Have recent revisions to international risk standards better aligned them to modern business needs?

Gareth Byatt

Principal Consultant, Risk Insight Consulting

Global Ambassador for the Institute of Risk Management

RISKINSIGHT

The contents of this information pack

1. Look at modern business needs

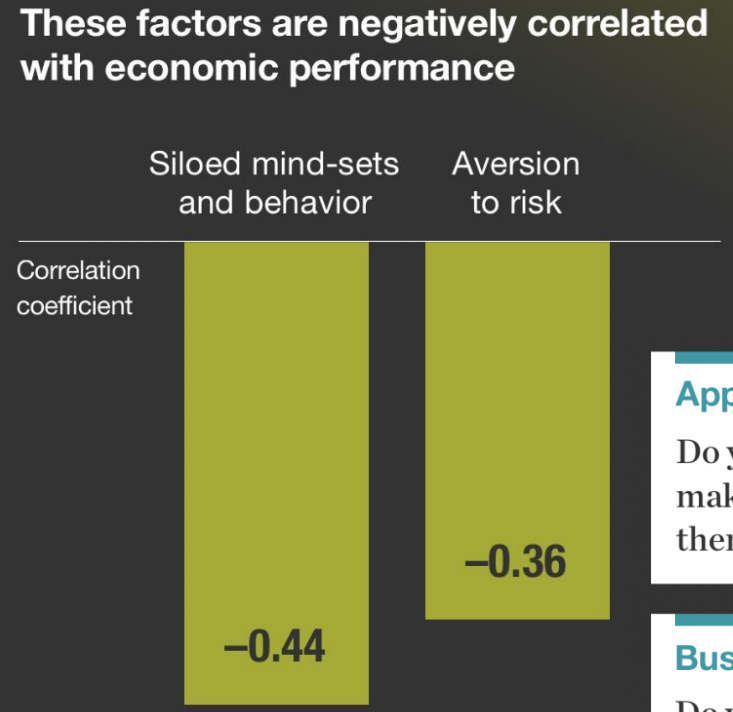
2. Look at good practices in modern risk management

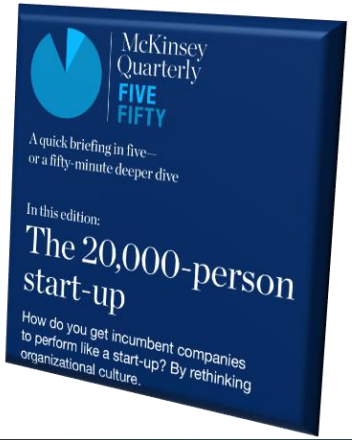
3. Review ISO 31000:2018 and COSO ERM 2017 in light of the first two items

What defines a modern business?

"Today, we are up against businesses that work out of a garage, take risks, operate in a nimble way, and have a different kind of energy and drive. Large incumbent companies that can't create a similar kind of culture just won't be able to compete. One of our rallying cries has been how do you create a 20,000-person start-up?"

Piyush Gupta
CEO of DBS





Appetize risk

Do you trust employees, at all levels, to make big enough bets without subjecting them to red tape?

Bust silos

Do you rotate executives between siloed functions and business units? Have you removed barriers that hinder collaboration?

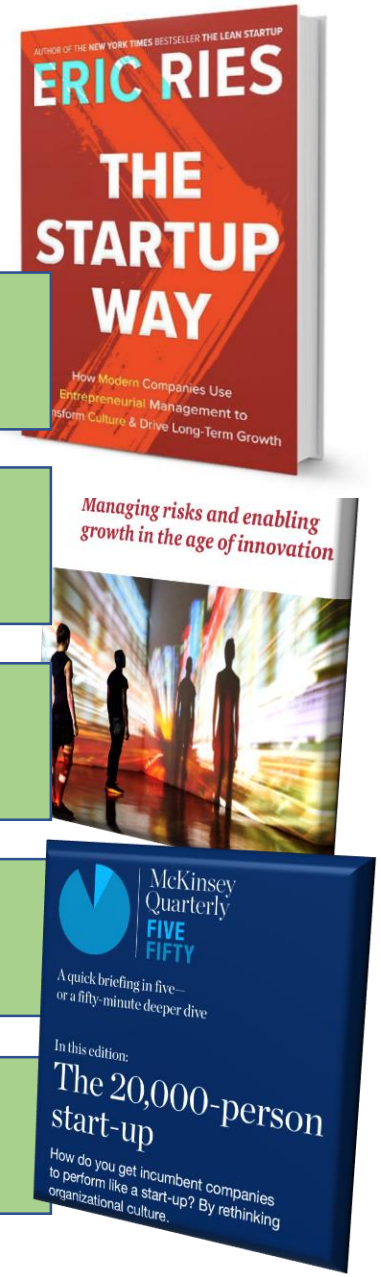
Customer first

Does data lead you to emerging customer behavior patterns and help you tailor your interactions with them?

Source:
McKinsey Five-Fifty, Apr 18
[The 20,000-person start-up]

What defines a modern business?

	KEY AREA OF FOCUS UNTIL NOW		NEW AREAS OF FOCUS
1	Steady growth, Structure & controls	→	Sustained impact Flexible & trusting
2	Big initiatives that take time	→	Rapid experimentation
3	Lots of multi-tasking	→	Passionate believers focus on single initiatives
4	Managers and “subordinates”	→	Leaders empower teams
5	Compete with barriers to entry	→	Compete with continuous innovation

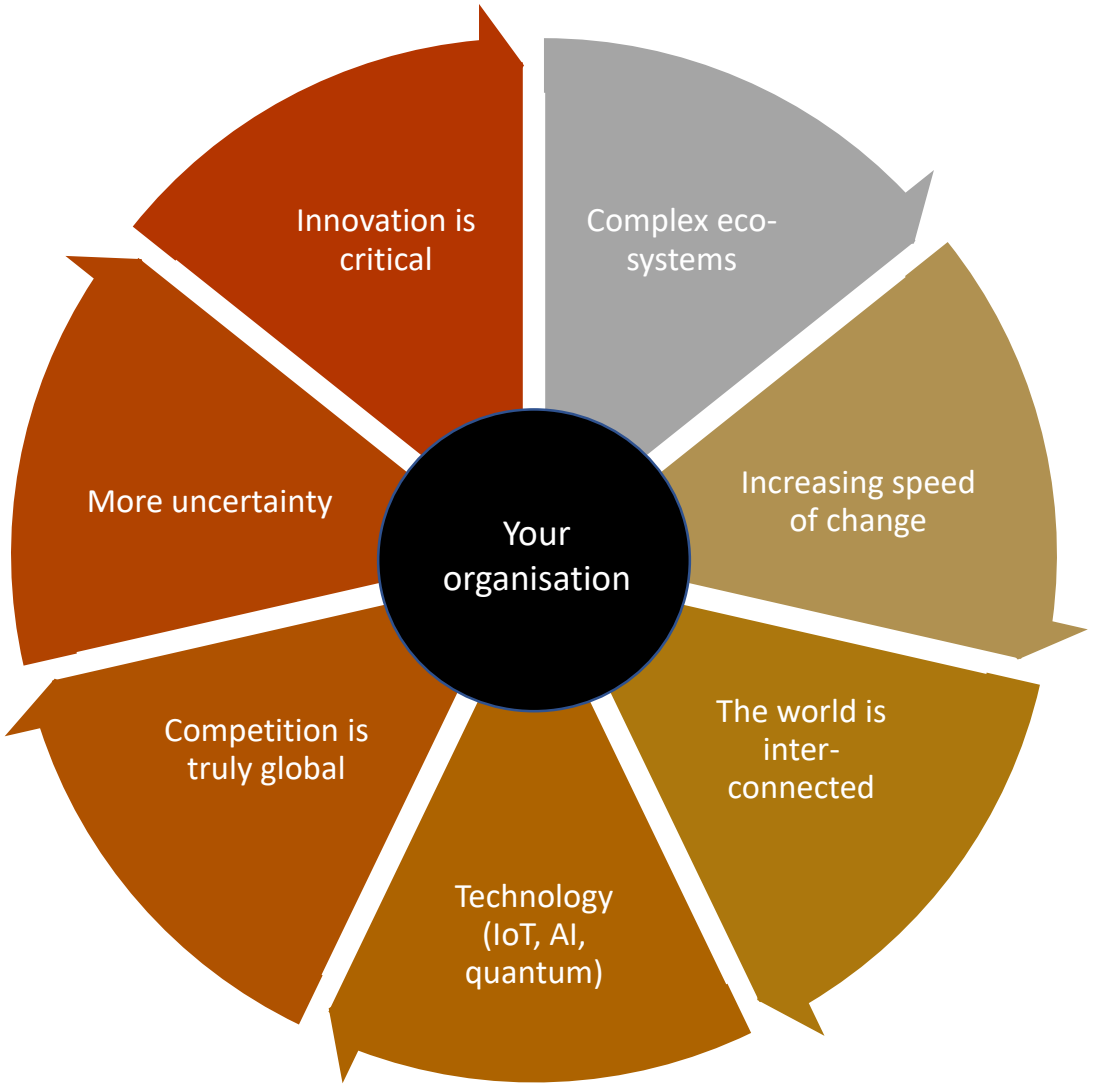


Source: adapted from The Start-up Way website: http://thestartupway.com

What factors does a modern business deal with?

NEW AREAS OF FOCUS

- Sustained impact
  Flexible & trusting
- Rapid experimentation
- Passionate believers focus on single initiatives
- Leaders empower teams
- Compete with continuous innovation



Mapping business elements to ‘risk drivers’

1 Assist strategy & structure

2 Provide good governance

3 Anticipate and adapt

Base

4 Foster a good culture

5 Risk-informed decision-making

6 Help digitisation & innovation

Build

7 Ensure resiliency & reliability

8 Continuous improvement

9 Risk-enabled operations

10 Risk-enabled projects

PDCA

How have ISO responded with ISO 31000?

Jason Brown, Chair of technical committee ISO/TC 262 on risk management that developed the standard:

"The revised version of ISO 31000 focuses on the integration with the organization and the role of leaders and their responsibility. Risk practitioners are often at the margins of organizational management and this emphasis will help them demonstrate that risk management is an integral part of business."

Source: ISO website 2018: https://www.iso.org/news/ref2263.html (provided with permission from Jason Brown)

How have COSO responded with COSO ERM?

Robert B Hirth Jr, COSO Board Chair:

"The complexity of risk has changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of enterprise risk management while asking for improved risk reporting. Our overall goal is to continue to encourage a risk- conscious culture."

PwC quote: the COSO ERM Framework is designed to turn a preventative, process-based risk monologue into a proactive, opportunities-focused conversation to uncover how risk management can create, preserve and realize value.

Source: COSO website 2017: https://www.coso.org/Documents/COSO-Issues-Important-Update-to-ERM-Framework-September-2017.pdf

Who have I spoken to about these standards…?

~15 Risk practitioners (consultants, managers, Heads of Risk)

~ 20 business and public sector professionals (in safety, operations, audit, projects)

What did Risk people tell me?

COSO ERM 2017 is painfully obvious with no innovation

ISO 31000 is really high level, which is fine…

Both focus on the link of risk to objectives – a welcome update

Both say a Risk framework should be tailored – but no guidance

COSO seems to be a bit more logical for me while ISO seems to have become a bit more complicated

They both fall short of explaining risk vs. uncertainty and decision making and their impacts on the management of risk

The definition of risk in ISO 31000 is really confusing…

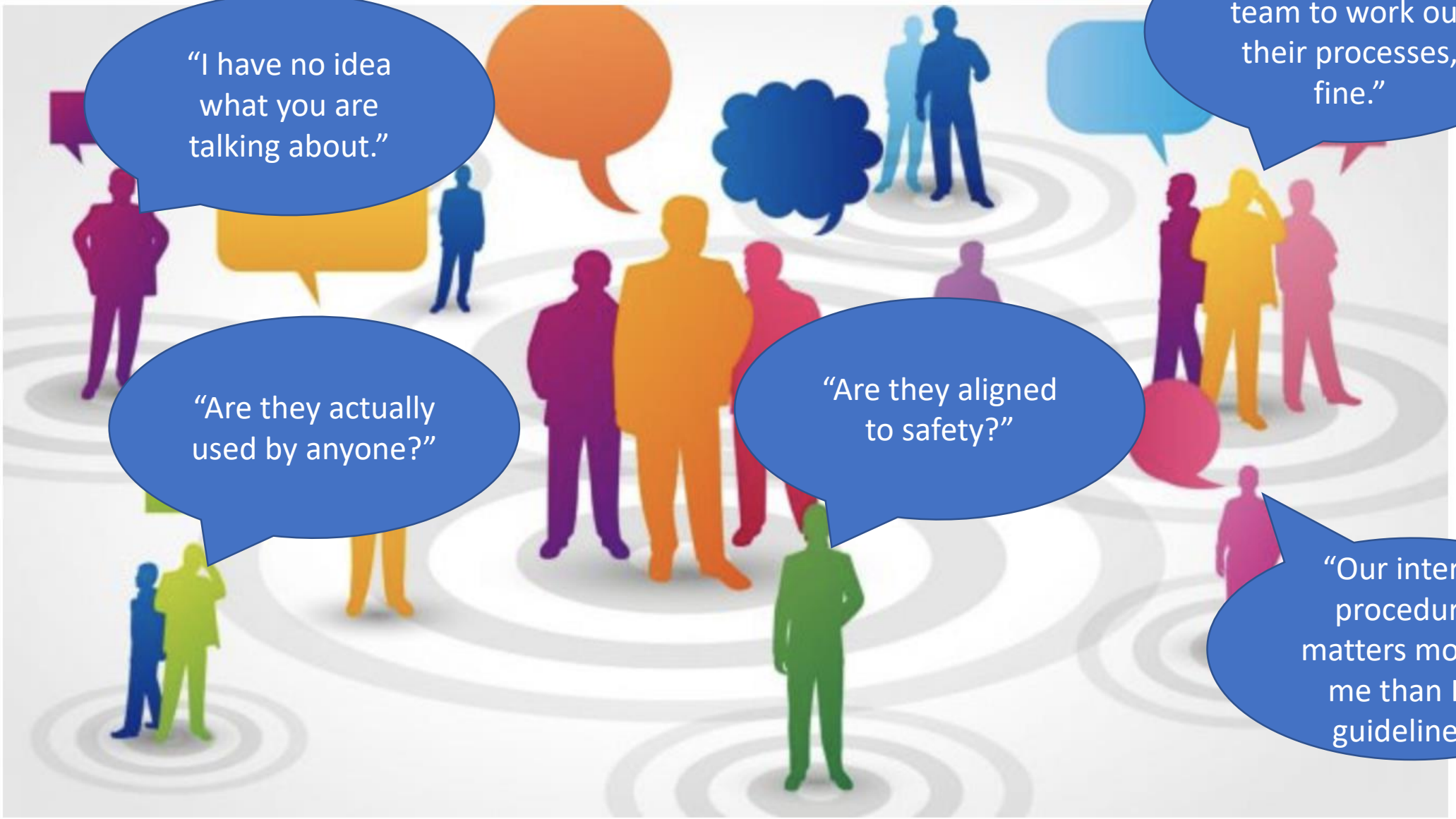
Great guidance on risk appetite in COSO…but why so many principles?

ISO 31000 circles to depict the iterative nature of risk management – great

I didn't know they were both out now…

At face value neither appear to be offering anything radically different, rather both appear to be offering exactly what they did in the past but in a shinier, slicker manner.

What did business people tell me?

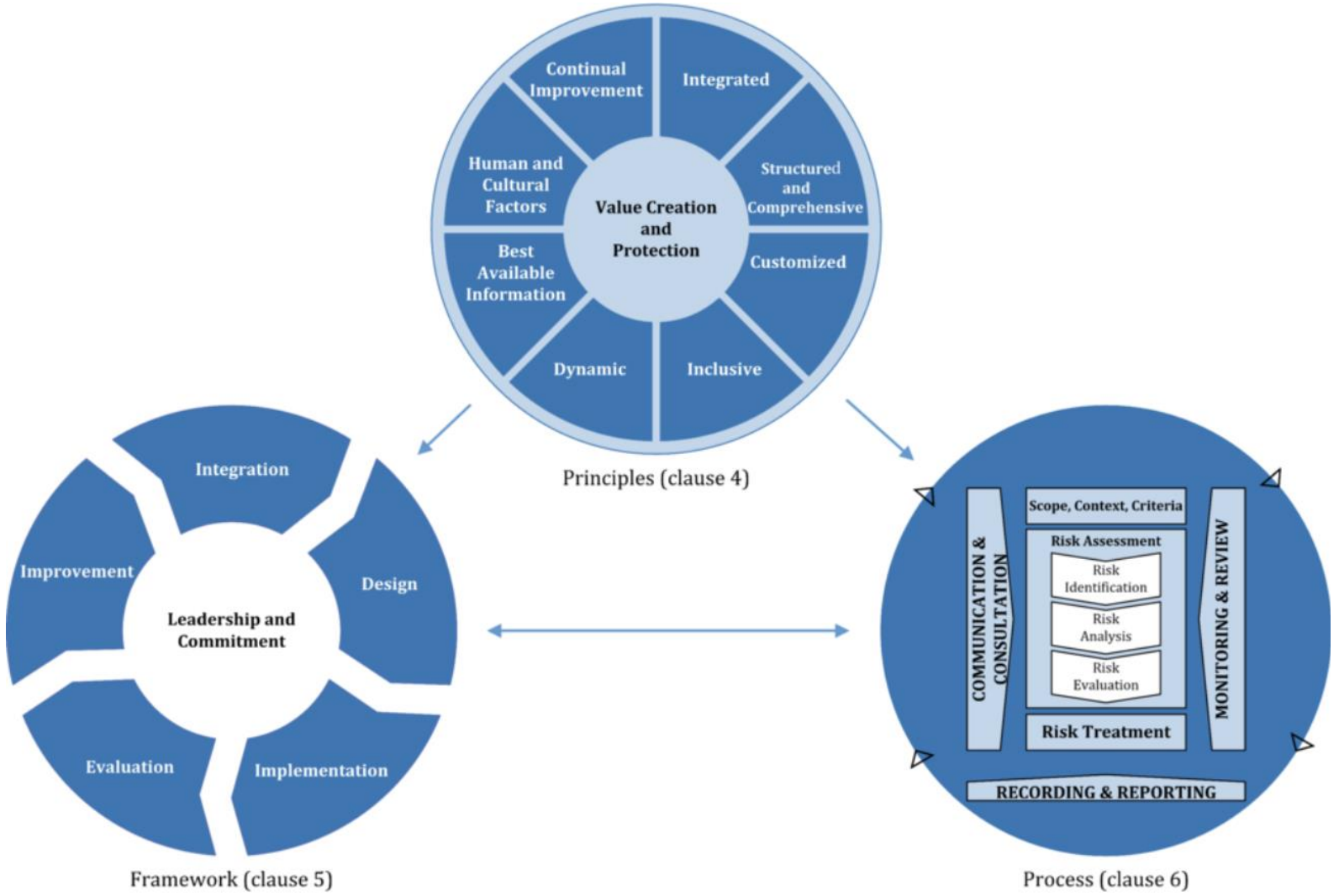


My thoughts on these standards…

ISO 31000: 2018 is **short, flexible** and focused on a few principles.
Integration is key.

The principles can be aligned to modern business needs = good.

The risk framework and process are customised and proportionate to your organisation.



My thoughts on these standards…

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

COSO ERM 2017 is long (265 pages). It is not a ready-made risk framework.

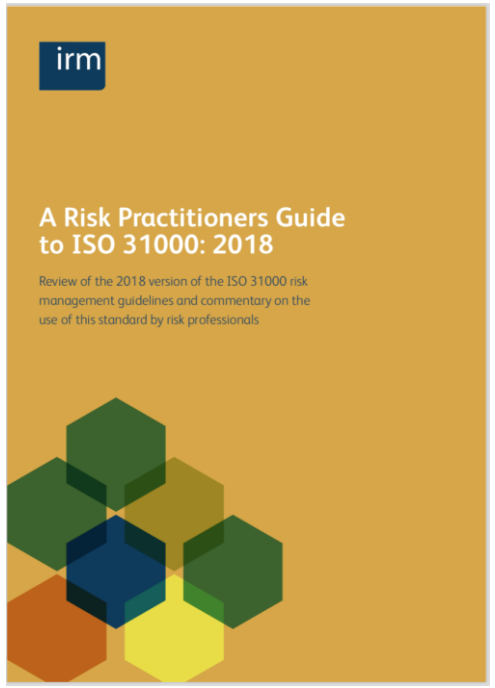
The 20 principles cover a lot. They are guidelines, not templates.

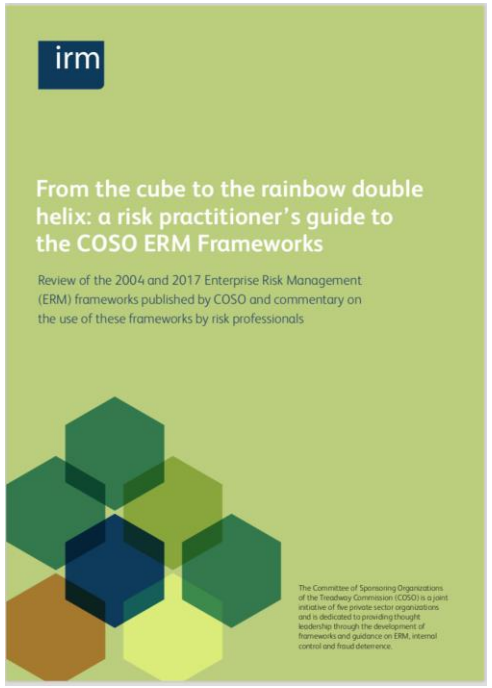
The principles are descriptive; they can **“spur thinking”** on your approach to risk.

Some suggested reading by the IRM

The IRM has an Asia-Pacific wide network of practitioners. We can share and collaborate about risk knowledge and region-specific matters.

For more information, contact Gareth Byatt, Global Ambassador of the IRM.





You need to be a member of the IRM to access these documents.

For articles, newsletters, interviews, papers and tools, visit www.riskinsightconsulting.com

RISKINSIGHT

Home | Why Risk Insight | Services | Forethought | Toolkit | Contact