RIMS Risk Forum 2016 MIDDLE EAST

13 – 14 December | Dubai, UAE

www.RIMS.org/Dubai2016

RIMS the risk management society

SPEAKING THE ‘RIGHT’ LANGUAGE

What is…

language

/ˈlaŋgwɪdʒ/

noun

1. the method of human communication, either spoken or written, consisting of the use of words in a structured and conventional way.
   "a study of the way children learn language"
2. a system of communication used by a particular country or community.
   "the book was translated into twenty-five languages"

"Right" ERM language is one of 20 best ERM practices
(Ingram, 2010)

What language is your organization speaking?

When IA reports to the board, what do they say? What do **YOU** say?

3 x 3 Risk Matrix

LIKELIHOOD				
	Likely	Medium Risk	High Risk	Extreme Risk
	Unlikely	Low Risk	Medium Risk	High Risk
	Highly Unlikely	Insignificant Risk	Low Risk	Medium Risk
		Slightly Harmful	Harmful	Extremely Harmful

CONSEQUENCES

Likelihood →	1	2	3	4	5
Consequence score ↓	Rare	Unlikely	Possible	Likely	Almost certain
5 Catastrophic	5	10	15	20	25
4 Major	4	8	12	16	20
3 Moderate	3	6	9	12	15
2 Minor	2	4	6	8	10
1 Negligible	1	2	3	4	5

Same risks repeated in the '**R**isks **T**hat **M**atter' list in different words.

What is the state of your communications?

Internal Audit

- Areas of risk to be managed.
- Roles and responsibilities
- Impact and Likelihood
- Exposure

Business Functions

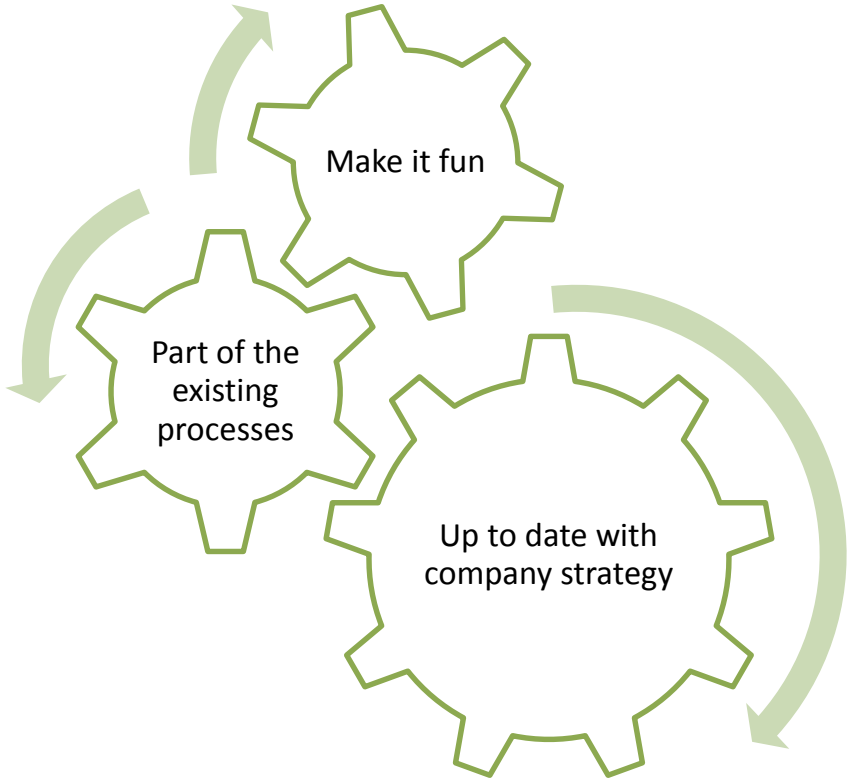
- Are the scenarios, simulation analysis and measurement business approved?
- Do they understand specific risk impacts i.e. financial, operational, reputation, etc.
- What does impact mean for different people? Likelihood?

Board/ Executive Management

- How many risks are you communicating with them?
- Has their appetite been defined? Has this been communicated with the executive management?

A common ERM (business risk) language will enable diverse people to communicate more effectively; and it has to be 'top-down'.

How to go about normalizing the language?



Risk Management bingo

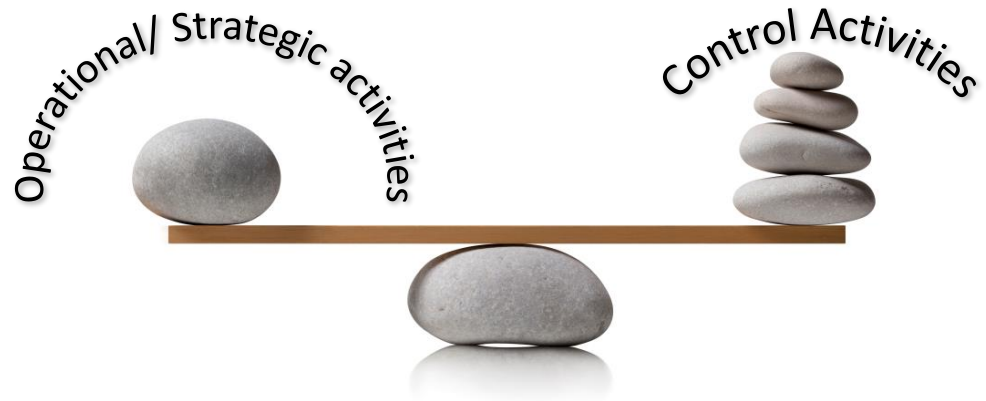
Take the help of Business Excellence to embed risk terminology into the company vocabulary

Discuss the strategy though the lens of risk management

Assurance language

- Risk model
  - Drive risk assessments
  - Strategy review
  - Due diligence
- Risk management glossary, risk processes, etc. (use from the Protiviti paper)

IA audits ERM also. Is the audit only to assess whether ERM is following leading practice?



Nothing authoritative as yet. However, "event categories" samples are laid out in an effort to encompass. But, always check suitability with your own organization.

COSO recommends a "top-down" approach. Management articulates objectives and risk categories and then, specific risk events are identified within each category. Beware of tunnel vision, though!

Business language

- Risk arises from the activities carried out by the entity. If the activities, in turn, the processes are complex (knowingly or unknowingly), it'll be difficult to build on it.
- What are the risks embedded within the processes

  E.g. "We are a nimble/ agile organization" – needs 10 signatures to change a website

Operations

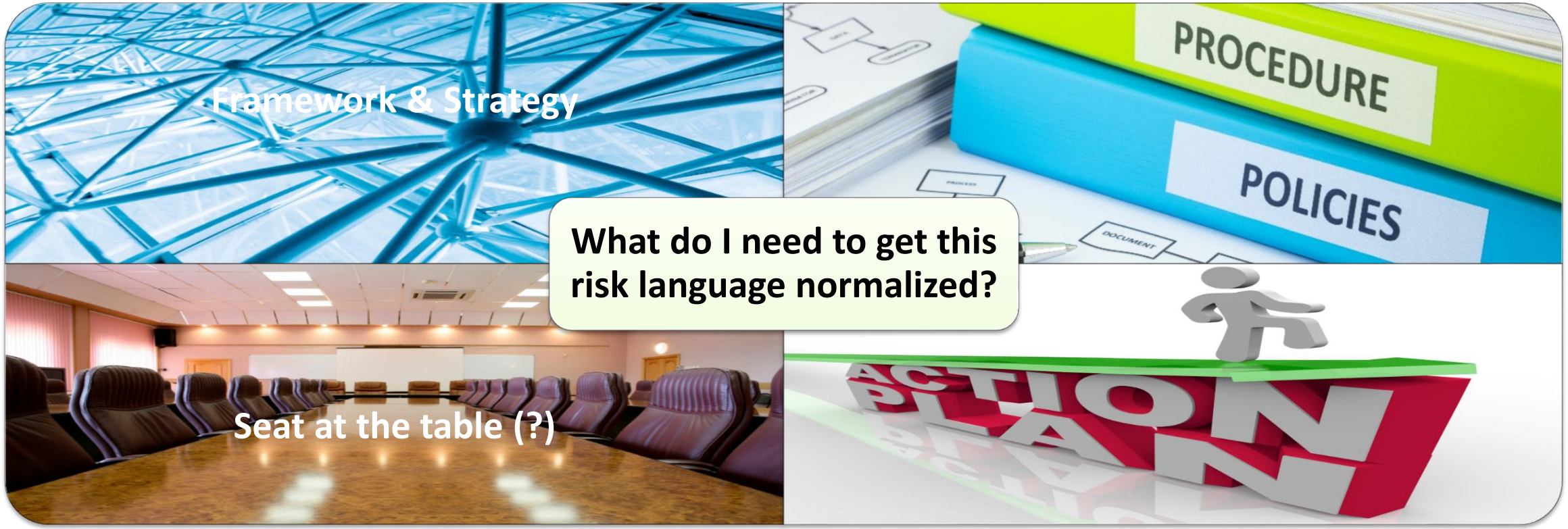
- If organization's strategy and priorities are changing without ERM keeping up, the risks, it's appetite and tolerance can become outdated (you are not speaking the same language).
- If the intent is to only mitigate the risks to being it down to acceptable limits, it's one side of the coin. What about the other side, "How much risk should we take on to begin with?"

Strategy

Risk Maturity Model Exercise

Adoption of ERM based approach	Uncovering risks	ERM Process Management	Risk Appetite Management	Root Cause Discipline	Business Resiliency and Sustainability	Performance Management
Does each business area, function and process identify their own risks in the context of a common risk language?	Is standardized evaluation criteria for risk impact, likelihood and control effectiveness used…	Is a common risk management framework available to and used by all business areas?	Is the risk tolerance formally defined for each business area and category of risk?	Is uniform ERM vocabulary and information classification used by all departments?	Are root cause categories considered in planning?	Do business areas consider their impact on other areas of the organization when determining their goals?

Resources needed



Goals and objectives

- Documentation (not just policies and procedures)
- Risk Classifications
  - Categories (give each area to the most relevant function)
  - Levels
  - Likelihood
  - Internal/ external
- Appetite (document and communicate – NOW)

THE ERM ROADMAP

COMPONENT OF COSO FRAMEWORK	SET FOUNDATION		BUILD CAPABILITIES			ENHANCE CAPABILITIES		
	Adopt common language	Establish oversight and governance	Assess risk and develop responses	Design/ implement capabilities	Continuously improve capabilities	Quantify risk enterprise-wide	Improve enterprise performance	Establish sustainable competitive advantage

Jacxine Fernandez

+965 98800743

jacxine@yahoo.com

References

- Enterprise Risk Management Initiative Staff, 2007. Risk Language. [Online]
  Available at: https://erm.ncsu.edu/library/article/languageofrisk
  [Accessed Nov 2016].
- Haimes, Y., 2009. Risk Analysis. In: On the complex definition of risk: a systems-based approach. s.l.:s.n., pp. 1647-54.
- Ingram, D., 2010. Eight Practices at the Heart of ERM. [Online]
  Available at: http://www.willisre.com/documents/publications/Analytics/Analytics/Enterprise_Risk_Management/ERM_Fundamentals.pdf
  [Accessed Nov 2016].
- Ingram, D., 2010. Planning and building an ERM program. [Online]
  Available at: https://riskviews.files.wordpress.com/2010/10/erm_intro_kazak_.pdf
  [Accessed Nov 2016].
- Marks, N., 2015. Explaining Risk Management in Common Sense Language. [Online]
  Available at: https://iaonline.theiia.org/blogs/marks/2015/explaining-risk-management-in-common-sense-language
  [Accessed Nov 2016].
- Miccolis, J., 2002. The Language of Enterprise Risk Management: A Practical Glossary and Discussion of Relevant Terms, Concepts, Models, and Measures. [Online]
  Available at: https://www.irmi.com/articles/expert-commentary/the-language-of-enterprise-risk-management-a-practical-glossary-and-discussion-of-relevant-terms-concepts-models-and-measures
  [Accessed Nov 2016].
- protiviti, 2006. Guide to Enterprise Risk Management - FAQ. [Online]
  Available at: http://www.ucop.edu/enterprise-risk-management/_files/protiviti_faqguide.pdf
  [Accessed 2016].
- Westerman, G. & Hunter, R., 2009. Developing a Common Language about IT Risk Management. IESE Insight, 2(1), pp. 21 - 27.
- Zawoyski, S. V., Chagares, M. J. & Hooper, K., 2015. How strategic is your ERM program?. [Online]
  Available at: www.pwc.com/us/ermexcellenceseries
  [Accessed Nov 2016].

Business language