verinixe.XP, 2015-09-16 Berlin

IT Sicherheitsnormen der ISO/IEC 27000er Normenfamilie

IT Sicherheitsnormen der ISO/IEC 27000er Normenfamilie

- Woher stammen Normen
- Was macht DIN
- Wie wirken Normen
- Wie entstehen Normen

DIN e. V.

DIN ist ein eingetragener gemeinnütziger Verein und wird privatwirtschaftlich getragen.

DIN ist laut eines Vertrages mit der Bundesrepublik Deutschland die zuständige deutsche Normungsorganisation für die europäischen und internationalen Normungsaktivitäten.

DIN ist ein Dienstleistungsunternehmen

- DIN fungiert als „runder Tisch“ –auch über elektronische Plattformen – an dem Vertreter der interessierten Kreise konsensbasierte Normen markt- und zeitgerecht erarbeiten.
- Die DIN-Mitarbeiter organisieren den gesamten Prozess der Normung auf nationaler Ebene und die deutsche Beteiligung auf europäischer und internationaler Ebene.
- DIN stellt die Einheitlichkeit der technischen Regeln sicher.
- DIN stellt die elektronische Infrastruktur für die Normen-entwicklung zur Verfügung

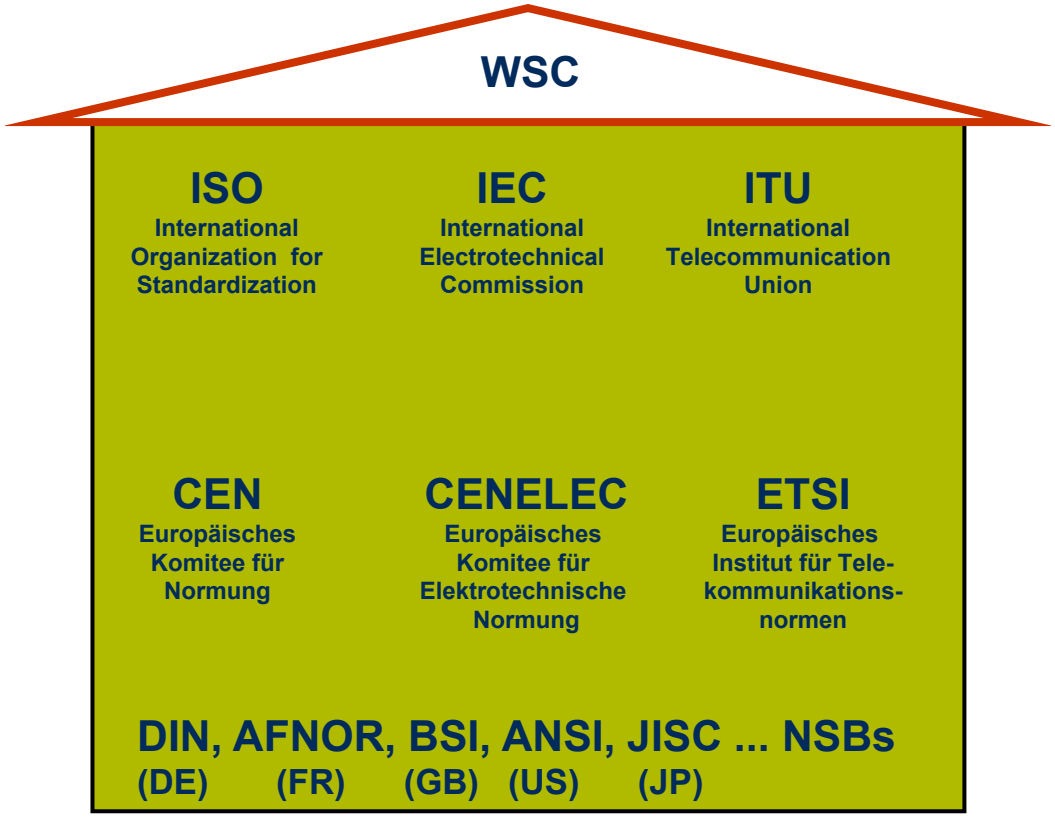
Die Leistungen des DIN e.V.

DIN

- handelt als Projektmanager in der Normung
- handelt als Dienstleister für seine Kunden
- führt die Sekretariate in internationalen Arbeitsgremien
- stellt die Einheitlichkeit der technischen Regeln sicher
- stellt die elektronische Infrastruktur für die Normenentwicklung zur Verfügung

DIN ist Teil der Internationalen Normungsstruktur

World Standards Cooperation



USA

270 SDOs von ANSI akkreditiert

- ASTM
- API
- NEMA
- SAE
- ASME
- IEEE

Normen in der Rechtsordnung

- Eine anerkannte Regel der Technik ist eine technische Festlegung, die von einer Mehrheit repräsentativer Fachleute als Wiedergabe des Standes der Technik angesehen wird.
- Der Stand der Technik ist ein entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind basierend auf den diesbezüglichen gesicherten Erkenntnisse von Wissenschaft, Technik und Erfahrung.

Normen in der Rechtsordnung

- Die Anwendung von Normen ist freiwillig
- Bindend werden Normen nur dann, wenn sie Gegenstand von Verträgen zwischen Parteien sind oder wenn der Gesetzgeber ihre Einhaltung vorschreibt
- Normen sind eindeutige (anerkannte) Regeln, daher bietet der Bezug auf Normen in Verträgen Rechtssicherheit
- Im Rechtsstreit billigt ein Richter der DIN-Norm den "Beweis des ersten Anscheins" zu.
  Eine widerlegbare Rechtsvermutung (Beweislastumkehr)

Normen wirken deregulierend

DIN-Normen entlasten den Staat in seiner Gesetzgebungstätigkeit. Der Staat verweist zur Erfüllung grundlegender Anforderungen in Gesetzestexten auf überbetriebliche Normen

- Gesetze schaffen den rechtlichen Rahmen und geben Schutzziele vor
- Normen konkretisieren den Stand der Technik und schreiben ihn flexibel fort

Beispiel: Bauwesen, Gesundheitsschutz, Umweltschutz

Was kann Normung leisten

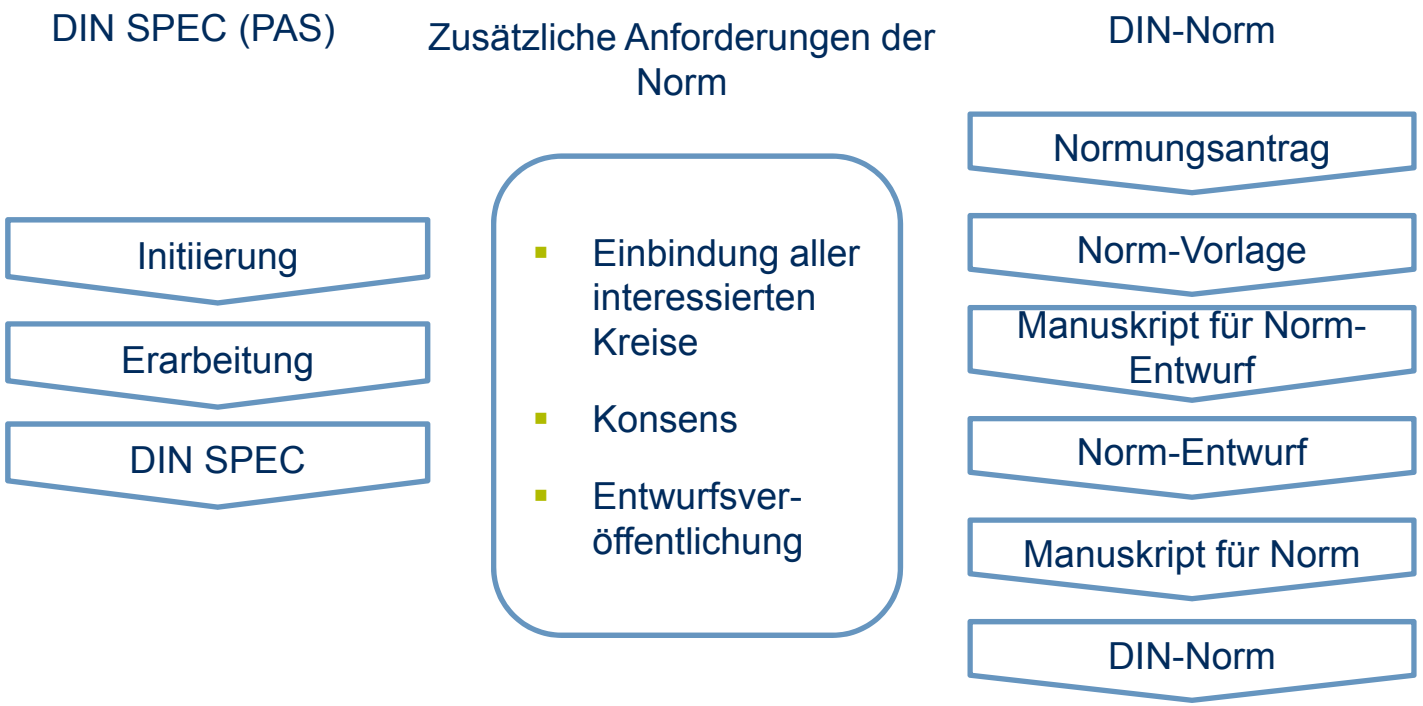
- Interoperabilität → Schnittstellennorm
- Komplexitätsreduktion → Bildung von Klassen
- Mindeststandards → Erfüllung gesetzl. Vorgaben
- Best Practice → Festhalten des „Stand der Technik“
- Transparenz → Label
- Qualitätssicherung → Norm als Referenz
- Zertifizierungsgrundlage → Bsp.: ISO 9001

Wie entstehen Normen

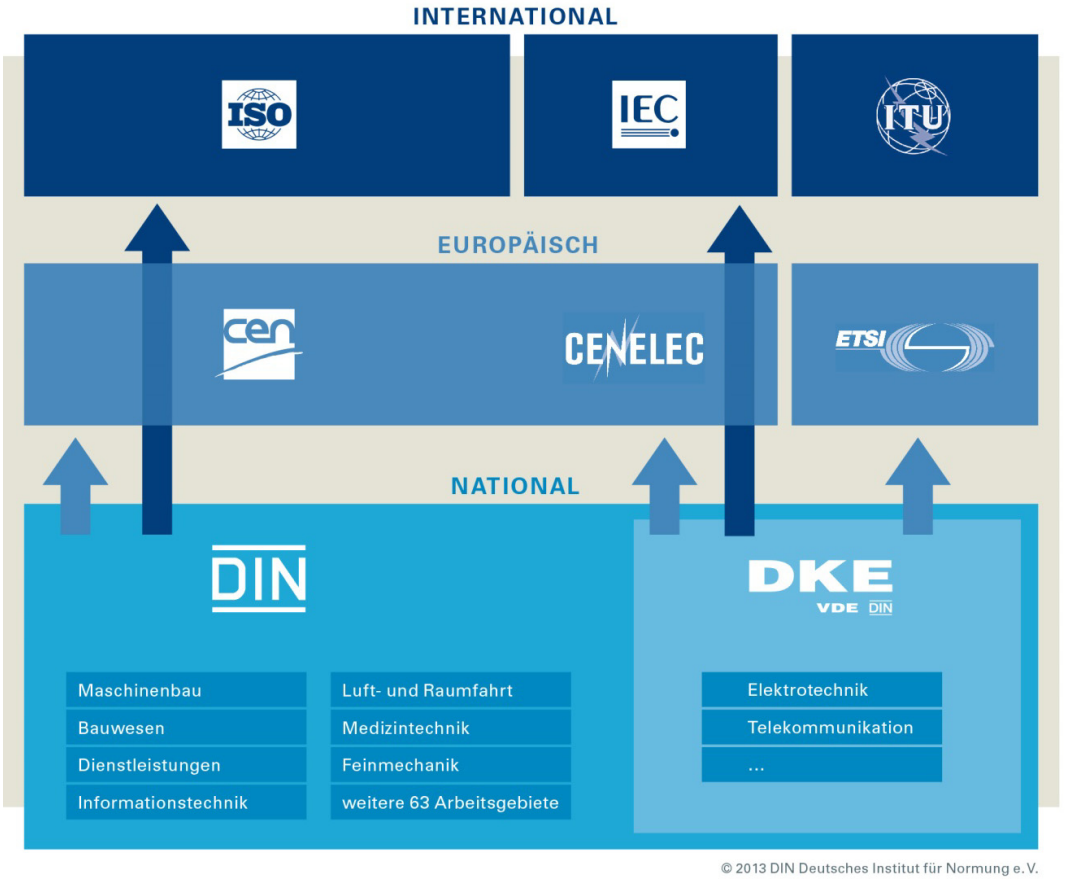
Gemeinschaftsaufgabe Normung

Eine demokratische Legitimation der Normung erfordert das Engagement aller interessierten Kreise.

Normerstellung: Zusätzliche Anforderungen



Nationale Interessensvertretung



ISO: Internationale Organisation für Normung

IEC: Internationale Elektro-technische Kommission

ITU: Internationale Fernmeldeunion

CEN: Europäisches Komitee für Normung

CENELEC: Europäisches Komitee für Elektrotechnische Normung

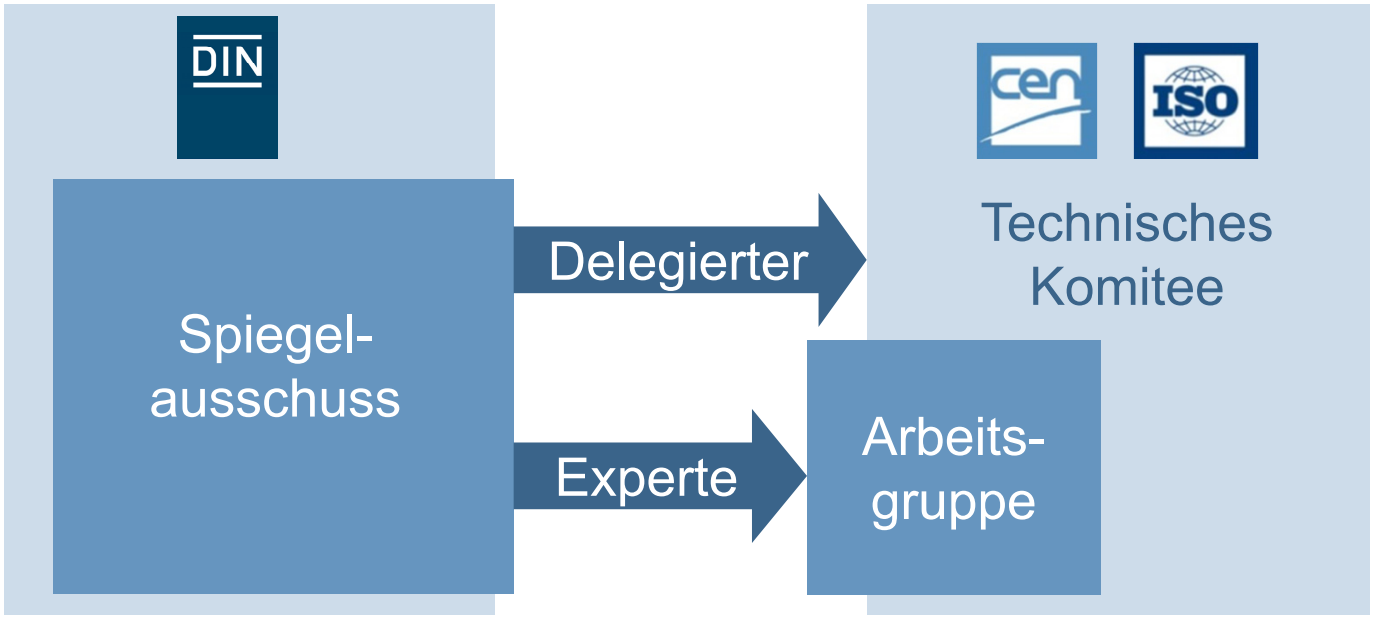
ETSI: Europäisches Institut für Telekommunikationsnormen

DIN: Deutsches Institut für Normung e. V.

DKE: Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

DIN und DKE vertreten die nationalen Interessen in der europäischen und internationalen Normung.

Mitarbeit in europäischen und internationalen Normungsgremien



Internationale Normungsorganisationen

ISO/IEC

- Je Land ist ein Mitglied (meist die nationalen Normungs-organisationen) in der jeweiligen Normungsorganisation vertreten
- Die Organe – wie Generalversammlung, politische und technische Lenkungsgremien, sowie die Technischen Komitees – stehen den Mitgliedern offen
- Es gibt in den Technischen Komitees Vollmitglieder (***P-members***) und Beobachtermitglieder (***O-members***)

Entstehung einer Internationalen Norm

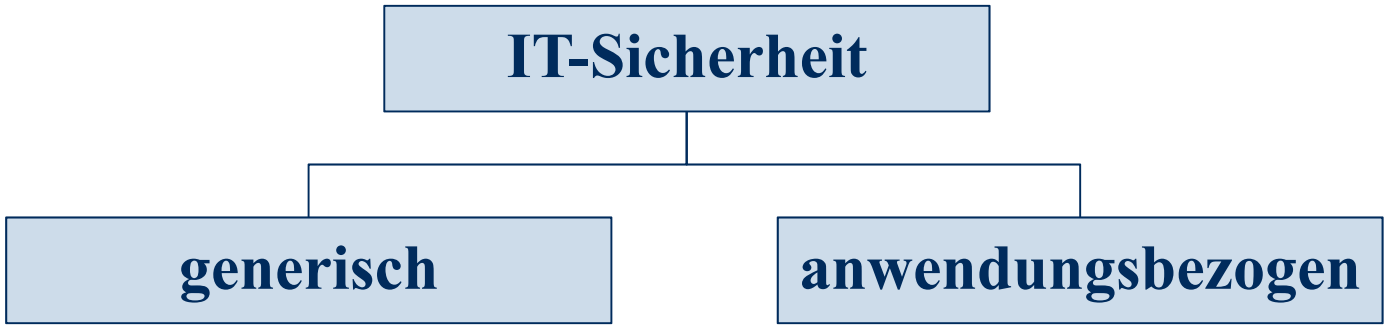
Vorschlagsstufe (Proposal Stage)	Vom Vorschlag (**NP**) bis zur Annahme eines neuen Normungsvorhabens
Bearbeitungsstufe (Preparatory Stage)	Von der Annahme des Normungsvorhabens bis zur Verabschiedung zur Registrierung als Komitee-Entwurf
Komiteestufe (Committee Stage)	Vom Komitee-Entwurf (**CD**, mehrere möglich) bis zur Verabschiedung zur Umfrage (Internationaler Norm-Entwurf)
Fast track → **Umfragestufe** (Enquiry Stage)	Von der Annahme zur Umfrage (Internationaler Norm-Entwurf (**DIS** bzw. **CDV**)) bis zur Verabschiedung zum Schlussentwurf
Fast track → **Annahmestufe** (Approval Stage)	Von der Annahme als Schlussentwurf (**FDIS**) bis zur Verabschiedung zur Internationalen Norm
Veröffentlichungs-stufe (Publication Stage)	Von der Annahme als Internationale Norm bis zur Veröffentlichung als ISO-, IEC- oder ISO/IEC-Norm

Internationale Normung – Veröffentlichungsformen (ISO)

- ISO Internationale Norm
- ISO/TS Internationale Technische Spezifikation
- ISO/TR Internationaler Technischer Bericht
- PAS Publicly Available Specification
- IWA International Workshop Agreement
- Guide Leitfaden

Normung im Bereich IT-Sicherheit

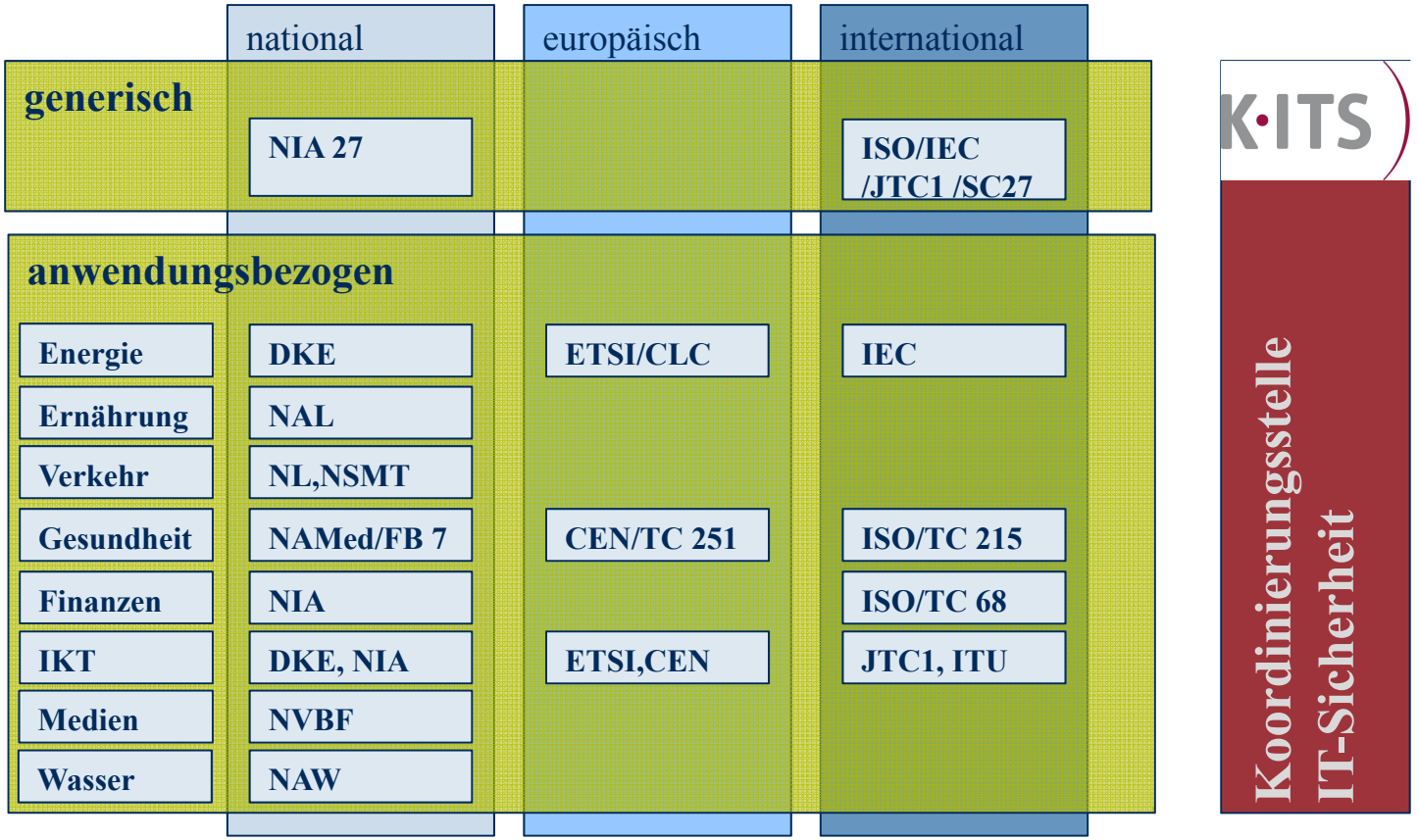
Normung von IT-Sicherheit



Unabhängig von
- Technologie
- Branche
- Anwendungsfall

Abhängig von
- Technologie (z.B. RFID)
- Branche (z.B. Medizin)
- Anwendungsfall (Bahnsignalanlagen)

IT-Sicherheitsnormung - Gremienübersicht

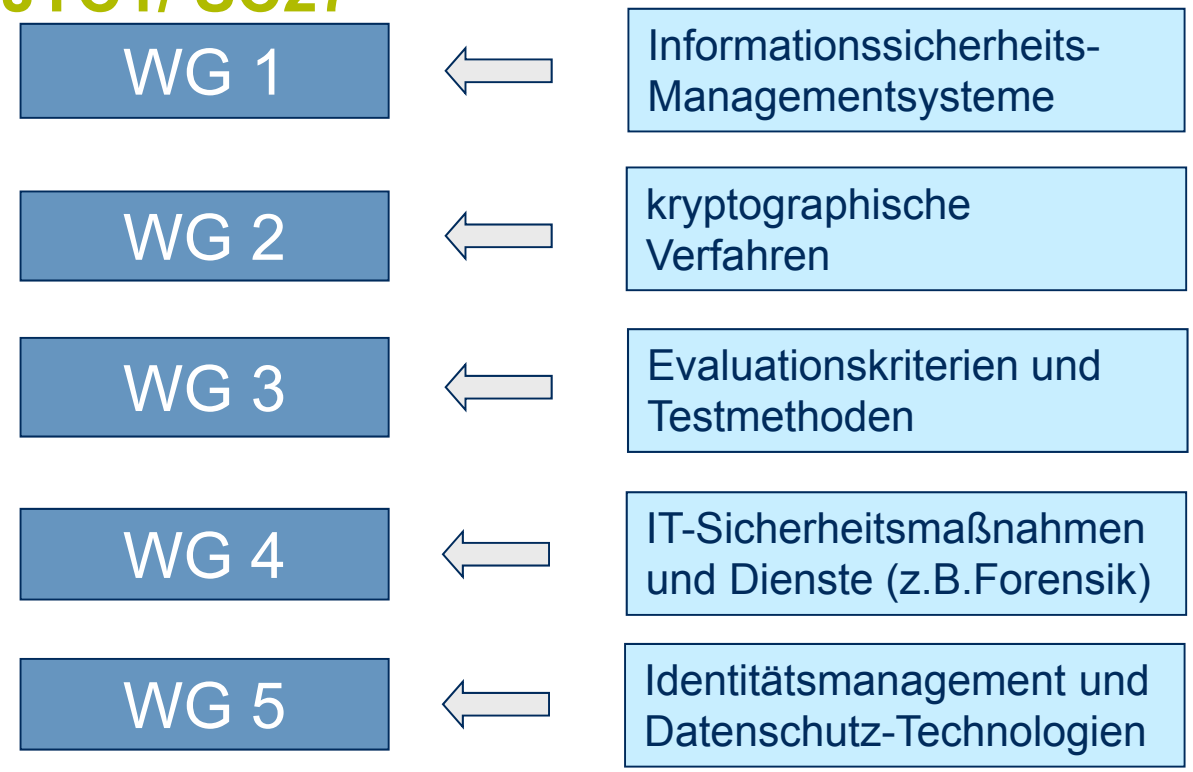


K·ITS

Koordinierungsstelle IT-Sicherheit

DIN

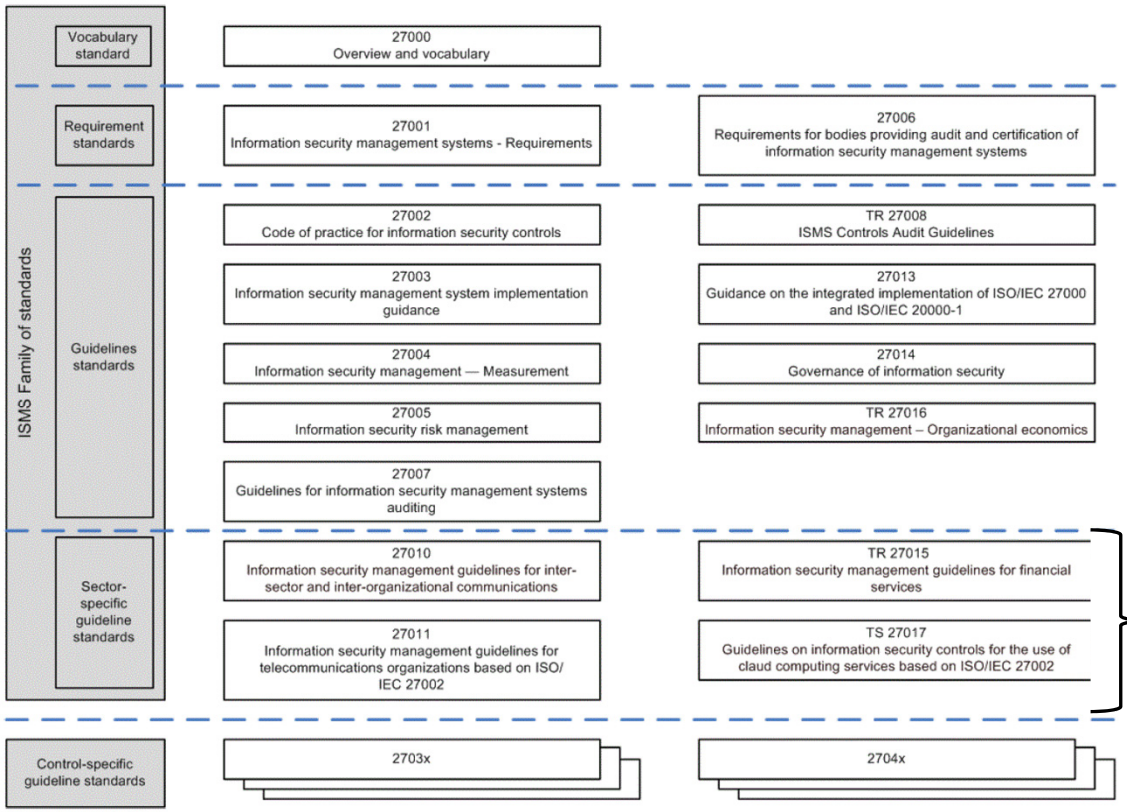
Generische IT-Sicherheitsnormung im JTC1/ SC27



www.jtc1sc27.din.de/en

ISO/IEC 270xx Normen

ISO/IEC 27000 - Normenfamilie



Erstellung nach ISO/IEC 27009

Übersicht ISO/IEC 270xx

- ISO/IEC 27000 (DIS) Overview and vocabulary
- ISO/IEC 27001 (Ausgabe 2013) Requirements
- ISO/IEC 27002 (Ausgabe 2013) Code of practice for information security controls
- ISO/IEC 27003 (CD) Information Security Management System – Guidance
- ISO/IEC 27004 (CD) Information security management -- Measurement
- ISO/IEC 27005 (WD) Information security risk management
- ISO/IEC 27006 (FDIS) Requirements for bodies providing audit and certification of ISMS
- ISO/IEC 27007 (WD) Guidelines for information security management systems auditing
- ISO/IEC 27008 (WD) Guidelines for auditors on information security controls
- ISO/IEC 27009 (DIS) Sector-specific application of ISO/IEC 27001 -- Requirements

Übersicht ISO/IEC 270xx (2)

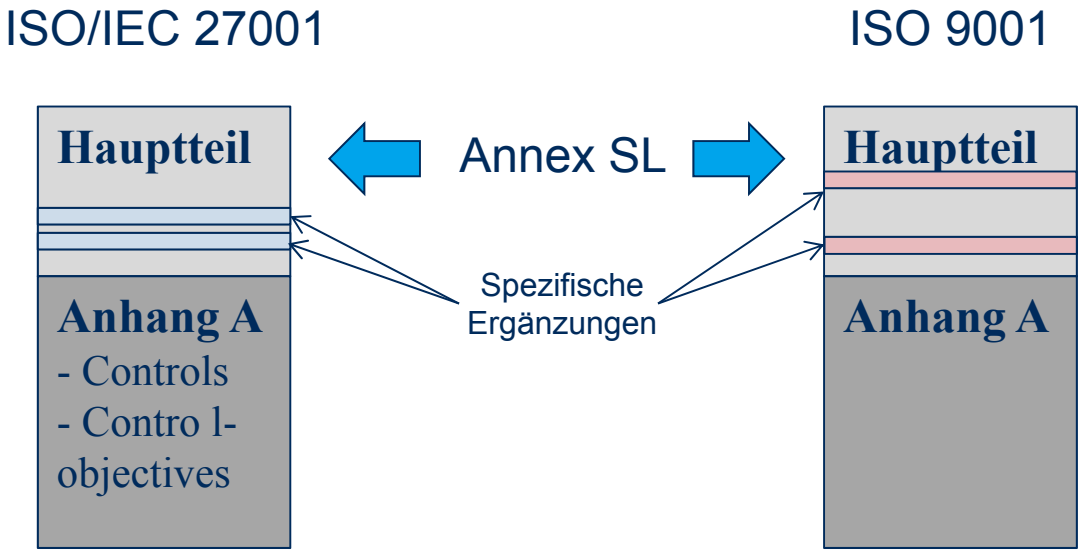
- ISO/IEC 27010 (DIS) ISM for inter-sector and inter-organizational communications
- ISO/IEC 27011 (DIS) Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
- ISO/IEC 27013 (Ausgabe 2013) Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27015 (Ausgabe 2012) Information security management guidelines for financial services
- ISO/IEC 27017 (Ausgabe 2013) Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC TR 27019

ISO/IEC 27001/27002 - Historie

- British Standard BS7799:1995 → ISO/IEC 17799:2005
- ISO/IEC 17799:2005 → ISO/IEC 27002:2005
- BS7799-2:2002 → ISO/IEC 27001:2005
- ISO/IEC 27001:2005 → ISO/IEC 27001:2013
- ISO/IEC 27002:2005 → ISO/IEC 27002:2013

ISO Managementsystem-Normen

Gemeinsame Struktur aller ISO Management System-Normen durch vorgegebenen Annex SL der ISO Direktiven



Systematik der ISO/IEC 27001/27002

ISO/IEC 27001 - Anforderungen	ISO/IEC 27002 - Umsetzungshilfe
6.1.1 *Maßnahme* Angemessene Kontakte mit relevanten Behörden werden gepflegt.	6.1.1 *Umsetzungshinweise* Organisationen sollten über Verfahren verfügen, die festlegen, wann und von wem Behörden (z. B. Strafverfolgungs- und Aufsichtsbehörden) benachrichtigt werden und wie erkannte Informationssicherheitsvorfälle rechtzeitig gemeldet werden (z. B. wenn der Verdacht einer Straftat besteht).

Zertifizierbarkeit von IT Sicherheitsmanagement-Systemen

- Nach ISO/IEC 27001
  - Anforderungen an ein Managementsystem zur Verankerung der IT-Sicherheit in der Organisation
- Nach BSI Grundschutz
  - BSI-Grundschutz ist abgestimmt mit ISO/IEC 27001
  - Zertifikat: ISO/IEC 27001 auf Basis IT-Grundschutz

Wie ist eine Norm zu lesen

DIN 820-2 *(identisch mit ISO/IEC Direktiven Teil2),*

Anhang H: Verbformen zur Formulierung von Festlegungen

- Anforderung
  - *muss*
  - *darf nicht*
- Empfehlung
  - *sollte*
  - *sollte nicht*

- *Zulässigkeit*
  - *darf*
  - *braucht nicht*
- *Möglichkeit und Vermögen*
  - *kann*
  - *kann nicht*

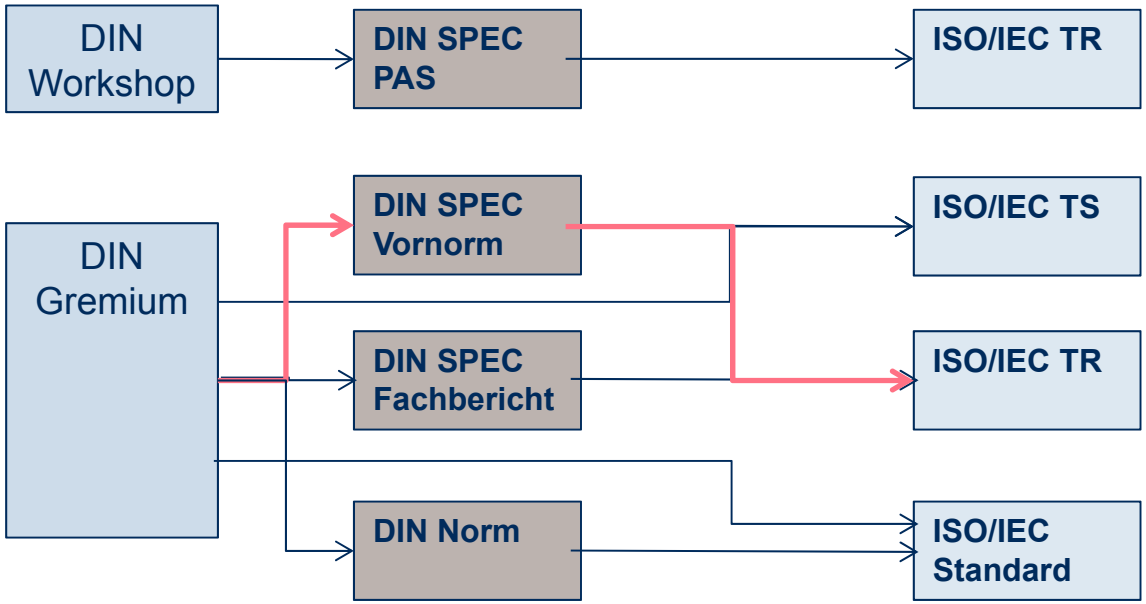
Anforderungen in Normen sind Zertifizierungsgrundlage !

Internationalisierung nationaler Normen

Internationalisierung – warum?

- IKT ist ein globaler Markt
- International Felder belegen
- Internationale Entwicklungen beeinflussen
- Deutschland als Referenzmarkt
- Skaleneffekte nutzen
- Reputation internationaler SDO‘s nutzen

Möglichkeiten der Internationalisierung



DIN SPEC 27009 → ISO/IEC TR 27019

www.din.de
www.din.de/go/nia
www.entwuerfe.din.de

www.din.de/go/kits

DIN e. V.
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin