

Introduction to IT Security

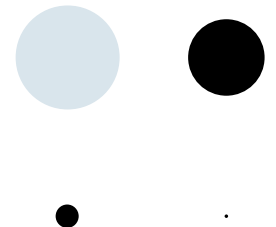
WIN+AIN

Hanno Langweg

02a Security Management – Standards

Security Management Topics

- IT security standards and processes
 - ISO 2700x
 - BSI IT-Grundschutz (base protection)
 - Personnel security
 - Physical security
- Vulnerability management
- Product evaluations using Common Criteria

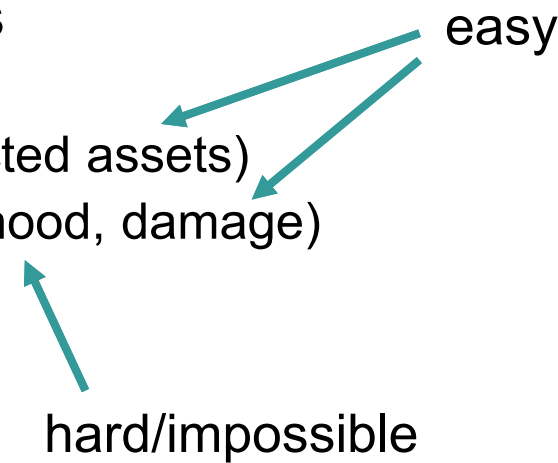


IT Security Standards and Processes

Security management

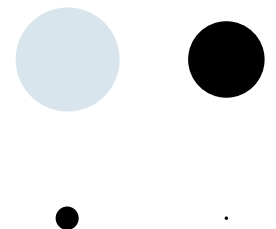
- Security is a people problem
 - Values, rules, technology
- Support from top management recommended
 - Awareness
 - Enforcement, incentives, penalties
- Model, measure, manage
 - Measuring security is hard
 - In many cases, no good metrics exist
 - Validation hard, because security not measured directly

Risk Management

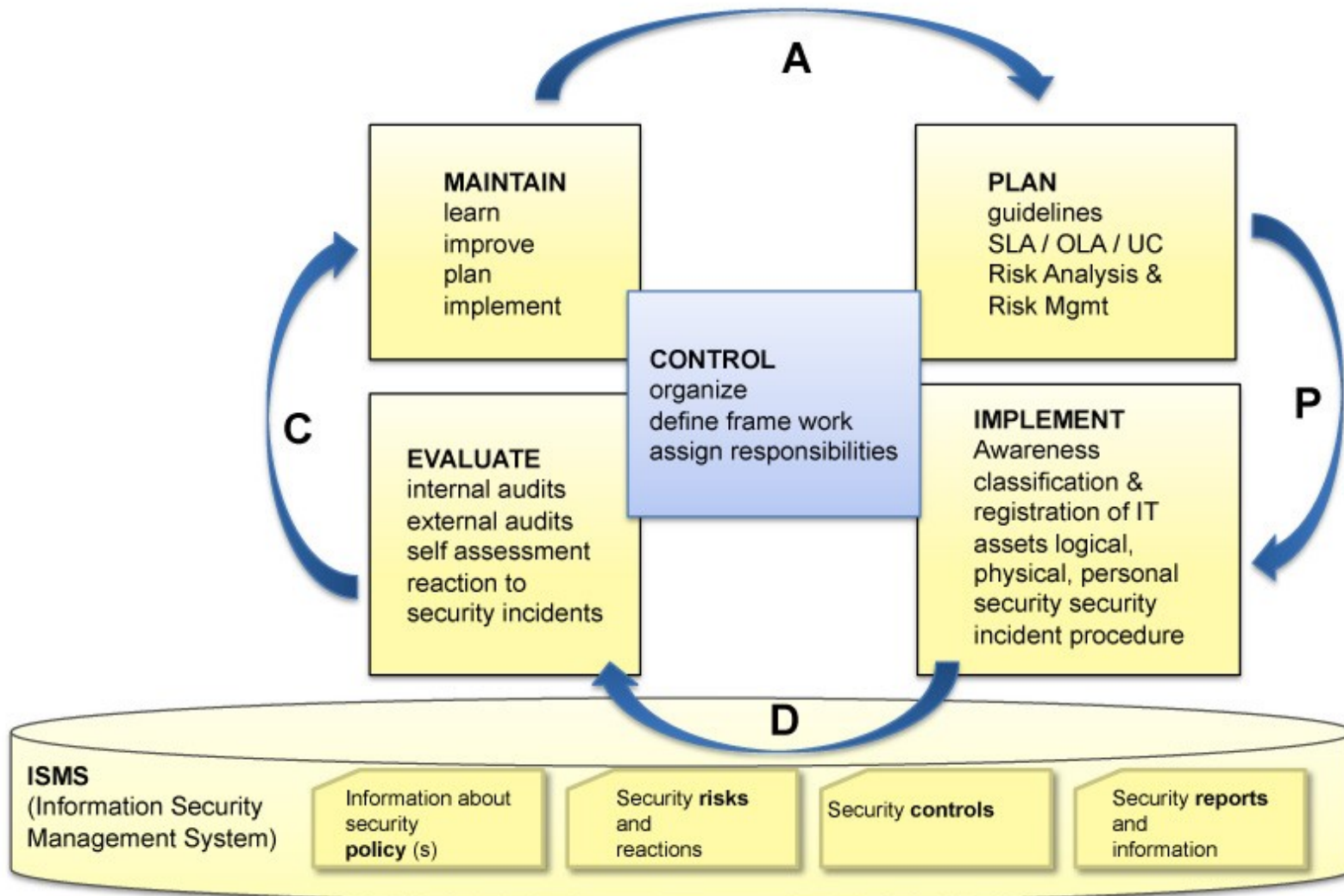
- Risk management process
 - Context
 - Risk identification (affected assets)
 - Risk assessment (likelihood, damage)
 - Risk treatment
 - Avoid/Prevent
 - Reduce
 - Accept
 - Transfer
 - Risk mitigation plan
 - Implementation
 - Review and evaluation
- 
- easy
- hard/impossible

ISMS

- Information Security Management System
- A systematic approach to managing sensitive company information so that it remains secure
- Includes people, processes, documents, and IT systems by applying a risk management process



ISMS Plan-Do-Check-Act cycle



ISO 27002:2013

- Guidelines for organisational information security standards and management practices
 - Select controls while implementing an ISMS
 - Implement commonly accepted controls
 - Develop own guidelines

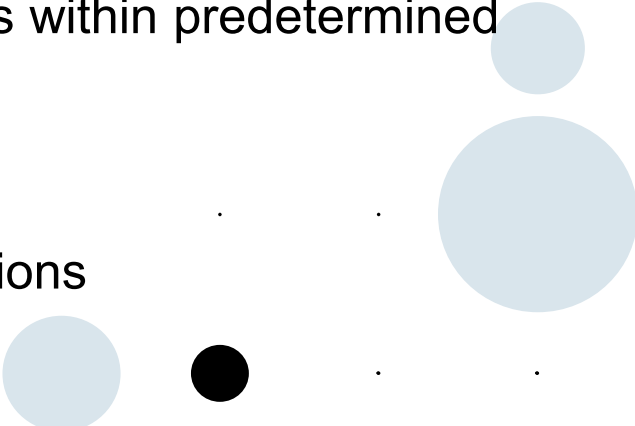
ISO 27002:2013 security controls

- 14 groups, 114 controls
 - Information security policies
 - High-level definition of secure behaviour for an organisation
 - Objectives
 - Constraints on organisation's members
 - Constraints on adversaries
 - Organisation of information security
 - Responsibility, reporting
 - Human resource security
 - Employees joining and leaving
 - Asset management
 - H/w, s/w lifecycle management; processes

ISO 27002:2013 security controls

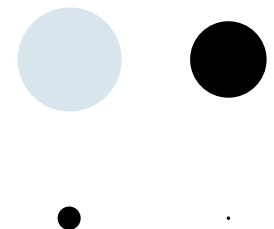
- 14 groups, 114 controls
 - Access control
 - Cryptography
 - Physical and environmental security
 - Facilities, resources, information stored on physical media
 - Operations security
 - Communications security
 - Systems acquisition, development and maintenance
 - SDLC, sourcing
 - Supplier relationships
 - Outsourcing

ISO 27002:2013 security controls

- 14 groups, 114 controls
 - Information security incident management
 - How to anticipate and respond to security breaches
 - Incident reporting systems
 - Learning from incidents
 - Information security aspects of business continuity management
 - Recover and restore critical functions within predetermined time
 - Loss of staff, equipment, data
 - Compliance
 - Legal, regulatory, contractual obligations
- 

BSI IT-Grundschutz (base protection) approach

- **Definition of values**
- Current state
- Protection requirements
- Modeling
- **Gap analysis**
- Additional security analysis, risk analysis for ca. 20% of assets; 80% covered by **configuration manuals**
- Consolidation of controls
- Verification of adapted controls
- Introduction of controls



BSI IT-Grundschutz



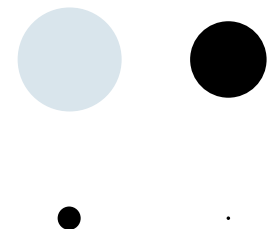
– Elementary threats

- Fire, water, local events/catastrophes
- Loss of service by supplier (e.g. power, connectivity)
- Electromagnetic emanation, wiretapping, espionage
- Theft, destruction, loss of devices
- Manipulation of data, infrastructure, communication
- Malfunctions, intended misuse, unintended misuse of systems
- Social engineering, identity theft, misuse of personal data

BSI IT-Grundschutz



- **Process** building blocks
 - ISMS
 - Organisation+Personnel
 - Concepts: Cryptography, Privacy, Backup, Selection of COTS software, Development and deployment of applications, Controlled data erasure, Business trips
 - **Operation**
 - Core IT operation: IT administration, Patch+Change management, Malware protection, Logging, Software testing and certification
 - Additional IT operation: Archival, Data exchange, Teleworking
 - Contracting of IT services
 - Detection and reaction



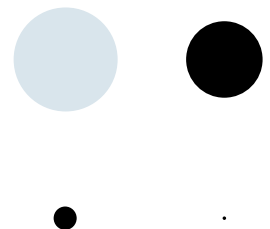
BSI IT-Grundschutz



- **System** building blocks
 - Applications: Office software, Network services, Business applications
 - IT systems: Servers, Desktops, Mobile devices, Embedded/IoT
 - Industrial IT
 - Networks and communication
 - Physical infrastructure

Personnel Security

- Manage security issues when employees join, move within and leave an organisation
 - Background checks (prediction of future behaviour based on past)
 - Personal issues that might affect security (debt, extortion, dissatisfaction with employer, planned change of employer)
 - Access management (configuration of access rights matching to current tasks/position)



Physical Security

- Prevention and deterrence of adversaries from accessing facilities, resources or information stored on physical media
 - Access to buildings, rooms, equipment (guards, locks, escorts, surveillance)
 - Restriction of movement of equipment, storage media (locks, trackers)

Vulnerability Management

CVE Common Vulnerabilities and Exposures

- IT operations
 - Use and configuration of existing systems
 - Tailored software → few users
 - COTS commercial off the shelf products → many users, can share info about vulnerabilities
 - Product version? Product configuration? Environment?
- CVE: list of identifiers and descriptions for discovered vulnerabilities
 - System administrators can determine if deployed systems are vulnerable (i.e. if there are known vulnerabilities)

CVE entry assignment

1. Discovery of potential vulnerability or exposure
2. Assignment of CVE ID by numbering authority
 - CVE-yyyy-nnnn
(sequence number might be longer than 4 digits)
 - Numbering authorities: CERTs (Computer Emergency Response Teams), vendors, projects, individual researchers, bug bounty programmes
 - Description
 - References, e.g. reports, advisories
3. Posting of CVE entry to list by primary numbering authority

CVE Entry Example

- CVE ID: CVE-2018-4916

Affected software, scope



- Description

An issue was discovered in Adobe Acrobat Reader 2018.009.20050 and earlier versions, 2017.011.30070 and earlier versions, 2015.006.30394 and earlier versions. The vulnerability is caused by the computation that writes data past the end of the intended buffer; the computation is part of the image conversion module that handles TIFF data. An attacker can potentially leverage the vulnerability to corrupt sensitive data or execute arbitrary code.

- References

<https://helpx.adobe.com/security/products/acrobat/apsb18-02.html>

<https://securitytracker.com/id/1040364>



Details, assessment, solutions

CVE Links to Other Resources

- CVE list is comprehensive
- Offers links to other resources, databases
 - Vulnerability details
 - Impact assessments
 - Solutions, workarounds
- Monitoring of deployed systems
- Reactions: accept risk, update, reconfigure, restrict access, disable, replace
- <https://nvd.nist.gov>, <https://www.cvedetails.com>

Summary

- IT security standards and processes
 - Standards as toolboxes, pick/adapt what you need based on risk assessment
 - Best practice? Average practice? Good enough?
- Vulnerability management
 - Awareness about vulnerabilities, dealing with vulnerabilities in products you do not control

