

ERM Standards of Practice and Shared Risk Principles







ERM 2011 Symposium – Chicago IL
March 15, 2011

Carol Fox
Director, Strategic and Enterprise Risk Practices

Agenda

- Global risk governance drivers
- Evolving standards and frameworks
- Most widely used standards and frameworks
- Purposes
- Common elements

Global Risk Governance Drivers

 France	<ul style="list-style-type: none"> • Vienot Committee • Marini Report • Levy-Lang Committee 	 Germany	<ul style="list-style-type: none"> ▪ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich ▪ Bill on The Control and Transparency of Companies KonTraG Bill
 Holland	<ul style="list-style-type: none"> • Commission on Corporate Governance 	 UK	<ul style="list-style-type: none"> • Cadbury • Turnbull • Greenbury
 South Africa	<ul style="list-style-type: none"> • Code of Best Practice • King Report I, II and III • Stakeholder Communication • Report on Effective Systems of Internal Control 	 USA	<ul style="list-style-type: none"> • Business Round Table • Securities Exchange Commission - Disclosures • NACD Blue Ribbon Commission • Sarbanes-Oxley Act • Dodd-Frank Act
 Italy	<ul style="list-style-type: none"> • Draghi Commission 	 Japan	<ul style="list-style-type: none"> • Corporate Governance Forum of Japan
 Canada	<ul style="list-style-type: none"> • Toronto Stock Exchange Committee • Canadian Securities Committee • Allen Committee Report • Canadian Institute of Chartered Accountants 	 Australia	<ul style="list-style-type: none"> • Blue Book • Company Law Review • Best Practice Statement of Management Discussion and Analysis • Stock Exchange Listing • New Accounting Standards

The World of Standards

What Standards Are

- A collection of best practices and guidelines
- Developed collaboratively
- Evolutionary
- Can be for management systems, products, services or procedures

What Standards Are Not

- Regulations
- Just controls
- Necessarily "how to implement" documents
- Certifications (nor require that an organization be certified to use a standard)

What is a Standard?

A [primary standard](#) (or “recognized” standard) is an established norm or requirement, usually a formal document that establishes criteria, methods, processes and practices under the jurisdiction of an international, regional or national standards body.

In contrast, a custom, convention, guidance document, company product, corporate standard, etc. that may be developed outside of a recognized standards setting body but which becomes generally accepted and dominant is often called a [de facto standard](#).

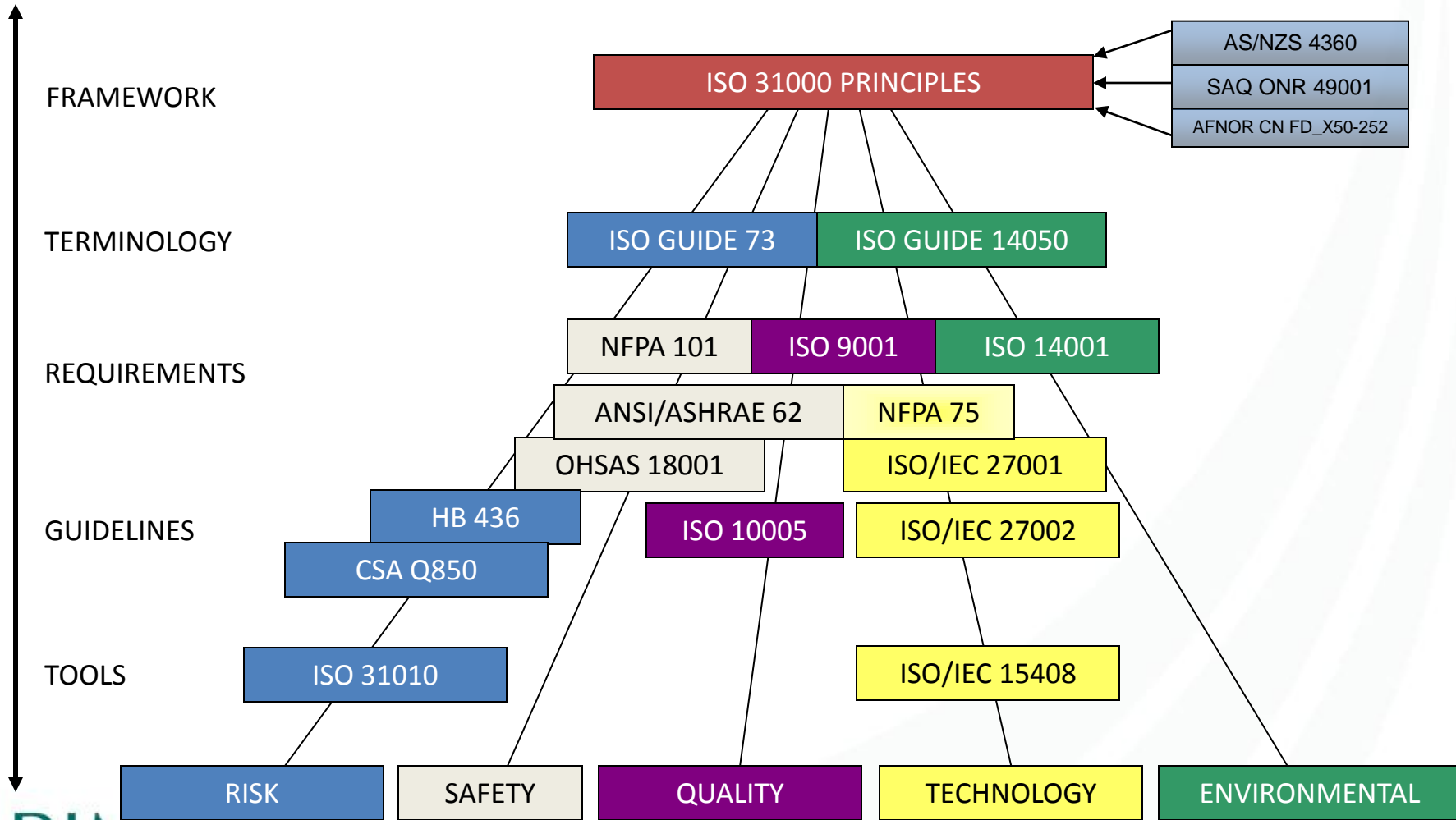
What is a Framework?

frame•work (frām'wûrk') n.

1. A structure for supporting or enclosing something, esp. a skeletal support used as the basis in something being constructed
2. an external work platform; a rig.
3. A basic arrangement, form, or system: *“social structure is a stronger framework for behavior than national feeling.”* (Stanley Kaufman)

Source: The American Heritage Dictionary, Second Edition, 1982

Standards Hierarchy



Why Use Standards?

- Set of benchmarked tools and processes
- Systematically identify risks and problems
- Problem-solving and decision-making tools
- Inclusive process
- Specialized training
- Establishes operational controls/procedures
- Measurable/verifiable goals and methods for accomplishing identified objectives
- Protect reputation and brand
- Model for continual improvement

Proactively improve organizational resilience and sustainability

Most Widely Used Non-Regulatory Risk Management Standards and Frameworks



ISO 31000:2009

- Risk Management – Principles and Guidelines



COSO:2004

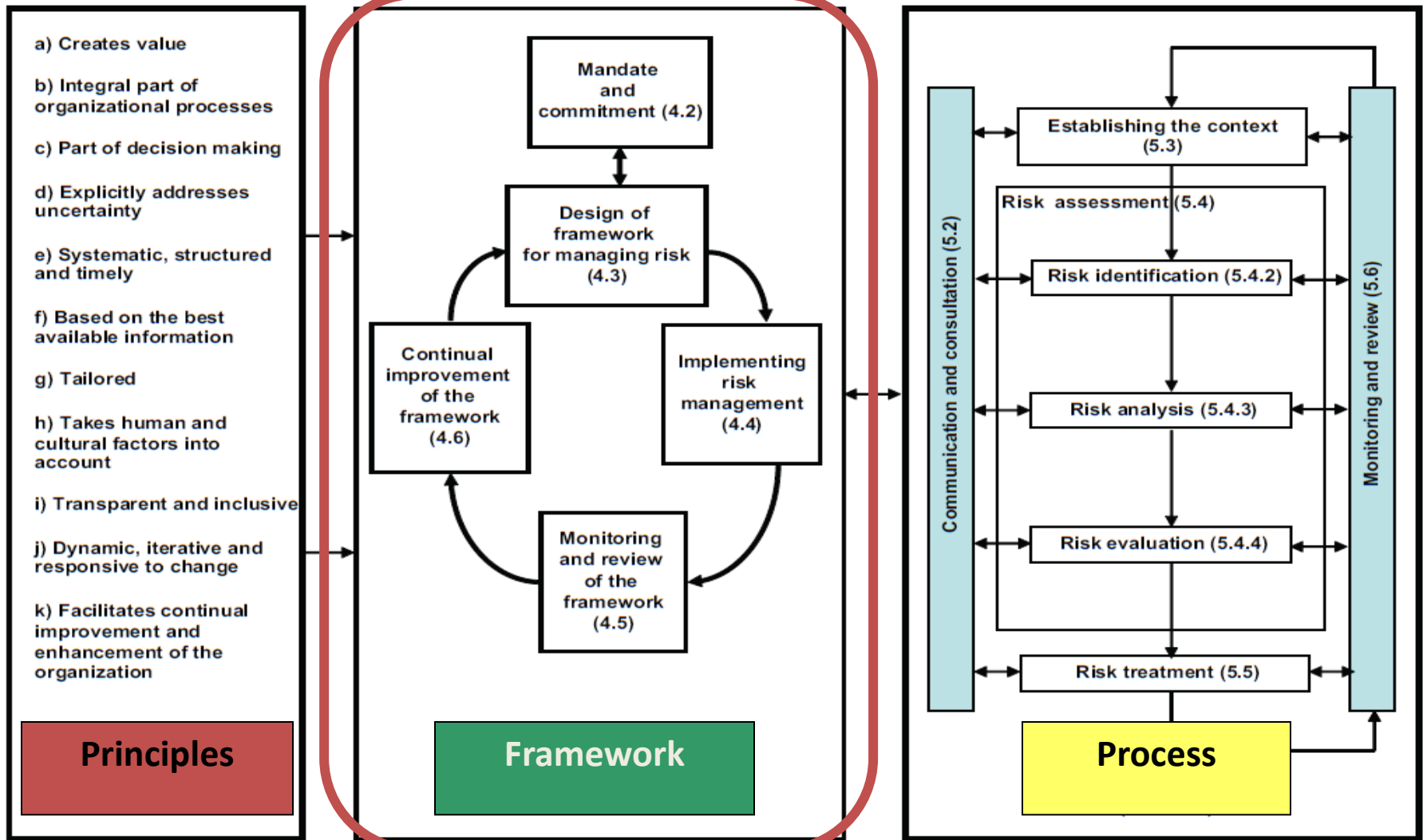
- Enterprise Risk Management – Integrated Framework



OCEG “Red Book” 2.0:2009

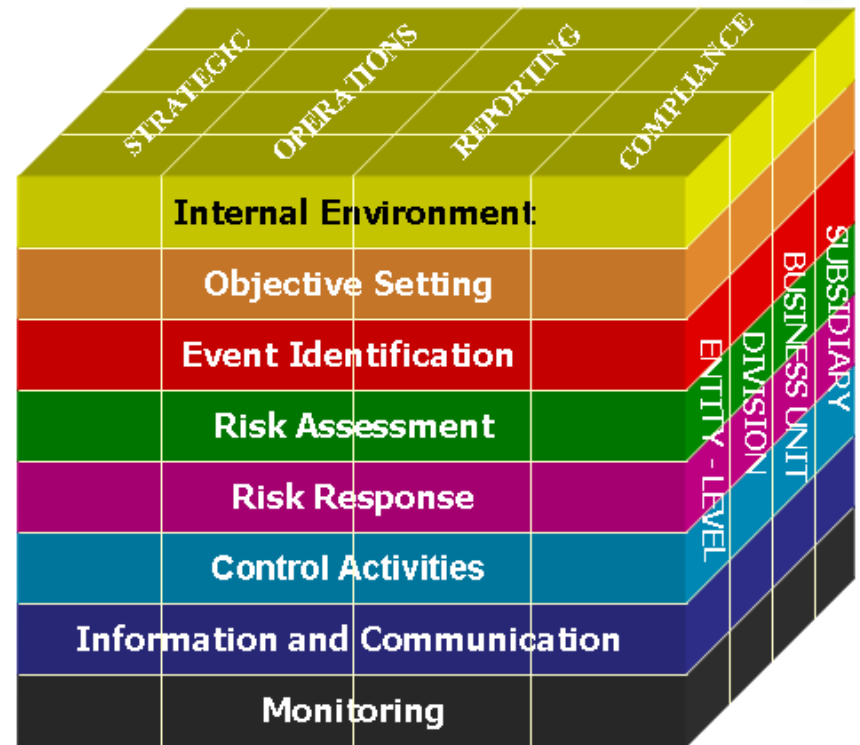
- GRC Capability Model™

ISO 31000 - Risk Management



COSO ERM Framework

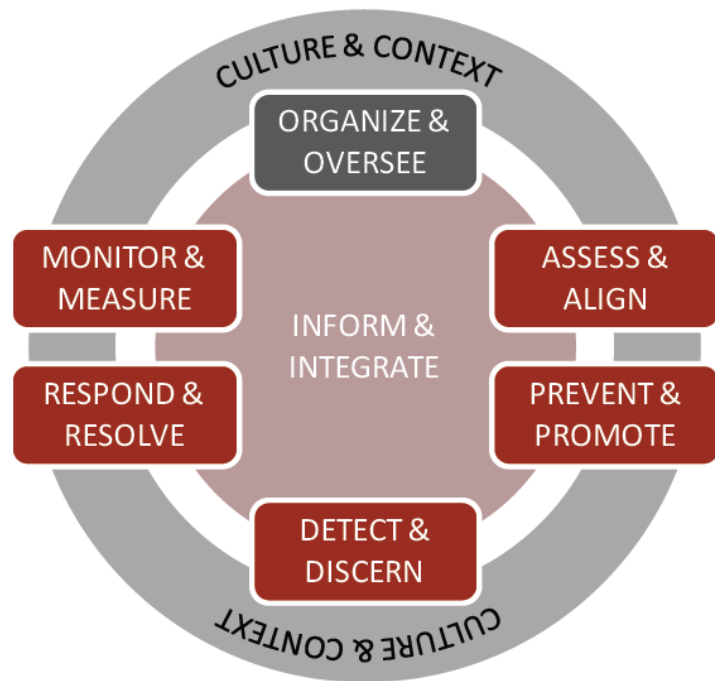
Internal Environment	<ul style="list-style-type: none"> •What is the internal philosophy and culture?
Objective Setting	<ul style="list-style-type: none"> •What are we trying to accomplish?
Event Identification	<ul style="list-style-type: none"> •What could stop us from accomplishing it?
Risk Assessment	<ul style="list-style-type: none"> •How bad are these events? •Will they really happen?
Risk Response	<ul style="list-style-type: none"> •What are our options to stop those things from happening?
Control Activities	<ul style="list-style-type: none"> •How do we make sure they don't happen?
Information and Communication	<ul style="list-style-type: none"> •How [and from/with whom] will we obtain information and communicate?
Monitoring	<ul style="list-style-type: none"> •How will we know that we've achieved what we wanted to accomplish?



Source: Committee of Sponsoring Organizations of the Treadway Commission www.coso.org. Used with permission.

OCEG GRC Capability Model™ Components

Culture and Context	<ul style="list-style-type: none"> • External and internal business context • Culture, values and objectives
Organize & Oversee	<ul style="list-style-type: none"> • Outcomes, commitment, role and responsibilities, accountability
Assess & Align	<ul style="list-style-type: none"> • Risk identification, analysis and optimization
Prevent & Promote	<ul style="list-style-type: none"> • Codes of conduct, policies, controls, awareness & education, incentives, stakeholder relations, risk financing and insurance
Detect & Discern	<ul style="list-style-type: none"> • Hotline notification, inquiry & survey, detective controls
Inform & Integrate	<ul style="list-style-type: none"> • Information management & documentation, internal & external communication, technology & infrastructure
Respond & Resolve	<ul style="list-style-type: none"> • Internal review and investigation, 3rd party inquiries & investigation, corrective controls, crisis response and recovery, remediation & discipline
Monitor & Measure	<ul style="list-style-type: none"> • Context monitoring, performance monitoring & evaluation, systemic improvement, assurance



Source: Open Compliance and Ethics Group,
 © 2003-2009 OPEN COMPLIANCE AND ETHICS GROUP
 Used with permission. www.oceg.org

Risk Management Purposes

Objectives-based

- Designed to improve an organization's ability to meet or exceed its objectives through enhanced decision-making and activities that address key uncertainties.

Compliance and Control

- Seeks primarily to transfer or mitigate risks through compliance and control activities; often based on historic losses, near-misses, etc.

Regulatory

- Used when an organization must apply a designated practice and/or standard in order to meet regulatory requirements (e.g., Basel II for financial institutions).

RIMS Review

APPENDIX B. OVERVIEW OF WIDELY USED RISK MANAGEMENT STANDARDS AND GUIDELINES

	ISO 31000: 2009 Risk Management Practices and Guidelines	OCEG "Red Book" 2.0: 2009 GRC Capability Model	BS 31100: 2008 Code of Practice for Risk Management	COSO: 2004 Enterprise Risk Management Integrated Framework	FERMA: 2002 A Risk Management Standard	SOLVENCY II: 2012 A Regulatory Standard
Applicable to	All industries and sectors	All industries and sectors	All industries and sectors	Companies interested in satisfying internal control needs and in moving to a fuller risk management process	All organizations	Insurance companies located in or doing business in the European Union
Primary Objective¹	Organizational	Compliance and Control	Organizational	Organizational, Compliance and Control	Organizational	Regulatory
Type of Document²	Primary standard	Guidance document	Primary standard	Guidance document	Guidance document	Primary standard

ERM Success Attributes

RIMS Risk Maturity Model

1. Adoption of ERM-based approach
2. ERM Process Management
3. Risk Appetite Management
4. Root cause discipline
5. Uncovering risks
6. Performance Management
7. Business resiliency and sustainability



Common Elements from RIMS Review

RIMS RMM	ISO 31000	OCEG	BS 31100	COSO	FERMA	SOLVENCY II
ERM-based Approach	X	X	X	X	X	X
Process Management	X	X	X	X	X	X
Risk Appetite Management	X	X	X	X	X	X
Root Cause Discipline	X		X			X
Uncovering Risks	X	X	X	X	X	X
Performance Management	X		X	X	X	X
Business Resiliency and Sustainability	X	X			X	X

Questions

Carol Fox

Director of Strategic and Enterprise Risk Practice

cfox@rims.org

ERM Center of Excellence

www.rims.org

Related Links

Risk Maturity Model
Guidelines and Standards
Education
Resource Library
eGroup
Annual ERM Summit
Links
What is ERM?
ERM for Dummies
Contact Us

Latest ERM News & Information

- **New to the CoE!** [Positioning GRC and ERM](#)--Placing these puzzle pieces together to improve performance, by Mary Peter. Knowledge Leadership Paper, Compliance Week, August 2010.
- **New to the CoE!** [Managing Risk in Government: An Introduction to Enterprise Risk Management](#), Financial Management Series - 2010 Second Edition, Dr. Karen Hardy, IBM Center for The Business of Government, October 2009
- **New to the CoE!** [Risk Appetite: Practical Issues for the Global Financial Services Industry](#), Trowbridge Deloitte Limited, September 2007
- **NEW to the CoE!** [Risk: Getting Appetite Right](#) Price Waterhouse Coopers, May 2009
- **NEW to the CoE!** [Risk Appetite: A multifaceted approach to risk management](#) based on an IBM Center for the Business of Government report, October 2009