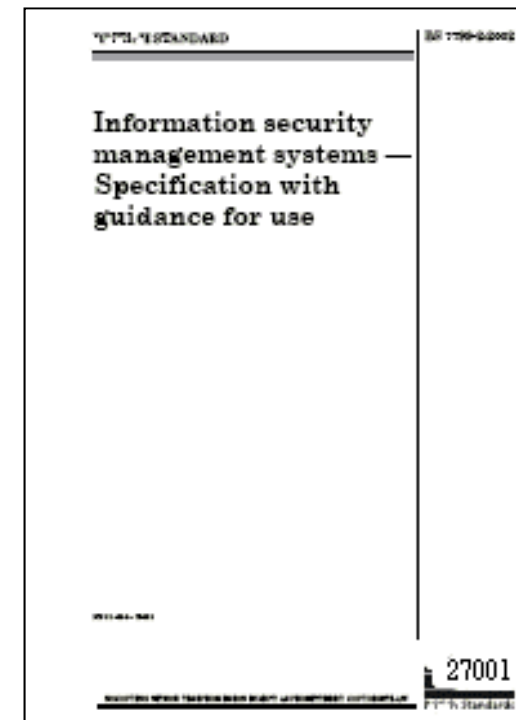




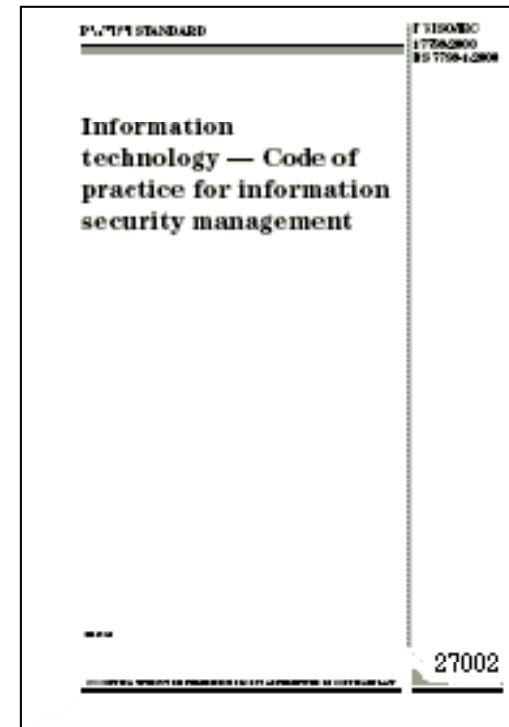
# Ansätze zum Informationssicherheitsmanagement und Informationssicherheits-Standards

### ■ ISO/IEC 27001 ...

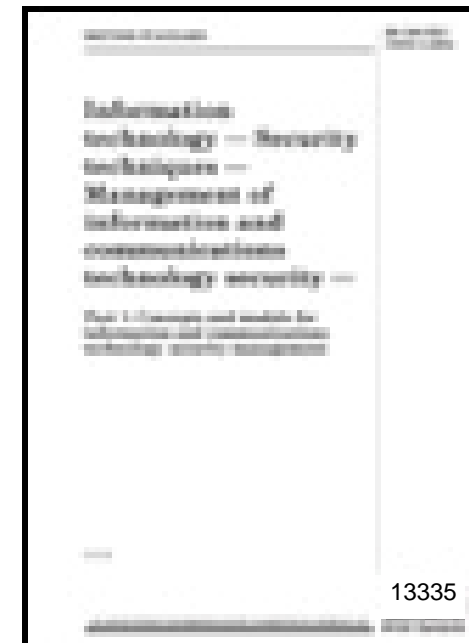
- Spezifiziert Anforderungen an Informationssicherheits-Managementssysteme (ISMS).
- Ist anwendbar in Organisationen jeglicher Art, Ausprägung und Größe.
- Kann als Grundlage für Vertragsbeziehungen zwischen Organisationen benutzt werden.
- Erlaubt die Implementierung und den Betrieb von integrierten Managementsystemen für Informationssicherheit (ISO 27001), Qualität (ISO 9001) und Umwelt (ISO 14001).
- Zertifizierung: Möglich.



- ISO/IEC 27002 ...
  - Ist „nur“ ein Leitfaden (keine Spezifikation, kein Zertifizierungsstandard).
  - Ergänzung zur ISO 27001 (Detaillierung der normativen Anlage A).
  - Dient zum besseren Verständnis der in der ISO 27001, Anlage A definierten Anforderungen.
  - Basis zur Entwicklung von organisationseigenen Verfahren und Regelungen.
  - Zertifizierung: Nicht möglich.



- ISO 13335 (-1, -2 und -5) ...
  - Allgemeine Leitlinie für die Initiierung und Umsetzung von IT-Sicherheits-Managementprozessen.
  - Zurzeit bei ISO in Überarbeitung:
    - Teil 1: Concepts and models for managing and planning ICT security (veröffentlicht, ersetzt die alten Teile 1 und 2)
    - Teil 2: Information security risk management (in Überarbeitung, soll die aktuellen Teile 3 und 4 ersetzen)
    - Teil 5: Management guidance on IT network security (in Überarbeitung, wird den aktuellen Teil 5 ersetzen).
  - Wird voraussichtlich komplett in ISO 27000ff. (und ggf. weitere Standards) einfließen.
  - Zertifizierung: Nicht vorgesehen.



- Basieren auf den in der Praxis bewährten
  - IT-Grundschutzhandbuch und
  - IT-Grundschutz-Vorgehensweise

<http://www.bsi.bund.de/gshb>



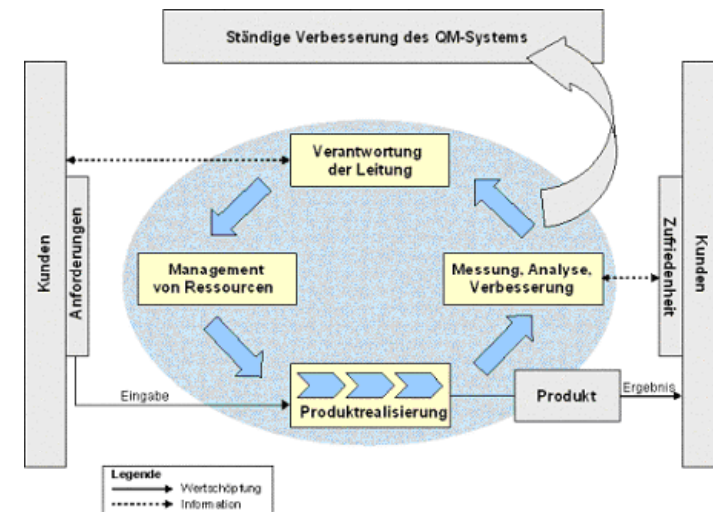
BSI-Standards

+



Loseblattsammlung

- Titel: „Anforderungen an Qualitäts-Managementsysteme“
- Inhalt: U. a. Anforderungen mit IT-Sicherheitsrelevanz:
  - Sicherstellung der Verfügbarkeit von Ressourcen und Informationen
  - Kennzeichnung, Schutz und Verfügbarkeit von Aufzeichnungen
  - Bereitstellung und Aufrechterhaltung der Infrastruktur, z. B. Prozessausrüstungen in Form von Hard- und Software
  - Schutz des Kundeneigentums.
- Zertifizierung: Möglich.



- Titel: „**Control *OB*jectives for Information and related *T*echnology**“
- Inhalt: Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben:
  - Auf Revision und Controlling orientierter Kontrollrahmen für das Management, die Ergebnis- und Leistungsmessungen für alle IT-Prozesse
  - Beschreibt mehrere Prozessbereiche jeweils mit definierten Kontrollzielen, Reifegradmodell und Messgrößen
  - Wird insbesondere von Wirtschaftsprüfern im Rahmen der Jahresabschlussprüfung zur Prüfung des IT-Kontrollumfelds eingesetzt.
- Zertifizierung: Keine möglich (im engeren Sinne).



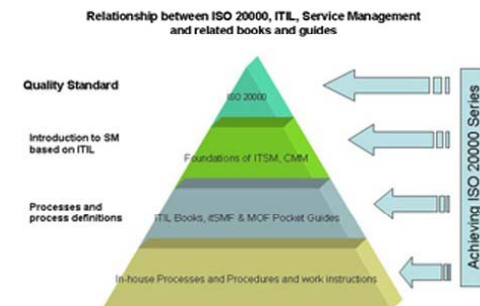
- Titel: „*IT Infrastructure Library*„ (aktuell: ITIL V3)
- Inhalt:
 

Sammlung mehrerer Bücher zum Thema IT-Service-Management aus Sicht eines IT-Dienstleisters:

  - Übergreifendes Ziel ist die Optimierung der Qualität und der Kosteneffizienz von IT-Services
  - IT-Sicherheitsmanagement-Prozess im Buch „Service Design“.
- Zertifizierung: Für Mitarbeiter möglich (nicht für Unternehmen).



- Titel: „*IT-Service-Management*“
- Inhalt:
  - Anforderungen an (interne oder externe) IT-Organisationen hinsichtlich der Erbringung von prozessorientierten Dienstleistungen in einer für die Kunden akzeptablen Qualität
  - Services of an acceptable quality for ist customers.
- Normteile:
  - **ISO 20000-1** (ehemals **BS 15000-1**) spezifiziert **Anforderungen** an das Management von IT-Services
  - **ISO 20000-2** (ehemals **BS 15000-2**) ist ein **Leitfaden** („Code of Practice“) für IT-Service-Management.
- Zertifizierung: Möglich.



- Titel: „*The ISF’s Standard of Good Practices for Information Security*“
- Inhalt:
 

„Good practice“ Ansatz für die betriebliche Informations-sicherheit, der auch ein „security benchmarking“ erlaubt.  
Behandelt fünf Themenbereiche der Informationsgeschäftlicher Perspektive:

  - IT-Sicherheitsmanagement,
  - Geschäftskritische Anwendungen,
  - Informationsverarbeitung,
  - Kommunikation/Netze und
  - Systementwicklung.
- Zertifizierung: Keine möglich (im engeren Sinne).



- Titel: „*Datenschutz-Gütesiegel beim Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein*“
- Inhalt:
 

Standard zur Prüfung und Zertifizierung einzelner IT-Produkte, basierend auf Begutachtung aus rechtlicher und technischer Sicht durch vertraglich gebundene, externe Sachverständige:

  - Das Datenschutz-Gütesiegel bescheinigt, dass das Produkt ohne erheblichen Aufwand datenschutzgerecht eingesetzt werden kann und dass es keine Funktionen enthält, die gegen bestehende Datenschutzbestimmungen verstoßen oder sicherheitstechnisch unzureichend sind.
- Zertifizierung: Möglich.



- Titel: „*Requirements for Cryptographic Modules*“
- Inhalt:
 

Vorschriften und Kriterien zur speziellen Evaluierung von Kryptomodulen:

  - Für Hersteller und Evaluatoren solcher Module interessant, wenn sie sich an FIPS 140-2 anlehnen wollen
  - Sicherheitsanforderungen enthalten zehn Themenbereiche, die sich auf das Design und die Implementierung eines kryptographischen Moduls beziehen
  - Die meisten Themenbereiche erfordern ein „security level rating“ zwischen 1 und 4; für die anderen müssen alle Anforderungen erfüllt werden.
- Zertifizierung: Möglich.



- Titel: „*Information Technology Security Evaluation Criteria*“
- Inhalt:
 

In mehreren europäischen Ländern übereinstimmend geltende Kriterien für die Bewertung der Sicherheit von Systemen oder Systemkomponenten der Informationstechnik:

  - Prüfung und Bewertung von IT-Produkten und -Systemen nach einheitlichen Kriterien durch unabhängige Stellen
  - Kriterien: Funktionalität und Vertrauenswürdigkeit
  - Evaluationsstufe: *E1* bis *E6*
  - Mechanismenstärke: *niedrig, mittel* und *hoch*.
- Zertifizierung: Möglich.

- Titel: „*Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik*“
- Inhalt:
 

Weiterentwickelte und harmonisierte Sicherheitskriterien, resultiert aus den europäischen Kriterien (ITSEC), dem Orange-Book (TCES) der USA und den kanadischen Kriterien (CTCPEC)

  - Korrektheitsprüfung aller Sicherheitsfunktionen (auf mehreren Spezifikationsebenen)
  - Wirksamkeitsprüfung der Sicherheitsmaßnahmen (z. B. durch Penetrationstests)
  - Prüfung der Entwicklungsumgebung und des Betriebs.
- Zertifizierung: Möglich