

Sicherheitsstandards – für wen?

Ein Leitfaden von BITKOM und DIN

Dr. Walter Fumy



SIEMENS

Agenda

- Motivation
 - Nutzen von Standards
 - Quellen und Arten von Standards
 - Klassifizierung von Sicherheitsstandards

- Kompass der IT-Sicherheitsstandards
 - Überblick
 - Die Matrix
 - Behandelte Standards / Vorschriften

- Zusammenfassung

Nutzen von Standards

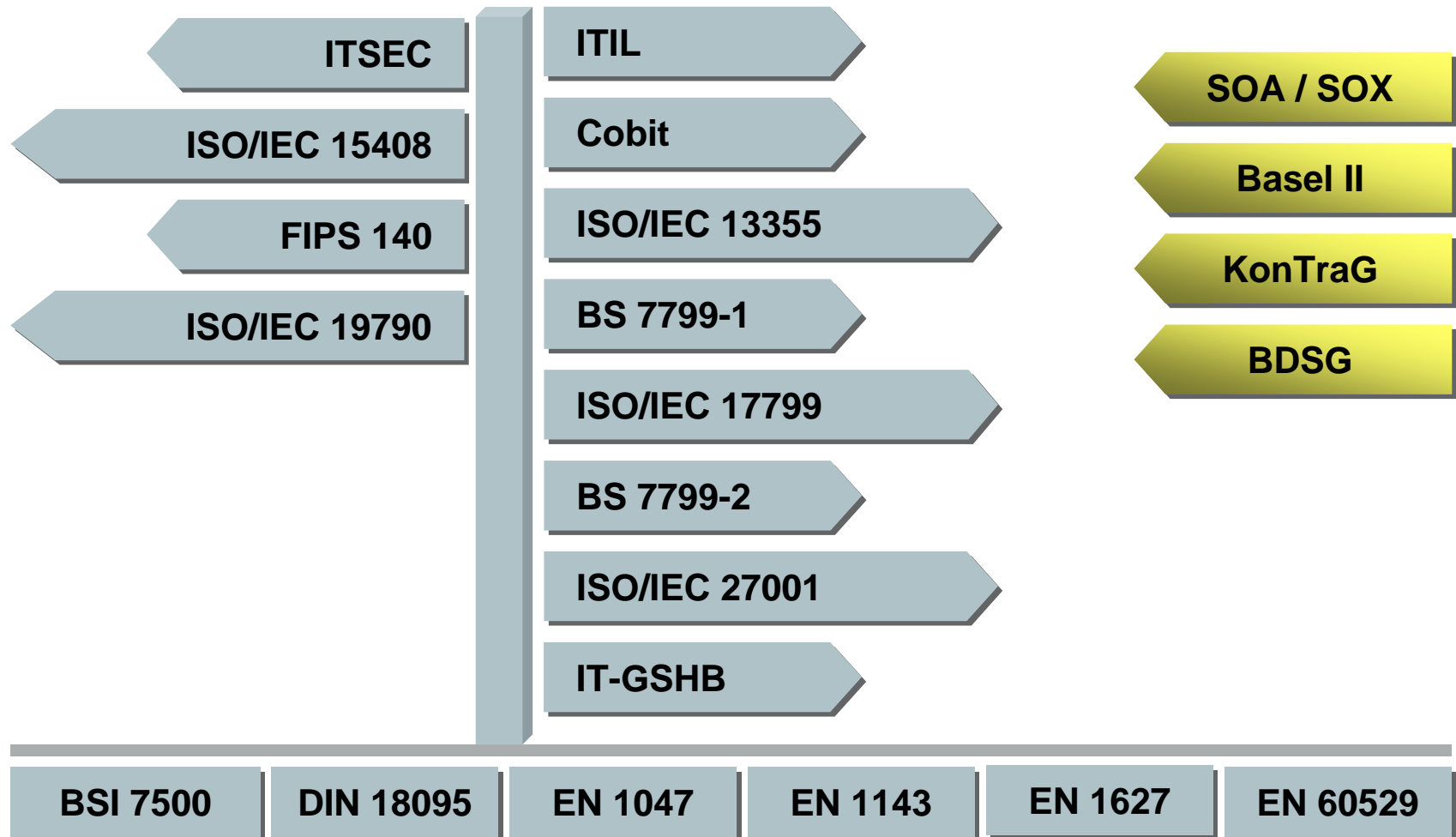
Kostensenkung	<ul style="list-style-type: none">▪ Nutzung vorhandener und praxiserprobter Vorgehensmodelle▪ Methodische Vereinheitlichung und Nachvollziehbarkeit▪ Ressourceneinsparung durch Kontinuität und einheitliche Qualifikation▪ Interoperabilität
Einführung eines angemessenen Sicherheitsniveaus	<ul style="list-style-type: none">▪ Orientierung am Stand der Technik und Wissenschaft▪ Gewährleistung der Aktualität▪ Verbesserung des Sicherheitsniveaus durch die Notwendigkeit der zyklischen Bewertung
Wettbewerbsvorteile	<ul style="list-style-type: none">▪ Zertifizierung des Unternehmens sowie von Produkten▪ Nachweisfähigkeit bei öffentlichen und privatwirtschaftlichen Vergabeverfahren▪ Verbesserung des Unternehmensimage▪ Stärkung der Rechtssicherheit

Quellen und Arten von Standards

ISO/IEC-Standards	<ul style="list-style-type: none">▪ internationale Normen▪ i.d.R. unter deutscher Mitwirkung nach einem Konsensverfahren entwickelt und mittels öffentlicher Umfrage bestätigt▪ Quelle überwiegend Subkomitee 27 "IT-Security Techniques" von ISO/IEC JTC1
DIN EN-Standards	<ul style="list-style-type: none">▪ Europäische Normen▪ von einer der Europäischen Normenorganisationen CEN, CENELEC oder ETSI, ebenfalls nach einem Konsensverfahren mit öffentlicher Umfrage entwickelt
Andere Standards	<ul style="list-style-type: none">▪ Entwickelt von Konsortien, Interessengruppen oder Behörden nach deren jeweiligen Regeln▪ Gegenüber Normungsorganisationen i.d.R. eingeschränkter Konsensrahmen bzw. Mitwirkungsmöglichkeiten



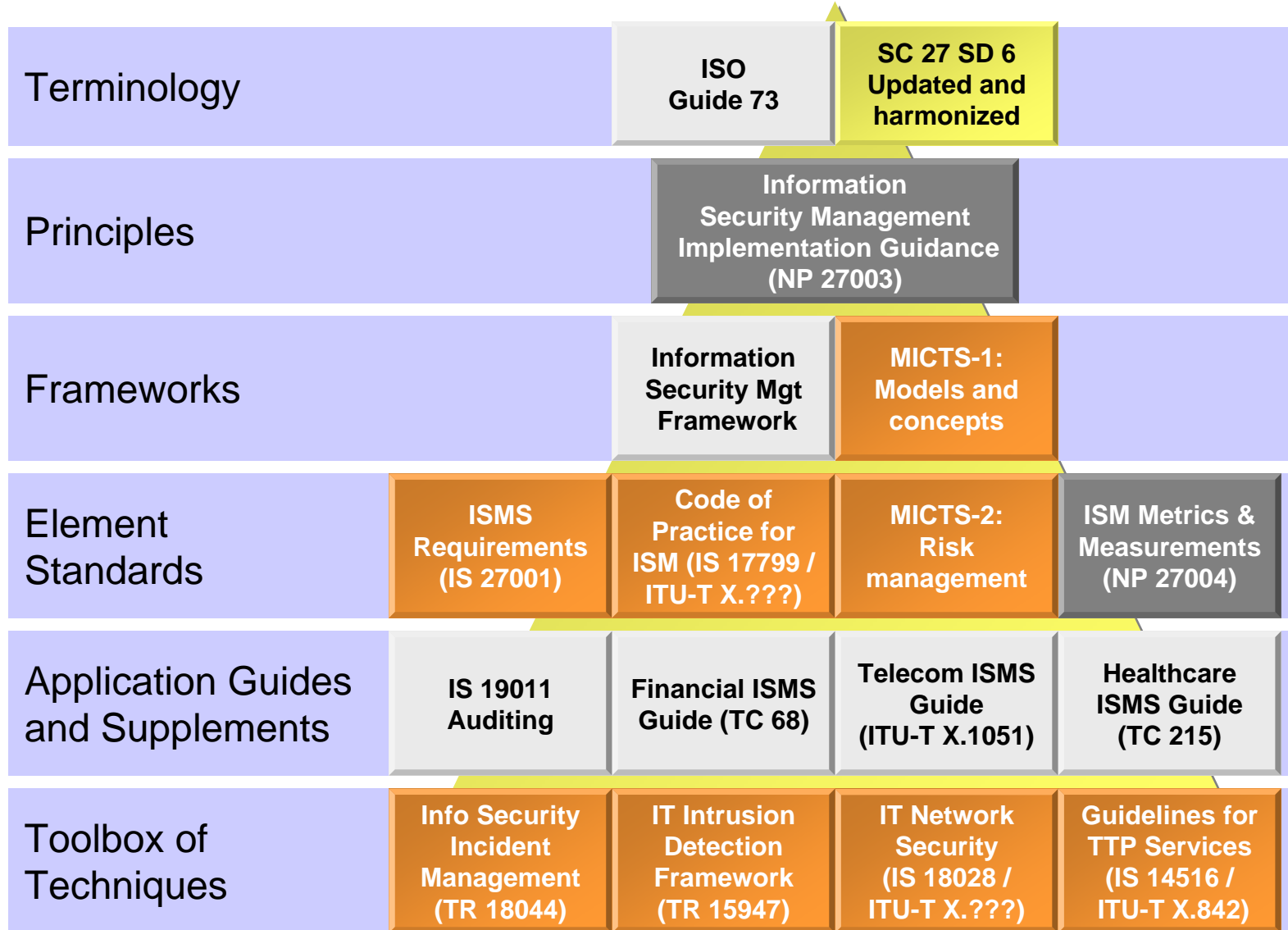
Sicherheitsstandards und Vorschriften – Beispiele



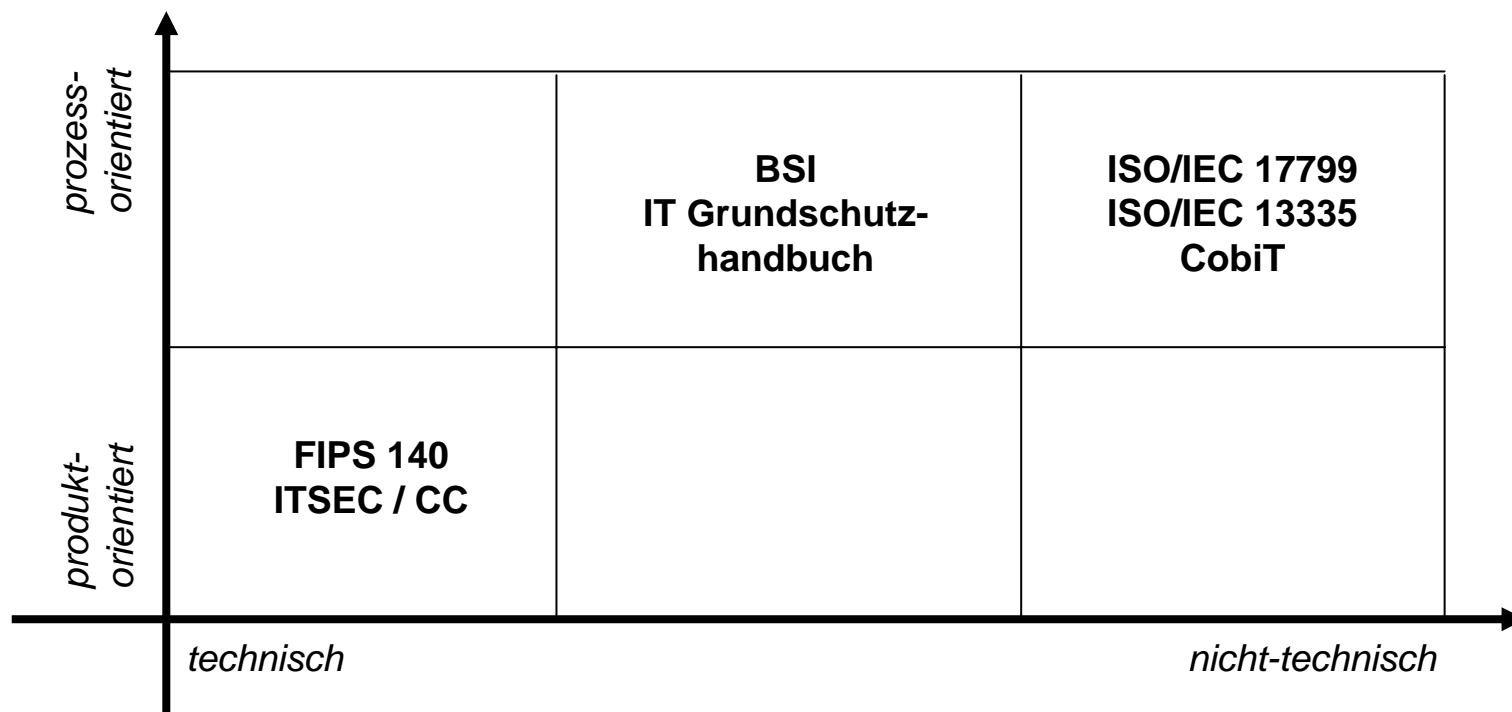


SC 27

Klassifizierung ausgewählter Standards – Beispiel 1 (Quelle: SC 27)



Klassifizierung ausgewählter Standards – Beispiel 2

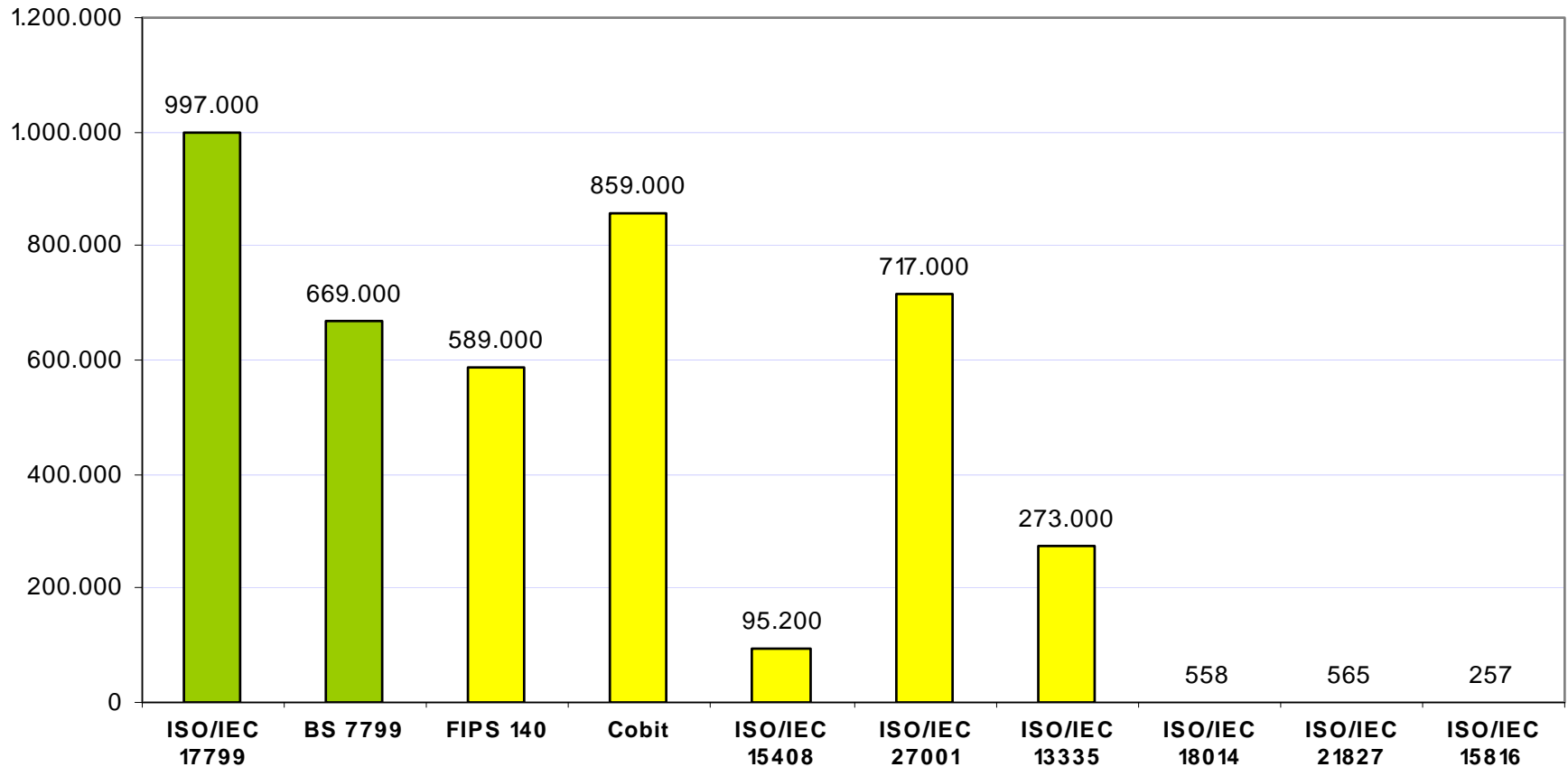


Quelle: Initi@tive **D²¹**

Klassifizierung ausgewählter Standards – Beispiel 3

Standard	Subject	Audience	Granularity	Certificate	Purpose	Focus
ISO/IEC 13335 (GMITS)	ICT Security	Security Officer	Medium (200+ pages)	No	System / Process	Functionality / Assurance
ISO/IEC 17799 (BS 7799-1)	Information Security	Security Officer	Medium (84 pages)	No	Process / System	Functionality
ISO/IEC 27001 (BS 7799-2)	Information Security	Management	Low (40 pages)	Yes	System	Assurance
BSI IT-GSHB	ICT Security	Security Officer & Administrator	High (3.000+ pages)	Yes	Process / System	Functionality / Assurance

Klassifizierung ausgewählter Standards – Beispiel 4 (Google Hits, 19.10.2006)



Kompass der IT-Sicherheitsstandards – Übersicht



- Kompass der IT-Sicherheitsstandards
Leitfaden und Nachschlagewerk

- Behandelt
 - 45 Standards
 - 4 Vorschriften
- Analysiert
 - 14 Merkmale Standard
 - 17 Merkmale Unternehmen
 - in 49 x 31 Matrix
- Umfang 2. Ausgabe: 92 Seiten
- Erhältlich unter
http://www.bitkom.org/de/publikationen/38337_40496.aspx

Kompass der IT-Sicherheitsstandards – Merkmale

Art des Unternehmens

- Banken/Versicherungen
- Behörden/Verwaltungen
- Beratung
- HW/SW-Hersteller
- IT-Dienstleister
- Gesundheitswesen
- Kanzleien
- Handwerk und Industrie
- Dienstleister
- internationale Ausrichtung

Rolle innerhalb des Unternehmens

- Management
- Revisoren
- IT-Sicherheitsbeauftragter
- IT-Leitung
- Administratoren
- Projektmanagement
- Entwicklung

Merkmale des Standards/der Vorschrift

- produktorientiert
- systemorientiert
- technisch
- organisatorisch
- strategisch
- konzeptionell
- operationell
- Zertifizierung
- Umfang (Seiten)
- Kosten

Quelle des Standards

- Nationale Normungsorganisation
- Europäische Normungsorganisation
- Internationale Normungsorganisation
- Andere Regelwerke

Kompass der IT-Sicherheitsstandards – Die Matrix (I)

Abbildung 2:
Kompass der IT-Sicherheitsstandards V2.0

	Grundlegende Standards zum IT-Sicherheits- und Risikomanagement										Standards mit IT-Sicherheitsaspekten			Vorschriften			Evaluierung von IT-Sicherheit									
	Informationswirtschafts-Managementsysteme (ISMS)					Sicherheitsmaßnahmen und Monitoring								Common Criteria					Schutzprofile							
	ISO/IEC 15335	ISO/IEC 27001	ISO/IEC 27799	ISO/IEC 27004	T-G-SMB	ISO/IEC 8028	ISO/IEC TR 8844	ISO/IEC 8043	ISO/IEC TR 8547	ISO/IEC 85316	CoBIT	ITIL	ISO/IEC 31000	KonTraG	Basel III	ISOX	BS95	ISO/IEC 15408 (CC)	ISO/IEC TR 15413	ISO/IEC 30045	ISO/IEC TR 9779	ISO/IEC 19790 (PPS 14.5-2)	ISO/IEC 19792	ISO/IEC 21827 (SSE-CMM)	ISO/IEC TR 15414	
Art des Unternehmens	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Banken/Versicherungen	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Behörden/Verwaltungen	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Beratung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
HW/SW-Hersteller	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
IT-Dienstleister	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Gesundheitswesen *	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Kanzleien **	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Handwerk und Industrie	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Dienstleister	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Internat. Ausrichtung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Rolle innerhalb des Unternehmens	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Management	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Revisoren	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
IT-Sicherheitsbeauftragter	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
IT-Leitung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Administratoren	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Projektmanagement	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Entwicklung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Merkmale des Standards/der Vorschrift	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
produktorientiert	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
systemorientiert	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
technisch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
organisatorisch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
strategisch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
konzepionell	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
operationell	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Zertifizierung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Umfang (Seiten)	206	40	84	37	24	206	50	55	22	20	75	1K	30	-	-	66	-	351	157	286	172	61	37	120	133	
Kosten	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
Quelle des Standards																										
Nationale Normungsorg.																										
Europäisch Normungsorg.																										
Internat. Normungsorg.	+	+	+	+		+	+	+	+	+																
Andere nat. Regelwerke					+						+	+	+													

Standards/Vorschriften

Merkmale Unternehmen

Merkmale Standard/Vorschrift

Legende:

- Relevanz hoch
- ⊖ Relevanz partiell
- Relevanz niedrig
- △ kostenlos
- ▲ kostenpflichtig

Kompass der IT-Sicherheitsstandards – Die Matrix (II)

Abbildung 2:
Kompass der IT-Sicherheitsstandards V2.0

Normen zu Kryptographischen und IT-Sicherheitsverfahren													Physische Sicherheit										
Verschlüsselung													Brandschutz										
Digitale Signaturen													Einbruchsbekämpfung										
Haftfunktionen													IS-Integrität										
Authentifizierung																							
PKI-Dienste																							
Schlüsselmanagement																							
Kommunikationsaustw.																							
Zeitsynchronisation																							
TL 7900																							
ISO/IEC 7064	ISO/IEC 9803	ISO/IEC 9016	ISO/IEC 9772	ISO/IEC 9796	ISO/IEC 14888	ISO/IEC 15946	ISO/IEC 10118	ISO/IEC 19031	ISO/IEC 19032	ISO/IEC 9798	ISO/IEC 9797	ISO/IEC 15945	ISO/IEC TR 14595	ISO/IEC 11770	ISO/IEC 13888	ISO/IEC 28014	TL 7900	DIN 4102	DIN 4095	DIN EN 1547	DIN EN 1143-1	DIN V ENV 9527	DIN EN 60929

Standards/Vorschriften

Art des Unternehmens	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Banken/Versicherungen	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Behörden/Verwaltungen	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Beratung	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
HW/SW-Hersteller	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
IT-Dienstleister	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Gesundheitswesen *	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Kanzleien **	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Handwerk und Industrie	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Dienstleister	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Internat. Ausrichtung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Merkmale Unternehmen

Rolle innerhalb des Untern	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Management	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Revisoren	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
IT-Sicherheitsbeauftragter	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
IT-Leitung	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Administratoren	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Projektmanagement	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Entwicklung	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Merkmale Standard/Vorschrift

Merkmale des Standards/de	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
produktorientiert	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
systemorientiert	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
technisch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
organisatorisch																								
strategisch																								
konzepcionell																								
operationell																								
Zertifizierung																								

Umfang (Seiten)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Umfang (Seiten)	19	276	48	30	137	78	193	182	134	24	132	37	66	33	118	41	95	57	14	20	51	39	29	38
Kosten	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲

Quelle des Standards	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
Nationale Normungsorg.																									
Europäisch Normungsorg.																									
Internat. Normungsorg.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
Andere nat. Regelwerke																									

Legende:

- Relevanz hoch
- ⊕ Relevanz partiell
- Relevanz niedrig
- △ kostenlos
- ▲ kostenpflichtig

Behandelte Standards (1) – Grundlegende Standards zum IT-Sicherheits- und Risikomanagement

Informationssicherheits- Management-systeme (ISMS)

- [ISO/IEC 13335](#): Management of information and communications technology security
- [ISO/IEC 27001](#): Information security management systems – Requirements
- [ISO/IEC 17799](#): Code of practice for information security management
- IT-GSHB: IT-Grundschatzhandbuch

SicherheitsmaBnahmen und Monitoring

- [ISO/IEC 18028](#): IT network security
- ISO/IEC 18043: Selection, deployment and operation of intrusion detection systems (IDS)
- ISO/IEC TR 18044: Information security incident management
- ISO/IEC TR 15947: IT intrusion detection systems (IDS)
- ISO/IEC 15816: Security information objects for access control

Behandelte Standards (2) – Standards mit IT-Sicherheitsaspekten und Vorschriften

Standards mit IT-

Sicherheitsaspekten

- Cobit: Control Objectives for Information and Related Technology
- ITIL: IT Infrastructure Library
- IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie

Vorschriften

- KonTraG: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- Basel II
- SOX: Sarbanes-Oxley Act
- BDSG: Bundesdatenschutzgesetz

Behandelte Standards (3) – Evaluierung von Sicherheit

Common Criteria

- ISO/IEC 15408 (CC): Evaluation criteria for IT security (Common Criteria)
- ISO/IEC TR 15443: A framework for IT security assurance
- ISO/IEC 18045: Methodology for IT security evaluation
- ISO/IEC 19790 (FIPS 140-2): Security Requirements for Cryptographic Modules
- ISO/IEC TR 19791: Security assessment for operational systems
- ISO/IEC 19792: Security evaluation of biometrics
- ISO/IEC 21827 (SSE-CMM): System Security Engineering – Capability Maturity Model

Schutzprofile

- ISO/IEC TR 15446: Guide on the production of protection profiles and security targets

Behandelte Standards (4) – Normen zu kryptographischen und IT-Sicherheitsverfahren (Auswahl)

Verschlüsselung

- ISO/IEC 7064: Check character systems
- [ISO/IEC 18033](#): Encryption algorithms
- ISO/IEC 10116: Modes of operation for an n-bit block cipher
- ISO/IEC 19772: Data encapsulation mechanisms

Digitale Signaturen

- ISO/IEC 9796: Digital signature schemes giving message recovery
- ISO/IEC 14888: Digital signatures with appendix
- ISO/IEC 15946: Cryptographic techniques based on elliptic curves

Hashfunktionen und andere Hilfsfunktionen

- ISO/IEC 10118: Hash functions
- ISO/IEC 18031: Random bit generation
- ISO/IEC 18032: Prime number generation

Authentifizierung

- ISO/IEC 9798: Entity authentication
- ISO/IEC 9797: Message Authentication Codes (MACs)

Schlüsselmanagement

- ISO/IEC 11770: Key management

Kommunikationsnachweise

- ISO/IEC 13888: Non-repudiation

Behandelte Standards (5) – Physikalische Sicherheit

- Technische Leitlinie 7500: Produkte für die materielle Sicherheit

Brandschutz

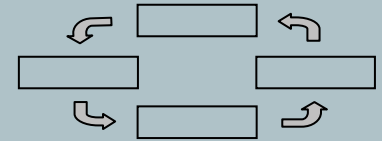
- DIN 4102: Brandverhalten von Baustoffen und Bauteilen
- DIN 18095: Rauchschutztüren
- DIN EN 1047: Wertbehältnisse - Klassifizierung und Methoden zur Prüfung des Widerstandes gegen Brand

Einbruchshemmung

- DIN EN 1143-1: Widerstandsgrad
- DIN V ENV 1627: Fenster, Türen, Abschlüsse - Einbruchhemmung

Gehäuse

DIN EN 60529: Schutzart durch Gehäuse



- “The good thing about (security) standards is ...
... there are so many to choose from”
- BITKOM Kompass der IT-Sicherheitsstandards
 - 1. Ausgabe März 2005
 - 2. Ausgabe Juni 2006 (in Kooperation mit DIN)
 - 3. Ausgabe 2007?
- Ihr Feedback und/oder Ihre Mitarbeit sind willkommen
 - BITKOM AK Sicherheitsmanagement (www.bitkom.org)
 - DIN NI-27 “IT Sicherheitsverfahren” (www.ni.din.de)



■ Kompass der IT-Sicherheitsstandards
Leitfaden und Nachschlagewerk

**Vielen Dank
für Ihr Interesse**

Dr. Walter Fumy
VP Security Technology
Siemens AG, Med GS SEC TE
81730 München

E-Mail: walter.fumy@siemens.com

Anhang



SIEMENS

Defining security standards

- International standards bodies (e.g., ISO, ITU-T, ETSI) have formal processes
 - Procedures and processes take time
 - Progress in streamlining the time for standards approvals
- IETF processes are less formal
 - Number of participants, transparency of the processes have sometimes slowed the work
- Industry groups and consortia focus on specific technologies and applications
 - Focus has allowed work products to be produced rapidly, although limited in scope
 - Maintenance?
- Experience has shown there is a role for each organization to play in continued security standards development



ISO/IEC JTC 1/SC 27 “IT Security Techniques” Scope & Organization



Standardization of generic IT security services and techniques, including

- identification of generic requirements for IT system security services,
- development of security techniques and mechanisms (cryptographic and non-cryptographic),
- development of security guidelines,
- development of management support documentation and standards,
- development of criteria for IT security evaluation and certification of IT systems, components, and products.

**ISO/IEC JTC 1/SC 27: Information technology -
Security techniques**

Chair: Mr. W. Fumy

Vice-Chair: Ms. M. De Soete

**SC 27 Secretariat
DIN**

Ms. K. Passia

**Working Group 1
Information security
management
systems**
*Convener
Mr. T. Humphreys*

**Working Group 2
Cryptography and
security
mechanisms**
*Convener
Mr. K. Naemura*

**Working Group 3
Security evaluation
criteria**
*Convener
Mr. M. Ohlin*

**Working Group 4
Security controls
and services**
*Convener
Mr. M.-C. Kang*

**Working Group 5
Identity management
and privacy
technologies**
*Convener
NN*

ISO/IEC 17799 – Highlights of 2005 Version

SC27

Enhanced structure and controls

- 11 Control areas (1 new) with
- 134 Controls (17 new)

Improved user friendliness

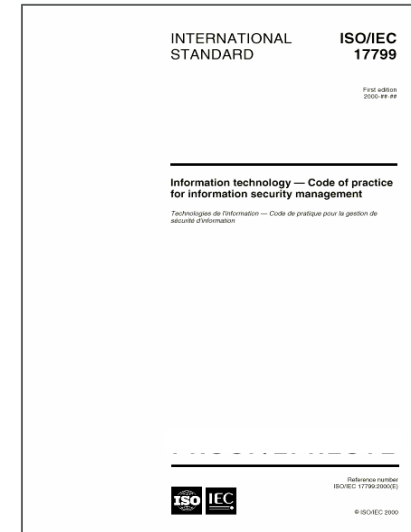
- E.g. new control text structure

New issues addressed include

- Security of external service delivery and provisioning of outsourcing
- Patch management
- Security prior to, during, and at termination of employment
- Greater focus on handling risks and incidents
- Mobile, remote, and distributed communications and information processing

However, still a Code of Practice (“should”)

- Selection of controls & their implementation up to user

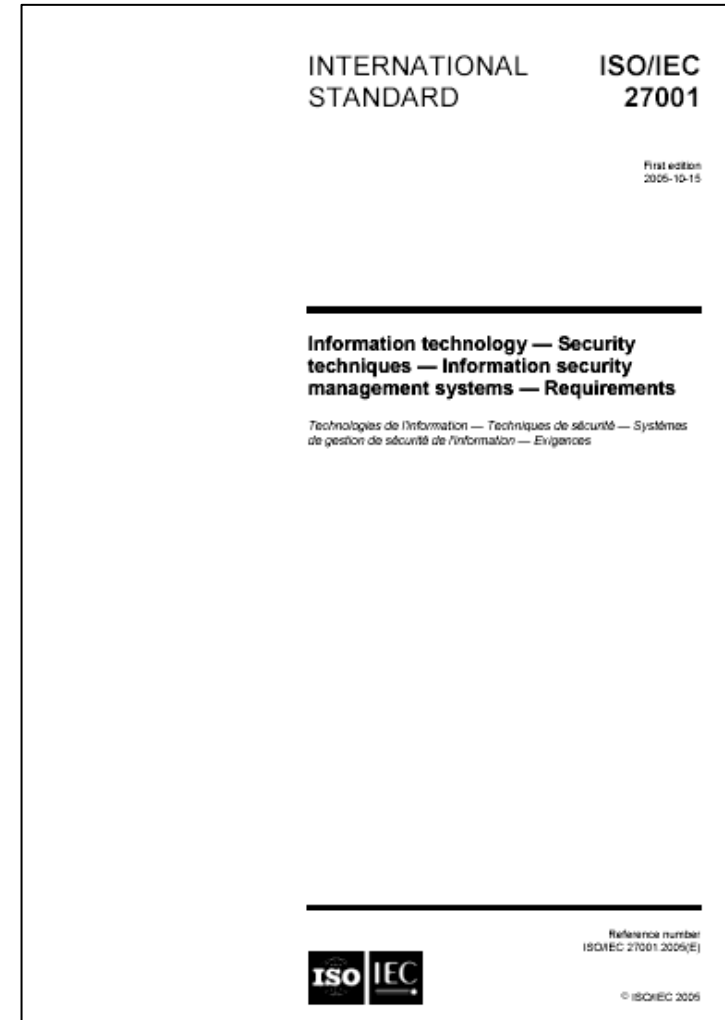


ISO/IEC 27001

ISMS Requirements

- ISO/IEC 27001 is a certification and auditable standard
- Based on a mandatory risk based approach
- Aims at achieving effective information security through continual improvement process (PDCA model)
- Uses the same management systems process model as ISO 9001 (QMS) and ISO 14001 (EMS)

- ISO/IEC 27001 is a revised version of BS 7799 Part 2:2002
- Publication date 2005-10-15
- BS 7799 Part 2:2002 has now been withdrawn





ISO Standards Supporting ISO/IEC 27001

