KPMG

PERFORMANCE & TECHNOLOGY - IT ADVISORY

Predstavenie štandardu ISO/IEC 27005

ISMS Risk Management

16.02.2011

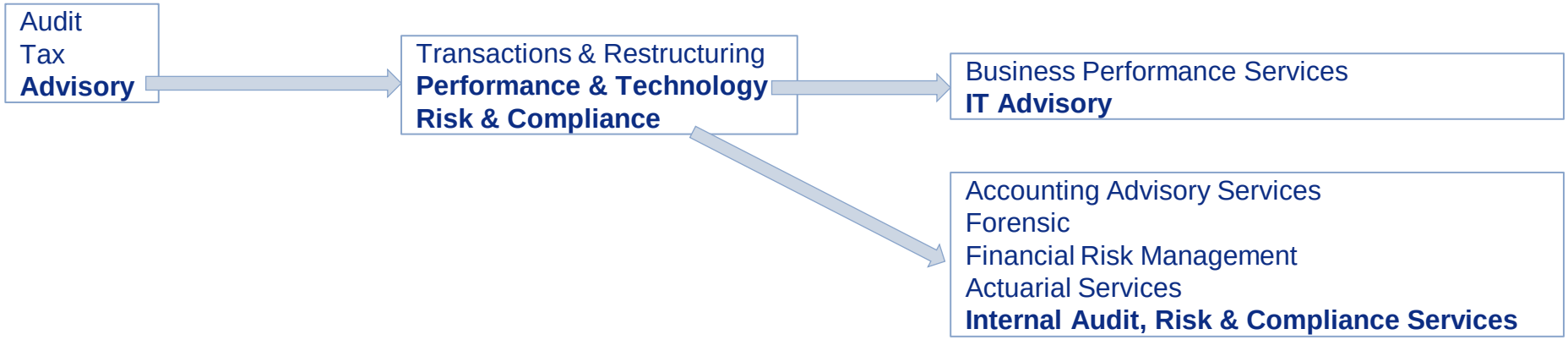
ADVISORY

KPMG details

KPMG is a global network of professional services firms providing audit, tax and advisory services. KPMG member firms have **140,000** outstanding professionals working together to deliver value in **146** countries worldwide.

KPMG established its office in Bratislava in **1991**. Since then KPMG in Slovakia has enjoyed dynamic growth, a trend that we expect to continue. Today, KPMG in Slovakia employs over **300** people and has **10** partners.

Service taxonomy:



Presenter's details

Michal Bubák

In KPMG since 2004

Supervisor (Assistant manager) at Performance & Technology / IT Advisory

Certifications:	**CISA, CISM** (member of ISACA)
	PRINCE 2 Practitioner
	ITIL Foundation
	ISO/IEC 20000
	BS 7799-2:2002
Field of experience:	**Information Security Management**
	Audit of IS and information security
	Risk Analysis / BIA
	Business Continuity Management
	Project Management
Industries/Sectors:	Banking
	Telecommunications
	Utilities

Standard identification

Published standards

ISO/IEC 27000 — Information security management systems — Overview and vocabulary

ISO/IEC 27001 — Information security management systems — Requirements

ISO/IEC 27002 — Code of practice for information security management

ISO/IEC 27003 — Information security management system implementation guidance

ISO/IEC 27004 — Information security management — Measurement

ISO/IEC 27005 — Information security risk management

ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27033-1 - Network security overview and concepts

In preparation

ISO/IEC 27007 - Guidelines for information security management systems auditing (focused on the management system)

ISO/IEC 27008 - Guidance for auditors on ISMS controls (focused on the information security controls)

ISO/IEC 27013 - Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

ISO/IEC 27014 - Information security governance framework

ISO/IEC 27015 - Information security management guidelines for the finance and insurance sectors

ISO/IEC 27031 - Guideline for ICT readiness for business continuity (essentially the ICT continuity component within business continuity management)

ISO/IEC 27032 - Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)

ISO/IEC 27033 - IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)

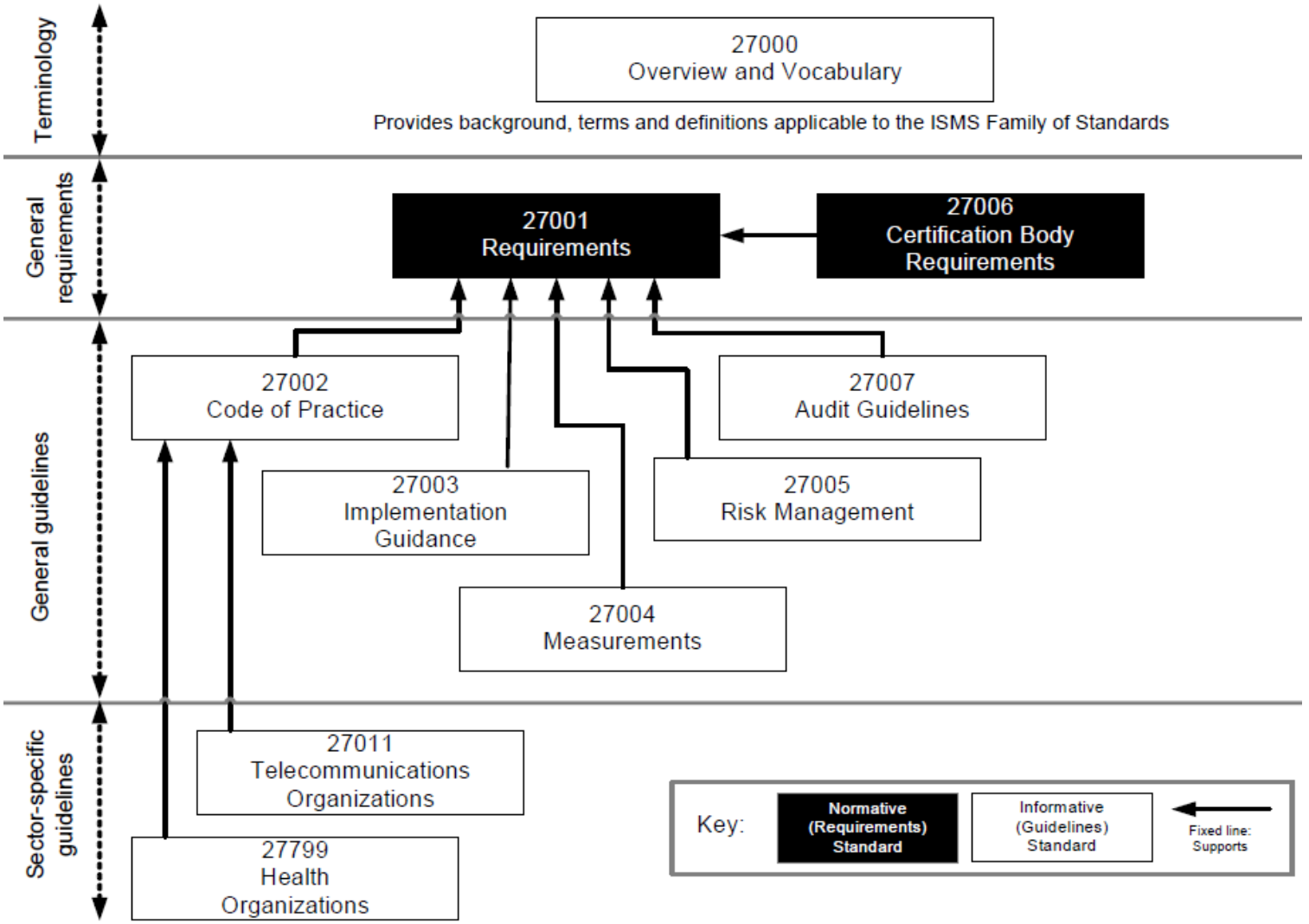
ISO/IEC 27034 - Guideline for application security

ISO/IEC 27035 - Security incident management

ISO/IEC 27036 - Guidelines for security of outsourcing

ISO/IEC 27037 - Guidelines for identification, collection and/or acquisition and preservation of digital evidence

Standard identification



Standard evolution and purpose

Publication:

•Standard published in 2008

•Prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques.*

Cancels and replaces:

•ISO/IEC TR 13335-3:1998 - Guidelines for the management of IT Security - Techniques for the management of IT Security

•ISO/IEC TR 13335-4:2000 - Guidelines for the management of IT Security - Selection of safeguards

Purpose and Scope:

•The standard provides guidelines for Information Security Risk Management in an organization, supporting in particular the requirements of an ISMS according **to ISO/IEC 27001**.

•The standard does not provide **any specific methodology** for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector.

•The standard is relevant to **managers and staff concerned with information security risk management** within an organization and, where appropriate, external parties supporting such activities.

•The standard is applicable to **all types of organizations** (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

Standard structure

1. Scope
2. Normative references
3. Terms and definitions
4. Structure of this International Standard
5. Background
6. Overview of the information security risk management process
7. **Context establishment**
8. **Information security risk assessment**
9. **Information security risk treatment**
10. **Information security risk acceptance**
11. **Information security risk communication**
12. **Information security risk monitoring and review**

Annex A - Defining the scope and boundaries

Annex B - Identification and valuation of assets and impact assessment

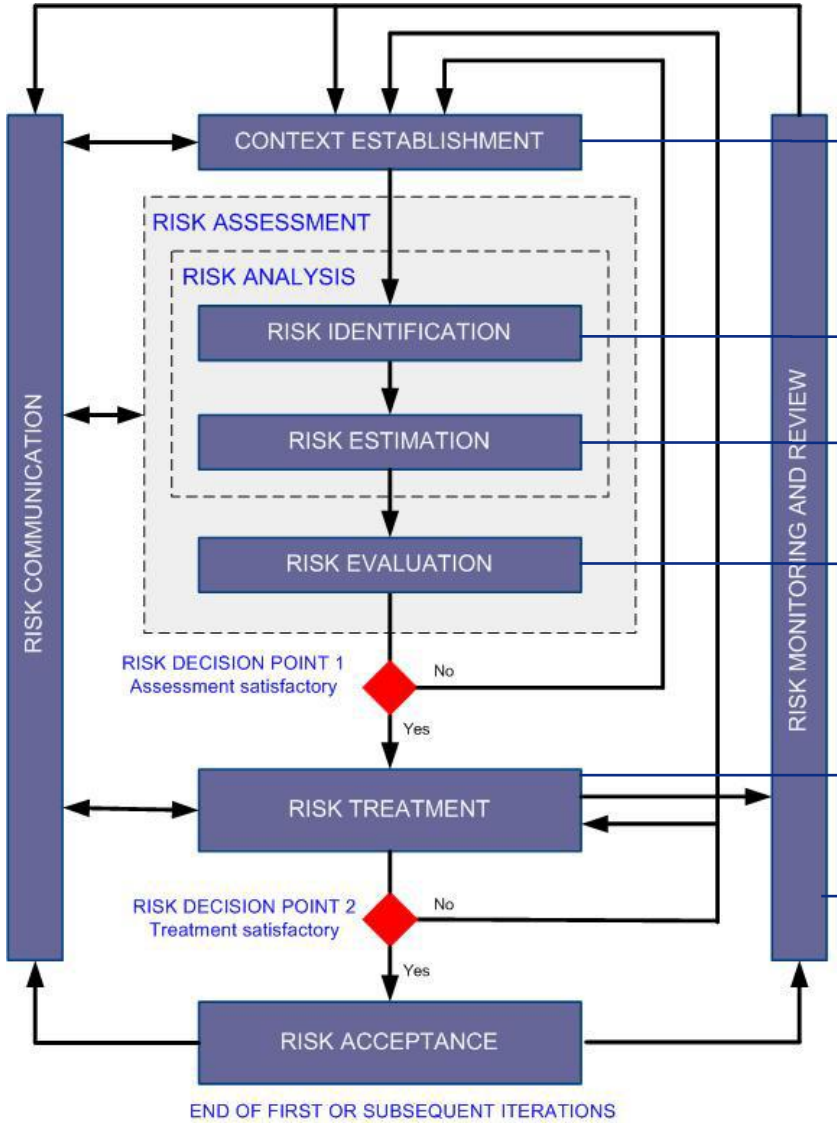
Annex C - Examples of typical threats

Annex D - Vulnerabilities and methods for vulnerability assessment

Annex E - Information security risk assessment approaches

Annex F - Constraints for risk reduction

Standard content



Risk evaluation criteria
Risk acceptance criteria
The scope and boundaries
Organization for information security risk management

Assets, Threats, Vulnerabilities, Controls

Qualitative / Quantitative estimation

Prioritized risks according to risk evaluation criteria

Risk reduction
Risk retention
Risk avoidance
Risk transfer

Monitoring and review of risk factors
Risk management monitoring, reviewing and improving

Standard assessment & Recommendations

ISO 27005 Certified Risk Manager

- Information security risk management - a **systematic approach**
- Should be aligned with **overall enterprise risk management.**
- Information security risk management should be a **continual process.**

Important chapters:

- **Context establishment**
  - Risk acceptance criteria
  - The scope and boundaries
  - Organization for information security risk management
- **Information security risk monitoring and review**
  - Monitoring and review of risk factors
  - Risk management monitoring, reviewing and improving
- **Annexes**

Annex B - Identification and valuation of assets and impact assessment

Annex C - Examples of typical threats

Annex D - Vulnerabilities and methods for vulnerability assessment

Annex E - Information security risk assessment approaches

ISMS Process	Information Security Risk Management Process
Plan	Establishing the context Risk assessment Risk treatment planning Risk acceptance
Do	Implementation of risk treatment plan
Check	Continual monitoring and reviewing of risks
Act	Maintain and improve the Information Security Risk Management Process

Questions ??