What is Risk IT?

Risk IT is:

- A framework to help establish effective governance and management of IT risk
- Part of ISACA's product portfolio on IT governance
- A framework based on a set of guiding principles for effective management of IT risk

What does Risk IT do?

Risk IT:

- Allows enterprises to customize the components provided in the framework to suit their particular needs
- Provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues
- Enables enterprises to understand and manage all significant IT risk types
- Provides tangible business benefits
- Allows the enterprise to make appropriate risk-aware decisions
- Explains how to capitalize on an investment made in an IT internal control system already in place to manage IT-related risk
- Enables integration with overall risk and compliance structures within the enterprise when assessing and managing IT risk

What are the benefits of using Risk IT?

The benefits of using Risk IT include:

- A common language to help communication amongst business, IT, risk and audit management
- End-to-end guidance on how to manage IT-related risks
- A complete risk profile to better understand risk, so as to better utilize enterprise resources
- A better understanding of the roles and responsibilities with regard to IT risk management
- Alignment with ERM
- A better view of IT-related risk and its financial implications
- Fewer operational surprises and failures
- Increased information quality
- Greater stakeholder confidence and reduced regulatory concerns
- Innovative applications supporting new business initiatives

www.isaca.org/riskit

ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Web site: *www.isaca.org*

Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@isaca.org*

Risk IT
BASED ON COBIT®

ISACA®
Trust in, and value from, information systems

Risk IT *A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk.*

In business today, risk plays a critical role. Almost every business decision requires executives and managers to balance risk and reward. Effectively managing the business risks is essential to an enterprise's success.

Too often, IT risk (business risk related to the use of IT) is overlooked. Other business risks, such as market risks, credit risk and operational risks have long been incorporated into the corporate decision-making processes. IT risk has been relegated to technical specialists outside the boardroom, despite falling under the same 'umbrella' risk category as other business risks: failure to achieve strategic objectives.

The problem is clear. The solution? Unclear.
Until now: **Introducing Risk IT**

Risk IT is a framework based on a set of guiding principles for effective management of IT risk. The framework complements COBIT®, a comprehensive framework for the governance and control of business-driven, IT-based solutions and services. While COBIT provides a set of controls to mitigate IT risk, Risk IT provides a framework for enterprises to identify, govern and manage IT risk. Simply put, COBIT provides the means of risk management; Risk IT provides the ends. Enterprises who have adopted (or are planning to adopt) COBIT as their IT governance framework can use Risk IT to enhance risk management.

The Risk IT Principles

The Risk IT framework is about IT risk — business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built. Effective enterprise governance and management of IT risk:

- Always connects to business objectives
- Aligns the management of IT-related business risk with overall enterprise risk management (ERM) — if applicable, i.e., if ERM is implemented in the enterprise
- Balances the costs and benefits of managing IT risk
- Promotes fair and open communication of IT risk
- Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Is a continuous process and part of daily activities

Managing and Understanding IT Risk

To prioritize and manage IT risk, senior executives need a frame of reference and a clear understanding of the IT function and IT risk. However, the enterprise's key stakeholders, including board members and executive management, the very people who should be accountable for risk management within the enterprise, often do not have a full understanding.

IT risk is not just a technical issue. While IT subject matter experts help to understand and manage aspects of IT risk, business management is the most important stakeholder. Business managers determine what IT needs to do to support their business; they set the targets for IT and are accountable for managing the associated risks.

The Risk IT framework explains IT risk, allows the enterprise to make appropriate risk-aware decisions and will enable users to:

- Integrate the management of IT risk into the overall enterprise risk management (ERM) of the organization
- Make well-informed decisions about the extent of the risk, the risk appetite and the risk tolerance of the enterprise
- Understand how to respond to the risk

In summary, the framework will enable enterprises to understand and manage all significant IT risk types. The Risk IT framework provides an end-to-end, comprehensive view of all risks related to the use of IT, as well as a similar view of risk management. The framework fills the gap between generic risk management frameworks like COSO ERM and AS/NZS 4360 (soon to be replaced by ISO31000) and its British equivalent, ARMS6, and detailed (primarily security-related) IT risk management frameworks.

Risk IT Publications

Risk IT consists of two publications: the *Risk IT Framework* and the *Risk IT Practitioner Guide*.

The *Risk IT Framework* provides:

- A set of governance practices for risk management.
- An end-to-end process framework for successful IT risk management.
- A generic list of common, potentially adverse, IT-related risk scenarios that could impact the realization of business objectives.
- Tools and techniques to understand concrete risks to business operations, as opposed to generic checklists of controls or compliance requirements.

From the building blocks the framework provides, a comprehensive process model for IT risk is built. For users of COBIT and Val IT, this will look familiar. Guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of each process. The model is divided into three domains — Risk Governance, Risk Evaluation, Risk Response — each containing three processes:

- Risk Governance
  Establish and Maintain a Common Risk View
  Integrate with Enterprise Risk Management (ERM)
  Make Risk-aware Business Decisions

- Risk Evaluation
  Collect Data
  Analyze Risk
  Maintain Risk Profile

- Risk Response
  Articulate Risk
  Manage Risk
  React to Events

The *Risk IT Practitioner Guide* is a support document for the Risk IT framework that provides examples of possible techniques to address IT-related risk issues more detailed guidance on how to approach the concepts covered in the process model.
Concepts and techniques explored in more detail include:

- Building scenarios, based on a set of generic IT risk scenarios
- Building a risk map, using techniques to describe the impact and frequency of scenarios
- Building impact criteria with business relevance
- Defining KRIs
- Using COBIT and Val IT to mitigate risk; the link between risk and COBIT and Val IT control objectives and key management practices

Your Solution to IT Risk

Applying good IT risk management practices as described in Risk IT will provide tangible business benefits, e.g., fewer operational surprises and failures, increased information quality, greater stakeholder confidence and reduced regulatory concerns, innovative applications supporting new business initiatives. The Risk IT framework is part of ISACA's product portfolio on IT governance. Although this document provides a complete and standalone framework, it does include references to COBIT and Val IT. As the Practitioner Guide, issued in support of this framework, makes extensive reference to COBIT and Val IT, it is recommended that managers and practitioners acquaint themselves with the major principles and contents of these two frameworks. Like COBIT and Val IT, Risk IT is not a standard, but a flexible framework. This means that enterprises can and should customize the components provided in the framework to suit their particular organization.