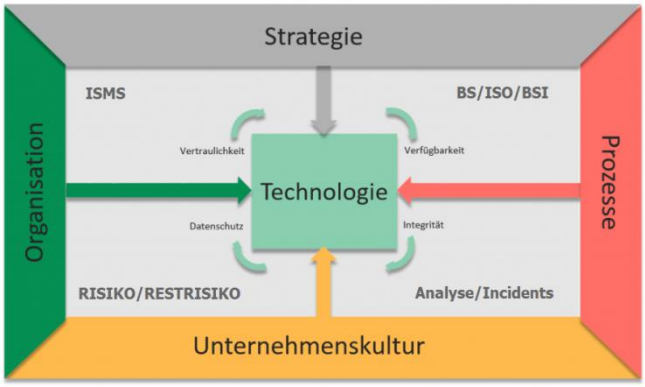
Introduction of an ISMS according to ISO 27001 - Creation of a governance - MSS
Bernhard Bowitz, Dipl. Ing. 2016



An **I**nformation **S**ecurity **M**anagement **S**ystem (ISMS) is a set of policies that deal with information security management or IT-related risks. The individual recommendations were made mainly from BS 7799 and, in turn, from ISO 27001 and BSI Grundschutz.

The governance behind an ISMS is that an organization must design, implement and maintain a uniform (based on the BSI) set of policies, processes, and systems to manage, prevent, and manage the risks to its information structure Acceptable level of **I**nformation **S**ecurity **R**est **R**isk (ISRR).

The Federal Office for Security in Information Security (BSI) has (2016) published a new certification strand for information security management systems (ISMS). The concept describes how certification can be carried out if the ISMS is set up according to ISO / IEC 27001 and a corresponding Technical Guideline (TR) of the BSI is taken into account. The conformity of a management system to a TR (in conjunction with conformity to ISO / IEC 27001) can be confirmed by a certification body for ISMS accredited by the DakkS (German Accreditation Service). In the course of this procedure, an auditor performs an assessment on the basis of the requirements specified in the Technical Directive.

The concept of certification is described in the notes for certification bodies of sector-specific management systems based on ISO / IEC 27001. TR-03108 Secure e-mail transport (BSI) is an example of the TR certification according to this concept:

What is information security?
Presence of
• Integrity
• Confidentiality
• Availability

The threat
Main long-term threat source:
• Employees ("HumanOS") "weakest link" in the safety chain
• Lack of security skills / training
• Lack of comprehensive human resources
• Easy victims for social engineering
• Often too far-reaching authorizations
• Unauthorized administrators

ISO 2700x ISMS standards
ISO 27000 Terms and Definitions
• ISO 27005 Risk Management
• ISO 27001 Information Security Management System

BS7799-2 (British Code of Practice) Model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system

ISO 27005 Risk Management
• ISO 27002 Code of Practice

BS7799-1 Set of controls, including policies, processes, procedures, organizational structures, software / hardware functions
ISO 27003 Implementation
• Guidance instructions on how to [technically] implement ISO 27001

ISO 27004 Metrics and Measurements
• Definition of KPIs, quantitative / qualitative measurements, metrics, etc.

ISO 27015 Accreditation Guidelines

The security process
Initiation of the security process:

• Create an ISMS policy
• Setting up IT security management

IT security concept: identification of controls

Implementation:
• Implementation of missing controls (control mechanisms) especially in the areas of ...
• Infrastructure
• Penetration test
• IT security analysis
• Organization
• Staff
• Technology
• Communication (i.e. email, messages, mobile phone, etc.)
• Data security (data center, server, cloud, FTP, etc.)
• Emergency care

In particular, awareness of IT security, training in IT security
Maintenance during operation

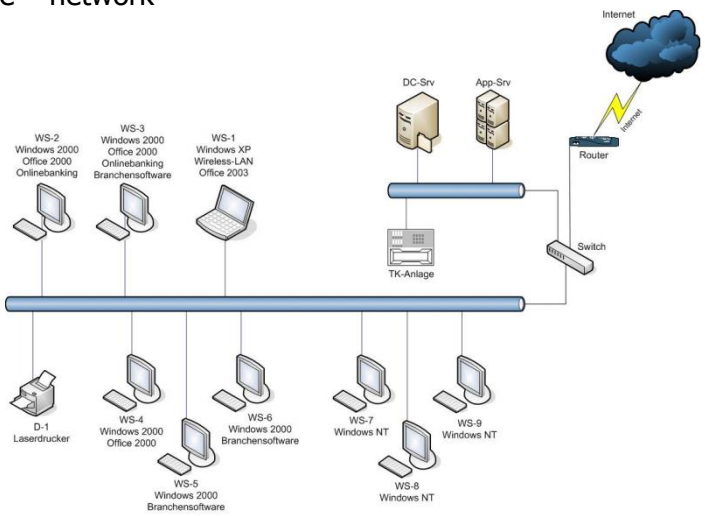
The first steps to the ISMS
• Management support for ISMS implementation and set-up
• Definition of the scope
• Definition of the safety guideline (ISMS Policy)
• Organizational analysis
• Risk analysis
• Identification of control mechanisms and measures
• (design) the ISMS

Initiation of the IT security process
Responsibility of the management

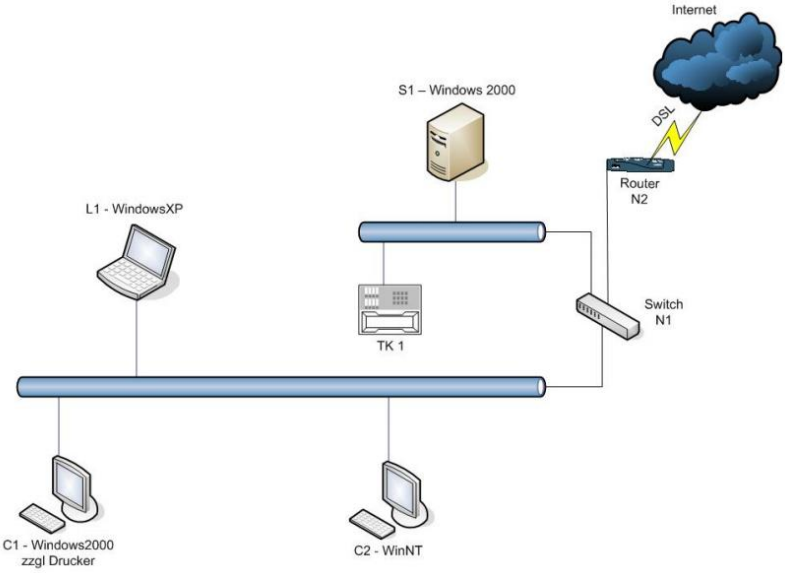
Basic rules
• The IT Security Initiative is managed by the management
• The responsibility for IT security lies with management
• IT security is the responsibility only when management is concerned about IT security
• Management role model

Setting up IT security management

Creating the network structure – network



Network Cleanup

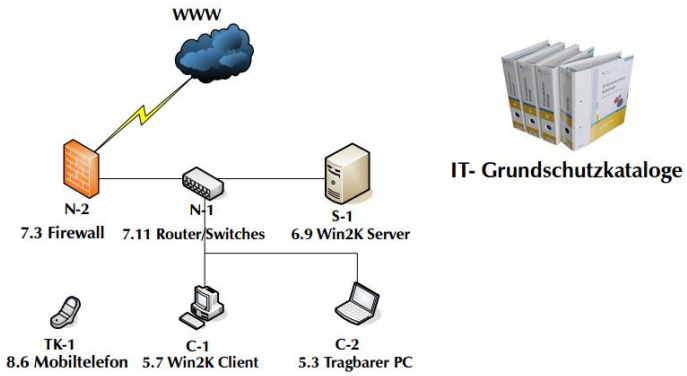


BSI basic protection catalog

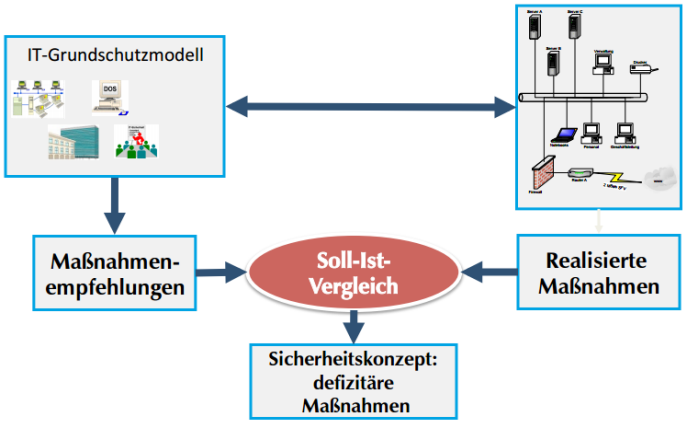
Building block description

- Presentation of the hazards situation (Hazard class catalog)
- Measures for action (measures catalog)
- Planning and design
- Procurement (if required)
- Implementation
- Business
- Segregation (if required)
- Emergency care

BSI Basic Protection Catalog



Basic security check



Protection requirement detection

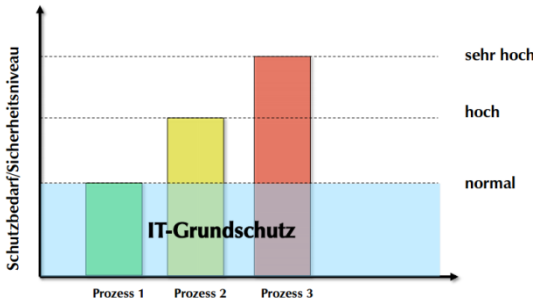
Definition of protection categories

- Definitions of the categories have to be adapted individually
- Normal damage effects are limited and manageable
- High-damage effects can be considerable
- Very high - Damage effects can reach an existentially threatening, catastrophic extent

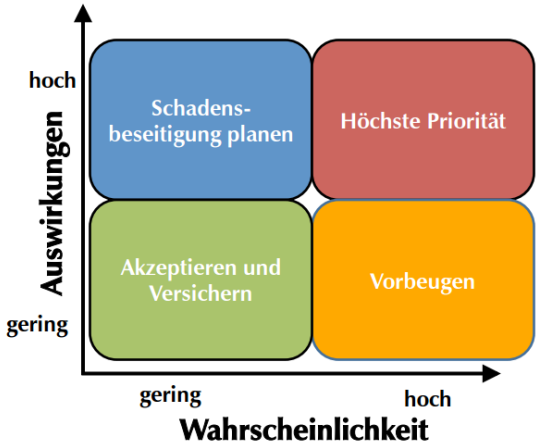
Legal issues

- Data protection, marketing, finance, health ...
- Confidentiality, integrity, availability

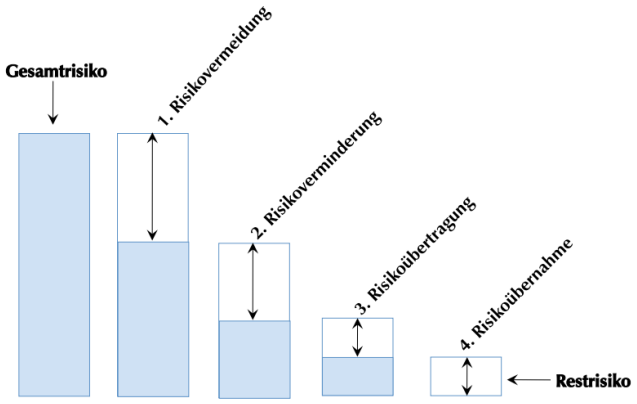
Protection processes



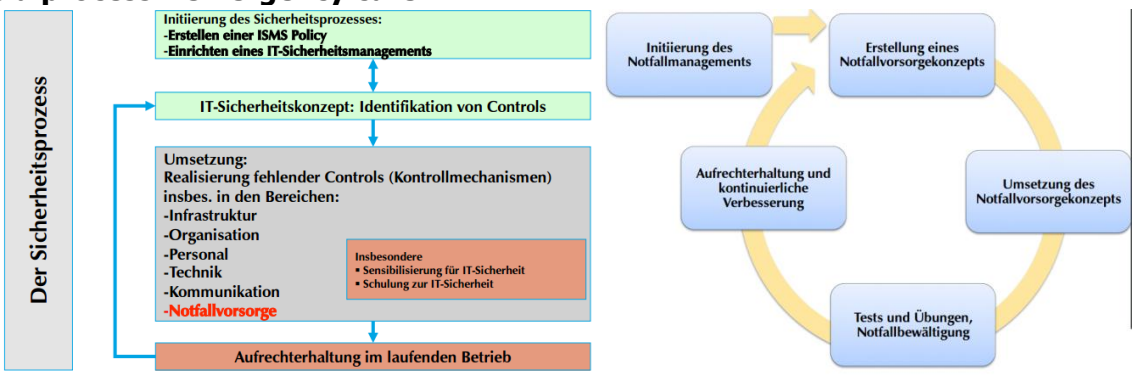
Higher protection, risk analysis



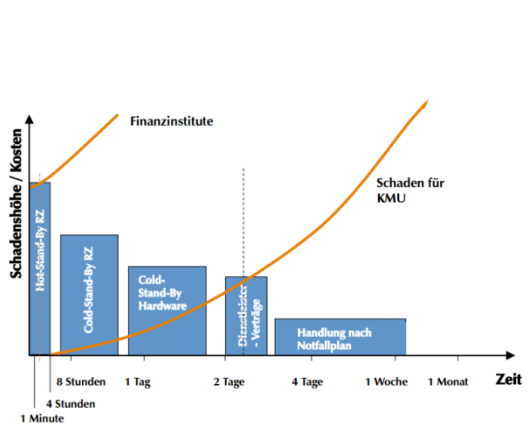
Graduated risk management

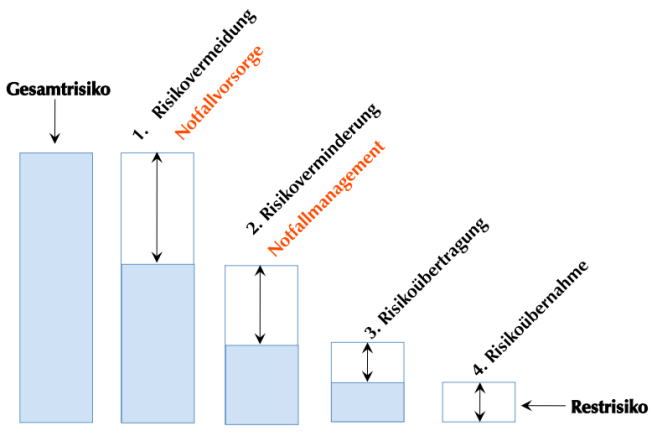


Security as a process - emergency care



Risk - residual risk





Summary:
To implement the requirements of the BnetzA / BSI, the measures from the ISO / IEC 27002 standard have to be
• Documented
• Repositioned
• and be tested