Presentation to BarnOwl Information Sharing Session Risk Maturity

Dr Arthur Linke

11th April, 2019

alinke@sun.ac.za

arthur@turricula.com

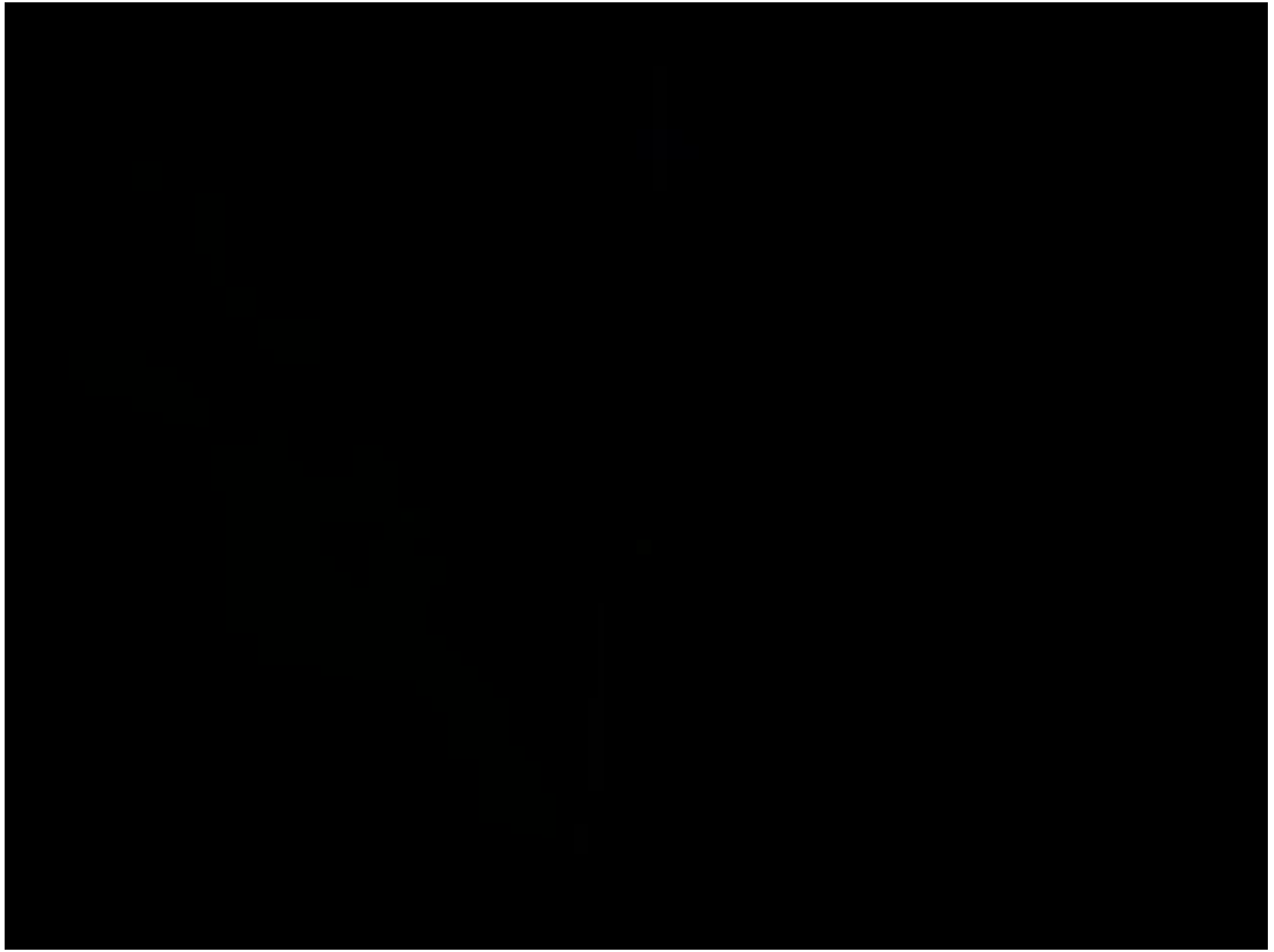
turricula

USB University of Stellenbosch Business School

Overview

- The Titanic - Kate & Leonardo
- What is ERM?
- Updates on COSO & ISO
- Risk maturity from various angles
- IRMSA – #impact
- Conclusion – lessons learned

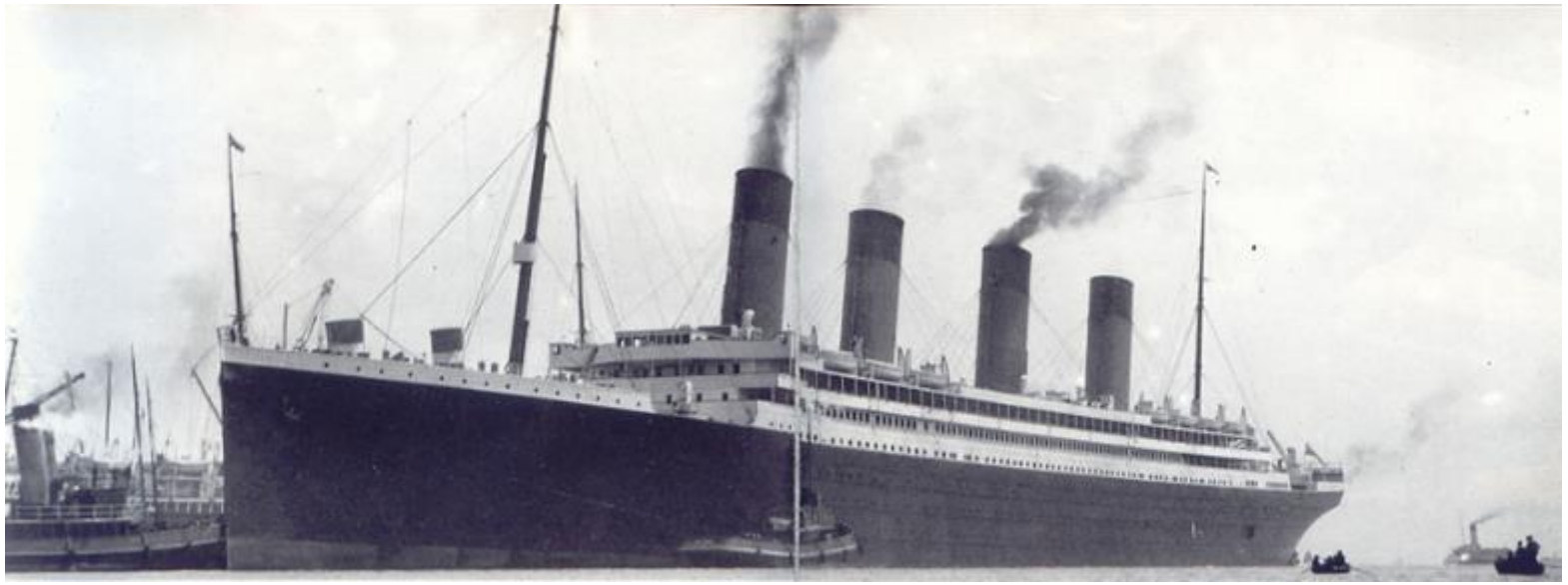
“Safety outweighing every other consideration”



turricula

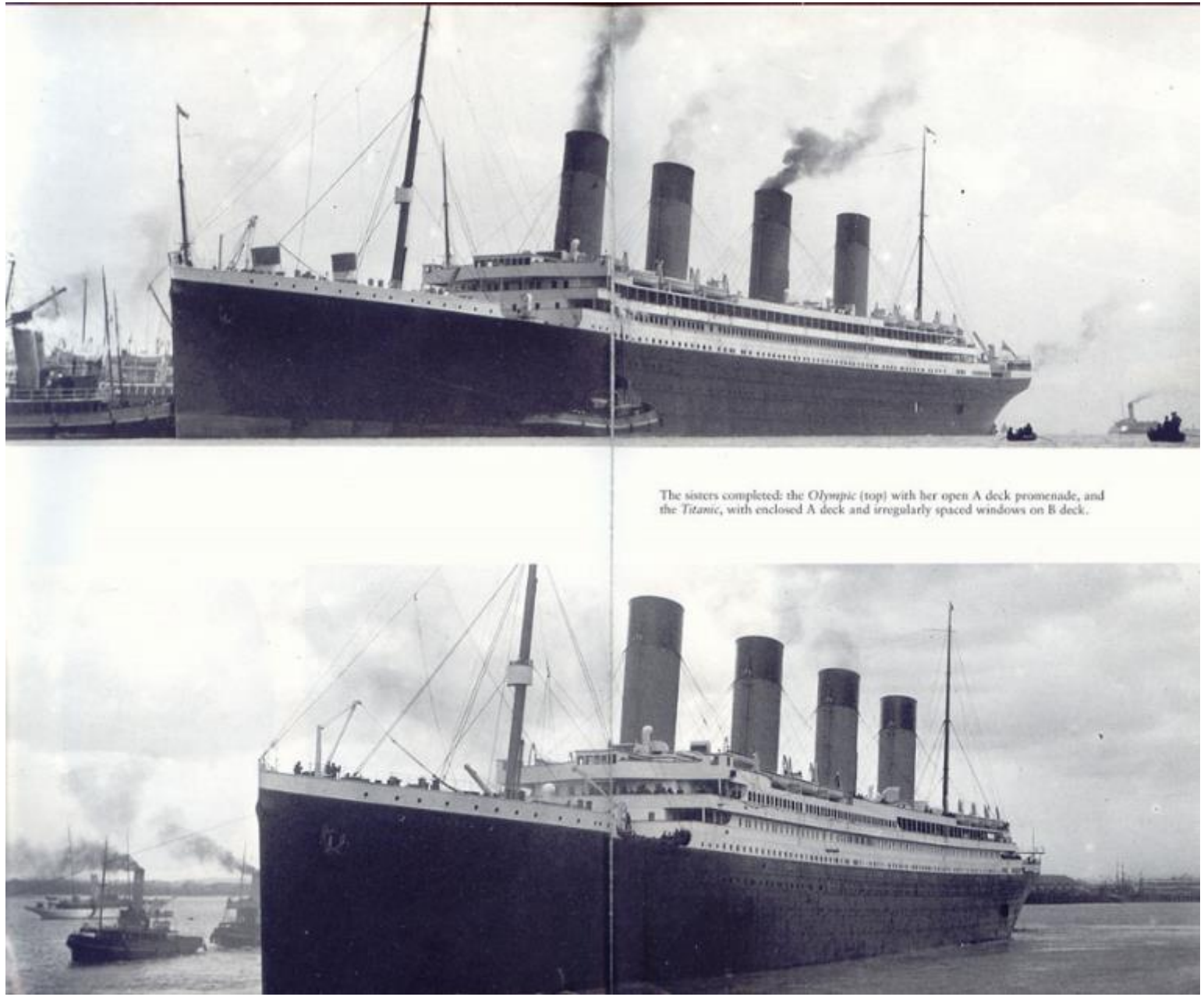
USB University of Stellenbosch Business School

Recognise this Ship?



White Star's *The Olympic*

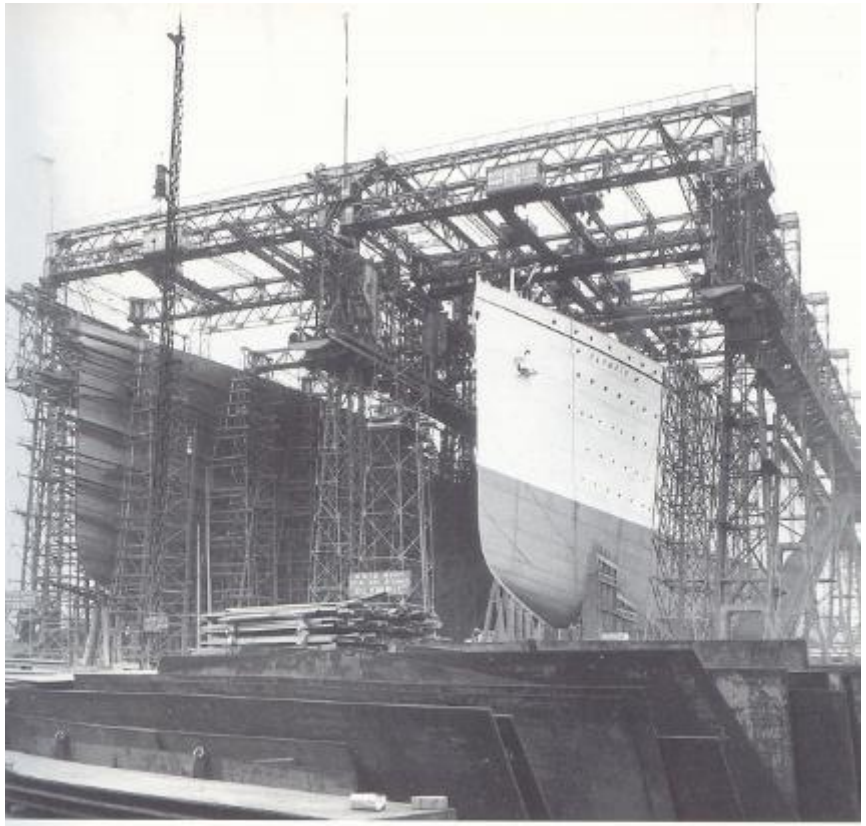
The Olympic:
Commissioned
14th June 1911



The sisters completed: the *Olympic* (top) with her open A deck promenade, and the *Titanic*, with enclosed A deck and irregularly spaced windows on B deck.

The Titanic:
Commissioned
11th April 1912

Olympic Class of White Star Steamers



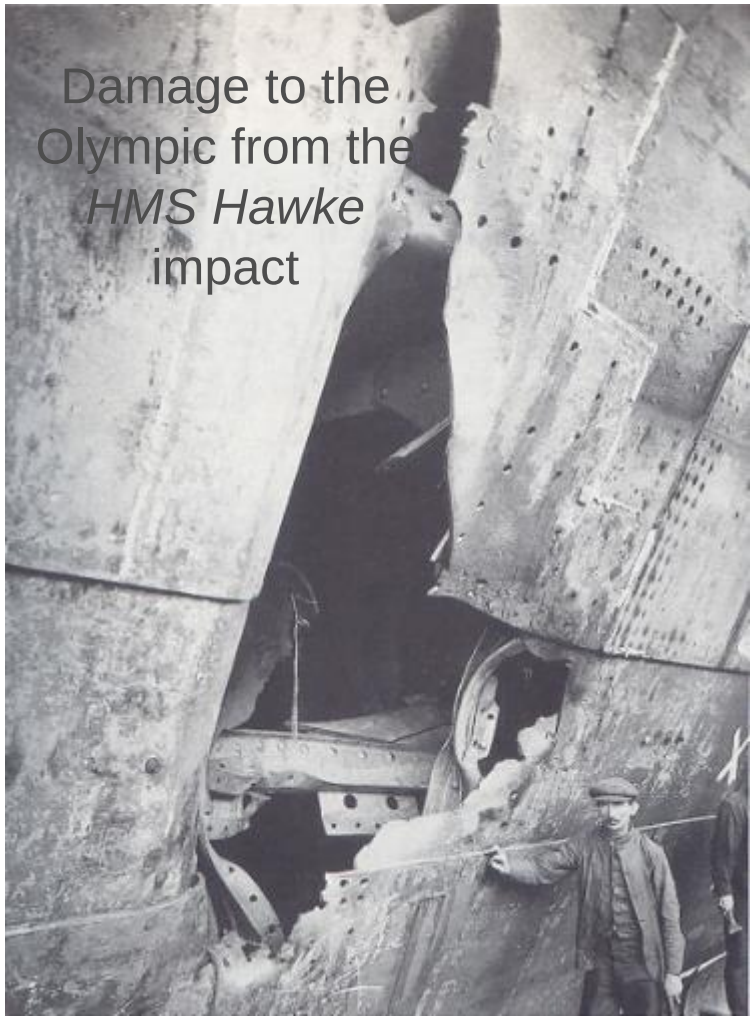
The sisters under construction at Harland and Wolff.

- Developed by JP Morgan's White Star shipping group
- Constructed by Harland & Wolff in Belfast included *The Olympic, The Titanic* and *The Britannic*
- Designed to compete with Cunard (QE2) & German Shippers on the prestigious transatlantic English Channel in the early 1900s
- Built for affluent travelers offering high-speed luxury

  - ❖ *The prized 'Blue Riband' was bestowed upon the ship with the fastest crossing. Held by Cunard's Mauretania 1907-1929*

Reference: 'The Riddle of the Titanic', Gardiner et. al. Orion, 1998

The Olympic – Prelude to Disaster



- 21st Jun 1911
  - Upon commissioning crashed into & almost sunk *O.L. Halenbeck* in Manhattan
- 20th Sep 1911
  - Crashed into the Naval Cruiser the *HMS Hawke* in Southampton
- 24th Feb 1912
  - Knocked-off one of its twenty-six ton propellers on a well-known wreck in the Grand Banks

Captained by Edward J. Smith.

Reference: 'The Riddle of the Titanic', Gardiner et. al. Orion, 1998

Captain Edward J. Smith

- 27th Jan 1889
  - Ran *The Republic* aground in New York
- 1st Dec 1890
  - Ran *The Coptic* aground in Rio de Janerio
- 4th Nov 1909
  - Ran *The Adriatic* aground outside New York

History of running ships too fast through narrow passages…. and of not adequately training his officers

Captain Smith was commissioned to command the Titanic – Maiden Voyage

Reference: 'The Riddle of the Titanic', Gardiner et. al. Orion, 1998

Titanic - Tragic Circumstances

- 14th April 1912
  - Smith received at least six warnings of an ice field from ships at dead stop in the area
  - No binoculars in the crow's nest meant that early warning was near impossible
  - Titanic sped toward ice field at 22.5 knots v/s a recommended 10 knots in such conditions
- Motivations for this speed
  - Desire to break the transatlantic speed record as encouraged by J. Bruce Ismay MD of White Star who was on board for the maiden voyage
- Safety Response Capability
  - Lifeboats on the ship had been reduced from sixty-four boats to twenty-two in lieu of more expansive promenades
  - The officers on board The Titanic had not trained with the lifeboats and were unsure of their holding capacity
  - There was not a standing safety-response plan.. the 'Women and Children first' response was a reaction more than a previously-agreed plan.

Reference: 'The Riddle of the Titanic', Gardiner et. al. Orion, 1998

The Outcomes

The first photographs following the sinking were taken from the *Carpathia* – here a *Titanic* lifeboat approaches.

- Lives Saved: 705
- Lives Lost: over 1500

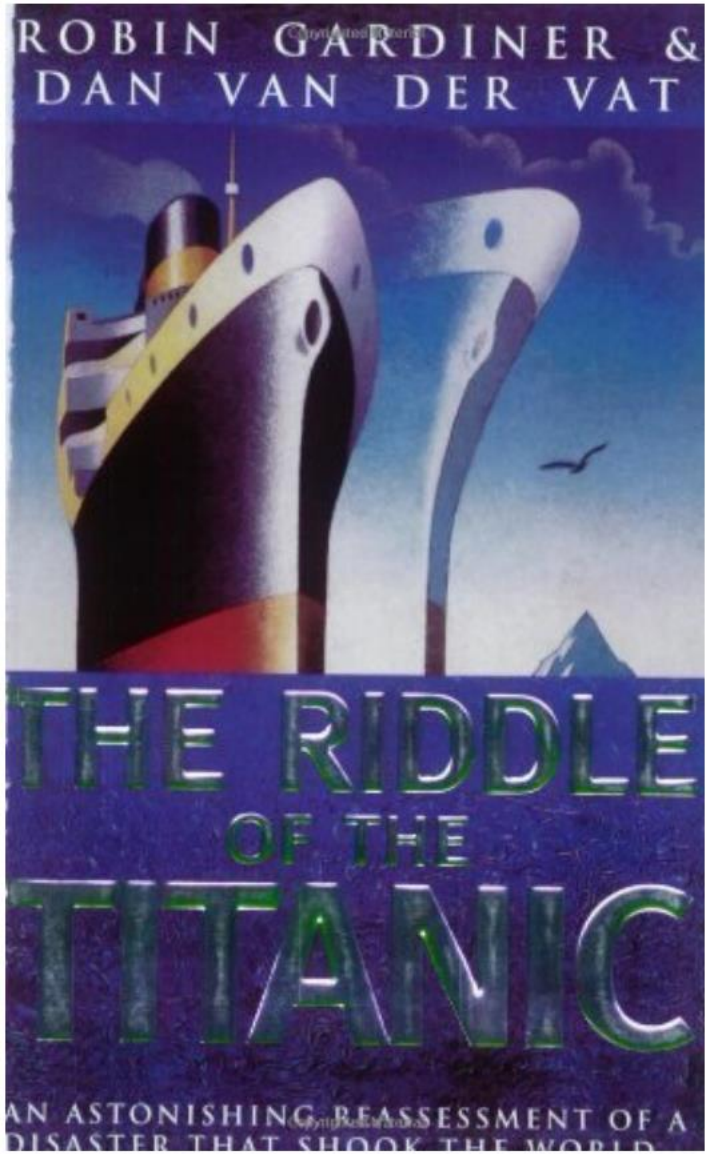
- Total passengers 2,205
- Max Lifeboat Capacity 1,600

- It wasn't until 45 minutes after the collision that officers commenced preparing the lifeboats
- Twenty lifeboats were launched
- Officers feared that the ship's davits & winches would not hold the weight of the recommended 70 people
- All but the last few lifeboats floated were half-filled
- It is a fact that had the Officers filled the lifeboats per their specification an additional 600+ people could have been saved.

Reference: 'The Riddle of the Titanic', Gardiner et. al. Orion, 1998

‘Safety outweighing every other consideration’

Was the framed notice in the
chart room of every White Star liner in 1912

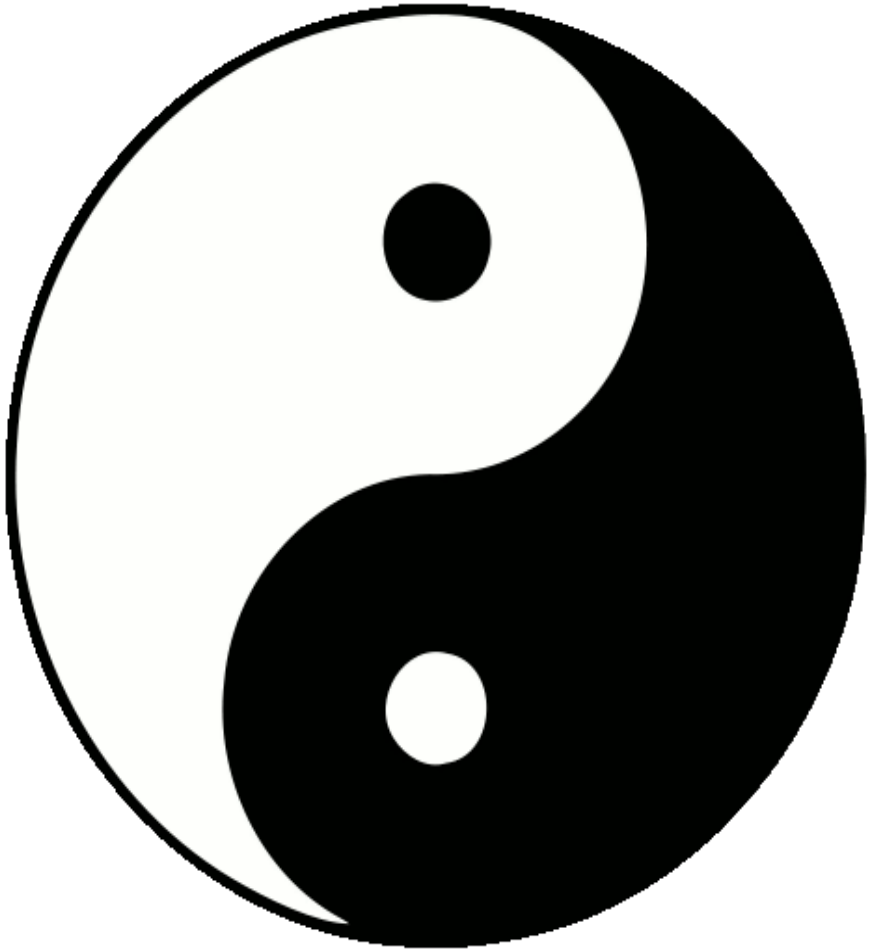


Reference: ‘The Riddle of the Titanic’, Gardiner et. al. Orion, 1998

Definition of “Risk”

機

Opportunity



危

Danger

turricula

USB University of Stellenbosch Business School

What is ERM?

- Enterprise Risk Management
- Risk management is a systematic process that identifies and evaluates events that could positively or negatively affect the achievement of objectives
- Events upside - opportunities
- Events downside - hazards

What is ERM?

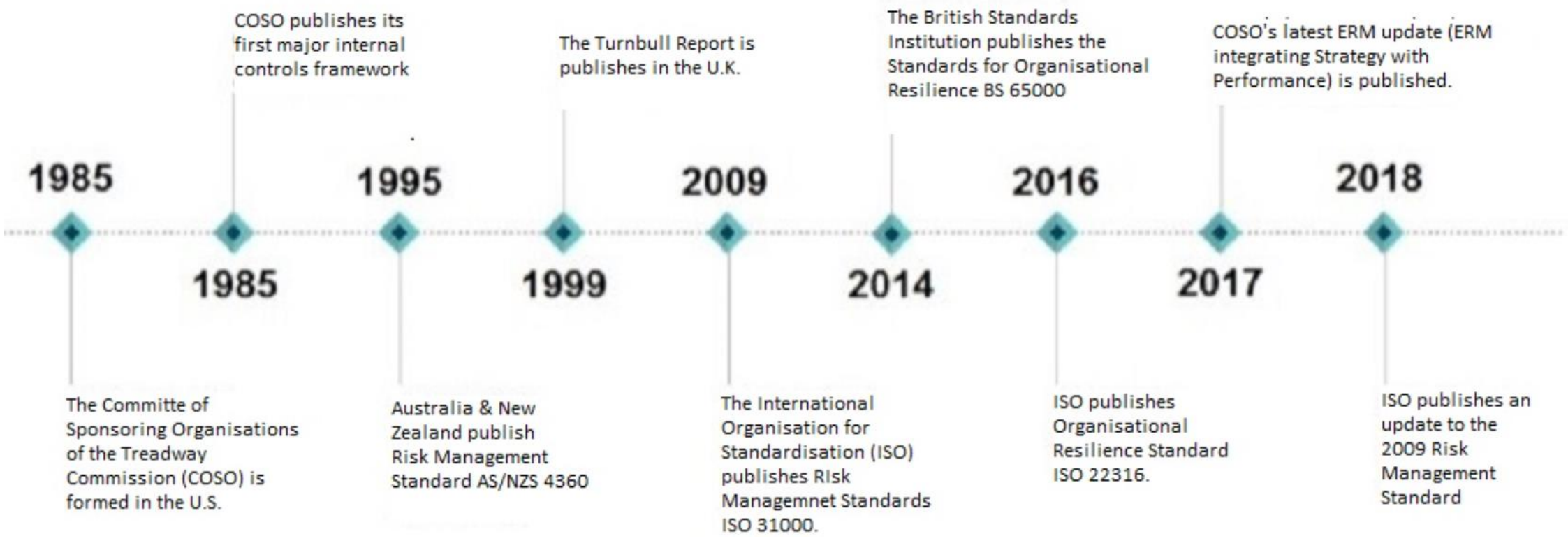
- Applicable to any industry, any country, any organisation
- ERM eco-system has strong links to:
  - Governance, Risk & Compliance (GRC) – “The Trinity”
  - Sustainability / CSR - natural & social capital
  - Objectives of the company – broad or narrow
- Integrated, Strategic, Enterprise-Wide
- Holistic, synergistic, integrated and aligned, inclusive

Ineffective management of risks: financial distress, loss of reputation, delisting, failure of the organisation

ERM is a holistic approach to managing the entire portfolio of risks faced by a business

- Risk-based view of the strategy:
  - What will “help” (opportunity) and what will “hinder” (danger) in achieving the strategy?
- Umbrella to view and manage risks across the organisation:
  - Creates common platform and language
  - Links back to strategy
  - Provides assurance that controls are in place
  - Provides quantitative metrics to manage the business
- Top-down and bottom-up engagement around strategy and key issues
- Provides confidence to stakeholders that organisation is running a tight ship

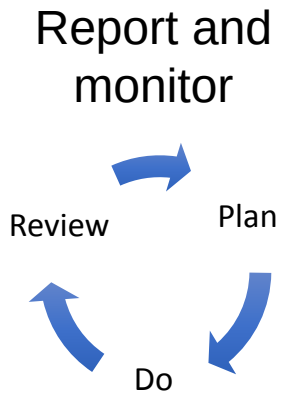
Selected timeline leading to ERM



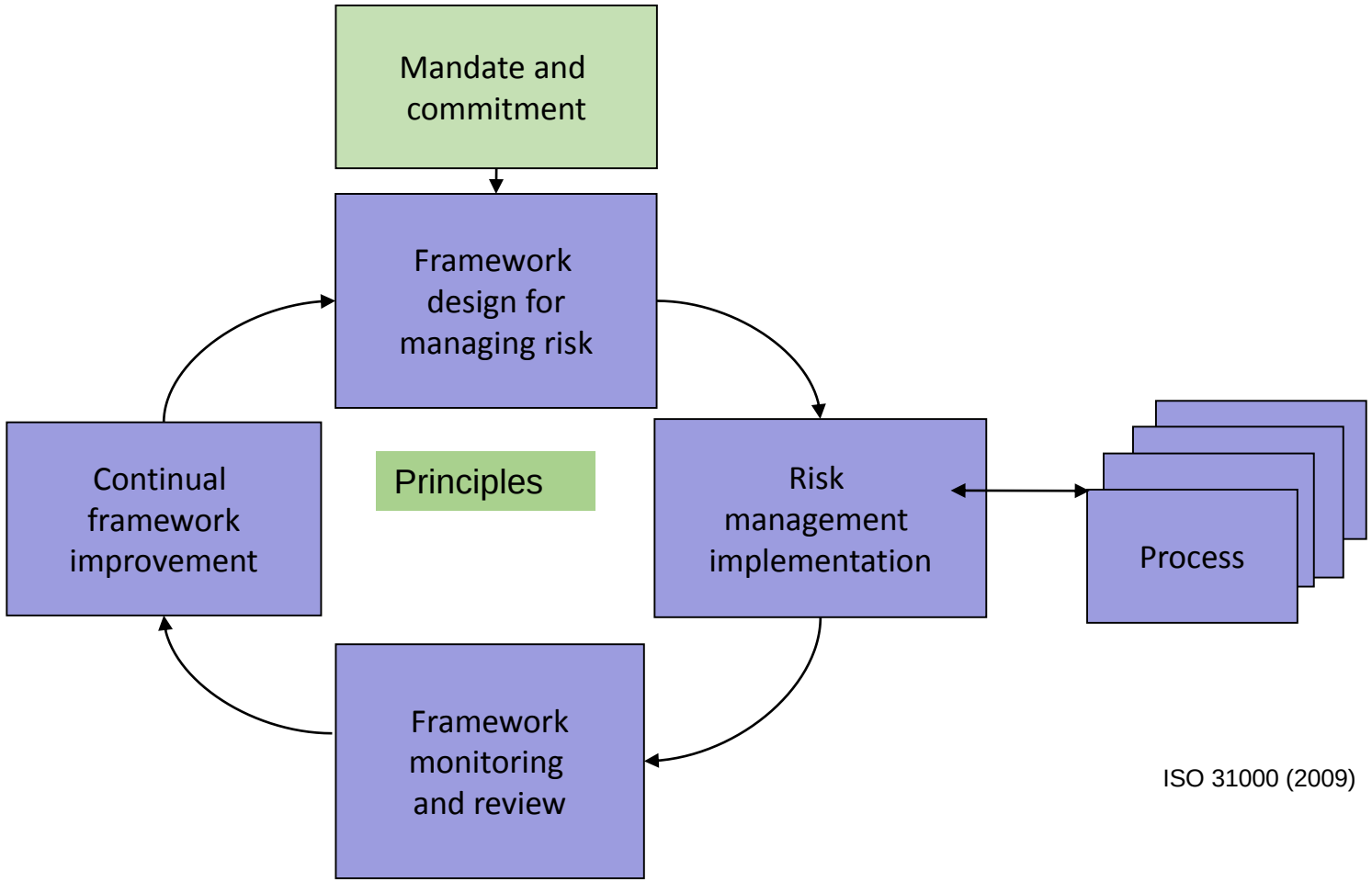
Source: Control Risks 2018

Definition of Risk Management

- Contextualise the organisation
  - Internal
  - External
- Identify
- Assess:
  - Likelihood
  - Impact
- Respond:
  - Treat (reduce impact / likelihood)
  - Tolerate (accept)
  - Transfer (insure / hedge)
  - Terminate (mitigate through risk-based control)

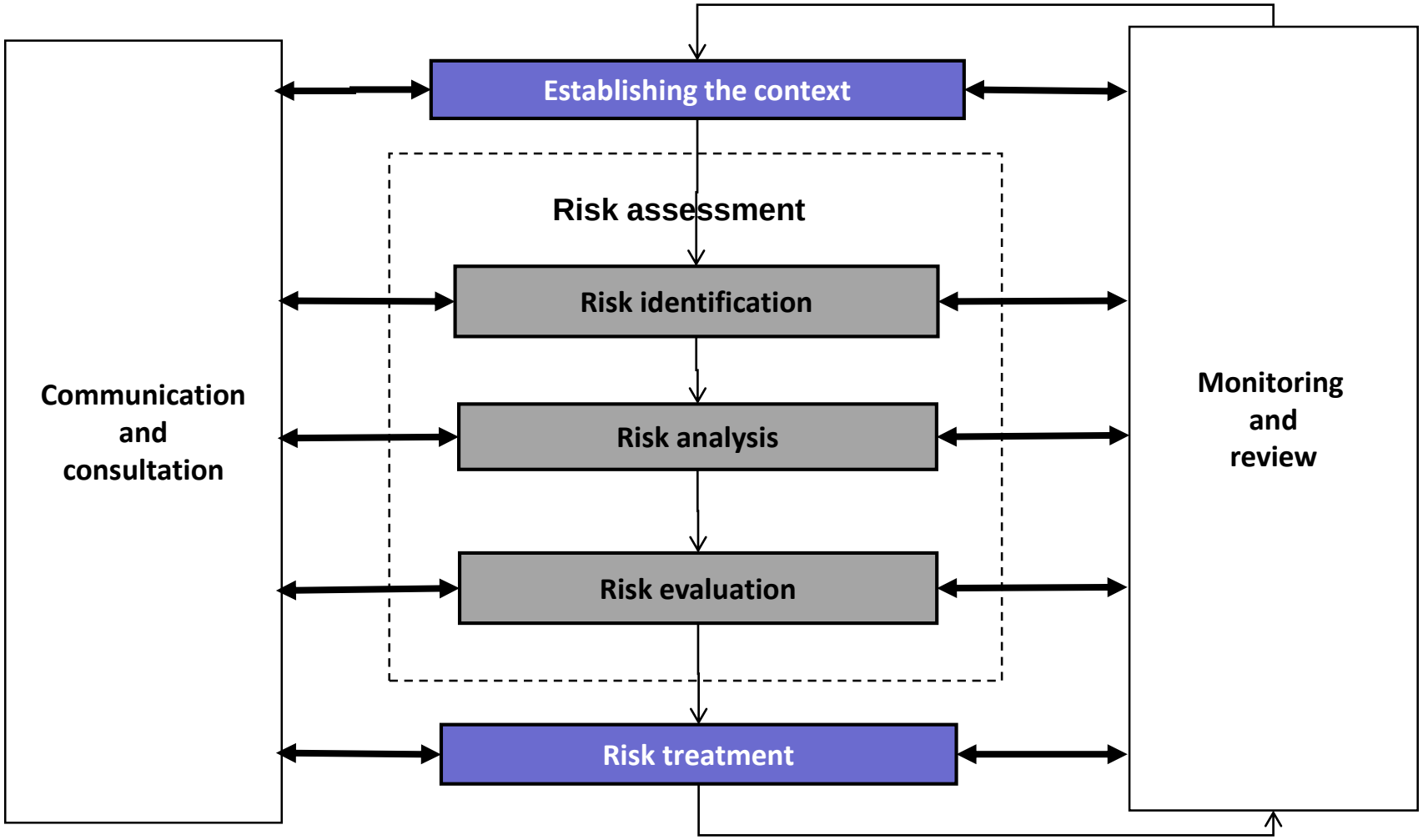


ERM Framework and Process



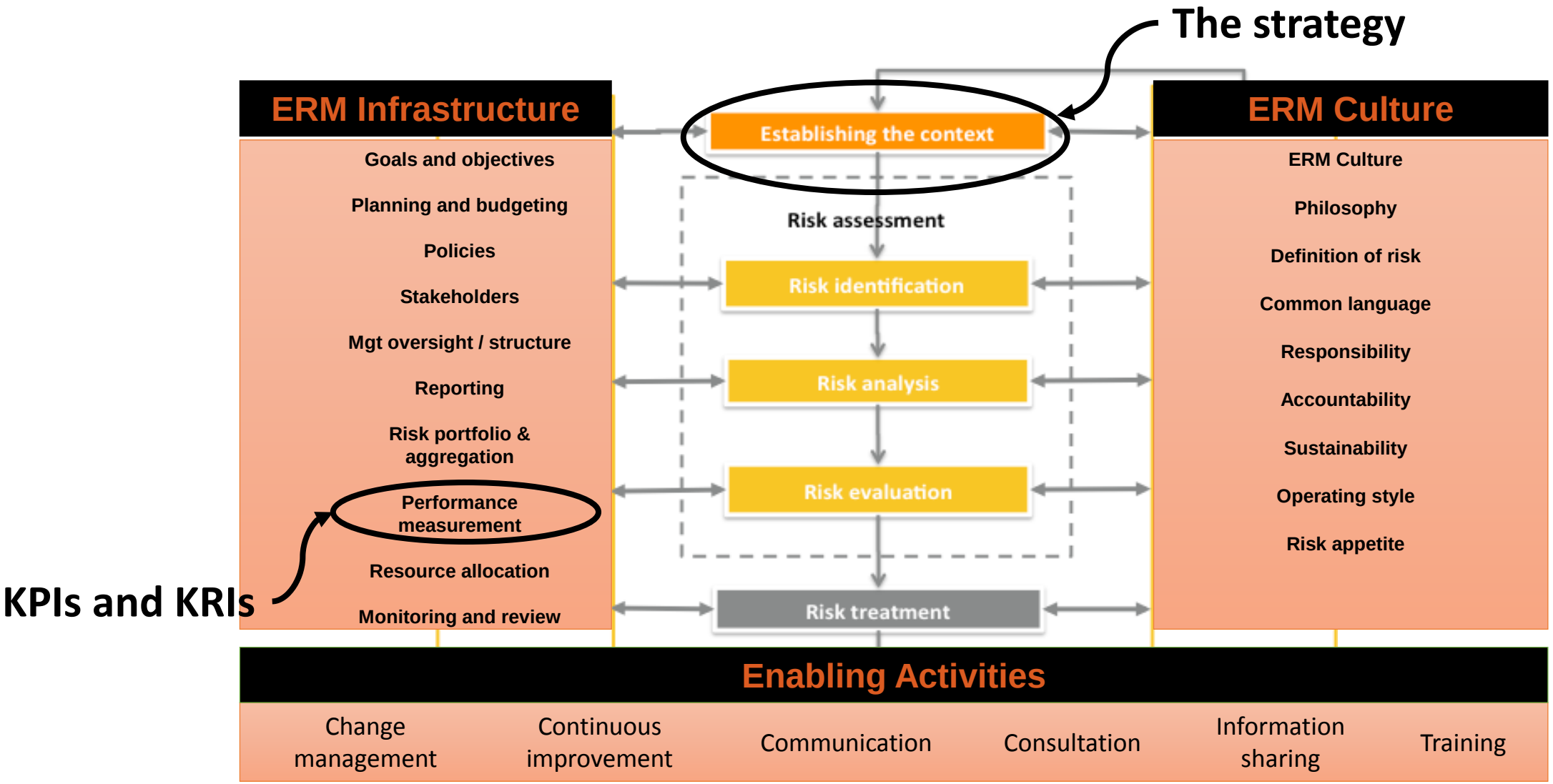
ISO 31000 (2009)

ERM Process



Source: URMIA 2007

Early ERM landscape and risk maturity



Source: URMIA 2007

ISO 31000 Risk Management (2018)

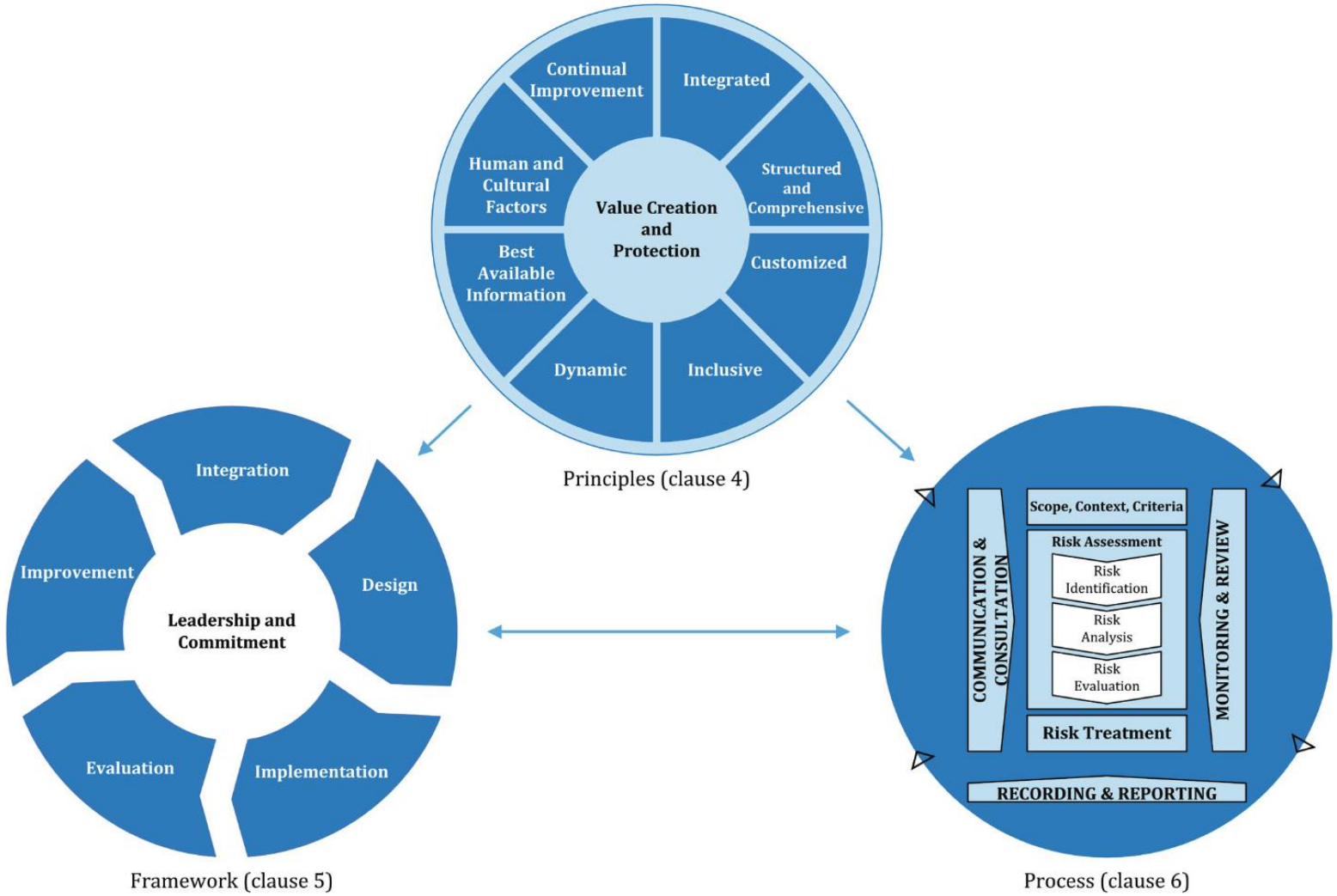


Figure 1 — Principles, framework and process

Source: ISO 31000 2018

ISO 31000 Risk Management (2018)

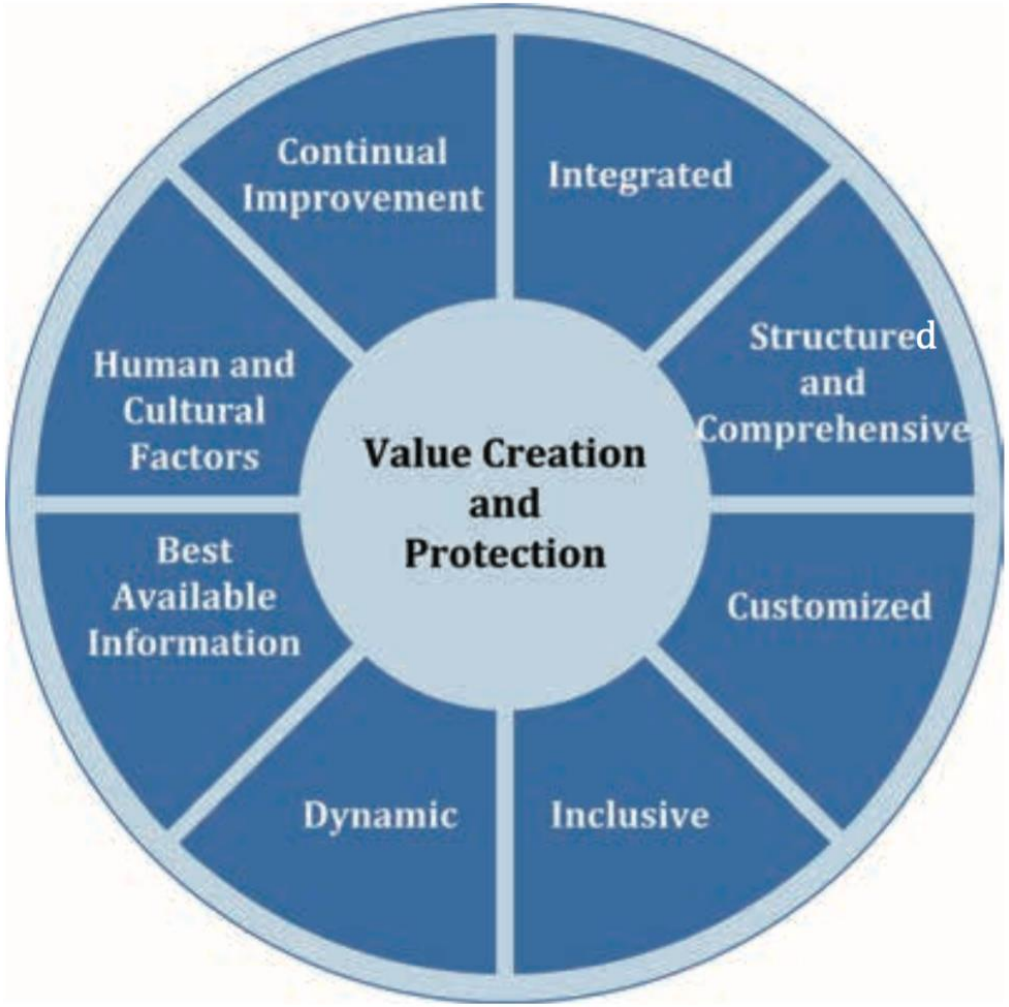


Figure 2 — Principles

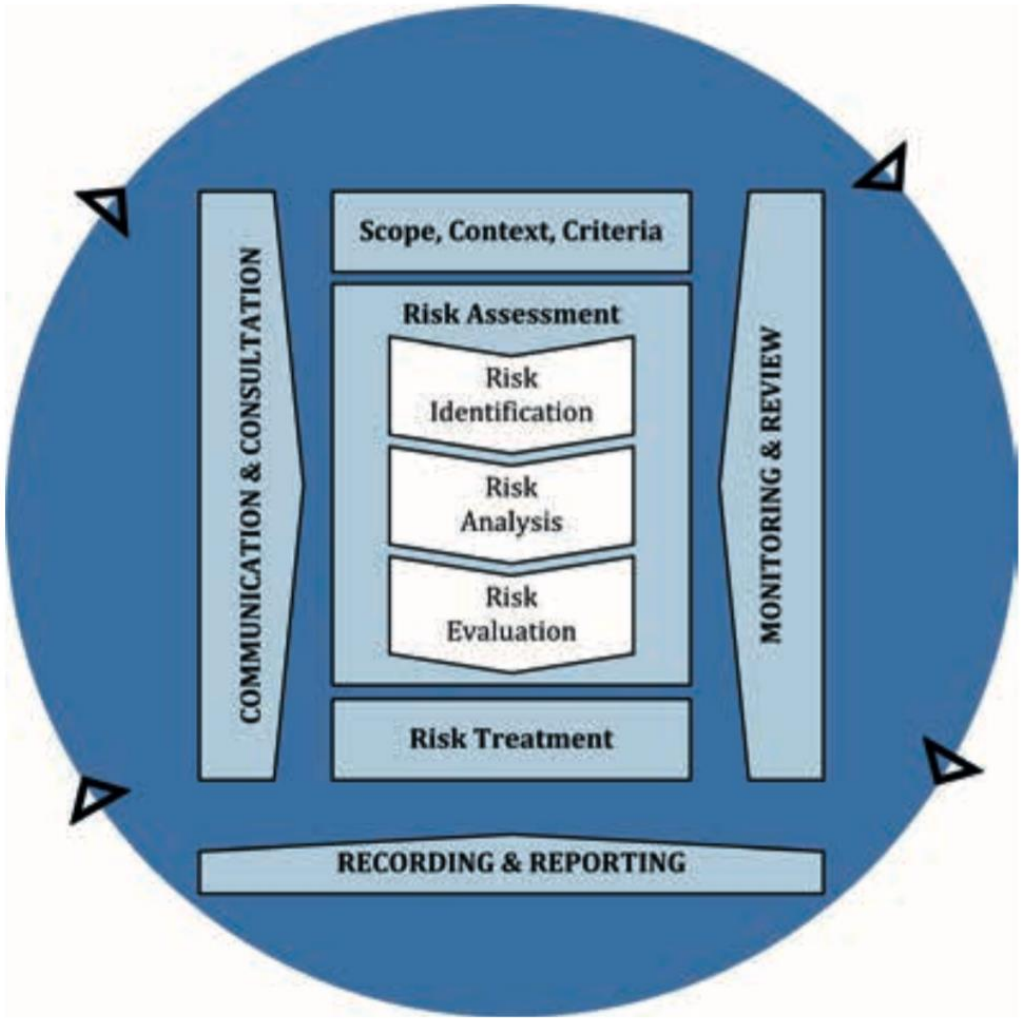


Figure 4 — Process

COSO

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly affect the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information & Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

For more information about COSO, visit coso.org.

COSO 2013

COSO 2017: Enterprise Risk Management Integrating with Strategy & Performance

COSO 2017: Enterprise Risk Management Integrating with Strategy & Performance

The Framework itself is a set of principles organized into five interrelated components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance**: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

COSO 2017: Enterprise Risk Management Integrating with Strategy & Performance

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

COSO 2017

Performance manage the organisation and its strategy using an ERM framework

It is also an incredibly powerful tool to turn employees into champions for the strategy.

Updates to ISO 31000 (2018) & COSO (2017)

- Risk management has moved from a separate and at times departmentalised activity to an integrated management competency.
- **The stated purpose of risk management is to create and protect value**
- Emphasise how ERM informs strategy and performance
- More clearly connecting enterprise risk management with a range of stakeholder expectations
- As with the ISO update, the COSO revision discusses the important influences that culture and biases carry in decision-making and risk management practices
- Enhanced emphasis on continual improvement i.e. improved risk maturity

Source: RIMS 2018

Calibration Exercise

In 1938 a British steam locomotive set a new speed record by going how fast in MPH / KMPH?

If, under punishment of electric shock (☺) or loss of ZAR 1,000 you had to be 90% sure (Confidence Interval), what range of speeds would you give?

Calibration Exercise

The *Mallard* is the holder of the world speed record for steam locomotives at 126 mph (203 km/h).

Mallard covered almost one and a half million miles (2.4 million km) before it was retired in 1963.

The Risk Frontier

The current risk paradigm

- **Hazard risk**
  - Property / casualty
  - Political
  - Environmental
  - Regulatory
- **Financial risk**
  - Currency
  - Interest rate
  - Commodity prices
  - Credit
- **Operating risk**
  - Inventory
  - Supply chain
  - Capacity
  - Information systems
- **Organisational risk**
  - Governance gaps
  - Wrong organisational structure
  - Talent / morale
  - M&A integration
- **Strategic risk**
  - Technology / Digital
  - Brand
  - One-of-a-kind competitor / disruptor
  - Industry economic collapse
  - Customer shift
  - New project / investment
  - Stagnation
  - Obsolete business design

Decreasing quantifiability / Increasing complexity

VUCA

HBR, 2014

turricula

USB University of Stellenbosch Business School

Risk Management Maturity (RMM)

”Companies in the top 20% of risk maturity generated three times the level of EBITDA as those in the bottom 20%.”

- *Turning Risk into Results (Ernst & Young)*

Risk maturity – risk culture

Risk culture key drivers of overall risk maturity models – stated in ISO 31000, COSO, RIMS, KING IV etc.

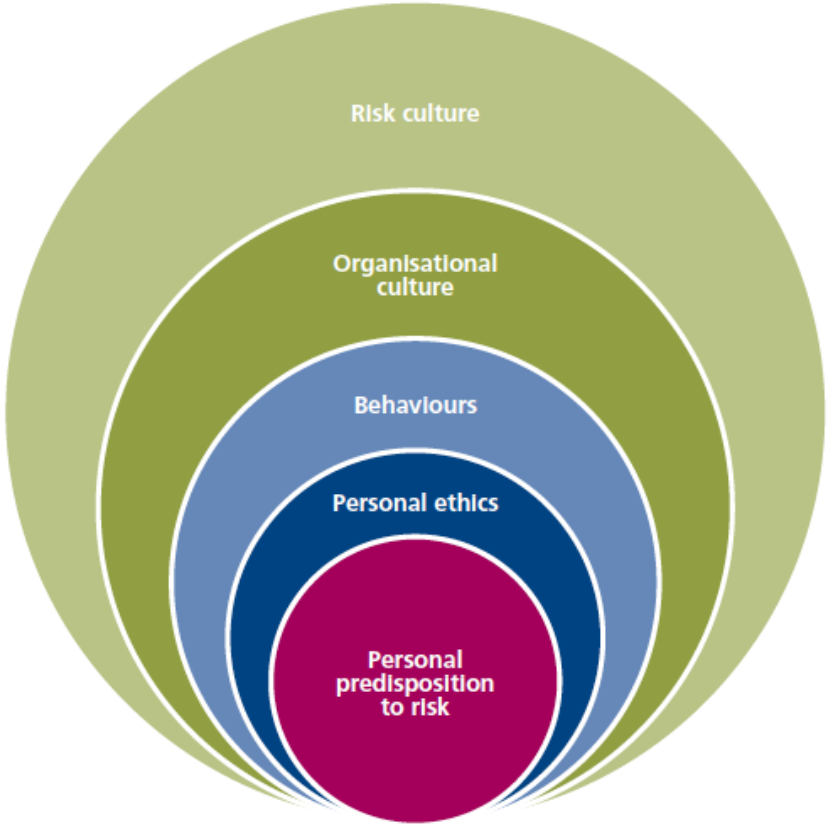
Critical Success Factors include:

- Risk culture, accountability and communication (RIMS)
- Tone at the top
- Clear lines of accountability and escalation
- All employees take accountability for continual improvement

Risk needs to become embedded into the culture of an organisation

The A-B-C approach:

- **A**ttitudes shape behaviors
- **B**ehaviors shape culture
- **C**ulture is the group's shared knowledge, beliefs, values and understanding



IRM (2013)

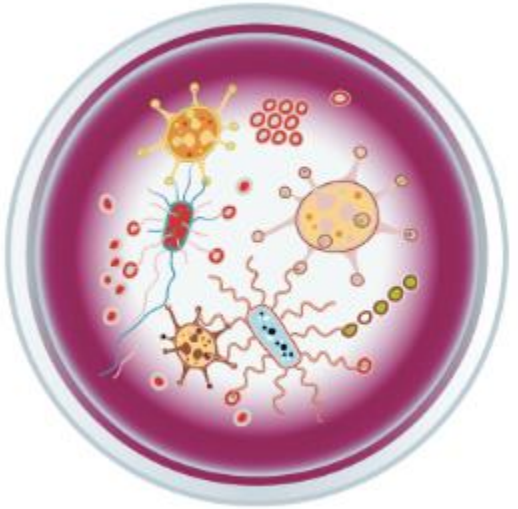
"People, present and past, make the place"

turricula

USB University of Stellenbosch Business School

10 critical considerations to driving risk culture

- Tone from the top
- Commitment to ethical principles
- Common acceptance of accountability and ownership
- Information flow
- Encouragement of risk event reporting
- Understand risks of large and complex issues
- Appropriate risk taking rewarded; inappropriate sanctioned
- Risk management skills and knowledge valued
- Diversity of perspectives, values and beliefs to ensure status quo is challenged
- Alignment of culture management with engagement and strategy



IRM (2013)

"Culture eats strategy for breakfast" – Peter Drucker

Risk Management Professional - Maturity

RIMS 2018

turricula

USB University of Stellenbosch Business School

Risk Maturity: Risk Identification / Quantification / Mitigation

Source Dilbert

Risk maturity – crisis management / scenario planning

Critical Success Factors of overall risk maturity models are linked to BCM / Disaster Planning / Resilience

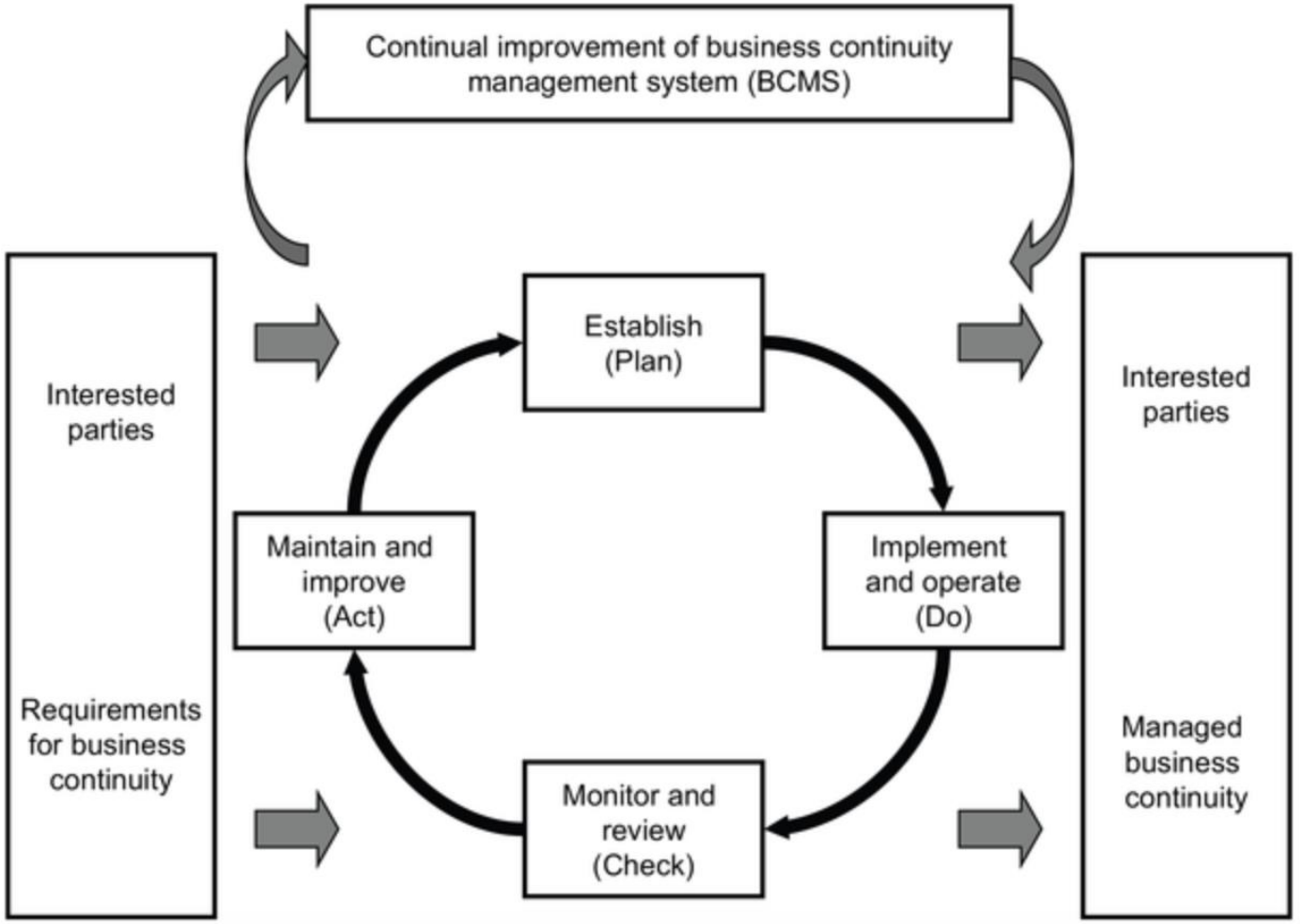
Examples include:

- RIMS Model – Attribute 7: Business Resilience & Sustainability
  - Driver 23 Analysis-based planning
  - Driver 24 Resilience and operational planning
  - Driver 25 Understanding consequences

- Local Model
  - Scenario planning
  - Whistleblowing
  - Action plans and KRIs – assigned and followed up
  - Comprehensive range of risks considered, regular cycles
  - Risk integrated with organisational processes

ISO 22301:2012 – Business Continuity Management

Figure 1 — PDCA model applied to BCMS processes

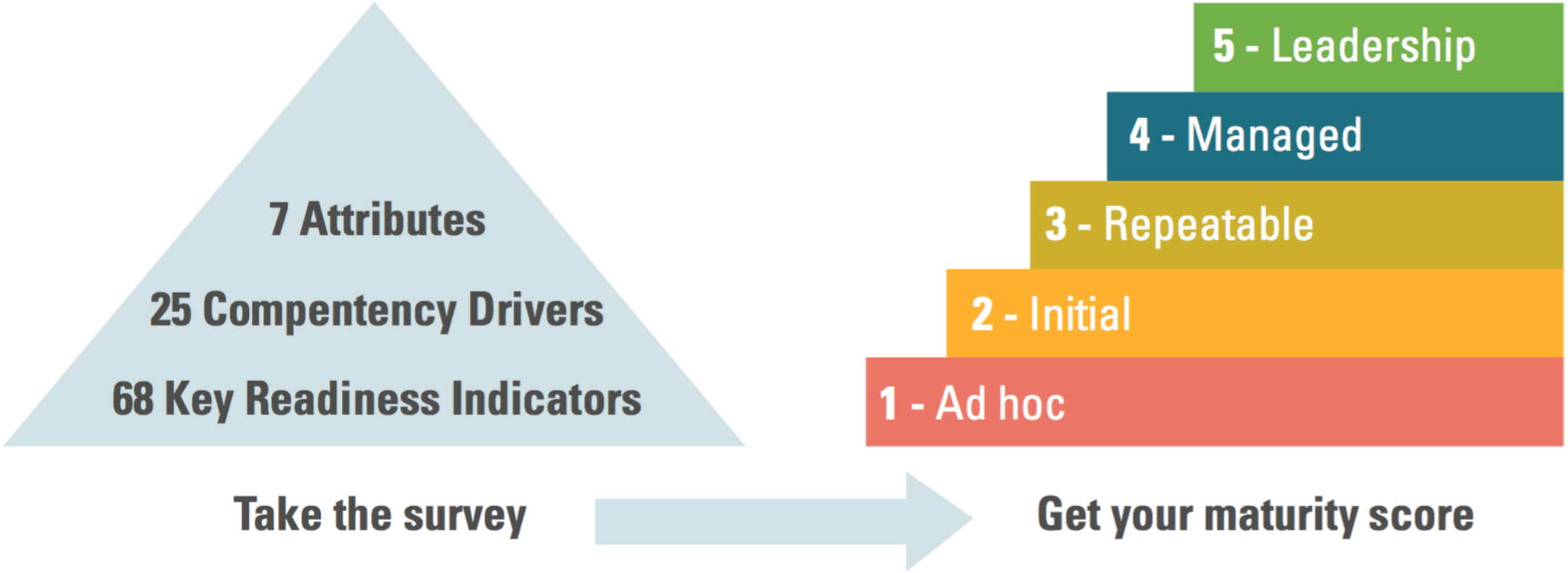


Source: ISO 22301 2012

Risk Management Information Systems (RMIS)

BARNOWL – THE ENABLER OF ERM & ASSURANCE

Risk Management Maturity (RMM) models - RIMS



RIMS 2018

turricula

USB University of Stellenbosch Business School

RIMS RMM model

ERM-based approach	Executive support within the corporate culture.
ERM process management	Integration into business processes.
Risk appetite management	Accountability within leadership and policy to guide decision-making.
Root cause discipline	Linking outcomes with their sources.
Uncovering risks	Analyzing and documenting risks and associated uncertainties in considering threats and opportunities.
Performance management	Executing vision, mission and strategy utilizing risk management methods.
Business resiliency and sustainability	Integration into operational planning and execution.

RIMS 2018

RIMS RMM model

7 Attributes	5 Maturity Levels →				
	Level 1 Ad hoc	Level 2 Initial	Level 3 Repeatable	Level 4 Managed	Level 5 Leadership
1 Adoption of ERM-based approach	Competency Drivers: Degree of: 1. Executive support of ERM 2. Business process definition and risk ownership 3. Far-sighted risk management vision 4. Front line and support process owner participation				
2 ERM process management	Competency Drivers: Degree of: 5. Repeatability and scalability 6. ERM program oversight 7. ERM process steps 8. Risk culture, accountability and communication 9. Risk management reporting				
3 Risk appetite management	Competency Drivers: Degree of: 10. Risk portfolio view 11. Risk-reward tradeoffs				

RIMS 2018

turricula

USB University of Stellenbosch Business School

RIMS RMM model

4 **Root cause discipline**	**Competency Drivers: Degree of:** 12. Dependencies and consequences 13. Indicator classifications 14. Risk (uncertainties) and opportunity information collection 15. Root cause consideration
5 **Uncovering risks**	**Competency Drivers: Degree of:** 16. Formalized risk indicators and measures 17. Adverse (potential) outcomes as opportunities 18. Follow-up reporting 19. Risk ownership by business areas
6 **Performance management**	**Competency Drivers: Degree of:** 20. ERM information and planning 21. Communicating goals 22. ERM process goals and activities
7 **Business resilience and sustainability**	**Competency Drivers: Degree of:** 23. Analysis-based planning 24. Resilience and operational planning 25. Understanding consequences

RIMS 2018

RIMS RMM model

14. Please identify secondary value that you gain from your ERM program (select up to three).

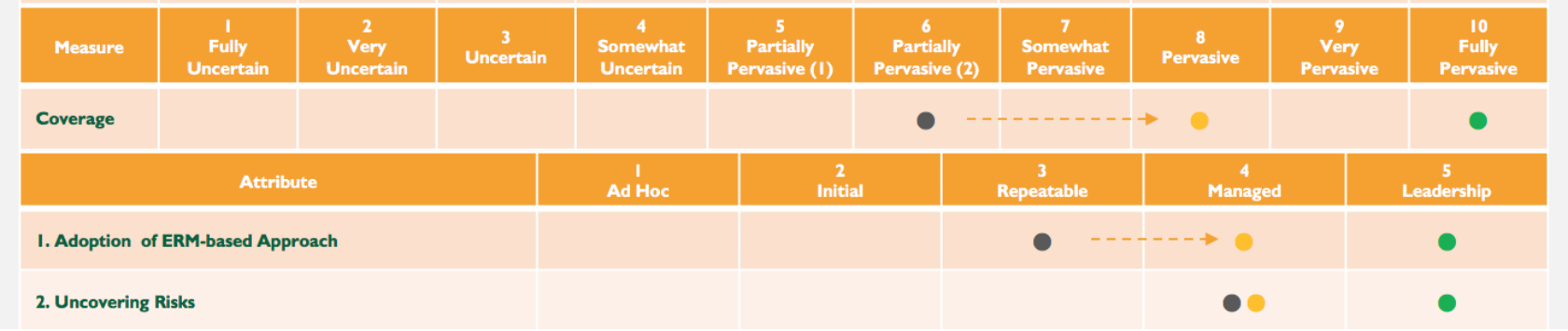
- ☐ Eliminating silos, e.g., viewing the entire portfolio of risks; increased coordination
- ☐ Avoiding and/or mitigating risk
- ☐ Consolidating processes, e.g., efficiency in data collection and risk assessment
- ☐ Increasing certainty in meeting strategic and operational objectives
- ☐ Providing assurance to shareholders
- ☐ Uncovering untapped opportunities
- ☐ Compliance with regulatory and legal requirements
- ☐ Increasing risk awareness
- ☐ Other (please specify)

RIMS 2018

RIMS RMM model

Each of the competency drivers are rated on a scale of 1 to 10 for capability, proactivity and coverage.

CAPABILITY (not capable – fully capable)	• Capability measures the degree to which an activity can be accomplished effectively. • Fully Capable organizations will have well-defined practices, policies, and procedures that have been proven to produce the desired results consistently over time.
PROACTIVITY (fully reactive – fully proactive)	• Is the competency driver ingrained in your organizational processes? • Are these activities scheduled, or only promoted in response to a risk event? • Is the activity undergone at an appropriate frequency?
COVERAGE (fully uncertain – fully pervasive)	• To what extent is this activity observed, analysed, and reported throughout your business? • Are the appropriate stakeholders involved in the execution of this activity, or is it limited to a small set of silo-specific personnel?

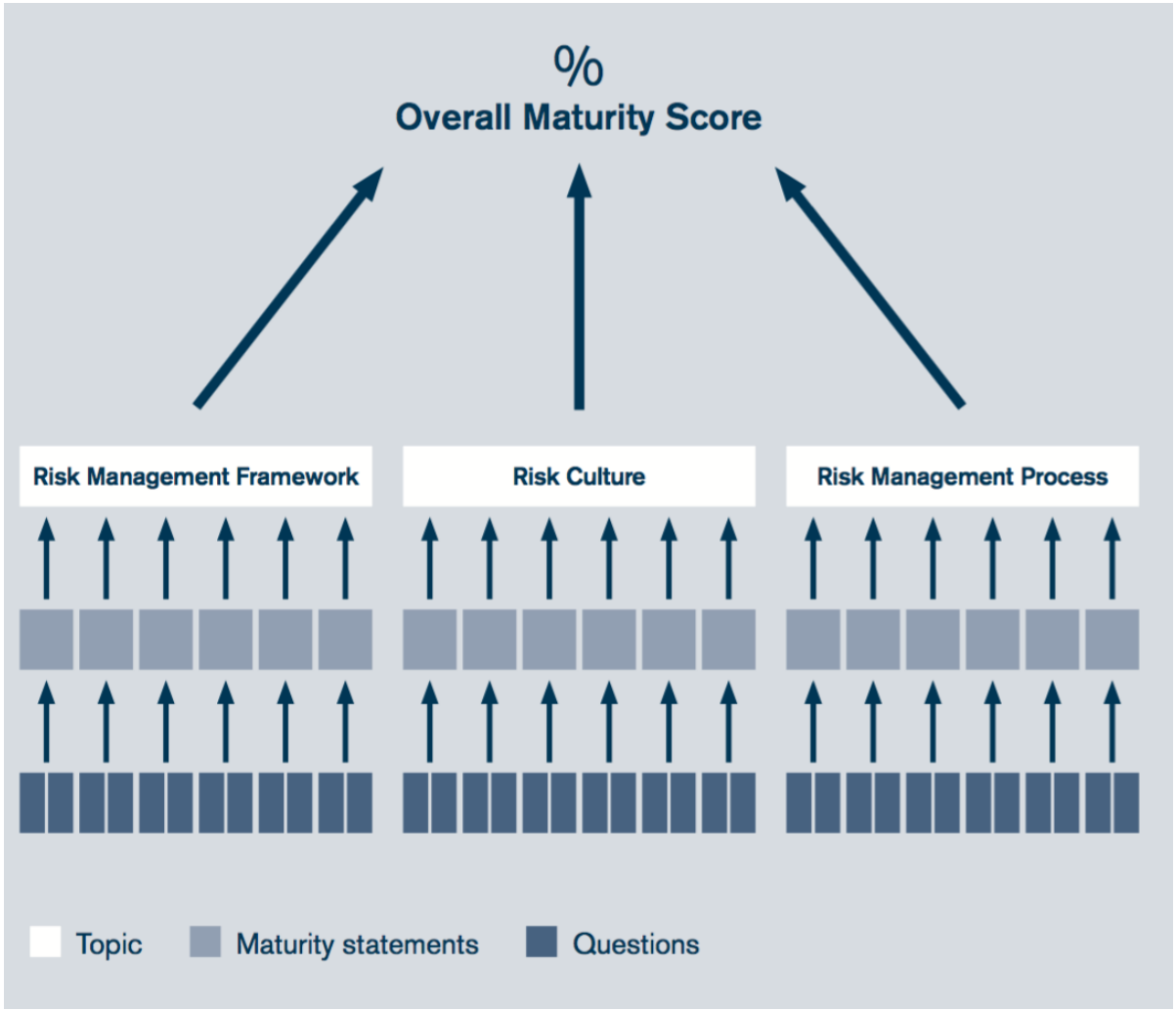


RIMS 2018

turricula

USB University of Stellenbosch Business School

VMIA RMM model



VMIA 2017

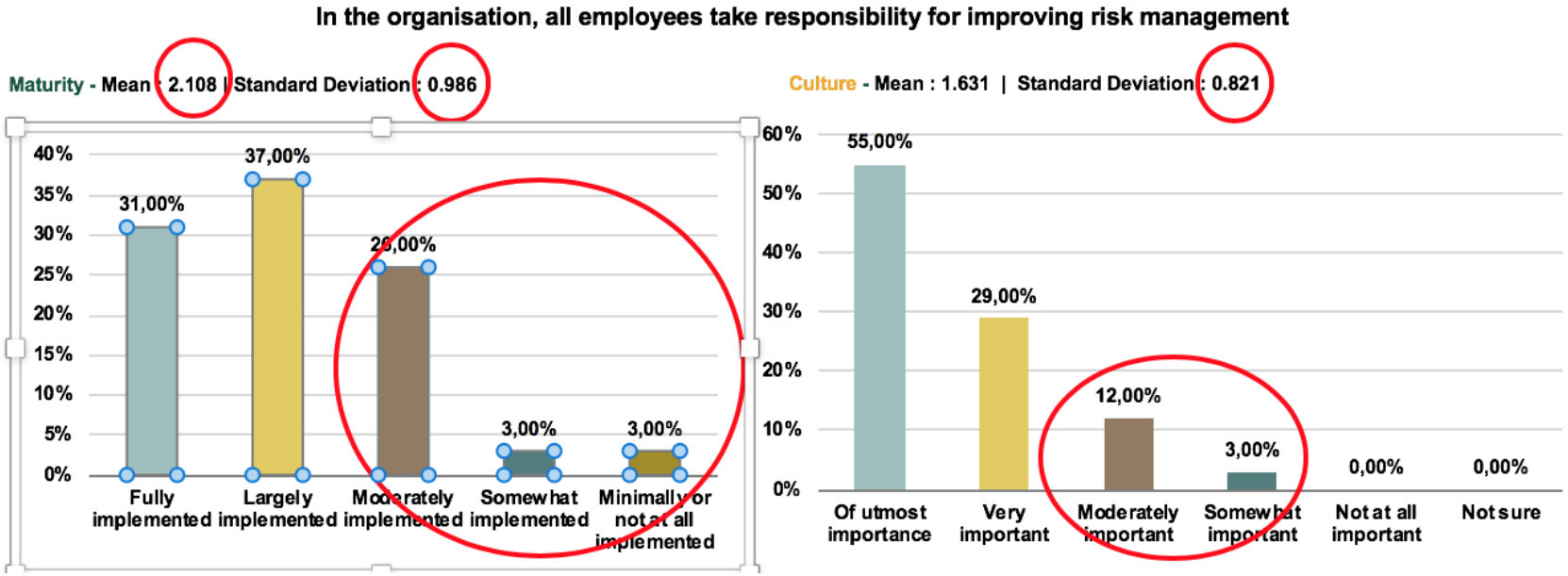
turricula

USB University of Stellenbosch Business School

Local RMM model

Item no.	Item alias	Item Statement
2	Escalation	The organisation has a clearly-defined chain of accountability and escalation for risk management issues
10	Relationships	The risk management function of the organisation builds and sustains relationships across all areas of the organisation, including executive leadership
21	Quality	Quality risk information is demanded as part of the decision-making process within the organisation
26	Whistle Blowing	The organisation provides employees the opportunity to raise serious risk or risk management concerns in an anonymous fashion without fear of retribution i.e. Whistleblowing Policy
13	Employees improving	In the organisation, all employees take responsibility for improving risk management

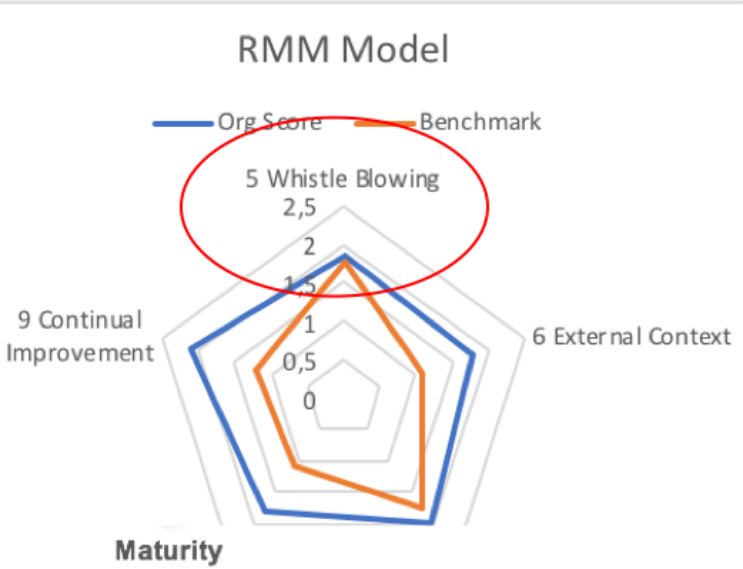
Examples of local RMM model outputs

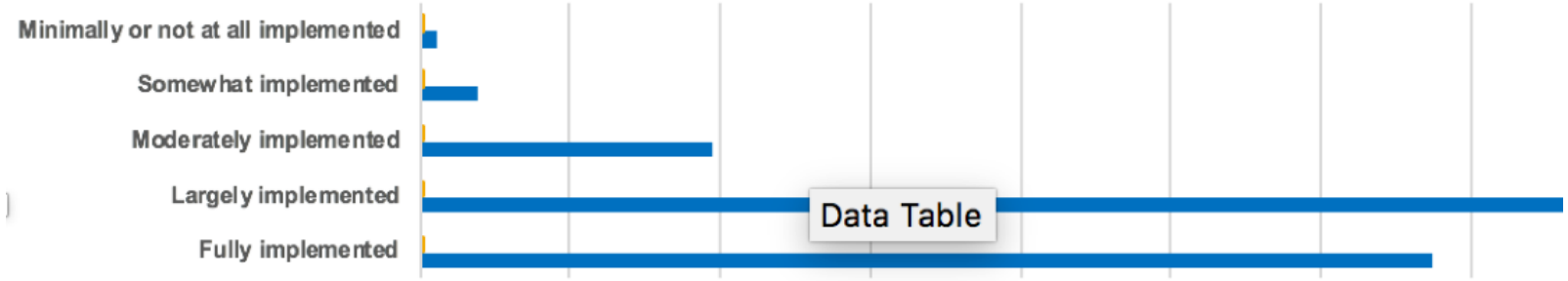


Linke RMM Survey	Practices Mean	Practices Deviation	Values Mean	Values Deviation	RIMS RMM Attribute	Comments
Learns from experience	1.723	0.696	1.569	0.706	5	Continually learn from the cause & effect chain.
Understand roles	1.846	0.795	1.523	0.640	7	Improved understanding by all personnel that they are accountable for goals & risks.
Understand external context	1.769	0.702	1.523	0.562	6	Business units to report on how external and internal events might impact their business models
Risk framework is holistic	1.908	0.879	1.631	0.675	2	All resources a company relies on should be assessed to determine criticality

Examples of local RMM model outputs

	RMM Item
5	Whistle Blowing
6	External Context
7	Scenario Planning
8	Communication
9	Continual Improvement





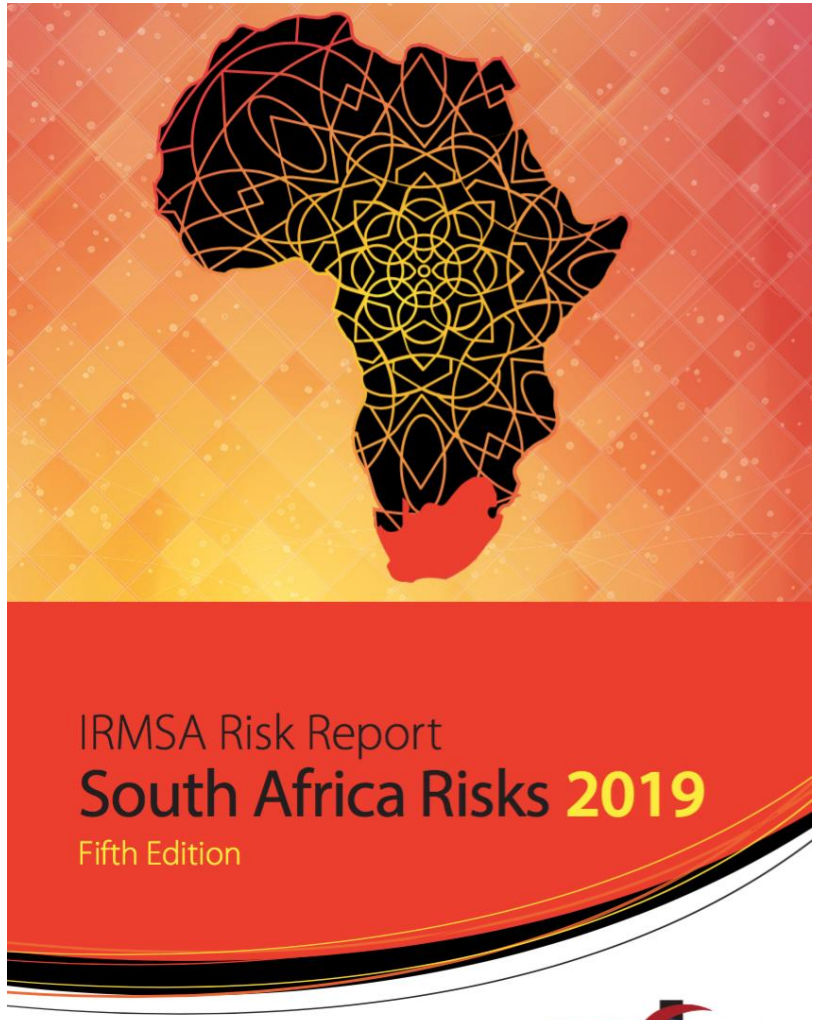
turricula

USB University of Stellenbosch Business School

IRMSA #impact

#impact
A YEAR OF RISK
ACTIVISM 2019
MORE INFO

https://www.irmsa.org.za



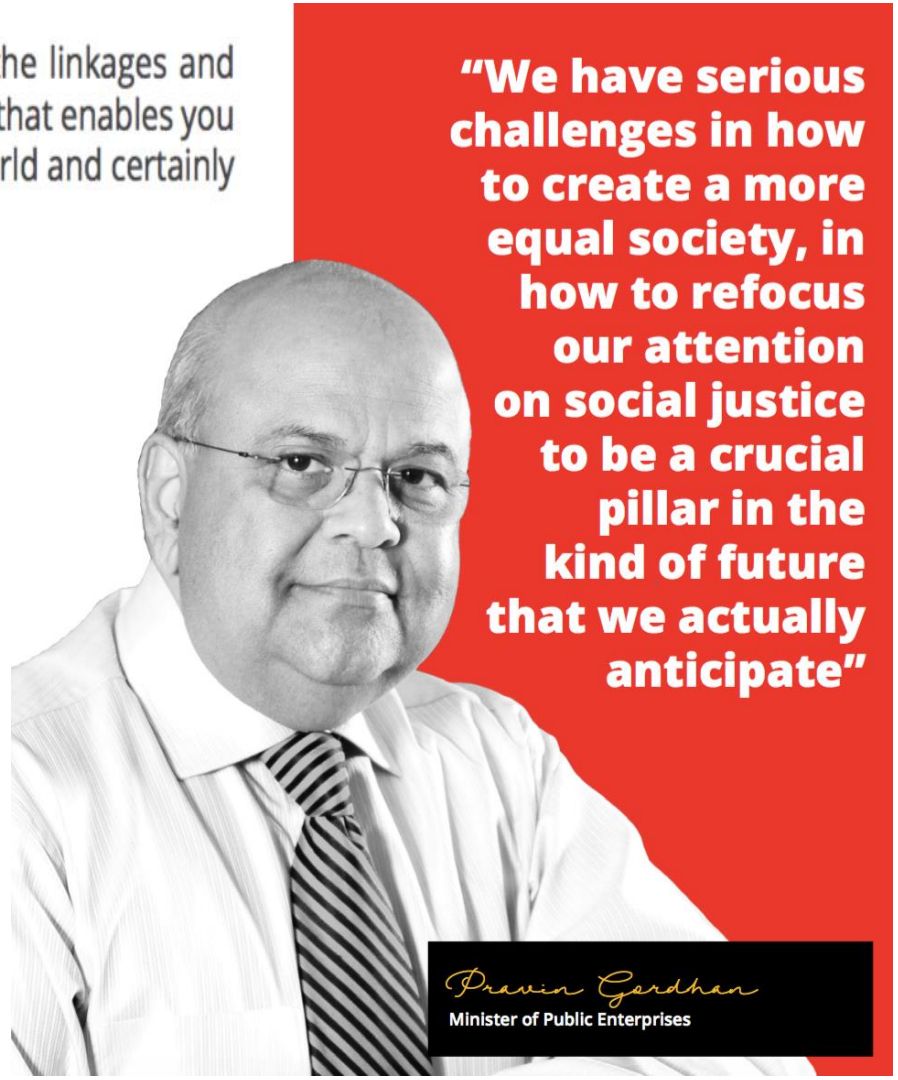
turricula

USB
University of Stellenbosch
Business School

IRMSA #impact – Personal accountability

Risk managers are in a unique position to connect the proverbial dots – finding the linkages and trends in information, vertically and horizontally, from a number of different planes that enables you to navigate the level and pace of complexity of what we are going through in the world and certainly in South Africa.

Where to from here and how do we as public officials or private operators in companies influence and chart our own destiny?



turricula

USB University of Stellenbosch Business School

IRMSA #impact – Risk maturity initiative

- Ongoing – RIMS risk maturity model – South African members of IRMSA invited to participate
- Results will reflect South African risk maturity overall and by industry - to global benchmarks
- IRMSA to follow up with targeted risk maturity interventions for organisations as requested
- Ultimate goal to shift the risk profile for South Africa

turricula

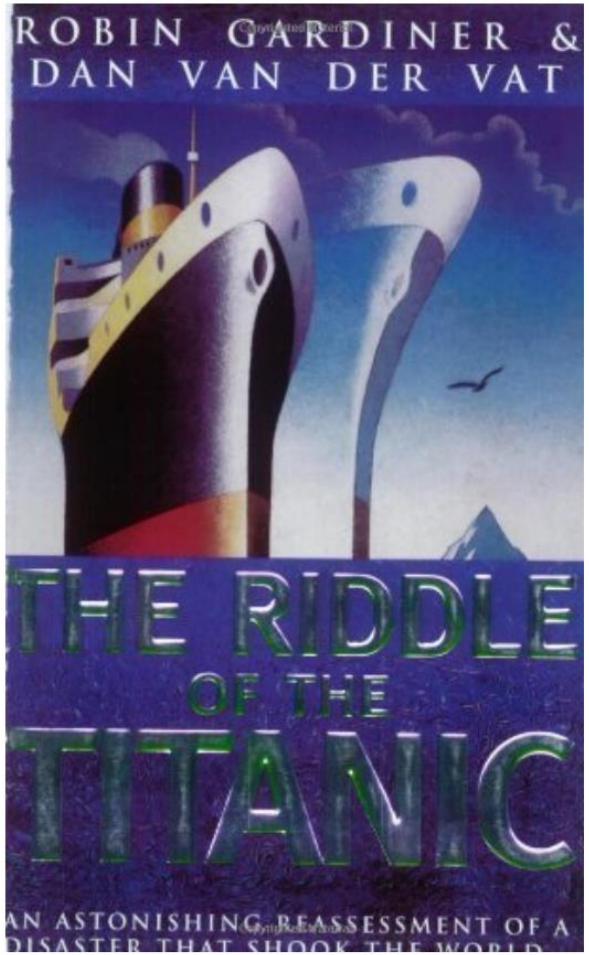
USB University of Stellenbosch Business School

Top Ten Risk Maturity Critical Success Factors

- Tone at the top
- Clearly defined and communicated objectives
- Understanding of internal & external context
- Holistic portfolio view of organisation – no silos
- Appropriate calibration and use of experts for risk identification / assessment and mitigation
- BCM in place - Scenario planning
- Effective KRIs and Action Plans
- Clear lines of accountability and escalation
- All employees take accountability for risk and continual improvement
- Holistic - the organisation is only as good as its weakest link

Risk Maturity lessons learned from the Titanic

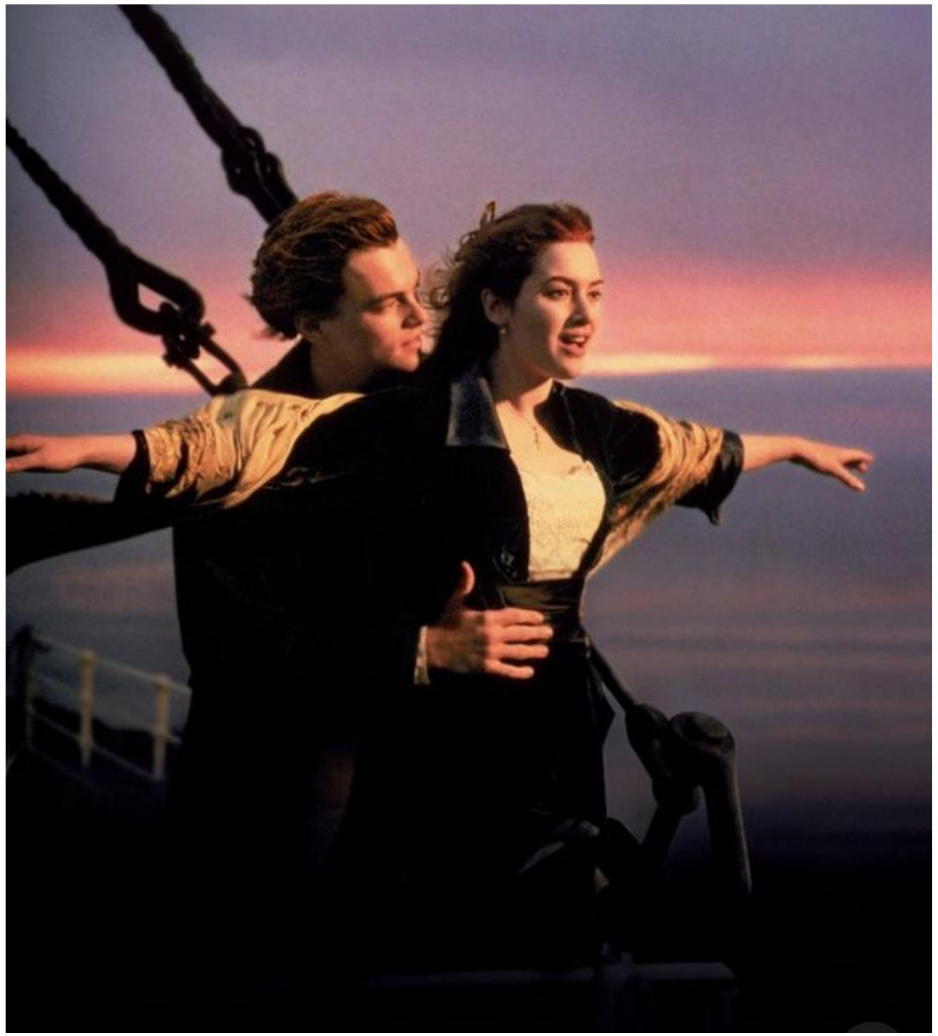
- Tone at the top – MD, Captain etc.
- Misalignment between stated objective - *'Safety outweighing every other consideration'* – and the actual objective – pride, prestige and *fastest Atlantic crossing*
- Risk identification / assessment / mitigation: Scenario planning – "Yes we are unsinkable, but what if…?"
- Appropriate BCM / Crisis Plan in place



turricula

USB University of Stellenbosch Business School

Risk Management Maturity



To protect and create value and achieve our strategic objectives…

Presentation to BarnOwl Information Sharing Session Risk Maturity

Dr Arthur Linke

11th April, 2019

alinke@sun.ac.za

arthur@turricula.com

turricula

USB University of Stellenbosch Business School