Security Standards, Methodologies and Guidelines

Matthias Hofherr, www.forinsect.com
License: Creative Commons CC BY-SA
Version 1.0

Security Management

- ISO 27005:2011: Information security risk management
- **IS Risk Management**
  - BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - Mehari (Information risk analysis and management methodology)
  - Octave - Operationally Critical Threat, Asset, and Vulnerability Evaluation (Risk Management Methodology)
    - Octave: Original for large organizations
    - Octave-S: for smaller organizations
    - Octave Allegro:focused on assets
  - NIST SP 800-39: Managing Information Security Risk - Organization, Mission, and Information System View
  - CWRAF: Common Weakness Risk Analysis Framework
- ISO 27000:2009: Information security management systems - Overview and vocabulary; free
- ISO 27001:2005: Information security management systems - Requirements
- ISO 27002:2005: Code of practice for information security management
- ISO 27003:2010: Information security management system implementation guidance
- ISO 27004:2009: Information security management - Measurement
- ISO 27011:2008: Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- PAS99: Integrated Management Systems
- PCI-DSS (Payment Card Industry - Data Security Standard)
- BSI IT Grundschutz "auf Basis von ISO 27001"
  - BSI Standard 100-1: Managementmentsysteme für Informationssicherheit
  - BSI-Standard 100-2: IT-Grundschutz Vorgehensweise
- COBIT (Control Objectives for Information and related Technology); Framework for IT Governance
- NIST SP 800-18: Guide for Developing Security Plans for Information Technology Systems
- NIST SP 800-40: Creating a Patch and Vulnerability Management Program
- NIST SP 800-55: Performance Measurement Guide for Information Security
- NIST SP 800-115: Technical Guide to Information Security Testing

Auditing

- **IDW: Prüfungsstandards des Instituts für Wirtschaftsprüfer**
  - IDW PS 980: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen
  - IDW PS 880: Die Prüfung von Softwareprodukten
  - IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie
    - IDW PH 9.330.1: Checkliste zur Abschlussprüfung bei Einsatz von Informationstechnologie
    - IDW RS FAIT 1: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie
    - IDW RS FAIT 2: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Electronic Commerce
    - IDW RS FAIT 3: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren
- SAS-70/SSAE-16: Statement on Auditing Standards No. 70 - Service Organizations
  - IDW PS 951: "Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen"; German variant of SAS-70
- BSI Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz

Business Continuity

- BS 25999: Business Continuity Management
  - BS 25999 part 1: Code of Practice for Business Continuity Management
  - BS 25999 part 2: Specification for Business Continuity Management
- BSI-Standard 100-4: Notfallmanagement

Technical

- **Hardening**
  - Security Technical Implementation Guides (STIGS) of NIST/NSA/DoD
  - Center of Internet Security (CIS) Benchmarks
- ISO 27033 [1-8: Security techniques — Network security (currently only part 1 released); formerly: ISO 18028 [1-5] IT network security
- BSI Technische Leitlinie TL 03420: Leitlinie für das Löschen und Vernichten von schutzbedürftigen Informationen auf Datenträgern; (available from BSI only on request)
- BSI Technische Richtlinie TR-03103 Sicheres Wireless LAN
- NIST SP 800-46: Guide to Enterprise Telework and Remote Access Security

Scoring

- CVSS: Common Vulnerability Scoring System
- CWSS: Common Weakness Scoring System

Penetration Testing and Technical Assessment

- OSSTMM (Open Source Security Testing Methodology Manual)
- ISSAF (Information Systems Security Assessment Framework)
- ASVS: OWASP Application Security Verification Standard Project
- PTF: Penetration Testing Framework

Products

- ISO 15408 Common Criteria
- PCI PA-DSS (Payment Card Industry - Payment Application Data Security Standard)
- PCI PTS (PIN Transaction Security)
- PCI P2PE (Point-to-Point Encryption)

Related Standards

- ISO 9001
- ISO 20000
  - ISO/IEC 20000 Part 1:2005 Information technology service management. Specification for Service Management
  - ISO/IEC 20000 Part 2:2005 Information technology service management. Code of Practice for Service Management
- ISO 31010:2009: Risk management — Risk assessment techniques
- ISO 19011:2002: Guidelines for quality and/or environmental management systems auditing
- ISO/IEC 38500: Corporate governance of information technology

Development

- Microsoft Security Development Lifecycle (SDL)
- NIST SP-800-64 Security Considerations in the System Development Life Cycle
- OWASP Secure Coding Practices
- OWASP Code Review Project
- OWASP Testing Project