ISACA
Trust in, and value from, information systems

Risk IT

BASED ON COBIT®

Presented by:
Urs Fischer, CISA, CRISC
ISACA Guidance and Practices Committee

About ISACA

- Founded in 1969; non-profit, independent association that helps members achieve greater trust in, and value from, their information systems
- Has more than 95,000 constituents in 160 countries and more than 190 chapters worldwide
- Sponsors international conferences and education
- Publishes original research
- Develops international IS audit and control standards
- Offers CISA, CISM, CGEIT and CRISC certifications
- Developed and continually updates the COBIT, Val IT and Risk IT frameworks, as well as the IT Assurance Framework and Business Model for Information Security

Risk IT: A Balance Is Essential

- Risk and value are two sides of the same coin.
- Risk is inherent to all enterprises.

BUT

Enterprises need to ensure that opportunities for value creation are not missed by trying to eliminate all risk.

Why Care About IT-related Risk?

ISACA
Trust in, and value from, information systems

- Enterprises are dependent on automation and integration.
- Need to cross IT silos of risk management.

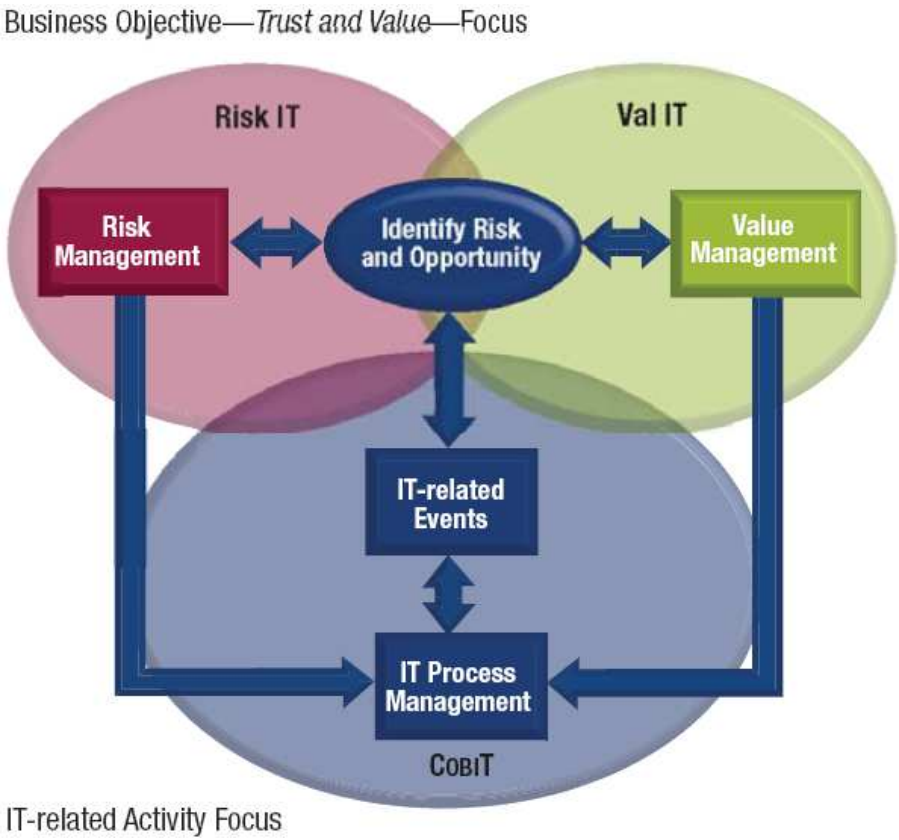
- Important to integrate with existing levels of risk management practices.

Manage and Capitalise on Business Risk

- Enterprises achieve return by taking risks.
- Some try to eliminate the very risks that drive profit.
- Guidance was needed on how to *manage* risk effectively.

Risk IT Extends Val IT and COBIT

Risk IT complements and extends COBIT and Val IT to make a more *complete* IT governance guidance resource.



Developed by ISACA International Experts

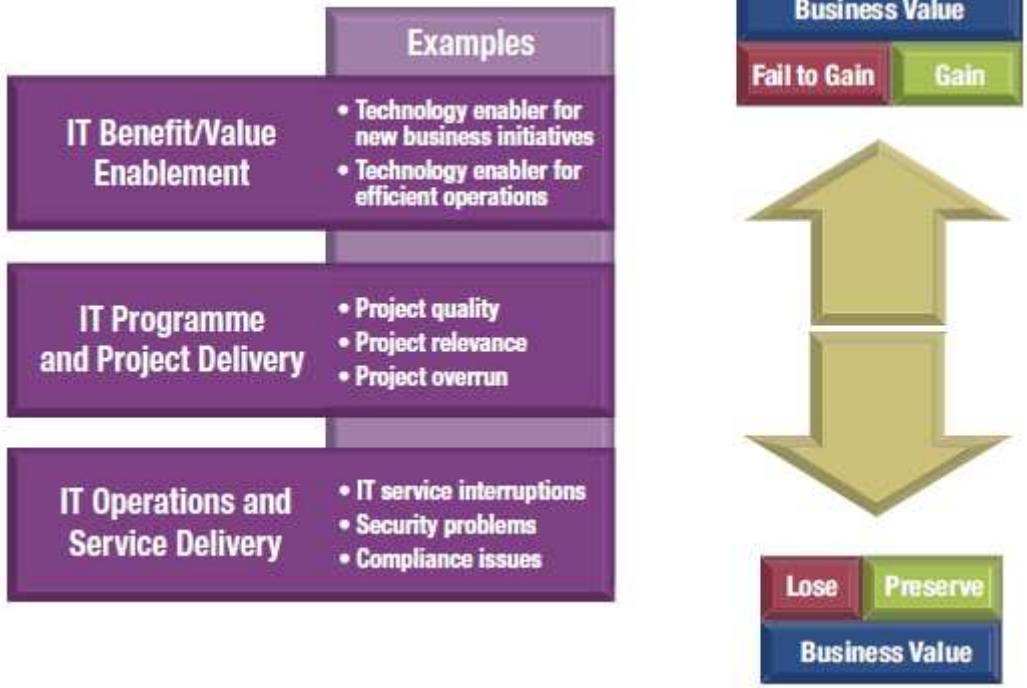
IT and business leaders from around the world who are members of ISACA volunteered thousands of hours to share their expertise.

The development team provided an exposure draft, which resulted in 1,700 SME and public comments.

IT-related Risk Management

Risk IT 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

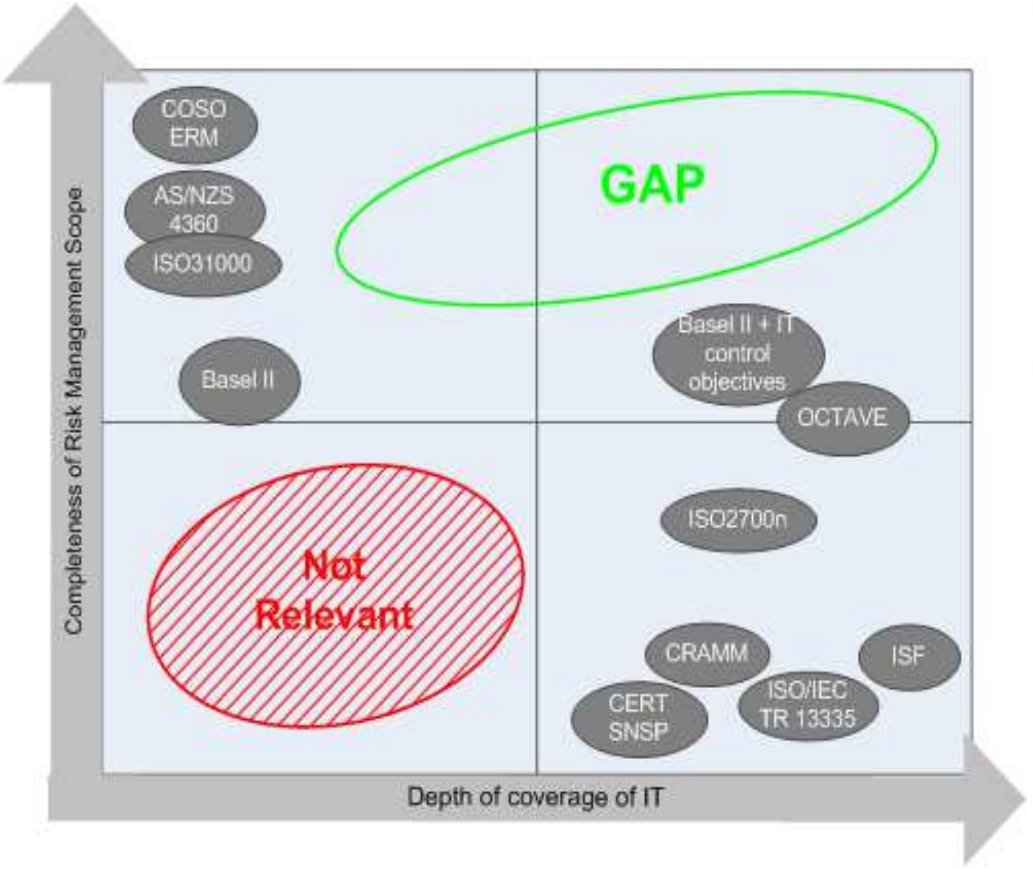


Where IT Risk Fits In

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.



What Risk IT Offers

- Provides guidance to help executives and management ask the key questions, make better, more informed risk-adjusted decisions and guide their enterprises so risk is managed effectively
- Helps save time, cost and effort with tools to address business risks
- Integrates the management of IT-related business risks into overall enterprise risk management
- Helps leadership understand the enterprise's risk appetite and risk tolerance
- Provides practical guidance driven by the needs of enterprise leadership around the world

Unique to the Marketplace

ISACA
Trust in, and value from, information systems

Risk IT provides a balanced view of an enterprise's IT-related business risks:

- Brings together all aspects of IT risk, including value, change, availability, security, project and recovery.
- Links with *enterprisewide* risk management concepts and approaches, such as COSO ERM, ARMS and ISO 31000.
- Other standards and frameworks are either too generic (e.g., ERM-oriented) or too focused on one aspect (e.g., IT security) (see next slide).
- Offers a single, comprehensive view of IT-related business risks, which can cost companies millions annually in lost revenues and opportunities.

Who Benefits From Risk IT?

ISACA
Trust in, and value from, information systems

All enterprises that use IT, whether one-person shops or multinational conglomerates, can benefit from Risk IT.

Risk IT can be customised for any type of enterprise in any geographic location.

Specifically, the following audiences can benefit from the Risk IT framework:

- Boards and executive management; C-suite
- Corporate and operational risk managers
- IT management
- IT service managers
- IT security managers
- Enterprise governance officers
- Business managers
- IT and external auditors
- Regulators

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

Nonfunctional/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

Guiding Principles of Risk IT

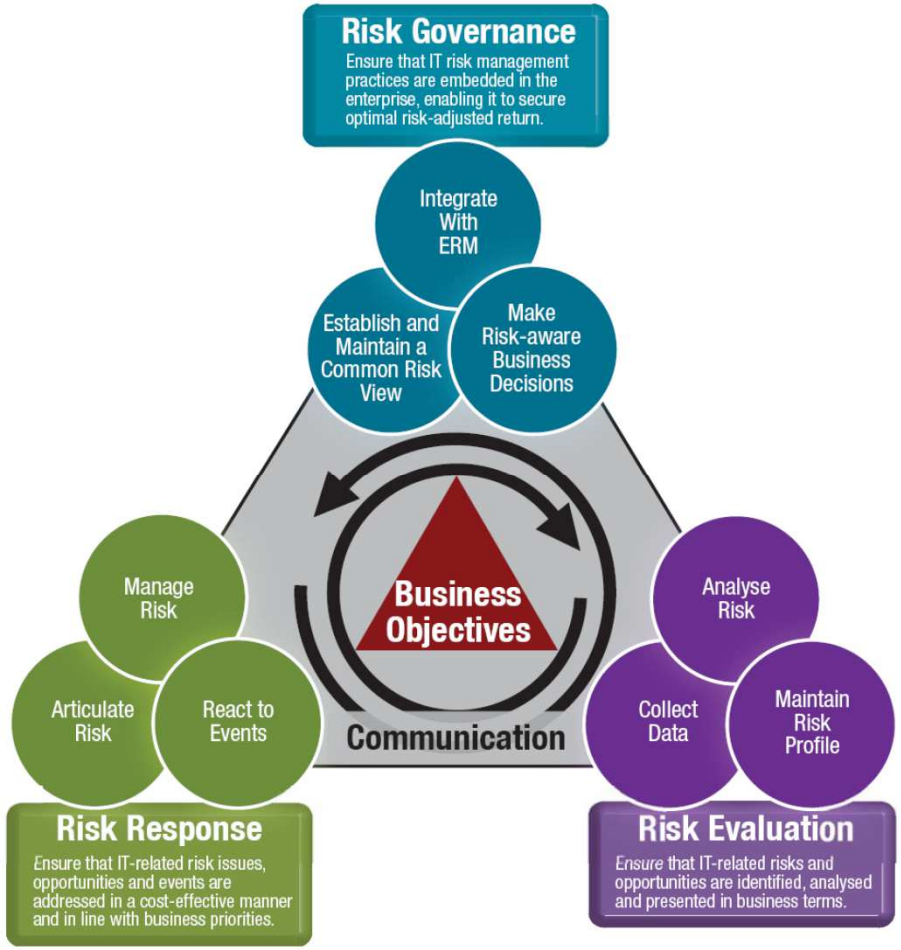
- ✓ Always connect to enterprise objectives.
- ✓ Align the management of IT-related business risk with overall enterprise risk management.
- ✓ Balance the costs and benefits of managing risk.
- ✓ Promote fair and open communication of IT risk.
- ✓ Establish the right tone from the top while defining 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.

Key Risk IT Content: The “What”

Key content of the Risk IT framework includes:

- Risk management essentials
  In **Risk Governance**: Risk appetite and tolerance, responsibilities and accountability for IT risk management, awareness and communication, and risk culture
  In **Risk Evaluation**: Describing business impact and risk scenarios
  In **Risk Response**: Key risk indicators (KRI) and risk response definition and prioritisation
- Section on how Risk IT extends and enhances COBIT and Val IT (*Note:* Risk IT does not require the use of COBIT or Val IT*.)*
- Process model sections that contain:
  Descriptions
  Input-output tables
  RACI (Responsible, Accountable, Consulted, Informed) table
  Goals and Metrics Table
- Maturity model is provided for each domain
- Appendices
  Reference materials
  High-level comparison of Risk IT to other risk management frameworks and standards
  Glossary

Risk IT Three Domains



Risk Governance Domain

Risk Governance Essentials:

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

Risk Evaluation Domain

Risk Evaluation Essentials:

- Risk scenarios
- Business impact descriptions

Risk Response Domain

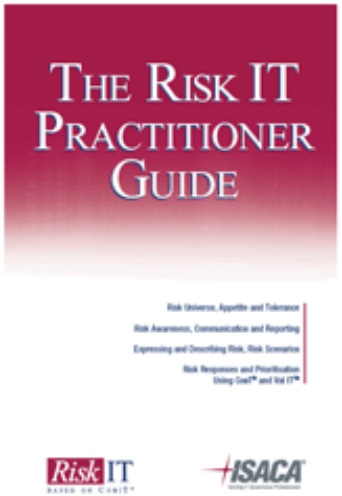
Risk Response Essentials:

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

Risk IT: The “How”

ISACA
Trust in, and value from, information systems

Key contents of *The Risk IT Practitioner Guide*:

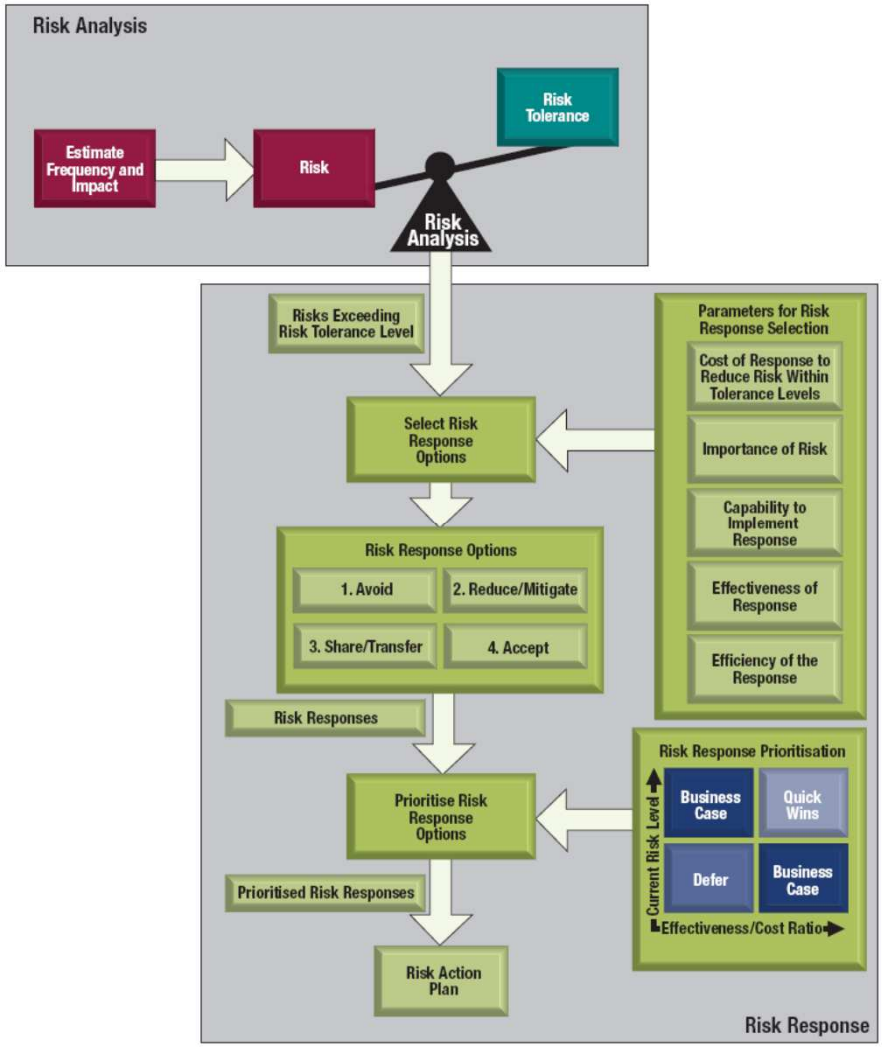


- Review of the Risk IT process model
- Risk IT to COBIT and Val IT
- How to use it:
  1. Define a risk universe and scoping risk management
  2. Risk appetite and risk tolerance
  3. Risk awareness, communication and reporting: includes key risk indicators, risk profiles, risk aggregation and risk culture
  4. Express and describe risk: guidance on business context, frequency, impact, COBIT business goals, risk maps, risk registers
  5. Risk scenarios: includes capability risk factors and environmental risk factors
  6. Risk response and prioritisation
  7. A risk analysis workflow: “swim lane” flow chart, including role context
  8. Mitigation of IT risk using COBIT and Val IT
- Mappings: Risk IT to other risk management standards and frameworks
- Glossary

Risk/Response Definition

The purpose of defining a risk response is to bring risk in line with the defined risk tolerance for the enterprise after due risk analysis.

In other words, a response needs to be defined such that future residual risk (=current risk with the risk response defined and implemented) is as much as possible (usually depending on budgets available) within risk tolerance limits.



Risk IT Benefits and Outcomes

- 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

Questions?

Thank you!

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
info@isaca.org
www.isaca.org/riskit