ICPAK
Uphold Public Interest

A case for ERM

Presentation by:

Stella Simiyu
Chief Operating Officer,
Sentinel Africa Consulting Ltd
Wednesday, 5th July 2017

Presenters Bio

Stella’s Bio	
Name	Makona Stella Simiyu
Bio	Stella has over 11 years work experience in Enterprise Risk Management. She was working as the Principal Enterprise Risk Manager-Safaricom and then the Head of Operational Risk Management at Bharti Airtel managing 17 countries before she embarked on Risk Management Consulting with Sentinel Africa. She holds a Bachelor of Commerce Degree from Strathmore University and is a Certified Enterprise Risk Manager CERM, Certified ISO 31000 Lead Risk Manager, Certified in Risk and Information Systems Control, AMBCI-Business Continuity Institute), ISO 27001:2013 Lead Implementer and Auditor Information Security Management) and ISO 22310 Lead Implementer and Auditor (Business Continuity Management).

The Art of Winning

- ❑ Most master chess players are 3 steps ahead of their opponents
- ❑ They are able to perceive and mitigate risks before they occur

- ❑ **ISO 31000**, **risk** is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected.

Our world today: The great disrupters of our time

ICPAK
Uphold Public Interest

□ Globalisation

□ Social Media

□ Outsourcing

□ Artificial Intelligence & other new Technologies

□ Cyber Security

□ Terrorism

So who are you and who can run you out of business?

- ❑ Brand
- ❑ Customer Demographics
- ❑ Technologies I use
- ❑ Products I sell
- ❑ Regulators
- ❑ My suppliers
- ❑ Employees

Five Questions every Manager must know

- ❑ What is our goal as business?
- ❑ What are our key strategies to get there?
- ❑ What can stop us?
- ❑ What can I do about it in the short/long term ?
- ❑ How well are we doing now?

What ails most organisations!

- ❑ No policy and our guidelines for assessing and managing risks?
- ❑ Poor understanding of cross cutting dependencies internally and externally?
- ❑ No documented risk appetite?
- ❑ No analysis of risk capacity?
- ❑ No assignment of responsibility on who can take on risk on behalf of the company?

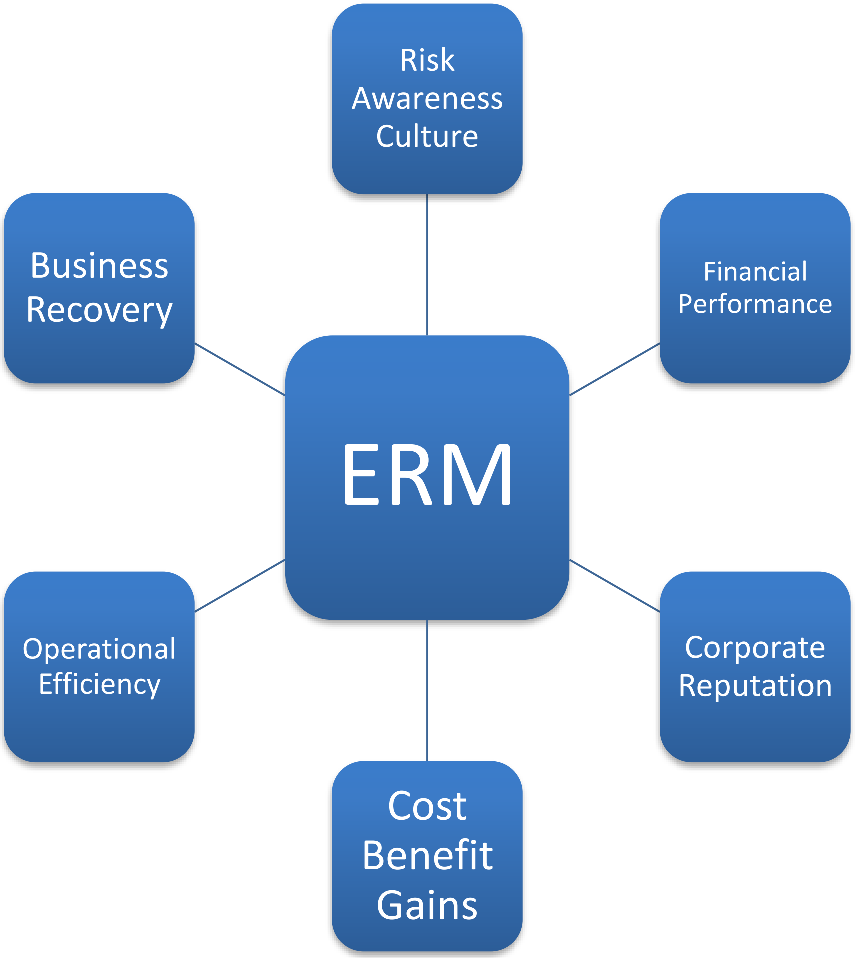
Common Approaches to assessing risk?

- ❑ Siloed approach focus on managing specific risk areas e.g H& S, Physical Security
- ❑ Use of checklists
- ❑ Dependency on auditors or risk managers to identify risks
- ❑ Compliance based
- ❑ Risk quantification that is not comparable across organisation
- ❑ Risk philosophy that is centered around avoidance

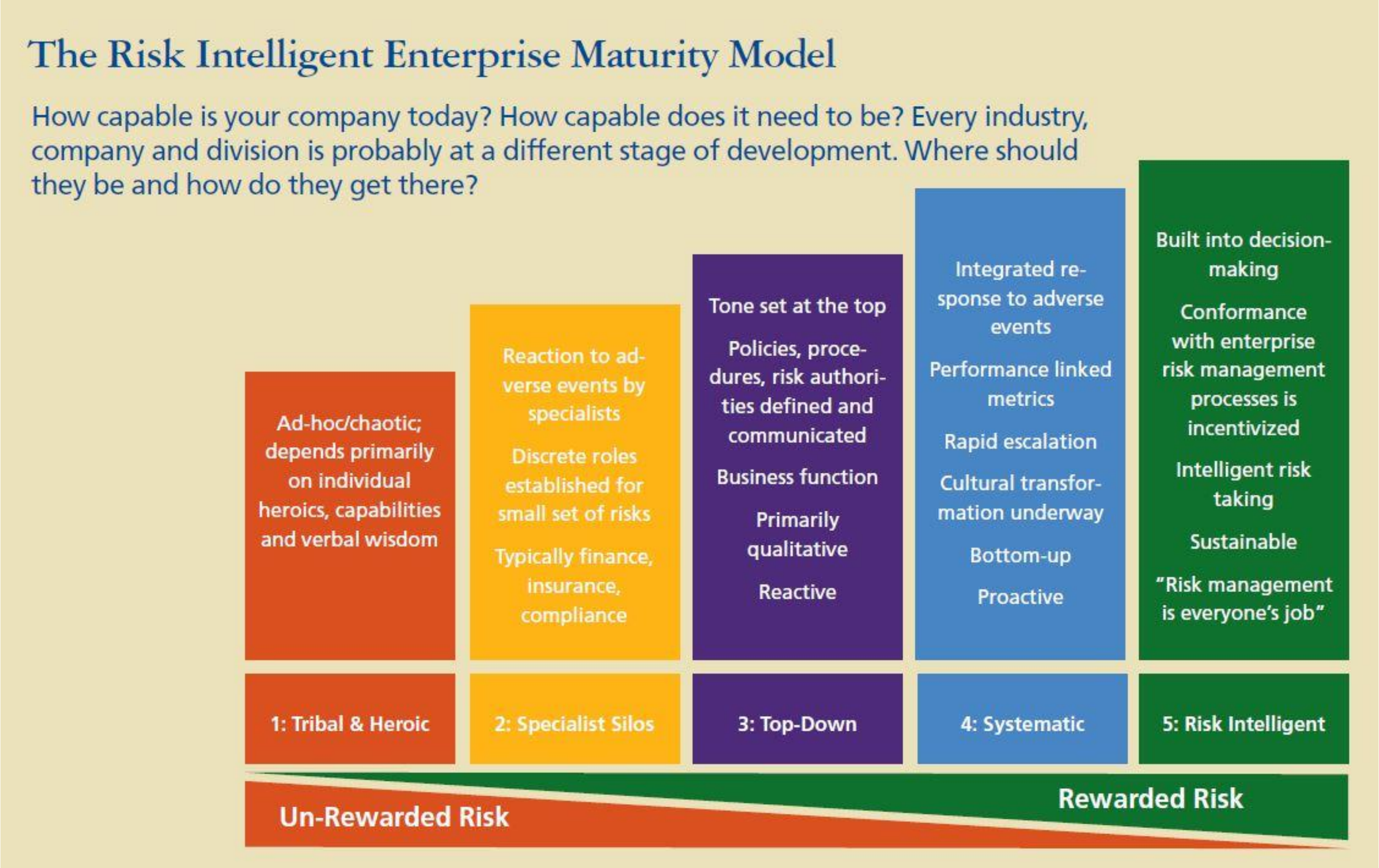
Common Approaches to assessing risk?

- Siloed approach focus on managing specific risk areas e.g H& S, Physical Security
- Use of checklists
- Dependency on auditors or risk managers to identify risks
- Compliance based
- Risk quantification that is not comparable across organisation
- Risk philosophy that is centered around avoidance

Why ERM and Why Now?



Rewarded vs Unrewarded Risk



The Risk Intelligent Enterprise Maturity Model

How capable is your company today? How capable does it need to be? Every industry, company and division is probably at a different stage of development. Where should they be and how do they get there?

1: Tribal & Heroic

Ad-hoc/chaotic; depends primarily on individual heroics, capabilities and verbal wisdom

2: Specialist Silos

Reaction to adverse events by specialists

Discrete roles established for small set of risks

Typically finance, insurance, compliance

3: Top-Down

Tone set at the top

Policies, procedures, risk authorities defined and communicated

Business function

Primarily qualitative

Reactive

4: Systematic

Integrated response to adverse events

Performance linked metrics

Rapid escalation

Cultural transformation underway

Bottom-up

Proactive

5: Risk Intelligent

Built into decision-making

Conformance with enterprise risk management processes is incentivized

Intelligent risk taking

Sustainable

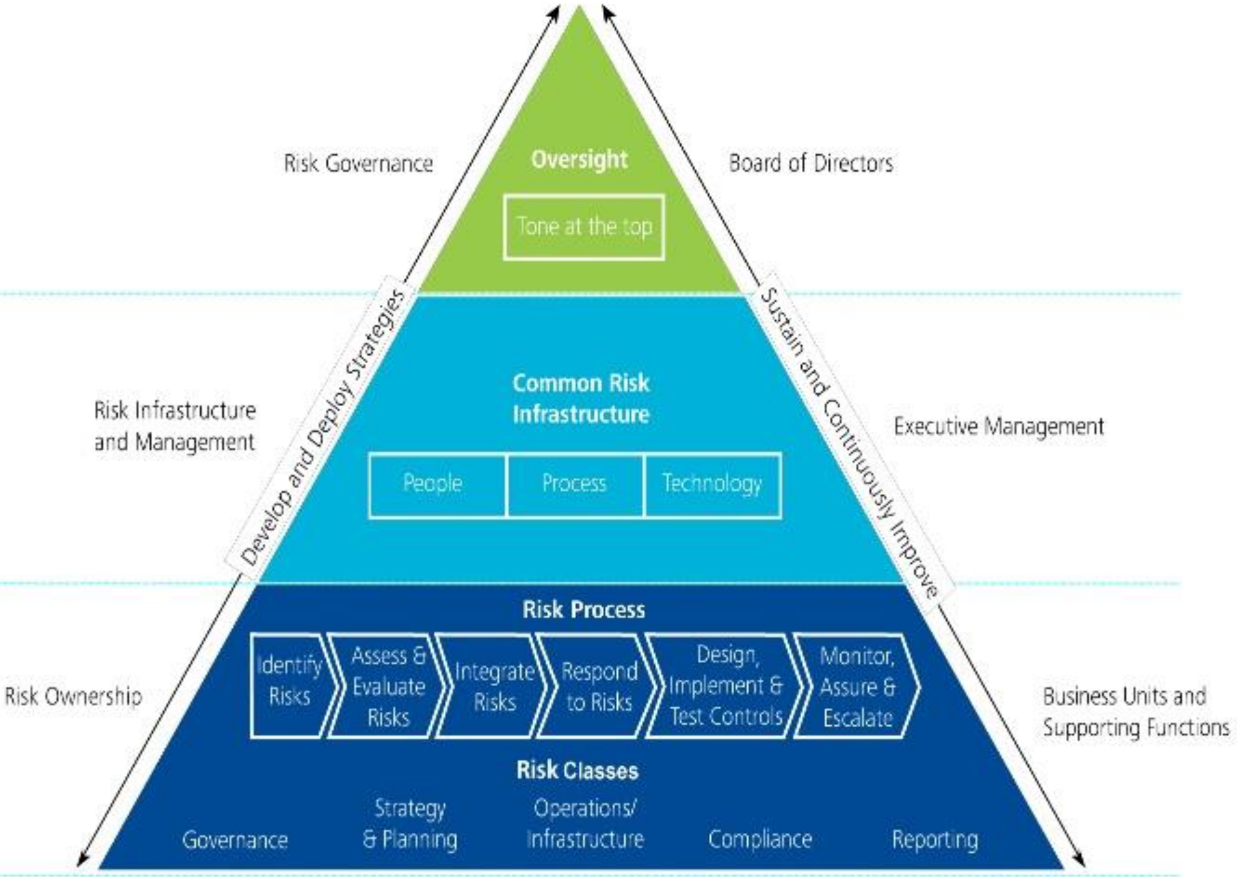
"Risk management is everyone's job"

Risk Intelligence

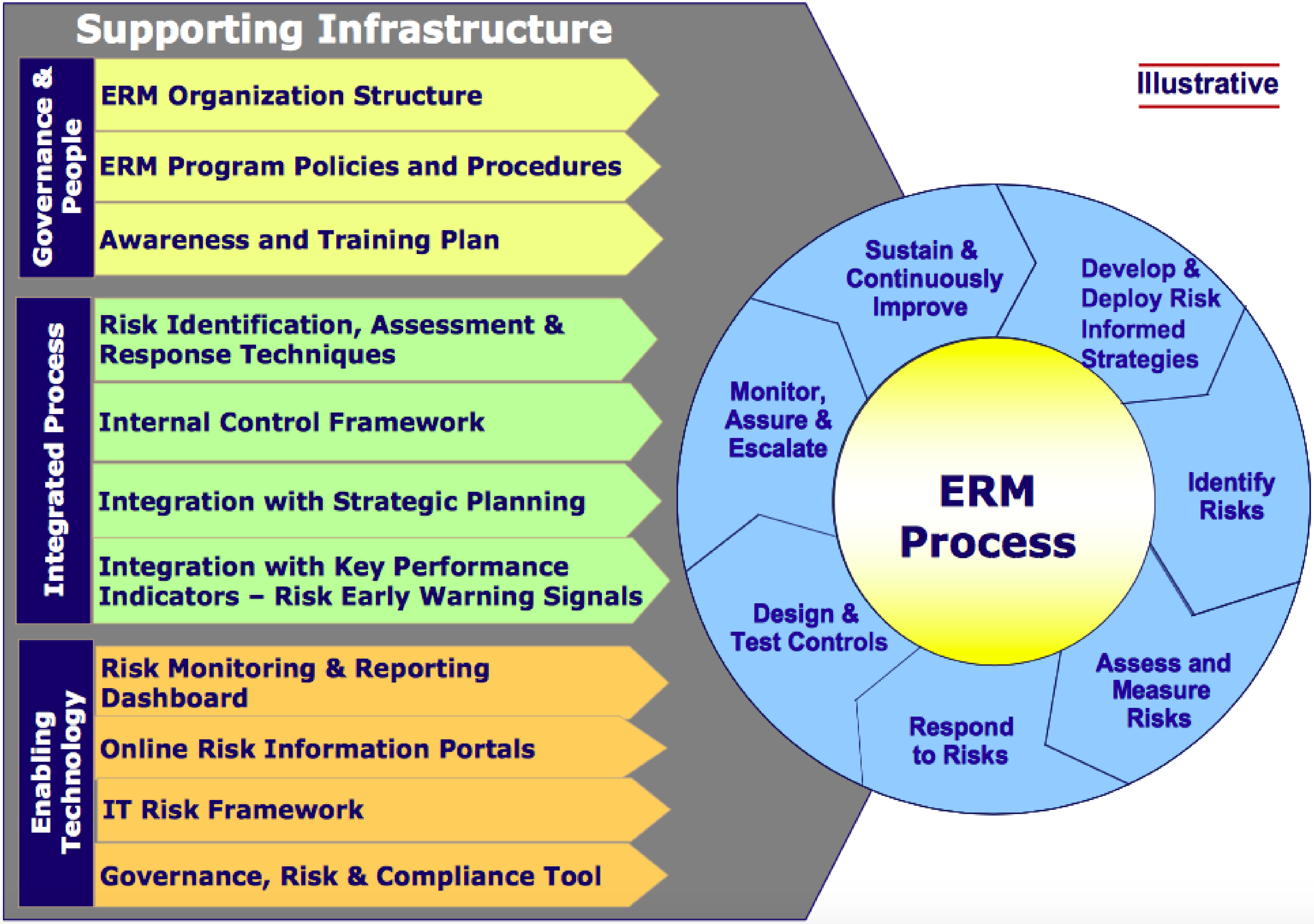
Nine Principles for Building a Risk Intelligent Enterprise

- **Governing Bodies Responsibility**
- **Roles & Responsibilities**
- **Common Definition of Risk**
- **Common Risk Framework**
- **Common Risk Infrastructure**
- **Executive Management Responsibility**
- **Objective Assurance and Monitoring**
- **Business Unit Responsibility**
- **Support of Pervasive Functions**

The Risk Intelligent Enterprise



Components of a Risk Intelligent Enterprise



Illustrative

Supporting Infrastructure

Governance & People

- ERM Organization Structure
- ERM Program Policies and Procedures
- Awareness and Training Plan

Integrated Process

- Risk Identification, Assessment & Response Techniques
- Internal Control Framework
- Integration with Strategic Planning
- Integration with Key Performance Indicators – Risk Early Warning Signals

Enabling Technology

- Risk Monitoring & Reporting Dashboard
- Online Risk Information Portals
- IT Risk Framework
- Governance, Risk & Compliance Tool

ERM Process

- Develop & Deploy Risk Informed Strategies
- Identify Risks
- Assess and Measure Risks
- Respond to Risks
- Design & Test Controls
- Monitor, Assure & Escalate
- Sustain & Continuously Improve

Risk Oversight
Typical Roles and Responsibilities

Illustrative

Board of Directors & CEO

The Board of Directors has ultimate ***accountability*** for all risk but can delegate ***responsibility*** to senior management

CRO & Risk Committee

"ERM Oversight"

Clearinghouse for risks,
policy, appetite setting, and governance

Business Areas

"Manage Risks"

- Risk identification
- Risk self-assessments
- Strategy and actions to address risk within policy
- Ensure compliance with ERM policies and procedures
- Provide assertions on risk exposure

ERM Organization

"Supports CRO, Risk Committee, Management, and the Board"

- Governance, policy, and appetite implementation and coordination
- Risk assessment methods
- Measurement, aggregation, reporting rules and tools
- Monitor risk exposure status and report to Board

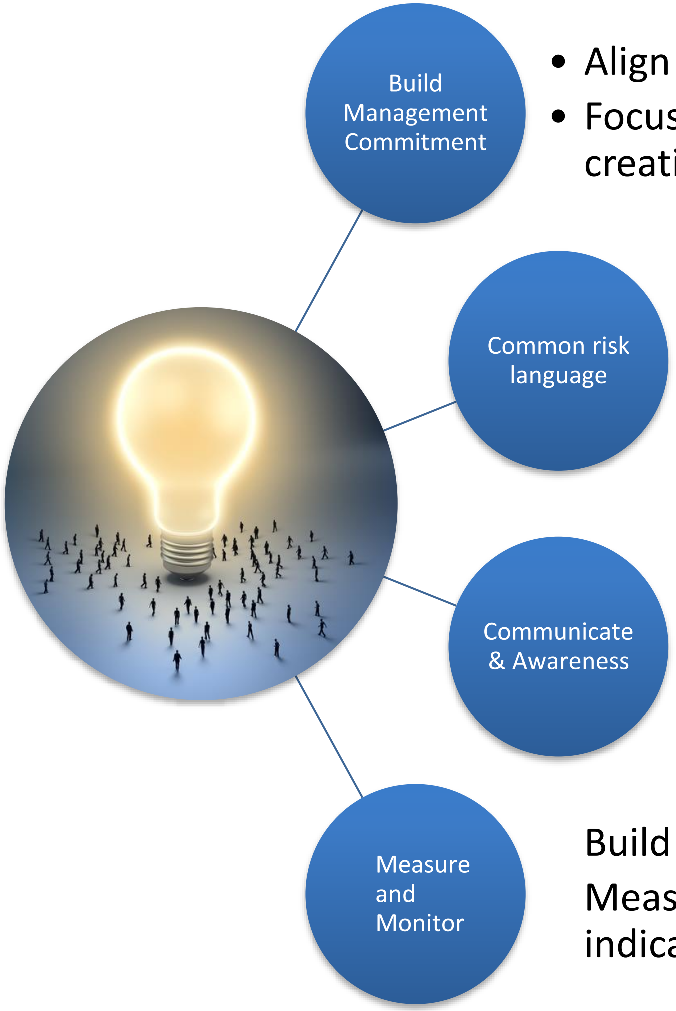
Audit

"Provides Independent Assurance"

- Periodic validation of control and compliance
- Objective review of risk management process
- Independent assurance to management and Board on assertions of risk exposure

How to improve your ERM efforts

□



Build Management Commitment

- Align to strategy
- Focus on value creation

Common risk language

Clearly articulate risk appetite

Invest in Risk automation

Communicate & Awareness

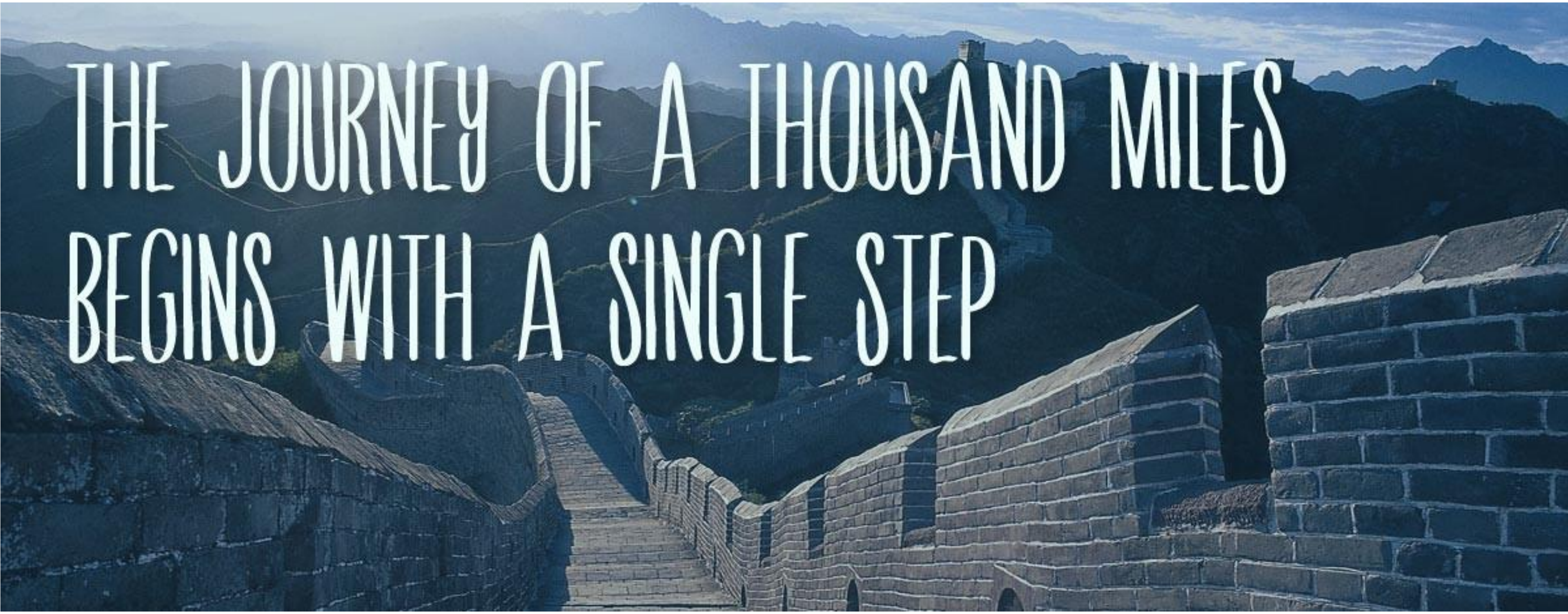
- Communicate upwards and downwards
- Training

Measure and Monitor

Build metrics

Measure risk indicators

Parting Shot



Start from where you are, start with what you have.