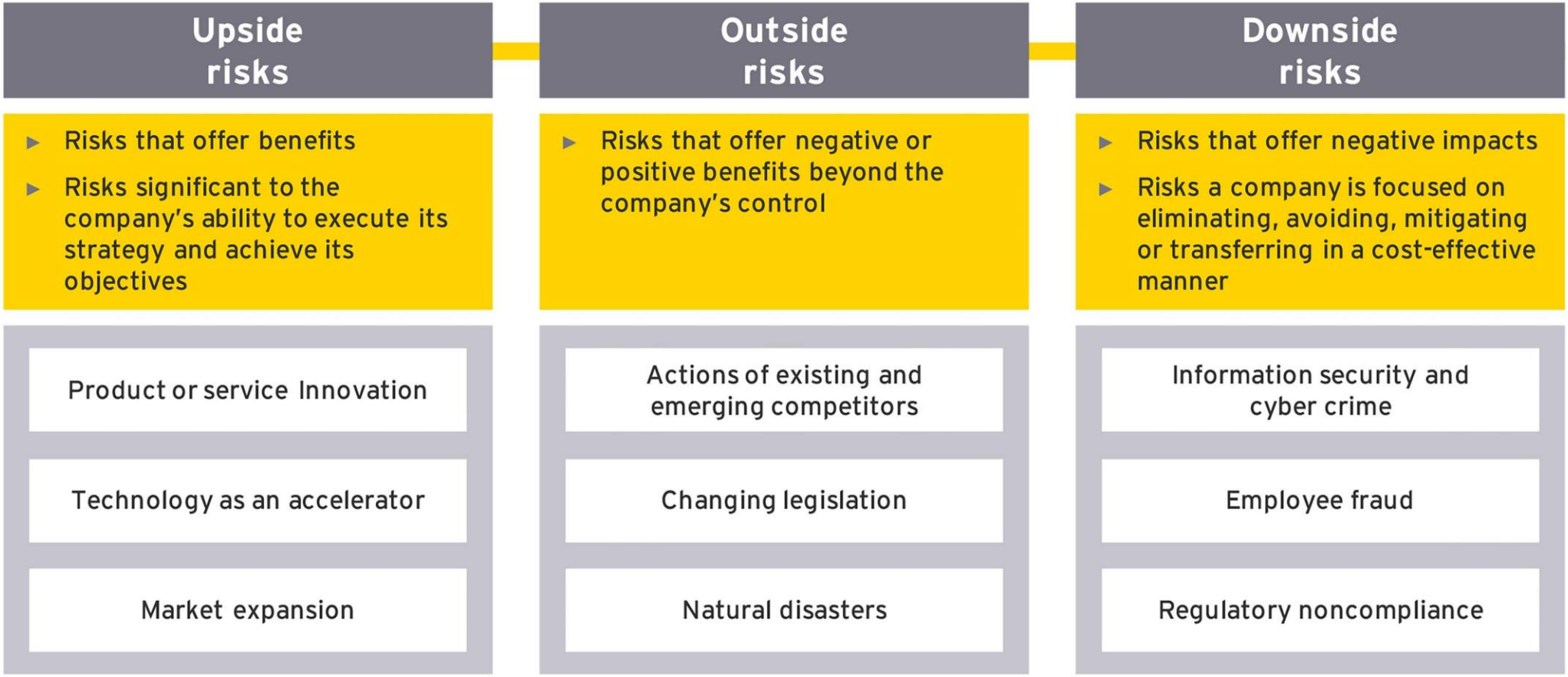
Downside risks

Risks that offer negative impacts – risks that an organization is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner

Outside risks

Risks that offer negative or positive benefits beyond the organization's control

Each of these risk categories requires a different management approach that will benefit organizations.



Upside risks – offer benefits and present opportunities to enable business strategy and achieve performance management objectives.

Upside risks cannot be managed through a rules-based control framework. The approach to managing those risks requires the selection of risk-strategic risks to take, such as:

- Improving an organization's ability to manage risk events if they occur
- Establishing risk tolerances
- Predicting the impact of possible risk events
- Monitoring of key risk indicators (KRIs)

Outside risks – risks that arise from events outside of the organization's control. These risks can offer negative and/or positive benefits.

Addressing these risks requires a different approach, one that includes identification and mitigation of their impact through scenario analysis and stress testing to determine whether the organization has the minimum resources to weather the full impact of external events.

Organizations cannot influence the likelihood of these events, but they can be prepared and reduce the cost of an impact.

Examples include:

- Competition
- Legislation
- Natural Disasters

Downside risks – internal risks that arise within the organization that are controllable and should be eliminated or avoided. These risks present only negative impacts.

The approach to managing these risks comes through active prevention and designing the controls to mitigate these risks. Much of the investment in the controls framework will be driven by preventable risks. It also provides structured monitoring of the threat level of the identified preventable risk.

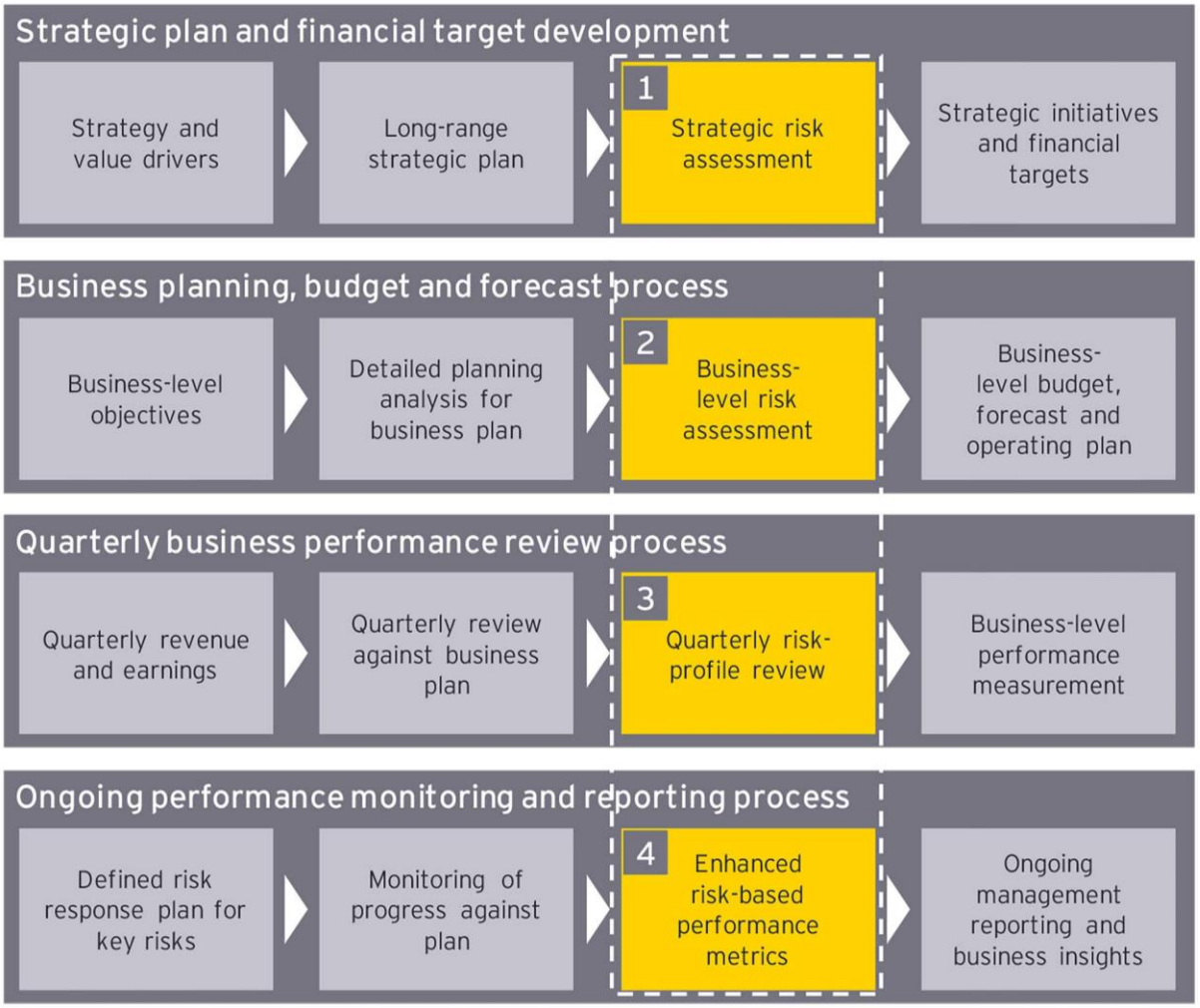
Examples include:

- Cybersecurity
- Fraud
- Regulatory noncompliance

Agenda

3. Alignment with ERM

Aligning risk, performance and tolerance within ERM



1 Strategic risk assessment

Creates enterprise-level risk profile aligned to strategy and business objectives

2 Business-level risk assessment

Provides basis for structured consideration of risk relative to business plan process

3 Quarterly risk profile review

Routinely challenges the impact of key risks on budget, plan, forecast and performance

4 Enhanced risk-based performance metrics

Enhances the monitoring of business performance with key risk and control factors

Get in touch:

Frank.Mwiti@ke.ey.com

+254706221597

EY

Building a better working world