2018 IIA INDONESIA NATIONAL CONFERENCE

Nurturing Agile Internal Auditors in Disruptive Times

COSO ERM & ISO 31000 – A reflection

The Institute of Internal Auditors Indonesia

2018 NATIONAL CONFERENCE
Indonesia Bali, 28-29 August

Your speaker

Tarling Assurance Risk
& Control Services

IIA Global Chairman – 2012-2013
ECIIA President 2010-2011
IIA UK and Ireland President 2005-2006

Holder of the CIA, CMIIA, CRMA, QIAL qualifications

----

32 years experience in Internal Audit
27 years at managerial level

IA Project Expert for the EC and the OECD

Experience in the Public and Private sectors, including spells as:

- VP Capability & Head of the Centre of Internal Audit Excellence - Huawei
- Head of Internal Audit for a number of Health organisations in the UK
- Head of Internal Audit for the UN Special Tribunal for the Lebanon
- Head of Internal Audit for the UN War Crimes Tribunal for Bosnia Herzegovina
- Project Manager for EC funded projects in Poland, Romania, Turkey
- Project Manager for Development Agency funded projects in Kenya, South Africa and Botswana
- Project Expert for EC/OECD funded projects in Croatia, Kosovo, Serbia, Hungary, Latvia, Estonia, Lithuania, Czech Republic, Macedonia

Your speaker

Managing Partner for the Consulting Practice at RSM Indonesia, which service includes Management Consulting, Governance Risk Control, IT Consulting, Corporate Finance & Transaction Support, with more than 18 years experience. Within the RSM network, Angela also hold the function of International Contact Partner for RSM in Indonesia, and sit as one of the member of the Asia Pacific Risk Consulting Committee.

RSM

Bachelor of Economy from Trisakti University, and holds a Master of Commerce in International Business and Management of Technology from The University of Sydney, Australia. Angela is also a member of Audit Committee, Risk Monitoring Committee, and Integrated Corporate Governance Corporate Governance Committee at one of the 10 largest bank in Indonesia.

Experienced in working in Indonesia and Australia. Member team that develop the Indonesia Code of Good Corporate Governance, the Indonesia Code of Good Public Governance, and the Indonesia Whistle blowing System Guidance. Was an Internal Audit lecturer at Master Program in the University of Indonesia and source person on governance section for the Indonesia CPA Exams.

IIA Indonesia Vice President – 2017-2013

Holder of the CIA, CRMA, CRISC qualifications

----

18 years experience in Governance, Risk & Control, incl. Internal Audit

----

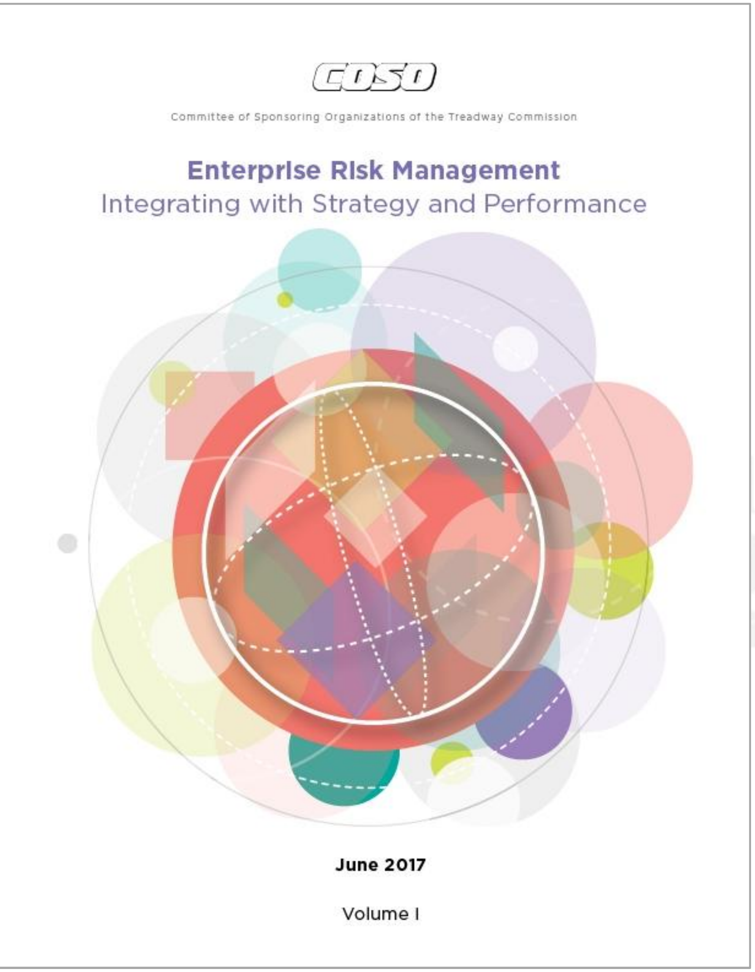
Corporate Governance Expert for ASEAN region representing Indonesia, as appointed by Otoritas Jasa Keuangan (Indonesia FSA)

Agenda

- COSO ERM
- ISO 31000
- What does it mean for Internal Audit

COSO ERM

What were the major changes?



COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management

Integrating with Strategy and Performance

June 2017

Volume I

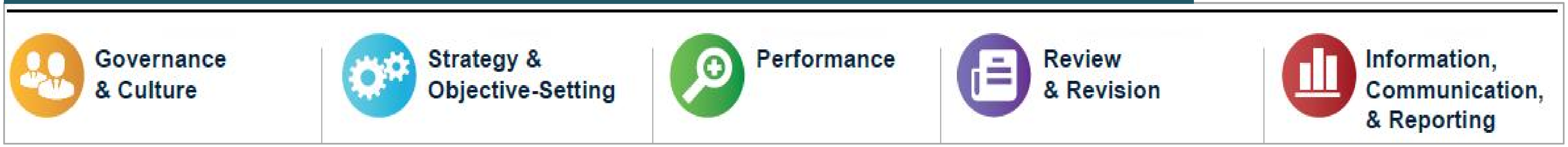
Retitled as *Enterprise Risk Management—Integrating with Strategy and Performance*

Recognises the importance of strategy and entity performance

Further distinguishes enterprise risk management from internal control

Provides a new structure

Framework focused on fewer components (five)



Governance & Culture

Strategy & Objective-Setting

Performance

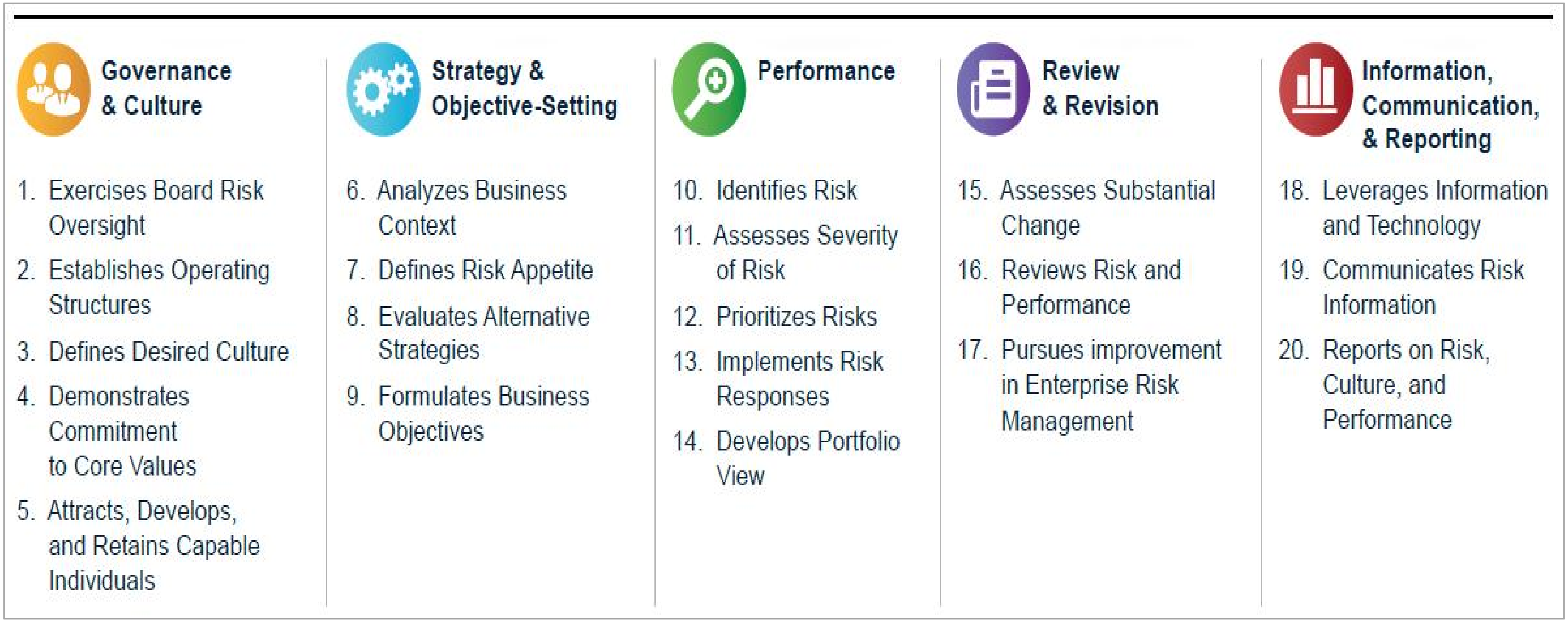
Review & Revision

Information, Communication, & Reporting

- Follows the business model versus an isolated risk management process

Introduces Principles

20 key principles within each of the five components



Governance & Culture	Strategy & Objective-Setting	Performance	Review & Revision	Information, Communication, & Reporting
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	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance

A Focus on Integration

- Integrating ERM with business practices results in better information that supports improved decision-making and leads to enhanced performance

- It helps organisations:
  - Anticipate risks earlier or more explicitly, opening up more options for managing the risks
  - Identify and pursue existing and new opportunities
  - Respond to deviations in performance more quickly and consistently
  - Develop and report a more comprehensive and consistent portfolio view of risk
  - Improve collaboration, trust and information sharing

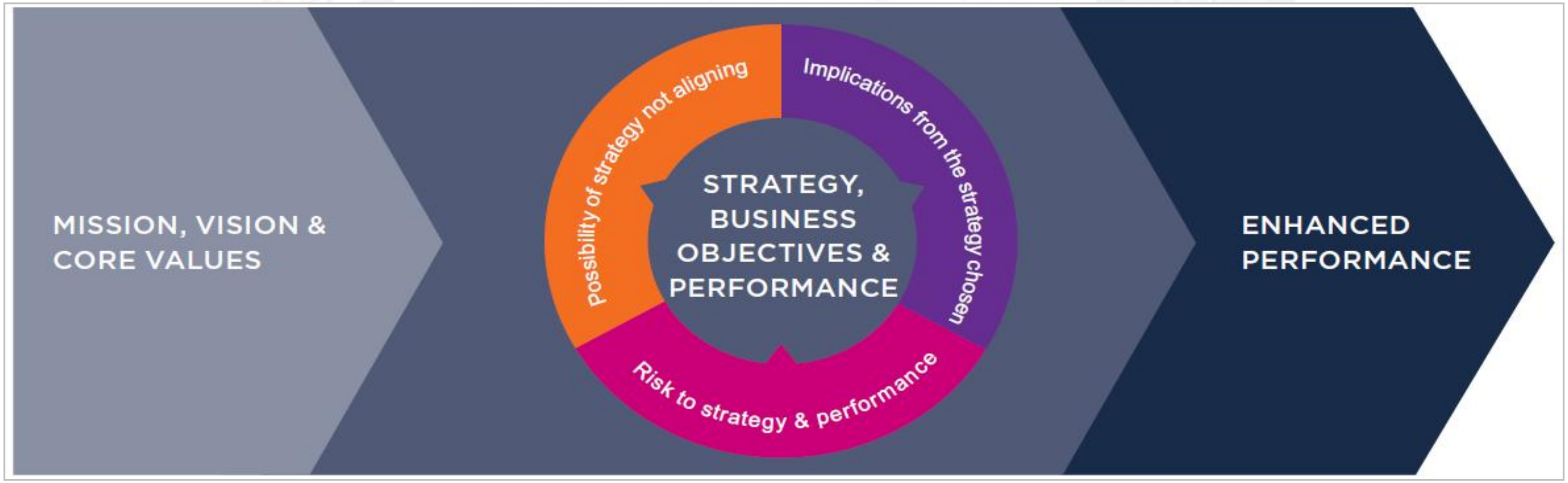
Emphasises Value

- Enhances the focus on value – how entities **create**, **preserve,** and **realise value**

- Embeds value throughout the framework, as evidenced by its:
  - Prominence in the core definition of enterprise risk management
  - Extensive discussion in principles
  - Linkage to risk appetite
  - Focus on the ability to manage risk to acceptable levels

Links to Strategy

- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy


MISSION, VISION & CORE VALUES
Possibility of strategy not aligning
Implications from the strategy chosen
STRATEGY, BUSINESS OBJECTIVES & PERFORMANCE
Risk to strategy & performance
ENHANCED PERFORMANCE

Links to Performance

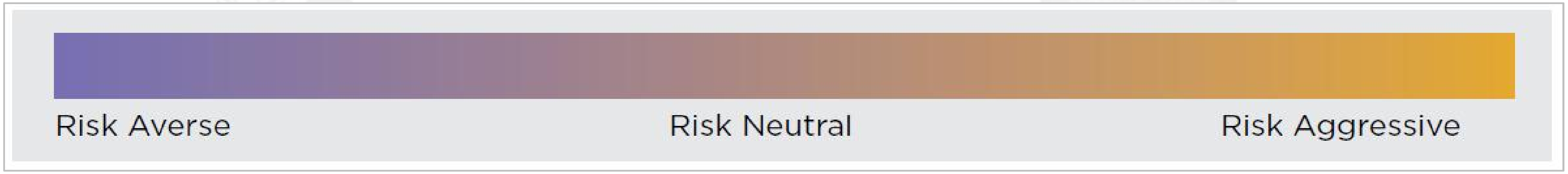
- Enables the achievement of strategy by actively managing risk and performance

- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing tolerance for variations in performance

- Manages risk in the context of achieving strategic and business objectives – not as individual risks

Recognises importance of Culture

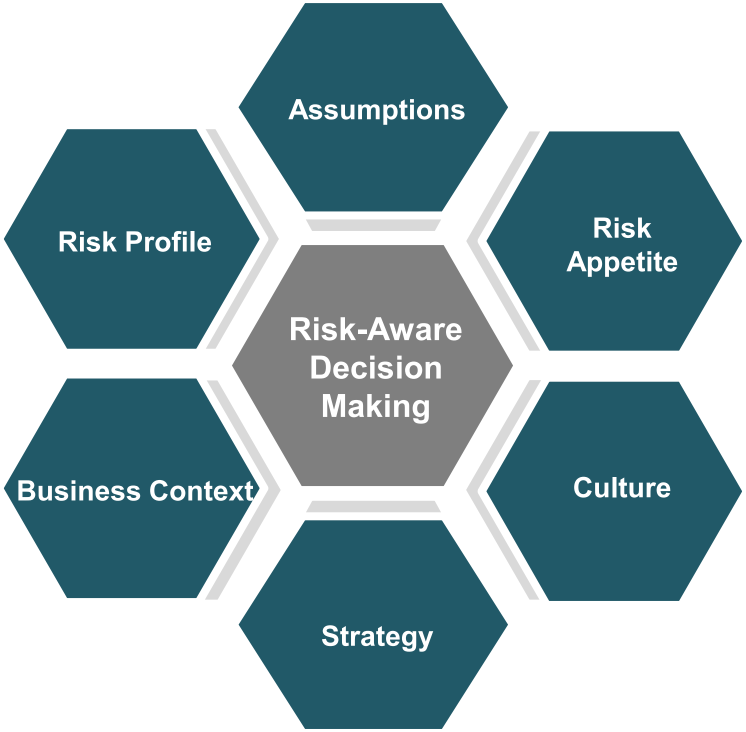
- Addresses the growing focus, attention and Importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within the broader context of overall core values
- Depicts culture behavior within a risk spectrum



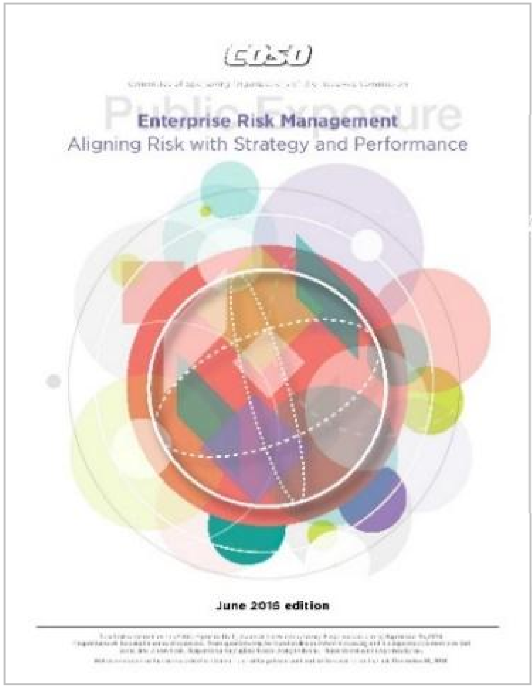
- Explores the possible effects of culture on decision making
- Explores the alignment of culture between individual and entity behavior

Focusses on Decision Making

- Explores how enterprise risk management drives risk-aware decision making
- Highlights how risk awareness optimizes and aligns decisions impacting performance
- Explores how risk-aware decisions affect the risk profile



Builds Links to Internal Control



COSO

Public Exposure

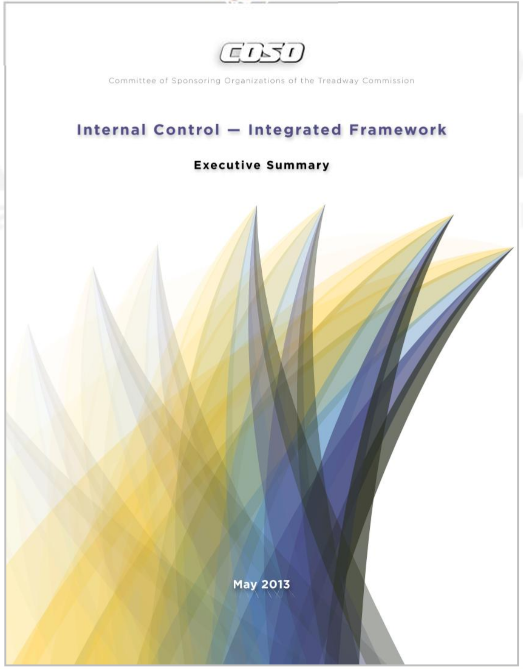
Enterprise Risk Management

Aligning Risk with Strategy and Performance

June 2016 edition

The document does **not** replace the 2013 *Internal Control – Integrated Framework*

The two frameworks are distinct and complementary



COSO

Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Executive Summary

May 2013

Both use a components and principles structure

Aspects of internal control common to Enterprise Risk Management are not repeated

Some aspects of internal control are developed further in this framework

ISO 31000

> Dealing with risk is part of governance and leadership, and is fundamental to how an organization is managed at all levels.

International Organization for Standardization

Updated Risk Management Guidance

ISO 31000: 2018 is an international guidance standard for Risk management. This edition cancels and replaces the first edition (ISO 31000:2009) which has recently been technically revised.

The updated standard focuses upon:

- Review of the principles of risk management, which are the key criteria for its success
- Highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;
- Greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process;
- Streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts.

Updated Risk Management Guidance

- highlighting of the leadership by top management and the integration of risk management, starting with the governance of the organization;
- greater emphasis on the iterative nature of risk management, noting that new experiences, knowledge and analysis can lead to a revision of process elements, actions and controls at each stage of the process;
- streamlining of the content with greater focus on sustaining an open systems model to fit multiple needs and contexts.

Value creation is the overall principle of risk management
Leadership and Commitment are addressed much more precisely
The integrated approach is more dominant

About ISO 31000: 2018

Who is ISO 31000 for ?

ISO 31000 is applicable to all organizations, regardless of type, size, activities and location, and covers all types of risk.

It was developed by a range of stakeholders and is intended for use by anyone who manages risks, not just professional risk managers.

About ISO 31000: 2018

What are the benefits for my business ?

ISO 31000 helps organizations develop a risk management strategy to effectively identify and mitigate risks, thereby enhancing the likelihood of achieving their objectives and increasing the protection of their assets.

Its overarching goal is to develop a risk management culture where employees and stakeholders are aware of the importance of monitoring and managing risk.

Implementing ISO 31000 also helps organizations see both the positive opportunities and negative consequences associated with risk, and allows for more informed, and thus more effective, decision making, namely in the allocation of resources. What’s more, it can be an active component in improving an organization’s governance and, ultimately, its performance.

What are the main differences ?

ISO 31000:2018 provides more strategic guidance than ISO 31000:2009 and places more emphasis on both the involvement of senior management and the integration of risk management into the organization.

This includes the recommendation to develop a statement or policy that confirms a commitment to risk management, assigning authority, responsibility and accountability at the appropriate levels within the organization and ensuring that the necessary resources are allocated to managing risk.

The revised standard now also recommends that risk management be part of the organization's structure, processes, objectives, strategy and activities. It places a greater focus on creating value as the key driver of risk management and features other related principles such as continual improvement, the inclusion of stakeholders, being customized to the organization and consideration of human and cultural factors.

The content has been streamlined to reflect an open systems model that regularly exchanges feedback with its external environment in order to fit a wider range of needs and contexts.

Breaking Down ISO 31000:2018

ISO 31000:2018 constitute a succinct and concentrated guide to help organizations improve the way they manage their risks, consists of four major sections:

1

The definitions of key terms such as risk, risk management, stakeholder, risk source, event, consequence, likelihood and control

2

The principles of risk management — namely, that risk management is integrated, executed via a structured and comprehensive approach, customized, inclusive, dynamic, based on the best information available regarding both human and cultural factors, and continuously improved

3

A framework for ensuring that risk management is properly implemented, well-integrated throughout the organization, carefully designed, regularly reviewed, and continuously adapted and improved

4

A section on the risk management process itself, including the traditional elements of risk identification, analysis, evaluation and treatment, bolstered by a monitoring and review element as well as a communication and consultation element — the former to improve the effectiveness and quality of the risk management process, and the latter to ensure that "factual, timely, relevant, accurate and understandable" risk information is being communicated and used for decision-making.

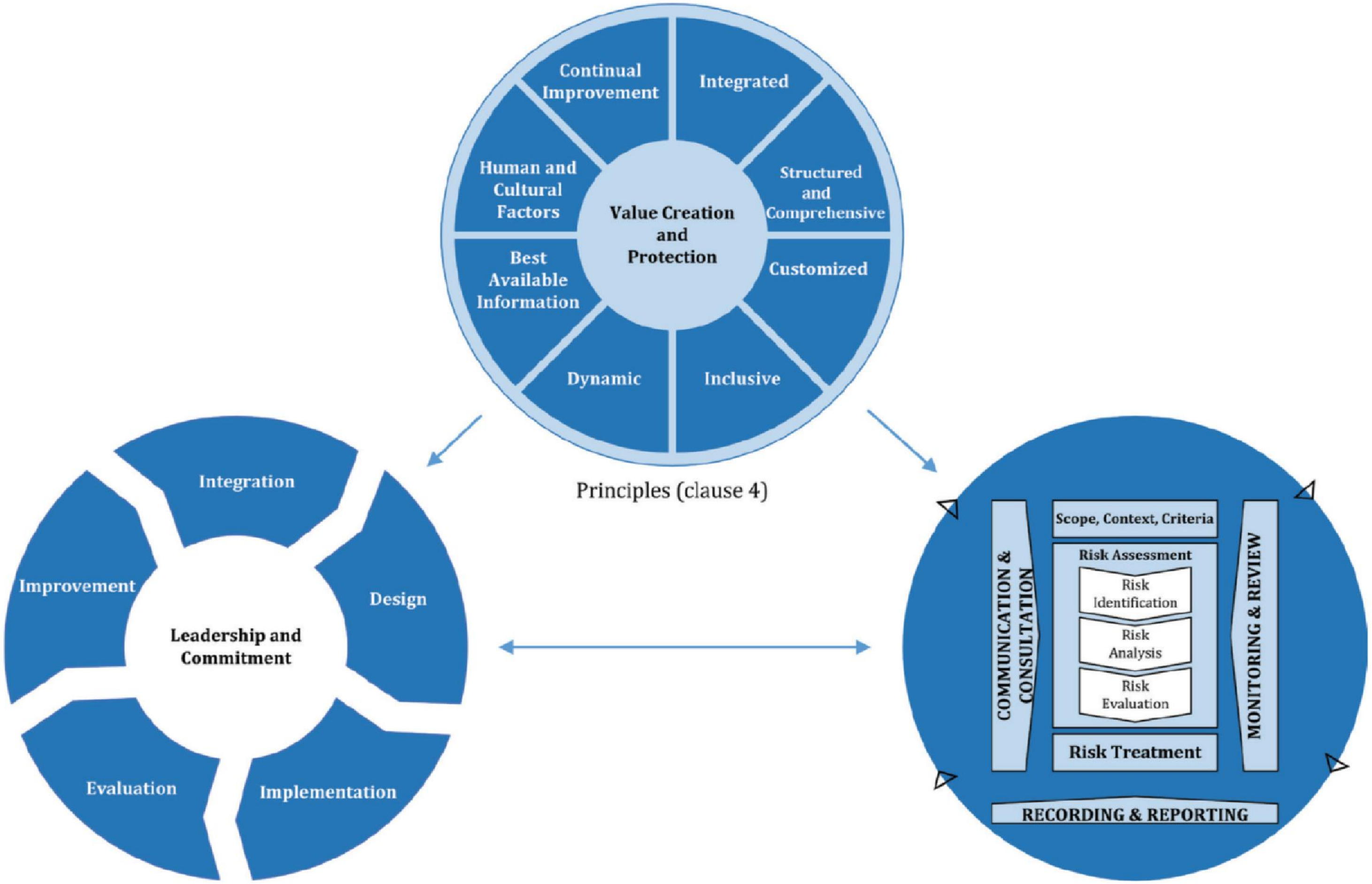
Principles, framework & risk management process from ISO 31000

ISO 31000 states that the guidelines should be used by people who create and protect value in organisations by managing risks, making decisions, setting and achieving objectives and improving performance.

The guidelines are applicable to all types and sizes of organisations and relevant to all external and internal factors and influences.

They also state that managing risk assists organisations in setting strategy, achieving objectives and making informed decisions. Managing risk is part of governance and leadership and is fundamental to how organisations are managed at all levels.

Principles, framework & risk management process from ISO 31000



Principles (clause 4)

Framework (clause 5)

Process (clause 6)

Principles

🟦 *provide guidance on how a risk management initiative should be designed*

🟥 *relate to the operation of the risk management initiative*

🟦 Framework and processes should be customised and proportionate.

🟦 Appropriate and timely involvement of stakeholders is necessary.

🟦 Structured and comprehensive approach is required.

🟦 Risk management is an integral part of all organisational activities.

🟦 Risk management anticipates, detects, acknowledges and responds to changes.

🟥 Risk management explicitly considers any limitations of available information.

🟥 Human and cultural factors influence all aspects of risk management.

🟥 Risk management is continually improved through learning and experience.

What does the principles means?

Aligned

Risk management activities need to be aligned with the other activities in the organisation

Comprehensive

In order to be fully effective, the risk management approach must be comprehensive

Embedded

Risk management activities need to be embedded within the organisation

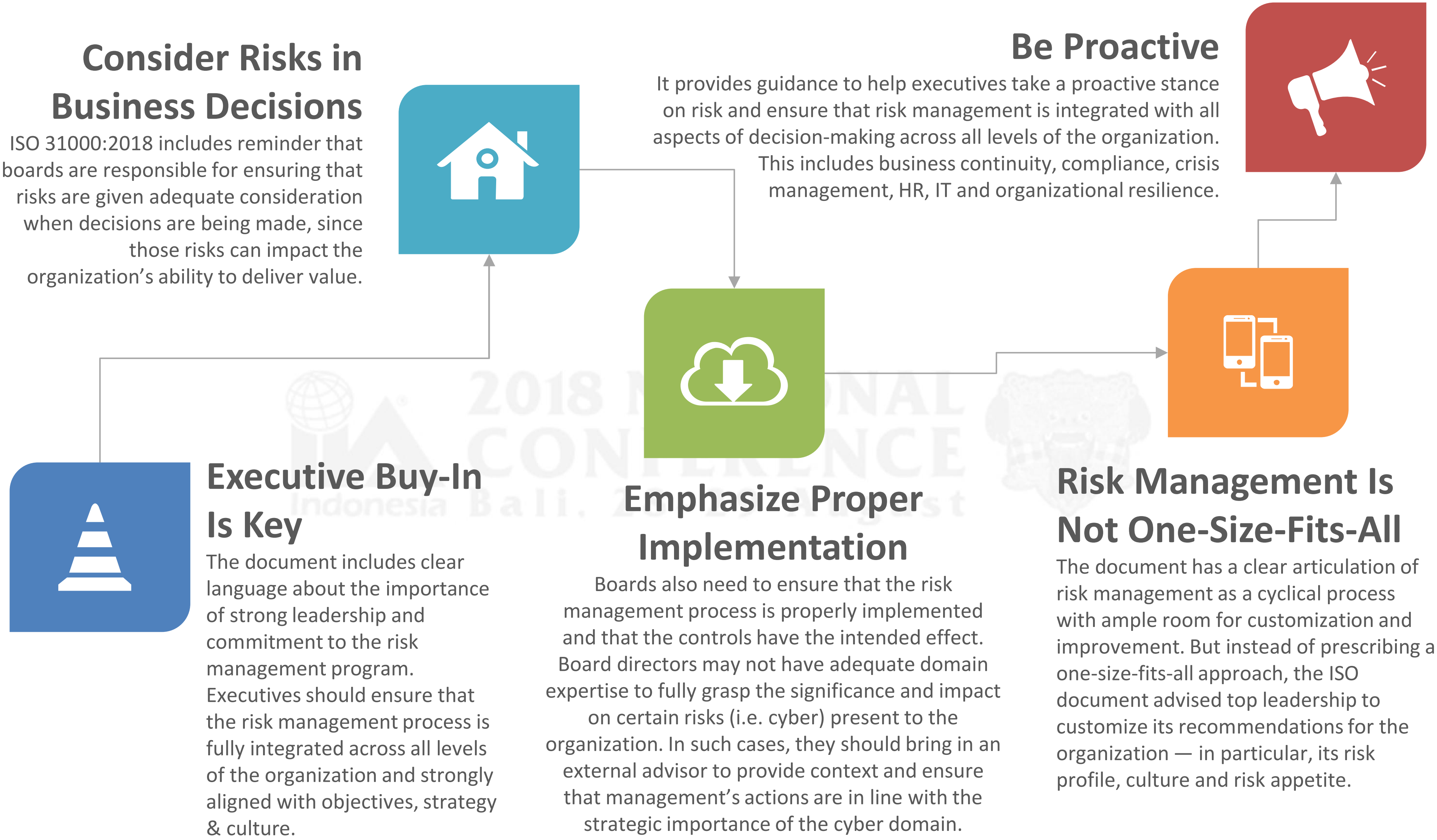
Proportionate

Risk management activities must be proportionate to the level of risk faced by the organisation

Dynamic

Risk management activities must be dynamic & responsive to emerging and changing risks

Takeaways for Boards & Top Leadership



Executive Buy-In Is Key

The document includes clear language about the importance of strong leadership and commitment to the risk management program. Executives should ensure that the risk management process is fully integrated across all levels of the organization and strongly aligned with objectives, strategy & culture.

Consider Risks in Business Decisions

ISO 31000:2018 includes reminder that boards are responsible for ensuring that risks are given adequate consideration when decisions are being made, since those risks can impact the organization's ability to deliver value.

Emphasize Proper Implementation

Boards also need to ensure that the risk management process is properly implemented and that the controls have the intended effect. Board directors may not have adequate domain expertise to fully grasp the significance and impact on certain risks (i.e. cyber) present to the organization. In such cases, they should bring in an external advisor to provide context and ensure that management's actions are in line with the strategic importance of the cyber domain.

Risk Management Is Not One-Size-Fits-All

The document has a clear articulation of risk management as a cyclical process with ample room for customization and improvement. But instead of prescribing a one-size-fits-all approach, the ISO document advised top leadership to customize its recommendations for the organization — in particular, its risk profile, culture and risk appetite.

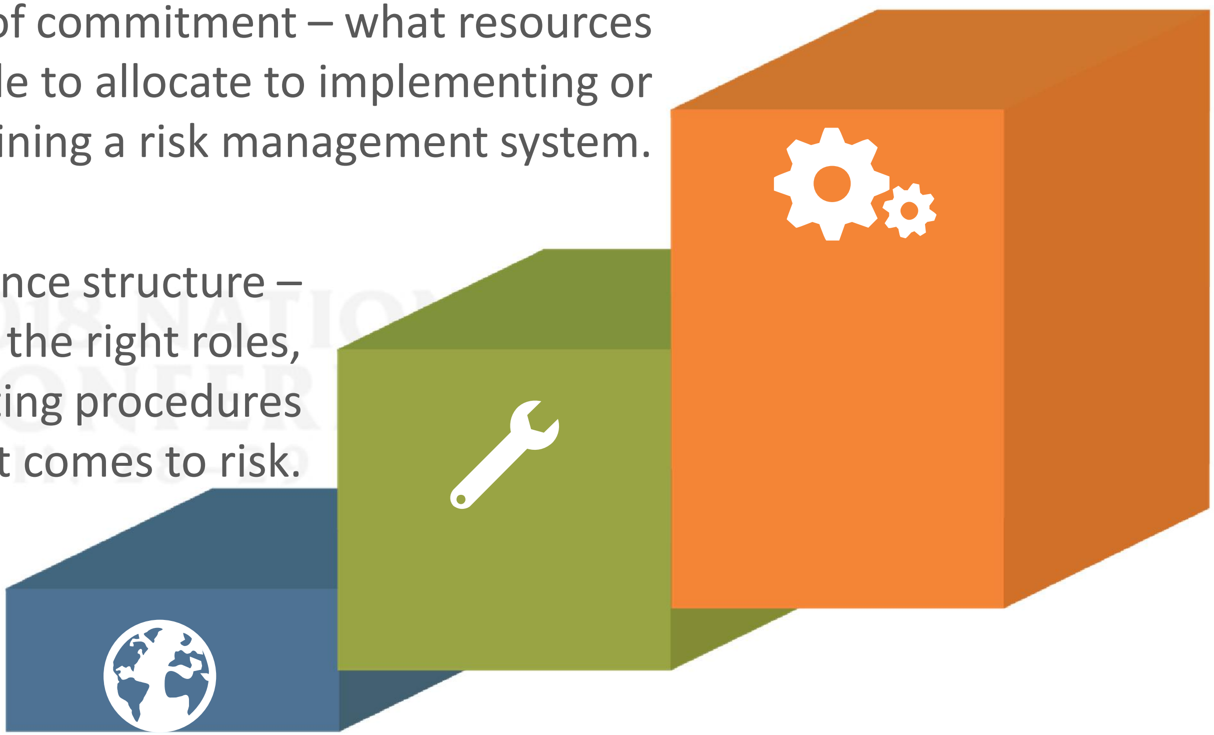
Be Proactive

It provides guidance to help executives take a proactive stance on risk and ensure that risk management is integrated with all aspects of decision-making across all levels of the organization. This includes business continuity, compliance, crisis management, HR, IT and organizational resilience.

How do I get started?

Define your level of commitment – what resources will you be able to allocate to implementing or maintaining a risk management system.

Assess your current governance structure – this will ensure you allocate the right roles, responsibilities and reporting procedures when it comes to risk.



Be aware of your organization’s key objectives – this will help you clarify the targets and requirements of your risk management system.

What Does it mean for Internal Audit

Which one to use?

There is no RIGHT or WRONG answer

There are a number of areas of overlap between the two

This largely comes through the emphasis from both on Principles

Integration

Culture

Improvement

Value

Internal Control/Process

Conclusion

COSO ERM focuses on:

- Integrating with strategy and performance
- Creating, preserving and realising value

- Drives better decision making
- Can be applied across all industries and organisations of any size

ISO 31000 focuses on:

- The process of Risk Management
- The recognition of value creation as a main element

The value for internal audit

Both sets of Standards can be used but

COSO integrates easily with the COSO Internal Control Framework and provides Internal Audit with an integrated approach to Risk Management and Internal Control, providing a better vehicle for Internal Audit to assist the improvement of Corporate Governance.

Thank You

Phil Tarling
Internal Audit Consultant
Tel:+441329282155
Mob:+447802656986
Email: Phil.tarling@outlook.com
http://www.tarlingassurancerisk.co.uk.

Angela Simatupang
angela.simatupang@rsm.id
https://www.rsm.global/indonesia/en