ISACA Releases the Risk IT Framework Draft

By [Sam Grier](http://itmanagersinbox.com/author/sam-grier/)

[](http://itmanagersinbox.com/wp-content/uploads/2009/02/risk-it-cover.gif)ISACA, the Information Systems Audit and Control Association has just released an exposure draft of of their initiative “**Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework**”.

Covering 94 pages the document frames IT risk as a business risk and goes into extensive detail on a framework for dealing with it. Packed full of charts, tables and control framework. Though not a final document it offers a great deal of insight into what the final document will look like.

The intended audience for the Risk IT Framework is vast. Boards and executive management, corporate risk managers, operational risk managers, IT management, IT service managers, business continuity managers, IT security managers, chief financial officers, enterprise governance officers, business managers, IT auditors, regulators, external auditors, insurers and rating agencies.

They categorize IT risk in three ways.

* IT Service Delivery Risk – associated with the performance and availability of IT services, and which can bring destruction or reduction of value to the enterprise.
* IT Solution Delivery/Benefit Realization Risk – associated with the contributions of IT to new or improved business solutions, usually in the form of projects and programs.
* IT Benefit Realization Risk – associated with (missed) opportunities to use technology to improve efficiency of effectiveness of business processes, or to use technology as an enabler for new business initiatives.

The document goes into great detail explaining what risk is. How to raise awareness and open communications. How to manage risk and the impact it can have on the business. Most of the document outlines the Risk IT Framework.

This IT enterprise risk management framework was designed to allow business managers to identify and assess IT-related business risks and manage them effectively. It provides the missing link between enterprise risk management (ERM) and IT risk management and control, fitting in the overall IT governance framework of ITGI, and building upon all existing risk related components within the current frameworks, i.e., COBIT and Val IT.

To download “Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework” in PDF format visit the [ISACA web site download section](http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742) and for more material available for download. Some material does require membership to access.

About ISACA

ISACA has over 86,000 members worldwide for information governance, control, security and audit professionals and is affiliated with the IT Governance Institute.

It provides three certifications.

* [The Certified Information Systems Auditor (CISA)](http://www.amazon.com/dp/0470231521/?tag=itman-20) is ISACA’s cornerstone certification. The CISA certification has been earned by more than 60,000 professionals since inception and is for the IS audit, control, assurance and/or security professionals who wish to set themselves apart from their peers. Since 1978, the CISA certification has been renowned as the globally recognized achievement for those who control, monitor and assess an organization’s information technology and business systems.
* **The**[Certified Information Security Manager](http://www.amazon.com/dp/0782144438/?tag=itman-20)**(CISM)** certification is a unique management focused certification that has been earned by over 10,000 professionals since its introduction in 2003. Unlike other security certifications, CISM is for the individual who manages, designs, oversees and assesses an enterprise’s information security program. CISM defines the core competencies and international performance standards that those who have information security management responsibilities must master.
* **The IT Governance certification (CGEIT)** is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices. Many CGEIT certificates have been awarded. It is designed for professionals who have management, advisory, or assurance responsibilities as defined by a “job practice” consisting of IT governance related tasks and knowledge. Earning this designation will enable professionals to respond to the growing business demand for a comprehensive IT governance program that defines responsibility and accountability across the entire enterprise.