secianus

Informationssicherheitszertifizierung von Leitstellen

Zertifizierung im Spannungsfeld von ISO▪27001 auf Basis IT-Grundschutz und KRITIS-Gesetzgebung

Zertifizierungen und Mitgliedschaften

secianus

Sachverständige für Datenschutz und Informationssicherheit

Bundesamt für Sicherheit in der Informationstechnik

Zertifizierter IT-Sicherheitsdienstleister

Zertifikat Nummer: BSI-APS-9037 gültig bis 28.02.2025

Horst Pittner
Qualifikationen und Erfahrungen

Geschäftsführender Gesellschafter der SECIANUS GmbH & Co. KG

Vom Bundesamt für Sicherheit in der Informationstechnik zertifizierter

- Lead-Auditor für ISO 27001 auf Basis IT-Grundschutz
- IS-Revisor
- Prüfer für Kritis-Unternehmen gemäß §8a BSI-Gesetz.

Tätig:

- Seit 1985 in der EDV
- Seit 2001 in der IT-Sicherheit
- Seit 2003 als Auditor
- Seit 2005 in der Informationssicherheit
- Seit 2005 im Datenschutz

Schwerpunkte:

- Behörden
- Industrie
- SAP-Systeme

Erfahrungen:

- Ab 1985 als Systemanalytiker und Programmierer für technische Software
- Ab 1991 als Netzwerk-Architekt für die Großindustrie
- Ab 1994 als SAP R/3 Systemarchitekt und Systemmanager
- Ab 2001 in der IT-Sicherheit
- Ab 2003 als Grundschutzauditor
- Ab 2005 als Lead-Auditor für ISO 27001 auf Basis IT-Grundschutz

Inhalt

Informationssicherheitszertifizierung von Leitstellen

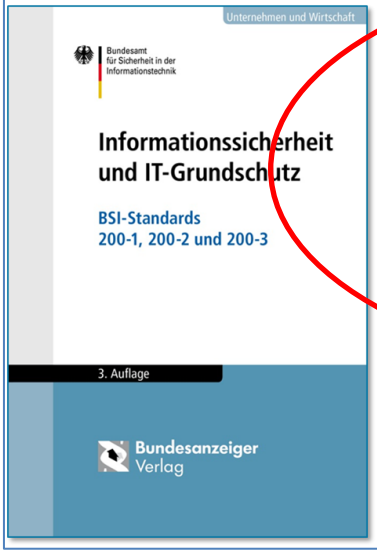
- Warum Zertifizieren, nach welchem Standard
- Was bedeutet ISO 27001 auf Basis IT-Grundschutz und KRITIS
- Wie geht eine Zertifizierung
- Wo sind die Fallstricke
- Empfehlungen
- Resümee

Warum Zertifizieren, nach welchem Standard

- IT-Sicherheitsgesetz (IT-SiG 2.0)
  - Staat und Verwaltung – Notfall und Rettungswesen einschließlich Katastrophenschutz
  - Kritische Infrastruktur gemäß BSI KRITIS-Verordnung
    - Gesundheit - Medizinische Versorgung
  - Verpflichtung zur Einführung eines Informationssicherheitsmanagementsystems (ISMS)
  - IT-Systeme (IT-Sicherheit) MÜSSEN nach dem Stand der Technik ausgeführt sein.
- Grundlage für den Anschluss an Digitalfunk BOS (ohne Zertifizierung)
- Bayern - IT-Sicherheitsrahmenkonzept vom 10.04.2017
  - Vorgabe **ISO 27001 auf Basis IT-Grundschutz**

Was bedeutet ISO 27001 auf Basis IT-Grundschutz und KRITIS

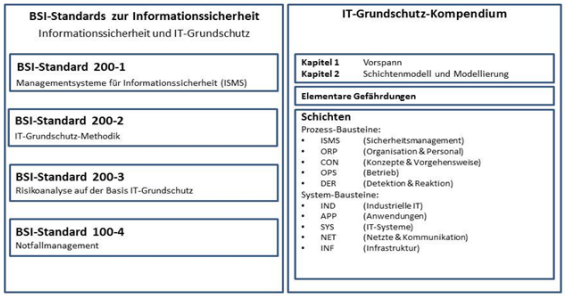
BSI-Sicherheitsstandards



BSI-Standard 200-1:	Managementsysteme für Informationssicherheit (ISMS)
BSI-Standard 200-2:	IT-Grundschutz-Methodik
BSI-Standard 200-3:	Risikomanagement
BSI-Standard 200-4:	Notfallmanagement

Was bedeutet ISO 27001 auf Basis IT-Grundschutz und KRITIS

Aufbau und Betrieb eines Managementsystems für Informationssicherheit (ISMS) in der Praxis



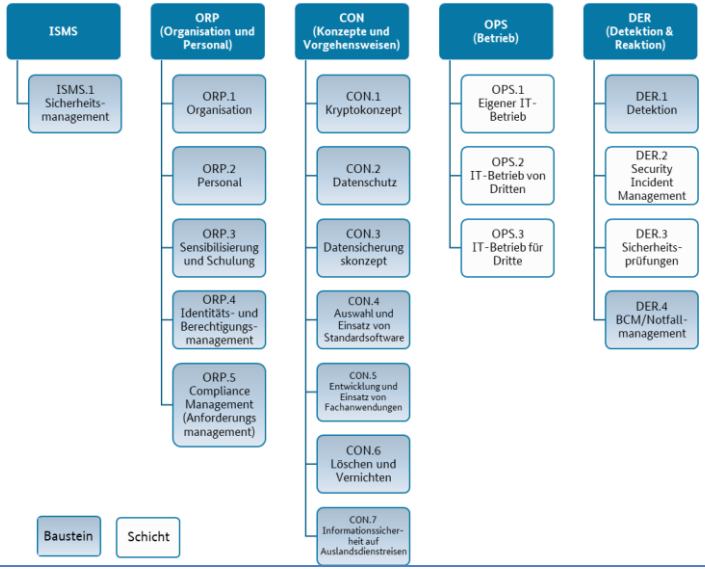
Anleitungen zu:

- Aufgaben des Informationssicherheitsmanagements
- Etablierung einer Informationssicherheitsorganisation
- Erstellung eines Sicherheitskonzepts
- Auswahl angemessener Sicherheitsmaßnahmen
- Informationssicherheit aufrecht erhalten und verbessern

© BSI

Was bedeutet ISO 27001 auf Basis IT-Grundschutz und KRITIS

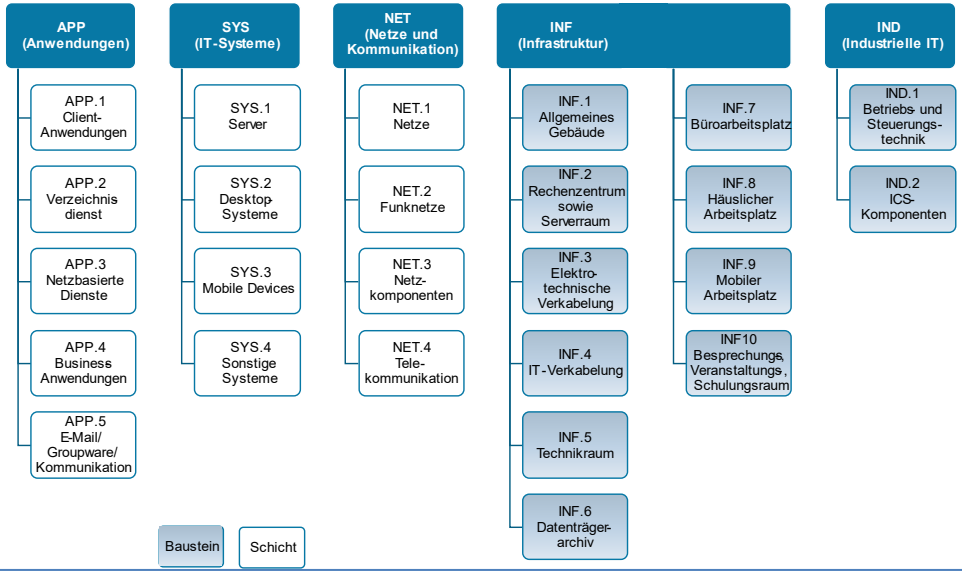
Struktur IT-Grundschutz-Kompendium
Prozess-Bausteine



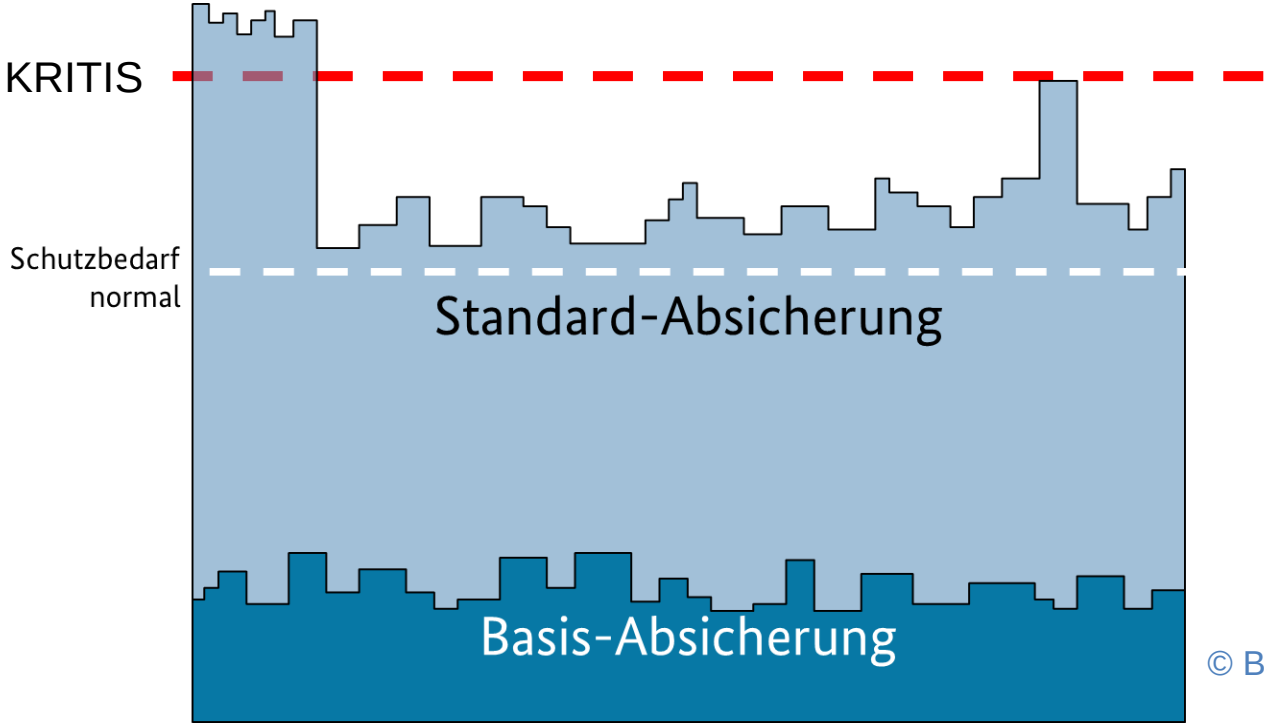
© BSI

Struktur IT-Grundschutz-Kompendium

System-Bausteine



Was bedeutet ISO 27001 auf Basis IT-Grundschutz und KRITIS

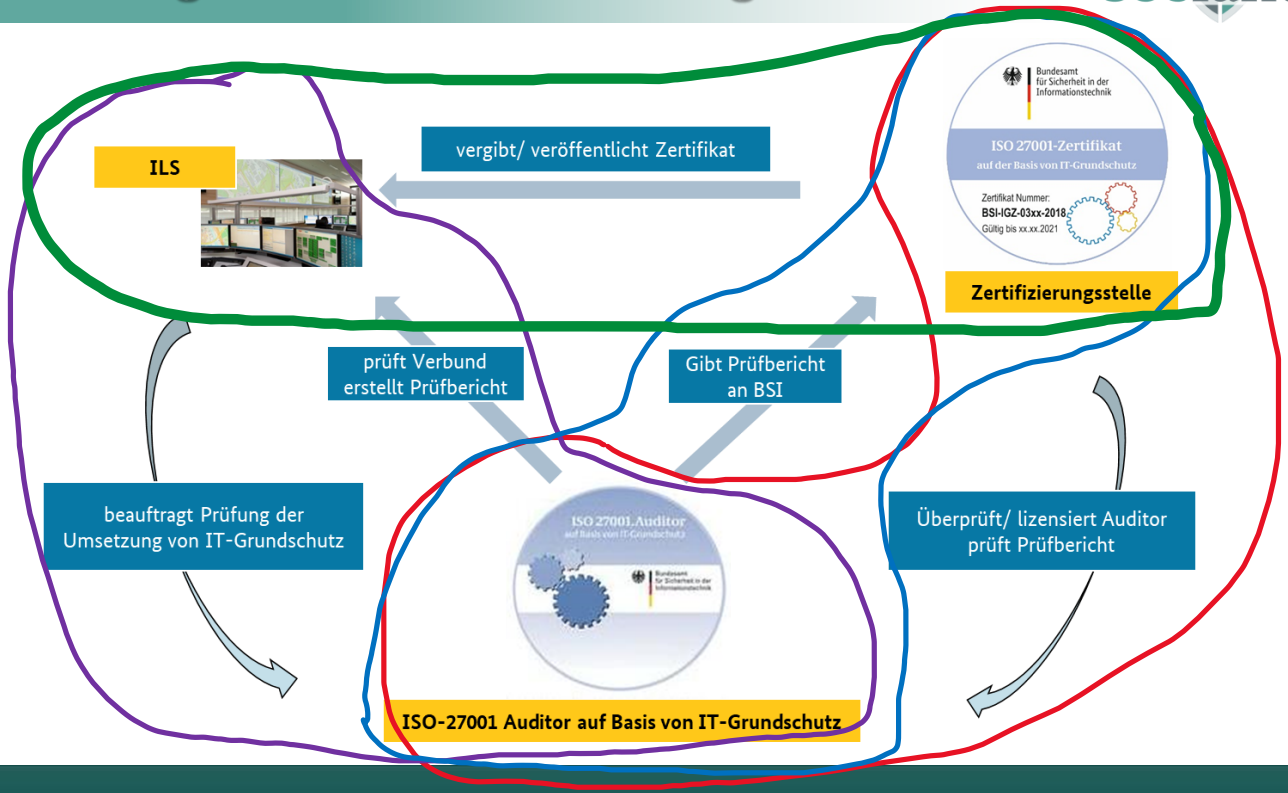


© BSI

Was bedeutet ISO 27001 auf Basis IT-Grundschutz und KRITIS

- Informationssicherheitsmanagementsystem
  - Bei der ILS als Betreiber
  - Bei den Dienstleistern, wenn diese im laufenden Betrieb einen Service zu erbringen haben
    (Fernwartung, Software-Updates, Hardware-Tausch …)
  - Bei den Lieferanten, wenn diese kritische Systeme liefern
  - Bei den Planern, wenn diese sensible Informationen über geplante ILS-Maßnahmen besitzen.
- Sicherheitskonzepte über sämtliche IT-Komponenten hinweg.
  - Härtung sämtlicher IT-Komponenten gemäß Grundschutzkompendium

Wie geht eine Zertifizierung



Wo sind die Fallstricke

- Beherrschung des Informationsverbundes
- Vorgaben der Ministerien / Städten / Bedarfsträgern
  - Einbindung von Services anderer Dienststellen.
- Dienstleistersteuerung
  - Einfluss auf die Dienstleister vorhanden?
    - Verträge werden landesweit (Bayern) oder gruppenweit ausgehandelt.
    - Veralteter Grundschutz wurde geliefert.
  - Dienstleister sind intern nicht sicher aufgestellt.
    - Umsetzung der relevanten Bausteine muss nachgewiesen werden.
- Monitoring und Protokollierung
  - Security Information and Event Management (SIEM)
  - Firewall-Protokolle auswerten

Wo sind die Fallstricke

- Physische Sicherheit (Grundschutz <> KRITIS)
  - Wer ist zuständig?
    - Perimeterschutz
    - Gebäudesicherheit
    - Serverräume
    - Leitstellenräume
  - Wer gibt die Regelungen vor?
    - Zutrittskontrolle
    - Sabotageschutz
    - Brandschutz
  - Wer prüft und überwacht?

Empfehlungen

- Planer und Lieferanten sollten sich auf eine eigene Zertifizierung vorbereiten.
- „Lex Huawei“
  - Kritische Komponenten dürfen nur nach einer Zertifizierung eingesetzt werden (§ 109 Abs. 4 TKG).
  - KRITIS-Betreiber müssen den geplanten Einsatz einer kritischen Komponente dem BSI anzeigen (§ 9b BSIG)
  - Einsatz kann vom BSI untersagt werden.
- Die Verwendung des Grundschutzprofils für Leitstellen erleichtert die Arbeit.

Resümee

- Die Informationssicherheit ist Chef-Sache.
- Die ISO 27001 auf Basis IT-Grundschutz ist in der Lage die Anforderungen an einen KRITIS-Verbund abzubilden.
- KRITIS-Anforderungen MÜSSEN in das ISMS und den Informationsverbund einfließen.
- Die Informationssicherheit gemäß Grundschutz und KRITIS MUSS sowohl von den Leitstellen als auch von den Dienstleistern / Lieferanten gewährleistet werden.
- Die Verwendung des Grundschutzprofils für Leitstellen ist für alle Beteiligten hilfreich.

Digital unterschrieben von Horst Pittner
Datum: 2022.10.02 13:16:38 +02'00'

Vielen Dank

SECIANUS GmbH & Co. KG

Further Straße 14
D-90530 Wendelstein

Tel.: +49 (0) 9129 29 39 808

eMail: info@secianus.de
Internet: www.secianus.de