Update on ISO 31000 and Practical Considerations in Implementing It

Dr. Karen Hardy
Deputy Director for Risk Management
Certified Global ISO 31000 Risk Management Professional
U.S. Department of Commerce

There is a link between performance and standards. Standardization, at a minimum, guarantees some level of performance expectation.

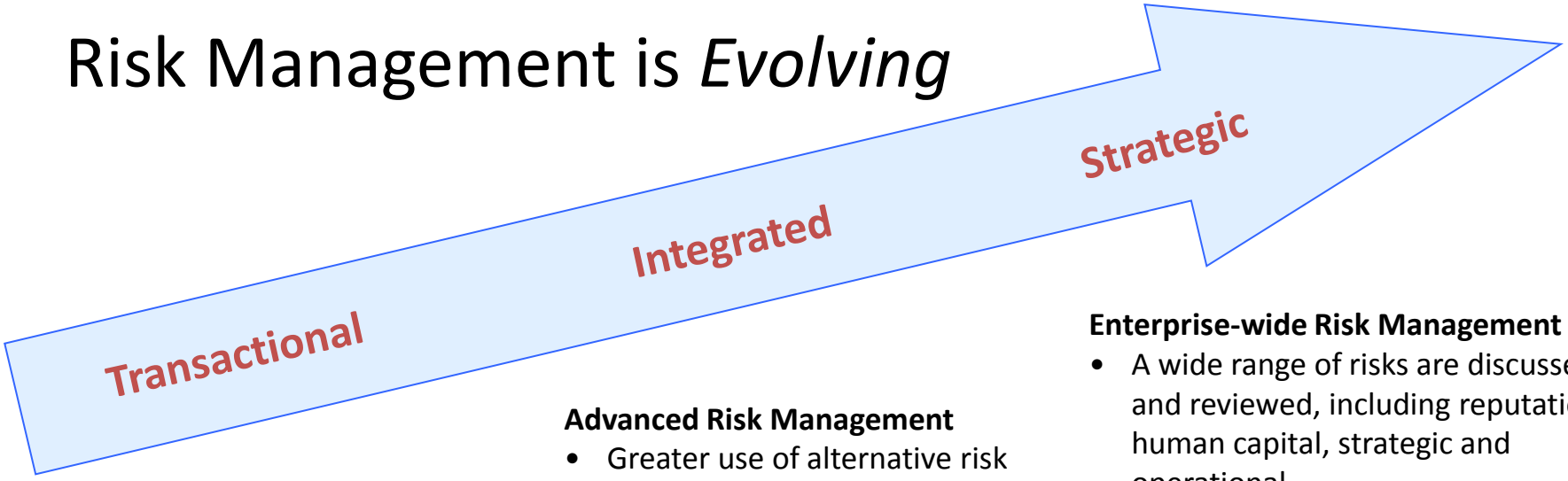
As fiscal constraints continue, agencies will need to create collaborations to share risk and help finance mission critical activities.

Risk Management Standardization- when a certain standard of practice is expected across all federal agencies, this will help optimize agency performance across the board.

Presentation Objectives

- What is a Standard?
- What are the benefits of standardization?
- Background on ISO31000 Risk Management Standard
- Is there policy support for ISO31000?
- Elements of Risk Management
  - ISO31000 process and framework
  - ISO 31000 as a standard for decision-makers
- Practical Examples of Implementation
  - Budget formulation
  - Integration into Board Decisions
  - Mission Critical Risk
- Where do we go from here?

Risk Management is *Evolving*



Traditional Risk Management

- Purchase insurance to cover risks
- Hazard-based risk identification and controls
- Compliance issues addressed separately
- Safety & emergency mgmt handled separately
- "Silo" approach – risk mgmt is not integrated across the organization
- Risk Manager is the insurance buyer

Advanced Risk Management

- Greater use of alternative risk financing techniques
- More proactive about preventing and reducing risks
- Integrates claims mgmt, contracts review, special event RM, insurance and risk transfer techniques
- Cost allocation used for education and accountability
- More collaboration – as depts are willing
- Risk Manager may be the risk owner

Enterprise-wide Risk Management

- A wide range of risks are discussed and reviewed, including reputational, human capital, strategic and operational
- Aligns RM process with strategy and mission
- May include "upside risks" (opportunities)
- Helps manage growth, allocate capital & resources
- Risks are owned by all & mitigated at the department level
- Many risk mitigation & analytical tools available
- Risk Manager is the risk facilitator and leader

Risk is bad – focus is on transferring risk

Risk is an expense – focus is on reducing cost-of-risk

Risk is uncertainty – focus is on optimizing risk to achieve goals

Source: Arthur J. Gallagher

What is a Standard?

- Definition as cited in the National Technology Transfer and Advancement Act of 1995 (NTTA).
- NTTA directs Federal Agencies to use consensus standards developed by consensus standards bodies.
- Encourages participation in voluntary consensus standards bodies
- NTTA brought civilian agencies into the practice of using private sector standards in place of government unique standards.
- Grew out of DoD's experience of relying more on voluntary consensus standards and less on Military Specifications (MIL SPECs)

The term “standard” includes…

1) **Common and repeated use of rules, conditions, guidelines** or characteristics for products or related processes and production methods, and related management system practices.

2) **The definition of terms**; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

OMB Circular A-119

Entitled: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities

<u>General Agency Requirements</u>: ***Use voluntary consensus standards in lieu of government-unique standards except where the use is consistent with law or otherwise impractical.***

- Guides Federal agencies on the implementation of the NTTAA.
- Establishes policies on Federal use and development of voluntary consensus standards and on conformity assessment activities.

OMB Circular A-119- GOALS

Goals of the government's use of voluntary consensus standards (VCS) are to:

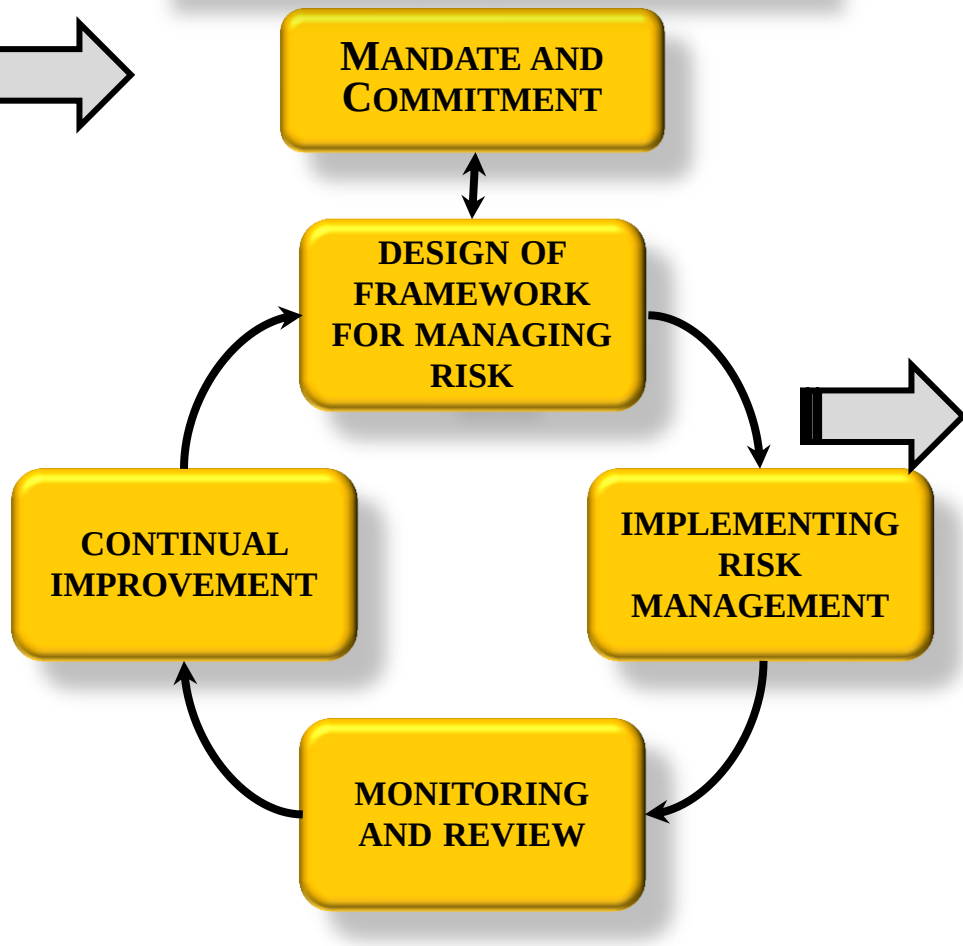
- Eliminate costs of developing in-house standards;
- Decrease cost of goods and services procured by the government;
- Minimize burden of complying with agency regulation;
- Provide incentives/opportunities to establish standards that serve national needs;
- Encourage long-term growth for US enterprises;
- **Promote efficiency** and economic competition;
- Further the government's policy of reliance upon the private sector to supply goods and services by the Federal government.

Objectives of ISO 31000

PRINCIPLES

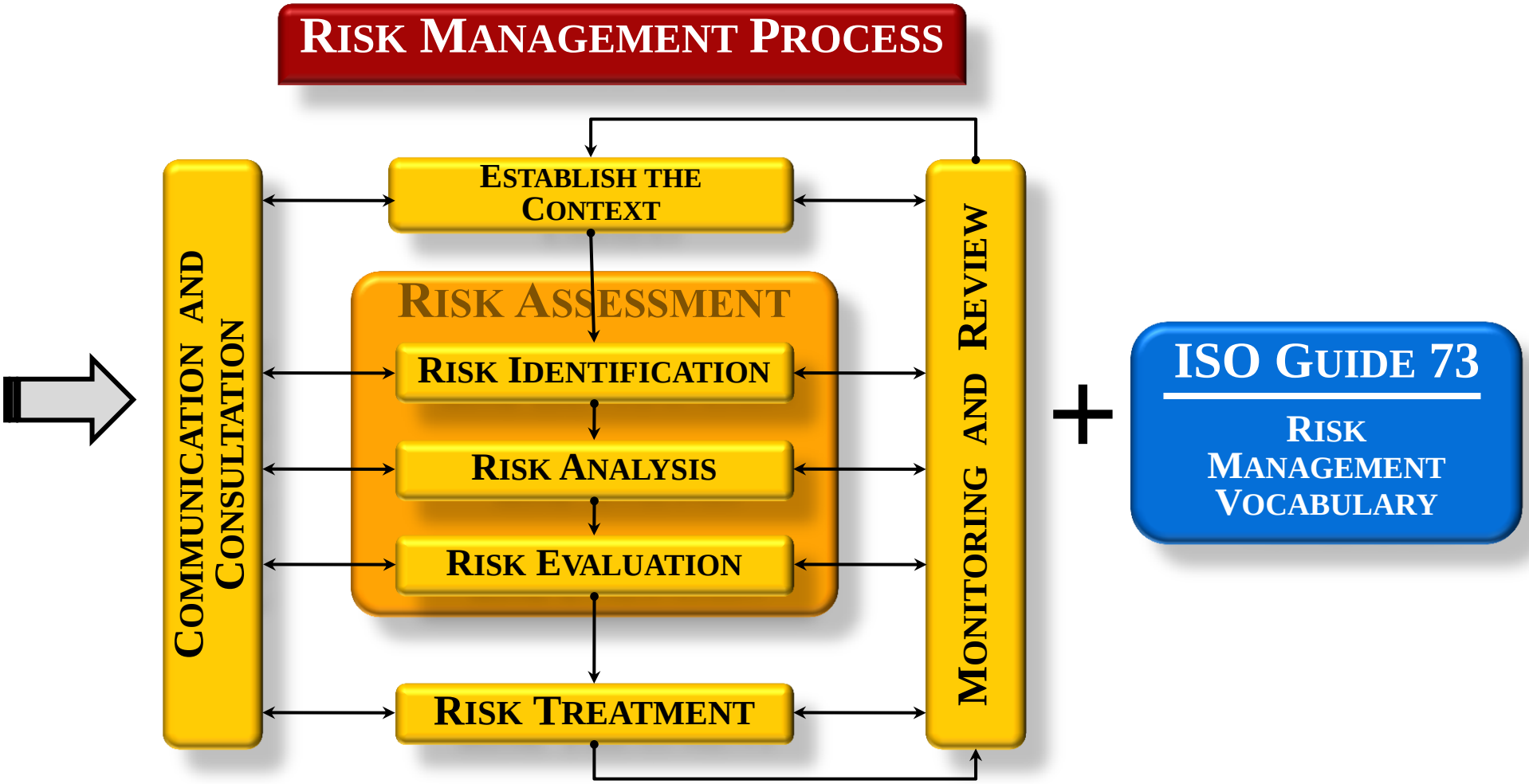
a) *Creates value*
b) *Integral part of organizational processes*
c) *Part of decision making*
d) *Explicitly addresses uncertainty*
e) *Systematic, structured and timely*
f) *Based on the best available information*
g) *Tailored*
h) *Takes human and cultural factors into account*
i) *Transparent and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

FRAMEWORK



Source: Global Risk Management Institute

Implementation of ISO 31000



Source: Global Risk Management Institute

Implementation of ISO31000

- **Establishing the Context-** Defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.
  - External environment in which the organization seeks to achieve its objectives.
  - Internal environment in which the organization seeks to achieve its objectives.

Establishing the Context

External Context

- The cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment;
- Key drivers and trends having impact on the objectives of the organization, and
- Relationships with, and perceptions and values of external stakeholders

Internal Context

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives, and the strategies that are in place to achieve them;
- The organization's culture;
- Standards, guidelines and models adopted by the organization;
- Form and extent of contractual relationships

External and Internal Context Issues to Consider

- Risk Assessment – FISMA requires following a separate Risk Management Framework for IT Security.
- FMFIA (Federal Manager's Financial Integrity Act)- Internal Controls Over Financial Reporting.
- Increased Continuing Resolutions and Sequestration.

ISO 31000 Implementation - Examples

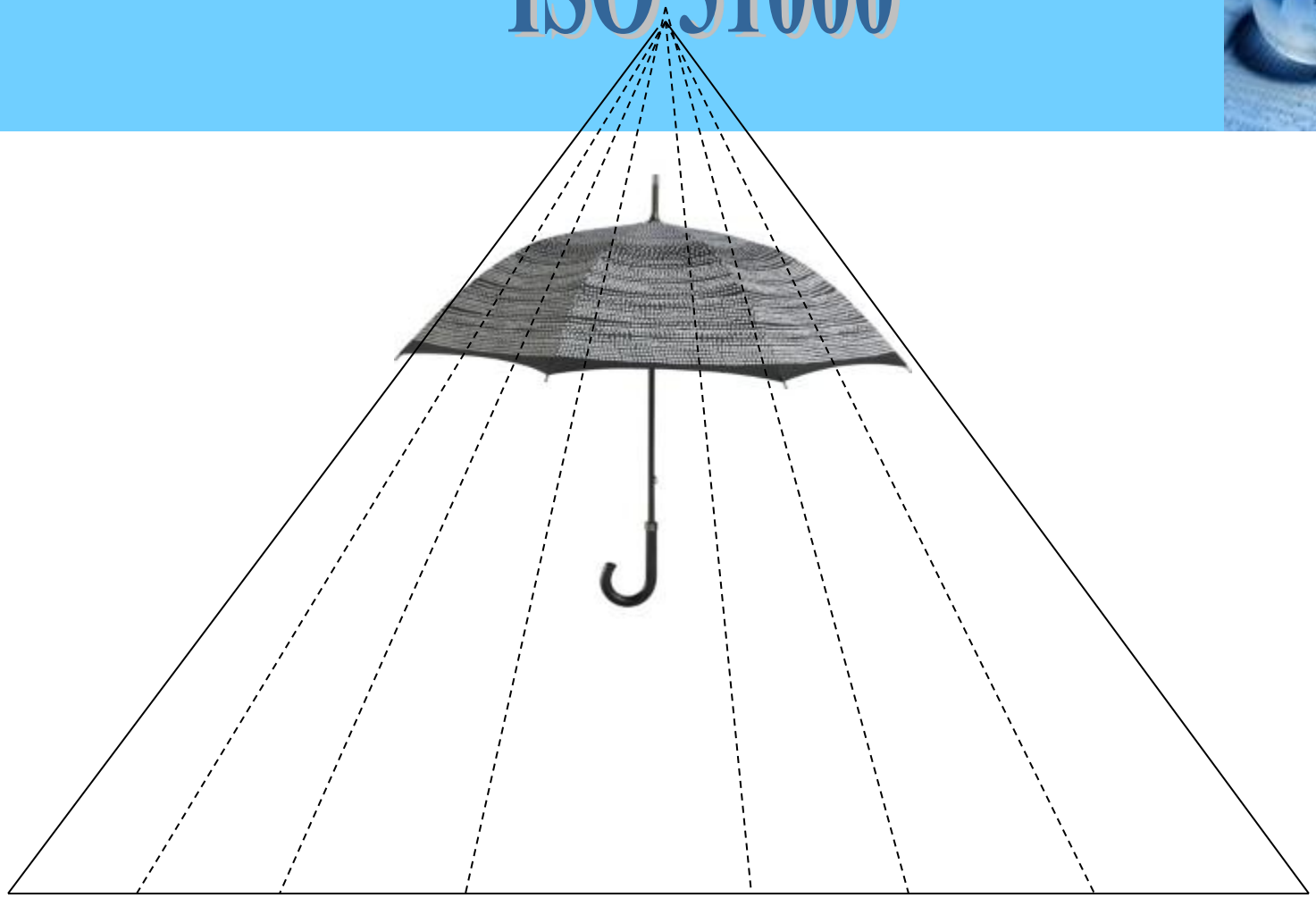
Application of Risk Management in all Decision-Making:

"All decision making within the organization, whatever the level of importance and significance involves the explicit consideration of risks and the application of risk management to some appropriate degree"- ISO 31000

EXAMPLES:

- Budget Formulation/Justification Process
- IT Review Board
- Milestone Review Board
- Mission Critical Risk using GAO High Risk List Model

ISO 31000



Quality OH&S Finance IT security Project

Environment Food safety Equipment Supply chain

Thank You!

For more information about ERM implementation:

Karen Hardy

khardy@doc.gov