IT Risk Management on the advance – even for SME's: boosting due to the new ISO 27005 Standard

Pressure exerted by data losses and laws.
IT is a pioneer: In 2009, the ISO Standard for Enterprise RM will follow

(October 2008) – The long-expected Standard for "Information Security Risk Management", ISO/IEC 27005 has recently been published within the well-known Series of Standards for Information Security ISO/IEC 2700x. This helps to make the abstract topic of risk management (RM) more tangible and easier to implement – even for small and medium-sized enterprises. The topic of IT is a prominent topic. For it is not until 2009 that ISO 31000, i.e. a Standard for Enterprise RM, is to follow. Risk management is one of the big challenges for companies, among other things in view of the latest laws and guidelines and directives. This is what **Dipl.-Ing. Herfried Geyer, RM Expert** of the Certification Body CIS, says in the interview.

Mr. Geyer, what role is IT Risk Management playing in the business context?
Data loss and theft are massive problems. In 2007, more than 167 million personnel data were stolen worldwide – this is three times more than in the previous year. At the moment there are political discussions as to whether companies will have to actively demonstrate due care relating to data in future. Before this background, risk management becomes the topic of the hour: For security gaps can be detected and minimized by means of risk management – which means the principle of due diligence is met. Catchword: recourse. The accredited body CIS conducts certifications acc. to ISO 27001, the Standard for Information Security absolutely requiring RM and making it possible to establish holistic security systems with process improvement and control mechanisms. For many IT Managers, this still is a new territory.

Is IT Risk Management boosted by the current development?
Availability of resources and data security and integrity are required for achieving good business results. The basis is formed by solid risk management, which is also required by the most recent laws and guidelines and directives, such as the Act regulating the Liability of Associations, Basle II or Euro-Sox. The topic will be made even more important when ISO 31000, a standard for company-wide risk management, will appear in 2009.Then IT Representatives with experience in RM might act as pioneers.

Is risk management a topic for SME's?
It is particularly small and medium-sized enterprises active in such sensitive industries as automotive, health, software or telecommunications that are addressed here and mostly have a higher need for catching up.

To what extent is ISO 27005 applicable to SME'S?
The standard is independent from the industry and size. By adapting its contents to their own business requirements, SME's can thus establish a lean and effective IT Risk Management. As there are clear lists of RM requirements in each chapter, it is easy to find out what clauses of ISO 27005 need to be implemented specifically.

What are the contents of ISO 27005?
Step-by-step instructions for risk management: The main part starts with the "information security risk management process". This part is followed by basic criteria and details for use. Then the elements will be described in a manner that is easy to grasp: Risk Assessment, Risk Treatment, Risk Acceptance, Risk Communication, Risk Monitoring and Review – each with checklists and explanations. It also is the comprehensive Annex with detailed examples that shows how practice oriented the standard is.

How do the IT Standard ISO 27005 and ISO 31000 for Enterprise RM fit together?
As there are similar structures, ISO 27005 can be integrated in a company-wide risk management. However, ISO 27005 can also be implemented "solo". The two standards include process improvement with a systemic approach. The trend goes towards integrated systems and interlinked teams.

Technical information:
ISO/IEC 27005 "Information Security Risk Management" offers guidelines, tables and examples relating to IT Risk Management, above all relating to the Certification Standard ISO 27001 for Information Security. The new ISO 27005 supersedes the Directives TR 13335-3:1998 and TR 13335-4:2000 and compiles and supplements these technical reports.