Clarifying the Confusion between COSO and ISO
Clarifying the Confusion between COSO and ISO
According to the Association of Certified Fraud Examiners, a typical organisation loses an estimated 5% of its annual revenues to fraud.
PwC Global Economic Crime Survey 2014 results

Incidence of the various types of economic crime

SA respondents reported more instances of procurement fraud, bribery & corruption, financial statement fraud and human resources fraud than their global counterparts.
Why COSO?

COSO’s structure and mission

- COSO is a joint initiative of five sponsoring organisations
  - American Accounting Association (AAA)
  - American Institute of Certified Public Accountants (AICPA)
  - Financial Executives International (FEI)
  - Institute of Management Accountants (IMA)
  - Institute of Internal Auditors (IIA)

COSO’s mission is...

“...to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.”

www.coso.org/aboutus.htm
COSO Internal Control-Integrated Framework

- First published in 1992
- Gained wide acceptance following financial control failures of early 2000’s
- Most widely used framework in the US
- Also widely used around the world

Original COSO Cube

Important update in 2013
The Updated Framework intends to reflect the major changes that have occurred in the economic environment, governance expectations, and associated risks since the original publication in 1992.

### Existing pre 2013:
- Internal Control – Integrated Framework, 1992
- Evaluation Tools, 1992
- Enterprise Risk Management, 2004
- Guidance for Smaller Public Companies, 2006

### New in 2013:
- Internal Control – Integrated Framework
- Evaluation Tools
- Compendium of Approaches and Examples of Internal Control over External Financial Reporting

### Other COSO Publications:
- Monitoring Guidance, 2009
- Embracing ERM, Practical Approaches for Getting Started, 2011
- ERM, Understanding and Communicating Risk Appetite, 2012
- Enhancing Board Oversight, Avoiding Judgment Traps and Biases, 2012
- ...
Context and Objectives for the COSO Update Project

Original Framework

  - Fundamental concepts relating to effective internal control
  - Changes in business, operating, and regulatory environments
  - Internal and non-financial reporting objectives

Enhancements to ease use and application

- Formalizes Principles Underlying Points of Focus
- Updates Context
- Expands Application

Updated Framework

What is Changing in COSO IC 2013?

**What is not changing...**

1. Core definition of internal control
2. Use of judgment remains important in designing, implementing, and conducting internal control, and in assessing effectiveness
3. Effective internal control requires five components

**What is changing...**

1. Expansion of the scope of reporting objectives beyond financial information
2. Governance (committee roles, alignment with business model...)
3. Succession planning and talent management for internal control
4. Articulation of 3 ‘lines of defense’ (operational management, support functions, internal audit)
5. Linkage between risk, performance, and reward
6. ‘Tone in the middle’ and across the entity
7. More explicit consideration of outsourced service providers and other third parties affecting internal control (adherence to code of conduct and expectations beyond reliability of financial reporting)
8. Adaptability and adequacy of the internal control system relative to changes in the business (processes, roles, structures, IT, scope of business...)

The Update formalises fundamental concepts embedded in the original Framework as 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
### Understanding the Framework

<table>
<thead>
<tr>
<th>5 Components consistent with the original Framework</th>
<th>17 Principles codifying what should be present and functioning</th>
<th>85 Points of Focus representing salient points for demonstrating the associated Principle</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Control Environment</td>
<td>1. The organization demonstrates a commitment to integrity and ethical values</td>
<td><strong>Sets the Tone at the Top</strong>—The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.</td>
</tr>
<tr>
<td>2. Risk Assessment</td>
<td>6. ...</td>
<td>...</td>
</tr>
<tr>
<td>3. Control Activities</td>
<td>10. ...</td>
<td>...</td>
</tr>
<tr>
<td>4. Information &amp; Communication</td>
<td>13. ...</td>
<td>...</td>
</tr>
<tr>
<td>5. Monitoring Activities</td>
<td>16. ...</td>
<td>81. ...</td>
</tr>
</tbody>
</table>
Does your entity’s system of internal control over financial reporting cover all 17 principles?

- Internal control programs often focus on the Control Activities component
- Are the other components present and functioning?
- To what extent are they operating together in an integrated manner?
Example of a flash diagnostic of the maturity of internal control in relation to the 17 principles of COSO 2013.
The COSO ERM standard delineates a principles-based framework

The framework provides:

• A definition of enterprise risk management

• The critical principles and components of an effective enterprise risk management process

• Direction for organisations to use in determining how to enhance their risk management

• Criteria to determine whether their risk management is effective, and if not, what is needed
The COSO ERM standard delineates a principles-based framework.

The Application Techniques framework provides:

- Illustrations of how critical principles may look within an organisation
- An overview of an implementation process
- Illustrations that consider varying entity:
  - Size
  - Strategy
  - Industry
  - Complexity
Three foundational aspects of the COSO ERM Framework

• Starts with objectives:
  ➢ strategic
  ➢ operations
  ➢ reporting
  ➢ compliance

• Applies to activities at all levels of the organisation

• Has eight interrelated components
Comparing COSO IC 2013 to COSO ERM 2004

Components
With the enhanced focus on risk, the ERM framework expands the internal control framework’s risk assessment, creating three components: event identification, risk assessment, and risk response.
Comparing COSO IC to COSO ERM

Enterprise risk management is broader than internal control, elaborating on internal control and focusing more directly on risk.

Internal control is an integral part of enterprise risk management, while enterprise risk management is part of the overall governance process.
Risk appetite & tolerance

The ERM framework introduced the concepts of risk appetite and tolerance.

Risk appetite is the broad-based amount of risk an entity is willing to accept in pursuit of its mission/vision.

Risk tolerance is the acceptable level of variation in performance relative to achievement of objectives. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.
Portfolio View

Enterprise risk management required considering composite risks from a portfolio perspective. This concept is not contemplated in the *Internal Control – Integrated Framework*, which focuses on achievement of objectives on an individual basis. Internal control does not require that the entity develop a portfolio view.
Why ISO?

- Link risk and performance and service delivery
- Link risk and objectives
- Cover all types of risks
- Cover all types of activity and sectors
- Input from all countries
- Input from all existing risk standards and guidelines
- Guideline for all existing standards
About ISO 31000
combinations of the probability of an event and its consequences...
Standards, Guidelines and Regulations
The need to move beyond a compliance & control risk management standard

- compliance
- regulations
- reporting
- Risk
- Controls
- audit
Why aren’t ERM Programs More Successful?

• Most ERM Programs are built on “Governance” or “Compliance” models
  • Value: “Did we do it? Good.”

• Measures are rarely in meaningful terms

• Not a KEY role in performance management, planning, budgeting and strategy formation

• Limited in scope and focus

• Not a “day-to-day” part of decision making

• Not based on or tied to a standard or tight framework
About ISO 31000

<table>
<thead>
<tr>
<th>Role</th>
<th>Risk Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineer</td>
<td>risk = hazard</td>
</tr>
<tr>
<td>Scenario</td>
<td>risk = event</td>
</tr>
<tr>
<td>Manager</td>
<td>risk = uncertainty on objectives</td>
</tr>
<tr>
<td>Health</td>
<td>risk = threat (purely negative)</td>
</tr>
<tr>
<td>Finance</td>
<td>risk = return</td>
</tr>
<tr>
<td>Public sector</td>
<td>risk = discontinuity of service</td>
</tr>
</tbody>
</table>

**Risk management =**

*Managing potential events?*
**Risk Management**

- **Risk Planning - future event scenarios**
  - Be they Upside (Focus on risks of GAINS)
    - (eg successful products or other investments)
  - Or Downside (Focus on risks of LOSSES)
    - (eg sabotage, fire, threat, threat quality, CAM & disaster recovery)
  - All represent both ways to control such risks & the locus of risk's impact, the risks themselves need to be more specifically expressed, as a threat in a setting.
  - Sources of energy may act at different points in the body in different ways e.g. mechanical energy from noise may cause deafness and also stress by other means.

- **Risk Assessment**
  - Key factors may be:
    - 'Level of uncertainty of size of risk & actual consequences' Probability of detection if risk starts to manifest itself
    - 'Prospect of corrective action mitigating risk at that stage'

- **Risk Controls**
  - Introduced for a health and safety hazard may transfer risk to other employees or members of the public e.g. furnace extraction. HSE treat this as risk transfer.
  - (Add to risks the ideas of Management - accurate internal control of risk and Mitigation - reducing the effects of the risk, usually by insurance)

- **Risk Communication**
  - Terms like risk, probability, reliability and uncertainty have different meanings in various sectors of industry and to the public many of whom treat them as synonymous. See HSE's Reducing Risks, Protecting People (R2P2) and HSG65. For more detail see: cr/01329 Social amplification of risk on risk communication.
  - cr/01339 Probabilistic Methods: Uses and abuses in structural integrity.
  - BS 6779-3:2000 Project management.

- **Uncertainty Management**

- **Definitions**

- **Acceptability of risks**
  - Independence
  - Professional from Risk Taking

- **Risk Stake Holders**
  - Risk Receiver
  - Benefit Receiver
  - Risk Taker / Imposers
  - Risk Stake Holders

- **Conflict over Risk Perception**
  - Reflecting different self Interest
  - Reflecting different perceptions of Justice
  - Reflecting different levels of Knowledge
The combination of governance, performance, decision-making and risk management has become the driving force for a global approach, structured methodology leading to risk management standardization.
Existing Risk Management Standards before ISO 31000

Australia/New Zealand
- AIRMIC/ALARMS/IRM 2002

UK
- ISO 31000:2009

USA
- COSO ERM 2004

International
- Proposed in 2004
The South African Bureau of Standards (SABS) is a South African statutory body that was established in terms of the Standards Act, 1945 (Act No. 24 of 1945).

ISO has 164 national members out of the 206 total countries in the world.
Objectives of ISO 31000 SCOPE

- **All organisation**: Any sector, any activity, any size
- **All risk**: Any type of risk, + or - consequences
- **Generic guidelines**: Harmonizes processus, not practices
- **Global reference**: Harmonize RM in existing and future standards
- **Global application**: Objectives, context, structure, operations, processes, functions, projects, products, services, or assets
About ISO 31000

Internationally-recognised reference

- International consensus
- Single global reference for stakeholders
- Wide application
- “Umbrella” for more than 60 standards

- ISO 31000 adopted in South Africa
ISO 31000 standard recognized as national risk management standard, worldwide

Argentina, Australia, Austria, Belarus, Bulgaria, Brazil, Canada, Chile, China, Czech Republic, Denmark, Estonia, Finland, France, Germany, India, Ireland, Israel, Italy, Japan, Latvia, Malaysia, Netherlands, New-Zealand, Norway, Poland, Portugal, Romania, Russia, Singapore, Slovak Republic, Slovenia, South-Africa, Spain, Sweden, Switzerland, Thailand, Turkey, United Kingdom, Uruguay, United States
Link between risk and objectives

Effect of uncertainty on objectives...
A compliance & control risk management standard

The need to move beyond a compliance & control risk management standard

compliance

regulations

reporting

Risk

Controls

audit
ISO 31000, a global risk management standard

**Uncertainty**

**Performance**

**Objectives**

**Risk**

**Decision-making**

**Best allocation of resources**

Philosophy of the ISO 31000 risk management standard

- Uncertainty
- Performance
- Objectives
- Risk
- Decision-making
- Best allocation of resources
- Philosophy of the ISO 31000 risk management standard
The three pillars of ISO 31000

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization

Principles for managing risk (Clause 3)

Principles

Framework

Framework for managing risk (Clause 4)

Design of framework for managing risk (4.3)

Mandate and commitment (4.2)

Implementing risk management (4.4)

Continual improvement of the framework (4.6)

Monitoring and review of the framework (4.5)

Risk assessment (5.4)

Risk analysis (5.4.3)

Risk evaluation (5.4.4)

Risk treatment (5.5)

Establishing the context (4.2)

Communication and consultation (6.2)

Monitoring and review (5.6)

Process for managing risk (Clause 5)
Objectives of ISO 31000

**Objectives**

- a) Creates value
- b) Integral part of organizational processes
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and cultural factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

**Structure**

1. **Mandate and Commitment**
2. **Design of Framework for Managing Risk**
3. **Implementing Risk Management**
4. **Continual Improvement and Review**
5. **Continual Improvement**
Objectives of ISO 31000

**STRUCTURE**

1. **Establish the Context**
2. **Risk Identification**
3. **Risk Analysis**
4. **Risk Evaluation**
5. **Risk Treatment**
6. **Communication and Consultation**
7. **Monitoring and Review**

**RISK MANAGEMENT PROCESS**

**ISO GUIDE 73**

**RISK MANAGEMENT VOCABULARY**
Comparable Standards
Essentially identical risk management processes in the two standards

ISO 31000

COSO ERM 2004

Source: Aon Risk Solutions, White Paper on Risk Management Committee, 2011
The Department of Water and Sanitation is implementing risk-based and incentive-based form of regulation.

It regulates 142 municipalities (Water Services Authorities) on risk management issues following the ISO 31000 standard following the Risk Management Framework (from National Treasury).

The objective is to make sure that municipalities identify and manage their risks properly in order ensure the sustainability of the water services business.”

6th August 2014

Solly Selowa
Department of Water Affairs
Republic of South Africa
Email: selowas@dwa.gov.za
Best Public Sector Organization

G31000 Global Awards 2014

- Deployment of ERM in all departments
- WCG ISO 31000 Maturity Tool Capability
- Training of 11 members of the ERM staff
- Training of 7 approved CT31000 trainers
- First female Certified ISO31000 Lead Trainer in Africa - Sanobia Abrahams
- Further deployment at municipalities 2014/2015
USEFUL LINKS

• ISO 31000 GLOBAL SURVEY 2011:

• ISO 31000 INTERNATIONAL CONFERENCE:

• LINKEDIN GROUP on ISO 31000:
  http://www.linkedin.com/groups?mostPopular=&gid=1834592

• About ISO 31000 – official link:
  http://www.iso.org/iso/catalogue_detail?csnumber=43170
Annexes

- Exploring the role of internal audit in respect of ISO 31000
- ARP 070:2009 – Risk Management – Vocabulary
- Statistics of growth per country in the world
- Statistics of growth per country in Africa
Exploring the role of internal audit in respect of ISO 31000
South African Risk Management Standard
SANS 31000:2009– Risk Management – Principles and guidelines

NATIONAL FOREWORD:
This South African standard was approved by National Committee SABS TC 178, Risk management, in accordance with procedures of the SABS Standards Division, in compliance with annex 3 of the WTO/TBT agreement. This SANS document was published in December 2009.

PREVIEW:
http://www.store.sabs.co.za/getsabspdf.php?hash=56cc0611d0506b53d466f0c2be56fd8bf2c0ba55&preview=yes

PURCHASE:
SANS 31000 – 11 December 2009 - R353 (PDF copy SABS)
http://www.store.sabs.co.za/sans-31000-2009-ed-1-00-223995

ISBN 978-0-626-23641-0
NATIONAL FOREWORD:
This South African standard was approved by National Committee SABS TC 178, Risk management, in accordance with procedures of the SABS Standards Division, in compliance with annex 3 of the WTO/TBT agreement. This SANS document was published in December 2009.

PREVIEW:
http://www.store.sabs.co.za/getsabspdf.php?hash=d98eb58459c5352f34d621bc1e8019f51907baf4&preview=yes

PURCHASE:
SANS 31010 – January 2010 - R517 (PDF copy SABS)
http://www.store.sabs.co.za/sans-31010-2010-ed-1-00

ISBN 978-0-626-23645-8
NATIONAL FOREWORD:
This recommended practice was approved by National Committee SABS TC 178, Risk management, in accordance with procedures of the SABS Standards Division, in compliance with annex 3 of the WTO/TBT agreement.
This document was published in December 2009.
This document supersedes ARP 070:2007 (edition 1).

PREVIEW:
http://www.store.sabs.co.za/getsabspdf.php?hash=fedc21845769ae787af353314f5e366bd06efa58&preview=yes

PURCHASE:
ARP 070:2009 (ed. 2) – December 2009 - R285 (PDF copy SABS)
