



Risk management standard BS7799-3 published

10.4.2006

British Standards Institute (BSI) has published in March a new security standard, number BS7799-3. It is officially titled "Guidelines for Information Security Risk Management", and is designed to support risk management according to the general security management standard ISO27001 (published in October 2005). BS7799-3 may be basis for risk management standard ISO 27005.

BS7799-3 specifies the following features of risk management:

- the assessment of risks,
- implementation of security controls to address risks,
- monitoring of the risks,
- maintenance of the risk control system.

The BS7799-3 document is organized as follows:

1. Scope
2. Normative references
3. Terms and definitions
4. Information security risks in the organization's context
5. Risk assessment
6. Risk treatment and management decision making
7. Ongoing risk management

Knowledge of Society Consulting arranges 6.6.2006 training 'Risk management and information security metrics' (in Finnish) where is considered also BS7799-3 standard.