COSO AND INTERNAL AUDIT

HOW CAN THEY CONTRIBUTE TO INSIGHT?

IAS Conference, November 27th, 2019

ista

FOCUS OF PRESENTATION

- Changing Risk Landscape
- Changing demand of stakeholders
- Integrate COSO principles into business practices
- Apply COSO and Internal Audit principles
- How to achieve Internal Audit’s mission

3 GROUPS OF RISKS ARE EVOLVING

Natural
Extreme weather events
Natural disasters
Failure of climate-change mitigation and adaptation

Digital
Cybersecurity
Data Protection
Identity theft

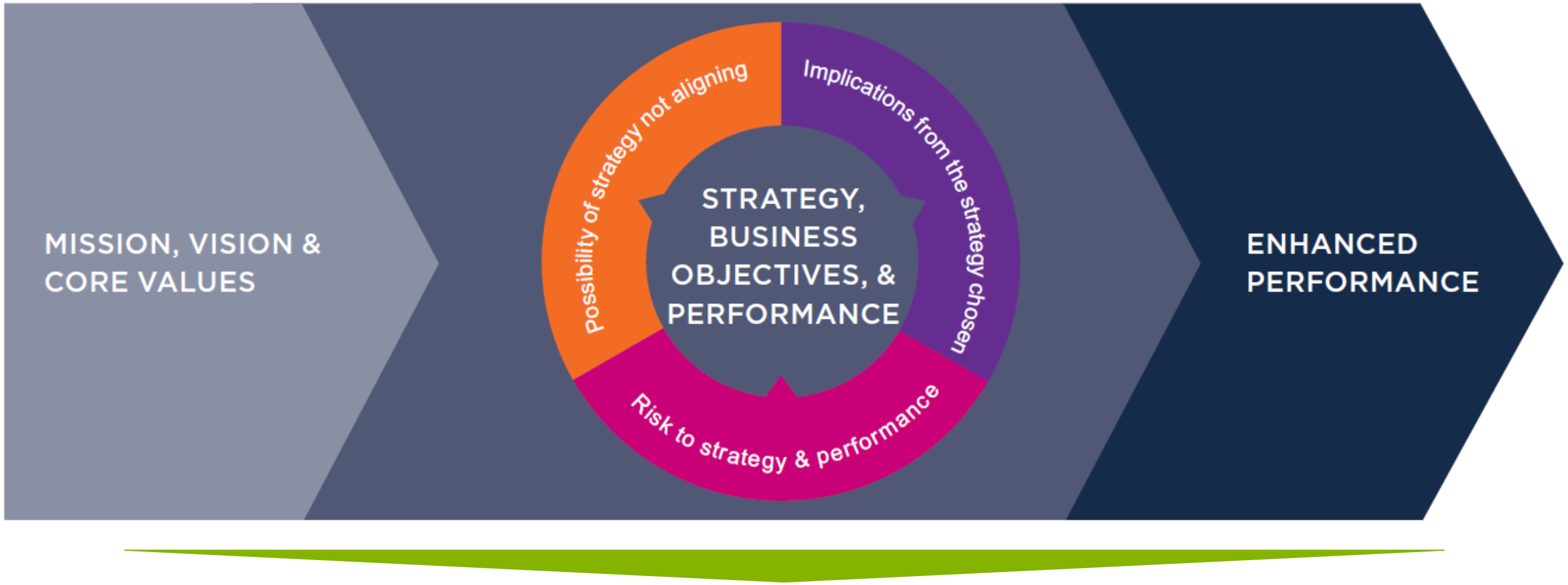
Geopolitical
Weapons of mass destruction
Embargo
Trade war

DEMAND (OR NEED) OF STAKEHOLDERS

- **Boards overconfidence**
  - Boards view the organization’s capability to manage risks higher than management.
- **Make misalignment transparent**
  - Internal Audit needs to set the right expectations – no horror scenario, but also no trivialisation
- **Implement/Enhance systematic ERM approach**
  - Internal Audit needs to evaluate Risk Management procedures and help to improve, professionalise them (e.g. using COSO ERM as possible approach)
- **Focus on current and future risks**
  - Internal Audit needs to look into current developments – listen to the business, but also look outside the company/industry

https://www.theiia.org/OnRisk

THE COSO ERM FRAMEWORK
INTEGRATING WITH STRATEGY & PERFORMANCE 2017


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

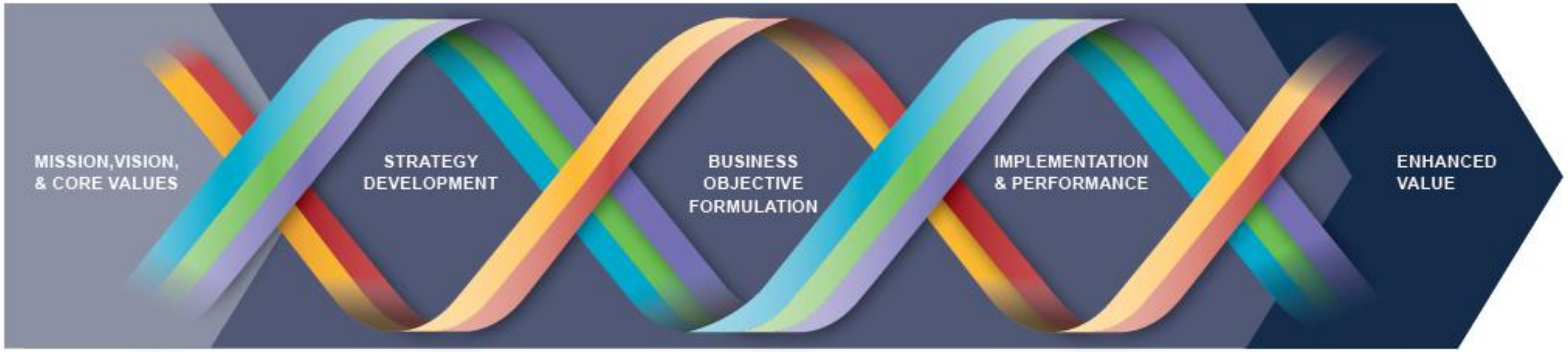
High level risks in Context of the strategy:

- Possibility of misalignment between strategy and Mission, Vision & Core Values
- Implications from the strategy chosen

Source: COSO ERM – Integrating with Strategy and Performance 2017

COSO ERM Framework 2017

RISK MANAGEMENT COMPONENTS & UNDERLYING PRINCIPLES


MISSION,VISION, & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE

Components	**Governance & Culture**	**Strategy & Objective-Setting**	**Performance**	**Review & Revision**	**Information, Communication, & Reporting**
Principles	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

Source: COSO ERM – Integrating with Strategy and Performance 2017

INTEGRATE COSO PRINCIPLES INTO BUSINESS PRACTICES

ERM or Internal Control???
BOTH !!!

COSO
Public Exposure
Enterprise Risk Management
Aligning Risk with Strategy and Performance
June 2016 edition
COSO
Internal Control — Integrated Framework
Executive Summary
May 2013

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

The two frameworks are distinct and complementary

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 the ERM framework

COSO INTERNAL CONTROL PRINCIPLES

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

CORE PRINCIPLES FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING

1. Demonstrates integrity
2. Demonstrates competence and due professional care.
3. Is objective and free from undue influence (independent).
4. Aligns with the strategies, objectives, and risks of the organization
5. Is appropriately positioned and adequately resourced.
6. Demonstrates quality and continuous improvement.
7. Communicates effectively.
8. Provides risk-based assurance.
9. Is insightful, proactive, and future-focused.
10. Promotes organizational improvement.

The Institute of Internal Auditors

HOW TO ACHIEVE OUR MISSION

To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.

- **It's important but not enough to meet Standards!**
- **Use research and educational material to know more!**
- **Take COSO and IIA material as reference to your Charter, Manual and procedures!**
- **Align your audit risk assessment to the organization’s risk assessment!**
- **Understand which business objectives may be influenced by your audit work!**
- **Look beyond to see future challenges and incorporate them into your audit plans and projects!**

THANK YOU

Günther Meggeneder

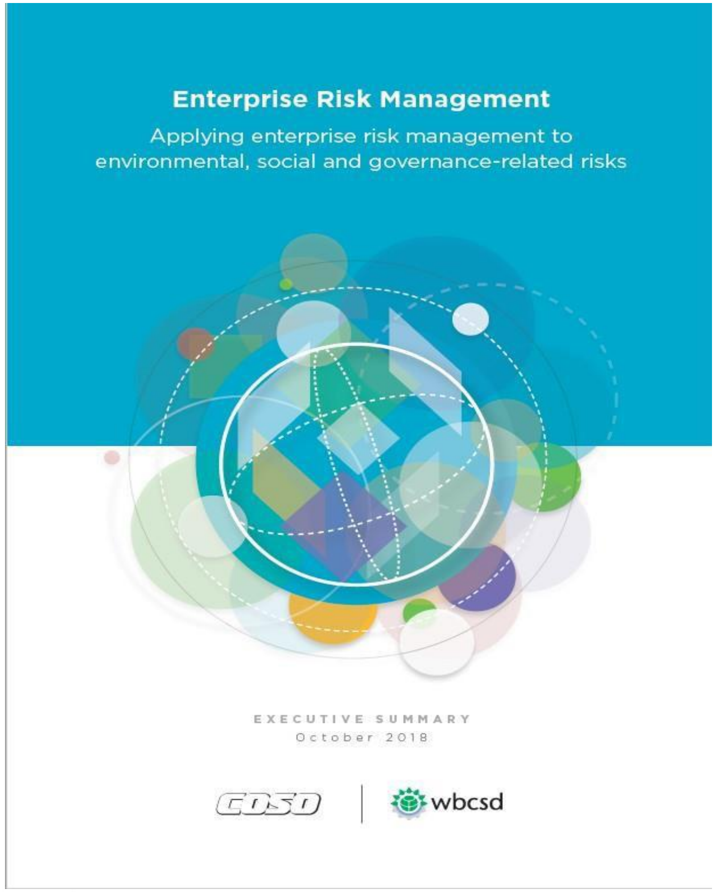
Head of Internal Audit and Compliance

ista international

Luxemburger Straße 1
DE - 45131 Essen

www.ista.com

APPLYING ENTERPRISE RISK MANAGEMENT TO ENVIRONMENTAL, SOCIAL AND GOVERNANCE-RELATED RISKS

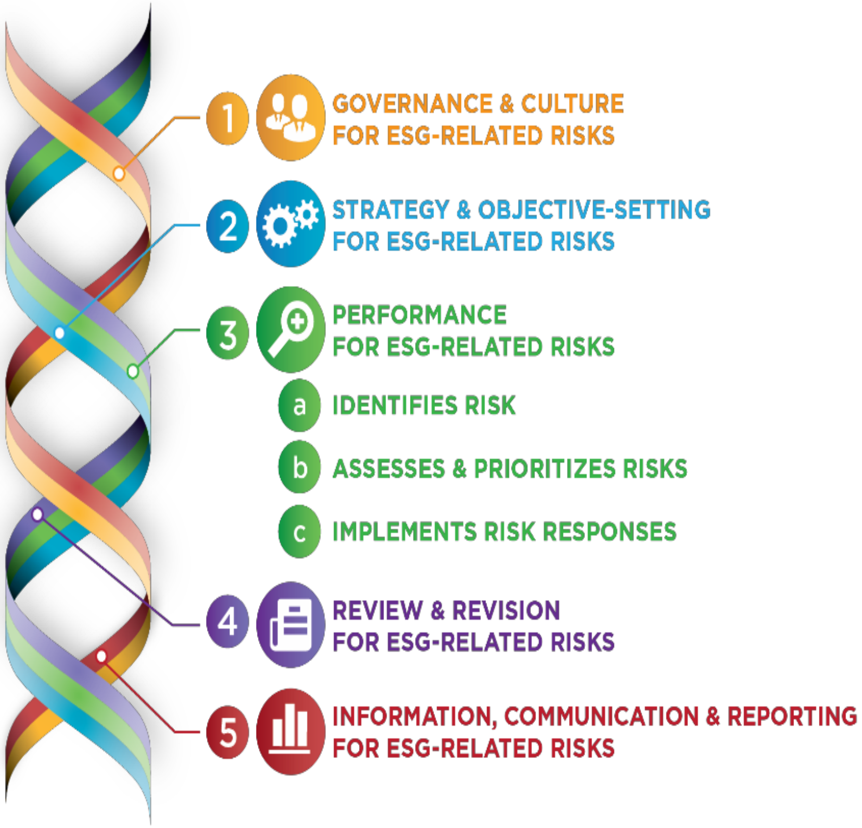


Enterprise Risk Management

Applying enterprise risk management to environmental, social and governance-related risks

EXECUTIVE SUMMARY
October 2018

COSO | wbcsd



1 GOVERNANCE & CULTURE FOR ESG-RELATED RISKS

2 STRATEGY & OBJECTIVE-SETTING FOR ESG-RELATED RISKS

3 PERFORMANCE FOR ESG-RELATED RISKS

a IDENTIFIES RISK

b ASSESSES & PRIORITIZES RISKS

c IMPLEMENTS RISK RESPONSES

4 REVIEW & REVISION FOR ESG-RELATED RISKS

5 INFORMATION, COMMUNICATION & REPORTING FOR ESG-RELATED RISKS

POTENTIAL UPDATES TO EXISTING GUIDANCE

COSO in the Cyber Age (Q4 2019)

Practical Approaches to Creating and Protecting Organizational Value (Q4 2019)

Understanding and Communicating Risk Appetite (Q4 2019)

Monitoring Guidance (TBD 2020)

ERM for Cloud Computing (TBD 2020)

POTENTIAL NEW GUIDANCE

Using COSO ERM to Manage Compliance Risks (Q1 2020)

Blockchain and its Impact on Internal Controls (Q1 2020)

ERM in an Agile Environment (Q1 2020)

Assessment Tools for Risk (Q2 2020)

Psychology and Sociology of Fraud (TBD)

Robotic Process Automation and Artificial Intelligence (TBD – no known authors at this time)