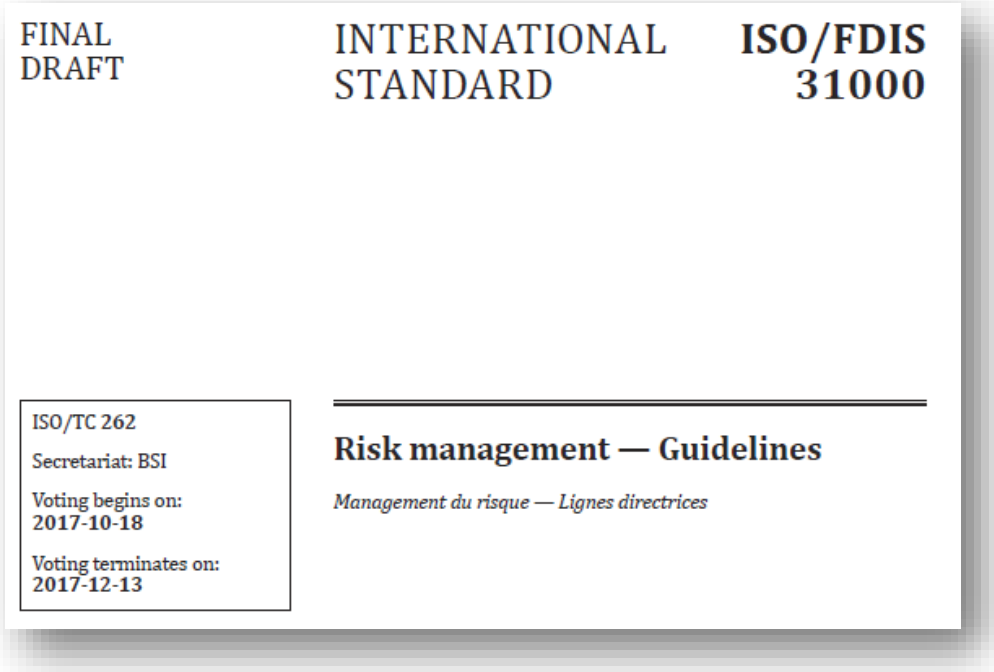
The Latest on ISO 31000: Advancing the Mission


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/FDIS 31000

ISO/TC 262

Secretariat: BSI

Voting begins on: **2017-10-18**

Voting terminates on: **2017-12-13**

Risk management — Guidelines

Management du risque — Lignes directrices

Carol Fox, ARM

Vice President Strategic Initiatives, RIMS

Chair, U.S. TAG to ANSI for ISO TC262-Risk Management

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

My Mission Today is for you to …

Gain a greater understanding of what goes into a standard's revision

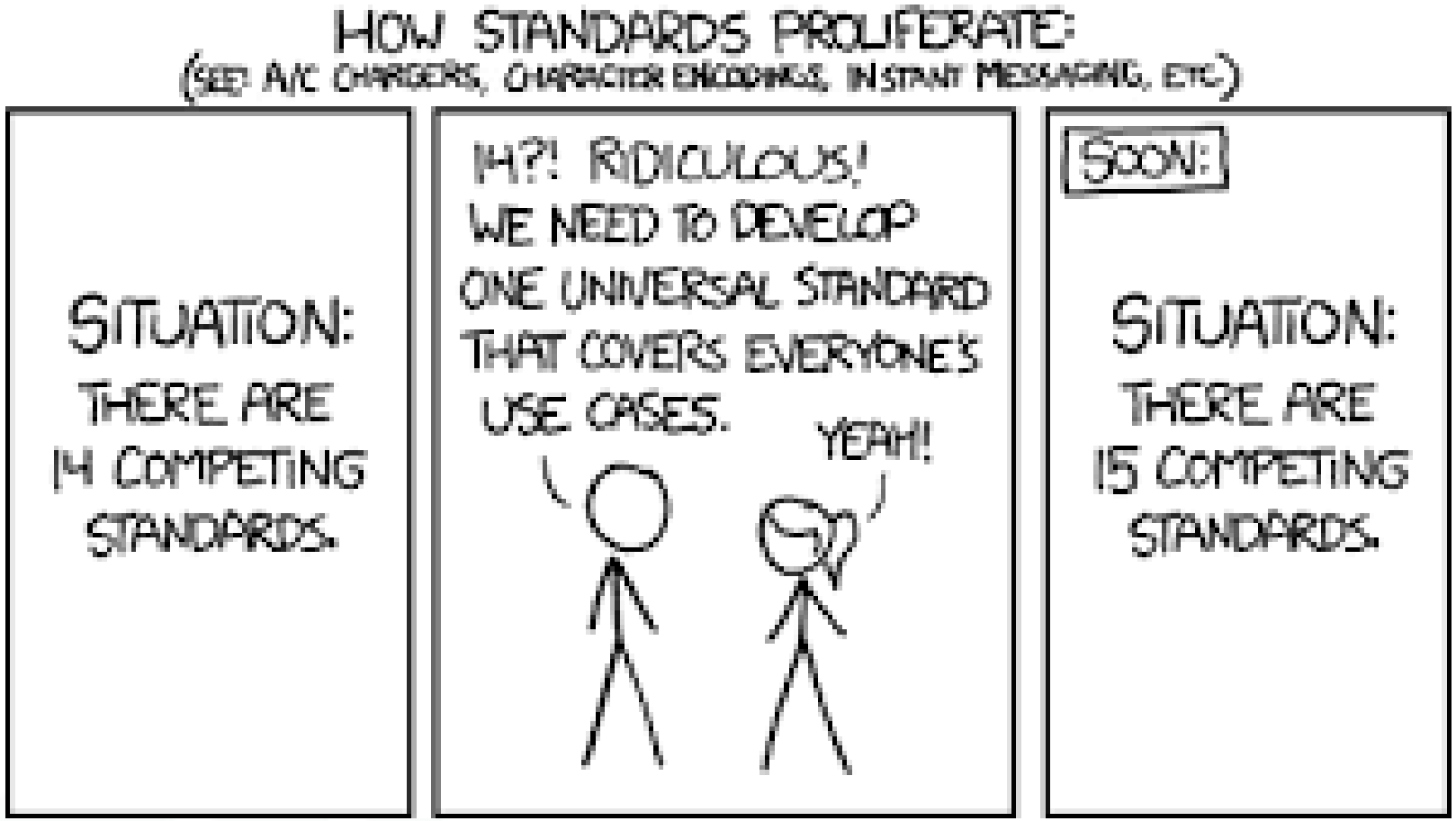
Learn how the development of ERM has affected the ISO 31000 standard

Understand the changes being incorporated into the ISO 31000 revision

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

RIMS the risk management society™

Why You Should Care About Standards



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

Polling Question 1.

How familiar are you with how international standards are developed through ISO, the International Organization for Standardization?

1. Very familiar
2. Somewhat familiar
3. Not familiar
4. What is an international standard?

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

STANDARDS 101

WHAT IS A STANDARD?

- Simply, a VOLUNTARY agreed-upon way of doing something or a solution to a problem.
- In practice, it is a document that sets guidelines or requirements.

WHO CREATES STANDARDS?

- Developed by a group of “experts” who have a stake in the topic.

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

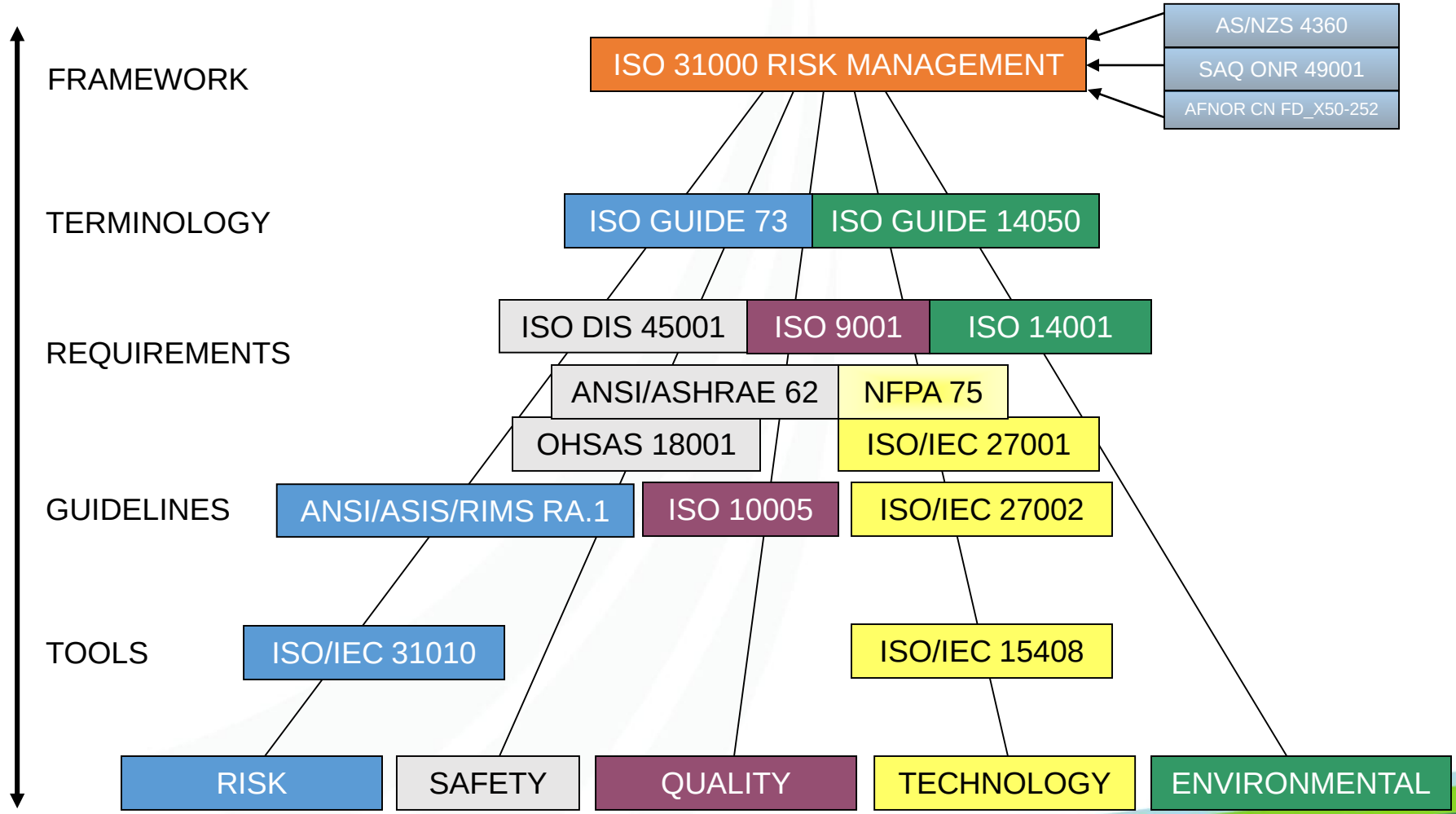
RIMS the risk management society

ANSI – as the U.S. national standards body – is a member of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) via the U.S. National Committee (USNC).

ANSI adopted ISO 31000:2009 as the American national standard for risk management.

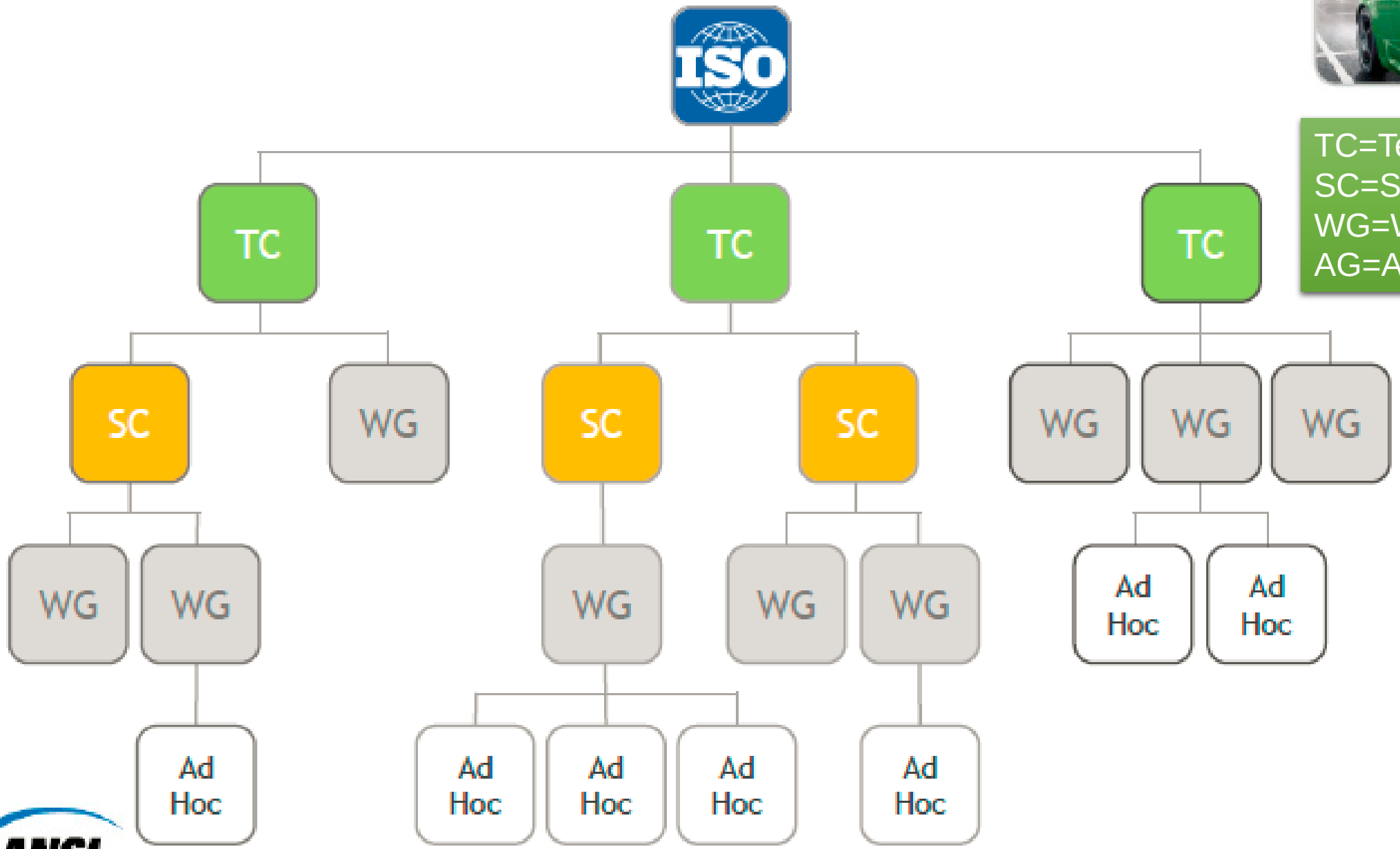
RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

Family of Standards



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

TC=Technical Committee
SC=Subcommittee
WG=Working Group
AG=Ad Hoc Group



© 2016

© 2016

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

Source: Survey by Norman Marks, May 2012

Point of View 2012: COSO or ISO 31000?

Why COSO ERM?

COSO is more comprehensive, has been tested over time and its applicability to many industries is well proven.

COSO is much stronger in the concepts of alignment of risk with strategy...

COSO ERM defines organizational structure with the 5 components of internal control …

Why ISO 31000?

ISO is structured, logical and covers practical and theoretical issues...

ISO is easier to understand and more applicable generally across the scope of activities ...

31000 makes it easier to speak the language of the public sector leaders to get buy in...

ISO is easier to explain to operations managers ...

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

RIMS the risk management society™

Polling Question 2.

Our ERM program is most closely aligned with …

1. COSO ERM Framework
2. ISO 31000
3. Other standard
4. Do not follow any particular standard or framework
5. Do not know

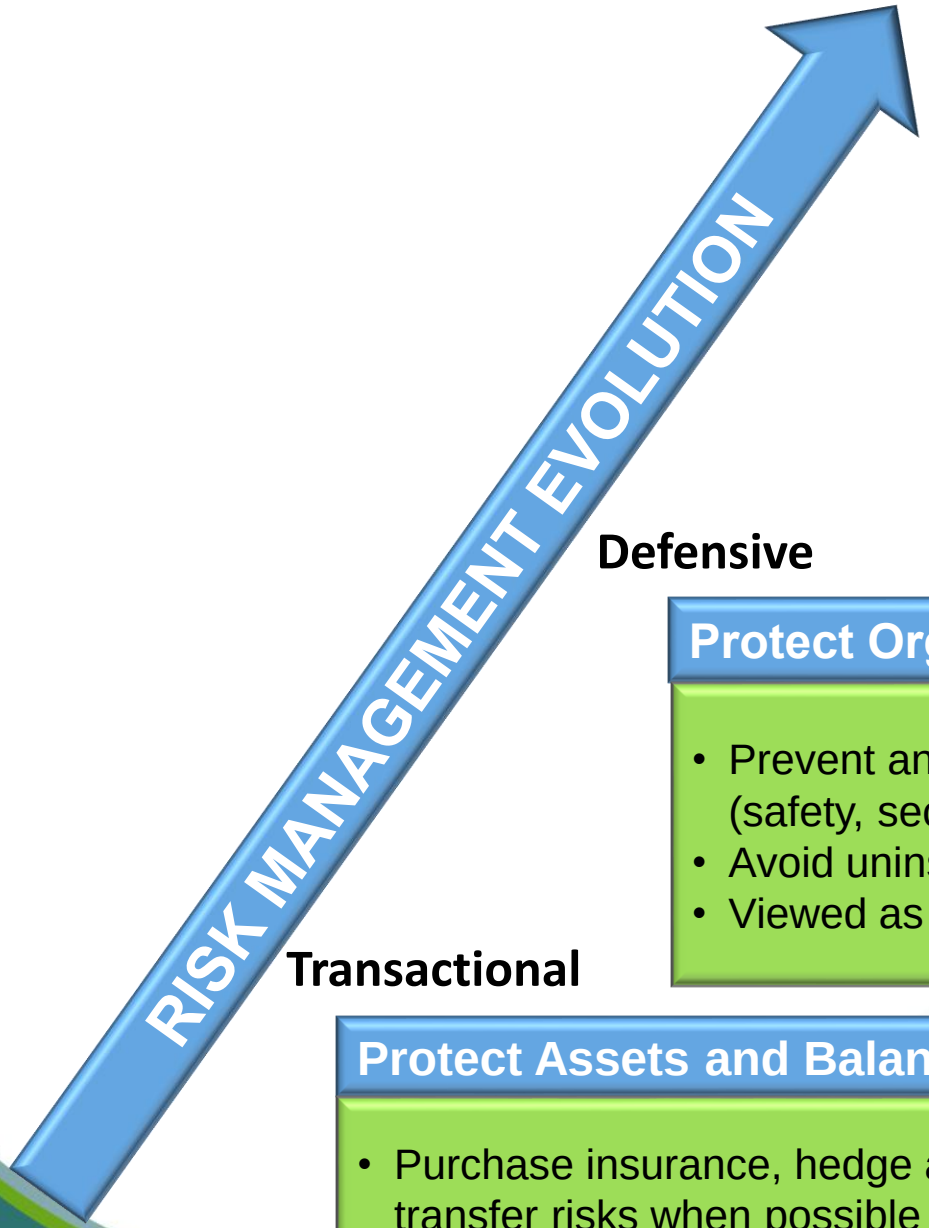
Circular A123 recognizes ISO 31000 and the COSO ERM Framework as guidance documents.

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

WHY REVISE ISO 31000?

What has changed since 2009?

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



Strategic

Create and Protect Value Throughout an Enterprise

- Horizontal competency in planning and activities
- Future- and objectives-focused
- Recognize and seize opportunities
- Inform capital allocation decisions
- Improve efficiencies

Focus on uncertainty and decision making

Defensive

Protect Organization's Mission and Value

- Prevent and reduce losses before/after incidents (safety, security, business continuity, etc.)
- Avoid uninsured expenses and improve cash flow
- Viewed as separate (vertical) cost centers

Focus on control activities

Transactional

Protect Assets and Balance Sheet

- Purchase insurance, hedge and transfer risks when possible
- Indemnification after the fact

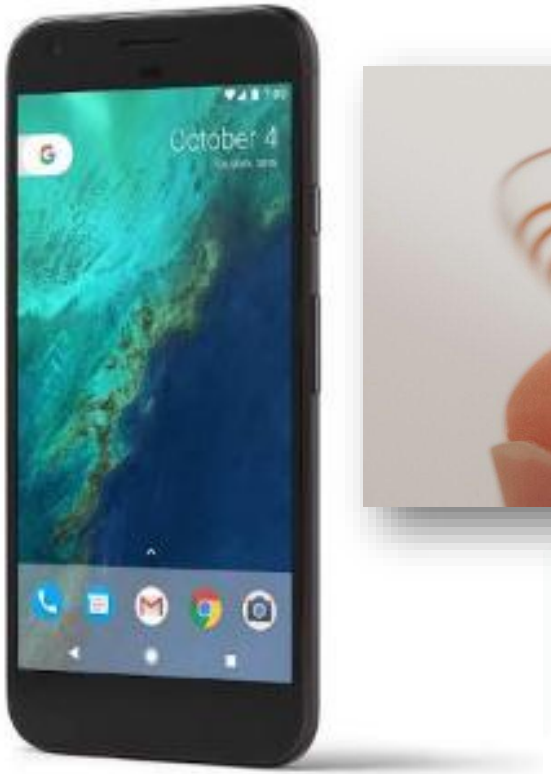
Focus on hazards, liabilities and threats

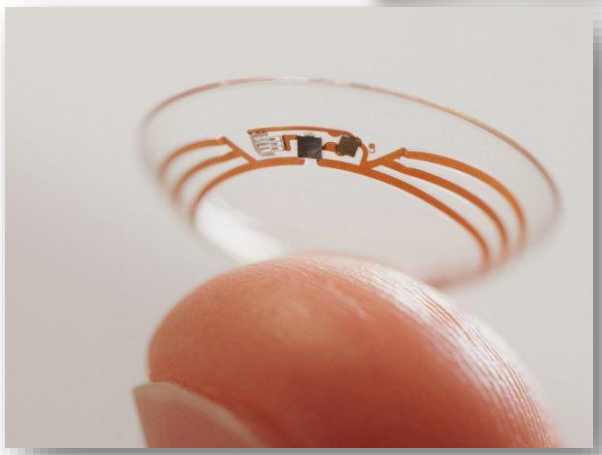
Copyright RIMS, the risk management society 2017. All rights reserved.

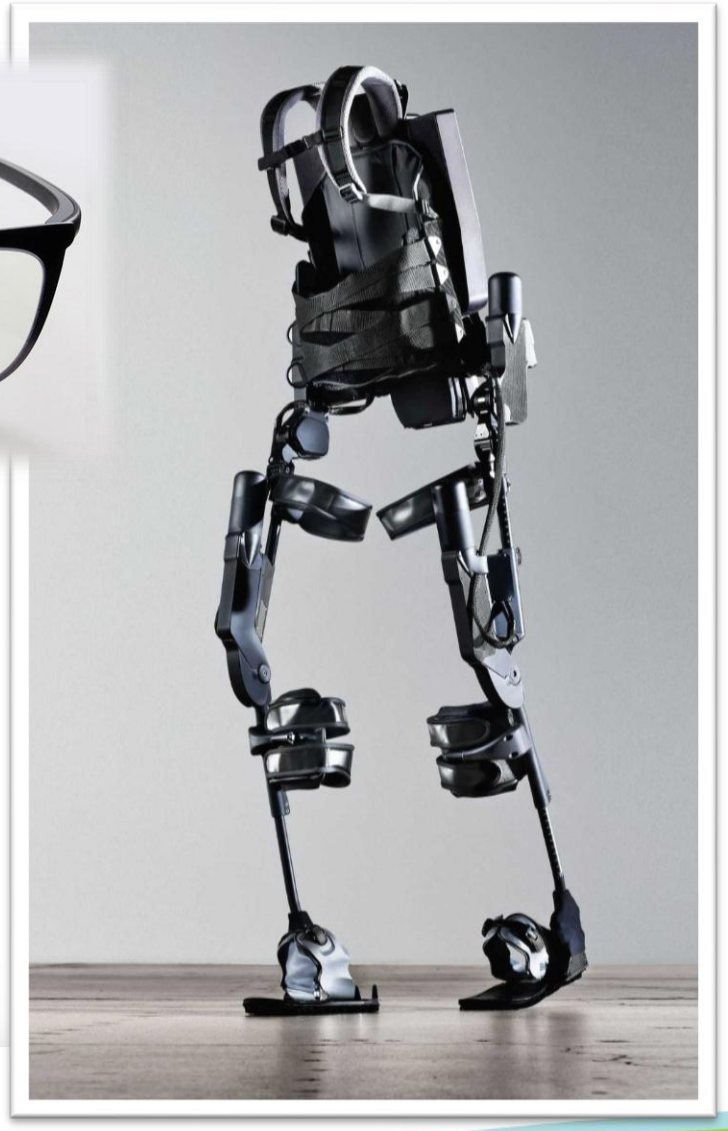
RIMS Confidential information. Do not disclose without express permission of RIMS general counsel.

RIMS the risk management society

Rapidly changing technological environment







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

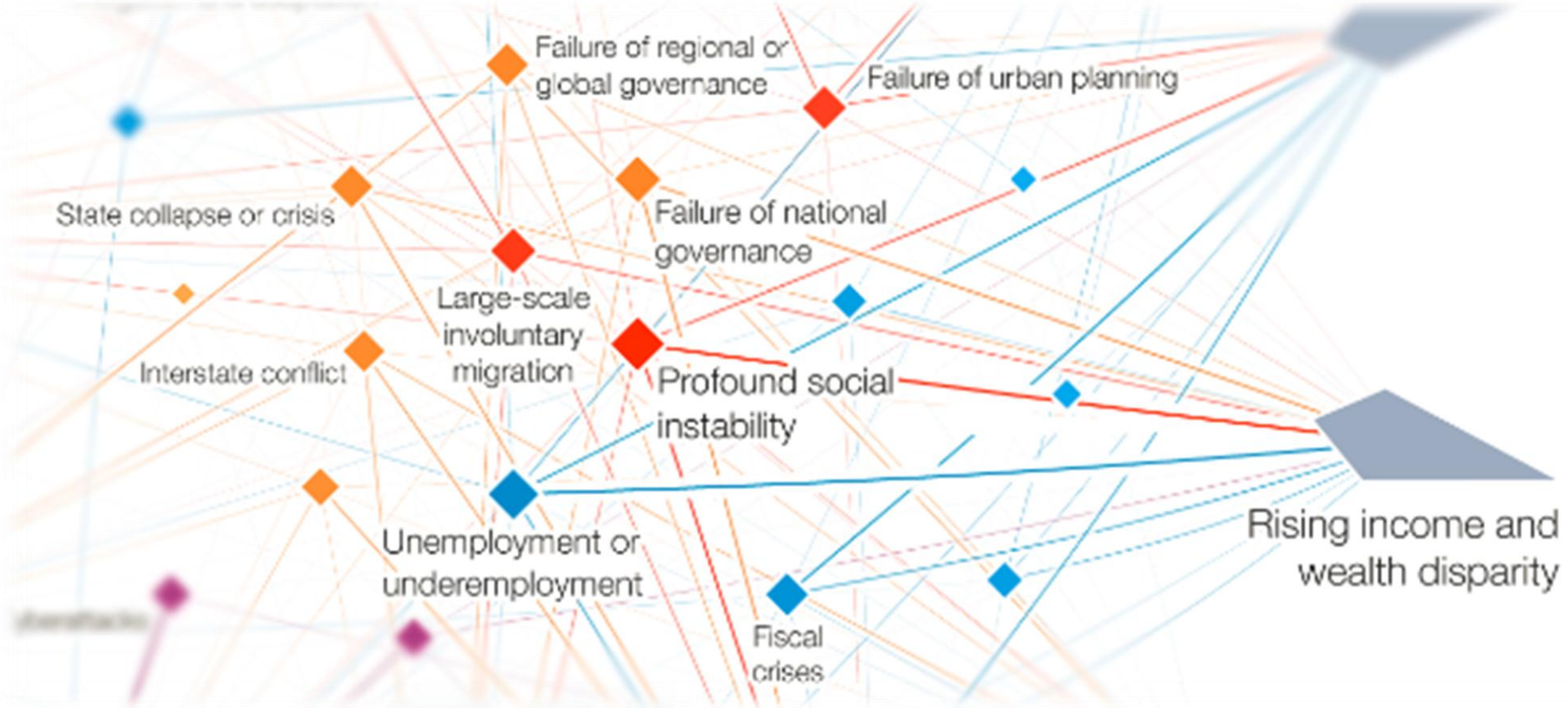
RIMS the risk management society

$230 BILLION

invested in the “Internet of Things” in 2016 by US companies; expected to grow to $370 billion by 2018.

SOURCE: INTERNATIONAL DATA CORP.

Rapidly changing social environment



"One of the key findings of this year's Global Risks Report is that *inequality and polarization* are now ranked in the top three as underlying drivers of global risks."

Source: https://www.weforum.org/agenda/2017/02/global-risks-report-2017/

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

Changing climate

"The UN estimates that an average of 22.5m people a year have been displaced by natural disasters since 2008, yet this remains a trickle compared with the flood of refugees and migrants that could result from the growing effects of global warming."

Simon Baptist
Chief Economist, EIU
September 17, 2017

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

CATALYSTS FOR CHANGE IN ISO 31000 STANDARD

- Demands from top management for greater insights into uncertainty when making decisions
- Emerging legal and regulatory requirements globally, including public disclosure
- Stakeholder demands for greater oversight, accountability and transparency

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

RIMS the risk management society

What are the focus areas for developing your company's risk management capabilities in 2017?

	RISK PROFESSIONALS		C-SUITE
1	Improve the use of data and analytics	1	Formalize risk management training/ education across the organization
2	Integrate risk management into strategic planning	2	Upgrade risk management technology and access to information
3	Formalize risk management training/ education across the organization	3	Improve the use of data and analytics
4	Upgrade risk management technology and access to information	4	Integrate risk management into strategic planning
5	Invest in broadening risk management resources with current employees	5	Improve risk governance structure

Improve communication and insights

Source: Marsh|RIMS Excellence in Risk Management XIV, *Ready Or Not, Disruption Is Here*, 2017

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

RIMS the risk management society™

Polling Question 3.

Are insights from your organization's ERM program being used to inform and influence the agency's strategy?

1. Yes
2. No
3. Not sure

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

REVISING ISO 31000

What is being changed in the revision?

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

ISO 31000 DESIGN SPECIFICATION

Recognized that **risk management is evolving** (for example, frequency and severity are not the only criteria that can be used for risk assessment).

The broad purpose of the revision is to:

- **improve the advice and the usability** of the standard, and
- make it **easier for organizations** to take into account the **effect of uncertainty on objectives** (including making decisions whatever their activities).

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

THREE KEY AREAS FOR REVISION CONSIDERATION

- Frame the revision around the **underlying needs of users** and how they create and protect sustainable value, regardless of the type of organization (rather than approaching risk management as a standalone activity).
- Develop a more direct and **explicit focus on activities, including decision-making**, in order to set or achieve the organization's objectives (recognition that risk management needs to adapt and continually improve – or mature – based on the needs of the organization).
- Reduce complexity with **clearer, simpler and improved language and advice** (whenever possible, remove redundancies and jargon).

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

Introduction

ISO 31000 revision in early 2018

- Managing risk is iterative and assists organizations in setting strategy, achieving objectives, and **making informed decisions**.

Source: ISO 31000 Draft International Standard (DIS), 2017

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

Structurally, the revised standard will be familiar to users of ISO 31000:2009

- Principles
- Framework and
- Process

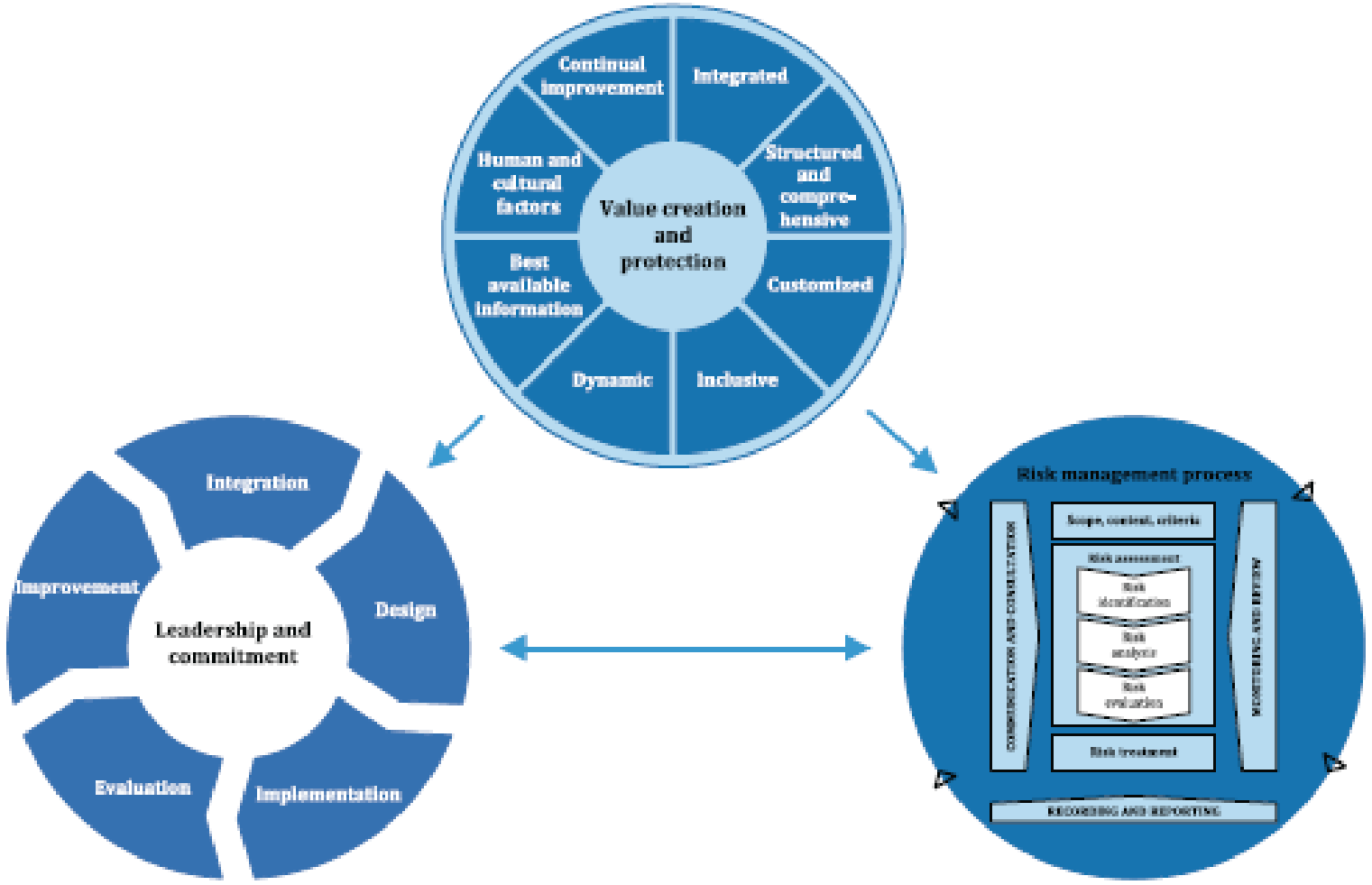


Figure 1 — Relationship between the principles, framework and process

©ISO. This material is reproduced from ISO/FDIS 31000 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved. ISO/FDIS 31000is an ISO draft document that is subject to change without notice. It cannot be referred to as an approved ISO standard.

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

Risk Management — Guidelines

Principles

- The purpose of risk management is the creation and protection of value. It **improves performance**, encourages innovation, and supports the achievement of objectives.

ISO 31000 revision in early 2018

Framework

Process

Source: ISO 31000 Draft International Standard (DIS), 2017

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

Risk Management — Guidelines

Principles

Framework

ISO 31000 revision in early 2018

- The effectiveness of risk management will depend on its integration into the governance and activities of the organization, including **decision making**.

Process

Source: ISO 31000 Draft International Standard (DIS), 2017

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

Risk Management — Guidelines

Principles

Framework

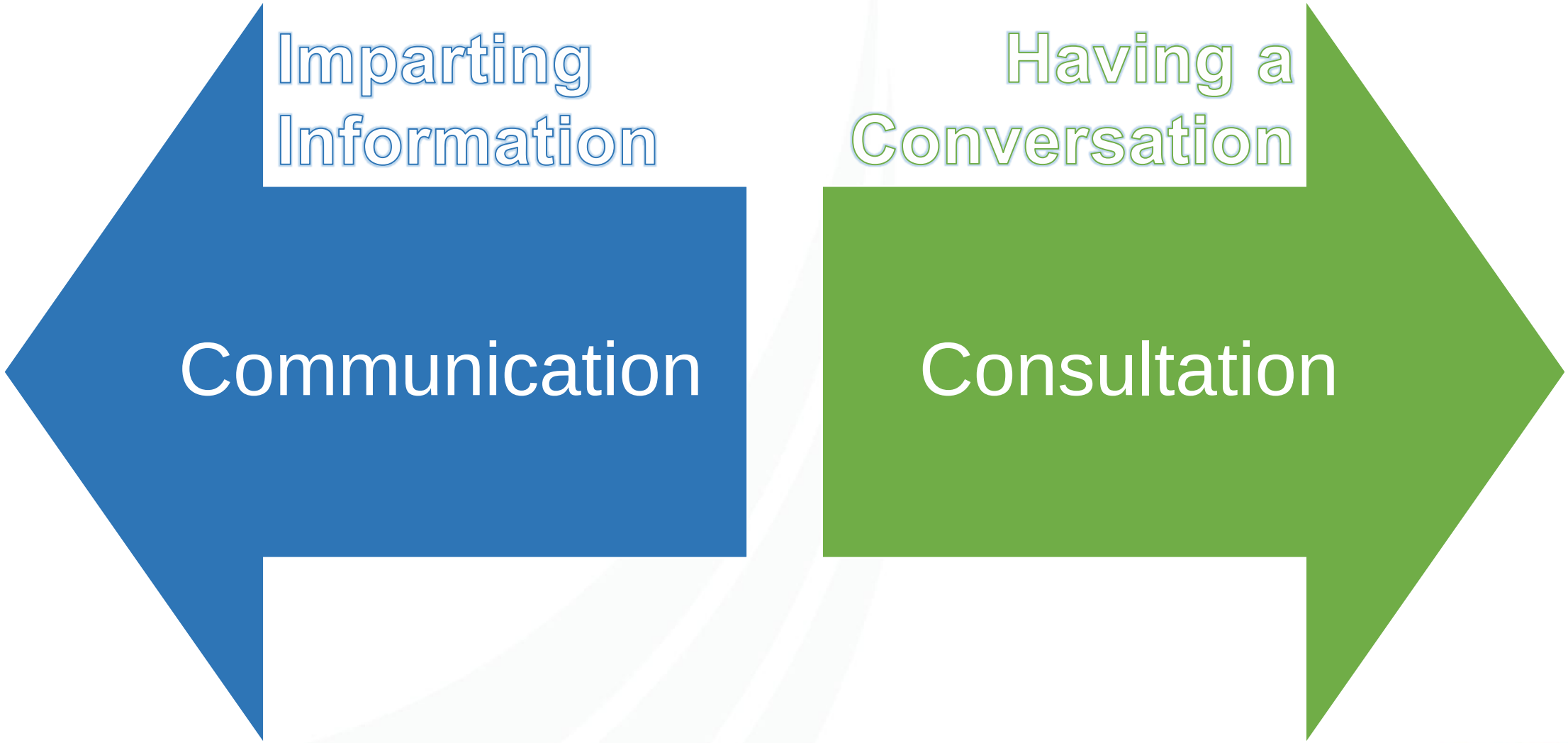
Process

ISO 31000 revision in early 2018

- The risk management process should be an **integral part** of management and **decision making** and integrated into the structure, operations and processes of the organization. It can be applied at strategic, operational, program or project levels.

Source: ISO 31000 Draft International Standard (DIS), 2017

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



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

CONCLUSIONS

Risk management has **evolved** to fundamentally change the way organizations think about risk.

Risk management can **change future outcomes**.

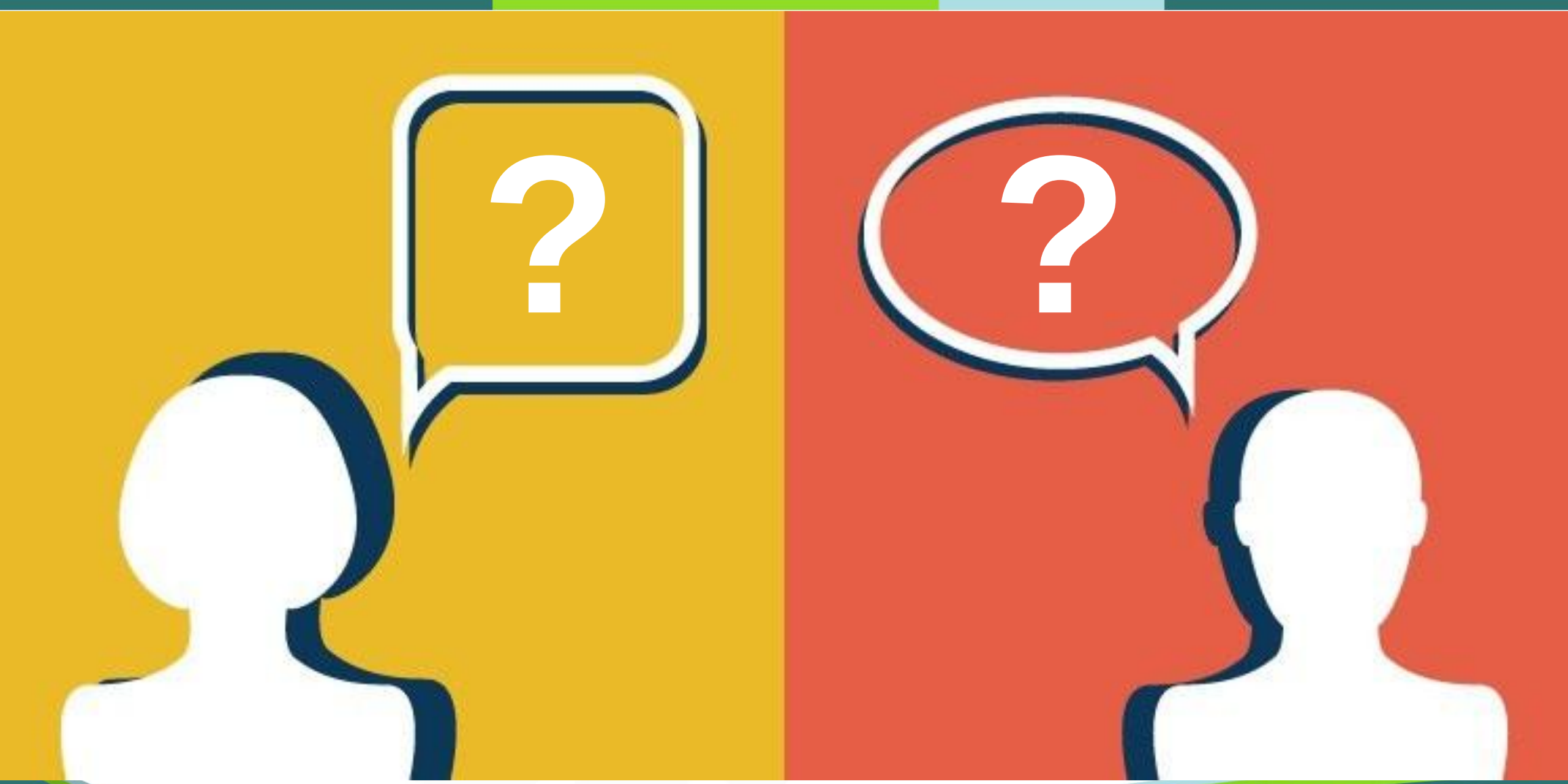
Risk management enables better overall **decision-making** and **performance**.

ISO 31000 is being revised to reflect this "new" reality.

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

RIMS the risk management society™

WHAT IS THE NEXT EVOLUTION IN RISK MANAGEMENT?



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

RIMS the risk management society

Risk Management — Guidelines

ISO 31000 revision in early 2018

Introduction

- Managing risk is iterative and assists organizations in setting strategy, achieving objectives, and **making informed decisions**.

Principles

- The purpose of risk management is the creation and protection of value. It **improves performance**, encourages innovation, and supports the achievement of objectives.

Framework

- The effectiveness of risk management will depend on its integration into the governance and activities of the organization, including **decision making**.

Process

- The risk management process should be an **integral part** of management and **decision making** and integrated into the structure, operations and processes of the organization. It can be applied at strategic, operational, program or project levels.

Source: ISO 31000 Draft International Standard (DIS), 2017

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