Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Presentation to NYSICA and NY PRIMA

May 21, 2015

ERM:
Start From Where You Are

DOROTHY GJERDRUM, ARTHUR J. GALLAGHER

Agenda

- Defining ERM – and Redefining Risk
- ERM Components and Roles
- Implementation Plan
- Resources

Defining ERM

Understand this new approach

- How risk management is evolving
- What is “risk” and why do we need an expanded view of risk?
- Defining ERM
- Why entities implement ERM

How Risk Management is Evolving

Transactional Approach

- 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

***Risk is bad* – focus is on transferring risk**

Integrated Approach

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

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

Strategic Approach

- A wide range of risks are considered (e.g. financial, strategic, legal, operational)
- Aligns RM process with strategy and mission
- Broader definition of risk to include opportunities; focus on uncertainty
- Helps manage growth, allocate capital & resources
- Risks are owned by those who control them
- Many risk treatment & analytical tools available
- Risk Manager is the risk facilitator and leader

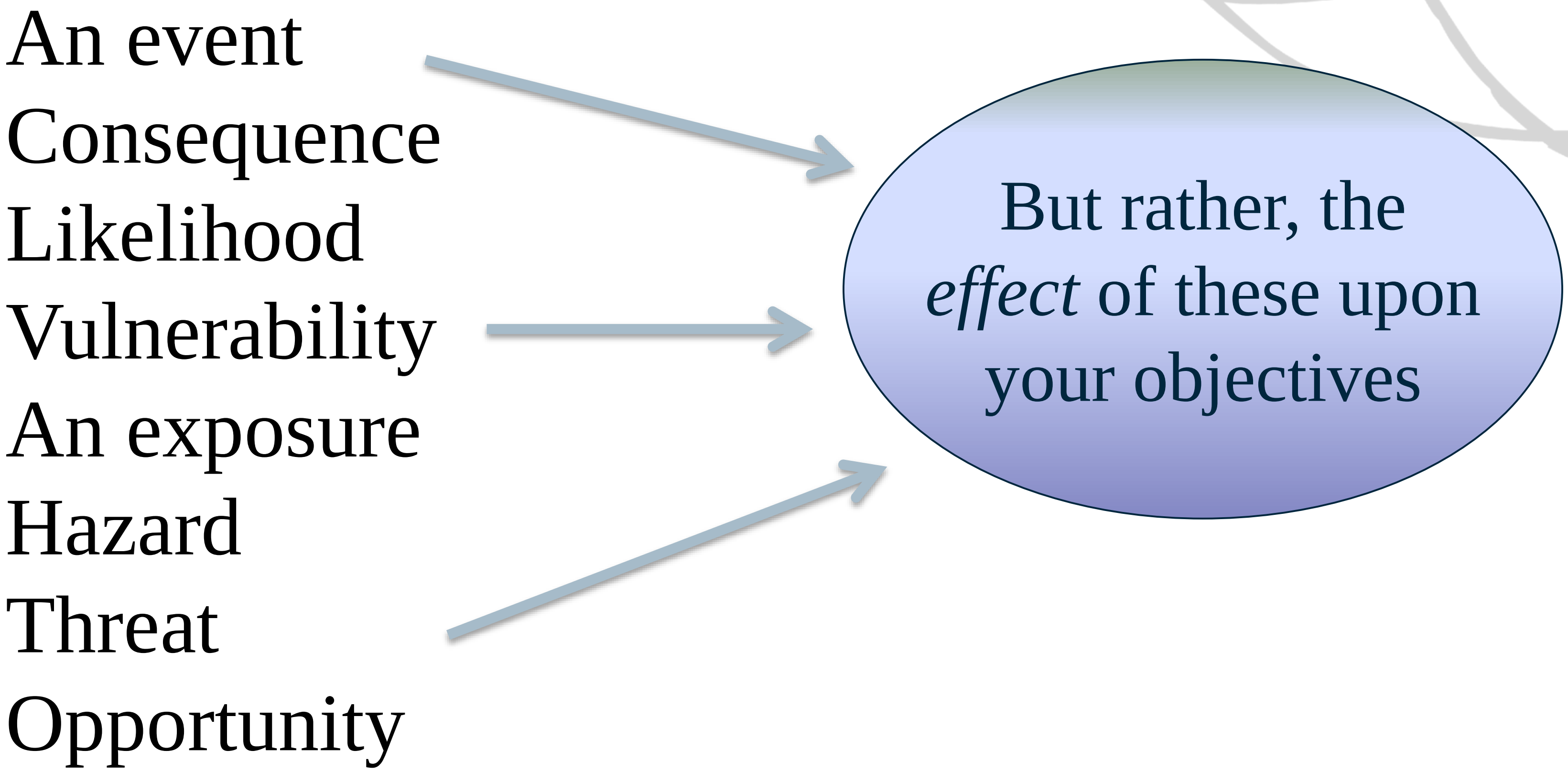
***Risk is uncertainty* – focus is on optimizing risk to achieve goals**

What is “risk”??

- Risk is the *effect* of *uncertainty* on our objectives.
- Risks can pose both threats and opportunities

- Anything that could harm, prevent, delay *or enhance* our ability to achieve our objectives = risk

Risk is not *just:*



An event
Consequence
Likelihood
Vulnerability
An exposure
Hazard
Threat
Opportunity

But rather, the *effect* of these upon your objectives

A closer look at *Uncertainty*

- Makes a clear connection to the environment, the world – and your context
- There are many causes and sources, internal and external
- It recognizes that some/much is out of your direct control
- It’s a broader view –both positive and negative consequences are possible

Why We Need to Manage Risk

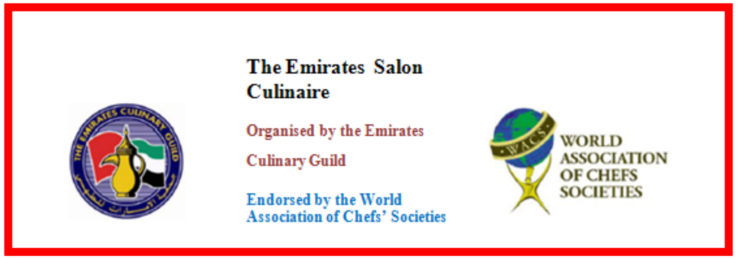
The purpose of managing risk is to increase the likelihood of an organization achieving its objectives by being in a position to manage threats and adverse situations and being ready to take advantage of opportunities that may arise.

National Guidance
on Implementing ISO 31000:2009
From NSAI in Ireland

ERM Also Supports Opportunities

A *Potential* International Culinary Competition:

- A key “ingredient” in a culinary arts training program
- An important opportunity for students, but the event occurred during uprisings in Egypt



The Emirates Salon Culinaire

Organised by the Emirates Culinary Guild

Endorsed by the World Association of Chefs' Societies

WORLD ASSOCIATION OF CHEFS SOCIETIES

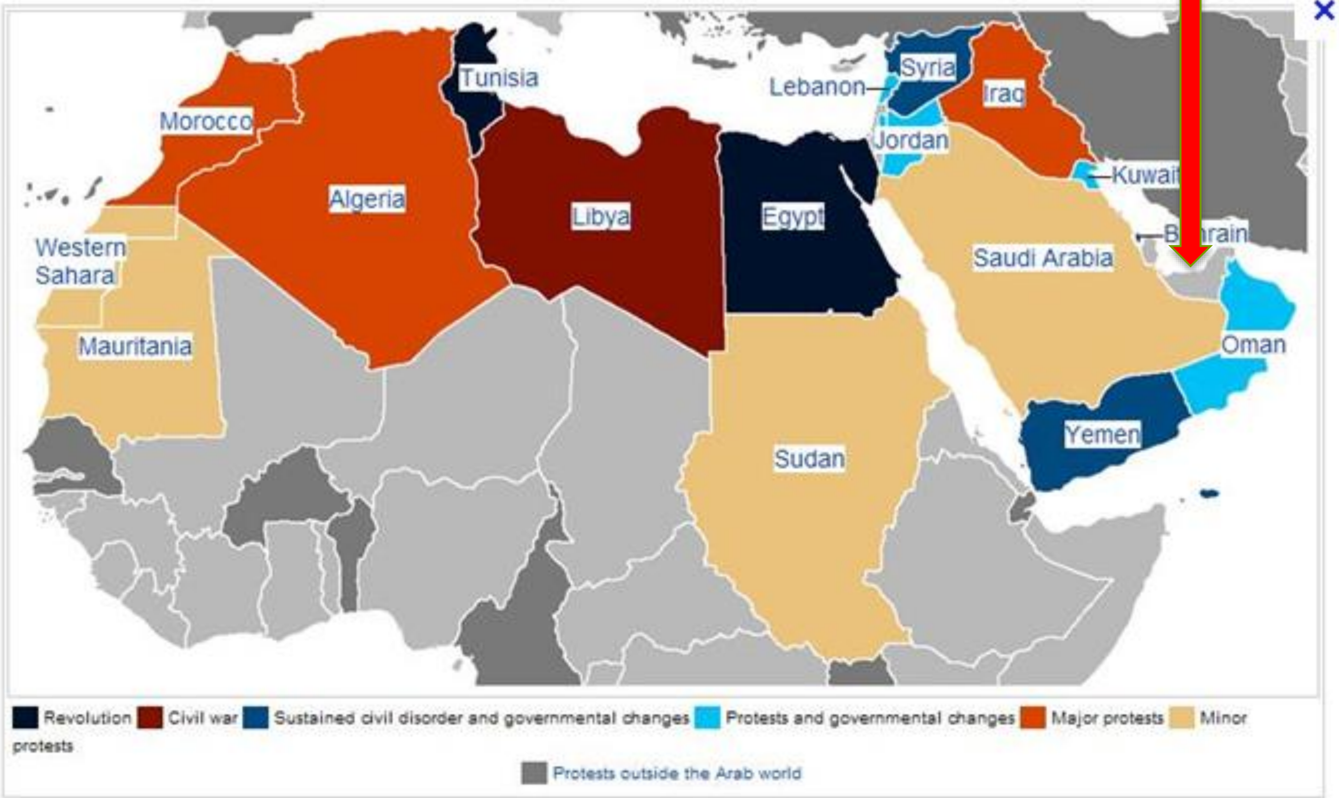
The Middle East and Northern Africa during the "Arab Spring"

The Emirates Salon Culinaire

Organised by the Emirates Culinary Guild

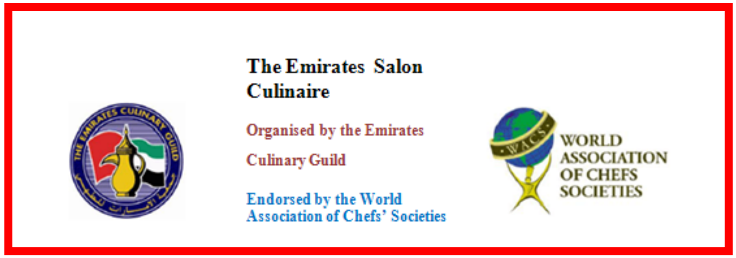
Endorsed by the World Association of Chefs' Societies

WORLD ASSOCIATION OF CHEFS SOCIETIES



Results

- The college decided to support the trip
- Six students & one faculty member participated
- Plans were developed to minimize the threats, including training on the appropriate code of conduct and cultural context, supervision by an experienced traveler & the purchase of travel abroad insurance
- Result: Awarded silver medal!



The Emirates Salon Culinaire

Organised by the Emirates Culinary Guild

Endorsed by the World Association of Chefs' Societies

WORLD ASSOCIATION OF CHEFS SOCIETIES

Defining ERM

(Enterprise) Risk Management is the coordinated effort to direct and control all activities related to risk.

It defines risk as the **effect of uncertainty on objectives**. It therefore ties the management of risk to what is most important to the organization.

The **responsibility for managing risk** is spread across the organization to those who have accountability and authority – **risk owners**.

ANSI/ASSE/ISO 31000:2009

Key Differentiators

Between “Traditional” Risk Management & ERM

- The definition of risk includes both negative and positive outcomes
- Accountability and ownership
- Managing risk is part of every decision, project and activity
- Prioritization of risk is linked to key objectives and strategy
- The consideration of *context* and *stakeholders* is incorporated throughout

Comparing the Practice

“Traditional” RM

- Focused on hazards & the downside of risk
- Many risk management “silos” – lack of integration
- Who’s responsible?
- Mitigation tools = insurance, risk transfer, prevention

Enterprise RM

- Anything that can affect your objectives
- Management of risk from top down & all across
- Risk owners assigned
- Risk owners identify and track mitigation
- Application to decision-making

ERM requires risk *leadership*, not just management

Motivation – Why ERM?

- External mandate
- Governing board or leadership wants it
- Internal audit
- Issuing bonds/public debt & financial rating agency review

- The desire for *RISK LEADERSHIP*

What about adoption?

And why does that matter??

The *International Community*

- ISO 31000 is *the only standard* on the practice of risk management
- COSO & ISO & the IIA working together
  - Revisions to ISO 31000
  - Revisions to COSO ERM Framework
  - Potential white papers and resource material – jointly
- Widespread adoption of ISO 31000 around the globe assures that this framework, this approach is not going away

From standardandpoors.com

Standard & Poors Ratings Services has expanded its review of the financial service industry's enterprise risk management (ERM) practices. This ERM initiative is an effort to provide more in-depth analysis and incisive commentary on the many critical dimensions of risk that determine overall creditworthiness.

This enhancement is part of Standard & Poor's holistic assessment ERM of corporations and financial institutions. Standard & Poors is continually enhancing its ratings process to respond to the emergence of new risks and marketplace needs and conditions.

The Benefits of Risk Management

- Increase likelihood of achieving objectives
- Encourage proactive management
- Be aware of the need to identify and treat risk throughout the organization
- Improve the identification of opportunities & threats
- Effectively allocate and use resources
- Improve governance
- Comply with relevant legal and regulatory requirements and international norms
- Improve mandatory and voluntary reporting
- Improve operational effectiveness & efficiency
- Improve stakeholder confidence and trust
- Establish a reliable basis for decision making & planning
- Improve controls

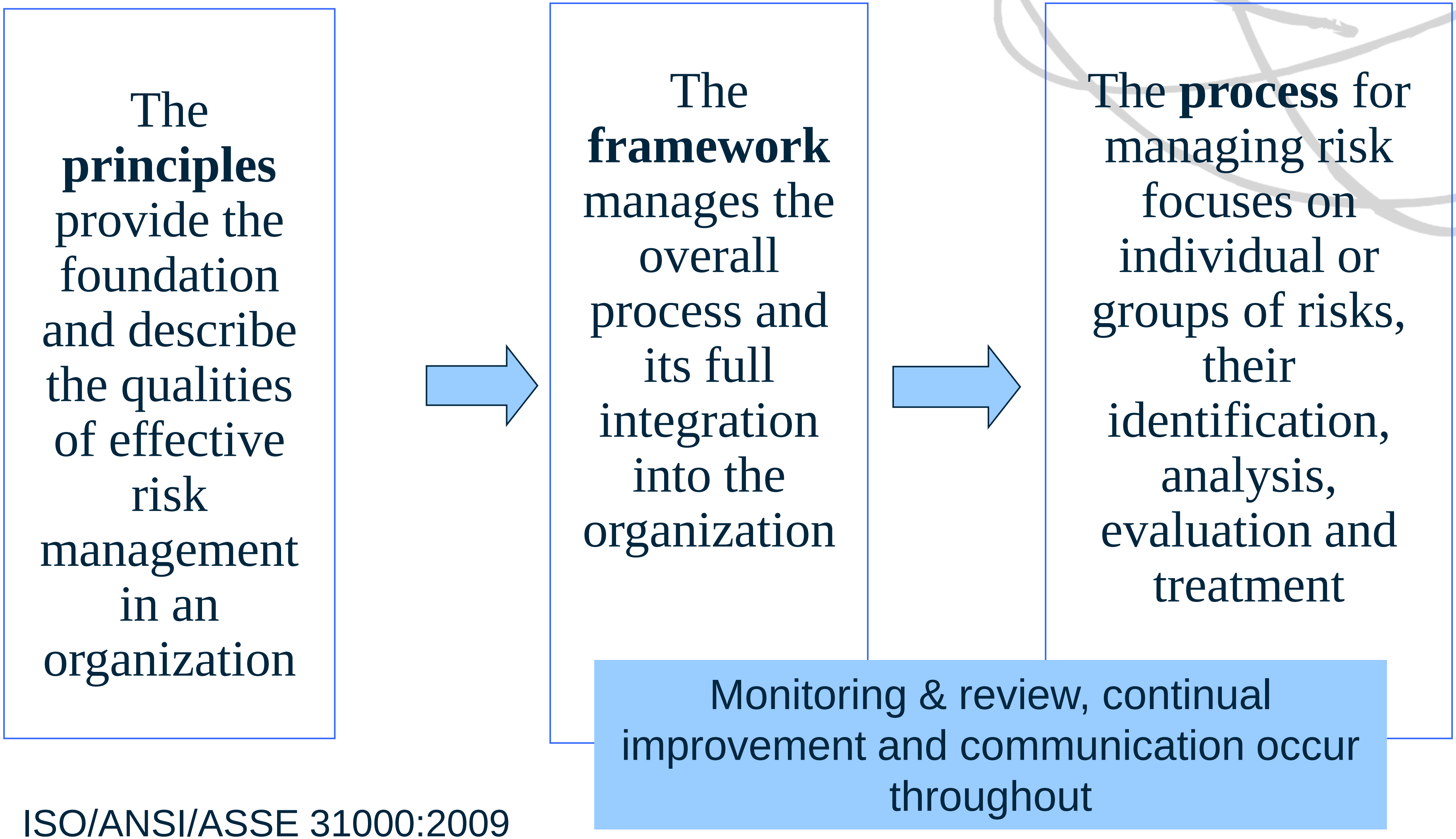
ISO/ANSI/ASSE 31000:2009
Risk management – Principles and Guidelines

ERM Components & Roles

Understand the framework and roles

- The architecture of ISO 31000
- Roles

The "Architecture" of ERM



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

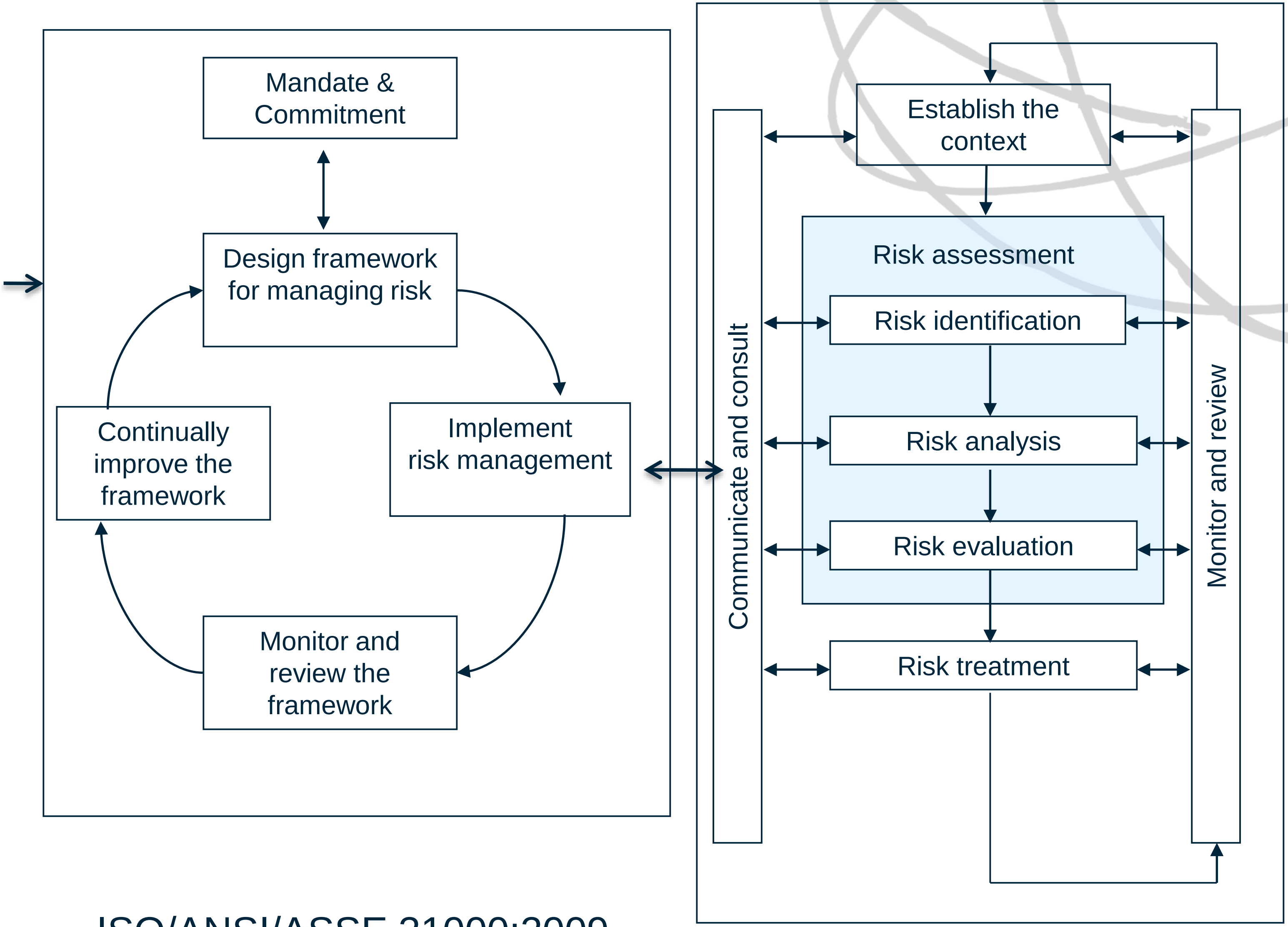
ISO/ANSI/ASSE 31000:2009

Principles

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

Framework

RM Process



Mandate & Commitment

Design framework for managing risk

Implement risk management

Monitor and review the framework

Continually improve the framework

Communicate and consult

Establish the context

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Monitor and review

ISO/ANSI/ASSE 31000:2009

Used with permission

Principles

- Creates & protects value
- Integral part of organizational processes
- Part of decision making
- Explicitly addresses uncertainty
- Systematic, structured & timely
- Based on best available info
- Tailored
- Takes human & cultural factors into account
- Transparent & inclusive
- Dynamic, iterative & responsive to change
- Facilitates continual improvement & enhancement of the organization

The principles provide guidance on the rationale for managing risk and the characteristics of effective risk management

These shape the design and structure of your *framework* for managing risk

The principles can assist in continual improvement and serve as a “maturity model” for implementation

Using Principles to Evaluate ERM

Principle	1 = No evidence or not known 2 = Partially implemented or planned 3 = Largely implemented & evident 4 = Fully implemented, auditable
Risk management creates and protects value – RM contributes to the demonstrable achievement of objectives and improvement of performance (e.g., human health & safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation)	Score = ___ Describe evidence; this may include policies, reports, audits, reviews, etc.
Risk management is part of decision making – RM helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action	Score = ___ Describe evidence; this may include policies, reports, audits, reviews, etc.

Using the Principles to Evaluate Progress

Principle	Potential Evidence
Risk management creates and protects value. Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.	•Linking RM to organizational performance objectives •Improvement of performance •Achievement of objectives •Efficiency in operations •Governance decisions & processes
Risk management is an integral part of all organizational processes. Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes.	•Integration into strategic planning process •Integration into key business processes •Consideration of risk in management responsibilities •Including risk assessment in project management •Including the responsibility for managing risk in position descriptions and performance reviews
Risk management is part of decision making. Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action.	•Examples of outcomes of the Risk Assessment Process applied to decision making

Using the Principles to Evaluate Progress

Principle	Evidence
Risk management explicitly addresses uncertainty. Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.	•Terminology and understanding of risk and uncertainty •Discussion of uncertainty built into all risk assessment processes and decision making •Periodic review of context – how is our world changing? •How certain are we of the results of our assessment of risks?
Risk management is systemic, structured and timely. A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.	•Risks are assessed using consistent criteria •Risk assessment process is consistent •Key risks are managed to within tolerance levels and reported on
Risk management is based on the best available information. The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modeling used or the possibility of divergence among experts.	•Review of potential sources of information for assessing risks; determine and select the most applicable, relevant and affordable •For complex risks, detailed analysis is performed – this may include more than one approach •Limitations, timeliness and variances are considered

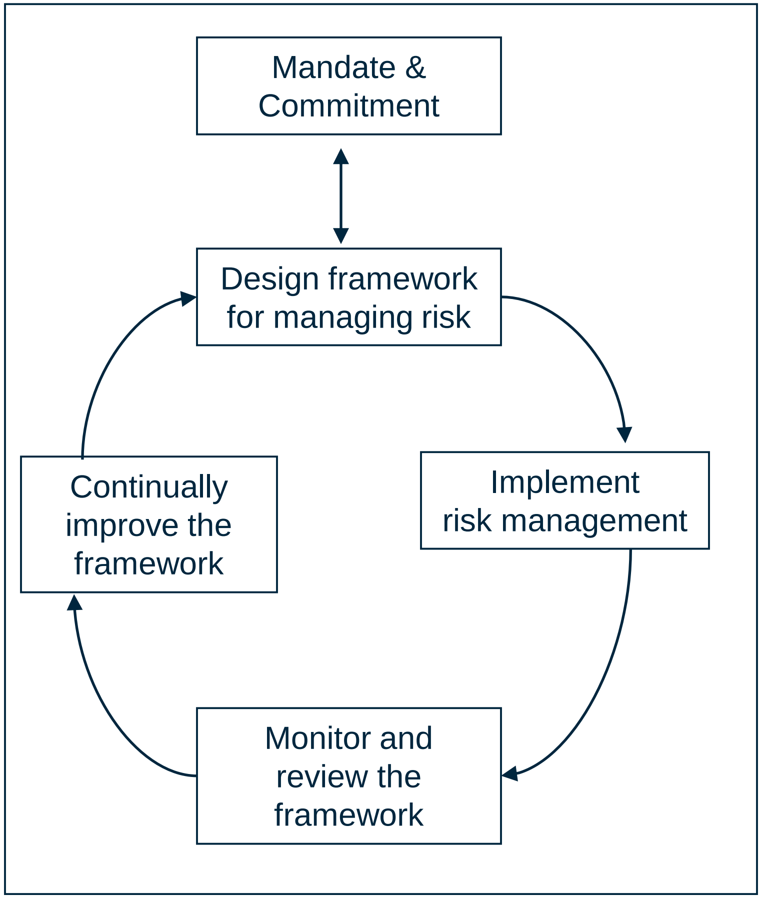
Using the Principles to Evaluate Progress

Principle	Evidence
Risk management is tailored. Risk management is aligned with the organization's external and internal context and risk profile.	•Annual review/update of context and profile •Documentation of the progress achieved in implementation plan and adjustments made as needed •How did you tailor the processes and framework to your organizational needs?
Risk management takes human and cultural factors into account. Risk management recognizes the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organization's objectives.	•Discussed and included in context and profile, and adjusted as changes are noted •Proof of the consideration of stakeholder perceptions •Do you engage appropriate stakeholders in the process?
Risk management is transparent and inclusive. Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.	•Plan for and results of including stakeholders – both internal and external •Communication plan – to whom, when, how much? •Were appropriate stakeholder opinions included in the determination of risk criteria? Risk assessment processes? And reported to?

Using the Principles to Evaluate Progress

Principle	Evidence
Risk management is dynamic, iterative and responsive to change. As external and internal events occur, context and knowledge change, monitoring and review take place, new risks emerge, some change, and others disappear. Therefore, risk management continually senses and responds to change.	•Constant monitoring of environment •Periodic review of context and operations •Have you adjusted and reviewed your framework as your organization changes? •Do your tools and trainings respond to the needs of your users?
Risk management facilitates continual improvement of the organization. Organizations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organization.	•Continual improvement model – documentation of review and improvements •Annual review of successes, problems and challenges, contributions of stakeholders, changes needed to framework, tools and training

Framework


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

Based upon a model of continual improvement, the framework is what will *sustain* your risk management efforts

This assures that you are consistent, *process*-focused and held accountable

Building the framework includes *planning* for implementation, monitoring & review and communication

Components of the Framework

- Understanding the organization & its context
- Establishing RM policy
- Accountability & Authority
- Integration into organizational processes
- Determining appropriate resources
- Establishing internal communication & reporting mechanisms
- Establishing external communication & reporting mechanisms

ISO/ANSI/ASSE 31000:2009
Risk management – Principles and guidelines

Components of the Framework

- **Understanding the organization & its context**
- Establishing RM policy
- Accountability & Authority
- Integration into organizational processes
- Determining appropriate resources
- Establishing internal communication & reporting mechanisms
- Establishing external communication & reporting mechanisms

ANSI/ASSE/ISO 31000:2009
Risk management – Principles and guidelines

Framework Example: Context

External Context

- Social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment
- Key drivers and trends that will have an impact on your organization
- Relationships with and perceptions & values of external stakeholders

Internal Context

- Governance, organizational structure, roles & accountabilities
- Policies, objectives & strategy
- Capabilities & resources
- Info systems
- Organizational culture
- Contractual relationships
- Relationships with, perceptions & values of internal stakeholders

Small Group Discussion

Key roles: Discussion leader, note taker, reporter (to large group)

- Describe the *external* context of your operations:
  - Social environment (describe the people you serve)
  - Cultural environment
  - Political landscape
  - Regulatory environment
  - Economic environment
  - Natural environment
  - Competitive environment
  - Stakeholders
  - Key drivers and trends

External Context Example

The External Context:	Local, regional, national & international influences
Social, cultural and legal environment	The Port has one of the most diverse portfolios in the nation, including 25 miles of prime waterfront property that hosts restaurants, retail, professional sports and diverse maritime operations as well as regional transportation facilities. Port assets include 50 pile-supported pier structures, 80 substructures, 285 commercial and industrial buildings, 25 miles of streets and sidewalks, and other assets such as historic structures, dry docks and a railroad track.
Regulatory environment	The State transferred port property to the City in 1952 via legislative act. The City/Port assumed $55 million of the State's bond debt and use of the waterfront is subject to the State's Public Trust Doctrine. This Doctrine, administered through the State Lands Commission, restricts certain private uses. The Conservation and Development Commission, a State regulatory agency, promotes public access to the waterfront and issues permits for development projects.
Financial environment	The Port is an enterprise agency and derives its income from Port tenants; it does not receive any General Fund revenue from the City. The Port recently developed a 10 year Capital Plan which includes pursuing public funding (through revenue bond issuances) and public-private partnerships to address the Port's critical capital needs.

Example of External Context

- Uncertain funding sources
- Affluent county but revenue is low
- New state mandates (re students and teachers) but no new funding
- Teacher associations & NEA are strong
- Diversified geography
- CO is a “purple” state
- CO is a “test case” state (e.g. legalization of marijuana)
- Large exodus of knowledge with retirements
- Active and aggressive community population
- PERA
- Diversity of available resources among member districts
- Continuing trend: fee for service
- Influence of the media
- Increase in construction
- A “pro-charter” school state
- SB 191
- Erosion of governmental immunity protections
- More natural hazards occurring
- Insurance market cycles/events

Example of Context – *Highlights*

Internal

- Oversight by board members with longevity & good working knowledge
- Good use of technology
- Strong personal values
- Committed and hard working staff and business partners
- Strong, solid reputation
- Financially stable

External

- Wide diversity among members and communities (liberal/conservative, cultural and resource differences)
- State funding ebbs & flows, but funding source is stable
- Statute requires colleges to insure facilities
- Lower wages + higher taxes in city versus member locations

How Do We Use This Information?

This informs the *framework* for managing risk:

- Implementation plan
- Policy and accountability
- How, when & to whom you will report
- How to incorporate stakeholders

It also might identify the potential need for a *risk management process*

And it informs and frames each risk management process

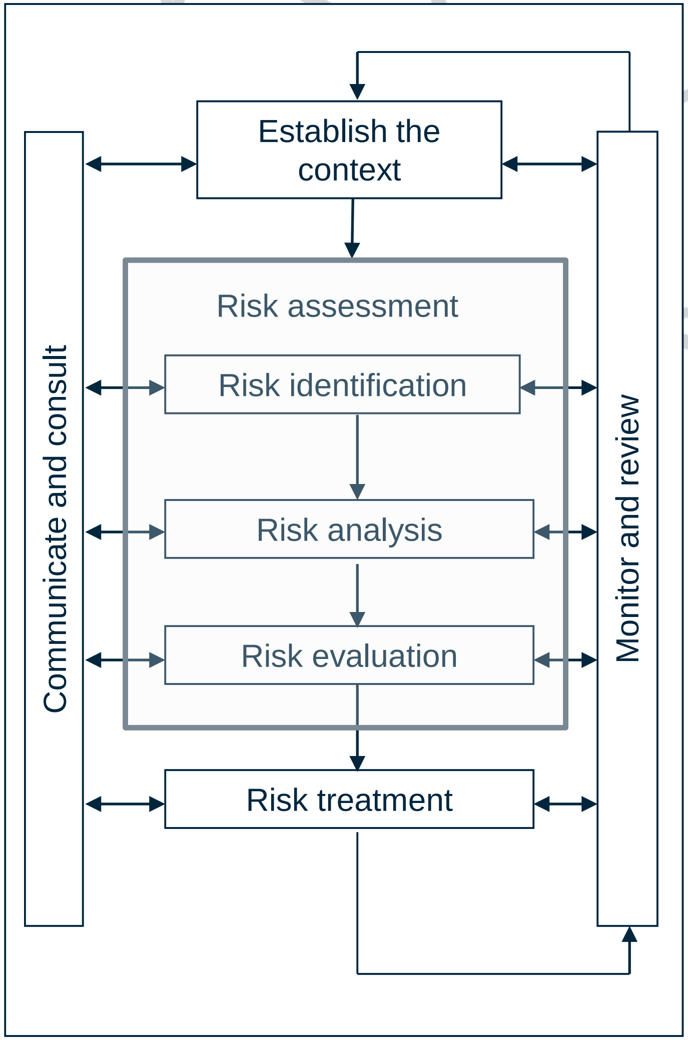
The Language of Risk

- Risk
- Risk identification
- Source, trigger
- Consequence
- Risk owner
- Risk management process

- Stakeholder
- Risk appetite
- Risk attitude
- Tolerance

RM Process

- The *context* applies to both the organization as a whole and the specific project, risk or portfolio of risks
- Several elements take stakeholder interest and *perceptions* into account
- Monitor and review – continually asks: “Do we have this right?”
- Communication and consultation is how the management of risk stays *connected* and *relevant*
- The same consistent process used across the organization, over and over again

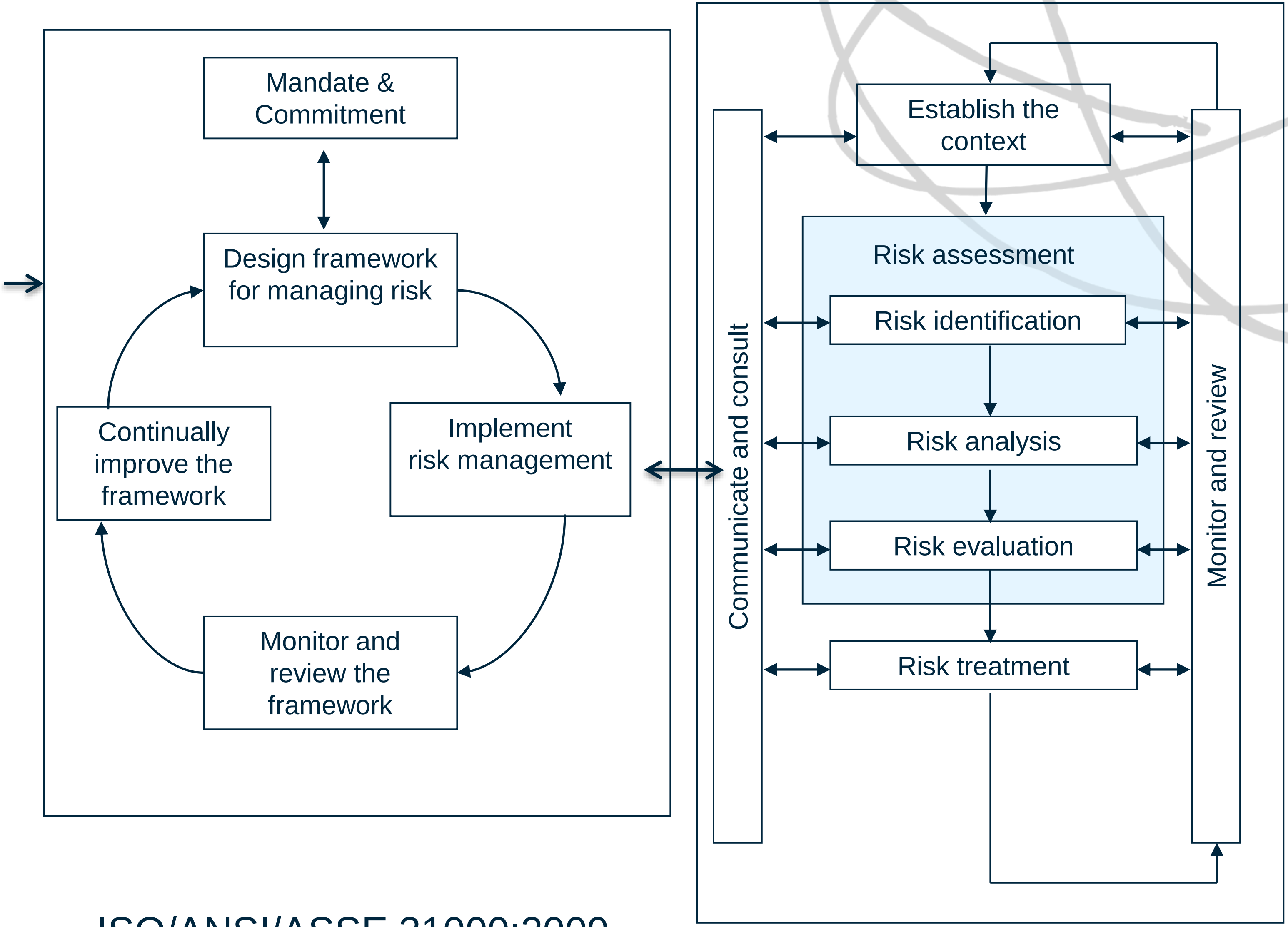


Principles

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

Framework

RM Process



Mandate & Commitment

Design framework for managing risk

Implement risk management

Monitor and review the framework

Continually improve the framework

Communicate and consult

Establish the context

Risk assessment

Risk identification

Risk analysis

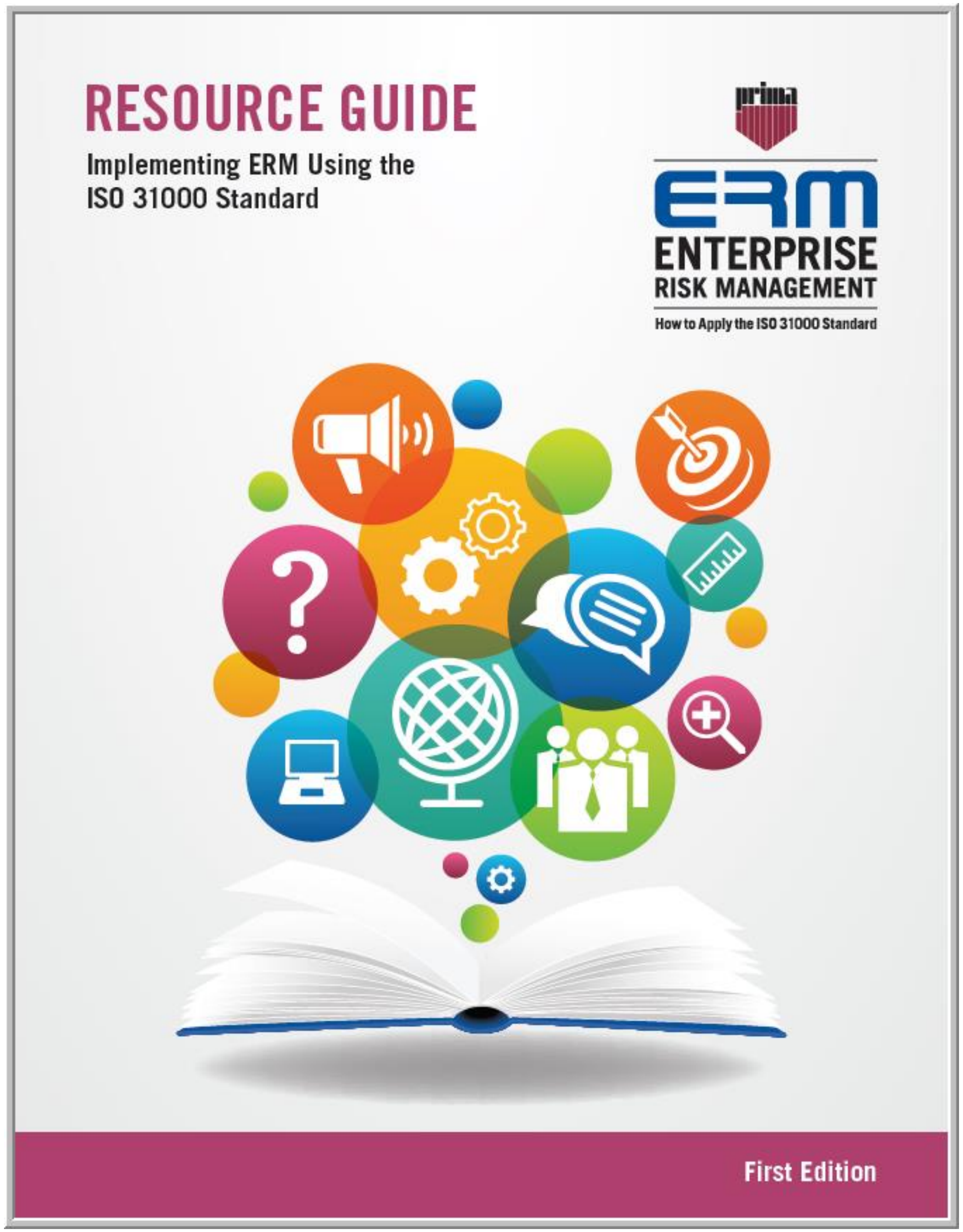
Risk evaluation

Risk treatment

Monitor and review

ISO/ANSI/ASSE 31000:2009

Used with permission



RESOURCE GUIDE

Implementing ERM Using the
ISO 31000 Standard

prima

ERM
ENTERPRISE
RISK MANAGEMENT
How to Apply the ISO 31000 Standard

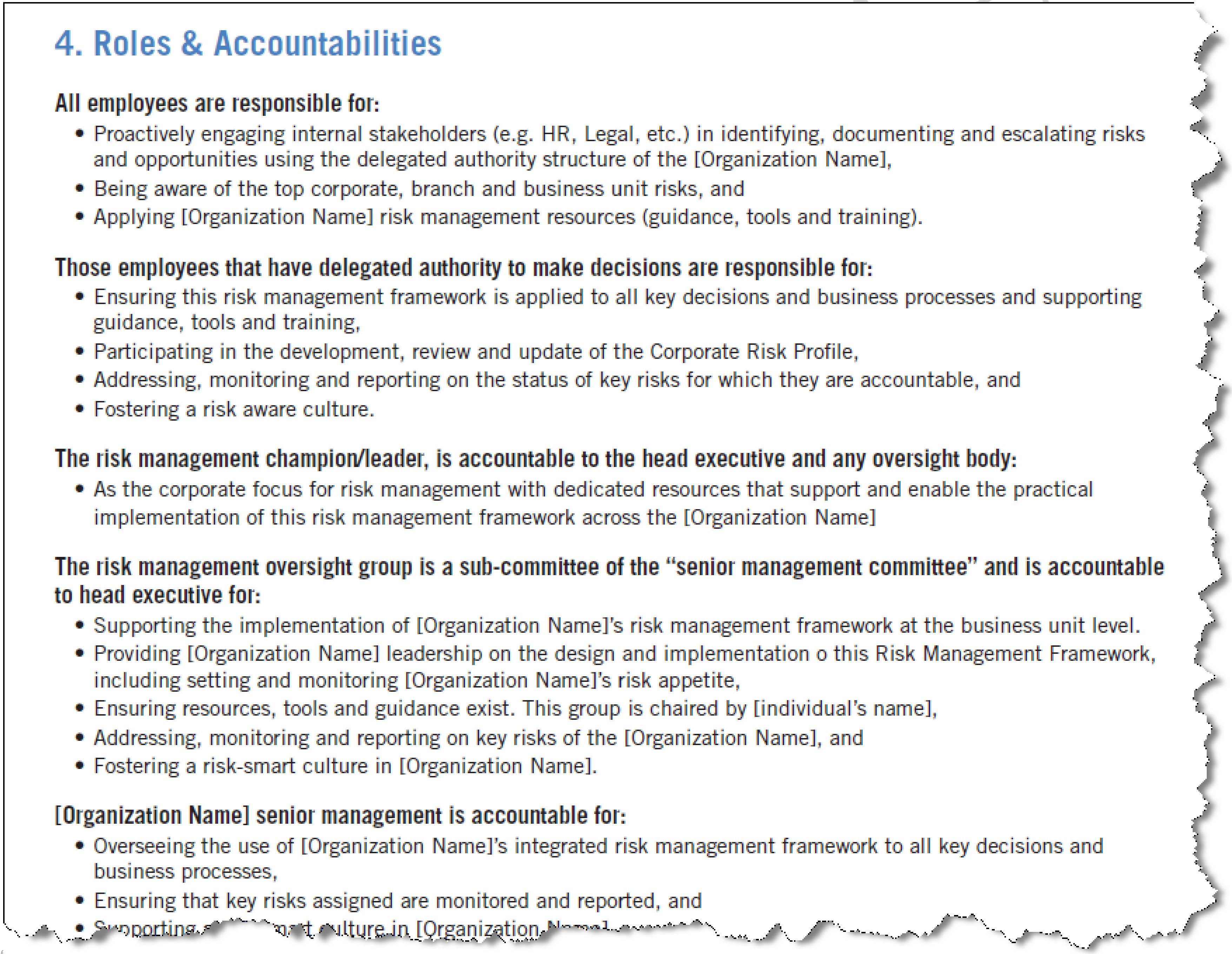
First Edition

Roles & Accountabilities

ISO Expectations re Accountability

Accountability is key to implementation

- Accountability for overall implementation, oversight and improvement of the *framework* for managing risk
- Accountability for the *management* of (key) risks



4. Roles & Accountabilities

All employees are responsible for:

- Proactively engaging internal stakeholders (e.g. HR, Legal, etc.) in identifying, documenting and escalating risks and opportunities using the delegated authority structure of the [Organization Name],
- Being aware of the top corporate, branch and business unit risks, and
- Applying [Organization Name] risk management resources (guidance, tools and training).

Those employees that have delegated authority to make decisions are responsible for:

- Ensuring this risk management framework is applied to all key decisions and business processes and supporting guidance, tools and training,
- Participating in the development, review and update of the Corporate Risk Profile,
- Addressing, monitoring and reporting on the status of key risks for which they are accountable, and
- Fostering a risk aware culture.

The risk management champion/leader, is accountable to the head executive and any oversight body:

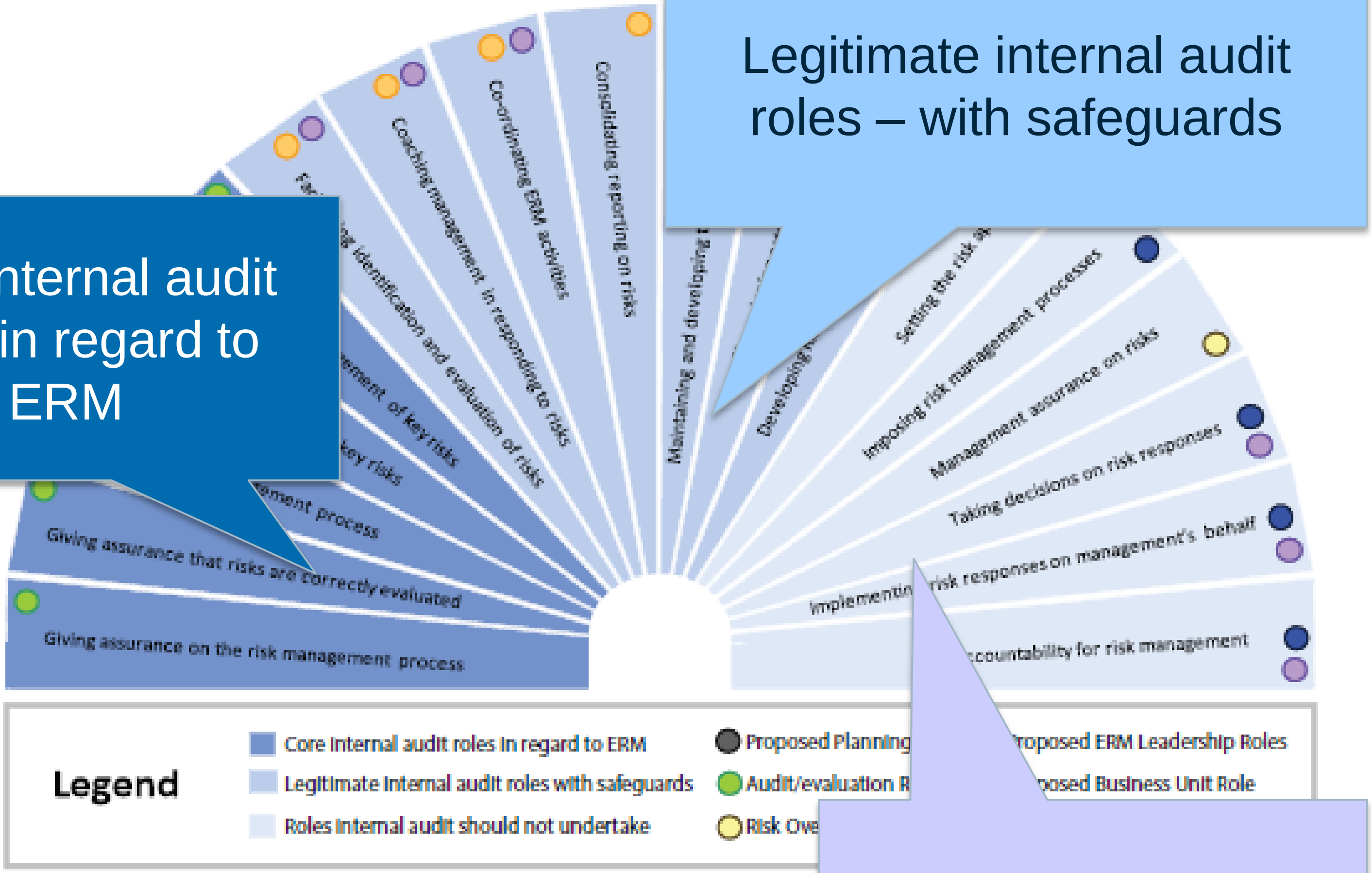
- As the corporate focus for risk management with dedicated resources that support and enable the practical implementation of this risk management framework across the [Organization Name]

The risk management oversight group is a sub-committee of the "senior management committee" and is accountable to head executive for:

- Supporting the implementation of [Organization Name]'s risk management framework at the business unit level.
- Providing [Organization Name] leadership on the design and implementation o this Risk Management Framework, including setting and monitoring [Organization Name]'s risk appetite,
- Ensuring resources, tools and guidance exist. This group is chaired by [individual's name],
- Addressing, monitoring and reporting on key risks of the [Organization Name], and
- Fostering a risk-smart culture in [Organization Name].

[Organization Name] senior management is accountable for:

- Overseeing the use of [Organization Name]'s integrated risk management framework to all key decisions and business processes,
- Ensuring that key risks assigned are monitored and reported, and
- Supporting a [illegible]mart culture in [Organization Name]

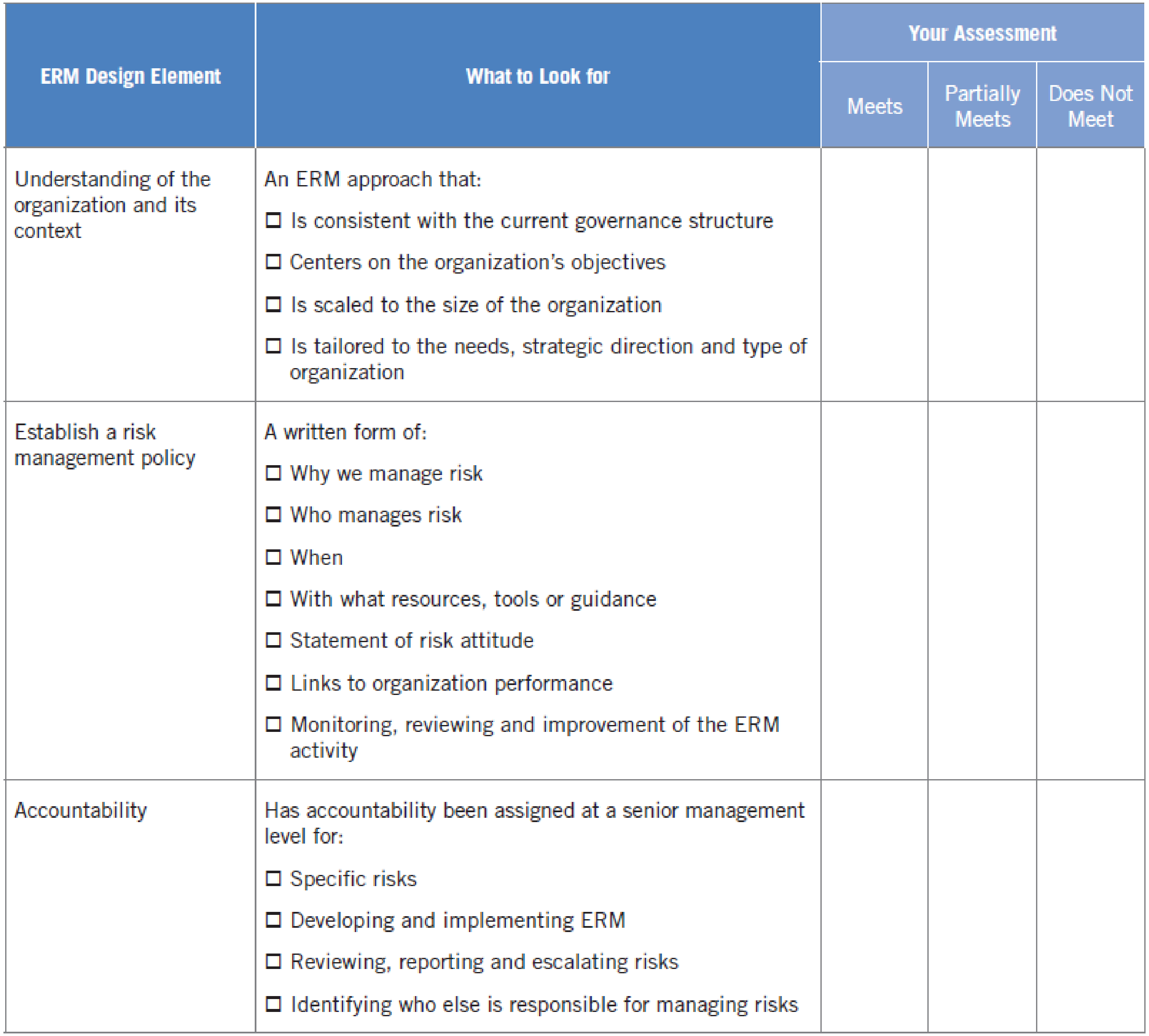

Giving assurance on the risk management process
Giving assurance that risks are correctly evaluated
...ement process
...key risks
...ment of key risks
Fa...
...g identification and evaluation of risks
Coaching management in responding to risks
Co-ordinating ERM activities
Consolidating reporting on risks
Maintaining and developing t...
Developing...
Setting the risk ap...
Imposing risk management processes
Management assurance on risks
Taking decisions on risk responses
Implementin... risk responses on management's behalf
...ccountability for risk management
Legend
Core internal audit roles in regard to ERM
Legitimate internal audit roles with safeguards
Roles internal audit should not undertake
Proposed Planning
Audit/evaluation R
Risk Ove
...roposed ERM Leadership Roles
...posed Business Unit Role

Core internal audit roles in regard to ERM

Legitimate internal audit roles – with safeguards

Roles internal audit should not undertake

[1] IIA position paper - The Role of Internal Auditing in Enterprise-wide Risk Management, September 29, 2004, www.theiia.org



ERM Design Element	What to Look for	Your Assessment		
		Meets	Partially Meets	Does Not Meet
Understanding of the organization and its context	An ERM approach that: ☐ Is consistent with the current governance structure ☐ Centers on the organization's objectives ☐ Is scaled to the size of the organization ☐ Is tailored to the needs, strategic direction and type of organization			
Establish a risk management policy	A written form of: ☐ Why we manage risk ☐ Who manages risk ☐ When ☐ With what resources, tools or guidance ☐ Statement of risk attitude ☐ Links to organization performance ☐ Monitoring, reviewing and improvement of the ERM activity			
Accountability	Has accountability been assigned at a senior management level for: ☐ Specific risks ☐ Developing and implementing ERM ☐ Reviewing, reporting and escalating risks ☐ Identifying who else is responsible for managing risks			

Excerpt from “Implementing ERM Using ISO 31000” – PRIMA 2015

Working Examples

Public sector and higher education

- CRO leads; Audit participates in Advisory Committee meetings and uses info to develop audit plan
- RM + Audit + Compliance lead together; Audit incorporates info into audit plan
- RM leads; Audit is a completely separate function

- Never the ‘twain shall meet…

Key Points re Roles

And “Who’s on First?”

- Must be tailored to your operations
- Needs to acknowledge expertise and leadership
- Ideally, discussed and agreed upon by all
- Should be incorporated into your implementation plan & policy

Open Discussion

Any examples we could share? Insights?

- What variations exist within this group?
- What's working – and not working?
- Any lessons learned?

Implementation Plan

How can I move my organization forward?

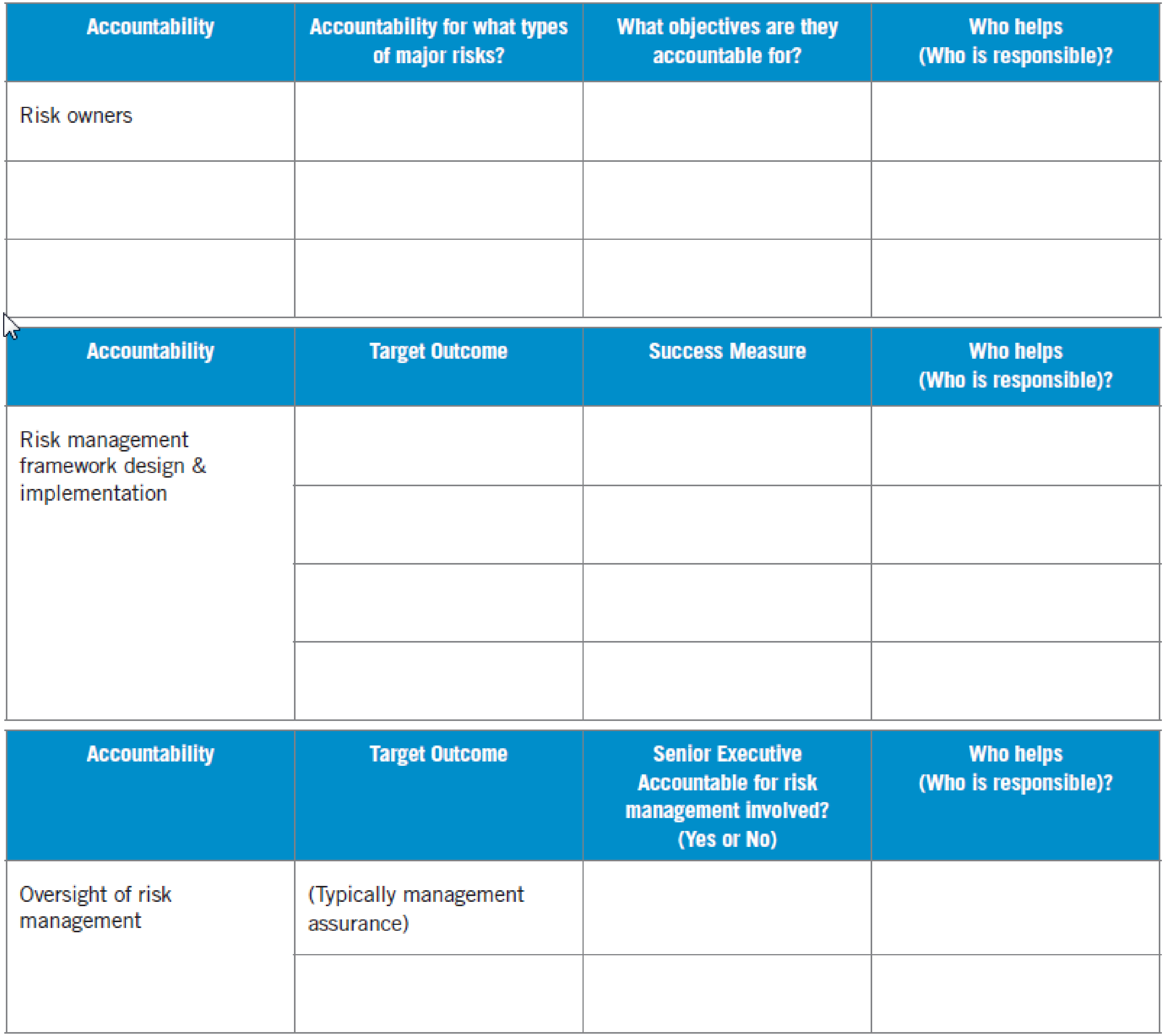
- ERM assessment –

  “Start where you are”
- Excerpts from PRIMA training
- Ideas for implementation
- Obstacle and barriers

Ways to Approach Implementation

This *must* be tailored to *your* organization and its context!

- Assess current RM approach
- Engage a group!
- Focus on key principles for *why*
- Link to objectives and strategy
- Make a plan – and then track & report



Accountability	Accountability for what types of major risks?	What objectives are they accountable for?	Who helps (Who is responsible)?
Risk owners			

Accountability	Target Outcome	Success Measure	Who helps (Who is responsible)?
Risk management framework design & implementation			

Accountability	Target Outcome	Senior Executive Accountable for risk management involved? (Yes or No)	Who helps (Who is responsible)?
Oversight of risk management	(Typically management assurance)		

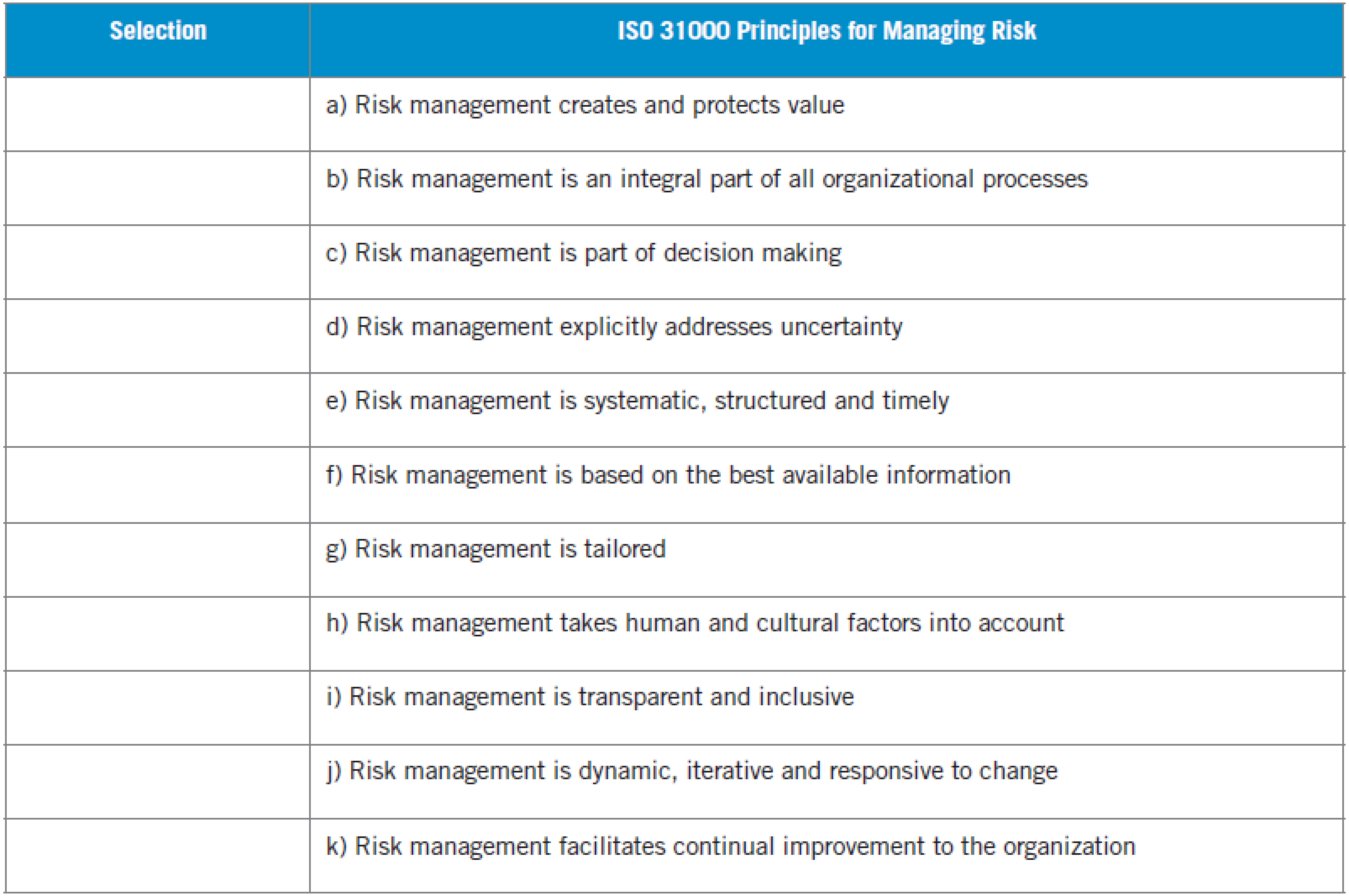
Excerpt from “Implementing ERM Using ISO 31000” – PRIMA 2015

Engage a Group

This *must* be tailored to *your* organization and its context!

- Create an ERM study group
- Create an ERM Advisory Group
- Expand an existing committee
- Create multiple layers:
  - – Advisory Group (leaders)
  - – Working Group (doers)

Consider the size and nature of your organization and select the principles that will support organizational objectives and leadership initiatives.



Selection	ISO 31000 Principles for Managing Risk
	a) Risk management creates and protects value
	b) Risk management is an integral part of all organizational processes
	c) Risk management is part of decision making
	d) Risk management explicitly addresses uncertainty
	e) Risk management is systematic, structured and timely
	f) Risk management is based on the best available information
	g) Risk management is tailored
	h) Risk management takes human and cultural factors into account
	i) Risk management is transparent and inclusive
	j) Risk management is dynamic, iterative and responsive to change
	k) Risk management facilitates continual improvement to the organization

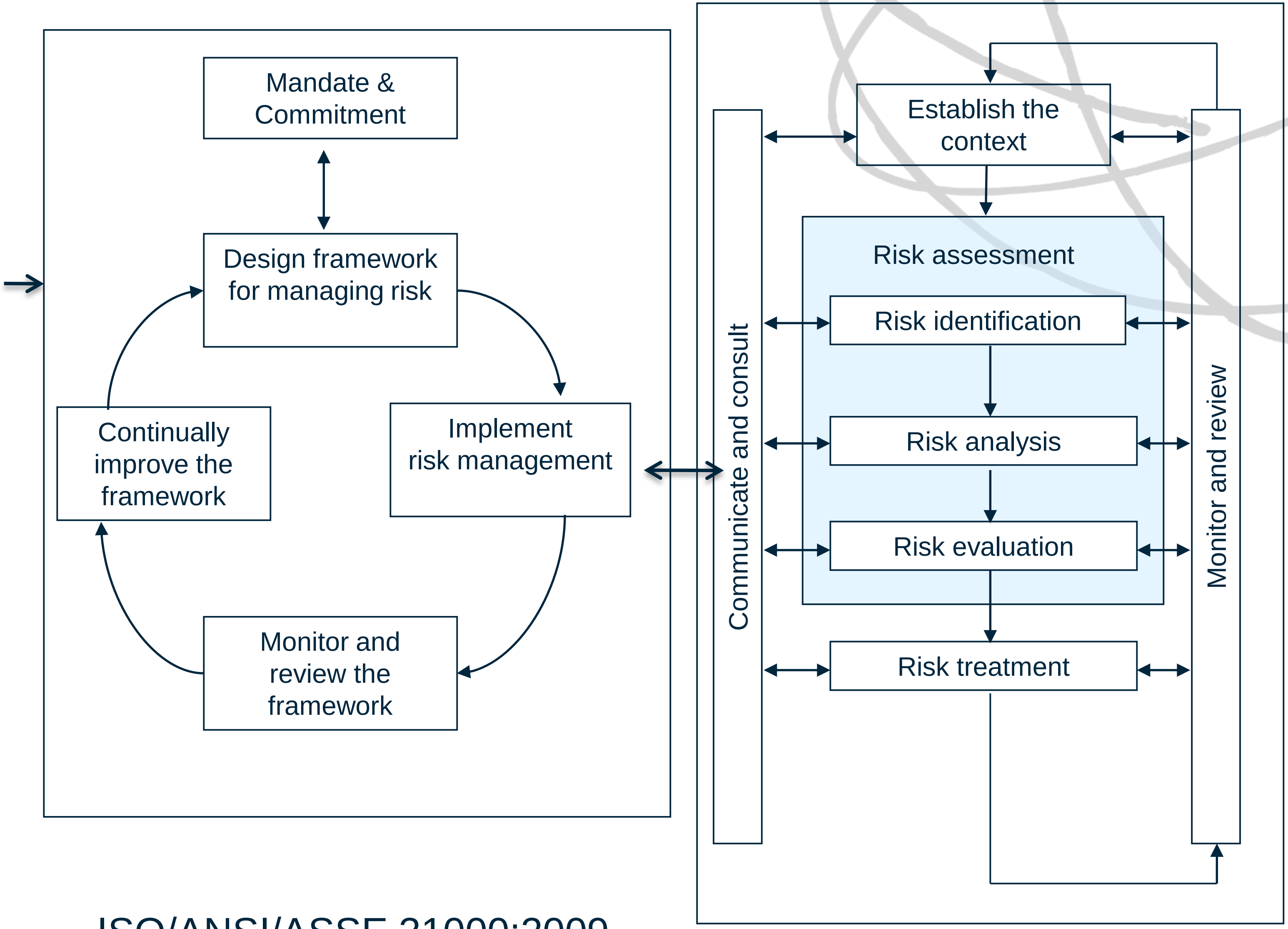
Excerpt from “Implementing ERM Using ISO 31000” – PRIMA 2015

Principles

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

Framework

RM Process



Mandate & Commitment

Design framework for managing risk

Implement risk management

Monitor and review the framework

Continually improve the framework

Establish the context

Communicate and consult

Monitor and review

Risk assessment

Risk identification

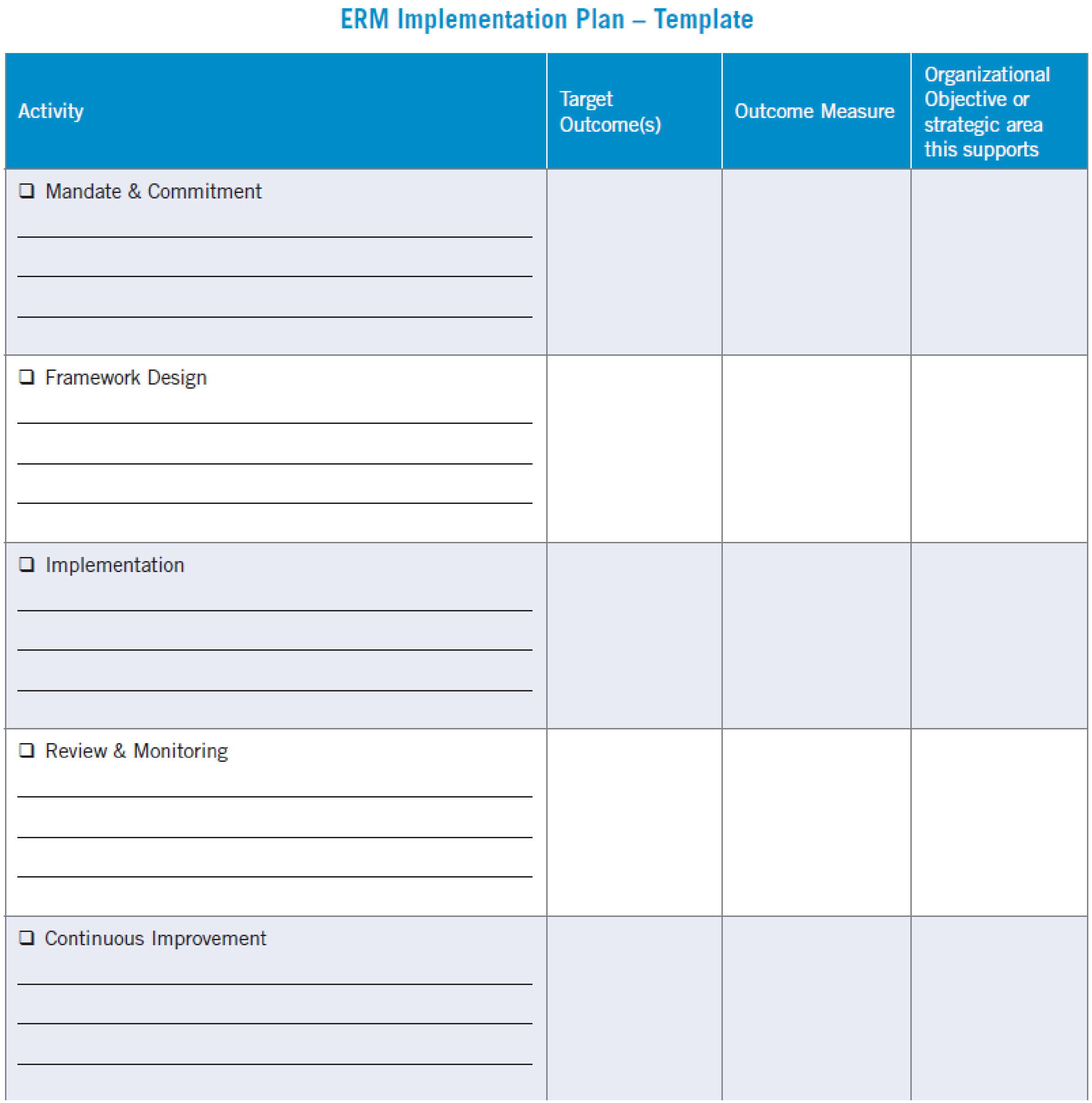
Risk analysis

Risk evaluation

Risk treatment

ISO/ANSI/ASSE 31000:2009

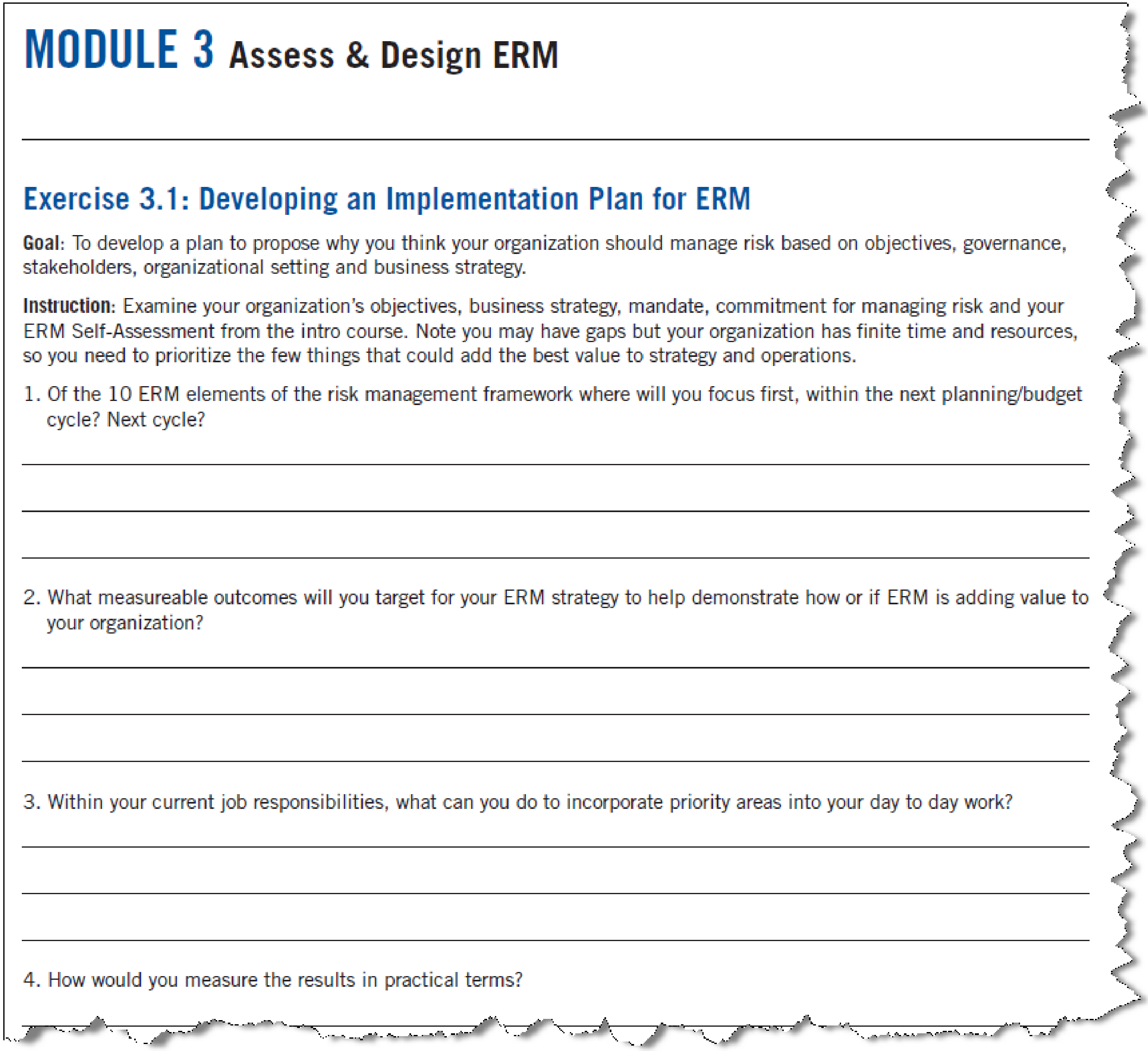
Used with permission



ERM Implementation Plan – Template

Activity	Target Outcome(s)	Outcome Measure	Organizational Objective or strategic area this supports
□ Mandate & Commitment			
□ Framework Design			
□ Implementation			
□ Review & Monitoring			
□ Continuous Improvement			

Excerpt from “Implementing ERM Using ISO 31000” – PRIMA 2015



MODULE 3 Assess & Design ERM

Exercise 3.1: Developing an Implementation Plan for ERM

Goal: To develop a plan to propose why you think your organization should manage risk based on objectives, governance, stakeholders, organizational setting and business strategy.

Instruction: Examine your organization's objectives, business strategy, mandate, commitment for managing risk and your ERM Self-Assessment from the intro course. Note you may have gaps but your organization has finite time and resources, so you need to prioritize the few things that could add the best value to strategy and operations.

1. Of the 10 ERM elements of the risk management framework where will you focus first, within the next planning/budget cycle? Next cycle?

2. What measureable outcomes will you target for your ERM strategy to help demonstrate how or if ERM is adding value to your organization?

3. Within your current job responsibilities, what can you do to incorporate priority areas into your day to day work?

4. How would you measure the results in practical terms?

Developing an Implementation Plan

Don’t do this alone!!

- Articulate *why* ERM is important to your organization
- Create a multi-year process with clear steps and measurable outcomes
- Incorporate current reality, skills and support
- Rinse and repeat!

Implementation Phases

Gallagher's ERM Practice Group – in Alignment with ISO 31000

Phase 1:

Commitment and Framework

- Build the case for ERM
- Understand your mandate and commitment
- Review roles and capabilities
- Begin to develop a sustainable framework

Phase 2:

Leadership and Context

- Train ERM leaders and advisory groups
- Describe the context of operations and identify key stakeholders
- Define roles and responsibilities
- Create an implementation plan

Phase 3:

Risk Assessment and Ownership

- Organize a broader approach to risk assessment
- Identify, analyze and evaluate key risks
- Assign risk owners
- Plan for data management, reporting and communication

Phase 4:

Risk Treatment and Integration

- Develop risk treatment plans and protocols
- Create appropriate progress reports
- Train employees & key stakeholders
- Integrate risk oversight into position descriptions, reviews and onboarding

Phase 5:

Monitor, Review and Continually Improve

- Review ERM goals and implementation plan
- Assess progress against goals, ISO principles and key performance indicators
- Identify opportunities for improvement
- Reiterate the process

Obstacles/Barriers

What can we learn from the mistakes of others?

- Rushing to the risk register, over-focus on “the product”
- Underdevelopment of the framework
- Not linking risk management to what matters most
- Overlooking everyday decision making and management
- Lack of leadership (gravitas), skills or engagement
- Sustaining the effort during times of transition
- Failure to continually improve

Resources

Where can I find help?

- Sources of information
- Training opportunities
- Networking opportunities

Sources of Information

Options in the U.S.

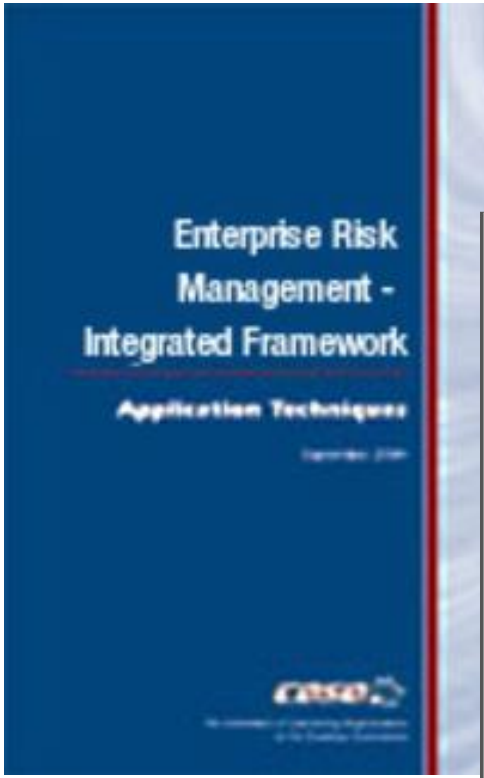
- ANSI/ASSE/ISO 31000 – the *only* international standard on risk management – 2009
- COSO ERM Framework – 2004
- The IIA Practice Guide: "Assessing the Adequacy of Risk Management Using ISO 31000:
- "Risk Management – An Accountability Guide for University and College Boards" by Janice Abraham – AGB & UE – 2013
- Consulting firms – KPMG, Protiviti, Deloitte, PwC & brokerage firms, too
- GRC – Governance, Risk & Compliance (software and consulting)

ANSI
AMERICAN NATIONAL STANDARD
ANSI/ASSE/ISO Guide 73 (Z690.1-2011)
Vocabulary for Risk Management
National Adoption of
ISO Guide 73:2009
ISO/ANSI/ASSE Technical Report
Risk Management—Guidance for
the Implementation of ISO 31000
ANSI/ASSE/IEC/ISO 31010 (Z690.3-2011)
Risk Assessment Techniques
National Adoption of
IEC/ISO 31010:2009
American Society of Safety Engineers

www.asse.org

ANSI/ASSE/ISO Risk Management Standards Package

ISO/ANSI/ASSE/TR-31004-2014 (Z690 TR-2014) Risk Management-Guidance for the Implementation of ISO 31004
(identical national adoption of ISO/TR 31004:2013)
ANSI/ASSE/ISO Guide 73 (Z690.1-2011) Vocabulary for Risk Management
(identical national adoption of ISO Guide 73:2009)
ANSI/ASSE/ISO 31000 (Z690.2-2011) Risk Management—Principles and Guidelines
(identical national adoption of ISO 31000:2009)
ANSI/ASSE/IEC/ISO 31010 (Z690.3-2011) Risk Assessment Techniques
(identical national adoption of ISO/IEC 31010:2009)

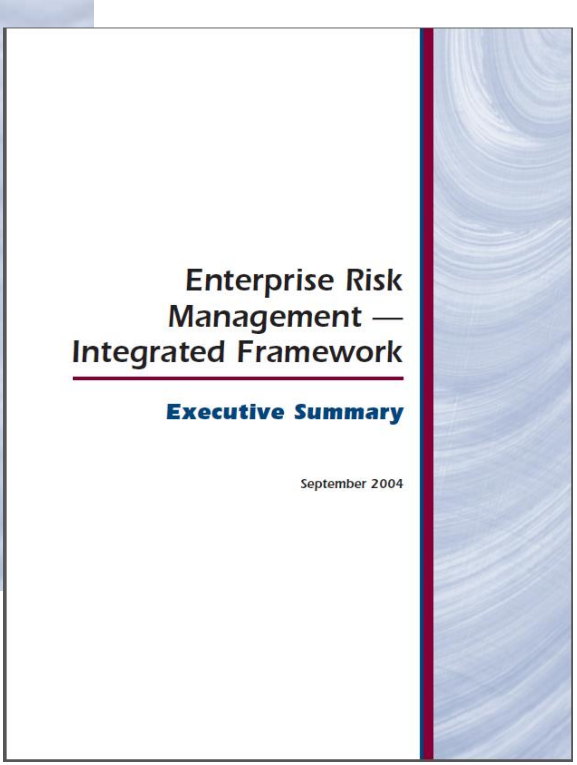


Enterprise Risk Management - Integrated Framework

Application Techniques

September 2004

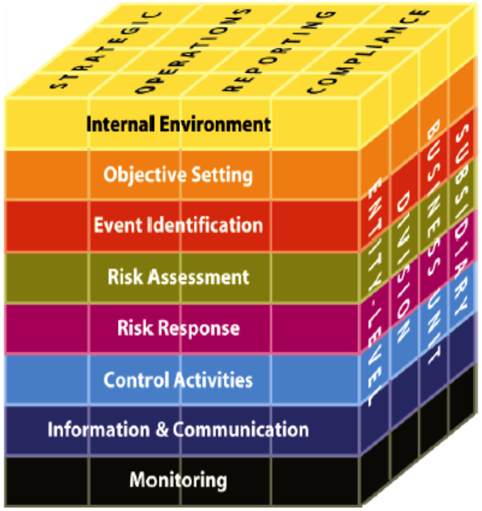
COSO



Enterprise Risk Management — Integrated Framework

Executive Summary

September 2004



www.coso.org

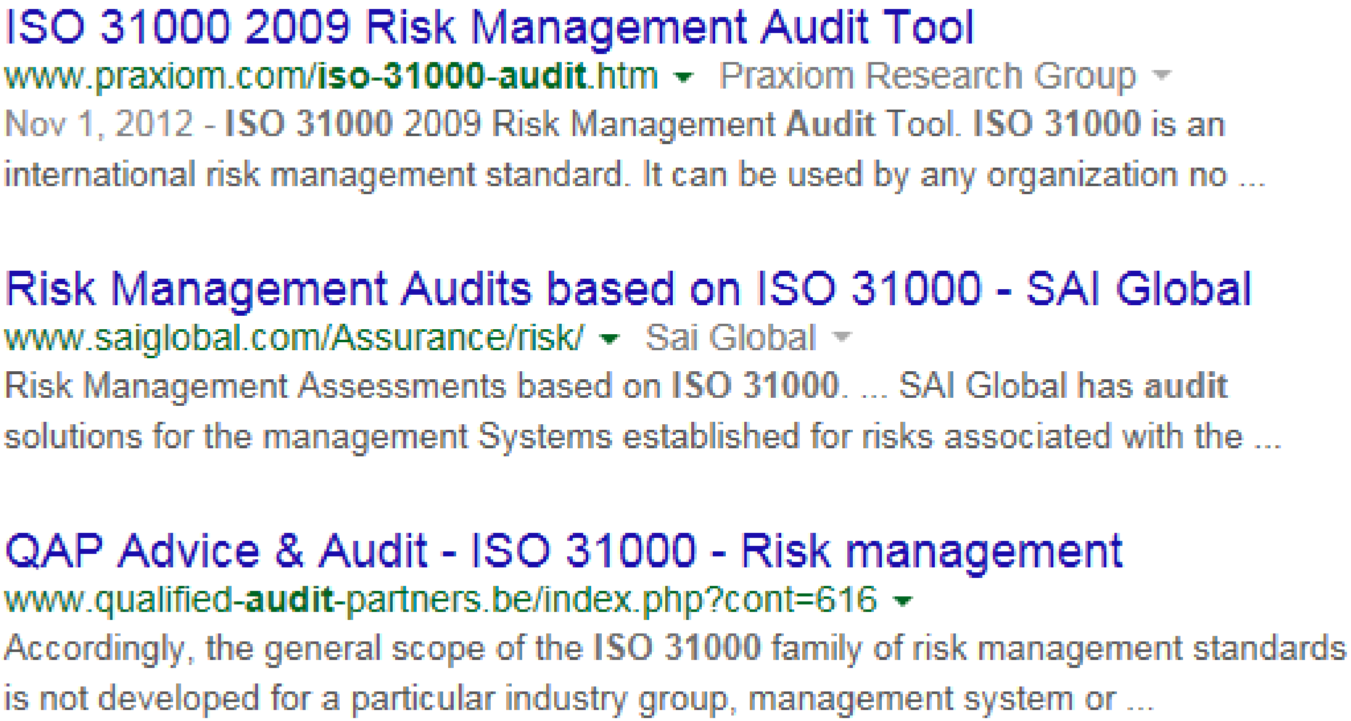
The IIA Practice Guide

Assessing the Adequacy of Risk Management Using ISO 31000

- Three approaches to assurance:
  - Process elements
  - Maturity model
  - Principles
- Assurance process should be tailored to the organization’s needs
- Intended to measure the effectiveness of risk management and form conclusion about maturity
- Establishing a suitable framework is one key criteria

www.theiia.org

A quick “google” search yielded…



ISO 31000 2009 Risk Management Audit Tool

www.praxiom.com/**iso-31000-audit**.htm ▾ Praxiom Research Group ▾

Nov 1, 2012 - **ISO 31000** 2009 Risk Management **Audit** Tool. **ISO 31000** is an international risk management standard. It can be used by any organization no ...

Risk Management Audits based on ISO 31000 - SAI Global

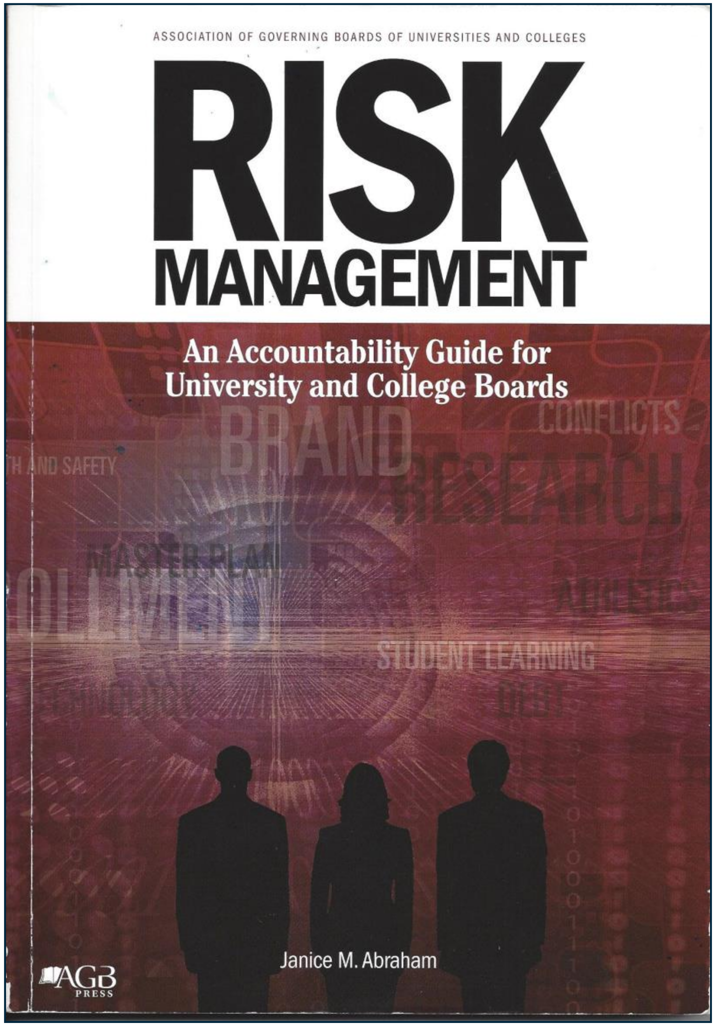
www.saiglobal.com/Assurance/risk/ ▾ Sai Global ▾

Risk Management Assessments based on **ISO 31000**. ... SAI Global has **audit** solutions for the management Systems established for risks associated with the ...

QAP Advice & Audit - ISO 31000 - Risk management

www.qualified-**audit**-partners.be/index.php?cont=616 ▾

Accordingly, the general scope of the **ISO 31000** family of risk management standards is not developed for a particular industry group, management system or ...



ASSOCIATION OF GOVERNING BOARDS OF UNIVERSITIES AND COLLEGES

RISK MANAGEMENT

An Accountability Guide for University and College Boards

Janice M. Abraham

AGB PRESS

- Published in 2013 by AGB Press, the Association of Governing Boards of Universities and Colleges and United Educators Insurance, a Reciprocal Risk Retention Group
- www.agb.org or 800.356.6317

How to Implement ERM Using ISO 31000

- Three-part training:
  - Webinar – How to apply the standard
  - Workshop – Introduction to ERM & ISO 31000
  - Workshop – Implementing ERM
- Info at www.primacentral.org or www.urmia.org
- PRIMA = Public Risk Management Association
- URMIA = University Risk Management and Insurance Association

This program funded by the Public Entity Risk Institute.

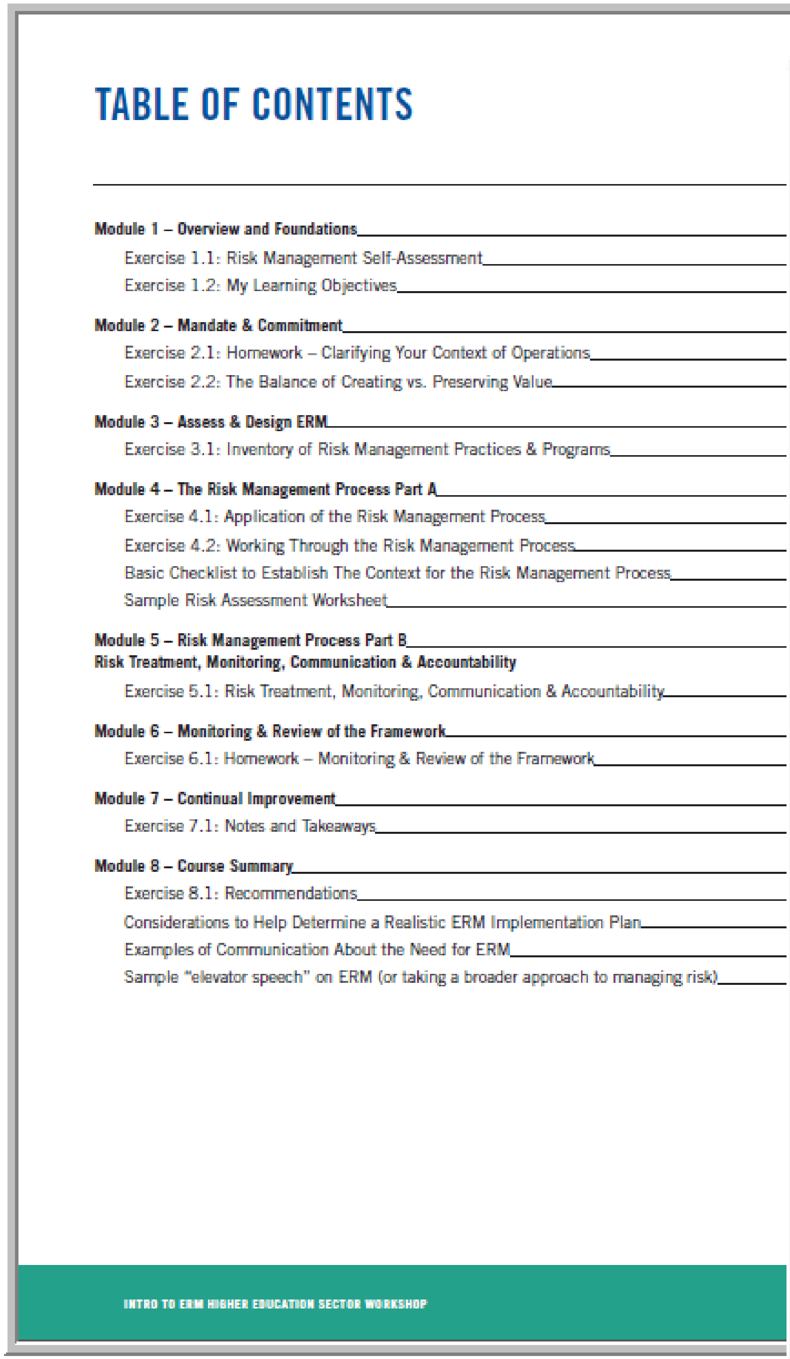
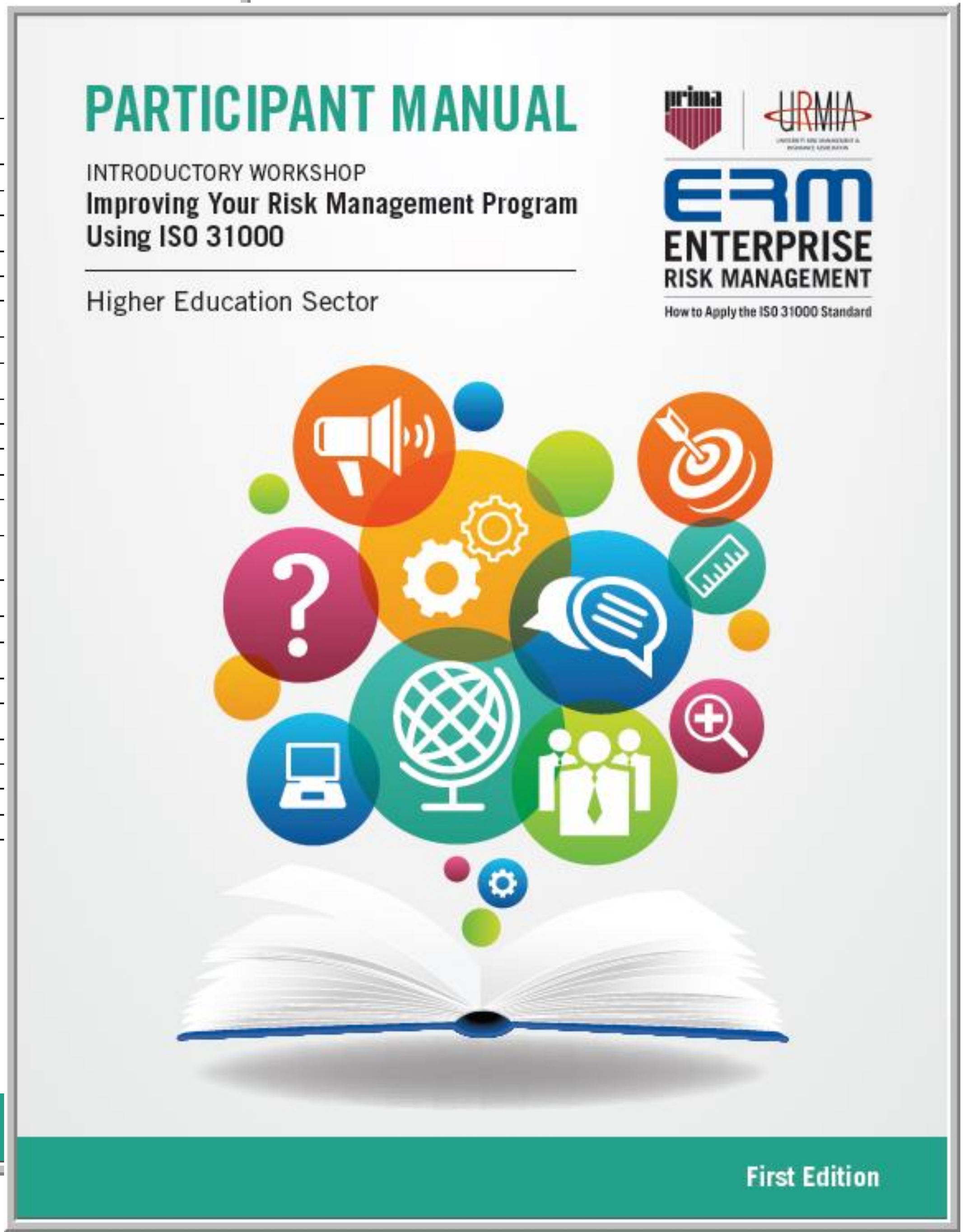


TABLE OF CONTENTS



PARTICIPANT MANUAL

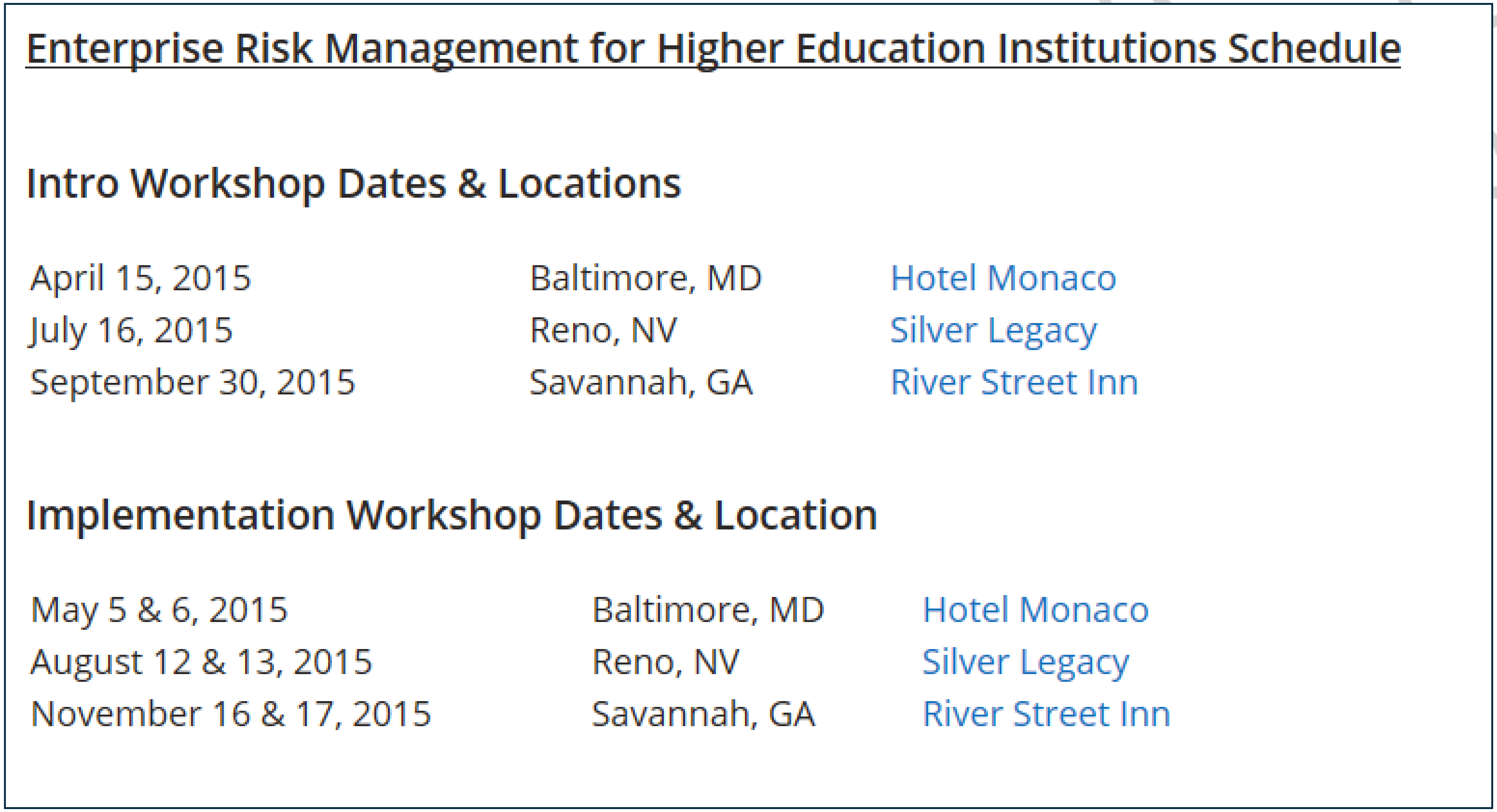
INTRODUCTORY WORKSHOP

Improving Your Risk Management Program Using ISO 31000

Higher Education Sector

First Edition

www.primacentral.org



Enterprise Risk Management for Higher Education Institutions Schedule

Intro Workshop Dates & Locations

April 15, 2015	Baltimore, MD	Hotel Monaco
July 16, 2015	Reno, NV	Silver Legacy
September 30, 2015	Savannah, GA	River Street Inn

Implementation Workshop Dates & Location

May 5 & 6, 2015	Baltimore, MD	Hotel Monaco
August 12 & 13, 2015	Reno, NV	Silver Legacy
November 16 & 17, 2015	Savannah, GA	River Street Inn

In 2016 – offered in New York?

Other Training & Networking Opportunities

- NYSICA and NY PRIMA meetings
- PRIMA National Conference
- PRIMA online – www.primacentral.org
- RIMS – national conference & ERM trainings
- Where else do you go??

Thank You!!

Dorothy Gjerdrum
Senior Managing Director – Public Sector
Managing Director – ERM Practice
Arthur J. Gallagher & Co.

952.358.7551
Dorothy_Gjerdrum@ajg.com