



Spotlight on ISACA's new framework, Risk IT



- IT risk is receiving growing attention from executive management, risk managers, regulators etc. The COBIT® Framework provides a generally accepted control framework – but it does not provide the full detail required for comprehensive risk management
- In this session, you will find out about ITGI's newest initiative: a new IT related risk management framework. I will discuss the issues around IT related risks, which standards and frameworks address this risk, which elements are still lacking, and how the new framework will address these issues



Steven Babb



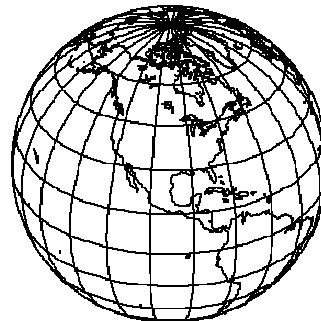
- **Senior Manager at KPMG**
 - Lead KPMG's national IT risk management service
- **Working with ISACA at an International level in various capacities:**
 - Member of the Risk IT Task Force
 - Member of the Frameworks committee
 - Member of the COBIT 5 Task Force
 - Member of the Cloud Computing Task Force



ISACA – at a glance



- Founded in 1969; non-profit, independent association that helps members achieve greater trust in, and value from, their information systems
- More than 86,000 constituents in 160 countries
- More than 180 chapters worldwide
- Sponsors international conferences and education
- Publishes original research
- Develops international IS audit and control standards
- CISA, CISM, CGEIT and CRISC certifications
- Developed and continually updates the COBIT, Val IT and Risk IT frameworks, which help professionals and enterprise leaders fulfil their IT governance responsibilities and deliver value to their business



Agenda



- What is IT related risk management?
- Risk management essentials
- *Risk IT*
 - Where does it fit in?
 - Development approach?
 - Who benefits from *Risk IT*?
 - Guiding principles and essentials
 - Framework and domain overview
- Questions



Agenda



- What is IT related risk management?
- Risk management essentials
- *Risk IT*
 - Where does it fit in?
 - Development approach?
 - Who benefits from *Risk IT*?
 - Guiding principles and essentials
 - Framework and domain overview
- Questions



What is IT related risk management?



- Covering all IT related risks, **not** limited to Information Security only!
 - Late project delivery, compliance issues, misalignment between IT and business, IT service delivery problems, inflexible IT architecture, obsolete IT architecture,...
- Covering all Risk Management activities
 - Risk governance, risk reporting, integration with ERM, etc.
- **Covering business risks due to IT related activities**

**IT Related risk = materialised business impact
because of an IT related event**



What is IT related risk management?



A Balance is Essential

- Risk and value are two sides of the same coin
- Risk is inherent to all enterprises
- Understanding risk and managing it is key for creating and safeguarding value

But...

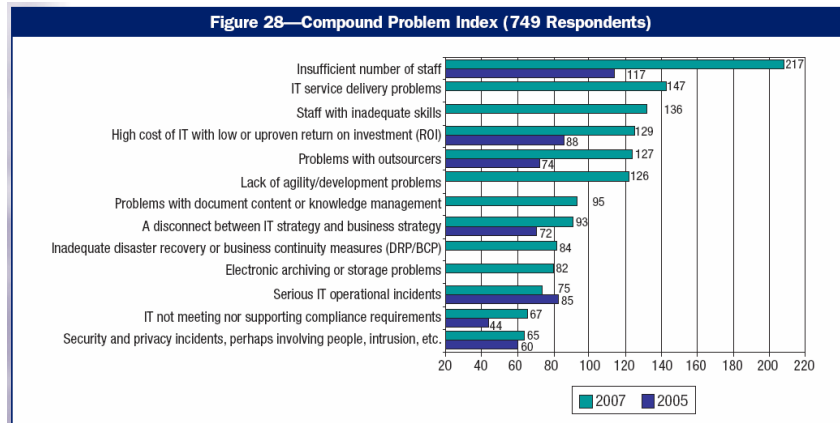
- Need to ensure opportunities for value creation are not missed by trying to eliminate all risk



What is IT related risk management?



ITGI survey on IT related problems:



What is IT related risk management?



Why Care About IT related Risk?

- Enterprises are dependent on automation and integration
- Need to cross IT silos of risk management
- Important to integrate with existing levels of risk management practices



Agenda



- What is IT related risk management?
- Risk management essentials
- Risk IT
 - Where does it fit in?
 - Development approach?
 - Who benefits from Risk IT?
 - Guiding principles and essentials
 - Framework and domain overview
- Questions



Risk Management Essentials



What are some essential qualities or features of a good IT related risk management framework?

- A. Comprehensive view on risk management, not only mechanical/technical
- B. Specific for the subject matter, i.e. IT
- C. End-to-end view on the subject matter, i.e. broadest view on IT related risks
- D. Business oriented
- E. Provide a continuous process, from risk identification to continuous monitoring and feedback
- F. Cover all risk treatment options
- G. Availability / Accessibility



Risk Management Essentials



Where does COBIT fit?

		COBIT 4.1 Product Suite	Comment
A	Comprehensive view on risk management, not only mechanical/technical	✓	The Risk dimension is mentioned throughout the framework
B	Specific for the subject matter, i.e. IT Related	✓✓	COBIT is all about IT controls
C	End-to-end view on the subject matter, i.e. complete view on IT related risks	✓	COBIT does not describe IT related risk in any explicit form, although the risk management dimension implicitly is present throughout the framework. COBIT also goes beyond pure security risk.
D	Business oriented	✓	COBIT provides a link to Business Goals and IT Goals, thus providing a business orientation.
E	Provide a continuous process, from risk identification to continuous monitoring and feedback	✗	COBIT is a process model, but is not specific to risk, or risk management is not made explicit; it is also not an end-to-end model for risk management
F	Cover all risk treatment options	✗	COBIT specifies IT controls, but without linking them back to specific risks; it also does not describe other risk treatment options in detail.
G	Availability / Accessibility of the Framework	✓✓	COBIT is publicly and freely available



Other ISACA Guidance



- ISACA **does** provide several instances of guidance on IT Related risk management, e.g.
 - COBIT 4.1 – Process PO9
 - Assurance Guide
 - Control Objectives for Basel II
 - IT Governance Series – IT Risk Management
 - Security Baseline
 - Control Objectives for Sarbanes Oxley



Other frameworks and guidance



- What other guidance is around for IT Related Risk Management ?

- COSO ERM
- NZS/AS 4360 – ISO31000
- ISO 27002
- ISO 27005
- OCTAVE
- ISF
- CRAMM
- Other (national) initiatives



- Other publications

- Westerman & Hunter book on IT Risk Management – Turning Business Threats into Competitive Advantage



COSO ERM



		COSO ERM	Comment
A	Comprehensive view on risk management, not only mechanical/technical	✓✓	Comprehensive view on Risk Management
B	Specific for the subject matter, i.e. IT Related	✗	Not specific to IT related risk at all.
C	End-to-end view on the subject matter, i.e. complete view on IT related risks	✗	End to end view on risk, but not on IT related risk
D	Business oriented	✓	Embedded in definition of risk, but not really specific or detailed treatment.
E	Provide a continuous process, from risk identification to continuous monitoring and feedback	✓	Provides end-to-end view, but not structured in the form of a process model.
F	Cover all risk treatment options	✓✓	
G	Availability / Accessibility of the Framework	✓	Not Free



ISO 31000



		ISO31000	Comment
A	Comprehensive view on risk management, not only mechanical/technical	✓✓	
B	Specific for the subject matter, i.e. IT Related	✗	
C	End-to-end view on the subject matter, i.e. complete view on IT related risks	✗	Very Generic
D	Business oriented	✓	
E	Provide a continuous process, from risk identification to continuous monitoring and feedback	✓✓	Provides guidance on risk management practices to be applied, but not a full fledged process model
F	Cover all risk treatment options	✓✓	
G	Availability / Accessibility of the Framework	✓	Will be available against small fee



ISO 27005



		ISO27005	Comment
A	Comprehensive view on risk management, not only mechanical/technical	✓✓	
B	Specific for the subject matter, i.e. IT Related	✓✓	
C	End-to-end view on the subject matter, i.e. complete view on IT related risks	✓	Security Focus
D	Business oriented	✓	
E	Provide a continuous process, from risk identification to continuous monitoring and feedback	✓	Provides guidance on risk management practices to be applied, but not a full fledged process model
F	Cover all risk treatment options	✓✓	
G	Availability / Accessibility of the Framework	✓	Will be available against small fee



Agenda



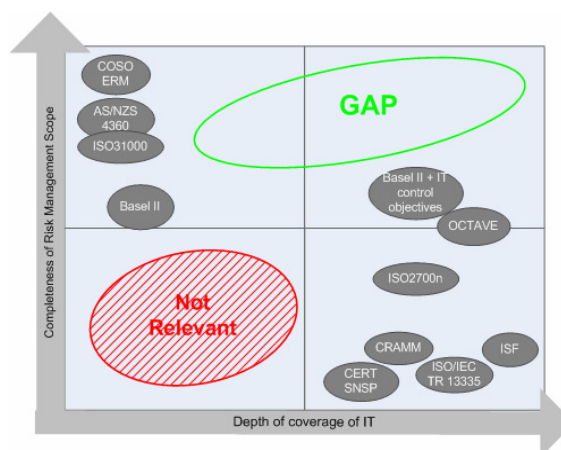
- What is IT related risk management?
- Risk management essentials
- *Risk IT*
 - Where does it fit in?
 - Development approach?
 - Who benefits from *Risk IT*?
 - Guiding principles and essentials
 - Framework and domain overview
- Questions



Where *Risk IT* fits in



- Standards and frameworks are available, but are either too:
 - Generic enterprise risk management oriented
 - IT security oriented
- No comprehensive IT-related risk framework available (until now)



Risk IT



- *Risk IT* is the first global IT-related risk guidance to provide a comprehensive view of *business* risks related to IT initiatives
- *Risk IT* helps enterprises manage risk to achieve goals, seize opportunities and seek greater return
- Although it is based on, and extends COBIT, *Risk IT* provides excellent stand-alone guidance
- *Risk IT* helps integrate other generic and domain-specific risk management standards and practices



Risk IT



This is not limited to information security. It covers *all* IT-related risks, including:

- Late project delivery
- Not achieving enough value from IT
- Compliance
- Misalignment
- Obsolete or inflexible IT architecture
- IT service delivery problems

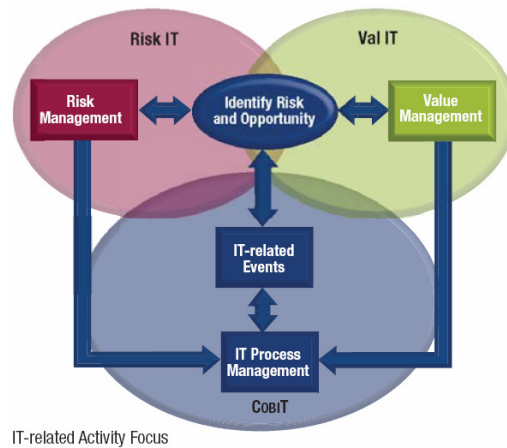


Risk IT

Risk IT complements and extends COBIT and Val IT to provide a *comprehensive IT governance* guiding resource:

- COBIT – IT governance and control
- Val IT – Investment and Portfolio management

Business Objective—Trust and Value—Focus



Risk IT

Practitioner-driven Requirements

Developed to fill the needs of enterprise leaders

Functional Requirements

- Link to business risk management approaches
- Use an end-to end business process performance approach
- Integrate silos of technology risk management

Non-functional/Ease of Use Requirements

- Practical stand-alone guidance; extends COBIT and Val IT
- Continuous process model, supported by maturity models and practical tools
- Includes a framework and good practice guidance



Risk IT



Developed by ISACA International Experts

- IT and business leaders from around the world who are members of ISACA volunteered thousands of hours to share their expertise
- The development team provided an exposure draft, which resulted in 1,700 SME and public comments



Risk IT



Unique to the Marketplace

- Brings together all aspects of IT risk, including value, change, availability, security, project and recovery
- Links with *enterprise wide* risk management concepts and approaches, such as COSO ERM, ARMS and ISO 31000
- Offers a single, comprehensive view of IT-related business risks



Risk IT



Who Benefits from *Risk IT*?

- All enterprises that use IT, whether one-person shops or multinational conglomerates
- Can be customised for any type of enterprise in any geographic location

Specifically:

Boards and executive management; C-suite
Corporate and operational risk managers
IT management
IT service managers
Regulators

IT security managers
Enterprise governance officers
Business managers
IT and external auditors



Risk IT



Guiding Principles of Risk IT

- Always connect to enterprise objectives
- Align the management of IT-related business risk with overall enterprise risk management
- Balance the costs and benefits of managing risk
- Promote fair and open communication of IT risk
- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Understand that this is a continuous process and an important part of daily activities



Risk IT – The “What”



- The *Risk IT Framework*
 - *Risk management essentials*
 - Risk appetite & tolerance, responsibilities and accountability for IT risk management, awareness and communication, risk culture, business impact and risk scenarios, key risk indicators (KRI's), risk response definition and prioritisation
 - *How Risk IT extends and enhances COBIT and Val IT*
 - *Process model*
 - Input-output tables, RACI (Responsible, Accountable, Consulted, Informed), Goals and Metrics
 - *Maturity model*
 - *Appendices*
 - Various reference materials

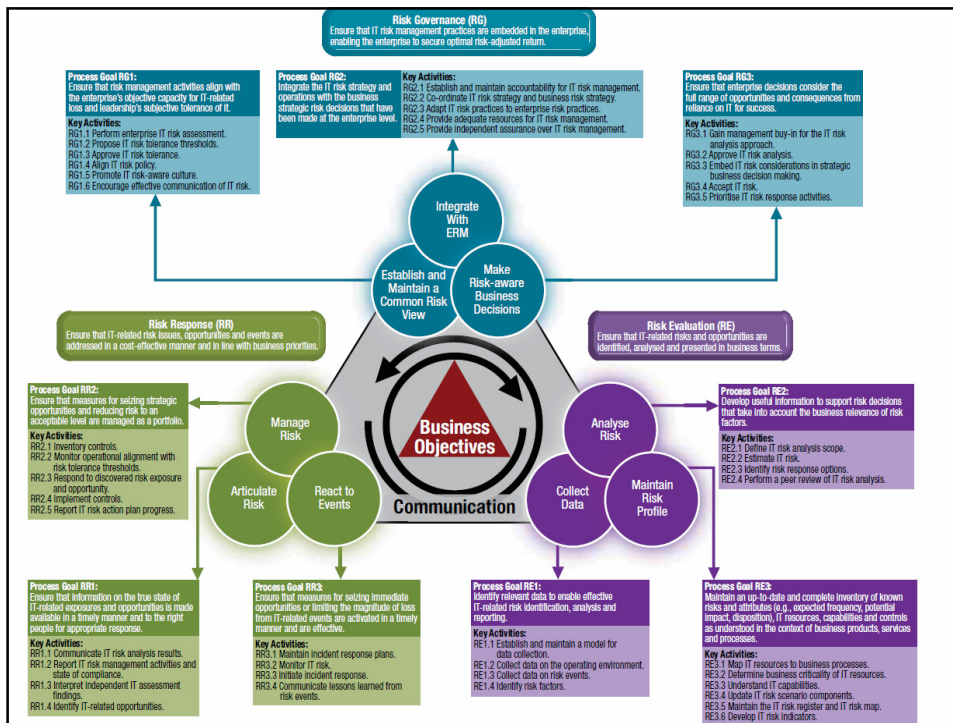


Risk IT – The “How”



- The *Risk IT Practitioners Guide*
 - *Review of the Risk IT process model*
 - *How to use it*
 - Define a risk universe and scoping risk management
 - Risk awareness, communication and reporting: includes key risk indicators, risk profiles, risk aggregation and risk culture
 - Express and describe risk: guidance on business context, frequency, impact, risk maps, risk registers
 - Risk scenarios: includes capability risk factors and environmental risk factors
 - Risk response and prioritisation
 - *Mappings: Risk IT to other risk management standards and frameworks*





Risk IT



Essentials of the Three Domains

Risk Governance

- Responsibility and accountability for risk
- Risk appetite and tolerance
- Awareness and communication
- Risk culture

Risk IT



Essentials of the Three Domains

Risk Evaluation

- Risk scenarios
- Business impact descriptions



Risk IT



Essentials of the Three Domains

Risk Response

- Key risk indicators (KRIs)
- Risk response definition and prioritisation



Risk IT



Benefits and Outcomes

- An Accurate view on current and near-future IT-related events
- End-to-end guidance on how to manage IT-related risks
- Understanding of how to capitalise on the investment made in an IT internal control system already in place
- Integration with the overall risk and compliance structures within the enterprise
- Common language to help manage the relationships
- Promotion of risk ownership throughout the organisation
- Complete risk profile to better understand risk



Risk IT certification



ISACA Announces New CRISC Certification for Risk Professionals

Rolling Meadows, IL, USA (13 January 2010)— ISACA, a global association of 86,000 IT audit, risk, governance and security professionals, is responding to market demand by introducing a new risk-related certification. The Certified in Risk and Information Systems Control (CRISC) designation is for IT professionals who identify and manage risks through the development, implementation and maintenance of information systems (IS) controls. These professionals help enterprises accomplish business objectives such as effective and efficient operations, reliable financial reporting, and compliance with regulatory requirements.

A grandfathering program, through which experienced professionals can earn the certification without passing an exam, will open in April. The first CRISC exam will be administered in 2011.

ISACA established CRISC (pronounced "see risk") to recognize IT professionals with skills and abilities related to:

- Risk identification, assessment and evaluation
- Risk response
- Risk monitoring
- IS control design and implementation
- IS control monitoring and maintenance

"The CRISC designation will demonstrate to employers that the certification holder is able to identify and evaluate the risks unique to a specific organization and help the enterprise accomplish its business objectives by designing, implementing, monitoring and maintaining risk-based, efficient and effective IS controls," said Urs Fischer, chair of ISACA's CRISC Task Force. "We conducted an extensive amount of research globally and found that enterprises are becoming more risk-aware and are looking to identify professionals who possess the skills to help them protect their assets and enhance their businesses. CRISC fills a gap that currently exists in the marketplace."



Questions?



Steven Babb
Senior Manager
KPMG LLP

steven.babb@kpmg.co.uk
M – 07717 511 554

Risk IT
BASED ON COBIT®

The Risk IT Framework

- Available as a free download to all

The Risk IT Practitioner Guide

- Available as a free download for ISACA members only

Both publications are available for purchase in print version

www.isaca.org/riskit

