Kompass der IT-Sicherheitsstandards

Auszüge als Sonderdruck zur it-sa 2013

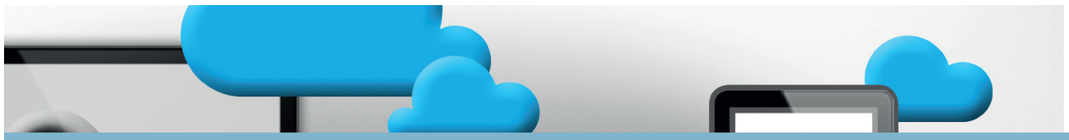
BITKOM

DIN

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org	DIN Deutsches Institut der Normung e.V. Normenausschuss Informationstechnik und Anwendungen (NIA) Burggrafenstraße 6 10787 Berlin Tel.: 030.2601-0 Fax: 030.2601-1231 nia@din.de www.nia.din.de
Ansprechpartner:	Marc Fliehe Tel.: 030.27576-242 m.fliehe@bitkom.org	Volker Jacumeit Tel.: 030.2601-2186 volker.jacumeit@din.de
Redaktion:	Dr. Walter Fumy (Bundesdruckerei GmbH) Lutz Neugebauer (TÜV TRUST IT GmbH) Marc Fliehe (BITKOM)	Volker Jacumeit (DIN e.V.) Martin Uhlherr (DIN e.V.)
Verantwortliches Gremium:	AK Sicherheitsmanagement	Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN, Arbeitsausschuss NIA-27, IT-Sicherheitsverfahren
Redaktionsassistenz:	Miriam Taenzer (BITKOM)	
Gestaltung/Layout:	Design Bureau kokliko / Astrid Scheibe (BITKOM)	
Copyright:	BITKOM 2013	
Stand:	Stand: September 2013, Sonderdruck zur it-sa 2013	

Die Inhalte dieses Leitfadens sind sorgfältig recherchiert. Sie wurden unter aktiver Mitwirkung der Mitglieder der o. g. BITKOM und DIN-Gremien erarbeitet. Sie spiegeln die Auffassung im BITKOM und DIN bzw. den Arbeitsstand in den Normungsgremien zum Zeitpunkt der Veröffentlichung wider. Die vorliegende Publikation erhebt jedoch keinen Anspruch auf Vollständigkeit. Wir übernehmen trotz größtmöglicher Sorgfalt keine Haftung für den Inhalt.
Der jeweils aktuelle Leitfaden kann unter www.bitkom.org/publikationen bzw. unter www.nia.din.de kostenlos bezogen werden. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim BITKOM und DIN.



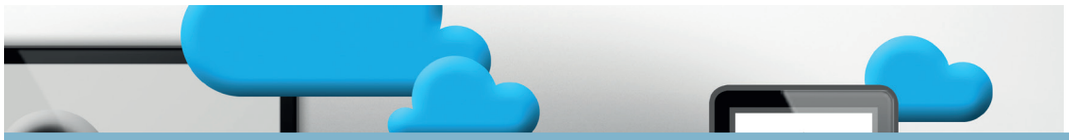
Kompass der IT-Sicherheitsstandards

Auszüge als Sonderdruck zur it-sa 2013

BITKOM

DIN

Inhaltsverzeichnis



1 Einleitung

Die Innovationskraft der ITK-Branche mit neuen Produkten und Dienstleistungen für ihre Unternehmenskunden ist weiterhin ungebremst. Informations- und Kommunikationstechnologie nimmt dabei zunehmend die Rolle des »Enablers« ein, die praktisch in jedem technologiebasierten Prozess wiederzufinden ist. Die Technik als solche tritt dabei immer mehr in den Hintergrund, für den Anwender ist der Nutzen von weit höherer Bedeutung.

Die folgenden Entwicklungen prägen heute und vermutlich zukünftig den Einsatz von IT in Unternehmen:

- Mobile Endgeräte, insbesondere Smartphones und Tablet-Computer, haben ihren Siegeszug fortgesetzt. Im Jahr 2012 wurden erstmalig mehr als 21 Mio. Smartphones allein in Deutschland verkauft.

- Begriffe wie »Bring your own device« oder »Consumerization« zeigen, dass die Grenzen zwischen privatem und beruflichen durch die Nutzung von moderner Informations- und Kommunikationstechnik immer weiter verwischen.

- Der Arbeitsplatz wird mobil und ist nicht mehr klassisch an das Büro im Gebäude des Arbeitgebers gebunden. Bestenfalls schafft diese Entwicklung – sowohl für Unternehmen, aber auch die Mitarbeiter – höhere Freiheitsgrade durch eine steigende Flexibilität oder beispielsweise die Einsparung von Reisezeiten und -kosten, die bei den Millionen Berufspendlern tagtäglich entstehen.

- Zunehmender Netzausbau und Vernetzung von Systemen, Virtualisierung, Cloud Computing und Big Data sind die korrespondierenden Entwicklungen auf der Infrastrukturseite, ohne die viele Aspekte der Nutzung mobiler Endgeräte im beruflichen wie privaten Kontext gar nicht möglich wären.

- Ein weiterer Aspekt dieser Entwicklung ist der Ausbau smarter Infrastrukturen. Die angestrebte Energiewende, intelligente Verkehrsnetze oder Industrie 4.0 werden erst durch den Einsatz moderner IKT-Lösungen möglich.

Hier zeigt sich aber auch die Kehrseite der Medaille. Eine zunehmende Durchdringung in ganz unterschiedlichen Anwendungsbereichen fordert die ständige Verfügbarkeit der Systeme und der dort verarbeiteten Informationen. Die insgesamt gestiegene Nutzung bedeutet gleichzeitig auch eine quantitative Zunahme an wichtigen, häufig sehr sensiblen Informationen von einzelnen Nutzern oder von kompletten Unternehmen. Informationen in IT-Systemen stellen Werte da, die es zu schützen gilt. Dass dies nicht nur blanke Theorie ist, zeigt die große Anzahl der spektakulären Fälle von Datendiebstählen und Identitätsmissbrauch durch Cyberkriminelle, die wir in den vergangenen Jahren erleben mussten. Die polizeiliche Kriminalstatistik berichtet für das Jahr 2012 im Vergleich zu 2011 einen Anstieg im Bereich der IuK-Kriminalität um rund 7,5 Prozent. Dazu gehört der bemerkenswerte Anstieg um 134 Prozent im Bereich von Datenveränderung und Computersabotage.

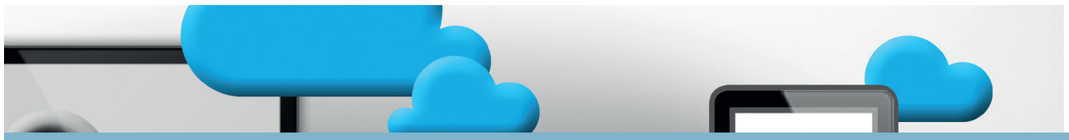
Da eine 100 prozentige Sicherheit nicht erreichbar ist, gilt es, die mit dem Einsatz von IT verbundenen Risiken auf ein Niveau zu bringen, das aus unternehmerischer Sicht vertretbar ist und dauerhaft gehalten werden kann. Um dieses Ziel zu erreichen, ist die Einführung eines IT-Risikomanagements für praktisch jedes Unternehmen notwendig. Standards spielen im Rahmen des IT-Risikomanagements eine wichtige Rolle. Der Einsatz von IT-Sicherheitsstandards im Unternehmen oder in einzelnen Bereichen macht die sicherheitsrelevanten IT-Prozesse des Unternehmens transparent und damit beherrschbar und reduziert somit das Gesamtrisiko. Großunternehmen haben dies schon lange erkannt und setzen Standards in wachsendem Maße ein. Aber auch mittelständische Unternehmen profitieren von der Anwendung geeigneter IT-Sicherheitsstandards.

Der Leitfaden nähert sich dem Thema aus der Nutzerperspektive: Unterschiedliche Rollen im Unternehmen benötigen unterschiedliche Rahmenwerke, damit sie erfolgreich in der täglichen Arbeit agieren können.

Dieser Leitfaden klassifiziert einschlägige Standards, so dass der Leser diese für seine Rolle im Unternehmen bewerten und gegebenenfalls als relevant einschätzen kann. Im Kompass sind auch ausgewählte Vorschriften und Gesetze aufgeführt, die im Zusammenhang mit IT-Sicherheit in Medien und Publikationen immer wieder erwähnt werden. Auch diese sind klassifiziert und können so auf ihre Relevanz überprüft werden. Nicht jeder Standard ist für jeden Nutzer und jedes Unternehmen sinnvoll. Nähere Erläuterungen und Informationen zu den aufgeführten Standards und Vorschriften sind in den darauf folgenden Kapiteln zu finden. Im Anhang sind die Bezüge der behandelten Standards untereinander aufgeführt, dort befinden sich auch Links zu weiteren Informationen.

Noch eine Anmerkung in eigener Sache:

Da BITKOM und DIN den Leitfaden permanent weiterentwickeln, möchte wir Sie zur aktiven Beteiligung ermutigen. Teilen Sie uns Ihre Ideen, Wünsche und Beträge mit! Das Kontaktformular auf der Webseite bietet Ihnen eine komfortable Möglichkeit, auf diese Weise zur Qualität, Quantität und Aktualität des »Kompass IT-Sicherheitsstandards« beizutragen.



2 Nutzer und Nutzen von Standards

So wie der Einsatz von Informations- und Kommunikationstechnologien in Unternehmen in der Regel kein Selbstzweck ist, so sollte auch die Verwendung von Sicherheitsstandards immer mit einem – bestenfalls quantifizierbaren – Nutzen verbunden sein. Beispielsweise ist die Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS) – je nach Wahl des Geltungsbereiches – durchaus mit einem spürbaren personellen und finanziellen Aufwand verbunden. Das gilt sowohl für den Zertifizierungsprozess als auch im nachfolgenden Betrieb des Managementsystems und den notwendigen Audits zur Aufrechterhaltung des Zertifikats. Unbestritten sind aber auch die Vorteile, die eine stringente und für das Unternehmen angemessene Einführung und Betrieb eines Managementsystems für die Informationssicherheit mit sich bringt.

In der Innenwirkung kann die Verwendung von etablierten Standards dabei unterstützen, die sicherheitsrelevanten IT-Prozesse zum Vorteil des Unternehmens, der Kunden, der eigenen Produkte sowie der Mitarbeiter zu verbessern. Sie bieten Hilfestellung bei der Entwicklung von generischen Maßnahmen auf Management-Ebene bis zu detaillierten technischen Implementierungen an. Sie liefern Methoden für ein leistungsfähiges IT-Sicherheitsmanagement oder definieren die IT-Sicherheit von ausgewiesenen Produkten. Sie können sowohl eigenständig als auch methodisch eingebettet in ein anderes System fortlaufend betrieben werden.

Ein ISMS ist sinnvollerweise Teil eines unternehmensweiten Risikomanagements, durch das insbesondere auch die IT-Risiken auf ein für das Unternehmen angemessenes Niveau reduziert werden können. Dabei kommt es insbesondere darauf an, die Risiken umfassend zu ermitteln und die Schutzmechanismen aus wirtschaftlichen Gründen nicht aufwendiger zu gestalten, als es das zulässige Risiko verlangt. Die Auswahl und die Anwendung angemessener IT-Sicherheitsstandards ist ein Teil des IT-Sicherheitsmanagements.

In der Außenwirkung entwickeln die Verwendung und insbesondere der Nachweis der Verwendung von IT-Sicherheitsstandards (also eine entsprechende Zertifizierung) eine immer größere Bedeutung – dies gilt insbesondere für Standards im Bereich Management und Prozesse:

- Zunehmend wird in Ausschreibungen von Unternehmen oder Behörden eine Zertifizierung gefordert, um die Gefahr zu minimieren, mit einem Partner mit hohen IT-Sicherheitsrisiken zusammenarbeiten zu müssen.

- Der Nachweis eines etablierten IT-Sicherheitsmanagements kann die Bereitstellung von Kapital bei Banken erleichtern oder die Prämie einer Cyber-Versicherung günstig beeinflussen, die von immer mehr Versicherungsunternehmen angeboten wird.

- Für Unternehmen aus dem Bereich Kritischer Infrastrukturen (KRITS) wird spätestens mit der bereits heute absehbaren Verabschiedung eines »IT-Sicherheitsgesetzes« in der 18. Legislaturperiode in Deutschland die nachweisliche Nutzung von sektorspezifischen IT-Sicherheitsstandards verpflichtend. Im aktuellen Gesetzentwurf ist unter anderem die Forderung verankert, branchespezifische Standards zu entwickeln und eine Prüfung in regelmäßigen Abständen durchzuführen. Es ist weiterhin absehbar, dass hiervon nicht nur die Unternehmen der KRITIS-Branchen, sondern auch Partner und Zulieferer betroffen sein werden.

Die Vielzahl und Vielfalt der heutigen Sicherheitsstandards hat sich aus den unterschiedlichen Bedürfnissen von Unternehmen (z. B. verschiedene Branchen) aber auch aus den Rollen und Verantwortlichkeiten von Personen im Unternehmen entwickelt.

Zieht man die tiefe Durchdringung fast aller Unternehmensprozesse mit IT in Betracht, ist die große Anzahl unterschiedlicher Rollen und Funktionen, die sich mit

IT-Sicherheit auseinandersetzen müssen nicht verwunderlich. Insbesondere ist bereits heute klar, dass sich nicht mehr nur die IT-Abteilung mit dem Thema IT-Sicherheit auseinandersetzen muss, sondern praktisch jede Unternehmensfunktion, die mit personenbezogenen oder sonstigen sensiblen Daten umgeht, bzw. mit der technischen und organisatorischen Bereitstellung von Infrastrukturen und Diensten zur Unterstützung der IT befasst ist.

Im Rahmen dieses Leitfadens soll nach drei wesentlichen Blöcken unterschieden werden.

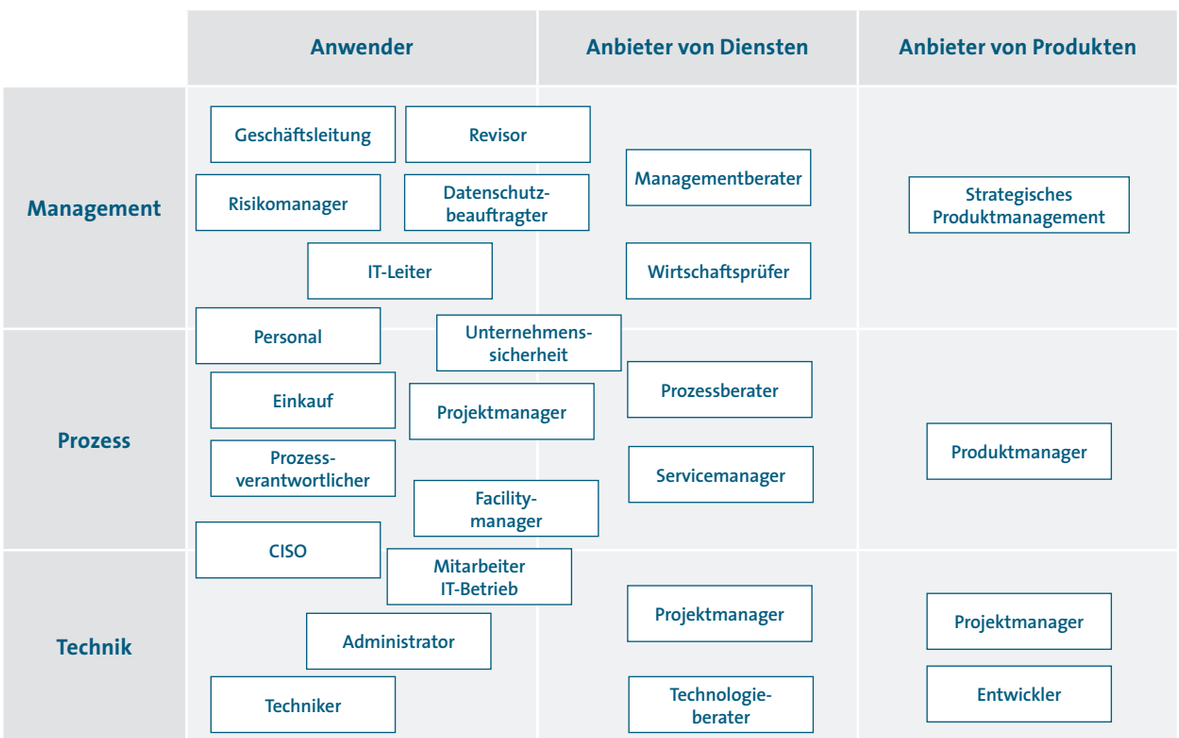
- **Management**
  Aus der Perspektive der Anwender gehören hierzu unter anderem die Rollen Geschäftsleitung, Revision, Risikomanagement, Leiter Unternehmens-IT oder Leiter Unternehmenssicherheit

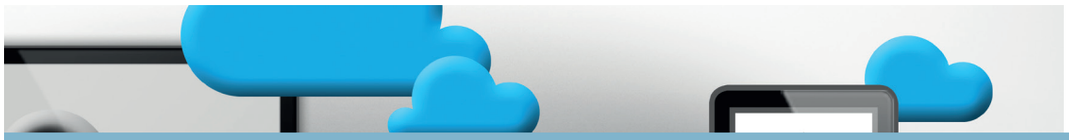
- **Prozesse**
  Hierunter können die Geschäftsprozessverantwortlichen, zentrale Unternehmensfunktionen (z. B. Einkauf, Facility Management, usw.) gezählt werden.

- **Technik**
  Hierzu gehört der IT-Betrieb, insbesondere Administratoren, Techniker.

Das folgende Bild zeigt die Zuordnung der Rollen aus der Perspektive der Anwender, ergänzt um die Sicht auf die Anbieter von Diensten und von Produkten im IT-Umfeld. Auch für die beiden letztgenannten ist eine ganze Reihe von Sicherheitsstandards maßgeblich, da die Anbieter neben den für sie selbst geltenden auch die für Kunden relevanten IT-Sicherheitsstandards als Anforderungen an Dienste und Produkte beachten müssen.

Bei den dargestellten Rollen kann keine scharfe Trennung zwischen den Blöcken Management, Prozesse und Technik vorgenommen werden. Vielfach finden sich daher Rollen wieder, die für zwei oder drei der genannten Blöcke gelten.





3 Arten von Standards und ihre Einsatzgebiete

3.1 Entwicklung von Normen und Standards

Weltweit gibt es zahlreiche Gremien, die sich mit der Entwicklung von Sicherheitsstandards bzw. Normen beschäftigen.

Die in diesem Leitfaden aufgeführten und beschriebenen Standards wurden von verschiedenen Gremien nach unterschiedlichen Verfahren entwickelt. In der Regel kann man das verantwortliche Gremium an der Zeichenkette zu Beginn der Kurzbezeichnung des Standards erkennen:

ISO/IEC-Standards

Bei der Mehrzahl handelt es sich um internationale Normen, die unter deutscher Mitwirkung im Subkomitee 27 »IT-Security Techniques« des Technischen Gemeinschaftskomitees »Information Technology« der Internationalen Normenorganisationen ISO und IEC, ISO/IEC JTC 1/SC 27 (http://www.jtc1sc27.din.de), nach einem Konsensverfahren entwickelt und in einer öffentlichen Umfrage bestätigt wurden. Diese Standards sind an der Zeichenkette ISO/IEC gefolgt von der Normennummer zu erkennen (Beispiel: ISO/IEC 27001).

DIN EN-Standards

Bei Standards, die mit der Zeichenkette EN beginnen, handelt es sich um Europäische Normen, die von einer der Europäischen Normenorganisationen CEN, CENELEC oder ETS, ebenfalls nach einem Konsensverfahren mit öffentlicher Umfrage, entwickelt wurden. Beginnt die Zeichenkette mit »DIN«, so handelt es sich um eine deutsche Norm. »DIN EN« bezeichnet eine Europäische Norm, die in das deutsche Normenwerk übernommen wurde.

Andere Standards

Andere Bezeichnungen (wie z. B. IT-GSHB) deuten auf Standards, die von Konsortien, Interessen-gruppen oder Behörden nach deren jeweiligen Regeln erarbeitet wurden. Diese Regeln sehen einen gegenüber den Normungsorganisationen eingeschränkten Konsensrahmen vor und legen die Mitwirkungsmöglichkeiten fest.

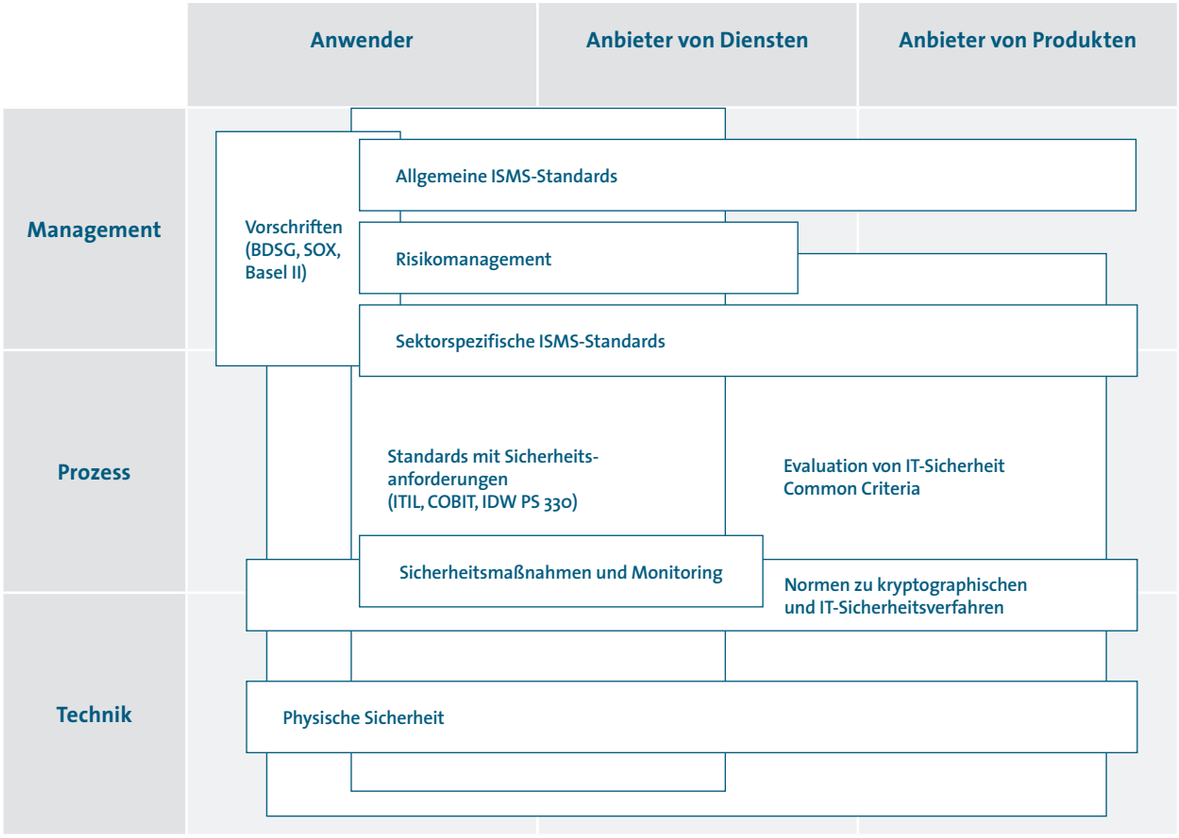
Die Erarbeitung deutscher Beiträge und Stellungnahmen zu internationalen Normen erfolgt durch das DIN, insbesondere durch den Arbeitsausschuss »IT-Sicherheitsverfahren« des Normenausschusses Informationstechnik NIA-27 (www.nia.din.de/ni27). Die Mitarbeit[1] in den Gremien des DIN ist, bei angemessener Beteiligung an den Kosten der Normungsarbeit, offen für alle interessierten Kreise – unabhängig von der Mitgliedschaft im DIN.

Die internationalen bzw. nationalen Standards werden im zeitlichen Abstand von maximal fünf Jahren einer Revision unterzogen und bei Bedarf überarbeitet. Das Veröffentlichungsdatum gibt jeweils den Abschluss der letzten Überarbeitung an. Bei der Anwendung der Standards ist es sinnvoll, bei einer aktuellen Datenbank (z. B. www.beuth.de, Verlag des DIN) die aktuelle Ausgabe anzufragen. Hier können die Standards auch bezogen werden.

[1] Anfragen zur Mitarbeit sowie zu den Projekten und Normen können gern an den Ausschuss (siehe Impressum) gestellt werden.

3.2 Wesentliche Einordnung von Standards

Standards lassen sich nach verschiedenen Kriterien sortieren. Sinnvollerweise findet eine Gruppierung nach dem Betrachtungsgegenstand (also den zu standardisierenden Inhalten statt. Die im Kompass der Sicherheitsstandards vorgesehenen Gruppen lassen sich in folgendem Bild ablesen. Im Wesentlichen orientiert sich die Struktur an der Einteilung der Standards des NIA-27 und seiner Arbeitsgruppen.



3.3 Zuordnung der Einzelstandards

Im Folgenden werden die grundlegenden Standards zum IT-Sicherheits- und Risikomanagement den oben dargestellten Gruppen zugeordnet.

Informationssicherheits-Managementsysteme (ISMS)

ISO/IEC 27001	Information security management systems – Requirements Informationssicherheits-Managementsysteme-Anforderungen
ISO/IEC 27002	Code of practice for information security management Leitfaden zum Informationssicherheitsmanagement
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems Anforderungen an Stellen, die Auditierung und Zertifizierung von Informationssicherheitsmanagementsystemen bereitstellen
IT-GS	IT-Grundschutz

Sektor-Spezifische ISMS

Richtlinie VDI/VDE2182	Informationssicherheit in der industriellen Automatisierung
ISO/IEC 27011	Information security management guidelines for telecommunications Informationssicherheitsmanagement-Leitlinien für die Telekommunikation
PCI DSS	Payment Card Industry Data Security Standard v 1.2
ISO/IEC TR 27015	Information security management guidelines for financial services Leitlinien zum Informationssicherheitsmanagement von Finanzdienstleistungen
ISO/IEC TR 27019	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry Leitlinien zum Informationssicherheitsmanagement auf Basis IISO/IEC 27002 für die Telekommunikation für die Energiewirtschaft

Sicherheitsmaßnahmen und Monitoring

ISO/IEC 27033	IT network security IT Netzwerksicherheit
ISO/IEC TR 18044	Information security incident management Management von Sicherheitsvorfällen in der Informationssicherheit
ISO/IEC 18043	Selection, deployment and operation of intrusion detection systems (IDS) Auswahl, Einsatz und Betrieb von Systemen zur Erkennung des Eindringens in Netze und Systeme (IDS)
ISO/IEC 15816	Security information objects for access control Sicherheitsobjekte für Zugriffskontrolle
ISO/IEC 24762	Security techniques – Guidelines for information and communications technology disaster recovery services
ISO/IEC 25777	Information and communications technology continuity management. Code of practice

Risikomanagement

■ MaRisk	Mindestanforderungen an das Risikomanagement für Banken
■ ISO/IEC 27005	Information security risk management Informationssicherheits-Risikomanagement
■ ISO/IEC 27014	Governance of information security Governance der Informationssicherheit

Standards mit IT-Sicherheitsanforderungen

■ Cobit	Control Objectives for Information and Related Technology Kontrollziele für Informations- und verwandete Technologie
■ ITIL	IT Infrastructure Library IT Infrastruktur Verfahrensbibliothek
■ IDW PS 330	Abschlussprüfung bei Einsatz von Informationstechnologie

Vorschriften

■ KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
■ Basel II	-
■ SOX	Sarbanes-Oxley Act
■ EURO-SOX	8. EU-Richtlinie in Anlehnung an Sarbanes-Oxley Act
■ BDSG	Bundesdatenschutzgesetz

Evaluierung von IT-Sicherheit

Common Criteria

■ ISO/IEC 15408 (CC)	Evaluation criteria for IT security (Common Criteria) Evaluationskriterien für IT-Sicherheit
■ ISO/IEC TR 15443	A framework for IT security assurance Rahmenrichtlinien für Sicherung von IT-Sicherheit
■ ISO/IEC 18045	Methodology for IT security evaluation Methodik zur Evaluation von IT-Sicherheit
■ ISO/IEC TR 19791	Security assessment for operational systems Bewertung der Sicherheit von Systemen im Betrieb
■ ISO/IEC 19790 (FIPS 140-2)	Security Requirements for Cryptographic Modules Anforderungen an kryptographische Module
■ ISO/IEC 19792	Security evaluation of biometrics Evaluierung der IT-Sicherheit biometrischer Technologien
■ ISO/IEC 21827 (SSE-CMM)	System Security Engineering – Capability Maturity Model Modell der Ablaufstauglichkeit (auch ISO 21827)
■ ISO/IEC 24759	Test requirements for cryptographic modules Prüfanforderungen für kryptographische Module

Schutzprofile

■ ISO/IEC TR 15446	Guide on the production of protection profiles and security targets Leitfaden zum Erstellen von Schutzprofilen und Sicherheitsvorgaben

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

■ ISO/IEC 7064	Check character systems Prüfsummensysteme
■ ISO/IEC 18033	Encryption algorithms Verschlüsselungsalgorithmen
■ ISO/IEC 10116	Modes of operation for an n-bit block cipher Betriebsarten für einen n-bit-Blockschlüssel-Algorithmus
■ ISO/IEC 19772	Data encapsulation mechanisms Daten verkapselnde Mechanismen
■ ISO/IEC 29192	Lightweight cryptography Leichtgewichtige Kryptographie

Digitale Signaturen

■ ISO/IEC 9796	Digital signature schemes giving message recovery Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht
■ ISO/IEC 14888	Digital signatures with appendix Digitale Signaturen mit Anhang
■ ISO/IEC 15946	Cryptographic techniques based on elliptic curves Auf elliptischen Kurven aufbauende kryptographische Techniken

Hash-Funktionen und andere Hilfsfunktionen

■ ISO/IEC 10118	Hash functions Hash-Funktionen
■ ISO/IEC 18031	Random bit generation Erzeugung von Zufallszahlen
■ ISO/IEC 18032	Prime number generation Primzahlerzeugung

Authentifizierung

■ ISO/IEC 9798	Entity authentication Authentisierung von Instanzen
■ ISO/IEC 9797	Message Authentication Codes (MACs) Nachrichten-Authentisierungscodes (MACs)

PKI-Dienste

■ ISO/IEC 15945	Specification of TTP services to support the application of digital signatures Spezifizierung der Dienste eines vertrauenswürdigen Drittens zur Unterstützung der Anwendung von digitalen Signaturen

ISO/IEC TR 14516	Guidelines for the use and management of Trusted Third Party Services Richtlinien für die Nutzung und das Management eines vertrauenswürdigen Dritten

Schlüsselmanagement

ISO/IEC 11770	Key management Schlüsselmanagement

Kommunikationsnachweise

ISO/IEC 13888	Non-repudiation Nicht-Abstreitbarkeit

Zeitstempeldienste

ISO/IEC 18014	Time-stamping services Zeitstempeldienste

Spezielle Sicherheitsfunktionen 2: Physische Sicherheit

Technische Leitlinie 03400 (BSI 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

Sichere Löschung von Datenträgern

DIN 32757	Vernichtung von Informationsträgern

3.4 Beschreibung der IT-Sicherheitsstandards

Jeder aufgeführte Standard bzw. Norm und jede aufgeführte Vorschrift wird in den folgenden Kapiteln kurz beschrieben:

- Die Beschreibung für jeden Standard, jede Vorschrift ist nach einem einheitlichen Schema strukturiert:
  - Inhalt und Anwendungsbereich
  - Methodik (wo sinnvoll)
  - Zertifizierung (wo sinnvoll)
  - Weitere Anmerkungen
  - Bisherige Ausgaben
  - Falls ein Abschnitt ohne Inhalte wäre, ist dieser in der Beschreibung nicht aufgeführt, z. B. können Vorschriften nicht zertifiziert werden, so entfällt bei der Vorschrift »Basel II« der Abschnitt »Zertifizierung«.

- Sofern es sich um internationale oder europäische Standards handelt, sind der Titel, das Arbeitsgebiet und der Name des Standards (englisch) aufgeführt. Englische Titel wurden verständnishalber um eine inoffizielle deutsche Übersetzung ergänzt, da nur die in das deutsche Normenwerk übernommenen Dokumente einen offiziellen deutschen Titel tragen. Bei mehrteiligen Standards bzw. einer Normenreihe wird die Nummer des jeweiligen Teils mit einem Bindestrich nach der Normennummer angefügt.

- Internationale und europäische Standards wurden formal meist nicht in das deutsche Normenwerk übernommen, weil die aufwändige Übersetzung in der Regel keinen entsprechenden Mehrwert für die Anwender schafft. Ist die Übernahme einer internationalen Norm ins deutsche Normenwerk erfolgt oder geplant, so wird dies bei den Erläuterungen im Abschnitt »Weitere Anmerkungen« ausgewiesen.

- Standards sind von anderen Standards abhängig oder beeinflussen diese. Der Bezug von Standards zu anderen Standards ist ebenfalls in der Online-Version erläutert. Diese Bezüge sind möglichst umfassend angegeben, eine Vollständigkeit kann nicht garantiert werden.

3.5 Einführung von IT-Sicherheitsstandards im Unternehmen

Die Einführung von Standards im Unternehmen erfolgt in drei generischen Schritten:

Auswahl des Standards

In der Regel entscheidet die Geschäftsführung mit Unterstützung des – falls vorhanden – IT-Sicherheitsbeauftragten, IT-Risikobeauftragten und IT-Verantwortlichen den IT-Betrieb vom Unternehmen an einem IT-Sicherheitsstandard auszurichten. Welcher Standard der richtige für ein Unternehmen ist, hängt von einigen Faktoren (siehe Kompass) ab:

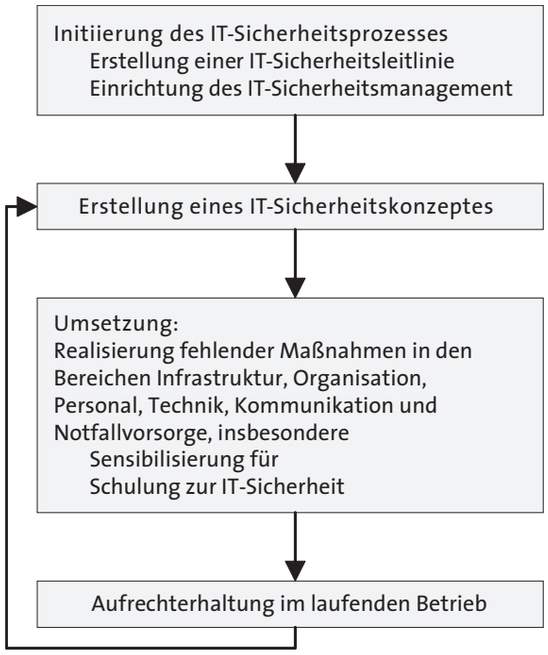
- Art des Unternehmens

- Relevanter Unternehmensbereich für die Standardisierung

- Relevante Charakteristika des Standards

Einführung

Die Einführung von IT-Sicherheitsstandards im Unternehmen erfolgt nach dem jeweiligen Vorgehensmodell des ausgewählten Standards. Als Beispiel sei hier das Vorgehensmodell nach BSI IT-Grundschutz aufgeführt:



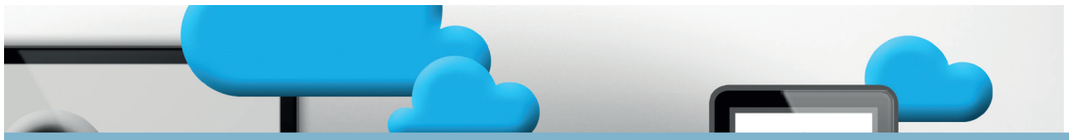
Die Notwendigkeit der einzelnen Schritte des jeweiligen Vorgehensmodells sollten vor der Einführung auf Relevanz geprüft werden. Anschließend sind die ausgewählten Schritte durchzuführen und die Maßnahmen zur Umsetzung des Standards festzulegen. Hierbei ist zu beachten, dass für die Umsetzung des Modells externes Know-how zugezogen bzw. Mitarbeiter entsprechend geschult werden sollten. Die Einführung eines Standards ohne externes oder internes Know-how führt in der Regel zu einem höheren Aufwand bei eventuell schlechterem Ergebnis.

Betrieb

Nach der Einführung des Standards müssen die getroffenen Maßnahmen (personell, organisatorisch, technisch) in den regulären Betrieb übergehen. Hierfür sind Mitarbeiterschulungen, -information sowie ggf. Prozessanpassungen notwendig. Im Rahmen des regulären IT-Betriebs kann die Einhaltung des Standards durch zwei aufeinander aufbauende Verfahren überprüft und gewährleistet werden:

- **Auditierung**
  Ein wichtiges Element des Vorgehensmodells ist, die Einhaltung und Aktualität der Sicherheitsmaßnahmen in regelmäßigen Audits von internen oder externen Partnern zu überprüfen. Mit diesem Vorgehen können Unternehmen ihre IT-Sicherheit immer weiter verbessern und sukzessive Sicherheitslücken schließen.
  Im Rahmen eines Audits kommt ein externer (zertifizierter) Auditor für einige Tage ins Unternehmen. Anhand der Vorgaben des Standards bzw. der Dokumentation des IT-Betriebs wird der Ist-Stand mit dem Soll-Konzept verglichen. Empfehlungen für die Verbesserung der IT-Sicherheit werden ausgesprochen. Diese sollten vom Unternehmen im Nachgang umgesetzt werden.
  Eine Auditierung kann den gesamten IT-Betrieb umfassen, kann sich aber auch nur auf beispielsweise neu eingesetzte Sicherheitskomponenten beschränken (z. B. neue Firewall).

- **Zertifizierung**
  Einige IT-Sicherheitsstandards können als Grundlage für eine Zertifizierung herangezogen werden. Ein Zertifikat ist eine unabhängige Bestätigung dafür, dass alle (soweit anwendbaren) im Standard geforderten Sicherheitsmaßnahmen zum Zeitpunkt der Zertifizierung dokumentiert und tatsächlich umgesetzt sind. Durch die Ausstellung eines Zertifikates, mit dem die Umsetzung des Standards bestätigt wird, kann dies Dritten transparent gemacht werden. Dritte können hierbei Kunden, Banken, Versicherungen oder auch die Öffentlichkeit sein.
  Der Aufwand für die Zertifizierung ist abhängig vom Unternehmen und dem Zertifizierungsziel. Hierbei kann jedoch von einem externen Aufwand von einigen Tagen bis einigen Wochen ausgegangen werden. Der interne Aufwand kann deutlich höher sein, je nach Vorbereitungsstand des Unternehmens. Eine generelle Aussage kann nicht getroffen werden.
  Bei der Auswahl des Zertifizierers ist zu beachten, dass einige Standards einen akkreditierten Zertifizierer fordern.



4 Neuerungen bei den Standards in 2013

Die vorliegende Sonderausgabe berücksichtigt eine Auswahl neuer oder aktualisierter Sicherheitsstandards aus dem Jahr 2013. Diese Auswahl hat nicht den Anspruch, vollständig oder thematisch erschöpfend zu sein. Vielmehr sollen die hier dargestellten Standards exemplarisch dazu dienen, dem Leser aktuelle Entwicklungen auf diesem Gebiet zu vermitteln und zur ausführlicheren Lektüre der Sicherheitsstandards anregen.

4.1 ISO/ IEC 27014:2013

ISO/ IEC 27014

Titel	ISO/IEC 27014
Arbeitsgebiet	IT-Sicherheitsverfahren
Name des Standards	Governance of information security Governance der Informationssicherheit

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 27014 bildet die Schnittstelle zwischen der Organisation, der Geschäftsleitung sowie den Verantwortlichen für die Umsetzung und den Betrieb eines Information Security Management Systems. Es ist eine Ergänzung zu den Anforderungen aus ISO/IEC27001. Der Standard beschreibt, wie Maßnahmen zur Informationssicherheit in der gesamten Organisation umgesetzt werden sowie IT-Sicherheitsberichte in einem geschäftlichen Kontext zurück an die Geschäftsleitung gelangen. Damit sind aussagekräftige und zeitnahe Entscheidungen zur Unterstützung der strategischen Ziele der Organisation möglich.

Methodik

Die Governance der Informationssicherheit muss die Ziele und Strategien für die Informationssicherheit an den wirtschaftlichen Zielen des Unternehmens ausrichten und gleichzeitig die Einhaltung von Gesetzen, Verordnungen und Verträgen sicherstellen. Dazu gehört ein Risiko-Management-Ansatz (z. B. nach ISO/IEC 27005) kombiniert mit einem internen Kontrollsystem (IKS). Zu den Ergebnissen einer effektiven Umsetzung der Governance gehört den Status der Informationssicherheit sichtbar zu machen, eine Entscheidungsfindung bei der Behandlung von Informationssicherheitsrisiken zu ermöglichen sowie eine effiziente und effektive Planung von Investitionen zu gewährleisten. Weiterhin werden externe, d.h. rechtliche, regulatorische oder vertragliche Anforderungen bestmöglich eingehalten.

Der Standard ISO/IEC 27014 definiert sechs Grundsätze:

1. Sicherstellen einer unternehmensweiten Informationssicherheit
2. Verfolgung eines Risikobasierten Ansatzes
3. Richtungsentscheidungen für Investitionsentscheidungen
4. Konformität mit internen und externen Anforderungen
5. Fördern eines positiven Sicherheitsumfelds
6. Bewertung der Kosten und des Nutzens der Informationssicherheit in Bezug auf die Geschäftsergebnisse

Bisherige Ausgaben

ISO/IEC 2014:2013

4.2 ISO/ IEC TR 27019:2013

ISO/ IEC TR 27019:2013

Titel	ISO/IEC 27019
Arbeitsgebiet	IT-Sicherheitsverfahren, Technischer Bericht
Name des Standards	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry Leitlinien zum Informations-sicherheitsmanagement auf Basis IISO/IEC 27002 für die Telekommu-nikation für die Energiewirtschaft

Inhalt und Anwendungsbereich

Der Standard ISO/IEC 27019 basiert auf dem Standard ISO/IEC 27002 »Code of practice for information security management« und stellt Leitlinien für ein Informationssicherheitsmanagementsystems (ISMS) für Prozessleitsysteme und Automatisierungstechnik in der Energieversorgungsindustrie vor. Im Fokus des Standards stehen Systeme und Netzwerke zur Steuerung und Überwachung der Erzeugung, Übertragung und Verteilung von elektrischer Energie, Gas und Wärme. Dazu gehören Steuerungs- und Automatisierungssysteme, Schutz- und Sicherheits- sowie Messsysteme inklusive der Kommunikationstechnik. Der Standard fasst diese als Prozessleittechnik zusammen. Im Unterschied zu ISO/IEC 27002 stehen hier kritische Infrastrukturen im Vordergrund, die für einen sicheren und zuverlässigen Betrieb notwendig sind und damit auch in den Managementprozessen entsprechend berücksichtigt werden müssen (Verfügbarkeit und Integrität der Daten).

Methodik

Der Standard ISO/IEC 27019 betrifft die folgenden Themengebiete:

- Die gesamte IT-gestützte zentrale und dezentrale Prozess-Steuerung, Überwachung und Automatisierungstechnik sowie die dazu notwendigen IT-Systeme für den Betrieb, die Programmierung und Parametrisierung der Geräte
- Digitale Steuerungs- und Automatisierungskomponenten (z. B. Sensoren und Aktor-Elemente)
- Alle unterstützenden IT-Systeme in der Prozesskontrolle (z. B. Datenvisualisierung, Überwachung, Archivierung, Dokumentation)
- Die gesamte Kommunikationstechnik in den Prozessleitsystemen (z. B. Netzwerke, Remote-Control, Messgeräte)
- Schutz- und Sicherheitssysteme (z. B. Relais, SPS-Steuerungen)
- Smart-Grid Umgebungen
- Alle Software, Firmware und Anwendungen zum Betrieb der oben genannten Systeme
- Alle im Standard ISO/IEC 27002 erwähnten Kapitel werden behandelt und aufgezeigt, wo ergänzende Massnahmen in der Energieindustrie notwendig sind.

Bisherige Ausgaben

ISO/IEC 2019:2013

4.3 ISO/IEC 9798-2:2008/Cor 3:2013

ISO/IEC 9798

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Entity authentication Authentisierung von Instanzen

Inhalt und Anwendungsbereich

Die Normenreihe legt informationstechnische Mechanismen zur Authentisierung von Instanzen fest. Diese werden zur Bestätigung dessen eingesetzt, dass eine Instanz tatsächlich die ist, die sie vorgibt zu sein. Eine zu authentisierende Instanz beweist ihre Identität, indem sie zeigt, dass sie einen geheimen Authentisierungsschlüssel kennt. Die Mechanismen sind für den technischen Austausch von Informationen zwischen Instanzen und, wo notwendig, mit einem vertrauenswürdigen Dritten (Trusted Third Party, TTP) gedacht.

Der Standard besteht aus den Teilen:

Teil 1: Allgemeines Modell (General)

Teil 2: Mechanismen auf Basis von symmetrischen Verschlüsselungsalgorithmen
(Mechanisms using symmetric encipherment algorithms)

Teil 3: Authentifikation von Instanzen unter Benutzung eines Algorithmus mit öffentlichem Schlüssel
(Mechanisms using digital signature techniques)

Teil 4: Mechanismen auf Basis einer kryptographischen Prüffunktion
(Mechanisms using a cryptographic check function)

Teil 5: Mechanismen auf Basis von Zero-Knowledge-Techniken
(Mechanisms using zero-knowledge techniques)

Teil 6: Mechanismen auf Basis von manuellem Datentransfer
(Mechanisms using manual data transfer)

Teil 1 führt in die grundlegenden Konzepte ein und beschreibt ein allgemeines Modell für die Authentifizierung von Instanzen.

Teil 2 legt Mechanismen zur Authentisierung von Kommunikationspartnern fest, die symmetrische Verschlüsselungsalgorithmen nutzen. Die zu authentisierenden Kommunikationspartner beweisen ihre Identitäten dadurch, dass sie einen geheimen Authentisierungsschlüssel kennen.

Teil 3 legt Mechanismen zur Authentisierung von Kommunikationspartnern fest, die einen Algorithmus für öffentliche Schlüssel und eine digitale Signatur zur Bestimmung der Identität einer Instanz nutzen. Die Anwendung dieses Teils ist nicht auf einen bestimmten Algorithmus begrenzt; jeder Algorithmus für öffentliche Schlüssel kann eingesetzt werden, der die Anforderungen der Authentisierungsalgorithmen erfüllt.

Teil 4 legt Mechanismen zur Authentisierung von Kommunikationspartnern fest, die eine kryptographische Prüffunktion nutzen, und beschreibt den notwendigen Inhalt von Nachrichten.

Teil 5 legt Mechanismen zur Authentisierung von Instanzen fest, die Zero-Knowledge Techniken nutzen. Mit Zero-Knowledge bezeichnet man dabei die Eigenschaft, nur die Gültigkeit einer Authentisierung aber kein darüber hinausgehendes Wissen ableiten zu können. Alle in diesem Teil der Normenreihe festgelegten Mechanismen bieten eine einseitige Authentisierung.

Diese Mechanismen sind zwar nach den Prinzipien des Zero-Knowledge aufgebaut, können gemäß der genauen (mathematischen) Definition aber keine völlige Zero-Knowledge-Eigenschaft umsetzen.

Teil 6 legt Mechanismen zur Authentisierung von Instanzen fest, die auf einem manuellen Datentransfer zwischen den authentisierenden Geräten aufbauen. Diese Mechanismen sind für unterschiedliche Gerätetypen geeignet.

Bisherige Ausgaben

- ISO/IEC 9798-1:1991; 1997; 2010
- ISO/IEC 9798-2:1994; 1999; 2008
- ISO/IEC 9798-2 COR1:2004
- ISO/IEC 9798-2:2008/Cor 1:2010
- ISO/IEC 9798-2:2008/Cor 2:2012
- ISO/IEC 9798-2:2008/Cor 3:2013
- ISO/IEC 9798-3:1993; 1998
- ISO/IEC 9798-3:1998/Cor 1:2009
- ISO/IEC 9798-3:1998/Amd 1:2010
- ISO/IEC 9798-3:1998/Cor 2:2012
- ISO/IEC 9798-4:1995; 1999
- ISO/IEC 9798-5:1999; 2004; 2009
- ISO/IEC 9798-6:2005; 2010
- ISO/IEC 9798-6:2005/Cor 1:2009

4.4 ISO/IEC 29192-4:2013

ISO/IEC 29192

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	Lightweight cryptography Leichtgewichtige Kryptographie

Inhalt und Anwendungsbereich

Das Gebiet der leichtgewichtigen Kryptographie befasst sich mit kryptographischen Verfahren, die aufgrund ihres geringen Ressourcenbedarfs besonders für den Einsatz in ressourcenbeschränkten Umgebungen (z. B. RFID-Tags, Sensoren) geeignet sind.

Leichtgewichtige Kryptographie heißt nicht unbedingt schwache Kryptographie: die in ISO/IEC 29129 spezifizierten Mechanismen bieten alle zumindest ein Sicherheitsniveau von 80 Bit.

ISO/IEC 29192 besteht aus den Teilen:

Teil 1: Allgemeines Modell (General)

Teil 2: Blockchiffren (Block ciphers)

Teil 3: Stromchiffren (Stream ciphers)

Teil 4: Asymmetrische Mechanismen
(Mechanisms using asymmetric techniques)

Teil 1 hat allgemeinen Charakter und beinhaltet Definitionen und Konzepte, die für die weiteren Teile dieser Normenreihe gelten, insbesondere die Kriterien für die Auswahl der in den weiteren Teilen festgelegten Algorithmen.

Teil 2 spezifiziert zwei Algorithmen für Blockchiffren: Present und CLEFIA.

Teil 3 spezifiziert zwei Algorithmen für Stromchiffren: Trivium und Enocoro.

Teil 4 definiert leichtgewichtige asymmetrische kryptographische Mechanismen zur Authentifizierung und zum Schlüsselaustausch. Diese sind cryptoGPS, ALIKE und IBS.

Weitere Anmerkungen

An einem weiteren Teil 5 mit dem Schwerpunkt Hashfunktionen wird gearbeitet. Dieser Teil befindet sich derzeit noch in einem frühen Stadium.

Bisherige Ausgaben

- ISO/IEC 29192-1:2012
- ISO/IEC 29192-2:2012
- ISO/IEC 29192-3:2012
- ISO/IEC 29192-4:2013

4.5 ISO/IEC 27033-5:2013

ISO/IEC 27033 (ehemals 18028)

Titel:	Informationstechnik
Arbeitsgebiet:	IT-Sicherheitsverfahren
Name des Standards:	IT Network security IT-Netzwerksicherheit

Inhalt und Anwendungsbereich

Durch diesen Standard soll Netzwerksicherheit detailliert für unterschiedliche Zielgruppen in einer Organisation adressiert werden. Dabei werden Sicherheitsaspekte bei Nutzung, Wartung und Betrieb von IT-Netzwerken und deren Beziehung, auch Außenverbindungen, betrachtet. Unter Außenverbindung sind sowohl der Fernzugriff von Nutzern, als auch logische Verbindungen zu verstehen. Für diejenigen die innerhalb einer Organisation für die IT-Sicherheit im Allgemeinen, und im speziellen für Netzwerksicherheit verantwortlich sind, können die Informationen dieses Standards in individuelle Anforderungen adaptiert werden.

ISO/IEC 27033 ist aus ISO/IEC 18028 hervorgegangen und besteht aus sechs Teilen, Teil 6 befindet sich dabei noch in einem frühen Stadium:

Teil 1: Überblick und Konzepte

Teil 2: Richtlinien für den Entwurf und die Einführung von Netzwerksicherheit

Teil 3: Referenzszenarien für Netzwerke; Bedrohungen, Entwurfstechniken und Kontroltechniken

Teil 4: Absicherung der Netzwerkkommunikation durch Sicherheits-Gateways

Teil 5: Absicherung der Kommunikation über Netzwerke durch Virtual Private Networks (VPN)

Teil 6: Absicherung des Zugangs zu kabellosen IP-Netzwerken

Methodik

Das Dokument vermittelt zunächst im übergeordneten Teil 1 eine grundlegende Einführung in die Normenreihe und die generelle Vorgehensweise, um ein geeignetes Sicherheitsniveau mittels Risikobewertung in Bezug zu den Organisationsprozessen zu erreichen. Grundsätzlich findet eine enge Anlehnung an andere Standards der ISO/IEC 270xx-Familie statt.

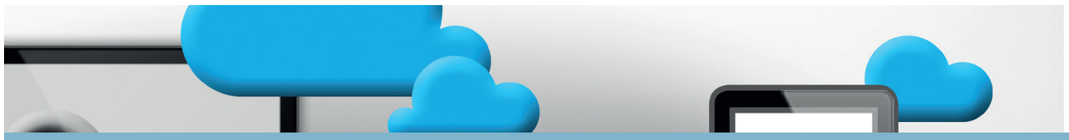
Teil 2 definiert eine Architektur zur Netzwerksicherheit, die auf Ende-zu-Ende-Sicherheit fokussiert und von der konkreten Netzwerktechnologie unabhängig ist. In den verbleibenden Teilen werden spezielle Netzwerktypen und deren Einbettung in die Netzwerksicherheitsarchitektur adressiert.

Weitere Anmerkungen

Das Dokument folgt in seiner generellen Vorgehensweise der ISO/IEC 27002 zur Etablierung eines IT-Sicherheitsniveaus und einer IT-Sicherheitsleitlinie.

Bisherige Ausgaben

- ISO/IEC 27033-1:2009
- ISO/IEC 27033-2:2012
- ISO/IEC 27033-3:2010
- ISO/IEC 27033-4:2014 (erwartet)
- ISO/IEC 27033-5:2013



5 Anhang

Bezug zu anderen Standards

Standards beziehen sich auch auf andere Standards. In der folgenden Liste sind diese Abhängigkeiten aufgeführt. Die Liste besitzt nicht den Anspruch auf Vollständigkeit.

Informationssicherheits-Managementsysteme (ISMS)

ISO/IEC 27001	ISO/IEC 27001 bezieht sich besonders eng auf ISO/IEC 27002 und hat eine inhaltliche Verbindung zu allen anderen Normen der 2700x-Familie. Im Kontext integrierter Managementsysteme ist auch ISO 9000 als Normenreihe zu nennen.
ISO/IEC 27002	Da hier Sicherheitsmanagement behandelt wird, besteht ein enger Bezug zu ISO/IEC 27001.
ISO/IEC 27006	Hier besteht ein enger Bezug zur ISO/IEC 27001. Weiterhin ist als Auditierungs- und Zertifizierungsstandard die ISO/IEC 17021 von Bedeutung.
IT-Grundschutz	Die Umstellung der IT-Grundschutz-Vorgehensweise erfolgte konform zur Verabschiedung des internationalen Standard ISO/IEC 27001, welcher aus der BS 7799-2 hervorgegangen ist. Ebenso werden die Empfehlungen der Norm ISO/IEC 27002 berücksichtigt, deren Umsetzung die Anforderungen des Standards ISO/IEC 27001 erfüllen. Methoden zur Risikoanalyse werden in der Norm ISO/IEC 27005 beschrieben.

Sektor-spezifische ISMS

ISO/IEC 27011	Dieser Standard kann als eine sektorspezifische Erweiterung von ISO/IEC 27002 gesehen werden.
Richtlinie VDI/VDE2182	Dieser Standard kann als eine sektorspezifische Erweiterung von ISO/IEC 27002 gesehen werden.

Sicherheitsmaßnahmen und Monitoring

ISO/IEC 18028	ISO/IEC 27005, ISO/IEC 27002:2005, ISO/IEC 27001:2005, ISO/IEC 18044:2004, ISO/IEC 18043
ISO/IEC TR 18044	Der Technische Bericht kann als Detaillierung des Kapitels «Behandlung von Sicherheitsvorfällen" von ISO/IEC 27002 gesehen werden. ISO/IEC 18043 liefert Hinweise zur Auswahl, Einsatz und Betrieb entsprechender technischer Eingriffserkennungssysteme. Die Methodik der Risikoanalyse wird in diesem Standard referenziert. Hierzu liefert wiederum ISO/IEC 27005 weitere Inhalte.

■ ISO/IEC 18043	Der Standard hilft bei der Implementierung einiger Anforderungen aus dem ISO/IEC 27002, nämlich der Erkennung nicht berechtigter Zugriffe auf IT-Systeme und deren sicherheitstechnischen Überwachung. ISO 18043 liefert Hinweise zur Auswahl, Einsatz und Betrieb entsprechender technischer Eingriffserkennungssysteme. Die Methodik der Risikoanalyse wird in diesem Standard referenziert. Hierzu liefert wiederum ISO/IEC 27005 weitere Inhalte.
■ ISO/IEC 15816	Es ist beabsichtigt, andere Normen auf die Definitionen aus diesem Dokument zu verweisen.
■ ISO/IEC 24762	Die Themenblöcke Desaster Recovery Management (ISO/IEC 24762) und Business Continuity Management (BS 25777) sind inhaltlich eng verwoben. Daher werden beide Normen häufig parallel betrachtet.
■ BS 25777	Daher werden beide Normen häufig parallel betrachtet.

Risikomanagement

■ MaRisk	MaRisk kann als Sektorspezifische Ausprägung der ISO/IEC 27005 gesehen werden. Weiterhin sind Bezüge zum IT-Grundschutz gegeben.
■ ISO/IEC 27005	Das Risikomanagement hat wesentliche inhaltliche Bezüge zur ISO/IEC 27001 und zur ISO 9000.

Standards mit IT-Sicherheitsaspekten

Cobit	Einen konkreten Bezug zu anderen Standards gibt es nicht. Cobit leitet sich mit Fokus auf Informationstechnologie aus dem COSO Framework ab. In Cobit sind Bestandteile aus insgesamt 41 nationalen und internationalen Standards eingearbeitet und gemeinsam ausgerichtet worden.
ITIL	Die IT-Sicherheitsmaßnahmen werden aus BS 7799 genommen, Zertifizierung erfolg über BS 15000 bzw. ISO/IEC 20000.
IDW PS 330	Der Standard für IT-Systemprüfungen baut auf dem »International Standard on Auditing (ISA 401)« auf. Der zeitliche Aufwand ist wesentlich geringer als bei einer Prüfung nach IT-Grundschutz oder ISO/IEC 27001. In Erfahrungsberichten ist von wenigen Tagen für Prüfungen im Mittelstand die Rede. Die Aufteilung der zu prüfenden Bereiche ■ IT-Umfeld (Richtlinien, IT-Strategie) ■ IT-Organisation ■ IT-Infrastruktur ■ IT-Anwendungen ■ IT-Geschäftsprozesse erinnert an Aufteilung im BSI-Grundschutz. Der Detaillierungsgrad der abzufragenden Maßnahmen bewegt sich jedoch eher auf der Ebene von der des ISO/IEC 27002.

Evaluierung von IT-Sicherheit

Common Criteria

■ ISO/IEC 15408 (CC)	Mehrere andere Dokumente stehen in Bezug zu diesem Standard: ISO/IEC 18045 definiert die Methodologie, mit der Evaluierungen gemäß 15408 durchgeführt werden. Insofern ist hier eine unmittelbare Abhängigkeit vorhanden. ISO/IEC 15446 gibt Hinweise, wie Schutzprofile (Protection Profiles) und Sicherheitsvorgaben (Security Targets) verfasst werden, die im Kontext der Evaluierung nach 15408 relevant sind. ISO/IEC 15292 stellt die Arbeitsweise von Registrierungsstellen für Protection Profiles dar. Der technische Bericht ISO/IEC 19791 stellt eine Möglichkeit dar, die Evaluierung auf IT-Systeme inklusive ihres Betriebs anzuwenden.
■ ISO/IEC TR 15443	Da es das Ziel dieses Standards ist, einen Weg zur Auswahl von Vertrauenswürdigkeitsmethoden aufzuzeigen, besteht naturgemäß ein Zusammenhang zu allen anderen Standards, die in diesem Abschnitt genannt sind. Fast alle von ihnen gehören zu einer der Vertrauenswürdig-keitsmethoden, die im Standard behandelt werden. Darüber hinaus werden aber auch viele ISO- und Nicht-ISO-Standards in ISO/IEC TR 15443 behandelt, die im vorliegenden Dokument nicht behandelt wurden.
■ ISO/IEC 18045	Ein Bezug besteht unmittelbar zur ISO/IEC 15408 (Common Criteria), und dadurch indirekt zu weiteren damit zusammenhängenden Standards.
■ ISO/IEC TR 19791	Ein Bezug besteht einerseits zu ISO/IEC 15408 (Common Criteria), da deren Methoden für in Betrieb befindliche IT-Systeme nutzbar gemacht werden sollen. Da hier Aspekte des IT-Sicherheits-managements eine große Rolle spielen, sind auch Standards zu diesem Thema relevant. Einige Beispiel sind: die ISO/IEC 2700x-Familie; ISO/IEC TR 15443-1/3; ISO/IEC 27002; ISO/IEC 18028-1/4; ISO/IEC 21827: 2002
■ ISO/IEC 19790 (FIPS 140-2)	Da viele kryptographische Verfahren, etwa zu Verschlüsselung, Signaturen, Hash-Funktionen, Zufallszahlen, in dem Standard erwähnt werden, sind alle Standards, die solche Algorithmen definieren, für ISO/IEC 19790 relevant. Sie werden hier nicht im Einzelnen aufgezählt, es sei auf die entsprechenden Abschnitte und kryptographischen Standards in dieser Liste verwiesen. Relevant ist zudem «Federal Information Processing Standard Publication (FIPS PUB) 140-2, Security requirements for cryptographic modules", wie im vorigen Abschnitt erwähnt. Relevant ist auch der Bezug zu 15408, also den allgemeinen Evaluations-kriterien. Diese erlauben auch die Evaluierung von Produkten, die als Kryptomodule dienen, und werden dafür (etwa im Fall von Chipkarten) auch genutzt. Die Tatsache, dass eine solche allgemeine Evaluationsnorm (15408) und eine spezielle Norm für Kryptomodule (19790) parallel existieren werden, ist wesentlich historisch bedingt, insbesondere auch durch die Nutzung von FIPS 140-2.
■ ISO/IEC 24759	27002

■ ISO/IEC 19792	Ein Bezug besteht natürlich einerseits zur ISO/IEC 15408 (auch Common Criteria), da auch diese ein allgemeines Kriterienwerk zur Evaluierung von Sicherheitsprodukten und –Systemen darstellen. Des Weiteren besteht ein enger Bezug zu Standards der WG5 aus der ISO/IEC JTC 1/SC 37, die sich mit den Testaspekten zu biometrischen Verfahren im Sinne ihrer Leistungsfähigkeit beschäftigen.
■ ISO/IEC 21827 (SSE-CMM)	SSE-CMM wurde ebenfalls als Fast Track in der ISO/IEC – als International Standard (IS) 21827 – eingereicht. Zu folgenden Standards besteht ein Bezug: ISO/IEC 12207, , ISO/IEC 15288, ISO/IEC TR 1504-2, ISO/IEC TR 1504-4, ISO/IEC 27002.

Schutzprofile

■ ISO/IEC TR 15446	Ein Bezug besteht unmittelbar zur ISO/IEC 15408 (Common Criteria), und dadurch indirekt zu weiteren damit zusammenhängenden Standards.

Spezielle Sicherheitsfunktionen 1: Normen zu kryptographischen und IT-Sicherheitsverfahren

Verschlüsselung

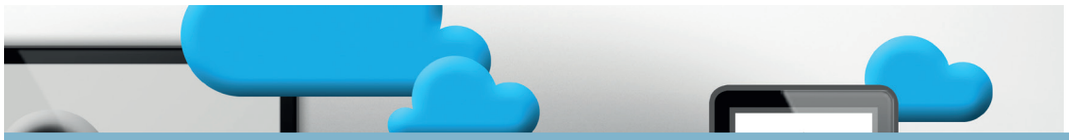
■ ISO/IEC 18033	ISO/IEC 10116
■ ISO/IEC 10116	ISO/IEC 8372, ANSI X3.106, FIPS Publication 81
■ ISO/IEC 19772	ISO/IEC 9796-2/6, ISO/IEC 9797-1/2, ISO/IEC 11770-1/4, ISO/IEC 14888-1/3, ISO/IEC 18033-1/4

Digitale Signaturen

■ ISO/IEC 9796	ISO/IEC 9797-2, ISO/IEC 10118-1/4, ISO/IEC 9798-1, ISO/IEC 14888-1/3
■ ISO/IEC 14888	ISO/IEC 8825-1, ISO/IEC 10118 (alle Teile), ISO/IEC 15946-1
■ ISO/IEC 15946	ISO/IEC 9796-3, ISO/IEC 11770-3

Hash-Funktionen und andere Hilfsfunktionen

■ ISO/IEC 10118	ISO/IEC 9797
■ ISO/IEC 18031	ISO/IEC 10116, ISO/IEC 10118-3, ISO/IEC 11770-1, ISO/IEC 18032, ISO/IEC 18033-3, ISO/IEC 19790
■ ISO/IEC 18032	ISO/IEC 18031



Authentifizierung

■ ISO/IEC 9798	ISO 7498-2, ISO/IEC 10181-2
■ ISO/IEC 9797	ISO 7498-2, ISO/IEC 10116, ISO/IEC 10118-1, ISO/IEC 10118-3

PKI-Dienste

■ ISO/IEC 15945	ISO/IEC 9594-8, ISO/IEC 9798-1, ISO/IEC 10118-1, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4, ISO/IEC 11770-1, ISO/IEC 11770-3, ISO/IEC 14888-2, ISO/IEC 14888-3 ISO/IEC 27002, ISO/IEC 13888-1, ISO/IEC 13888-2, ISO/IEC 13888-3 ISO/IEC TR 14516 ergänzt diesen Standard durch Richtlinien zur Nutzung und Management eines vertrauenswürdigen Dritten (in der Regel Trust Center).
■ ISO/IEC TR 14516	ISO/IEC 9594-8, ISO/IEC 10181-1, ISO/IEC 10181-4, ISO 7498-2, ISO/IEC IS 15945 ergänzt diesen TR durch die technische Spezifikation von Protokollen für solche Services.

Schlüsselmanagement

■ ISO/IEC 11770	ISO/IEC 9796-3, ISO/IEC 9798-2, ISO/IEC 9798-3, ISO/IEC 10118-1, ISO/IEC 10118-3, ISO/IEC 15946-1, ISO/IEC 18031, ISO/IEC 18032, ISO/IEC 18033-1

Kommunikationsnachweise

■ ISO/IEC 13888	ISO/IEC 9796, ISO/IEC 9797, ISO/IEC 10118 (alle Teile), ISO/IEC 14888 (alle Teile)

Zeitstempeldienste

■ ISO/IEC 18014	ISO/IEC 9798-1, ISO/IEC 10118-1, ISO/IEC 10118-2, ISO/IEC 10118-3, ISO/IEC 10118-4, ISO/IEC 11770-1, ISO/IEC 11770-3, ISO/IEC 14888-2, ISO/IEC 14888-3, ISO/IEC 15946-2

Spezielle Sicherheitsfunktionen 2: Physische Sicherheit

Technische Leitlinie 03400	Die Leitlinie prüft die Komponenten anhand von verschiedensten physischen Standards, die in der Leitlinie aufgeführt sind.

Brandschutz

■ DIN 4102	Es besteht Bezug zu vielen Normen, als dass sie einzeln hier aufgeführt werden könnten.
■ DIN 18095	DIN 4102-18:1991
■ DIN EN 1047	DIN EN 206-1, DIN EN 1363-1, DIN EN 1363-2, DIN EN 1364-1, DIN EN 1365-1, DIN EN 1365-2

Einbruchshemmung

■ DIN EN 1143-1	DIN EN 1300:2004
■ DIN V ENV 1627	DIN V ENV 1628, DIN V ENV 1629

Gehäuse

■ DIN EN 60529	IEC 60050-195:1998, IEC 60050-826:1982, IEC 60068-1:1988, IEC 60068-2-68:1994, IEC 60071-2:1996.

Links

BSI / IT-Grundschutz

Alle Unterlagen zum IT-GSHB findet man auf der Webseite des Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de).
Alle Unterlagen zum IT-Grundschutzhandbuch sind beim BSI unter www.bsi.bund.de/gshb/index.htm zu finden, sowohl der Leitfaden (http://www.bsi.bund.de/gshb/Leitfaden/index.htm) als auch das Grundschutztool (www.bsi.bund.de/gstool/index.htm).

CC

Der internationale Standard ISO/IEC 15408 steht kostenlos zur Verfügung, z. B. unter http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

FIPS 140-2

Der internationale Standard steht kostenlos zur Verfügung, z. B. unter csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

ISO

Informationen zur ISO-Organisation findet man auf der Webseite (www.iso.org).

ITTF

Informationen zu ISO/IEC Joint Technical Committee 1 (JTC 1) und dem Arbeitsprogrammen einzelner Unterkomitees des JTC 1 sowie zu prozeduralen Fragen findet man auf der Webseite (isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/ITTF.htm)

ISO/IEC JTC 1

Webseite des ISO/IEC Joint Technical Committee 1 (JTC 1): isotc.iso.org (siehe dann: Home, dann: ISO/IEC 001 JTC 1 »Information technology)

ISO/IEC JTC 1/SC 27

Informationen über das ISO/IEC-Unterkomitee ISO/IEC JTC 1/SC27 »IT Security techniques« sind unter www.jtc1sc27.din.de/en verfügbar

SD 6 »Glossary of IT Security Terminology«

Standing Document 6 (SD6) – Glossary of IT Security Terminology ist verfügbar unter www.jtc1sc27.din.de/sce/sd6 (siehe dann: Downloads)

SD 7 »Catalogue of SC27 Projects and Standards«

Standing Document 7 (SD7) – ISO/IEC JTC 1/SC27 Catalogue of Projects and Standards kann heruntergeladen werden unter www.jtc1sc27.din.de/sce/sd7 (siehe dann: Download)

NIST

Das National Institute of Standards and Technology des US Handelsministerium hat eine Webseite unter www.nist.gov

DIN

Informationen über die Tätigkeiten des Deutschen Institut für Normung findet man auf der Webseite (www.din.de).

DIN NI

Informationen über den DIN-Normenausschuss »Informationstechnik« (NI) und seine Arbeitsausschüsse sind unter www.nia.din.de verfügbar

DIN VDE

Das VDE-Vorschriftenwerk umfasst Satzungen und sonstige Grundsatzschriftstücke des VDE, DIN VDE-Normen (VDE-Bestimmungen), VDE-Leitlinien und Beiblätter zu den vorgenannten Schriftstücken (www.vde-verlag.de/normen.html)

ISACA

Information Systems Audit and Control Association – Verband Internationaler Auditoren der Informatik. Der Cobit Standard kann kostenlos bei www.isaca.de heruntergeladen werden.
(Es existiert nur von der Version 4.0 eine deutschsprachige Fassung)

6 Ausblick – so geht's weiter

Mit dieser Sonderauflage zur it-sa 2013 haben die Autoren in aktuelle Entwicklungen zur Standardisierung von Sicherheitsprozessen eingeführt und Ihnen als Leser (hoffentlich) die strategischen Dimensionen des Themas Sicherheitsstandards vermittelt. Die vorliegende Auswahl der Standards beschreibt dabei nur einen Teil der verfügbaren Standards. Weitere Standards finden Sie auf der Kompass-Internetseite.

Mit den Möglichkeiten des Internets verbunden sind ebenfalls eine Reihe von Eigenschaften, die dazu beitragen, den Kompass der IT-Sicherheitsstandards kontinuierlich zu erweitern und für Sie noch nutzbarer zu machen. Neben fortlaufenden Aktualisierungen profitieren Sie online auch von komfortablen Möglichkeiten zur Qualitätsverbesserung des »Kompass der IT-Sicherheitsstandards« beizutragen und sich mit Ihren Anmerkungen und Anregungen aktiv einzubringen. Wir freuen uns auf Ihre Rückmeldungen und wünschen Ihnen abschließend eine gute Lektüre unter:
www.kompass-sicherheitsstandards.de

Auch die Online-Version sowie dieser Sonderdruck des Leitfadens »Kompass der IT-Sicherheitsstandards« entstanden durch die enge Zusammenarbeit zwischen BITKOM und DIN. Allen Beteiligten danken wir für die Mitarbeit, die diese Ausgabe ermöglicht hat, sehr herzlich auf unserer Webseite.

Notizen

BITKOM

DIN

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 2.000 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

Das DIN ist ein eingetragener gemeinnütziger Verein mit Sitz in Berlin (DIN Deutsches Institut für Normung e. V., gegründet 1917). Das DIN ist die für die Normungsarbeit zuständige Institution in Deutschland und vertritt die deutschen Interessen in den weltweiten und europäischen Normungsorganisationen. Dieser Status wurde im Vertrag mit der Bundesrepublik Deutschland am 5. Juni 1975 anerkannt.
Das DIN ist der runde Tisch, an dem sich Hersteller, Handel, Verbraucher, Handwerk, Dienstleistungsunternehmen, Wissenschaft, technische Überwachung, Staat, d. h. jedermann, der ein Interesse an der Normung hat, zusammensetzen, um den Stand der Technik zu ermitteln und unter Berücksichtigung neuer Erkenntnisse in Deutschen Normen niederzuschreiben.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

DIN

Deutsches Institut der Normung e.V.
Normenausschuss Informationstechnik und Anwendung (NIA)

Burggrafenstraße 6
10787 Berlin
Telefon 030/2601-0
Telefax 030/2601-1231
nia@din.de
www.nia.din.de