Comments from US ISO TAG
US ISO TAG

• International Standards Organization Technical Advisory Group for the United States
• Chair – Dorothy Gjerdrum, ARM-P
  Executive Director, Public Entity & Scholastic Division
  Arthur J. Gallagher Risk Management Services
• Vice Chair – Wayne Salen
  Risk Manager, Labor Finders, Int’l & RIMS
ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards.

Established in 1947, ISO is a network of the national standards institutes of 159 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.
Risk management — Principles and guidelines

Management du risque — Principes et lignes directrices

GUIDE 73

Risk management — Vocabulary

Gestion des risques — Terminologie
ISO 31000, Guide 73 and ISO 31010

- Published in November, 2009
- Four years+ and seven work group meetings
- Participation by 28 countries and 100’s of practitioners and experts
- AUS/NZ 4360 was the genesis
- Proposed to ISO by Australia, New Zealand and Japan
Evolution of the US TAG

• ANSI sought support early in process – no qualified organization (SDO) stepped up until 2008
• ASSE Council on Practices & Standards agreed to serve as secretary to US TAG
• ASSE turned to its membership to recruit Technical Advisory Group (TAG) members
US ISO TAG Participants

- AH & T Insurance
- AIHA
- AJ Gallagher
- ASSE
- Bayer Materials
- Brazosport College
- Eide Bailly, LLP
- ESIS
- Federal Gov’t ERM
- McCulley Eastham
- PMMI

- Pilz Automation
- Project Mgmt Trust
- PRIMA
- RIMS
- Safety Mgmt Consultants
- TC 176 TAG
- Washington Group
- Woods Hole
- Wyeth
US ISO TAG – Ongoing Involvement

• Approved ISO 31000 – Now the U.S. Standard on Risk Management
• Considered co-publishing an Implementation Guide with CSA
• Occasionally comment on other standards
Next Phase for ISO 31000 et al

- Question re harmonization of country guides – UK, Canada, Japan, Germany, US, Australia/NZ
- New work group (??) being considered to create an Implementation Guide
- Up for revisions in 2012 (after three years)
Implementation of ISO in the US

• Typically? At least five years to implement
• A LOT of interest by certain groups
• Crossover interests – Security, Resilience and Recovery, Business Continuity
• New training on ERM developed by the other IIA – Insurance Institutes of America “ARM 57”
The Flow of Risk Management

The principles provide the foundation and describe the qualities of effective risk management in an organization.

The framework manages the overall process and its full integration into the organization.

The process for managing risk focuses on individual or groups of risks, their identification, analysis, evaluation and treatment.

Monitoring & review, continual improvement and communication occur throughout.
The Structure & Process

**Principles**
- Creates value
- Part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best avail info
- Tailored
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic, iterative & responsive to change
- Facilitates continual improvement

**Framework**
- Mandate & Commitment
- Design framework for managing risk
- Implement risk management
- Continually improve the framework
- Monitor and review the framework

**RM Process**
- Establish the context
- Risk assessment
  - Risk identification
  - Risk analysis
  - Risk evaluation
  - Risk treatment
- Communicate and consult
- Monitor and review
- Continually improve the framework
- Monitor and review
Scope

ISO 31000

This int’l standard provides principles and generic guidelines on risk management... it can be used by any public, private or community enterprise, association, group or individual. Therefore, this standard is not specific to any industry or sector.

COSO ERM Framework

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.
## Definition of Risk Mgmt

<table>
<thead>
<tr>
<th>ISO 31000</th>
<th>COSO ERM Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordinated activities to direct and control an organization with regard to risk.</td>
<td>Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.</td>
</tr>
</tbody>
</table>
Definition of Risk

ISO 31000

The effect of uncertainty upon objectives.

An effect is a deviation from the expected – positive or negative. Risks may be described as a combination of likelihood and consequences.

COSO ERM Framework

The possibility that an event will occur and adversely affect the achievement of objectives.
## Risk Management Process

<table>
<thead>
<tr>
<th>ISO 31000</th>
<th>COSO ERM Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continually and interactively: Communicate and Consult</td>
<td>Internal environment</td>
</tr>
<tr>
<td>Risk assessment:</td>
<td>Objective setting</td>
</tr>
<tr>
<td>•Risk identification</td>
<td>Event identification</td>
</tr>
<tr>
<td>•Risk analysis</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>•Risk evaluation</td>
<td>Risk response</td>
</tr>
<tr>
<td>•Risk treatment</td>
<td>Control activities</td>
</tr>
<tr>
<td>Continually and interactively: Monitor and Review</td>
<td>Info &amp; communication</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
</tr>
</tbody>
</table>
Practitioners:

• Appreciate ISO’s brevity, accessibility and broad applicability
• Like that ISO is grounded in management, not compliance & is objectives based
• Believe ISO does a better job with opportunity risks
• Will pick and choose what works best (even if it’s a hybrid)
What We’re Hearing – COSO

Practitioners:

• The controls-based approach is too limiting
• It is lacking re opportunity risks
• Lacks the involvement of external stakeholders
• It’s WAY too complex, wordy, difficult to understand or explain
• Risks are more than just events
What We’re Hearing – Needs

Practitioners:

• Want more help with risk appetite, risk aggregation, correlations of risks, key risks and key risk indicators

• Hear from their consultants that they’ve got a mandate to use COSO/not talk about ISO
Global Corporate Governance Models

INTERNATIONAL - Basel I & II; ISO 31000 & 31010

France
- Vienot Com.
- Mrini Report
- Levy-Long Com.

UK
- Cadbury
- Turnbull
- Greenbury Rpt
- BS 31100 RM

All EU Countries
- Directives on Governance

Germany
- Bill on The Control and Transparency of organizations
- Kon TraG Bill

Netherlands
- Code Tabaksblatt

Italy
- Draghi Commission

US
- Business Round Table
- NYSE listing Requirements
- Blue Ribbon Commission
- Sarbanes Oxley Act
- COSO ERM Framework

Canada
- Toronto Stock Exchange Committee
- Canadian Securities Committee
- Allen committee Report
- COCO

Japan
- Corporate Governance Forum of Japan
- J-SOX

Australia/New Zealand
- HB 327 Communicating & Consulting About Risk
- Providing Assurance on Risk
- Stock Exchange Listing
- New Accounting Standards
- Best Practice Stmt Mgmt

South Africa
- Code of Best Practice
- King Report I, II, III
- Stakeholder Communication
- Public Finance Mgmt Act

Developed by Dorothy Gjerdrum, AJG & Mary Peter, Eide Bailly LLP
The RIMS Crosswalk Project

- Comparing the major standards to the RIMS Maturity Model (RMM) for ERM
- Developing a White Paper that will describe strengths and weaknesses and applicability of each

- ISO 31000
- COSO ERM Framework
- BSA 31100
- HM Treasury “Orange Book”
- Basel II
- FERMA Risk Mgmt Standard
- Solvency II
The Role of Audit and the IIA?

• Internal audit should be about providing assurance, not creating or implementing a risk management process

• Audit and Risk Management should work together and support a broader approach to risk

• Recommend participation in ISO TAGs
Specific Ways That Audit Can Support Risk Management

• Clarify your role
• Workshops on risk controls
• Tests re whether controls are working or adequate
• Changes to risk rankings – do they make sense?
• Assurance that key risks have been identified and are being addressed
Framework Design: Clarifying WhoDoes What

(Sample Federal Organization from Canada)

(Based on the Institute of Internal Auditors Position Paper www.theiia.org) and revised by the Canadian Standards Association
Closing Comments

• We have too much at stake NOT to cooperate
• Our skills are complimentary – and a part of the whole
• The goal of Risk Management = helping our entities manage uncertainty and achieve our most important objectives/strategies
Thank You!

Dorothy Gjerdrum, ARM-P
Executive Director, PESD
Arthur J. Gallagher Risk Mgmt Services
Dorothy.Gjerdrum@ajg.com
651.642.2999