

ISO/IEC 27005 Risk Management standard

31.7.2008

ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management, (19.6.2008)

ISO/IEC 27005:2008 international standard describes the information security risk management system.

Risk assessment specifies and describes threats by probability and consequences. It offers to managers means to prioritize risks according to their seriousness.

Guidelines and general framework for information security risk management are specified in the information security management system standards ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements* and ISO/IEC 27002: 2005, *Information technology – Security techniques – Code of practice for information security management*.

Standard ISO/IEC 27005: 2008 is designed to assist the implementation of ISO/IEC 27001 and ISO/IEC 27002. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and 27002 is important for a complete understanding of standard.

The information security risk management process consists of:

- context establishment
- risk assessment
- risk treatment
- risk acceptance
- risk communication, and
- risk monitoring and review.

ISO/IEC 27005:2008 does not provide any specific methodology for information security risk management. It is up to the organization to define its approach to risk management.

According to ISO 27001 are certified worldwide over 4400 Information Security Management Systems.

ISO Press release:

<http://www.iso.org/iso/pressrelease.htm?refid=Ref1139>

Other ISO/IEC 27000 standards and their preparations situation:

<http://www.iso27001security.com/html/27000.html>

ISO 27001 certification:

<http://www.iso27001certificates.com/>