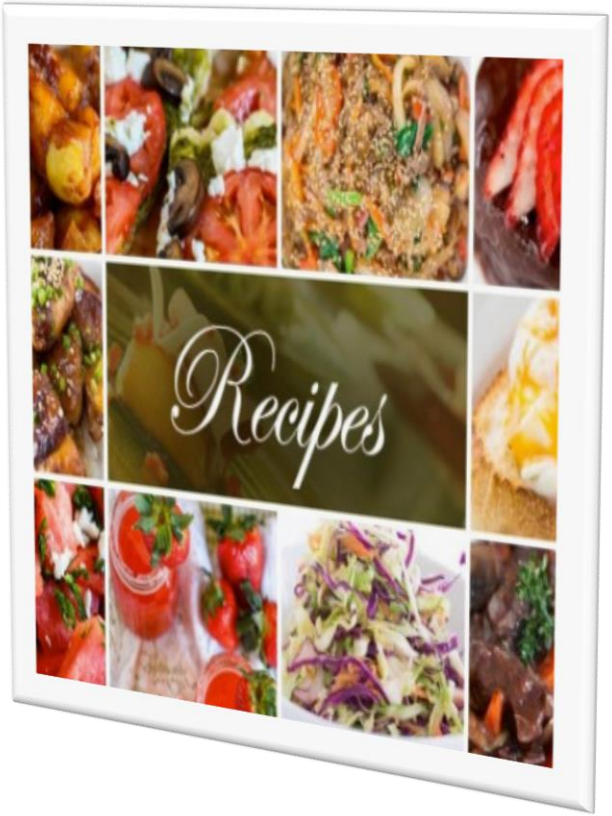
A NEW "COOKBOOK" STANDARD FOR RISK ASSESSMENTS

EVERYTHING YOU WANT TO KNOW ABOUT THE NEW AMERICAN NATIONAL RISK MANAGEMENT STANDARD

THE ANSI/ASIS/RIMS RISK ASSESSEMENT STANDARD RA.1-2015



RIMS Oregon Chapter Event
May 19, 2016

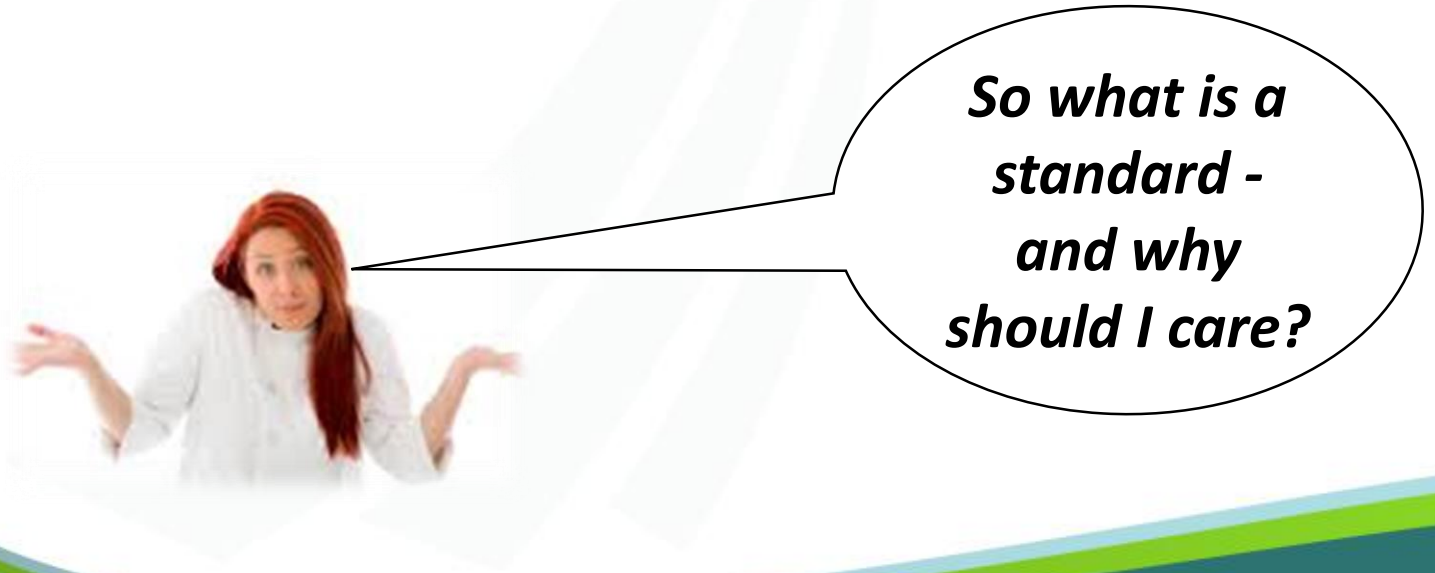
Carol Fox, ARM
Vice President, Strategic Initiatives
RIMS, *the risk management society*™

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

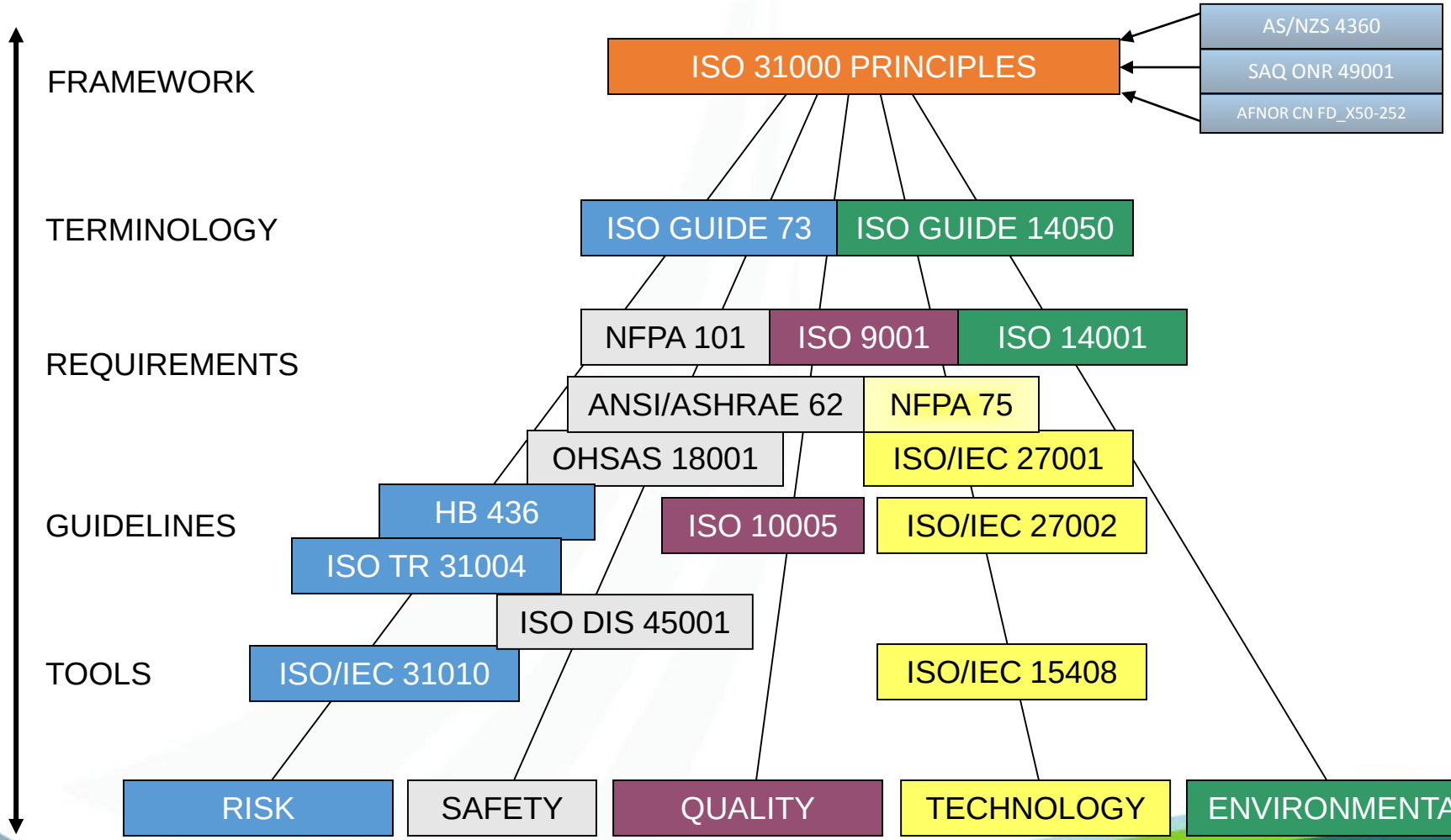
Just like fine meals, risk assessment programs can be flavored to satisfy the tastes of organizations, their different purposes and the decisions being made. Even so, certain basic ingredients are essential for feeding the organizational need in evaluating the "effect of uncertainty on the achievement of strategic, operational and tactical objectives".

Find out how you can prepare these "ingredients and flavorings" - as covered in the recently published national ANSI/ASSE/RIMS Risk Assessment Standard - within your own organization.



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Standards Development in Risk Management



© 2010 Risk and Insurance Management Society, Inc. All rights reserved.

3

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

RIMS Approved as Accredited Standards Organization by American National Standards Institute

7/15/2011

NEW YORK (July 15, 2011) — RIMS today announced that it has been approved as an accredited standards development organization by the American National Standards Institute (ANSI) Executive Standards Council. This status will increase RIMS' profile in the standards and practices arena by enabling it to take a lead role in shaping and developing risk management standards.

Collaborating with other associations and SDOs on standards development

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

WHY PARTNER WITH ASIS INTERNATIONAL?

Largest professional society for security management practitioners

- Founded in 1955
- More than 38,000 Members in 133 Countries
- 218 Chapters in 60 countries
- 31 Councils; ranging from disaster management, financial services, physical security, IT security, supply chain security, utilities, hotels and hospitality and retail
- Recognized as international body by ISO – Liaison Status
- Chair and Secretariat of ISO/PC284 – Security Operations
- Recognized as European body by CEN – Liaison Status
- Accredited by ANSI as American SDO – OPEN TO MEMBERS GLOBALLY
- Standards Development and Training
- Credentialing and Certification of Security Professionals

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

AGENDA

THE “KITCHEN”

THE “COOKBOOK”

THE BASIC INGREDIENTS

THE “RECIPES”

THE FLAVORINGS

ADAPTING THE RECIPES

VOILA!

QUESTIONS

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

THE “KITCHEN”

AKA Risk Management

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

THE ROLE OF RISK MANAGEMENT HAS CHANGED

FROM MERELY CLEANING UP THE MESSES

Event Focused

TO BEING PART OF THE MANAGEMENT TEAM

Objectives Focused

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

RISK MANAGEMENT

- **IS a discipline for building a strong organizational foundation**
- **IS a competency for informed decision making**
- **IS a process for maximizing opportunities while minimizing harm and loss**
- **IS used to support proactive measures to enhance agility and the adaptive capacity of an organization**
- **IS NOT an end in and of itself, but a capability for achieving objectives**

MUCH MORE THAN A PROCESS

CHANGE IN PERSPECTIVE

Expanding organizational risk management competencies

Reactive mode	**Proactive mode**
Event-focused	**Objectives-focused**
Post-action response	**Predictive indicators**
Afterthought	**Foresight**
Transactional	**Strategic**
Protecting value	**Creating and capturing value**

Risk defined as the “effect of uncertainty on the achievement of strategic, tactical, and operational objectives”

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

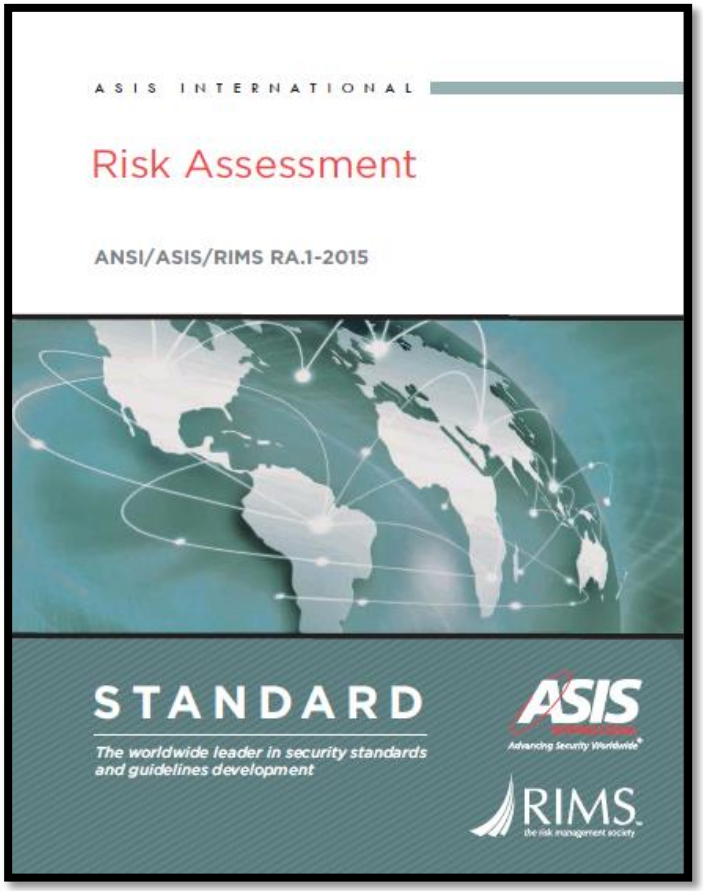
Joint Copyright ©ASIS and RIMS 2016

A STANDARD IS LIKE AN ITALIAN RECIPE

- **“TAILORED” to the “taste” (needs) of the organization.**
- **Tells you what – you decide how.**
- **Risk management that recognizes that risk assessments are about value creation, products, and services – NOT ABOUT RISK MANAGEMENT.**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016



THE “COOKBOOK”

ANSI/ASIS/RIMS.RA.1-2015 Risk Assessment

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

- Provides guidance for establishing a ***risk assessment program*** and ***conducting individual risk assessments*** consistent with the ISO 31000:2009 Risk management — Principles and Guidelines, and the COSO Enterprise Risk Management (ERM) framework
- Provides guidance on conducting risk assessments for risk and resilience based management system standards, including ***principles*** of risk assessments, managing the risk assessment program, and conducting risk assessments, as well as ***evaluation of competence of persons involved in the risk assessment process***
- Describes the process for conducting risk assessments consistent with the ***Plan-Do-Check-Act Model***, and
- Provides the informational basis necessary for decision makers to **make informed decisions** about managing risks in the organization and its supply chain.

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

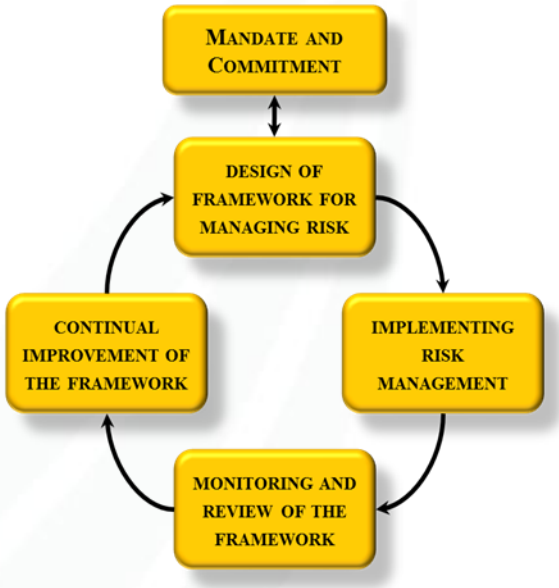
Uses ISO 31000:2009 as a Base

ISO 31000:2009 Risk Management – Principles and Guidelines

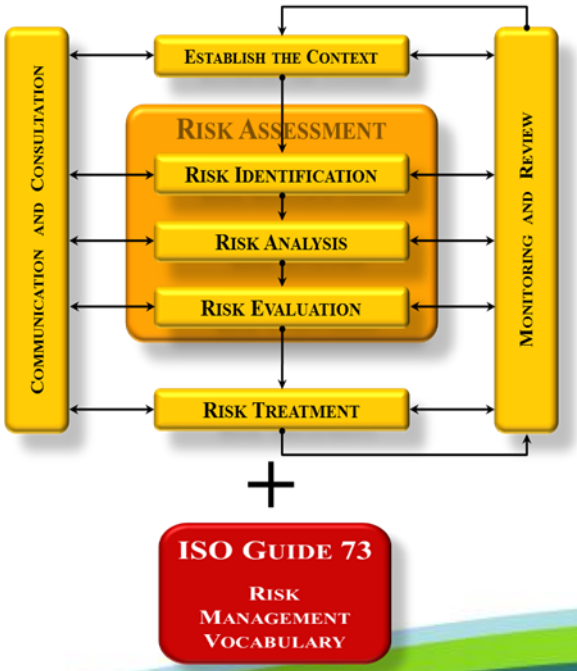
Principles

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

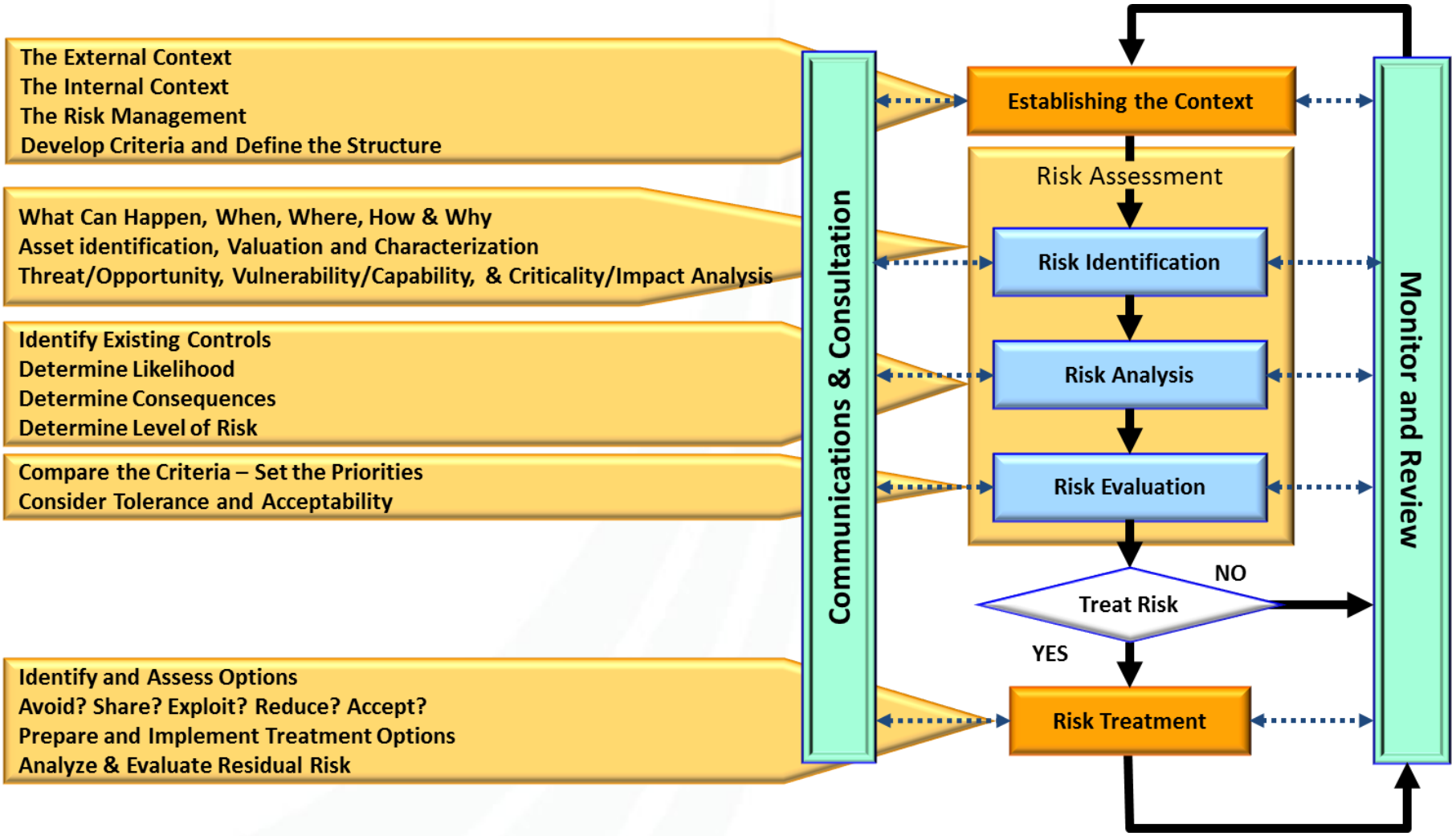


Process



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016



Expands the Process

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

THE BASIC INGREDIENTS

Building a consistent program approach –
NOT a new management system

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Planning the Meal: Understanding YOUR Organization

- What is important to the organization?
- What are short, medium, and long-term strategic, tactical and operational objectives?
- What are the human, tangible and intangible assets?
- What and who determines value?
- What are the measures of success?
- What is the risk attitude?

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

RISK ASSESSMENT:
A Critical Decision Making Tool

- **Whether an activity should be undertaken**
- **How to maximize opportunities**
- **Whether risks need to be treated**
- **Choosing between options with different risks**
- **Prioritizing risk treatment options**
- **The most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level and make reward outcomes for risk-taking more certain**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Principles

- Impartiality, independence and objectivity
- Trust, competence, and due professional care
- Honest and fair representation
- Responsibility and authority
- Consultative approach
- Fact-based approach
- Confidentiality
- Change management
- Continual improvement

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

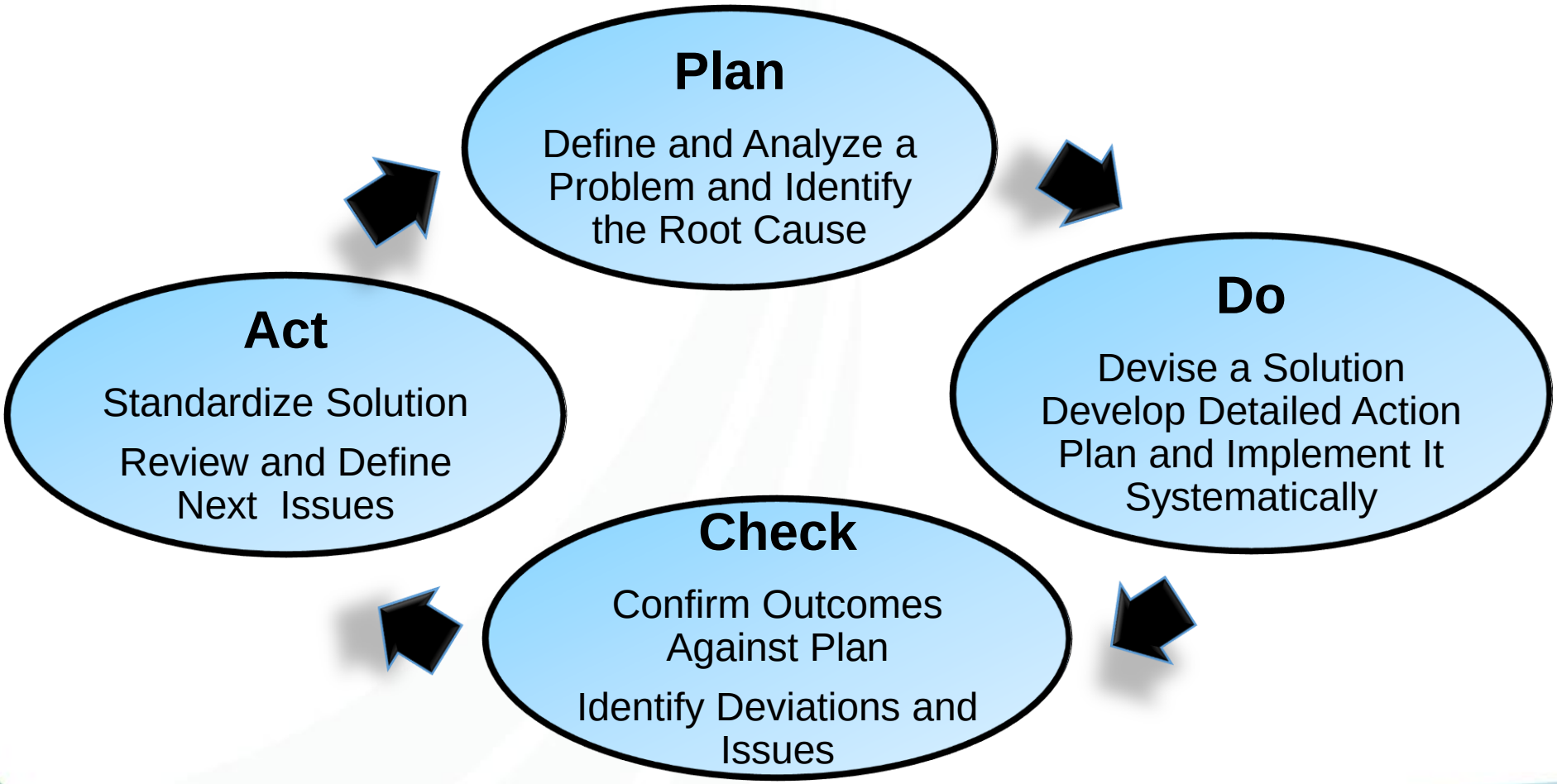
Consultative Approach

- **Should take place during all stages of the risk management process.**
- **Creates a dialogue among stakeholders.**
- **Develops communication strategy at the planning stage.**
- **Ensures stakeholders' perception of risk is addressed.**
- **Seeks to improve performance based on informed, mutual decisions.**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Anticipates Continual Improvement



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

THE “RECIPES”

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

$$\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z} = 0$$

$$\rho\left(\frac{\partial u}{\partial t} + u\frac{\partial u}{\partial x} + v\frac{\partial u}{\partial y} + w\frac{\partial u}{\partial z}\right) = -\frac{\partial p}{\partial x} + \mu\left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2}\right) + \rho g_x$$

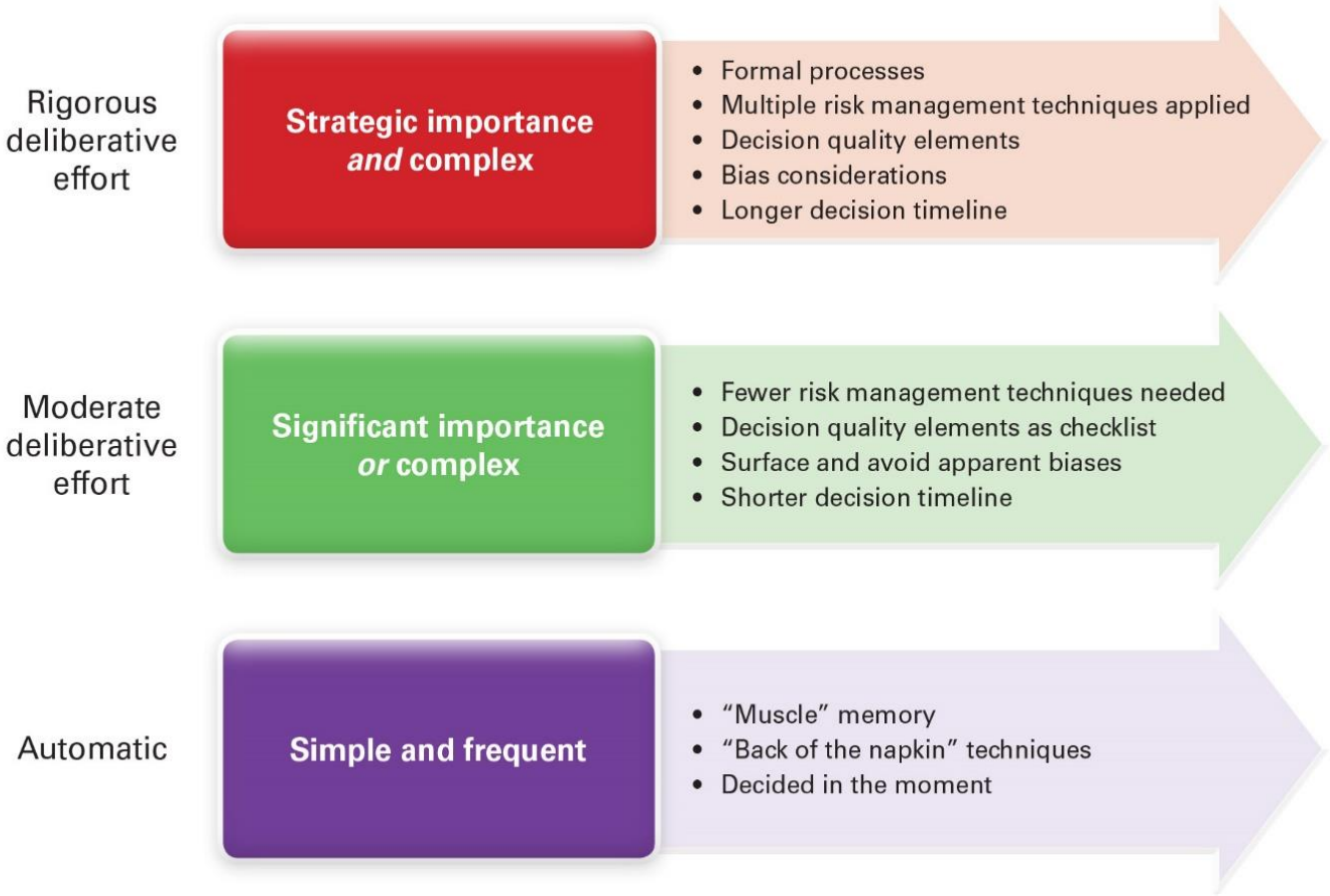
$$\rho\left(\frac{\partial v}{\partial t} + u\frac{\partial v}{\partial x} + v\frac{\partial v}{\partial y} + w\frac{\partial v}{\partial z}\right) = -\frac{\partial p}{\partial y} + \mu\left(\frac{\partial^2 v}{\partial x^2} + \frac{\partial^2 v}{\partial y^2} + \frac{\partial^2 v}{\partial z^2}\right) + \rho g_y$$

$$\rho\left(\frac{\partial w}{\partial t} + u\frac{\partial w}{\partial x} + v\frac{\partial w}{\partial y} + w\frac{\partial w}{\partial z}\right) = -\frac{\partial p}{\partial z} + \mu\left(\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} + \frac{\partial^2 w}{\partial z^2}\right) + \rho g_z$$

Navier–Stokes equations are nonlinear partial differential equations describing almost every real situation.

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Formal vs. Informal Risk Assessments



Adapted from A Cultural Approach to Decision Making Presentation at RIMS 2011 ERM Conference by Dr. Carl Spetzler

Copyright © 2013-2015 Risk and Insurance Management Society, Inc. All rights reserved.

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Managing to a Common Approach

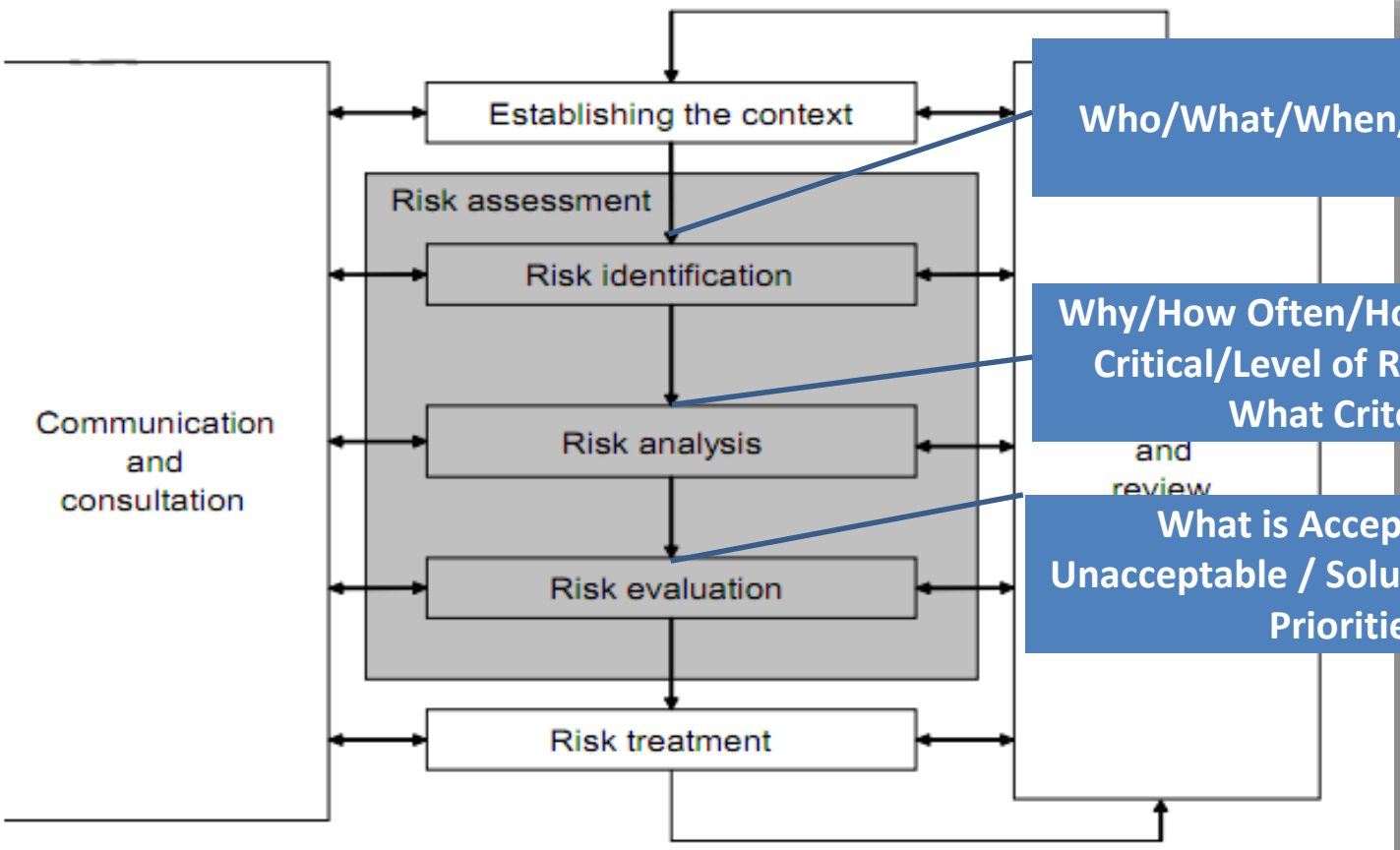
Handy Kitchen Measurements

1 Gallon	=	4 Quarts	=	16 Cups	=	8 Pints	=	3-3/4 L
1/4 Gallon	=	1 Quart	=	4 Cups	=	2 Pints	=	.94 L
1/8 Gallon	=	1/2 Quart	=	2 Cups	=	1 Pint	=	16 Fl Oz
1 Cup	=	8 Fl Oz	=	16 Tbsp	=	48 Tsp	=	237 mL
3/4 Cup	=	6 Fl Oz	=	12 Tbsp	=	36 Tsp	=	177 mL
2/3 Cup	=	5-1/3 Fl Oz	=	10-2/3 Tbsp	=	32 Tsp	=	158 mL
1/2 Cup	=	4 Fl Oz	=	8 Tbsp	=	24 Tsp	=	118 mL
1/3 Cup	=	2-2/3 Fl Oz	=	5-1/3 Tbsp	=	16 Tsp	=	79 mL
1/4 Cup	=	2 Fl Oz	=	4 Tbsp	=	12 Tsp	=	59 mL
1/8 Cup	=	1 Fl Oz	=	2 Tbsp	=	6 Tsp	=	30 mL
				1 Tbsp	=	3 Tsp	=	15 mL
						1 Tsp	=	5 mL

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Risk Assessment Starts with Questions



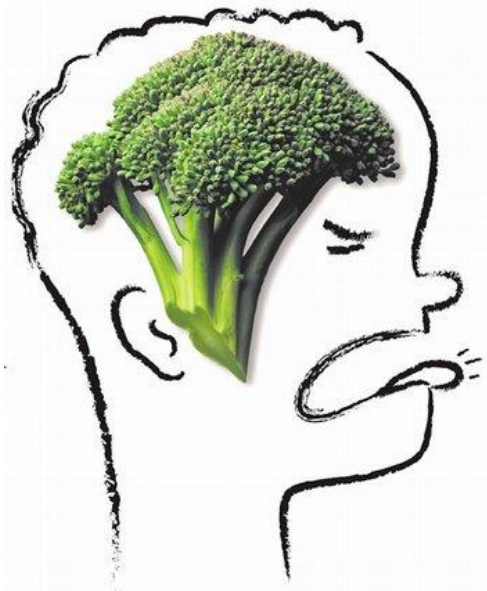
Reproduced from *ISO 31010* www. iso.org. Copyright remains with IEC|ISO.

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Understanding Biases

- Social and cultural biases
- Familiarity and confirmation bias
- Perception, observational selection, and memory biases
- Belief and behavioral biases
- Relational, group-think, and tribal biases
- Confirmation and post rationalization biases
- Information availability bias
- Decision making biases
- Illusion of control biases



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

The Flavorings: Performing Individual Assessments

Recognizing Tangible and Intangible Elements

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Confirming the Competence of Risk Assessors

- Determine competence criteria
- Evaluate training and competence
- Monitor competence in performance
- Improve competence
- Validate (e.g., personnel records)
- Check credentials
- Obtain non-disclosure agreements
- Apply accountability
- Maintain records as required
- Using external risk assessors and technical experts

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Performing Individual Risk Assessments

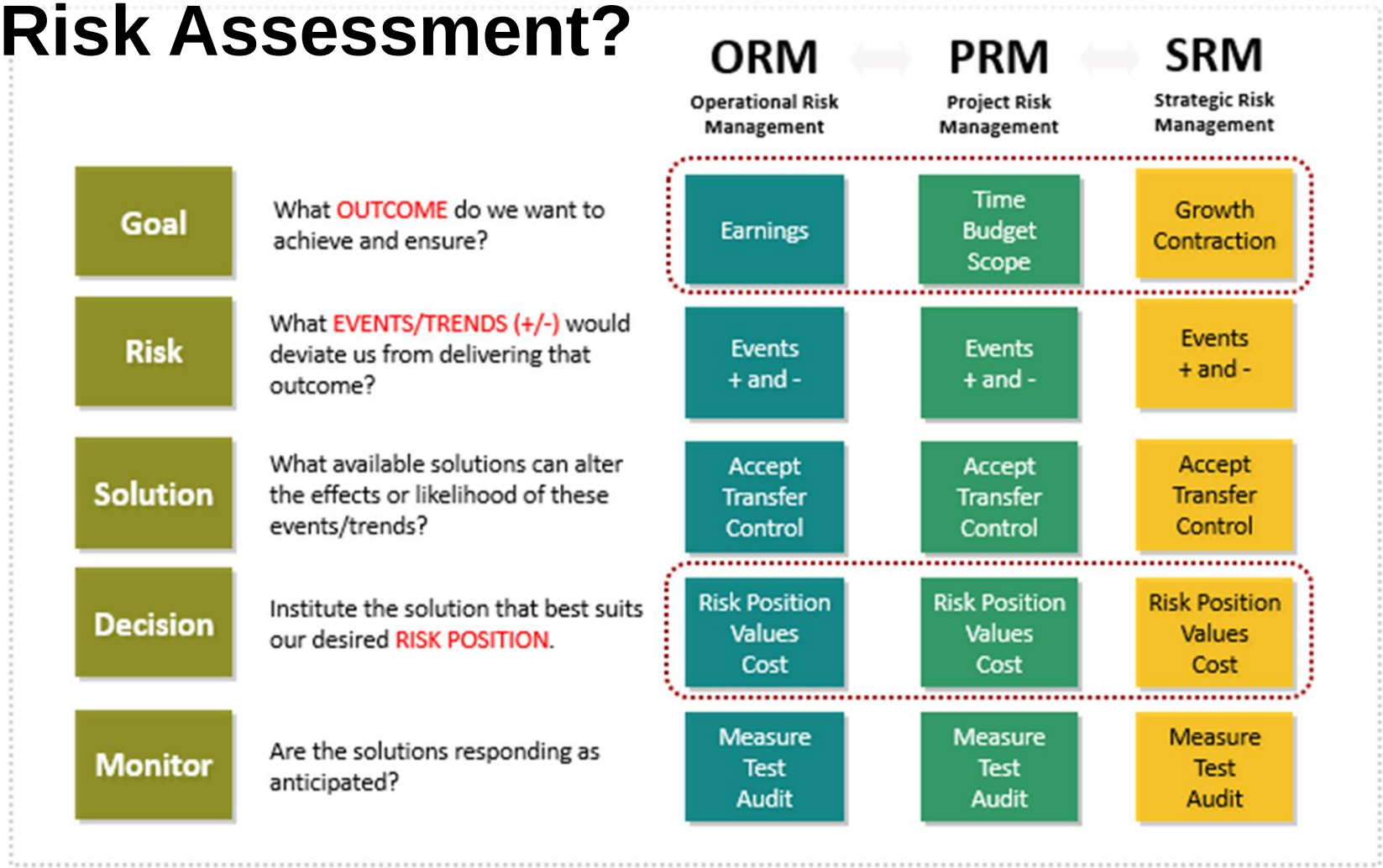
RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

- **Setting objectives**
- **Identification of stakeholders**
- **Identification of internal context and variables**
- **Documenting assumptions**
- **Defining scope and statement of work**
- **Policy and management commitment**
- **Commitment of resources**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

What is the Context for the Individual Risk Assessment?



Adapted from 2012 RIMS Conference presentation by Joana Makomaski. Copyright © 2012 Risk and Insurance Management Society, Inc. All rights reserved.

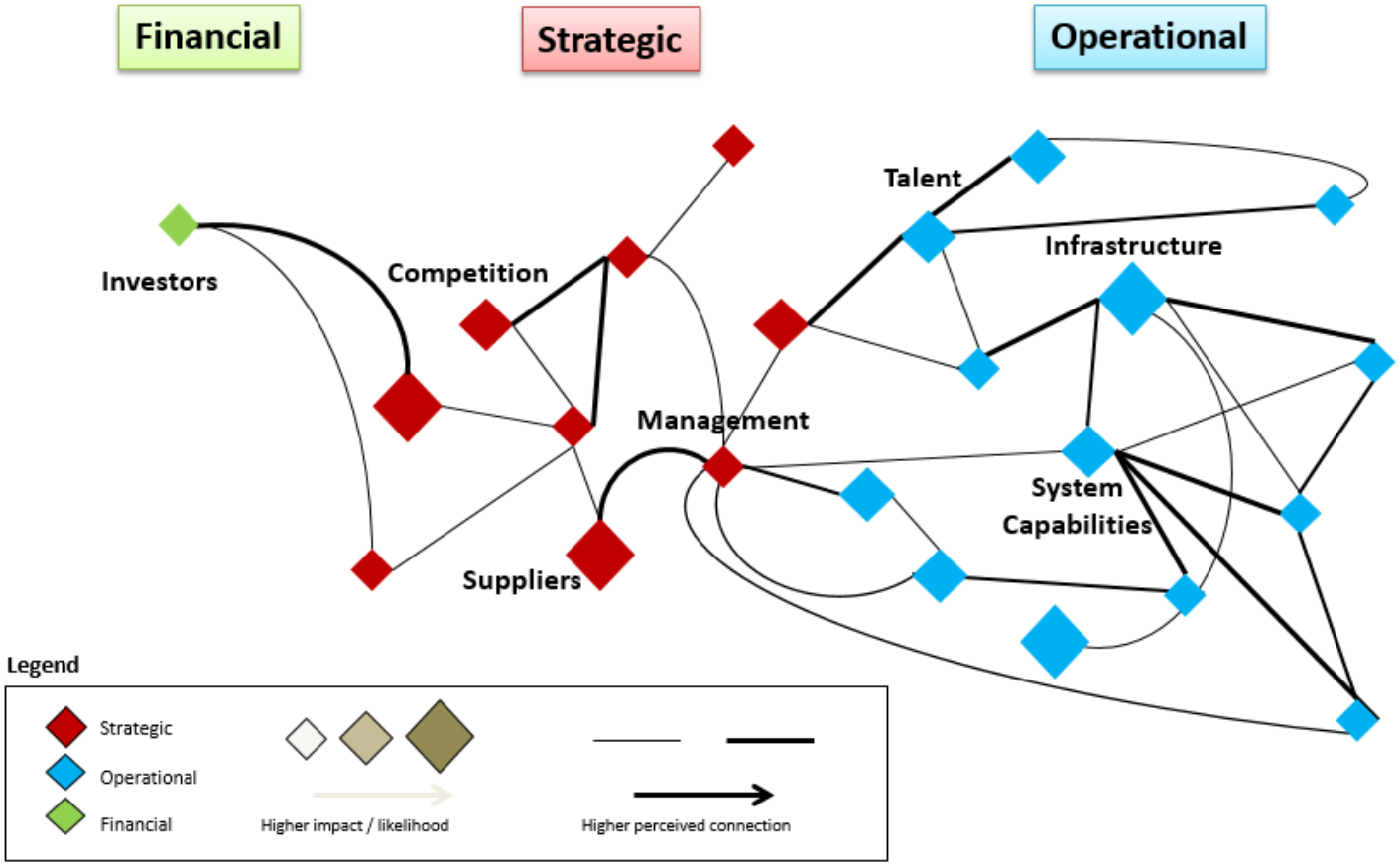
RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

- **Gap analysis**
- **Legal and other requirements**
- **Objectives, targets and strategies**
  - Analysis methodology
  - Data gathering
  - Review of documentation
- **Preparing the risk assessment plan**
  - Establishing the risk assessment team
- **Determining feasibility**
  - Documentation and document control

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Analysis Methodology: Influence Diagram Example



Risks are Changeable and Influence Each Other

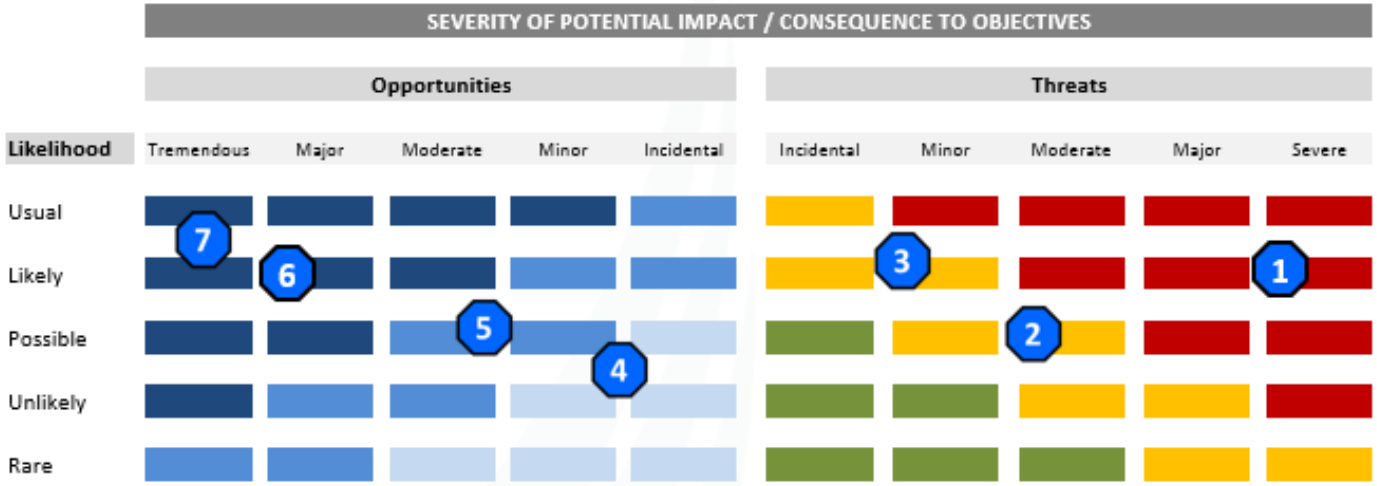
RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

- **Preparing work documents**
- **Assigning roles and facilitating communication among team members**
- **Conducting a pre-assessment meeting**
- **Implementing**
  - ***Risk identification***
    - Asset identification, valuation and characterization
  - ***Risk analysis***
    - Threat and opportunity analysis
    - Vulnerability/capability analysis
    - Criticality and consequence (impact) analysis
  - ***Risk evaluation***
- **Generating findings and conclusions**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Findings and Conclusions: Sample Outcome Matrix



Copyright Risk and Insurance Management Society, Inc. All rights reserved. Used with permission.

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

- **Conducting post-assessment debriefing**
- **Reports and records**
- **Follow-up and monitoring**
- **Checking and review**
- **Improvement**

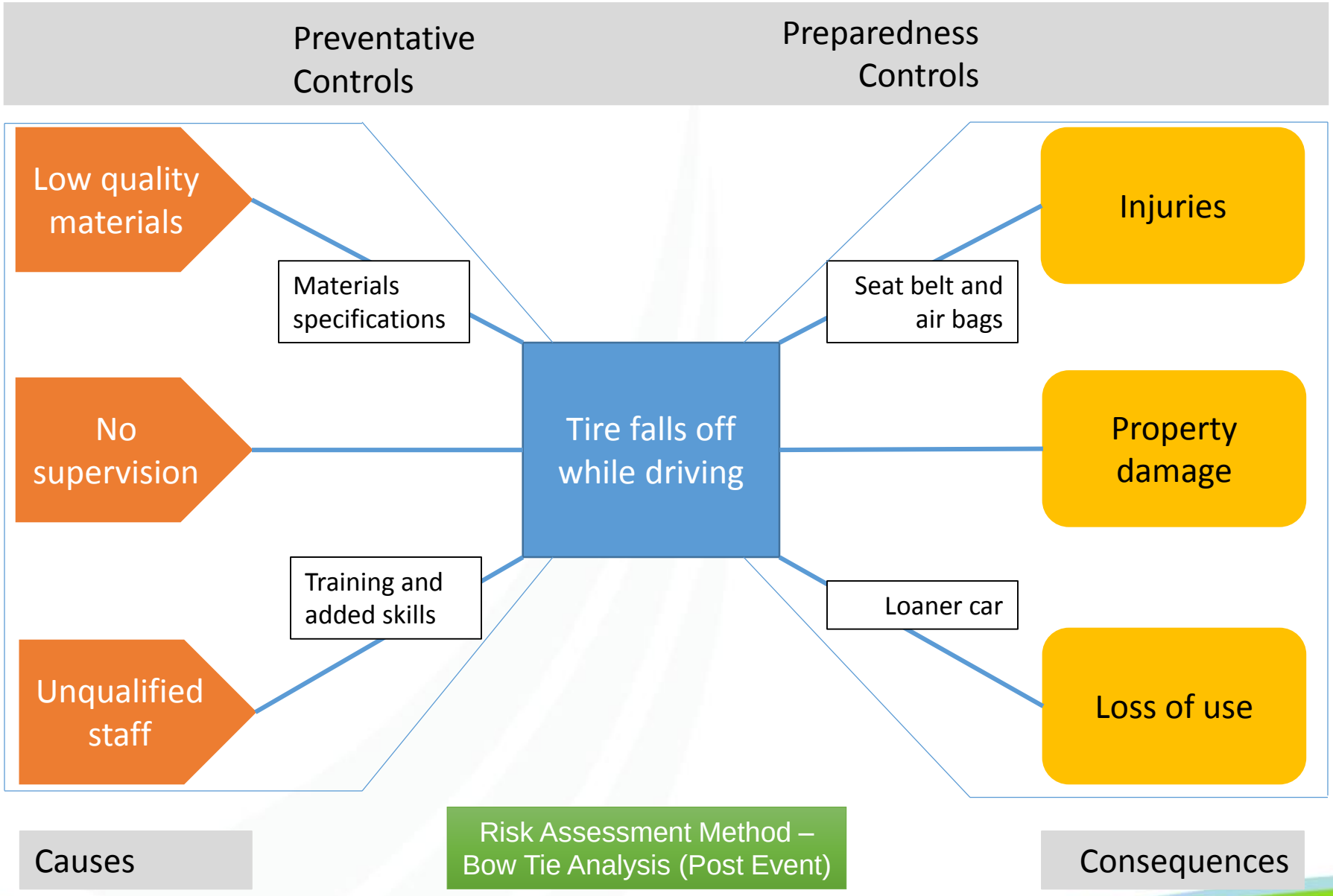
RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Adapting the Recipes

Decision-making and variability

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

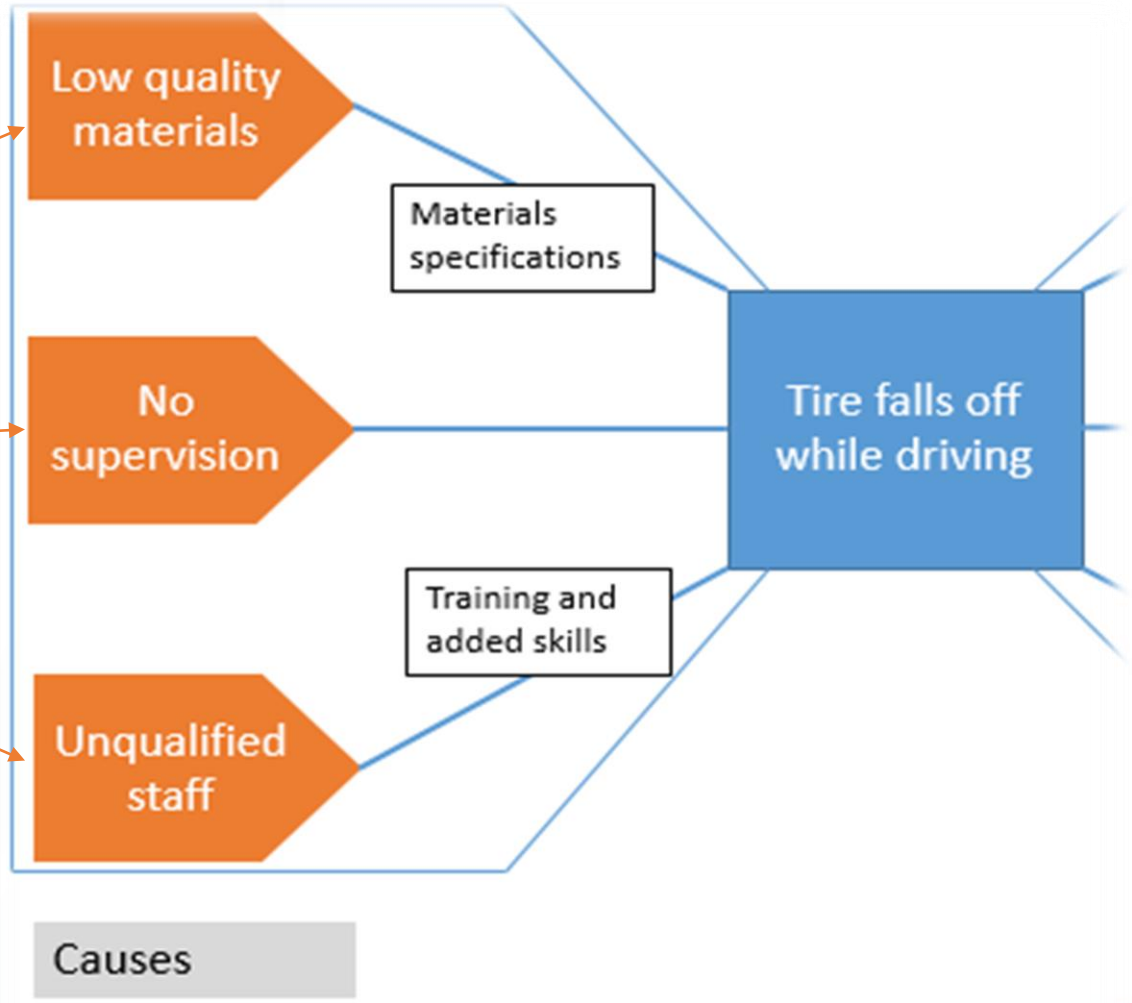
Joint Copyright ©ASIS and RIMS 2016

Objective:
Produce safe tires for sports cars

Engineering / finance decision in initially specifying materials

Management decision regarding labor

Operations/ HR decisions regarding staffing qualifications



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Risk Assessment Drives Decision Making

- **Risk management is based on specific business objectives and is objectives focused.**
- **Risk assessment is defined in terms of organizational objectives.**
- **Key performance indicators linked to business objectives.**
- **Risk management supports decision making, and is therefore proactive.**
- **Risk management protects and creates value.**
- **Risk management process consistency depends on clear governance structure.**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Objective

Decision-making and risk management

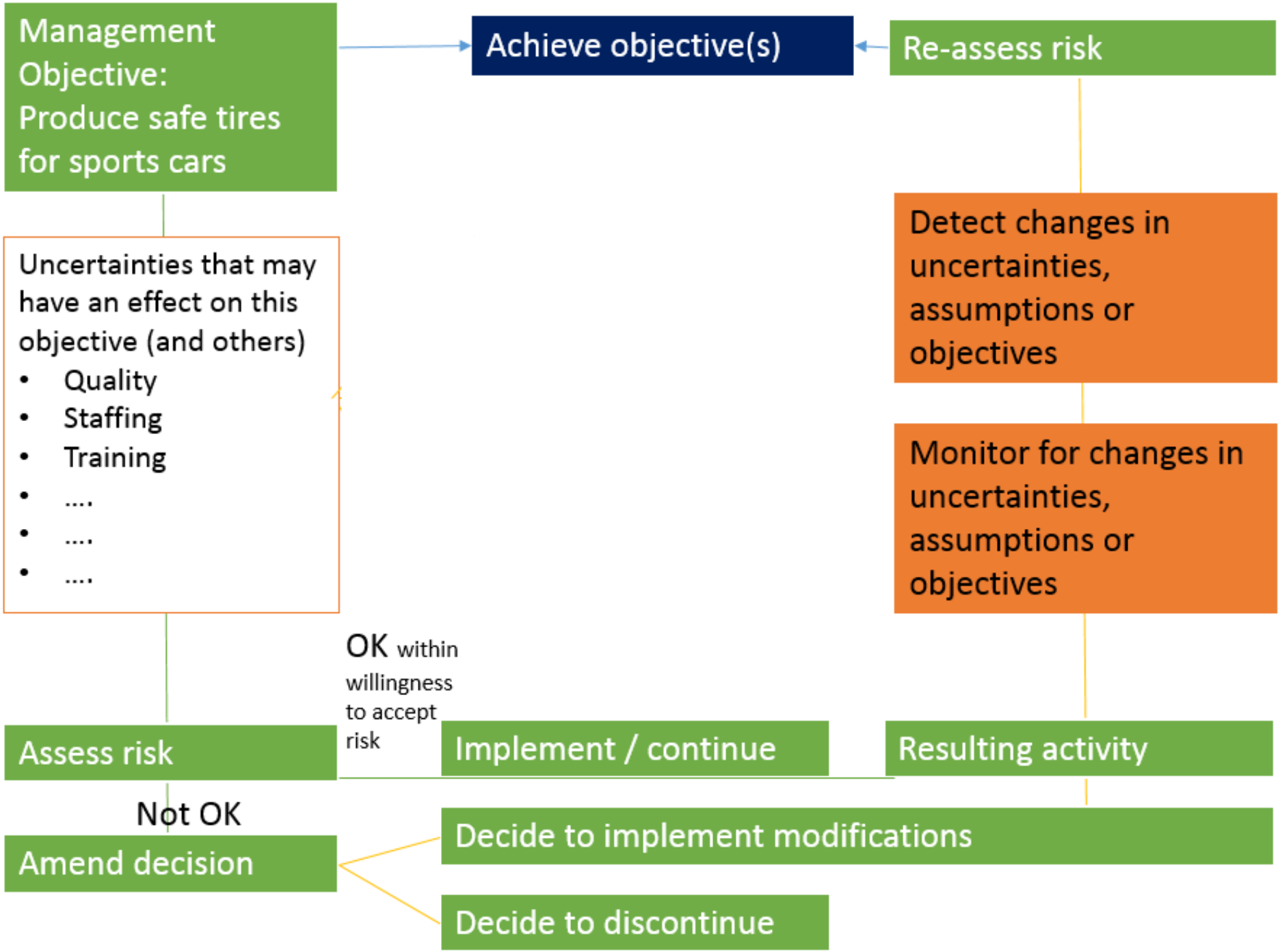
Decision-making steps

1. Frame: issue/need defined
2. Doable alternatives
3. Meaningful, reliable alternatives
4. Developing options
5. Clear values and trade-offs
6. Logically, correct reasoning
7. Acting on the decision

Related uncertainties in each step

1. Is solving this problem or realizing this opportunity worthwhile?
2. What options are available and how effective or disruptive will each one be in solving the problem or realizing the opportunity? What unintended consequences will this alternative create?
3. Is the information accurate, applicable, and useful and how will this affect the decision-making process?
4. What different interpretations of the data are possible and how will each one affect the decision-making process?
5. How feasible, acceptable, or desirable is each option and which will be most useful in achieving the objective?
6. What biases may be influencing reasoning?
7. Are there resources available for allocation to the decision and will the decision be accepted and supported by stakeholders?

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016


Management Objective: Produce safe tires for sports cars
Achieve objective(s)
Re-assess risk
Uncertainties that may have an effect on this objective (and others)
• Quality
• Staffing
• Training
• ….
• ….
• ….
Detect changes in uncertainties, assumptions or objectives
Monitor for changes in uncertainties, assumptions or objectives
OK within willingness to accept risk
Assess risk
Implement / continue
Resulting activity
Not OK
Amend decision
Decide to implement modifications
Decide to discontinue

Annexes

- **Risk assessment methods, data collection and sampling**
- **Root cause analysis**
- **Background screening and security clearances**
- **Contents of risk assessment report**
- **Confidentiality and document protection**
- **Examples of risk treatment procedures that enhance resilience of the organization**
- **Business impact analysis**

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

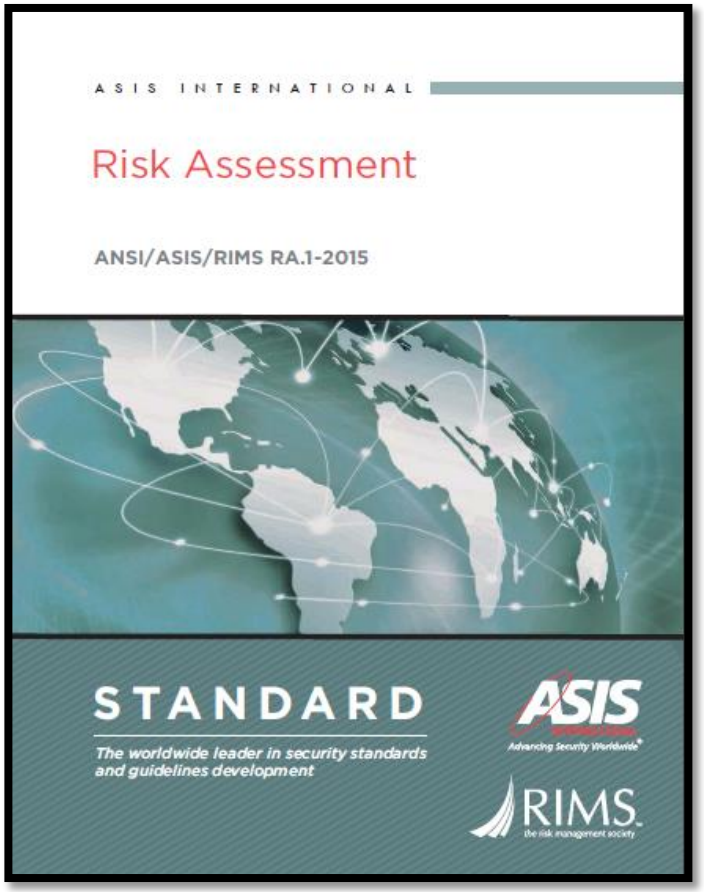
Joint Copyright ©ASIS and RIMS 2016

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.
Joint Copyright ©ASIS and RIMS 2016

Where can I get a copy of the Risk Assessment Standard?

Available on the ASIS and RIMS Websites

www.asisonline.org
www.RIMS.org



RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Thank You – Questions?

Marc Siegel
ASIS International
Commissioner,
Global Standards
+1 (858) 484-9855
siegel@msiegel.net

Carol Fox
RIMS Vice President,
Strategic Initiatives
+1 (212) 655-6004
cfox@rims.org

So you want to be a ….

RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Joint Copyright ©ASIS and RIMS 2016

Referenced Recognized Standards

ISO 31000: 2009 Risk Management – Principles and Guidelines
AS/NZS 4360:2004 Risk Management Australian/New Zealand Standard
ISO GUIDE 73:2009 Risk Management – Vocabulary
HB 436:2004 Risk Management Guidelines: a Companion to AS/NZS 4360:2004
ISO TR 31004:2013 Risk Management – Guidance for the implementation of ISO 31000
ISO 31010:2009 Risk Management – Risk Assessment
NFPA 101:2009 Life Safety Code®
ANSI/ASHRAE 62.1-2007 Standard on Ventilation for Acceptable Indoor Air Quality
OHSAS 18001:2007 Occupational Health and Safety
ISO 9001:2008 Quality Management Systems – Requirements
ISO 10005:2005 Quality Management Systems – Guidelines for Quality Plans
NFPA 75:2009 Standard for the Protection of Information Technology Equipment
ISO/IEC 27001:2005 Information Security Management Systems – Requirements
ISO/IEC 27002:2005 Information Technology – Code of Practice
ISO/IEC 15408:2005/2008 (3 parts) Evaluation Criteria for IT Security
ISO 14050:2009 Environmental - Vocabulary
ISO 14001:2004 Environmental Management Systems - Requirements
ISO 28000:2007 Security Management Systems for the Supply Chain
ANSI / ASIS SPC.1:2009 Organizational Resilience: Security Preparedness, and Continuity Management Systems – Requirements with Guidance for Use

RIMS Confidential Information. Do not disclose without express permission of RIMS general counsel.