

bw digitronik, Security Management Event, Dienstag, 30.9.2008

Informationssicherheit Standards: Vom Hilfsmittel zum Zwang?

Prof. Dr. Peter Heinzmann, cnlab AG und
HSR Hochschule für Technik Rapperswil

Standardtypen

- Internationale Standards (z.B. ISO)
- Industriestandards (z.B. ECMA)
- Standards von Staatsstellen (z.B. NIST NVD)
- De Fakto Standards (z.B. MS Office)
- Standards von Berufsorganisationen und Verbänden (z.B. IEEE, OSTTMM)
- „Open Source“ Standards (z.B. Internet RFCs)
- Hersteller spezifische Standards
- Interne Standards

Wozu nutzen wir Standards?



Kompatibilität

Markterweiterung (Export)

Differenzierung gegenüber Mitbewerbern

Checkliste, Framework

Antwort auf Kundenforderung

Unabhängige Prüfung

Best Practice Bestätigung

**Internes Kontrollsystem
(IKS, OR728a)**



Protected by
PRIVACY LABEL



**Auszeichnung
(Gütesiegel)**

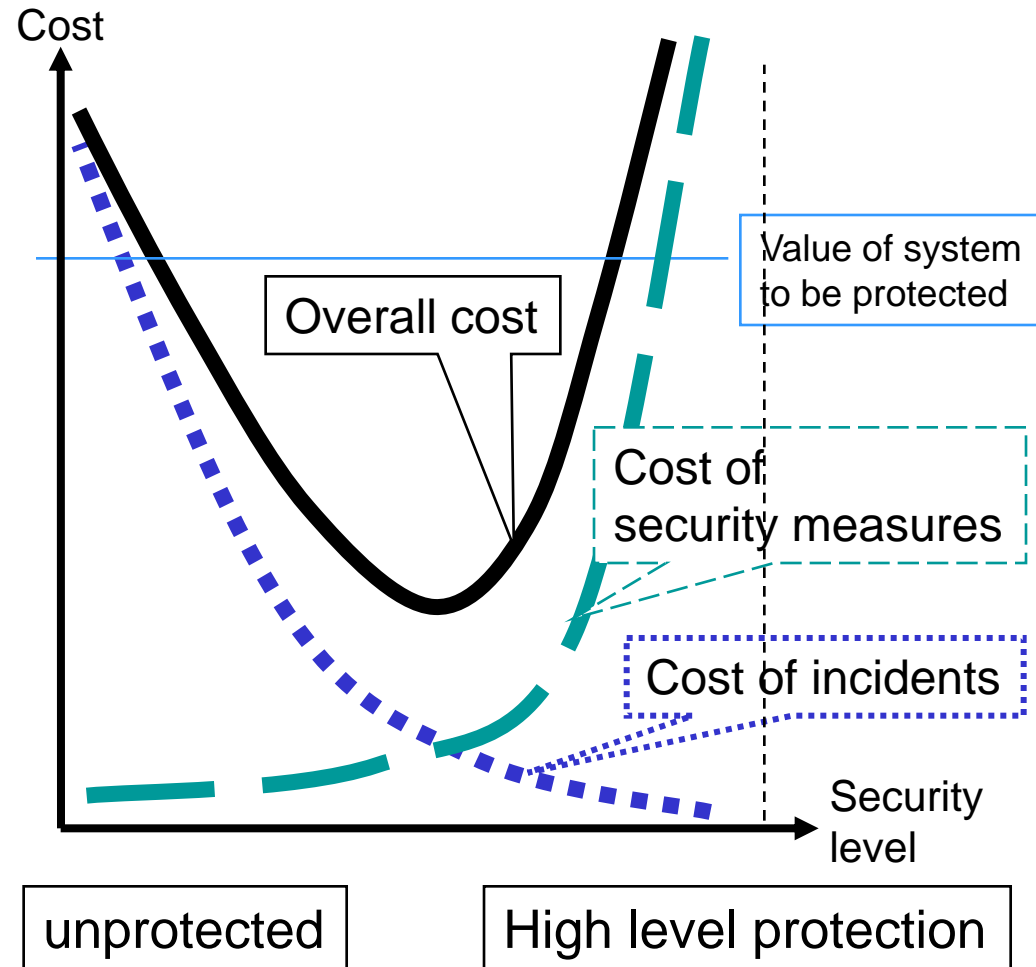
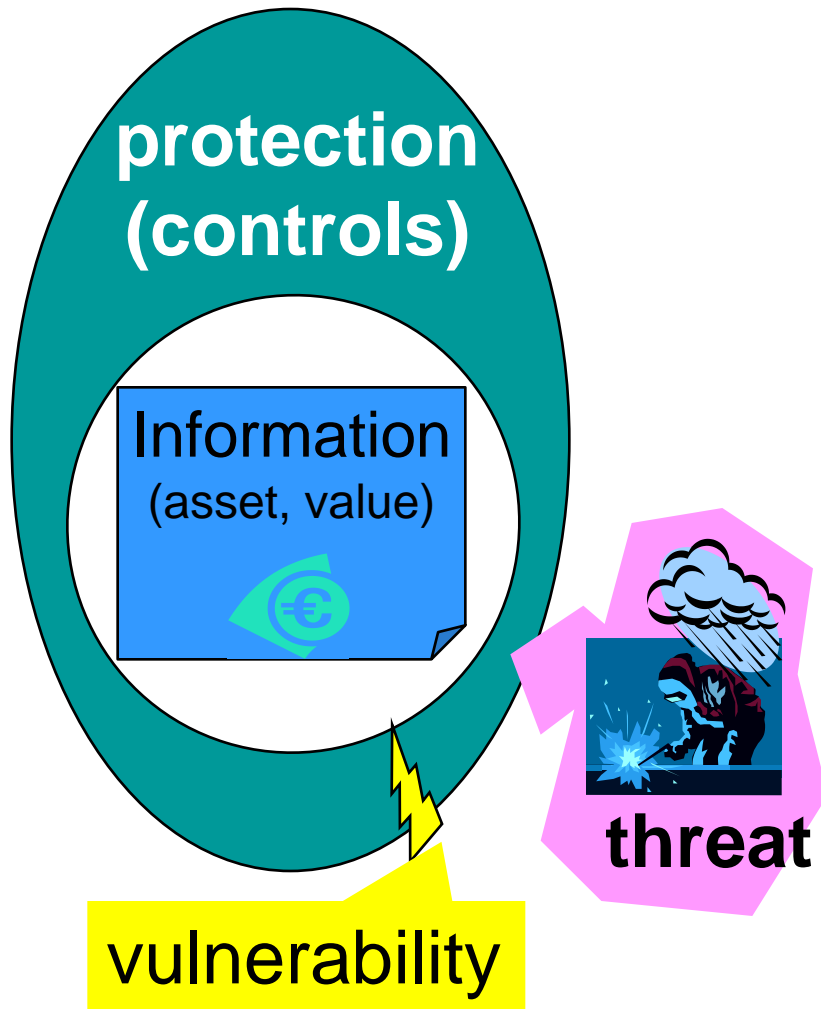
Was heisst „Informationssicherheit“?

- Informationen sind
 - Im Kopf
 - In der „Luft“ (Gespräch, Telefonat)
 - Auf Papier (Dokument, Buch)
 - Auf elektronischen Speichermedien (Disk, USB, Tonband, Video)
- Informationen sind
 - Vertraulich (confidentiality)
 - Echt, unverfälschbar (integrity)
 - Verfügbar (availability)



Das „Informationssicherheitsproblem“

Risiko = WSK Zwischenfall ■ Schaden = Bedrohung ■ Verletzlichkeit der Schutzmassnahmen ■ Schaden



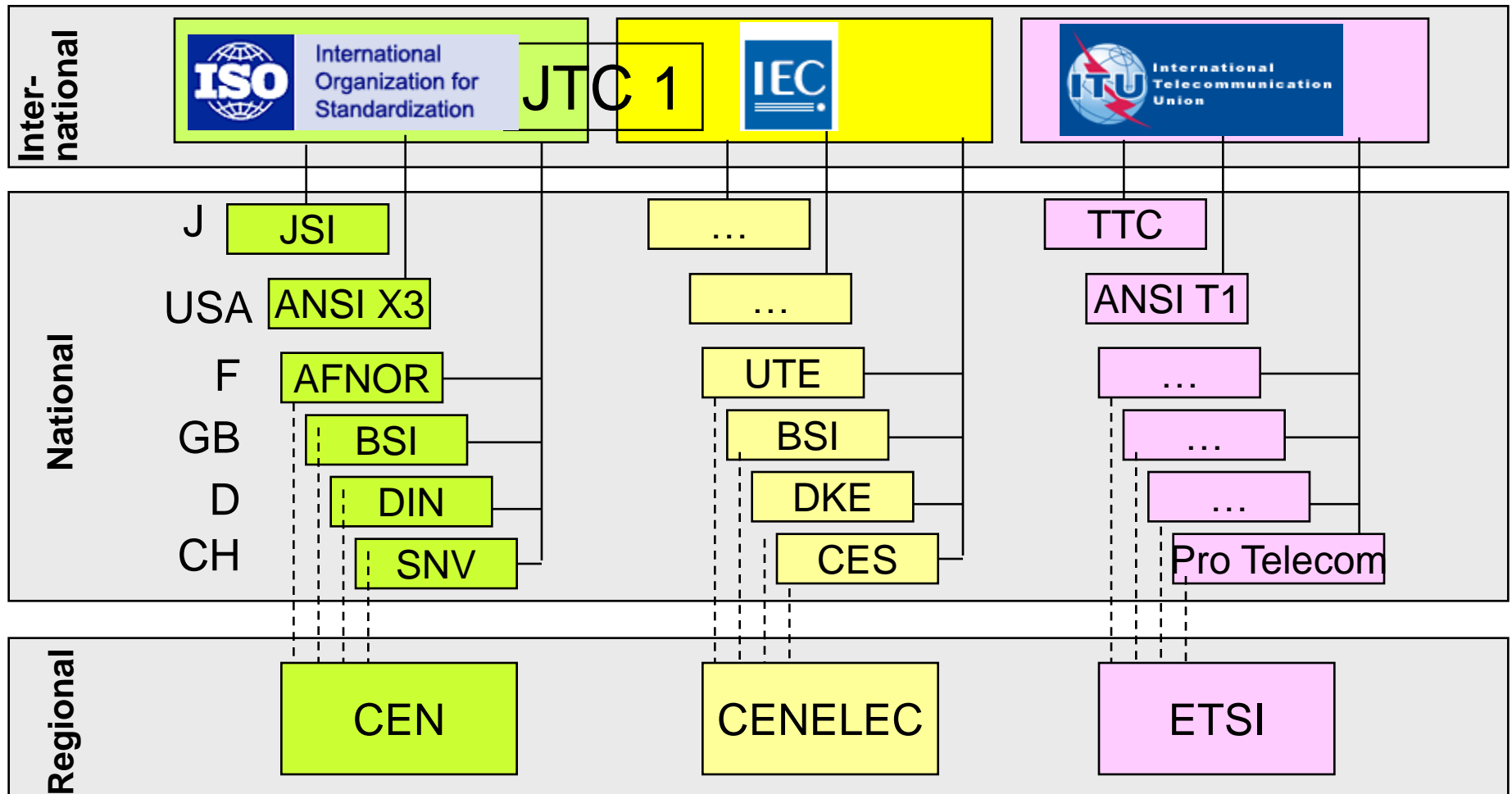
Standardisierungsgremien und Standardisierungsprozesse

International Standardization Groups

(Informatics)

Electrical

Telecommunications





IEEE

Institute of Electrical and Electronics Engineers IEEE Standards Board

Technical Committees (TC)

Technical Committee on
Computer Communication
TCCC

Technical Committee on
Security and Privacy
TCSP

Projects

**IEEE Project 802
Local and Metropolitan
Area Network Standards**

Executive Committees

802.0 Executive Committee

Working Groups (WG)

802.1
Higher Layer
Interfaces

802.2
Logical
Link
Control

802.3
CSMA/CD
BUS

802.4
Token
Bus

802.5
Token
Ring

802.6
MANs

802.7
Broadband
TAG

802.8
Fiber
Optical
TAG

802.9
Integration
voice and
data LAN
Interfaces

802.10
Standards
for inter-
operable
LAN secur

802.11
Wireless
LANs

Technical Advisory
Groups (TAG)

Internet Society (ISOC)

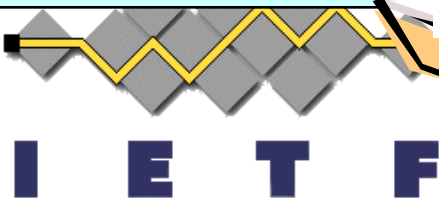


Internet Society

(>6'000 individuals and 150 organisations)

Internet Architecture Board (IAB)

Internet
Engineering Task
Force (IETF)



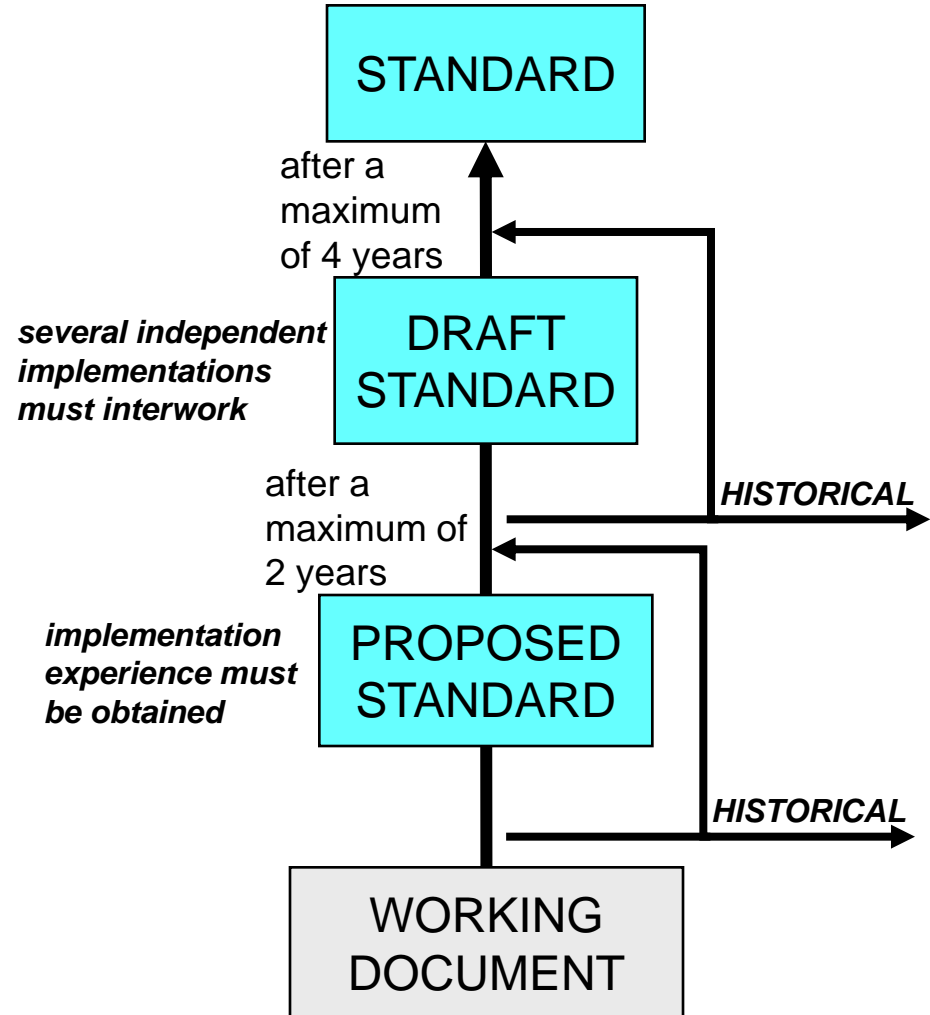
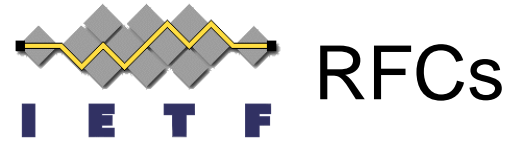
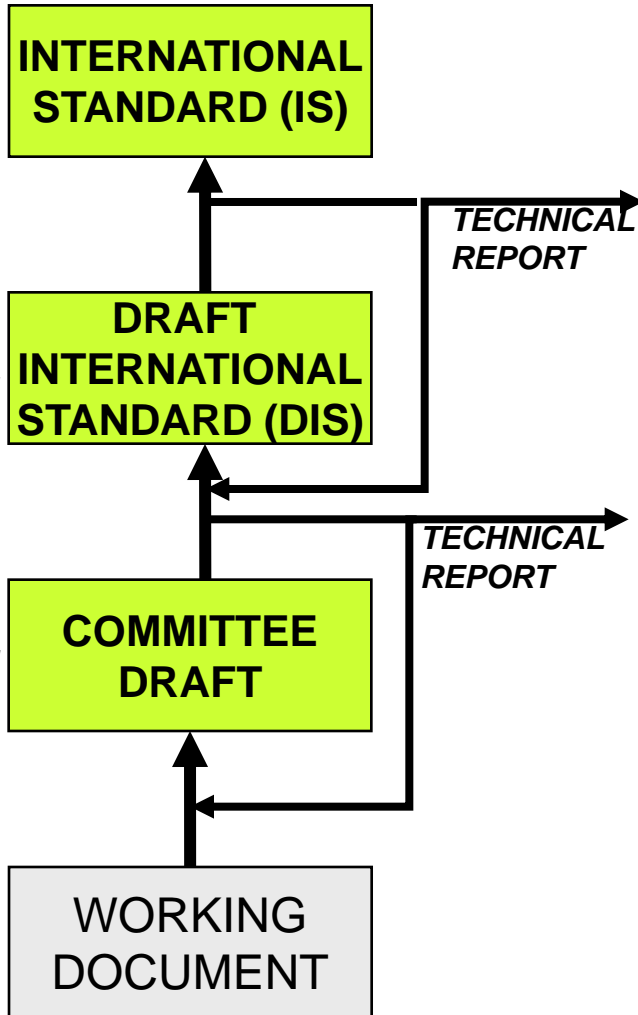
Internet
Research Task
Force (IRTF)

Internet Assigned
Numbers Authority
(IANA)

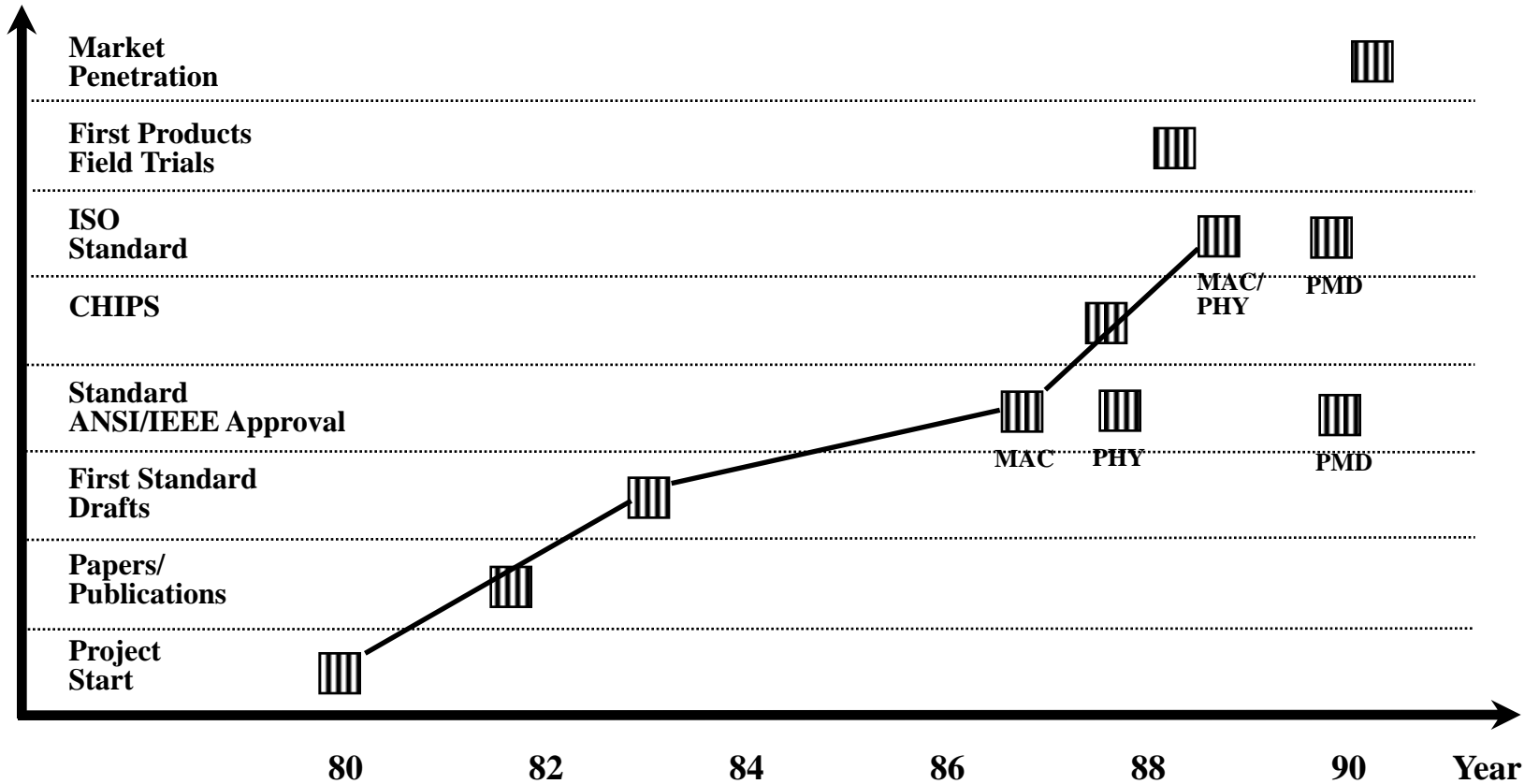


<http://www.networksorcery.com/enp/default0701.htm>

ISO and IETF Standardization Processes



ANSI Example: FDDI



Security Standards

ISO 27000 Series: Information Security

Information Security Management Systems (ISMS) - Requirements

BS 7799-2:2002

**BS ISO/IEC 27001:2005 (34p, \$159)
BS 7799-2:2005**

Code of Practice for Information Security Management

BS 7799-1:1995

BS ISO/IEC 17799:2000

BS ISO/IEC 27002:2007 (p. 115, \$199)

Guidance for the implementation of an ISMS

ISO 27003:2009

Information Security Management measurement & metrics

ISO 27004 (Draft)

Information Security Risk Management (ISRM)

BS 7799-3:2005

ISO 27005:2008 (55p, \$324)

Requirements for bodies providing audit and certification of ISMS

ISO 27006:2007 (46p, \$271)



IT-Grundschutzhandbuch des BSI:

5 BSI-Schichten (und Auswahl von „Bausteinen“)

Übergreifende Aspekte

- Sicherheitsmanagement
- Organisation
- Personal
- Notfall-Vorsorgekonzept
- Datensicherungskonzept
- Virenschutzkonzept
- Hard- und Software-Management
- Outsourcing

Infrastruktur

- Gebäude
- Verkabelung
- Büroraum
- Serverraum
- häuslicher Arbeitsplatz
- Rechenzentr.

IT-Systeme

- Unix-Server
- Novell Netw.
- Windows 2k
- TK-Anlage
- Telearbeit

Netze

- Netz-, Systemmanagement
- Firewall
- Remote Access
- Router u. Switches

Anwendungen

- E-Mail
- WWW-Server
- Datenbanken
- IIS/ Apache
- Exchange/ Outlook
- Archivierung

IT-Verbund

BSI Kataloge

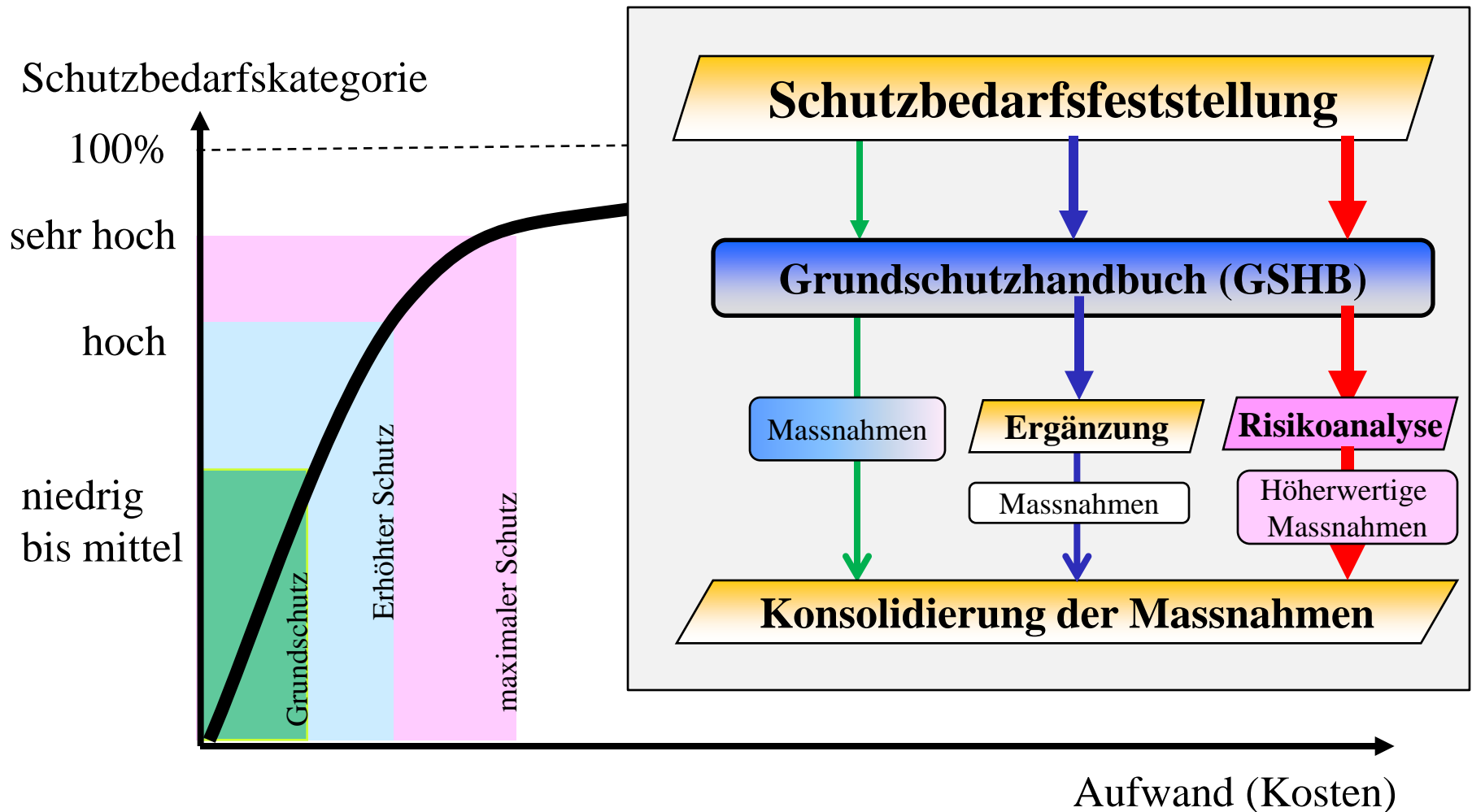
Gefährdungskataloge

- G 1 Höhere Gewalt
- G 2 Organisatorische Mängel
- G 3 Menschliche Fehlhandlungen
- G 4 Technisches Versagen
- G 5 Vorsätzliche Handlungen

Massnahmenkataloge

- M 1 Infrastruktur
- M 2 Organisation
- M 3 Personal
- M 4 Hardware/Software
- M 5 Kommunikation
- M 6 Notfallvorsorge

BSI Schutzbedarfsfeststellung: Schutzbedarfskategorien und Aufwand



International Standardization Organisation (ISO)		British Standardization Institution (BSI)		(Deutsches) Bundesamt für Sicherheit in der	
Nummer	Titel	Nummer	Titel	Nummer	Titel
ISO 27001:2005	Specification for an information security management system (ISMS) 40 pages, CHF 140	BS 7799-2:2002	Information Technology - Code of Practice for Information Security Management, 34 pages	100-1 Ver 1.0 Dec 2005	Managementsysteme für Informationssicherheit (ISMS) 35 pages, free
ISO 27002:2007	Code of Practice for Information Security Management 80 pages, CHF 235	BS 7799-1:2005 (ISO/IEC 17799:2005)	Code of practice for Information Security Management Systems - Specification with Guidance for	100-2 Ver 2.0 Dec 2005	IT-Grundschutz-Vorgehensweise 80 pages, free
ISO 27003:2005	Guidance for the implementation of an ISMS				IT-Grundschutzkataloge (Grundschutz-Handbuch) jährlich neu 3000 pages, free
ISO 27004 (Draft)	Information Security Management measurement & metrics				
ISO 27005:2005	Information Security Risk Management (ISRM) 55p, \$324	BS 7799-3:2005	Guidelines for Information Security Risk Management \$ 161	100-3 Ver 2.0 Dec 2005	Risikoanalyse auf der Basis von IT-Grundschutz 10 pages, free
ISO 27006:2005	Guidelines for information and communications technology disaster recovery services 46p, \$271				
ISO 27007	Requirements for bodies providing audit and certification of ISMS				

US Government Security Standards

- Information Security Automation Program (ISAP)
 - U.S. government multi-agency initiative to enable automation and standardization of technical security operations
- Security Content Automation Protocol (SCAP)
 - method for using specific standards to enable
 - automated vulnerability management, measurement, and policy compliance evaluation
- National Vulnerability Databas (NVD)
 - U.S. government content repository for ISAP and SCAP

National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD)

National Vulnerability Database - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://nvd.nist.gov/

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

Search CVE, Download CVE, Statistics, Contact, FAQ

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the CVE vulnerability naming standard.

Resource Status

NVD contains:
12792 CVE Vulnerabilities
38 US-CERT Alerts
1090 US-CERT Vuln

Search CVE Vulnerability Database (Perform Advanced Search)

Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Show only vulnerabilities that have the following associated resources:

- US-CERT Technical Alerts
- US-CERT Vulnerability Notes
- US-CERT Technical Alerts or Vulnerability Notes
- OVAL Queries

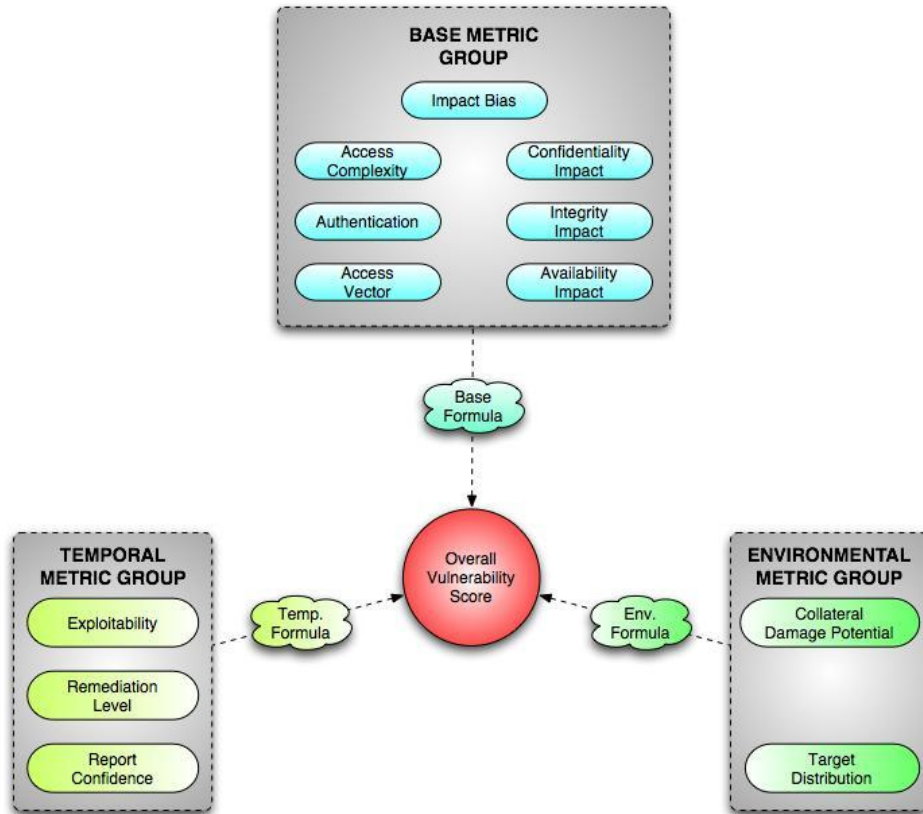
Recent CVE Vulnerabilities

CAN-2005-2337 Publish Date: 10/7/2005
Ruby 1.6.x up to 1.6.8, 1.8.x up to 1.8.2, and 1.9.0 development up to 2005-09-01 allows attackers to bypass safe level and taint flag protections and execute disallowed code when Ruby input (stdin).

<http://nvd.nist.gov>

Vulnerability Scoring System Calculator

<http://nvd.nist.gov/cvss.cfm?calculator>



Base Metrics

- **Related exploit range** (AccessVector): local, remote
- **Attack complexity** (AccessComplexity): high, low
- **Level of authentication needed** (Authentication): required, not required
- **Confidentiality impact** (ConfImpact): none, partial, complete
- **Integrity impact** (IntegImpact): none, partial, complete
- **Availability impact** (AvailImpact): none, partial, complete
- **Impact value weighting** (ImpactBias): weight confidentiality, weight integrity, weight availability

Environmental Metrics

- **Organization specific potential for loss** (CollateralDamagePotential): none, low (light loss), medium (significant loss), high (catastrophic loss)
- **Percentage of vulnerable systems** (TargetDistribution): none (0%), low (0-25%), medium (26-75%), high (75-100%)

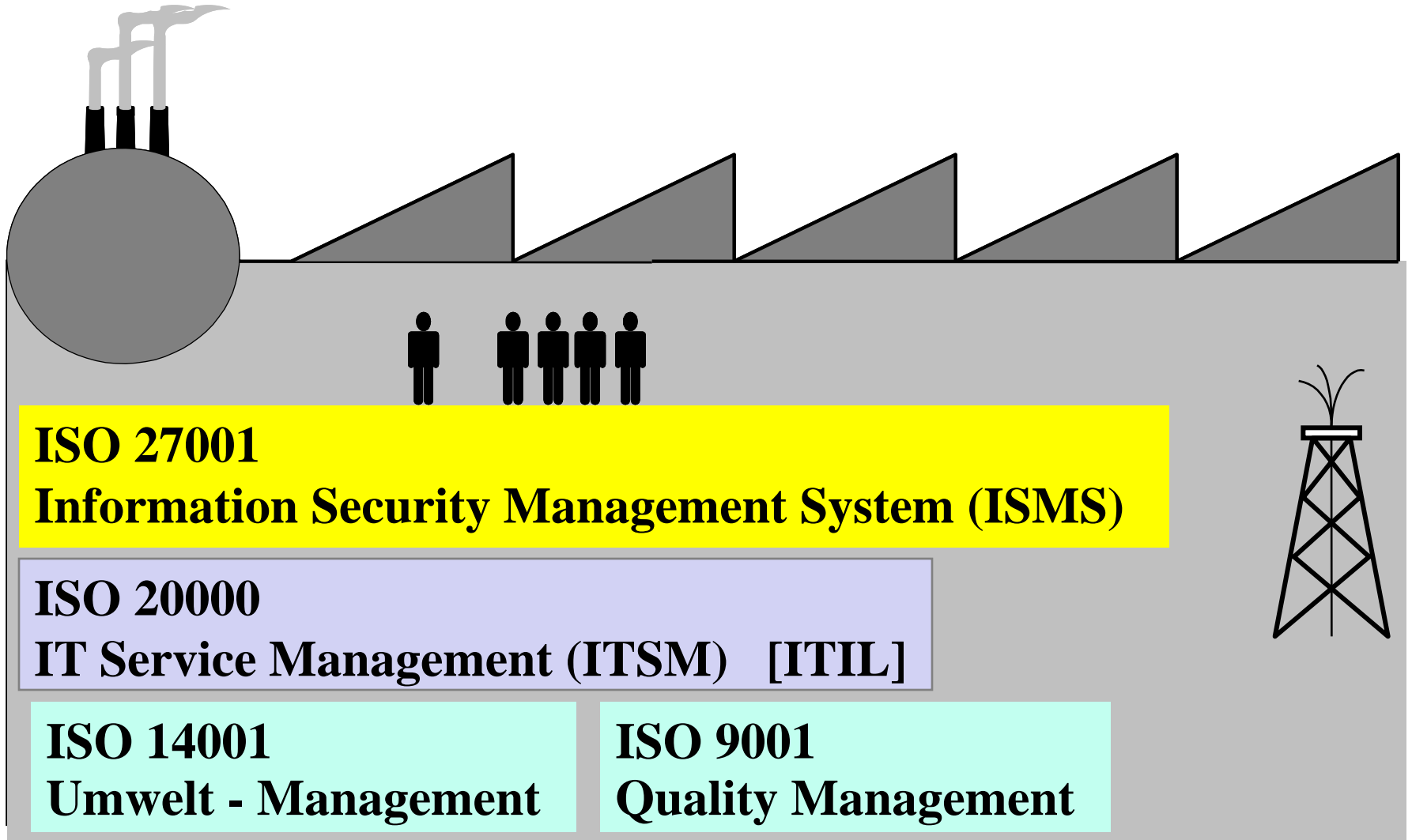
Temporal Metrics

- **Availability of exploit** (Exploitability): unproven that exploit exists, proof of concept code, functional exploit exists, high
- **Type of fix available** (RemediationLevel): official fix, temporary fix, workaround, fix unavailable
- **Level of verification that vulnerability exists** (ReportConfidence): unconfirmed, uncorroborated, confirmed

- **Offene und frei verfügbare Methodik** zur Planung, Durchführung und Dokumentation von Security Audits
- **Sicherheitsniveau als Zahlenwert** (Risk Assessment Value)
- **Verhaltenskodex** für Tester (Rules of Engagement)
- **Compliant** zu ISO/IEC 2700x, ITIL, GSHB, ...

Zertifizierung

ISO Management Zertifizierungsstandards



Standard Zertifizierungsstellen

Schweizerische Akkreditierungsstelle (SAS)
(Bundesamt für Metrologie und Akkreditierung, Bund)

akkreditiert

ISO 27001
Zertifizierungsstelle (KPMG, SQS, ...)

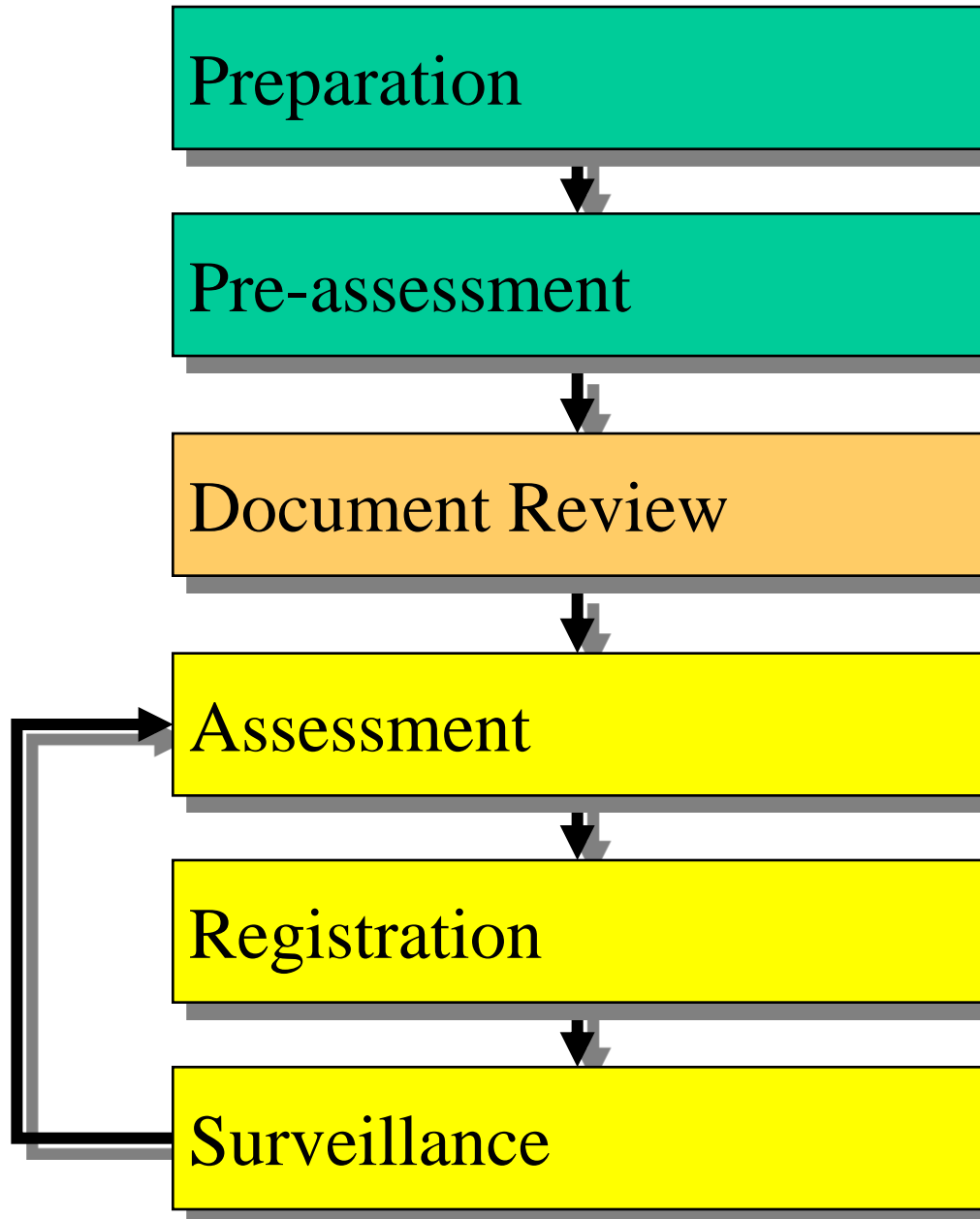
anerkennt
(zertifiziert)

Firma mit
ISO 27001 ISM

Firma mit
ISO 27001 IS

Firma mit
ISO 27001 ISMS-Implementierung

Ablauf der Zertifizierung



BSI IT-Grundschutz-Zertifizierung: Erfahrungen

- IT-GS-Zertifizierung ist sowohl für kleine Unternehmen als auch für große Rechenzentren geeignet!
- Umsetzung GSHB: 6 - 12 Monate
- Aufwand des Auditors: ca. 10 Tage
- Erfolgsfaktoren:
 - Unterstützung durch die Geschäftsleitung
 - Verständnis, Kooperationsbereitschaft und aktive Unterstützung durch die IT- und TK-Verantwortlichen
 - konsequente Gruppenbildung
 - Tool-Unterstützung

BSI IT-Grundschutz-Zertifizierung

Ausprägungen

	Selbsterklärung Einstiegsstufe	Selbsterklärung Aufbaustufe	Zertifikat
Anzahl der Maßnahmen			
Anforderungen an den Prüfer	keine	keine	lizenzierter Auditor
Prüfung des Auditreports	keine	keine	BSI
Kosten (BSI)	20 €	20 €	2500 €

Information Security Management System (ISMS): Certifications in Switzerland, April 2008

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
ACM Advanced Currency Markets SA	Switzerland	GB07/72810	SGS United Kingdom Limited	ISO/IEC 27001:2005
AlpTransit Gotthard AG	Switzerland	13827	SQS	BS 7799-2:2002
Beda Informatik AG	Switzerland	30671	SQS	BS 7799-2:2002
innova Versicherungen AG, innova Krankenversicherung AG	Switzerland	30768	SQS	BS 7799-2:2002
Reuters SA	Switzerland	IS 509254	BSI	ISO/IEC 27001:2005
RTC Real Time Center AG, Liebefeld	Switzerland	20279	SQS	BS 7799-2:2002
Serono International S.A.	Switzerland	GB05/64392	SGS United Kingdom Limited	BS 7799-2:2002
Serono International SA The Information Technology Function	Switzerland	GB05/64392	SGS United Kingdom Limited	ISO/IEC 27001:2005
SRG SSR idée suisse	Switzerland	20794	SQS	BS 7799-2:2002
Swiss Post Post Finance Information Technology, Berne	Switzerland	001 / 2002	KPMG SA	BS 7799-2:2002
Swisscom IT Services AG	Switzerland	11992	SQS	BS 7799-2:2002
T-Systems Schweiz AG	Switzerland	068379 ISMS	DQS GMBH	ISO/IEC 27001:2005

Wieso sollen wir zertifizieren ?



Kompatibilität

Markterweiterung (Export)

Differenzierung gegenüber Mitbewerbern

Checkliste, Framework

Antwort auf Kundenforderung

Unabhängige Prüfung

Best Practice Bestätigung

**Internes Kontrollsystem
(IKS, OR728a)**



**Auszeichnung
(Gütesiegel)**