ISO 31000:2009 & COSO ERM

Jakarta, 2018

Facilitators:

Dr. Antonius Alijoyo MBA., ERMCP., CERG., CGAP., CCSA., CFSA., CGEIT., CFE

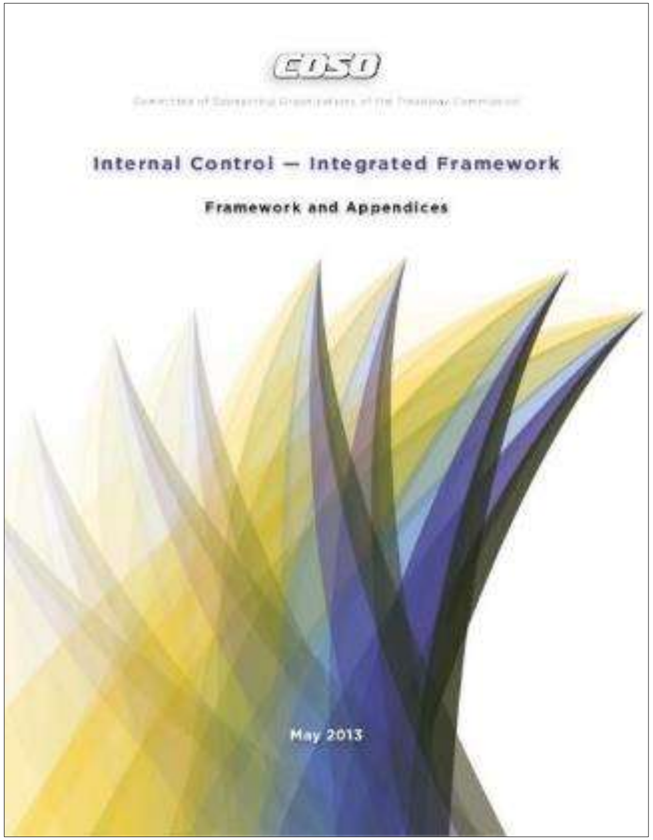
- Ketua KomTek 03-10 BSN

- Founder CRMS Indonesia

- Ketua Umum IRMAPA

COSO References

2 COSO frameworks do not replace each other, are distinct, & complimentary


COSO

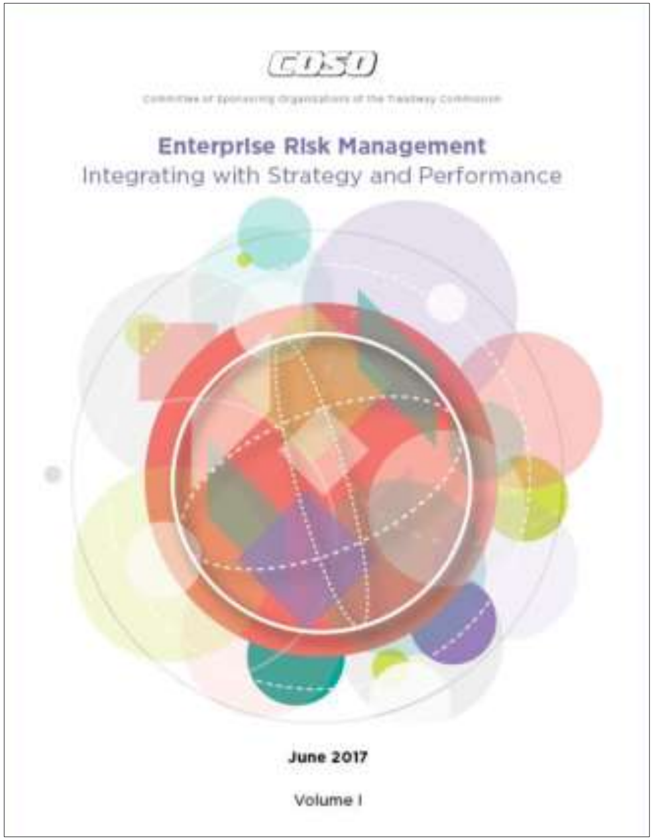
Committee of Sponsoring Organizations of the Treadway Commission

Internal Control — Integrated Framework

Framework and Appendices

May 2013

Internal Control Framework - 2013


COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management
Integrating with Strategy and Performance

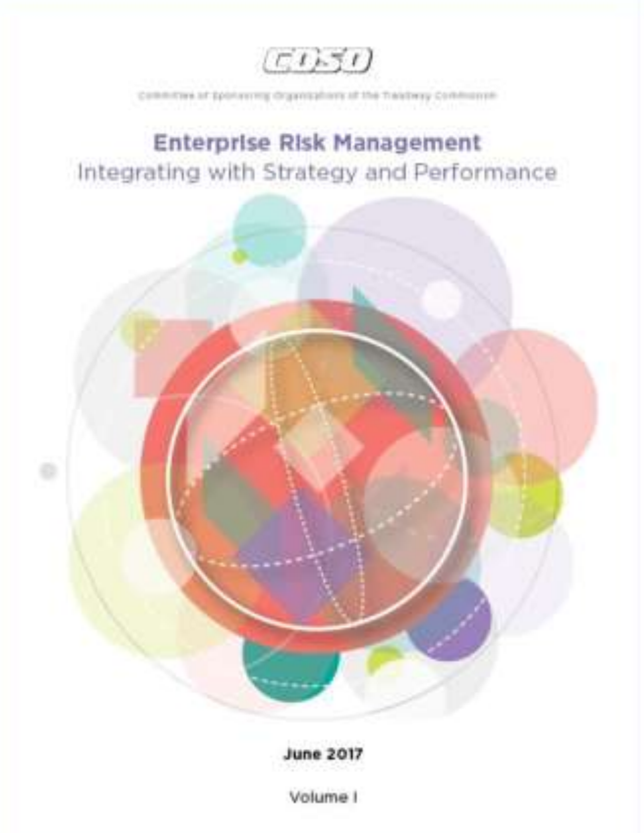
June 2017

Volume I

ERM Framework - 2017

COSO References

COSO ERM Framework – Integrating with Strategy and Performance



COSO

Committee of Sponsoring Organizations of the Treadway Commission

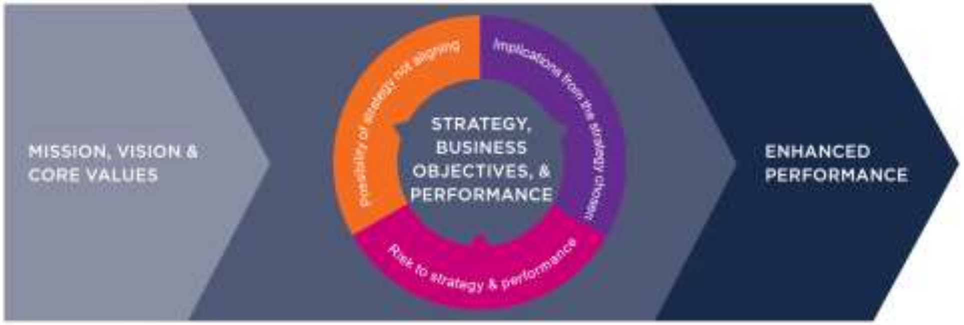
Enterprise Risk Management

Integrating with Strategy and Performance

June 2017

Volume I

ERM Framework -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

Explores ERM and strategy from 3 different perspectives:

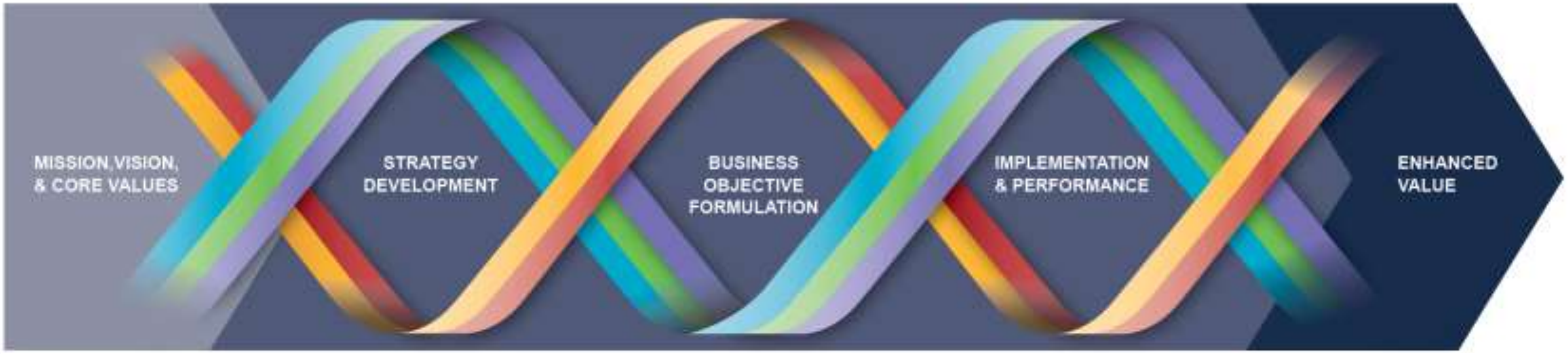
- The possibility of strategy and business objectives not aligning with mission, vision, and values
- The implications from the strategy chosen
- Risk to executing the strategy

CRMS INDONESIA
Center for Risk Management Studies

COSO References

COSO ERM Framework – Integrating with Strategy and Performance

ENTERPRISE RISK MANAGEMENT


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

Governance & Culture

Strategy & Objective-Setting

Performance

Review & Revision

Information, Communication, & Reporting

Focuses on 5 interrelated components

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

Plus, introduces 20 principles

COSO References

COSO ERM Framework – Integrating with Strategy and Performance

Governance & Culture | Strategy & Objective-Setting | Performance | Review & Revision | Information, Communication, & Reporting

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.

COSO References

COSO ERM Framework – Integrating with Strategy and Performance

Governance & Culture | Strategy & Objective-Setting | Performance | Review & Revision | Information, Communication, & Reporting

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 & Revision**: By reviewing entity performance, an organization can con-sider 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, & 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 ERM & ISO 31000

COSO ERM Framework

Governance & Culture

1. **Exercises Board Risk Oversight**—The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.

2. **Establishes Operating Structures—**The organization establishes operating structures in the pursuit of strategy and business objectives.

3. **Defines Desired Culture—**The organization defines the desired behaviors that characterize the entity's desired culture.

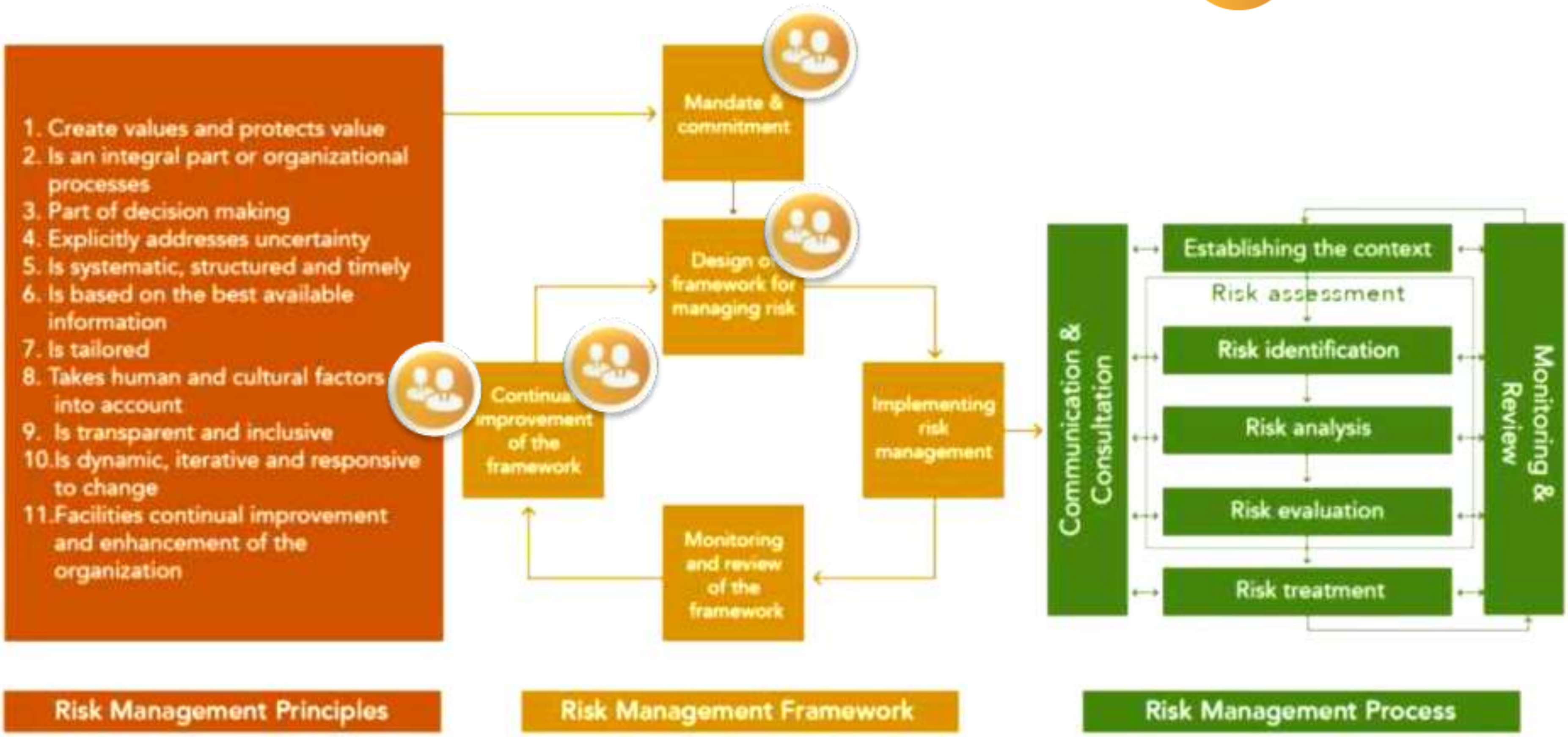
4. **Demonstrates Commitment to Core Values**—The organization demonstrates a commitment to the entity's core values.

5. **Attracts, Develops, and Retains Capable Individuals**—The organization is committed to building human capital in alignment with the strategy and business objectives.

COSO ERM & ISO 31000

COSO ERM in ISO 31000 perspective

Governance & Culture



1. Create values and protects value
2. Is an integral part or organizational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and responsive to change
11. Facilities continual improvement and enhancement of the organization

Mandate & commitment
Design of framework for managing risk
Continual improvement of the framework
Implementing risk management
Monitoring and review of the framework
Communication & Consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring & Review
Risk Management Principles
Risk Management Framework
Risk Management Process

CRMS INDONESIA
Center for Risk Management Studies

COSO ERM & ISO 31000

COSO ERM Framework

6. **Analyzes Business Context**—The organization considers potential effects of business context on risk profile.

7. **Defines Risk Appetite**—The organization defines risk appetite in the context of creating, preserving, and realizing value.

8. **Evaluates Alternative Strategies**—The organization evaluates alternative strategies and potential impact on risk profile.

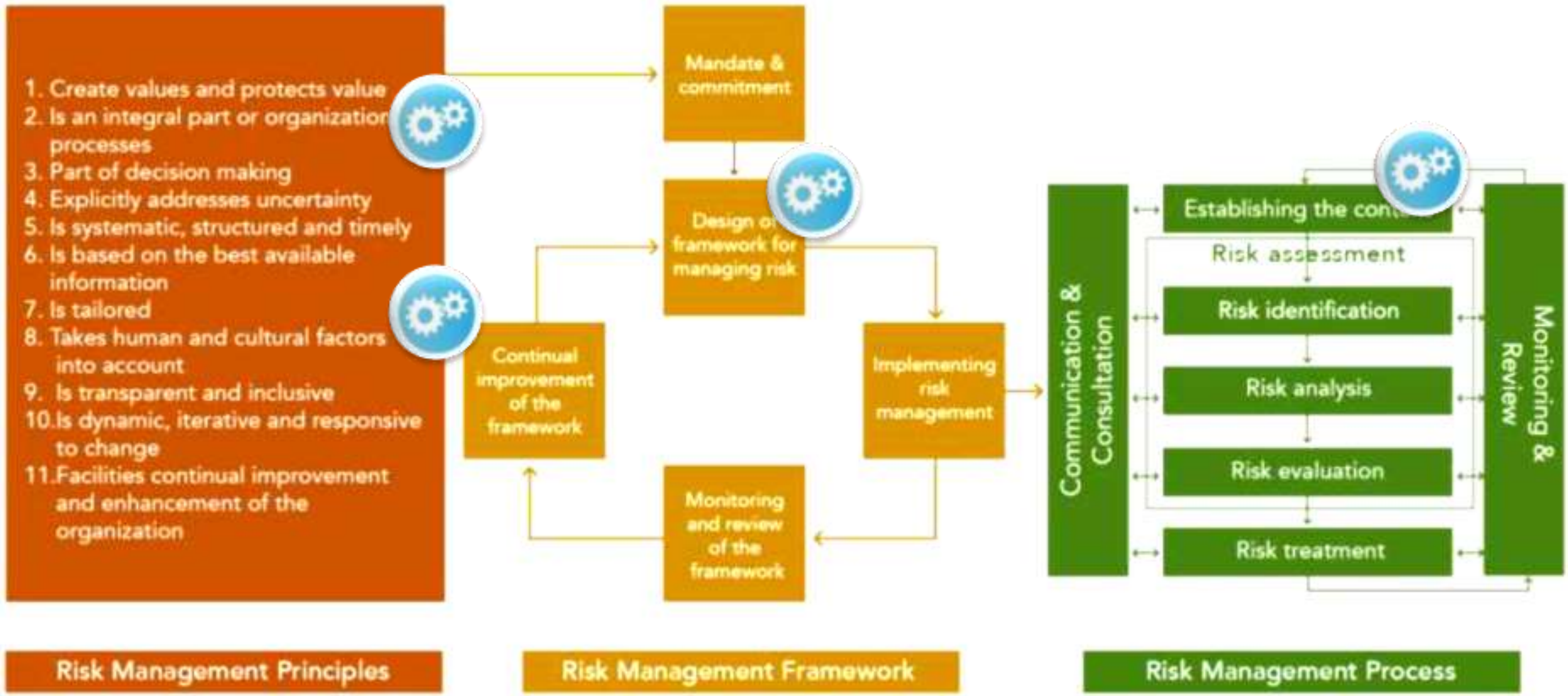
9. **Formulates Business Objectives**—The organization considers risk while establishing the business objectives at various levels that align and support strategy.

Strategy & Objective-Setting

COSO ERM & ISO 31000

COSO ERM in ISO 31000 perspective

Strategy & Objective-Setting



1. Create values and protects value
2. Is an integral part or organization processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and responsive to change
11. Facilities continual improvement and enhancement of the organization

Mandate & commitment
Design of framework for managing risk
Implementing risk management
Monitoring and review of the framework
Continual improvement of the framework
Communication & Consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring & Review
Risk Management Principles
Risk Management Framework
Risk Management Process

COSO ERM & ISO 31000

COSO ERM Framework

Performance

10. **Identifies Risk**—The organization identifies risk that impacts the performance of strategy and business objectives.

11. **Assesses Severity of Risk**—The organization assesses the severity of risk.

12. **Prioritizes Risks**—The organization prioritizes risks as a basis for selecting responses to risks.

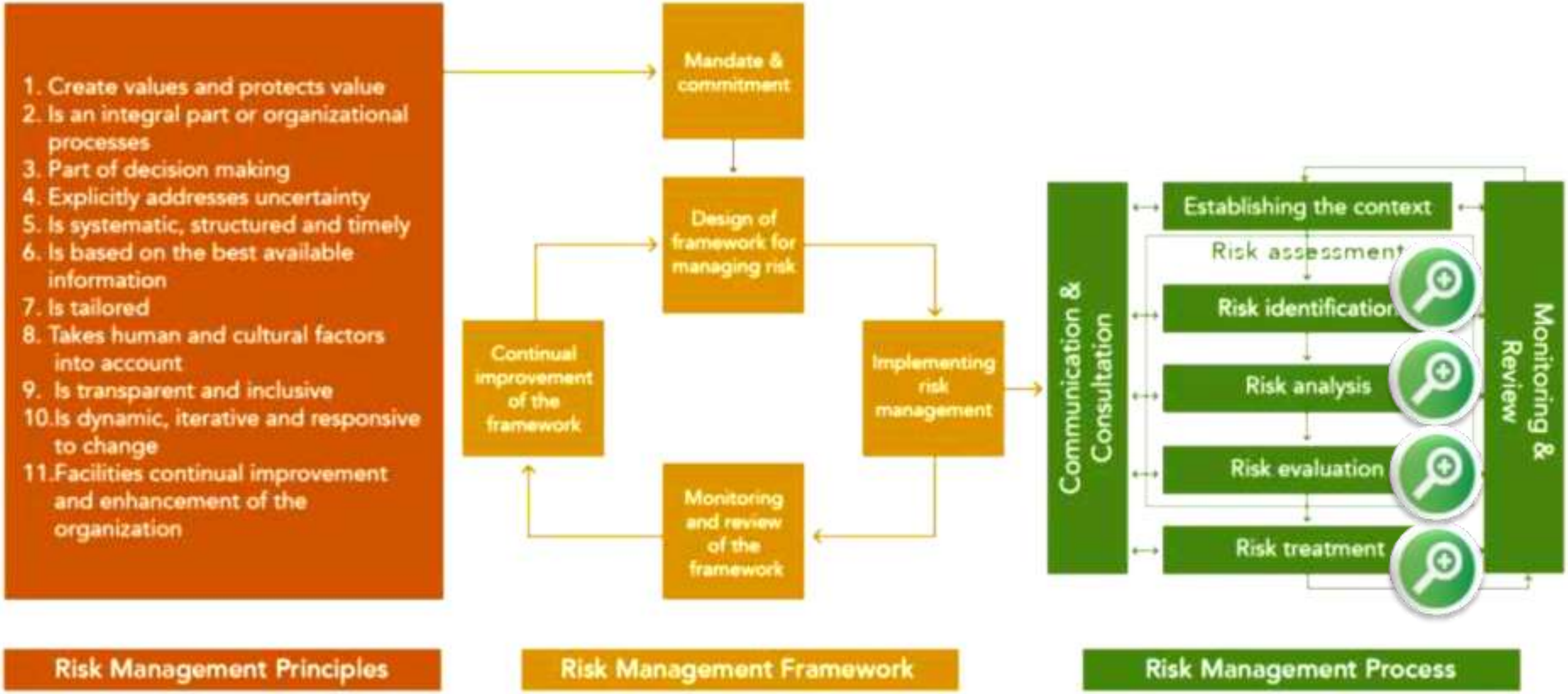
13. **Implements Risk Responses**—The organization identifies and selects risk responses.

14. **Develops Portfolio View**—The organization develops and evaluates a portfolio view of risk.

COSO ERM & ISO 31000

COSO ERM in ISO 31000 perspective

Performance



1. Create values and protects value
2. Is an integral part or organizational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and responsive to change
11. Facilities continual improvement and enhancement of the organization

Mandate & commitment

Design of framework for managing risk

Implementing risk management

Monitoring and review of the framework

Continual improvement of the framework

Communication & Consultation

Establishing the context

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Monitoring & Review

Risk Management Principles

Risk Management Framework

Risk Management Process

COSO ERM Framework

15. **Assesses Substantial Change**—The organization identifies and assesses changes that may substantially affect strategy and business objectives.

16. **Reviews Risk and Performance**—The organization reviews entity performance and considers risk.

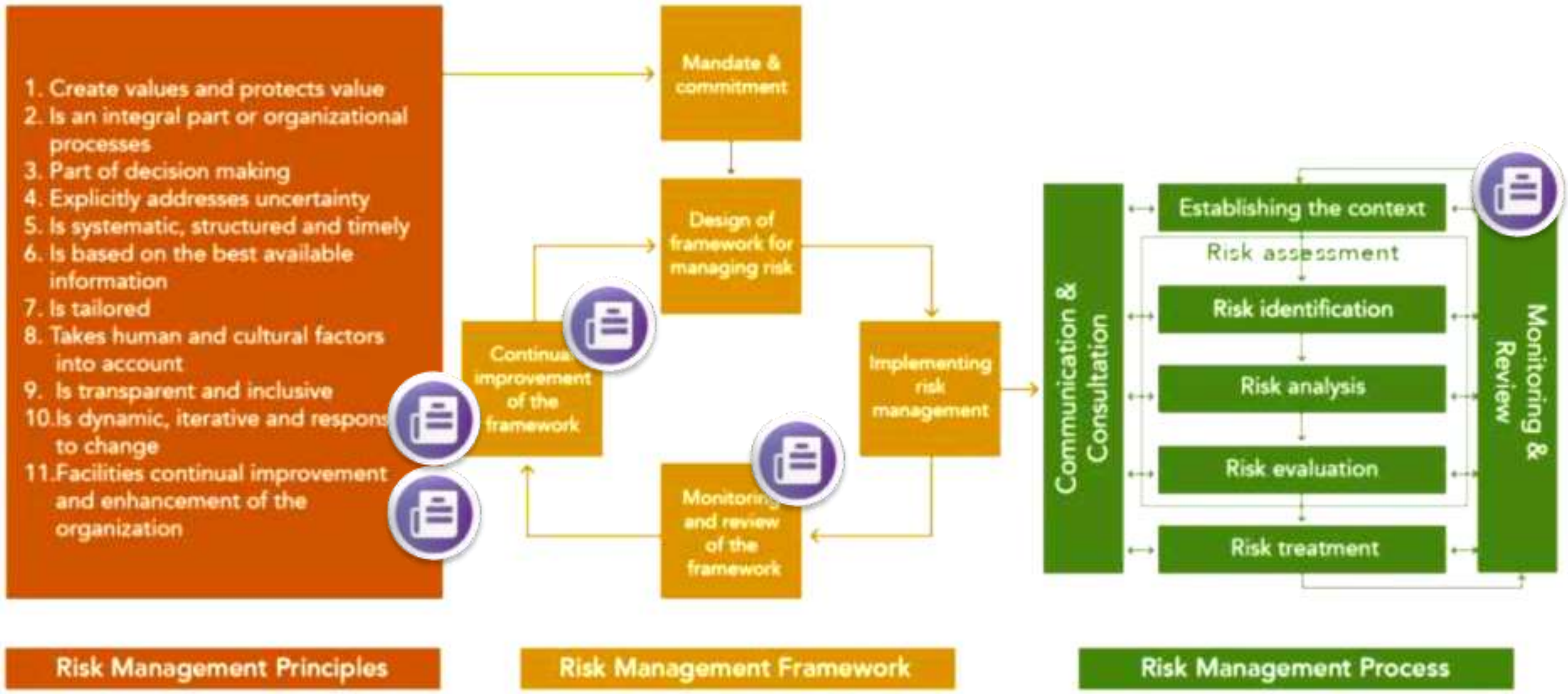
17. **Pursues Improvement in Enterprise Risk Management**—The organization pursues improvement of enterprise risk management.

Review & Revision

COSO ERM & ISO 31000

COSO ERM in ISO 31000 perspective

Review & Revision



1. Create values and protects value
2. Is an integral part or organizational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and respons to change
11. Facilities continual improvement and enhancement of the organization

Mandate & commitment

Design of framework for managing risk

Continua improvement of the framework

Implementing risk management

Monitoring and review of the framework

Communication & Consultation

Establishing the context

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Monitoring & Review

Risk Management Principles

Risk Management Framework

Risk Management Process

COSO ERM & ISO 31000

COSO ERM Framework

Information, Communication, & Reporting

18. **Leverages Information Systems**—The organization leverages the entity's information and technology systems to support enterprise risk management.

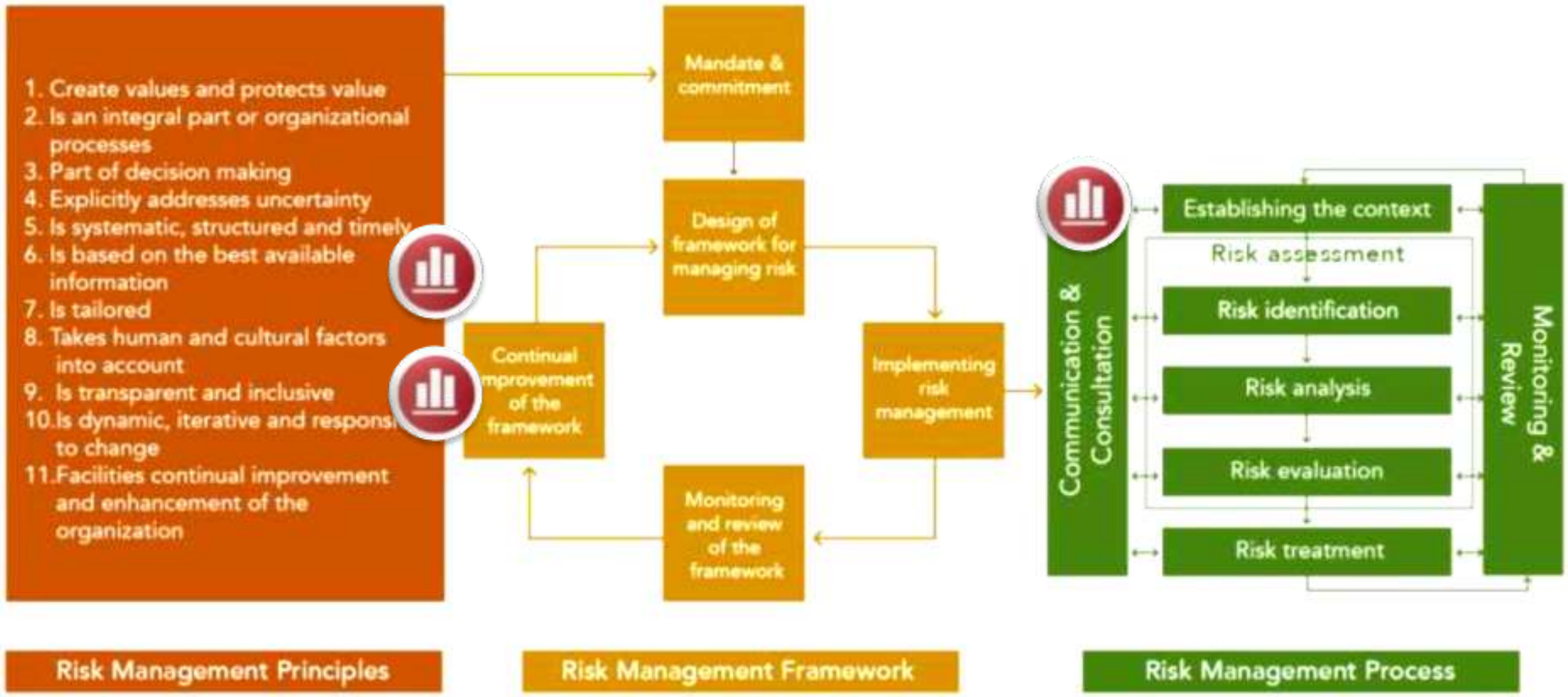
19. **Communicates Risk Information**—The organization uses communication channels to support enterprise risk management.

20. **Reports on Risk, Culture, and Performance**—The organization reports on risk, culture, and performance at multiple levels and across the entity.

COSO ERM & ISO 31000

COSO ERM in ISO 31000 perspective

Information, Communication, & Reporting



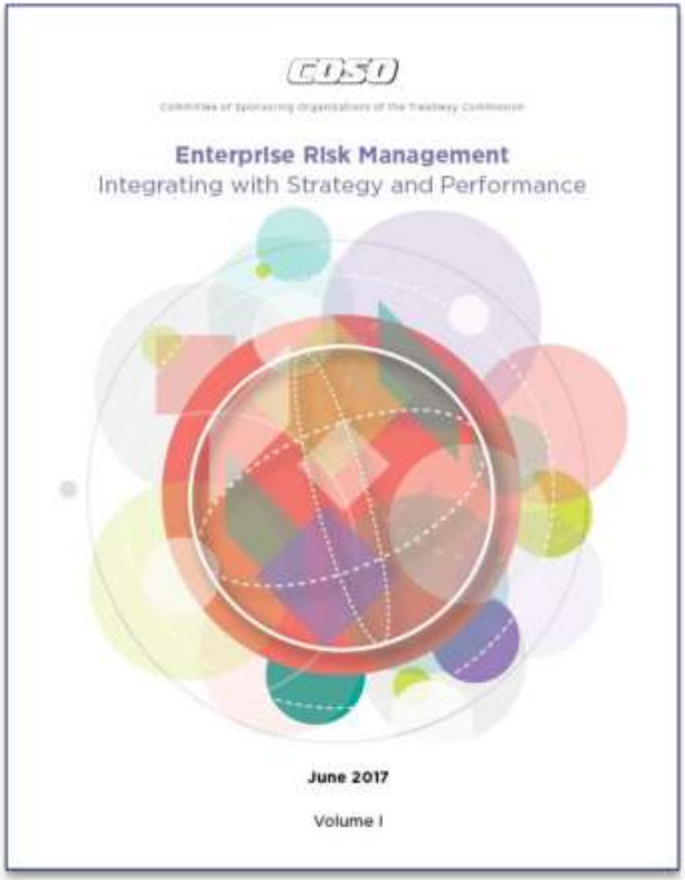
1. Create values and protects value
2. Is an integral part or organizational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and respons to change
11. Facilities continual improvement and enhancement of the organization

Mandate & commitment
Design of framework for managing risk
Implementing risk management
Monitoring and review of the framework
Continual improvement of the framework
Communication & Consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring & Review
Risk Management Principles
Risk Management Framework
Risk Management Process

Some Challenges with COSO ERM

- Understanding the scope

Enterprise Risk Management Framework: Integrating with Strategy and Performance


COSO

Committee of Sponsoring Organizations of the Treadway Commission

Enterprise Risk Management
Integrating with Strategy and Performance

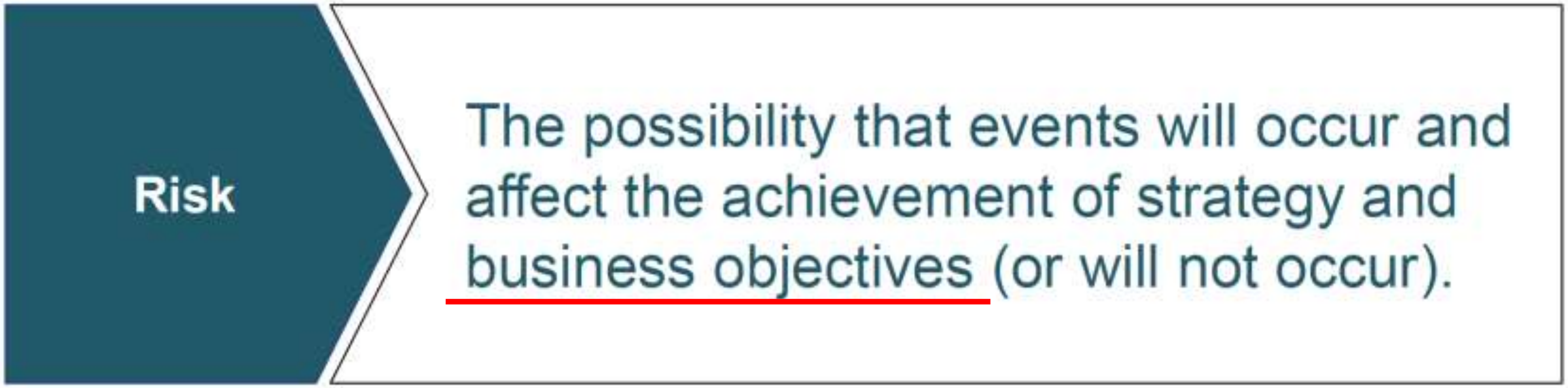
June 2017

Volume I

Enterprise is not the only type of organization that needs risk management (public organizations, project mgt. office, program task force).

Some Challenges with COSO ERM

- Understanding the scope



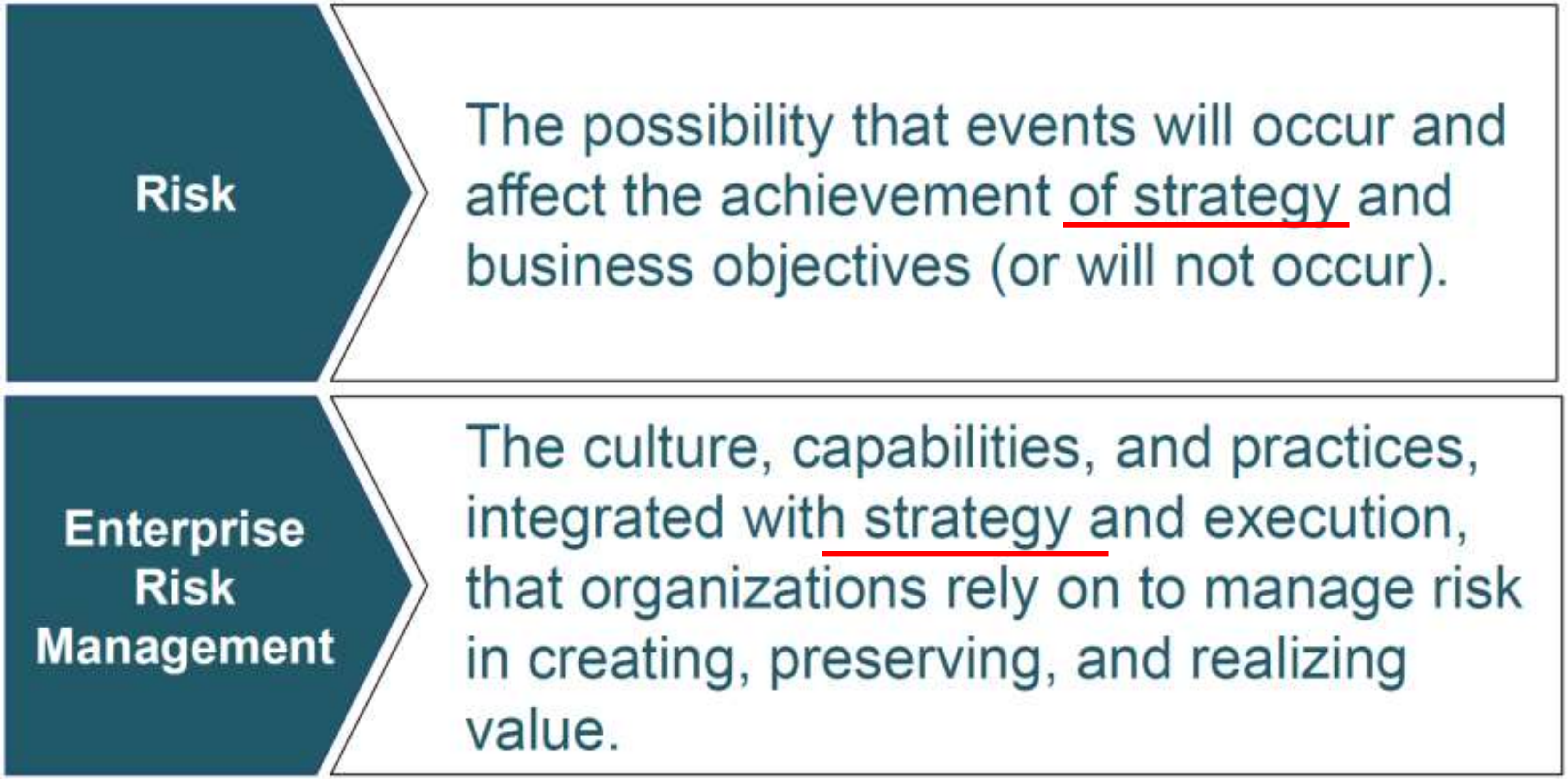
Risk

The possibility that events will occur and affect the achievement of strategy and business objectives (or will not occur).

Not every organization is aiming business-oriented objectives (public sector organizations, social institutions). As a matter of fact, business objectives are only applied to profit-oriented organizations.

Some Challenges with COSO ERM

- Prerequisite to effectiveness



Risk

The possibility that events will occur and affect the achievement of strategy and business objectives (or will not occur).

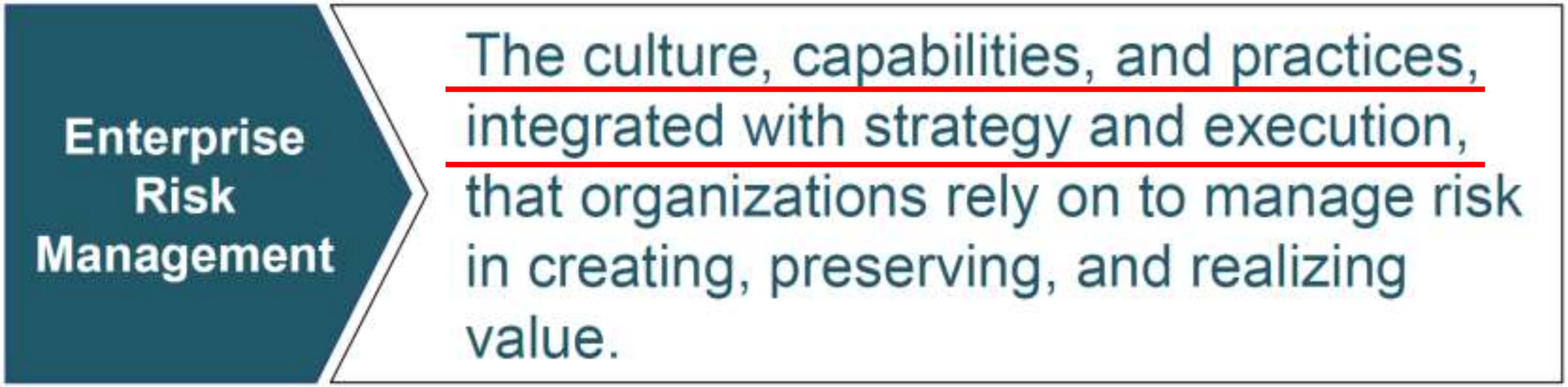
Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value.

Not every organization has been matured enough and has a well-defined strategy in place. Moreover, there is a risk of defining a wrong strategy (which is acknowledged by COSO ERM).

Some Challenges with COSO ERM

- Prerequisite to effectiveness



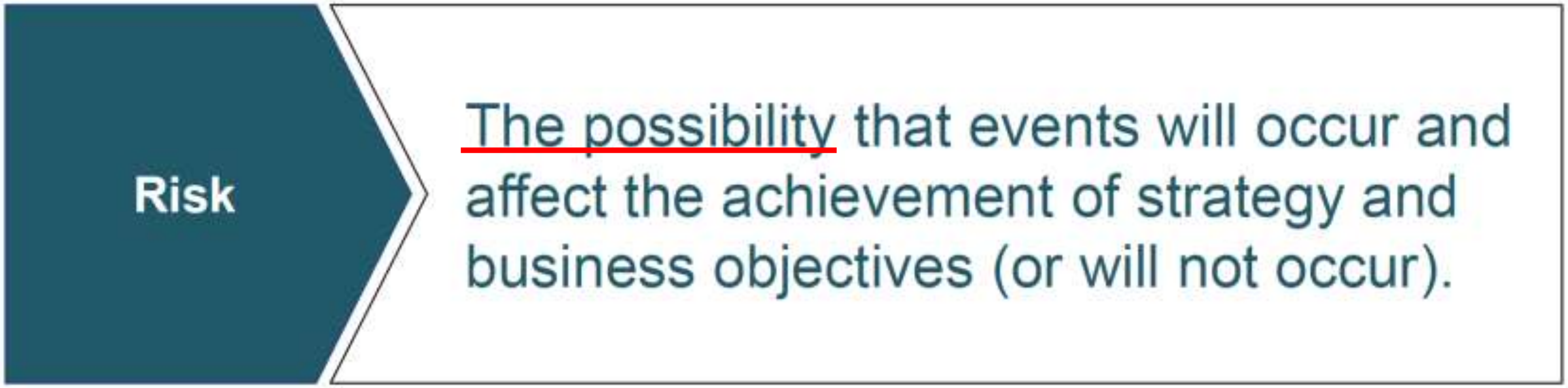
Enterprise Risk Management

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value.

Having a sound risk management culture, and necessary capabilities to manage risk, integrated with strategy and execution will surely increase the effectiveness of risk management practices. It may not be a problem for (or to apply to) a mature organization with adequate resources, but it will in the context of organizations which don’t have such privilege.

Some Challenges with COSO ERM

- Practicing the definition



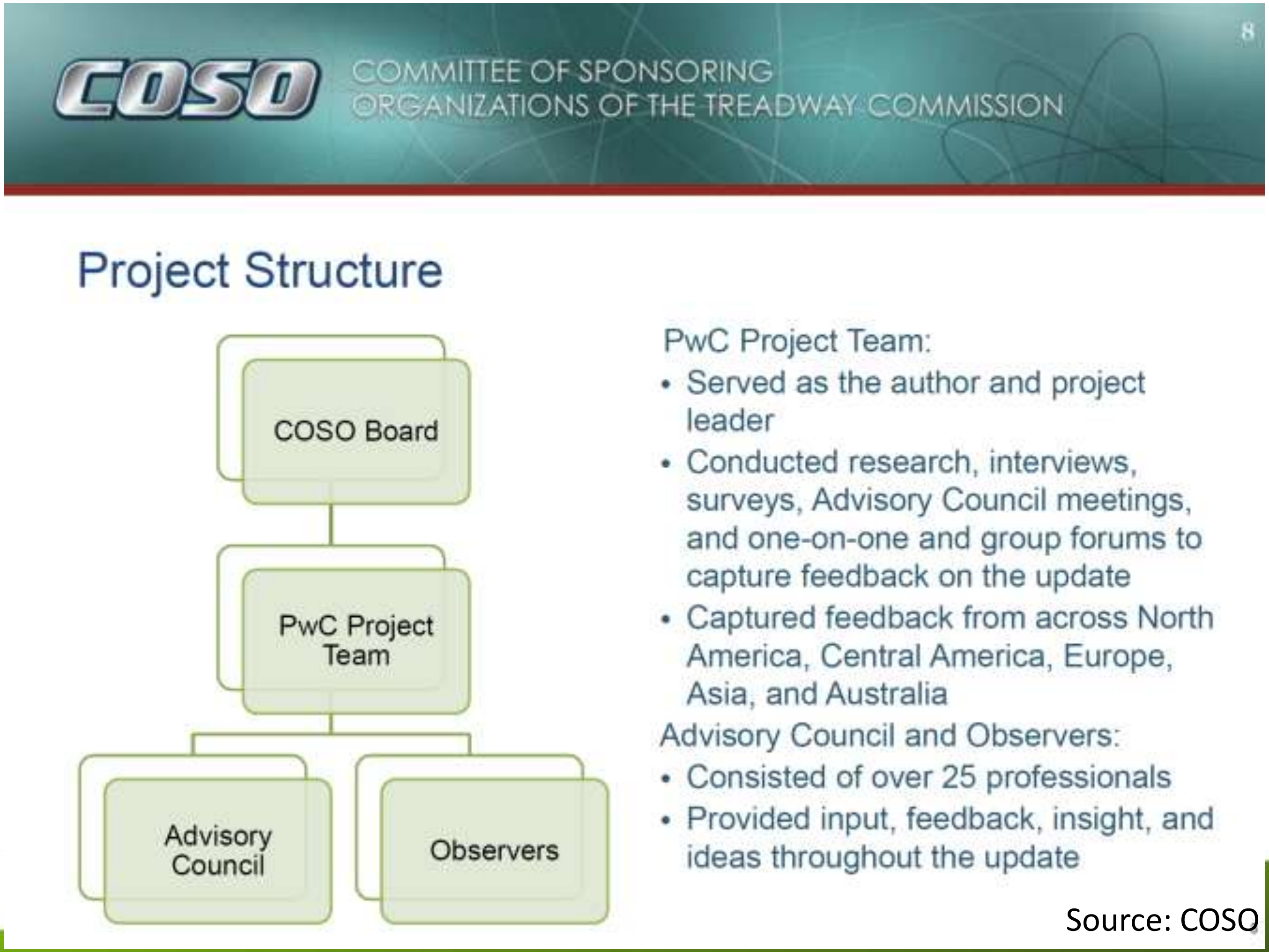
Risk

The possibility that events will occur and affect the achievement of strategy and business objectives (or will not occur).

Managing the risk, or by definition, managing “the possibility that events will occur and affect the achievement of …” might mislead the risk management to focusing only on the preventive actions, whilst in the real life a good risk management even might encourage us in taking more risks, in term of exploiting the opportunity.

Some Challenges with COSO ERM

- Comments from independent parties



8

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Project Structure

COSO Board

PwC Project Team

Advisory Council

Observers

PwC Project Team:

- Served as the author and project leader
- Conducted research, interviews, surveys, Advisory Council meetings, and one-on-one and group forums to capture feedback on the update
- Captured feedback from across North America, Central America, Europe, Asia, and Australia

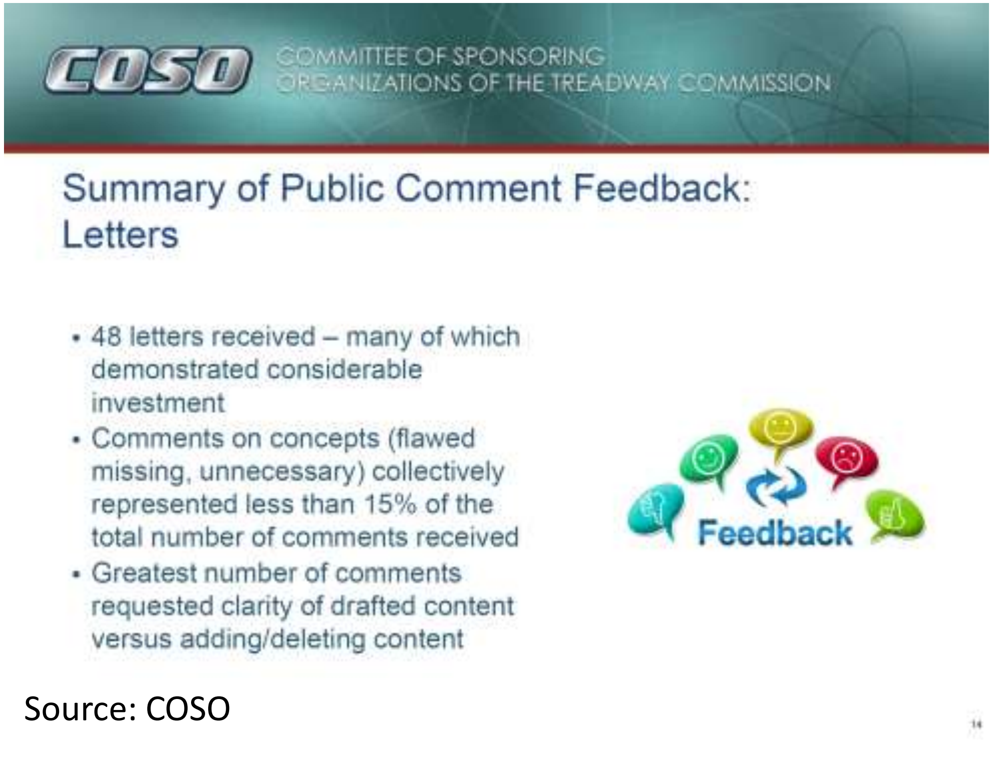
Advisory Council and Observers:

- Consisted of over 25 professionals
- Provided input, feedback, insight, and ideas throughout the update

Source: COSO

Some Challenges with COSO ERM

- Comments from independent parties



COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Summary of Public Comment Feedback: Letters

- 48 letters received – many of which demonstrated considerable investment
- Comments on concepts (flawed missing, unnecessary) collectively represented less than 15% of the total number of comments received
- Greatest number of comments requested clarity of drafted content versus adding/deleting content

14

Source: COSO

IFAC International Federation of Accountants®

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.ifac.org

September 30, 2016

Robert Hirth
Chairman
Committee of Sponsoring Organizations of the
Via upload link

Re: Comments on *Enterprise Risk Managem*

Dear Mr. Hirth,

Within organizations across the globe, many pr
strategic or functional leadership, or are otherw
implementation, execution, evaluation, and imp
arrangements. In addition, many professional a
objective, accurate, and timely information and
the Professional Accountants in Business (PAI
Accountants (IFAC) values the opportunity to c
the Treadway Commission (COSO)'s Exposure
Integrated Framework ("ERM Framework").

With the increased volatility in the modern busi
crises around the world, the effective managem
control—has taken on even greater importance
an organization's objectives, while complying w
enables the organization to better respond and
commends COSO on taking up the challenge t

IFAC also greatly values COSO's invitation to p
allowed us to actively contribute to all stages of
views on the effective management of risk are
Summary stating that "integrating enterprise ris
growth and enhance performance by more clos
opportunity." This is closely aligned with IFAC's
argues that organizations should primarily focu
sustainable value and growth and that managin
part of that.

IFAC also supports many of the other intention
Executive Summary. For example, it supports t

- Organizations need to become more a
  opportunities and threats;

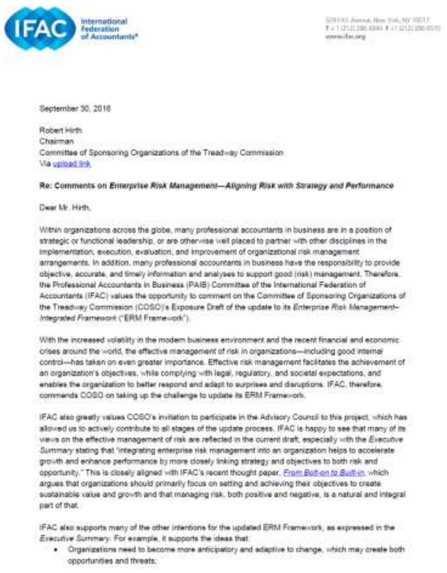
A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000

airmic alarm irm

Source: IFAC, AIRMIC, ALARM, IRM

Some Challenges with COSO ERM

- Comments from independent parties



International Federation of Accountants®

529 Fifth Avenue, New York, NY 10017
T +1 (212) 286-9344 F +1 (212) 286-9570
www.ifac.org

September 30, 2016

Robert Hirth
Chairman
Committee of Sponsoring Organizations of the Treadway Commission
Via upload link

Re: Comments on *Enterprise Risk Management—Aligning Risk with Strategy and Performance*

Dear Mr. Hirth,

Within organizations across the globe, many professional accountants in business are in a position of strategic or functional leadership, or are otherwise well placed to partner with other disciplines in the implementation, execution, evaluation, and improvement of organizational risk management arrangements. In addition, many professional accountants in business have the responsibility to provide objective, accurate, and timely information and analyses to support good (risk) management. Therefore, the Professional Accountants in Business (PAIB) Committee of the International Federation of Accountants (IFAC) values the opportunity to comment on the Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s Exposure Draft of the update to its *Enterprise Risk Management–Integrated Framework* ("ERM Framework").

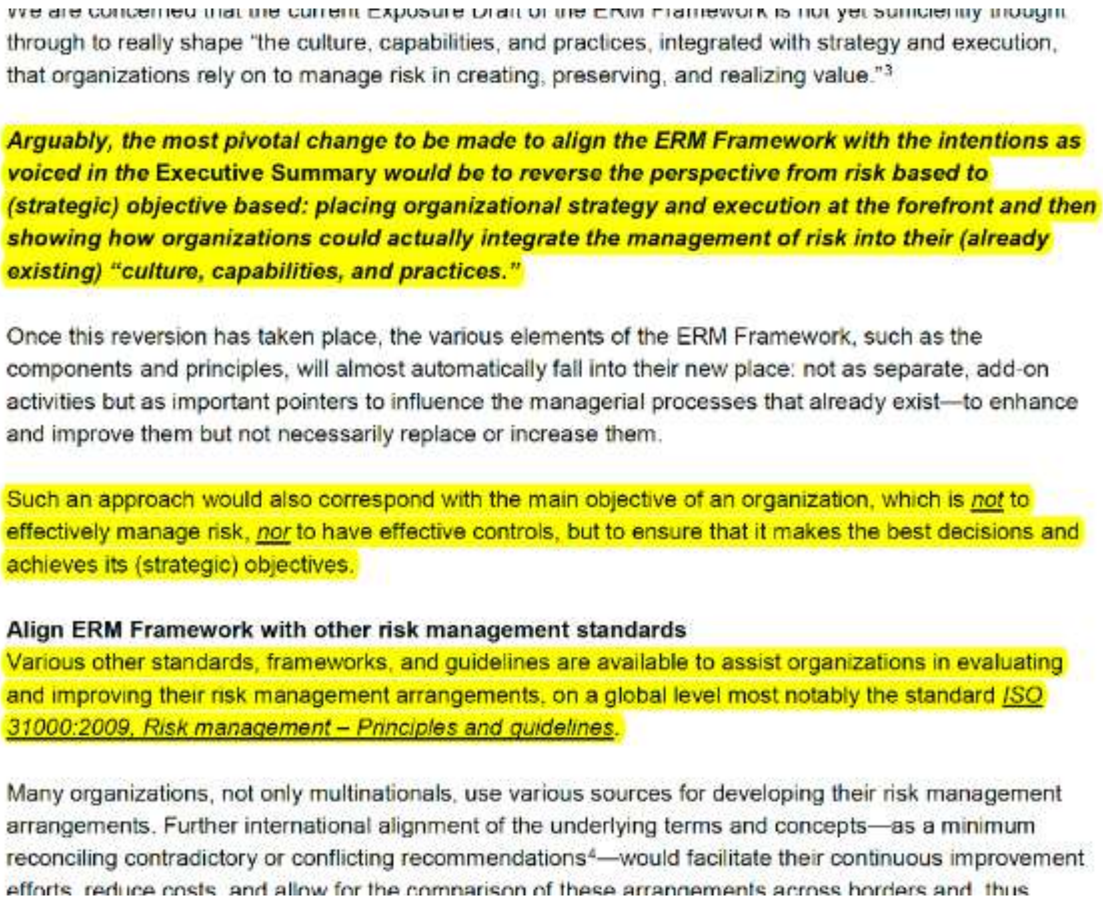
With the increased volatility in the modern business environment and the recent financial and economic crises around the world, the effective management of risk in organizations—including good internal control—has taken on even greater importance. Effective risk management facilitates the achievement of an organization's objectives, while complying with legal, regulatory, and societal expectations, and enables the organization to better respond and adapt to surprises and disruptions. IFAC, therefore, commends COSO on taking up the challenge to update its ERM Framework.

IFAC also greatly values COSO's invitation to participate in the Advisory Council to this project, which has allowed us to actively contribute to all stages of the update process. IFAC is happy to see that many of its views on the effective management of risk are reflected in the current draft, especially with the *Executive Summary* stating that "integrating enterprise risk management into an organization helps to accelerate growth and enhance performance by more closely linking strategy and objectives to both risk and opportunity." This is closely aligned with IFAC's recent thought paper, From Bolt-on to Built-in, which argues that organizations should primarily focus on setting and achieving their objectives to create sustainable value and growth and that managing risk, both positive and negative, is a natural and integral part of that.

IFAC also supports many of the other intentions for the updated ERM Framework, as expressed in the *Executive Summary*. For example, it supports the ideas that:

- Organizations need to become more anticipatory and adaptive to change, which may create both opportunities and threats;

Source: IFAC



We are concerned that the current Exposure Draft of the ERM Framework is not yet sufficiently thought through to really shape "the culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value."[3]

Arguably, the most pivotal change to be made to align the ERM Framework with the intentions as voiced in the Executive Summary would be to reverse the perspective from risk based to (strategic) objective based: placing organizational strategy and execution at the forefront and then showing how organizations could actually integrate the management of risk into their (already existing) "culture, capabilities, and practices."

Once this reversion has taken place, the various elements of the ERM Framework, such as the components and principles, will almost automatically fall into their new place: not as separate, add-on activities but as important pointers to influence the managerial processes that already exist—to enhance and improve them but not necessarily replace or increase them.

Such an approach would also correspond with the main objective of an organization, which is *not* to effectively manage risk, *nor* to have effective controls, but to ensure that it makes the best decisions and achieves its (strategic) objectives.

Align ERM Framework with other risk management standards

Various other standards, frameworks, and guidelines are available to assist organizations in evaluating and improving their risk management arrangements, on a global level most notably the standard *ISO 31000:2009, Risk management – Principles and guidelines*.

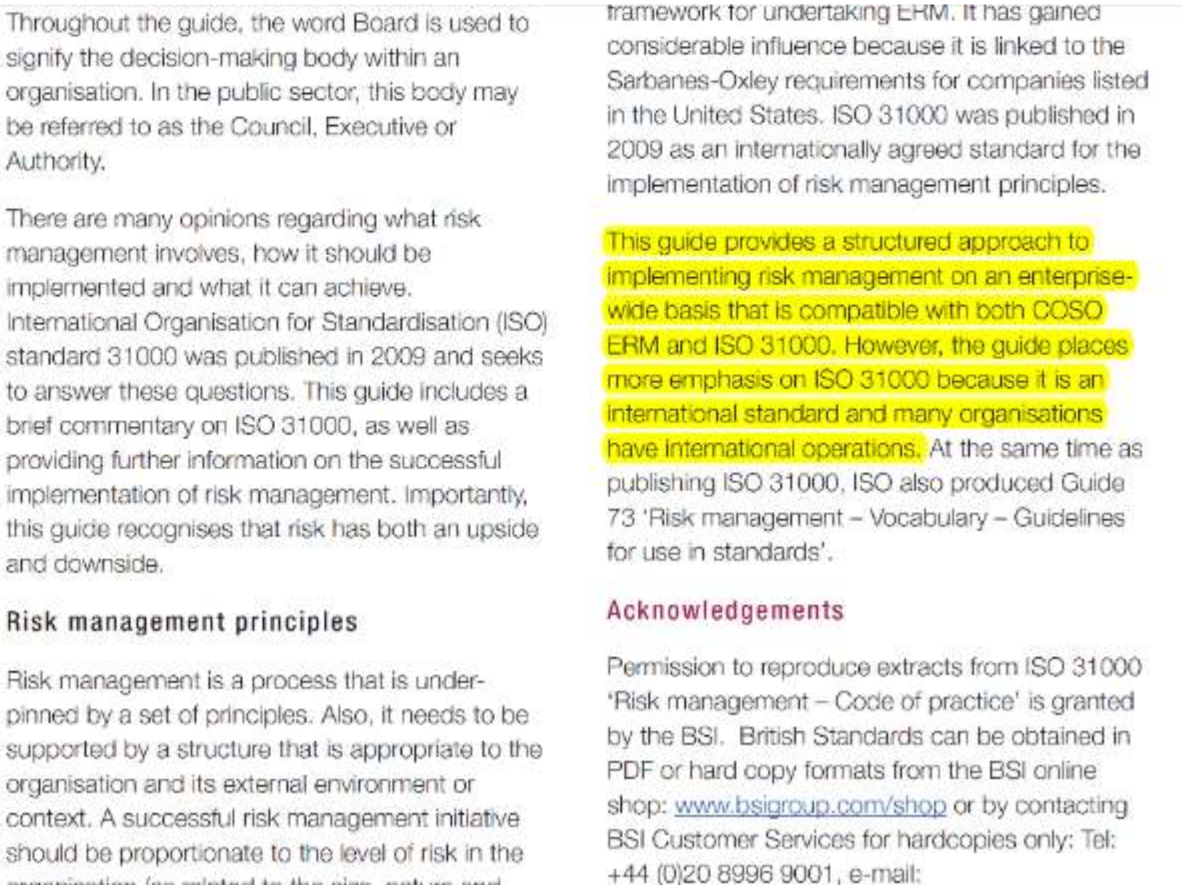
Many organizations, not only multinationals, use various sources for developing their risk management arrangements. Further international alignment of the underlying terms and concepts—as a minimum reconciling contradictory or conflicting recommendations[4]—would facilitate their continuous improvement efforts, reduce costs, and allow for the comparison of these arrangements across borders and, thus

Some Challenges with COSO ERM

- Comments from independent parties

airmic
alarm
irm
A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000
airmic
alarm
irm

Source: AIRMIC, ALARM, IRM



Throughout the guide, the word Board is used to signify the decision-making body within an organisation. In the public sector, this body may be referred to as the Council, Executive or Authority.

There are many opinions regarding what risk management involves, how it should be implemented and what it can achieve. International Organisation for Standardisation (ISO) standard 31000 was published in 2009 and seeks to answer these questions. This guide includes a brief commentary on ISO 31000, as well as providing further information on the successful implementation of risk management. Importantly, this guide recognises that risk has both an upside and downside.

Risk management principles

Risk management is a process that is underpinned by a set of principles. Also, it needs to be supported by a structure that is appropriate to the organisation and its external environment or context. A successful risk management initiative should be proportionate to the level of risk in the organisation (as related to the size, nature and

framework for undertaking ERM. It has gained considerable influence because it is linked to the Sarbanes-Oxley requirements for companies listed in the United States. ISO 31000 was published in 2009 as an internationally agreed standard for the implementation of risk management principles.

This guide provides a structured approach to implementing risk management on an enterprise-wide basis that is compatible with both COSO ERM and ISO 31000. However, the guide places more emphasis on ISO 31000 because it is an international standard and many organisations have international operations. At the same time as publishing ISO 31000, ISO also produced Guide 73 'Risk management – Vocabulary – Guidelines for use in standards'.

Acknowledgements

Permission to reproduce extracts from ISO 31000 'Risk management – Code of practice' is granted by the BSI. British Standards can be obtained in PDF or hard copy formats from the BSI online shop: www.bsigroup.com/shop or by contacting BSI Customer Services for hardcopies only: Tel: +44 (0)20 8996 9001, e-mail:

Some Considerations in Choosing ISO 31000 over COSO ERM

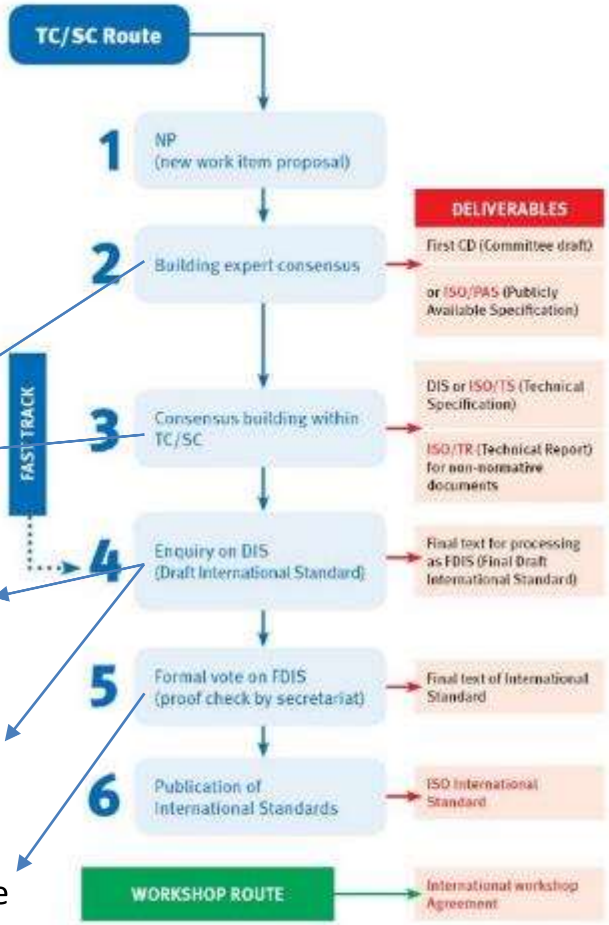
- Standard development process

ISO/TC 262 has 54 Participating Countries and 17 Observing Counties as well as numerous liaisons. BSI in the United Kingdom is responsible for the secretariat.

The Draft International Standard (DIS) is submitted to ISO Central Secretariat by the committee secretary. It is then circulated to all ISO members who then have 12 weeks to vote and comment on it. (The submission interface should be used to submit the draft).

The DIS is approved if a two-thirds of the P-members of the TC/SC are in favor and not more than one-quarter of the total number of votes cast are negative

If the DIS is approved and no technical changes are introduced in the draft, the project goes straight to publication. However, if technical changes are introduced, FDIS stage is mandatory.

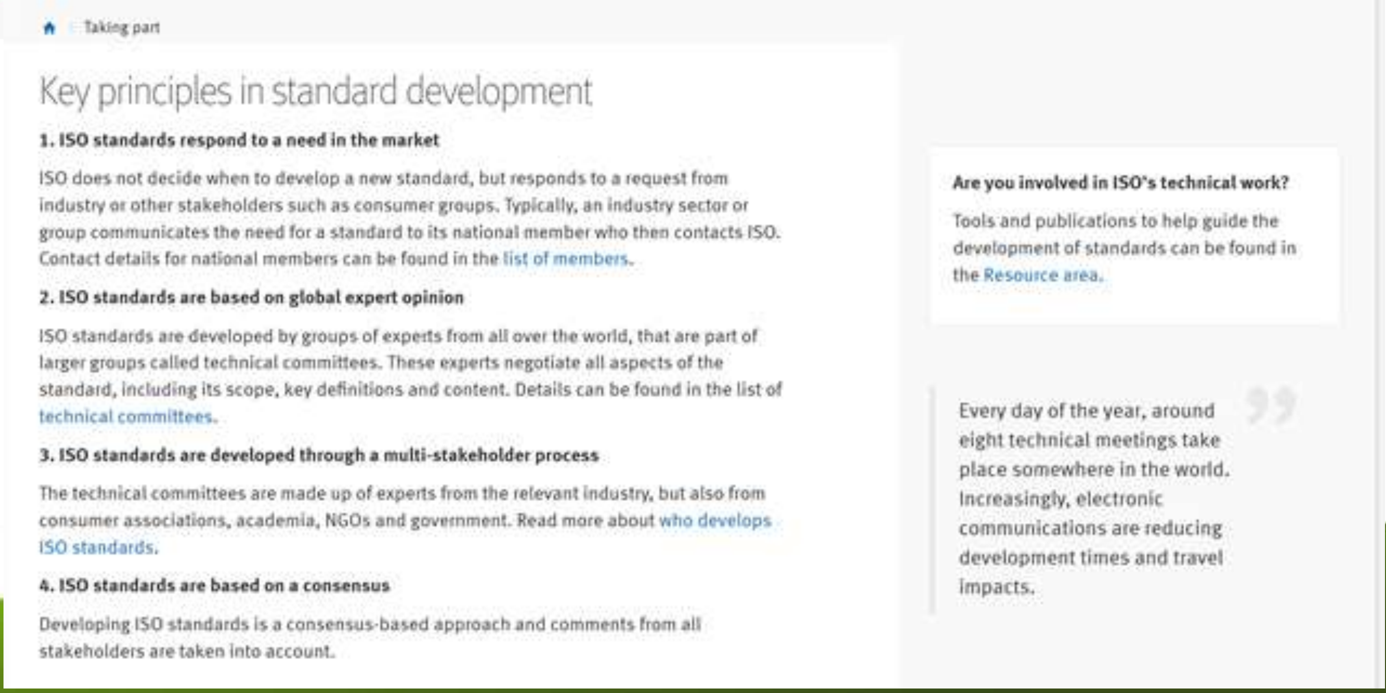


TC/SC Route
FAST TRACK
1 NP (new work item proposal)
2 Building expert consensus
3 Consensus building within TC/SC
4 Enquiry on DIS (Draft International Standard)
5 Formal vote on FDIS (proof check by secretariat)
6 Publication of International Standards
WORKSHOP ROUTE
DELIVERABLES
First CD (Committee draft)
or ISO/PAS (Publicly Available Specification)
DIS or ISO/TS (Technical Specification)
ISO/TR (Technical Report) for non-normative documents
Final text for processing as FDIS (Final Draft International Standard)
Final text of International Standard
ISO International Standard
International workshop Agreement

Source: ISO, TC 262

Some Considerations in Choosing ISO 31000 over COSO ERM

- Standard development process



Key principles in standard development

1. ISO standards respond to a need in the market

ISO does not decide when to develop a new standard, but responds to a request from industry or other stakeholders such as consumer groups. Typically, an industry sector or group communicates the need for a standard to its national member who then contacts ISO. Contact details for national members can be found in the list of members.

2. ISO standards are based on global expert opinion

ISO standards are developed by groups of experts from all over the world, that are part of larger groups called technical committees. These experts negotiate all aspects of the standard, including its scope, key definitions and content. Details can be found in the list of technical committees.

3. ISO standards are developed through a multi-stakeholder process

The technical committees are made up of experts from the relevant industry, but also from consumer associations, academia, NGOs and government. Read more about who develops ISO standards.

4. ISO standards are based on a consensus

Developing ISO standards is a consensus-based approach and comments from all stakeholders are taken into account.

Are you involved in ISO's technical work?

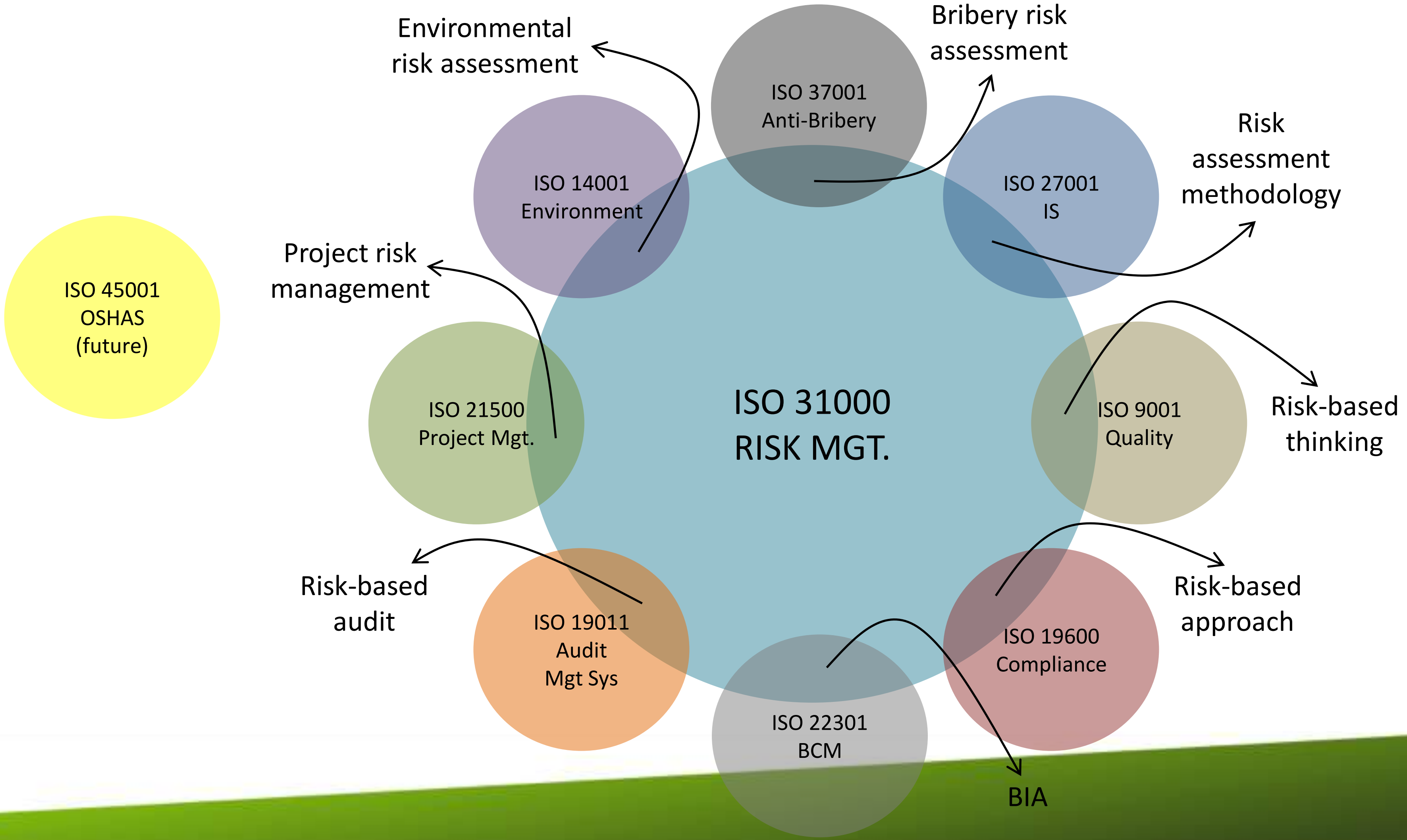
Tools and publications to help guide the development of standards can be found in the Resource area.

> Every day of the year, around eight technical meetings take place somewhere in the world. Increasingly, electronic communications are reducing development times and travel impacts.

Source: ISO

Some Considerations in Choosing ISO 31000 over COSO ERM

- Integration with other ISO standards

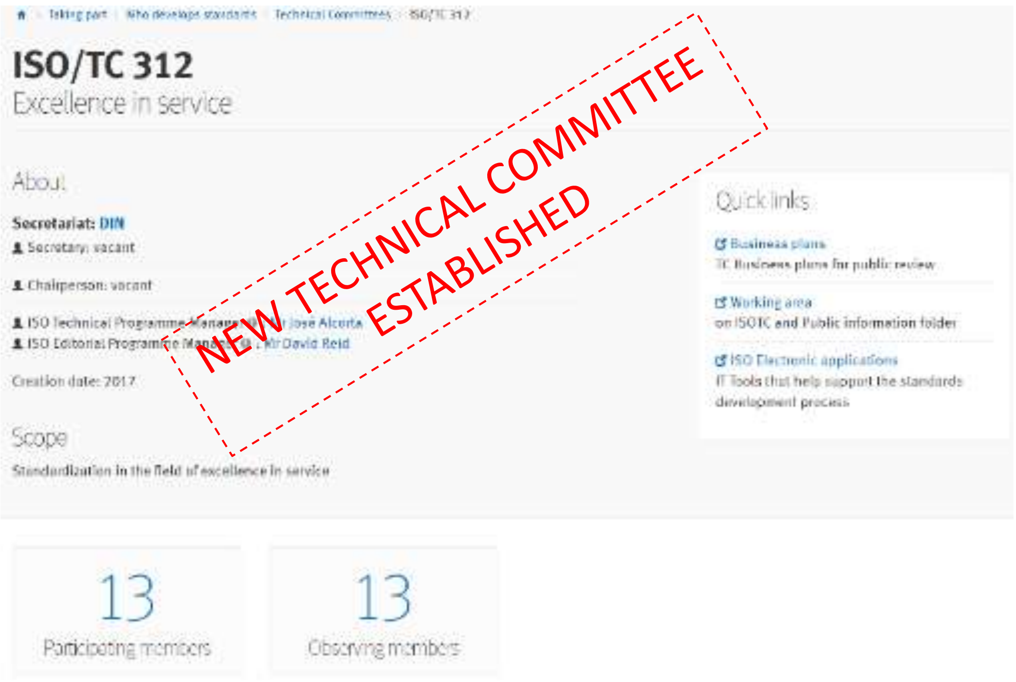


Some Considerations in Choosing ISO 31000 over COSO ERM

- Integration with other ISO standards, and supports Malcolm Baldrige criteria (KPKU)

petunjuk penyusunan laporan implementasi **Kriteria Penilaian Kinerja Unggul (KPKU)** pada Badan Usaha Milik Negara

Kementerian Badan Usaha Milik Negara
JL Medan Merdeka Selatan No. 13 Jakarta Pusat 10110



Taking part | Who develops standards | Technical Committees | ISO/TC 312

ISO/TC 312
Excellence in service

About

Secretariat: DIN
Secretary: vacant

Chairperson: vacant

ISO Technical Programme Manager[TPM] : Mr José Alcorta
ISO Editorial Programme Manager[EM] : Mr David Reid

Creation date: 2017

Scope

Standardization in the field of excellence in service

Quick links

Business plans
TC Business plans for public review

Working area
on ISOTC and Public information folder

ISO Electronic applications
IT Tools that help support the standards development process

13
Participating members

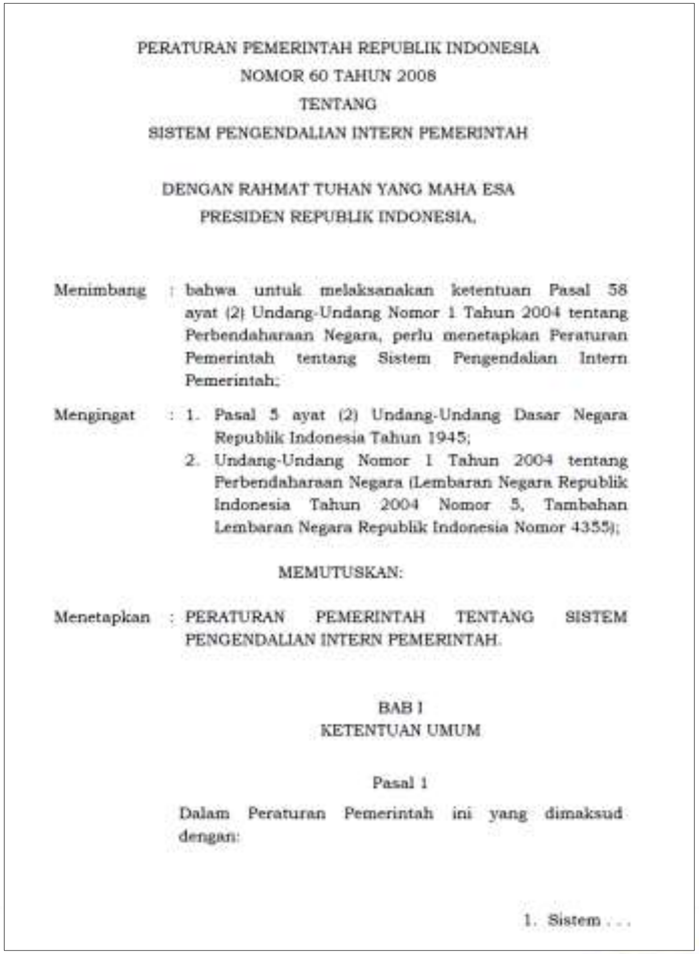
13
Observing members

NEW TECHNICAL COMMITTEE ESTABLISHED

Source: KBUMN

Some Considerations in Choosing ISO 31000 over COSO ERM

- Compatible with and supports SPIP



PERATURAN PEMERINTAH REPUBLIK INDONESIA
NOMOR 60 TAHUN 2008
TENTANG
SISTEM PENGENDALIAN INTERN PEMERINTAH

DENGAN RAHMAT TUHAN YANG MAHA ESA
PRESIDEN REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 58 ayat (2) Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara, perlu menetapkan Peraturan Pemerintah tentang Sistem Pengendalian Intern Pemerintah;

Mengingat : 1. Pasal 5 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 5, Tambahan Lembaran Negara Republik Indonesia Nomor 4355);

MEMUTUSKAN:

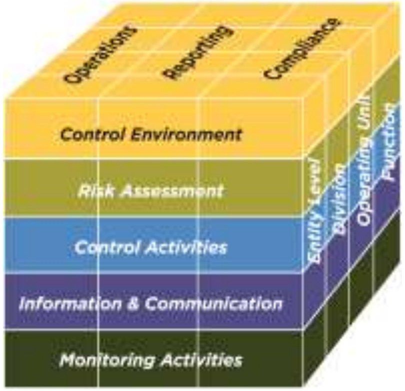
Menetapkan : PERATURAN PEMERINTAH TENTANG SISTEM PENGENDALIAN INTERN PEMERINTAH.

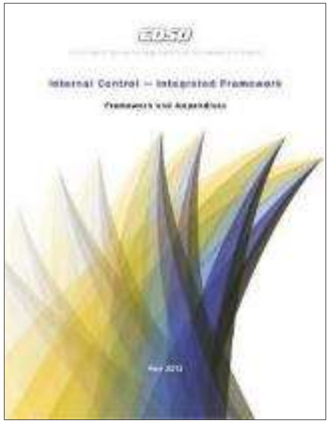
BAB I
KETENTUAN UMUM

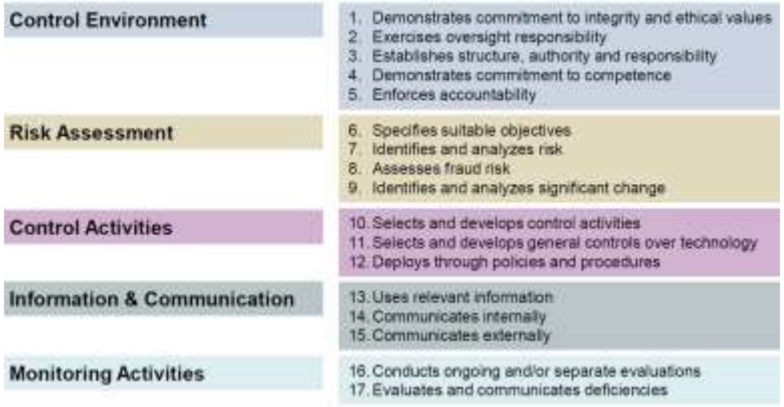
Pasal 1

Dalam Peraturan Pemerintah ini yang dimaksud dengan:

1. Sistem . . .





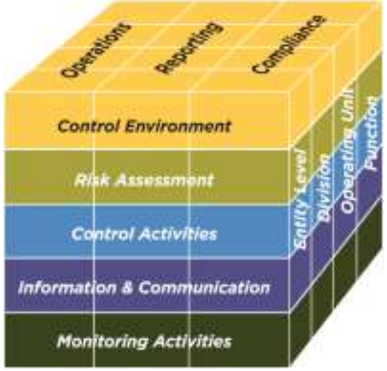


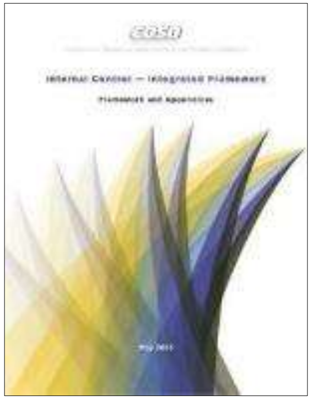
Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies 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

COSO Internal Control - Integrated Framework (ICIF)

Some Considerations in Choosing ISO 31000 over COSO ERM

- Compatible with and supports SPIP



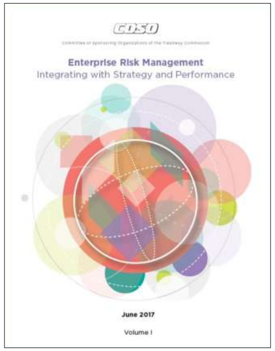

COSO

Internal Control — Integrated Framework

Framework and Appendices

May 2013

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


COSO

Enterprise Risk Management

Integrating with Strategy and Performance

June 2017

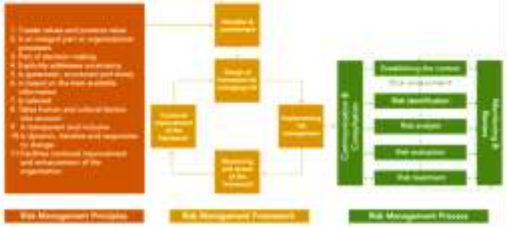
Volume I

≈

INTERNATIONAL STANDARD

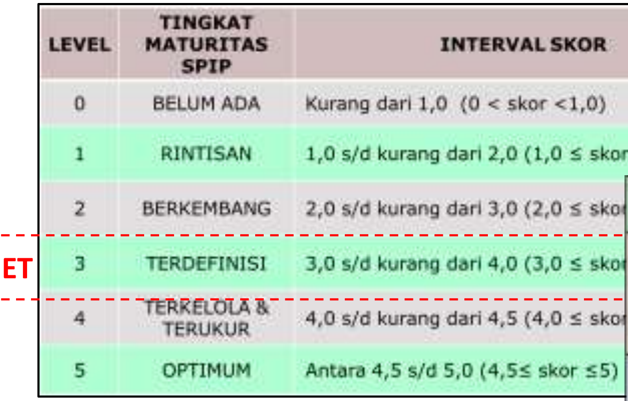
ISO 31000

Risk management — Principles and guidelines



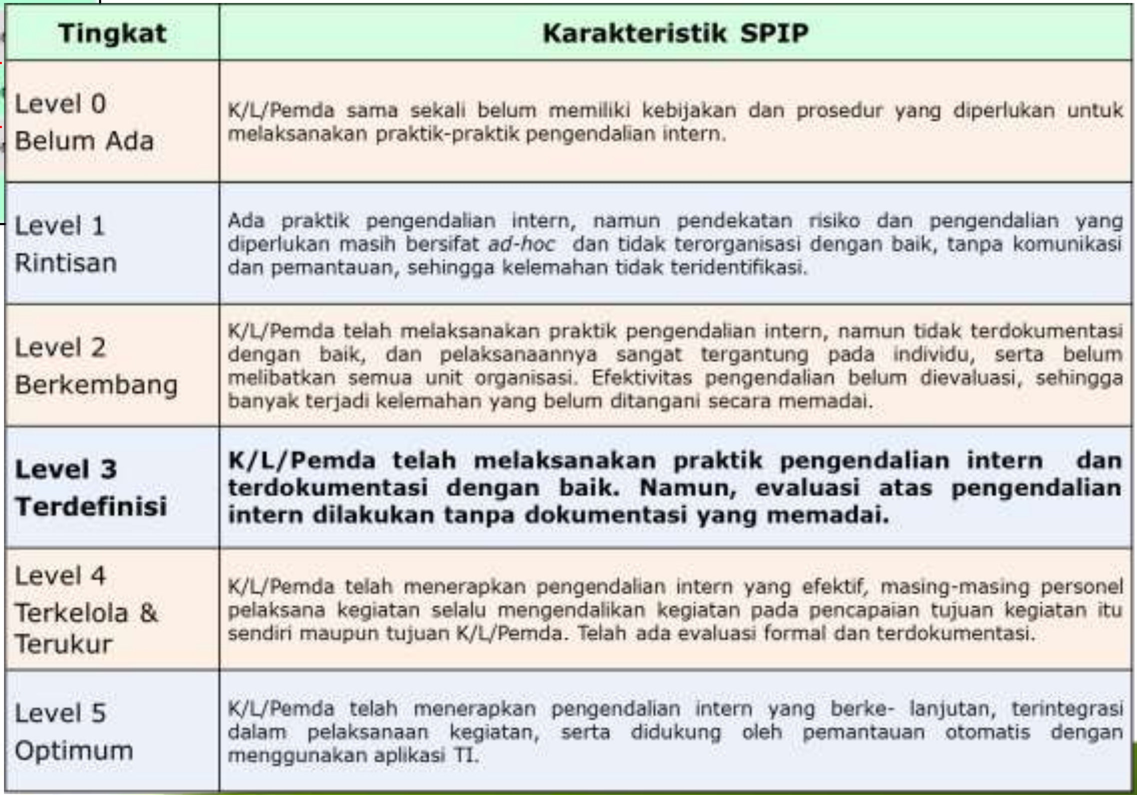
Some Considerations in Choosing ISO 31000 over COSO ERM

- Compatible with and supports SPIP



LEVEL	TINGKAT MATURITAS SPIP	INTERVAL SKOR
0	BELUM ADA	Kurang dari 1,0 (0 < skor <1,0)
1	RINTISAN	1,0 s/d kurang dari 2,0 (1,0 ≤ skor < 2,0)
2	BERKEMBANG	2,0 s/d kurang dari 3,0 (2,0 ≤ sko
3	TERDEFINISI	3,0 s/d kurang dari 4,0 (3,0 ≤ sko
4	TERKELOLA & TERUKUR	4,0 s/d kurang dari 4,5 (4,0 ≤ sko
5	OPTIMUM	Antara 4,5 s/d 5,0 (4,5≤ skor ≤5)

TARGET



Tingkat	Karakteristik SPIP
Level 0 Belum Ada	K/L/Pemda sama sekali belum memiliki kebijakan dan prosedur yang diperlukan untuk melaksanakan praktik-praktik pengendalian intern.
Level 1 Rintisan	Ada praktik pengendalian intern, namun pendekatan risiko dan pengendalian yang diperlukan masih bersifat *ad-hoc* dan tidak terorganisasi dengan baik, tanpa komunikasi dan pemantauan, sehingga kelemahan tidak teridentifikasi.
Level 2 Berkembang	K/L/Pemda telah melaksanakan praktik pengendalian intern, namun tidak terdokumentasi dengan baik, dan pelaksanaannya sangat tergantung pada individu, serta belum melibatkan semua unit organisasi. Efektivitas pengendalian belum dievaluasi, sehingga banyak terjadi kelemahan yang belum ditangani secara memadai.
Level 3 Terdefinisi	**K/L/Pemda telah melaksanakan praktik pengendalian intern dan terdokumentasi dengan baik. Namun, evaluasi atas pengendalian intern dilakukan tanpa dokumentasi yang memadai.**
Level 4 Terkelola & Terukur	K/L/Pemda telah menerapkan pengendalian intern yang efektif, masing-masing personel pelaksana kegiatan selalu mengendalikan kegiatan pada pencapaian tujuan kegiatan itu sendiri maupun tujuan K/L/Pemda. Telah ada evaluasi formal dan terdokumentasi.
Level 5 Optimum	K/L/Pemda telah menerapkan pengendalian intern yang berke- lanjutan, terintegrasi dalam pelaksanaan kegiatan, serta didukung oleh pemantauan otomatis dengan menggunakan aplikasi TI.

REPUBLIK INDONESIA

LAMPIRAN
PERATURAN PRESIDEN REPUBLIK INDONESIA
NOMOR 2 TAHUN 2015

TENTANG

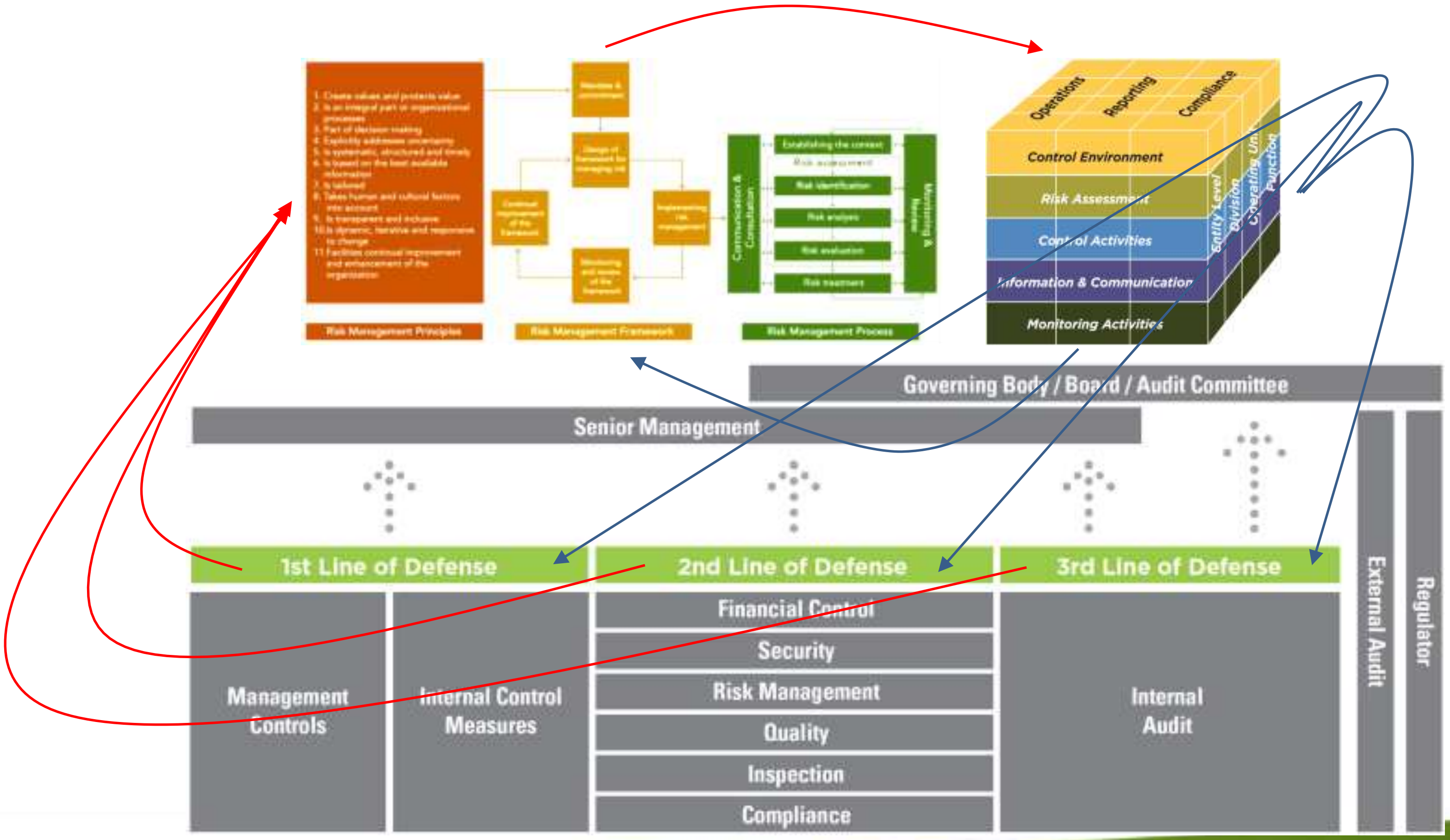
RENCANA PEMBANGUNAN
JANGKA MENENGAH NASIONAL
(RPJMN)
2015-2019

Indonesia yang Berdaulat, Mandiri dan Berkepribadian
Berlandaskan Gotong Royong

Buku II
Agenda Pembangunan Bidang

Some Considerations in Choosing ISO 31000 over COSO ERM

- Compatible with and supports SPIP


1. Create values and protects value
2. Is an integral part or organizational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Is systematic, structured and timely
6. Is based on the best available information
7. Is tailored
8. Takes human and cultural factors into account
9. Is transparent and inclusive
10. Is dynamic, iterative and responsive to change
11. Facilities continual improvement and enhancement of the organization
Mandate & commitment
Design of framework for managing risk
Continual improvement of the framework
Implementing risk management
Monitoring and review of the framework
Communication & Consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring & Review
Risk Management Principles
Risk Management Framework
Risk Management Process
Operations
Reporting
Compliance
Control Environment
Risk Assessment
Control Activities
Information & Communication
Monitoring Activities
Entity Level
Division
Operating Unit
Function
Governing Body / Board / Audit Committee
Senior Management
1st Line of Defense
2nd Line of Defense
3rd Line of Defense
Management Controls
Internal Control Measures
Financial Control
Security
Risk Management
Quality
Inspection
Compliance
Internal Audit
External Audit
Regulator

Some Considerations in Choosing ISO 31000 over COSO ERM

- Participations & supports the endorsement of SNI

INTERNATIONAL STANDARD

ISO 31000

First edition
2009-11-15

Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

ISO

Reference number
ISO 31000:2009(E)

© ISO 2009

SNI

Standar Nasional Indonesia

SNI ISO 31000:2011

Manajemen Risiko – Prinsip dan Pedoman

Risk management – Principles and guideline
(ISO 31000:2009, IDT)

ICS 03.100.01

Badan Standardisasi Nasional

BSN

CRMS INDONESIA
Center for Risk Management Studies

Thank You

"This document is intended only for recipients who are authorized to receive it. It may contains confidential and/ or legally privileged information belong to Center for Risk Management Studies Indonesia (CRMS Indonesia), therefore the authorized recipients shall protect this confidential information disclosed pursuant to provisions of CRMS Indonesia's policy. Please also be notified that any disclosure, copying, distribution or taking any action based on the contents of this document is prohibited and may be unlawful."