

Risk IT and COBIT in practice

Contents

- History and Context
- Stakeholders and Target Audience
- Key Features and Principles
- What Is Risk IT?
- Which Issues Can It Help to Resolve?
- Early Examples and Cases
- Q & A

HISTORY AND CONTEXT

Risk IT History

- Is Risk IT New ?

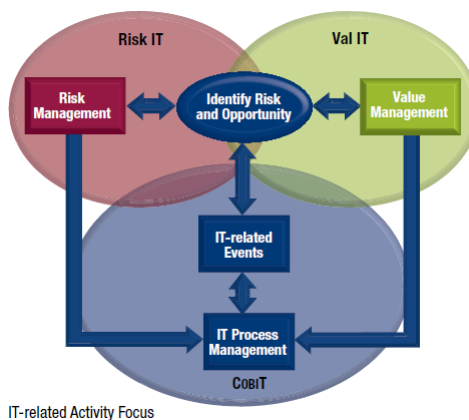
Yes – it is a new framework and publication

No – ISACA has been providing guidance on how to deal with IT risk for decades

Risk IT Context



Business Objective—Trust and Value—Focus



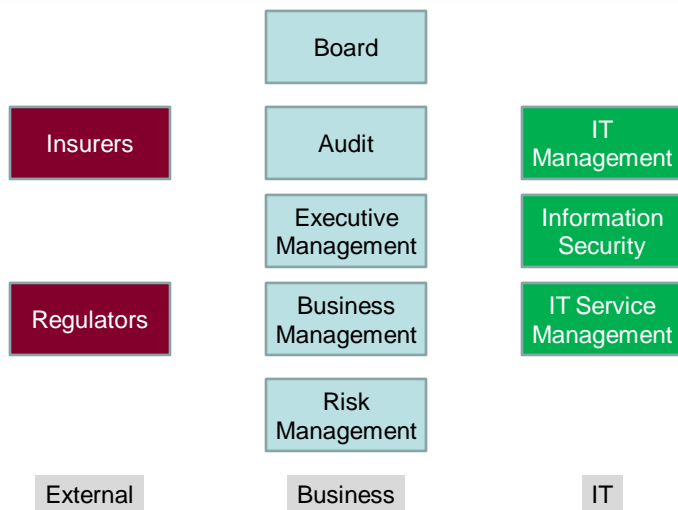
Risk IT Future



- The Risk IT Future is called COBIT 5.
- COBIT 5 will, amongst many other things, integrate the guidance in COBIT, Val IT and Risk IT.
- None of the current materials will be eliminated, but
 - They will be integrated with each other.
 - They will be even easier to access.
 - They will have more attention for the culture aspect and the human factor...

KEY STAKEHOLDERS

Risk IT Stakeholders



KEY RISK IT FEATURES AND CONCEPTS

Risk...

10



Risk...



11



- What is the risk ?
- Lesson learnt:
 - Obvious risk not always the most important.
 - Doing only superficial analysis may be dangerous.

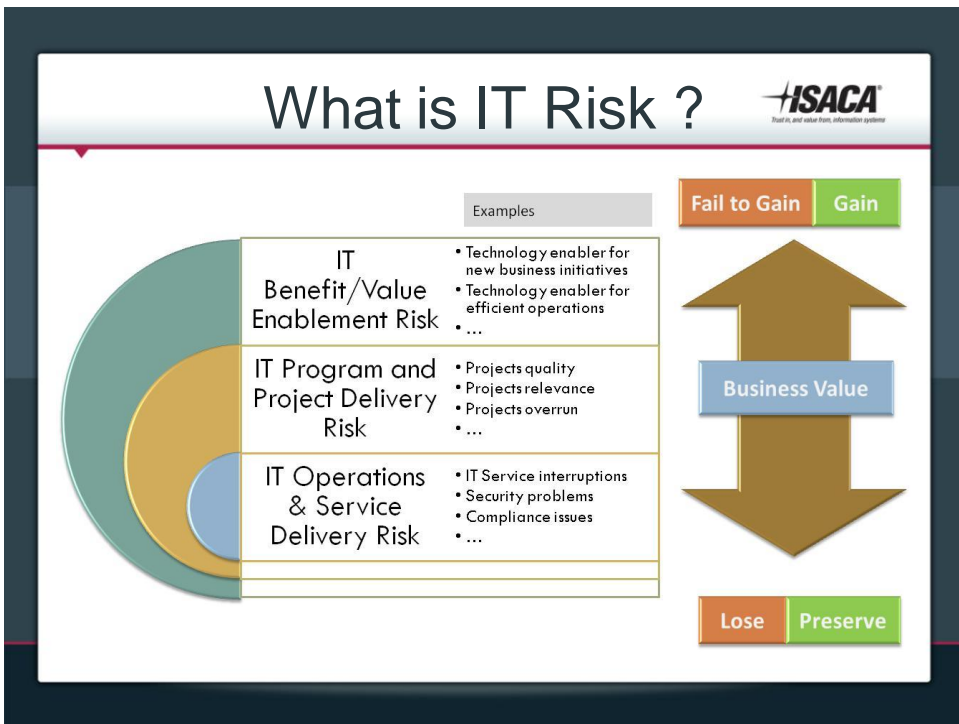
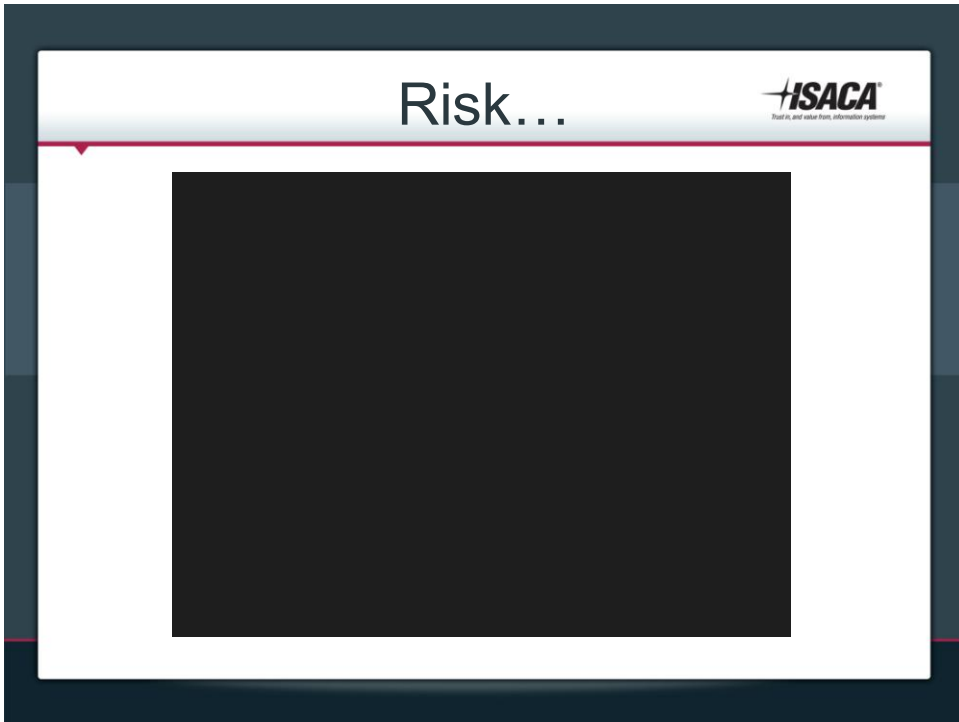
Risk...


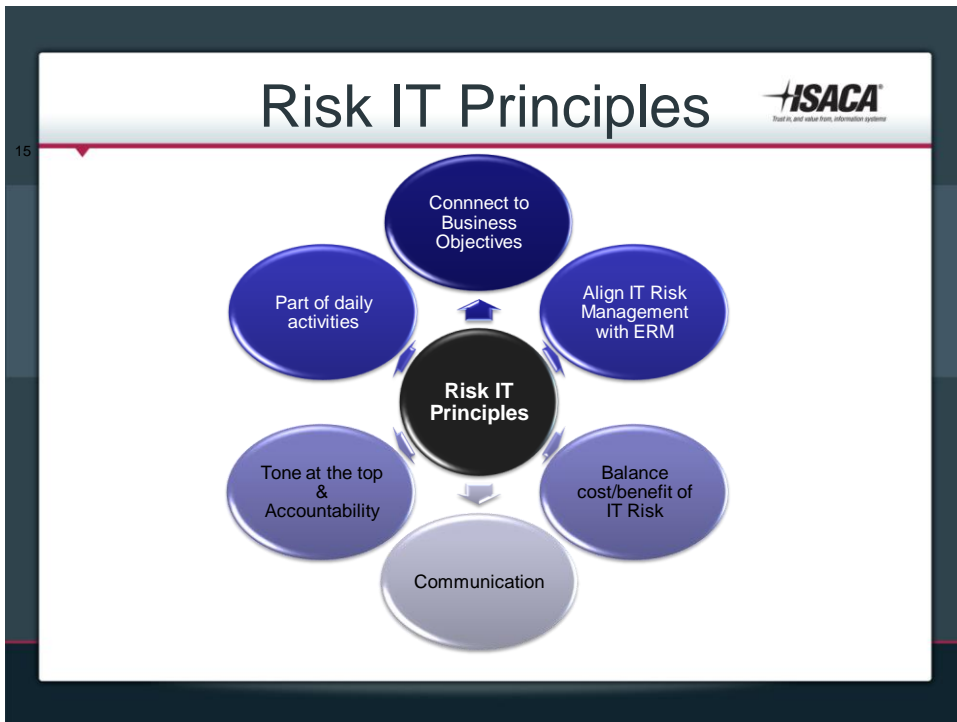


12

- What is the risk here?
- It depends...
- It depends on the objective:
 - If getting to the other side safe and dry: yes, there is risk
 - If having fun during a team building exercise: probably much less





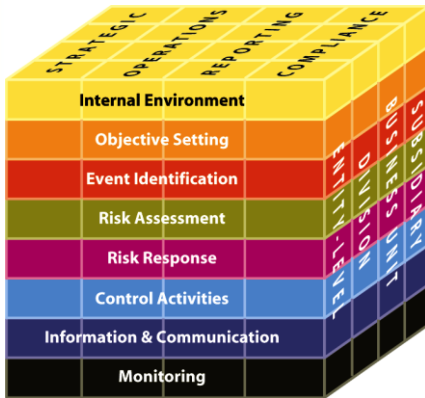


WHAT IS RISK IT IN PRACTICE?

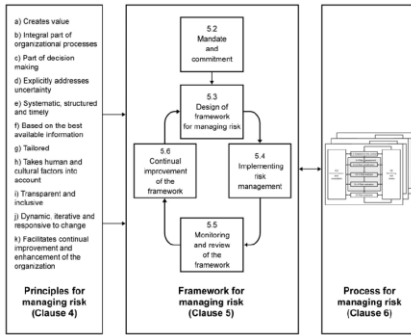
Risk IT Inspiration



COSO ERM



ISO 31000

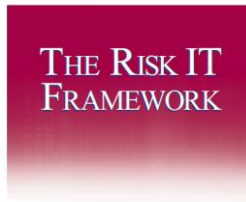


18

Risk IT in Practice...



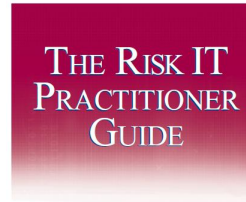
Risk IT Framework



Principles
Process Details
Management Guidelines
Maturity Models



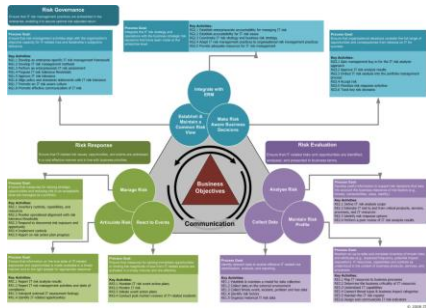
Risk IT Practitioner Guide



Risk Universe, Appetite and Tolerance
Risk Awareness, Communication and Reporting
Expressing and Describing Risk, Risk Scenarios
Risk Responses and Prioritization
Using CoITSM and Net ITSM



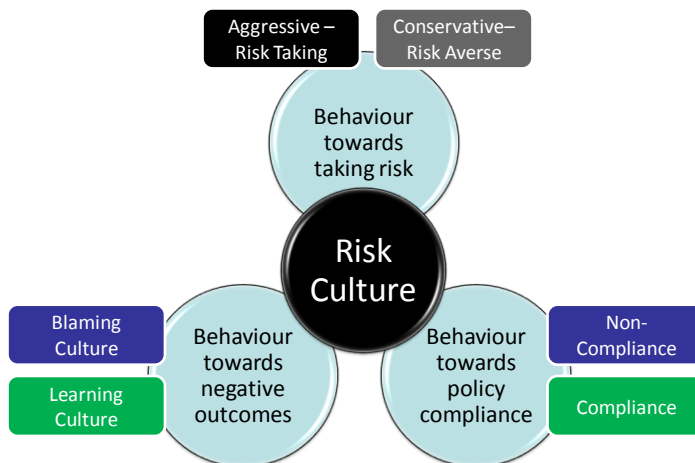
Risk IT Framework



- Process Model (similar to COBIT and Val IT)
- Three domains
 - Risk Governance
 - Risk Evaluation
 - Risk Response
- Additional components to further assist

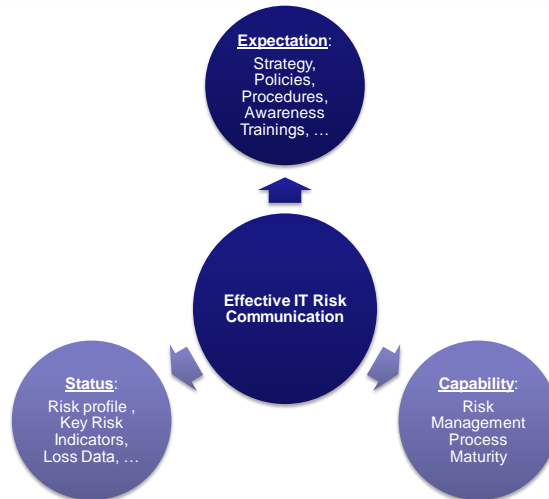
19

Risk Culture



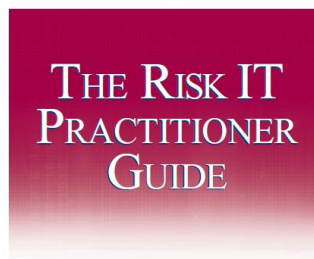
20

Communication on IT Risk



21

Risk IT Practitioner Guide



Risk Universe, Appetite and Tolerance
Risk Awareness, Communication and Reporting
Expressing and Describing Risk, Risk Scenarios
Risk Responses and Prioritisation
Using COBIT® and Val IT™

Risk IT
BASED ON COBIT®

ISACA
INTEGRATED INFORMATION SECURITY PROFESSIONALS

- Eight sections
 - Risk Universe & Scoping
 - Risk Appetite & Risk Tolerance
 - Risk Awareness, Communication & Reporting
 - Expressing & Describing Risk
 - Risk Scenarios
 - Risk Response & Prioritisation
 - Risk Analysis Workflow
 - Mitigation of Risk using COBIT & Val IT
- Appendix
 - Risk IT compared to COSO ERM, ISO31000, ISO27005

WHICH ISSUES CAN IT HELP TO RESOLVE?

Risk IT Benefits

- Risk IT Benefits
 - End-to-end guidance on risk management
 - ERM principles applied
 - Business-oriented
 - Promotion of risk responsibility throughout enterprise
 - Tools and techniques to support all IT risk management activities
 - Process model to allow process improvement

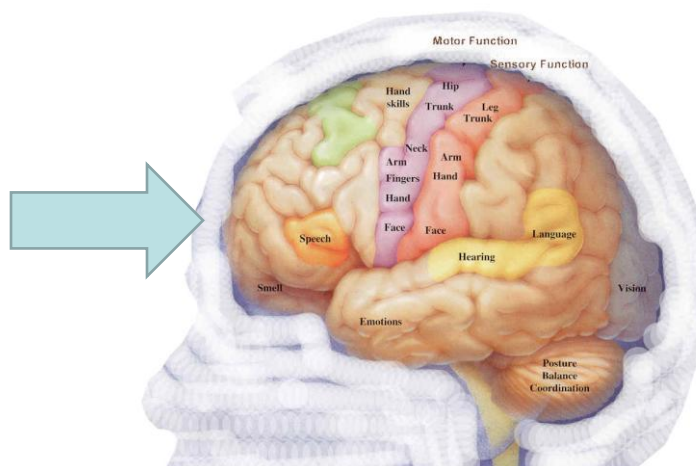
Risk IT: When and How? ISACA Trust it, and value from, information systems

- Short answers
 - When to use Risk IT: For all IT Risk management-related activities
 - How to use Risk IT: Do not implement Risk IT... but adopt it.

Risk IT & COBIT ISACA Trust it, and value from, information systems



Risk IT & COBIT



What to Do With Risk IT ?



31

- It depends...
- Some possible uses:
 - Integrate IT risk management practices with existing ERM practices
 - (Self-)Diagnosis of risk management processes and responsibilities
 - RACI Charts
 - Process Maturity

What to Do With Risk IT ?

32

- Some more possible uses:
 - Communication and risk profiles – which information on risk to communicate to whom?

What to Do With Risk IT ?

33

- Some more possible uses:
 - Develop a consistent risk taxonomy for expressing and analysing risk
 - Conduct a completeness check against some tables (risk scenarios).

What to Do With Risk IT ?

34

- Some more possible uses:
 - Develop and maintain a relevant set of risk scenarios.
 - Discussing and defining risk appetite within an organisation

Using Risk IT?

- And one more reason....
- It's FREE (at www.isaca.org/riskit)

EARLY EXAMPLES AND CASES

Early Experience (1)

- Case: Company in telecom industry, having to resolve an audit recommendation on inadequate information security
- Outcome:
 - Techniques used out of the *Risk IT Practitioner Guide*
 - Easier to convince management to support investments in IT security
 - Allowed to identify very quickly the major weaknesses and risks
 - Opening the discussion on better enterprise risk management
 - Allowed to capitalise on (some of the) Sarbanes-Oxley investments
 - Risk analysis methodology will be used going forward for ISO27000 initiative

Early Experience (2)

- Case: Review an organisation's risk management practices
- Outcome:
 - Used RACI chart's dimensions (roles and responsibilities) to compare and assess current practices
 - Used maturity model to assess risk management process maturity and suggest improvements

Early Experience (3)

- Case: Bring an objective view to claimed privacy risks
- Outcome:
 - Defined taxonomy and risk appetite
 - Defined focussed set of risk scenarios
 - Performed and discussed high-level risk analysis

Lessons Learnt (1)

- Lessons learnt so far...
 - ‘Breadth’ of scope – especially in terms of risk management activities and in terms of range of IT risks – is appreciated
 - Constructs in both books are found to be useful, depending on needs
 - RACI charts
 - Maturity models
 - Risk scenarios constructs
 - Generic risk scenarios and mapping with COBIT and Val IT

Lessons Learnt (2)

- Lessons learnt so far...
 - Developing and adopting risk impact criteria – and linking them to strategic objectives – remains a challenge for many organisations
 - Once this challenge has been overcome, it can be an eye-opener for general ERM purposes as well

Lessons Learnt (3)

- Lessons learnt so far...
 - People starting to ask for tools beyond the current 'compliance-checking' tools
- Emphasize that Risk IT
 - Is the link between very high-level ERM and (technical) IT risk management and mitigation
 - And therefore is NOT the detailed risk checklist at all possible levels of detail



Q&A

Dirk Steuperaert



44

- Education
 - Master Engineering (Ugent, 1986)
 - Master Computer Auditing (UAMS, 1995)
 - CISA (1995), CGEIT (2009)
- Professional Career
 - Software Engineer (SWIFT) (1988-1992)
 - IT Auditor (SWIFT, BBL, Cedel) (1992-1997)
 - Consultant (PwC, 1997-2008)
 - Independent Consultant (2008 - ...)
- Professional Organisations
 - ISACA (COBIT Steering Committee, Risk IT Task Force, COBIT 5 Development Team)
- Contact
 - Dirk.steuperaert@it-in-balance.be

