Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz

22. Juni 2026

Standards zur Informationssicherheit und zum Datenschutz

Heiko Behrendt
Experte für Datenschutz und Informationssicherheit
ISO 27001, ISO 27701 Lead-Auditor, Fachbegutachter der DAkkS
0179 2184795 - mail@heiko-behrendt.de - https://www.heiko-behrendt.de

Niemeyerweg 2 - 24226 Heikendorf

0179 218 47 95

https://www.datenschutz-expert.de

mail@datenschutz-expert.de oder mail@heiko-behrendt.de

Prüfer, Gutachter und Berater für Datenschutz und Informationssicherheit beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, ISO/IEC 27001, ISO/IEC 27017+18 und ISO/IEC 27701 Leadauditor der datenschutz cert GmbH, Fachbegutachter der Deutschen Akkreditierungsstelle (DAkkS) für Zertifizierungsstellen und Produkte.

In der Funktion als Datenschutz- und Informationssicherheitsexperte einer Aufsichtsbehörde führe ich bei Organisationen Datenschutz- und Informationssicherheits-**Audits** sowie datenschutzrechtliche **Kontrollen** der Einhaltung der Datenschutzgrundverordnung (DSGVO) durch. Darüber hinaus begleite ich als ISO 27001 Auditor Organisationen bei der Umsetzung und Aufrechterhaltung der **Zertifizierung** ihres Informationssicherheitsmanagements (ISMS). Die **Ausbildung** von Datenschutzbeauftragten und die **Überprüfung** der Datenverarbeitung auf vorhandene technische und organisatorische Schwachstellen gehören zu meinen Schwerpunkten.

Als **ISO 27001 Auditor** führe ich Audits z. B. in folgenden Sektoren durch:

- Colocation-, Hyperscale- und Cloud-Rechenzentren
- IT- und Consulting-Dienstleister
- Softwareentwicklung
- Gesundheitswesen
- Immobilienmanagement
- Rennwettgesellschaften

Als **Referent** führe ich Lehrtätigkeiten bei folgenden Institutionen durch:

- KEDUA GmbH in Berlin
- Fortbildungskampagne öffentliches Recht in Berlin
- Studieninstitut für kommunale Verwaltung Westfalen-Lippe in Münster
- Christian-Albrechts-Universität zu Kiel im Studiengang Informatik
- Datenschutzakademie Schleswig-Holstein
- Berufsverband der Datenschutzbeauftragten Deutschlands

Informationsquellen

- VdS Schadenverhütung GmbH
  https://vds.de
- Informationssicherheitsmanagementsystem (ISMS) in 12 Schritten
  https://cisis12.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi.bund.de/DE/Home/home_node.html
- ISO: Global standards for trusted goods and services
  https://www.iso.org
- National Institute of Standards and Technology (NIST)
  https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Inhalte

- Datenschutz und Informationssicherheit
- Datenschutz- und Informationssicherheitsmanagement
- Gefährdungen, Risiken und Maßnahmen
- Standards zur Informationssicherheit und zum Datenschutz
  - VdS
  - CISIS12
  - IT-Grundschutz
  - ISO 27001
  - ISO 27701
  - NIST 800-53

Hinweis: Der Inhalt des Vortrags stellt die persönliche Rechtsauffassung des Referenten anhand der Gesetzesmaterialien dar. Informationen zur Umsetzung der Inhalte sind als Empfehlungen und bewährte Vorgehensweisen (best practice) zu verstehen.

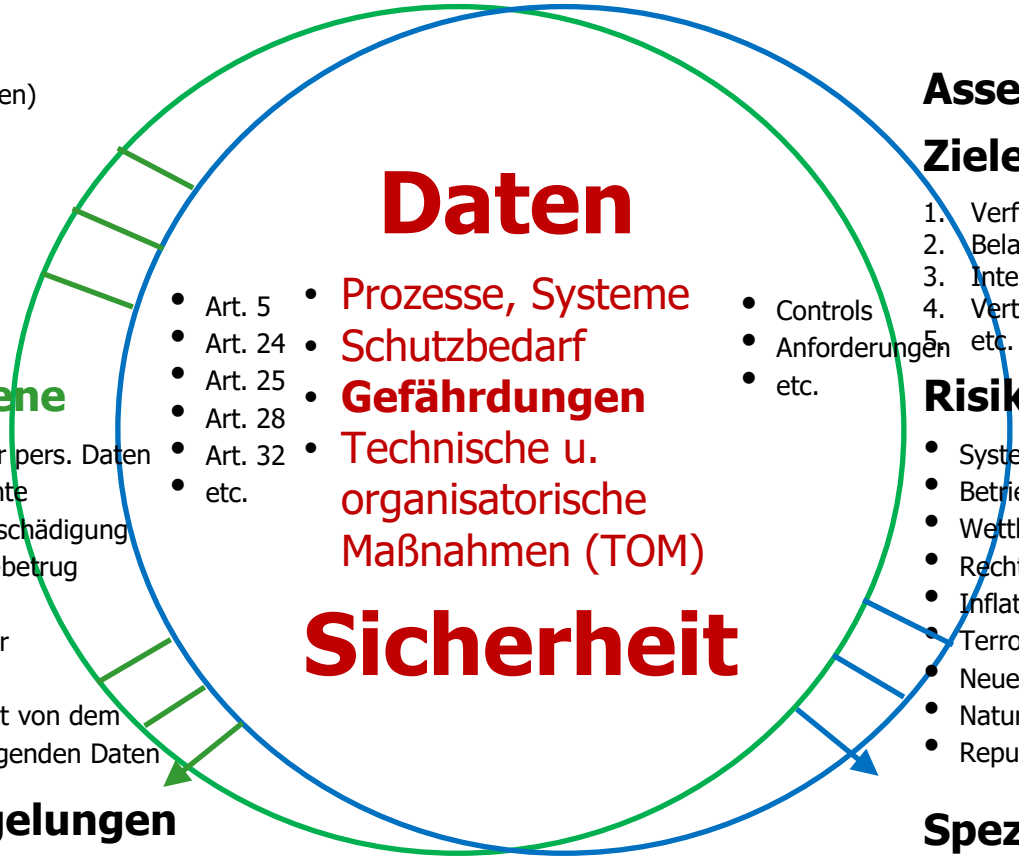
Datenschutz und Informationssicherheit

Kombination – Synthese

Datenschutz DSGVO
Datenschutzanforderungen

Organisation

Informationssicherheit
ISMS ISO 27001



Daten (personenbezogen)

Ziele

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit
4. Transparenz
5. etc.

Risiken Betroffene

- Verlust der Kontrolle über pers. Daten
- Einschränkung ihrer Rechte
- Diskriminierung oder Rufschädigung
- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- Unbefugte Aufhebung der Pseudonymisierung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

Spezifische Regelungen

- Betroffenenrechte, Informationspflichten
- Datenschutz-Folgenabschätzung
- Verzeichnis der Verarbeitungstätigkeiten
- etc.

Assets/Werte

Ziele

1. Verfügbarkeit
2. Belastbarkeit
3. Integrität
4. Vertraulichkeit
5. etc.

Risiken Unternehmen

- Systemausfall, Viren, Hackerangriffe
- Betriebsunterbrechung
- Wettbewerber Konkurrenz
- Rechtliche Veränderungen
- Inflation
- Terrorismus
- Neue Technologien
- Naturkatastrophen
- Reputationsverlust

Spezifische Regelungen

- ISO 27002 Leitfaden für ISO 27001
- ISO 27005 Risikomanagement
- ISO 27017+18 Cloud
- ISO 27701 Datenschutz
- BSIG (Kritische Infrastruktur)
- etc.

Datenschutz- und Informationssicherheitsmanagement

Datenschutz auf der Basis eines Standards zur Informationssicherheit – **DISM**

	Datenschutzmanagement **DSGVO**		**Informationssicherheitsmanagement** **Standard**
ZWECK	- **Schutz des Einzelnen** vor dem Missbrauch **personenbezogener** Daten - Schutz des informationellen Selbstbestimmungsrechts der betroffenen Personen		- **Schutz der Prozesse und der Informationen des Unternehmens bzw. der Behörde** - Festlegung von Assets/Werten
	Datenschutzrecht	**Datensicherheit**	**Informationssicherheit**
KERNELEMENTE	- Datenschutzgrundverordnung - Landesdatenschutzgesetz - Bundesdatenschutzgesetz - Bereichsspezifische Gesetze z.B. SGB - Grundsätze der Datenverarbeitung - Zulässigkeit der Datenverarbeitung - Zweckbindung - Transparenz - Datenvermeidung und Datensparsamkeit - Nachweispflicht - Rechte der Betroffenen - Informationspflichten - Datenschutz-Folgenabschätzung - Datenschutzbeauftragte(r) - Ordnungswidrigkeiten	- Risikoanalyse - Schutzbedürftigkeit - Datenschutz durch Technikgestaltung und Voreinstellungen - Technische und organisatorische Sicherheitsmaßnahmen - Dokumentation der Datenverarbeitungsprozesse - Überwachung und Audits	- Leitlinie für Informationssicherheit - IT-Sicherheitsbeauftragte(r) - Abgrenzung der Datenverarbeitung - Schutzbedarfsfestlegung - Grundschutzmaßnahmen - Basis- oder Standardabsicherung - Risikoanalyse - Sicherheitsmaßnahmen für hohen Schutzbedarf - Dokumentation d. Sicherheitsprozesse - Überwachung und Audits
§	- Datenschutzvorschriften müssen Behörden und Unternehmen beachten!		- Keine gesetzliche Vorschrift

Datenschutz auf der Basis eines Standards zur Informationssicherheit

Datenschutz- u. Informationssicherheitsmanagement

Basis: DISM-Team

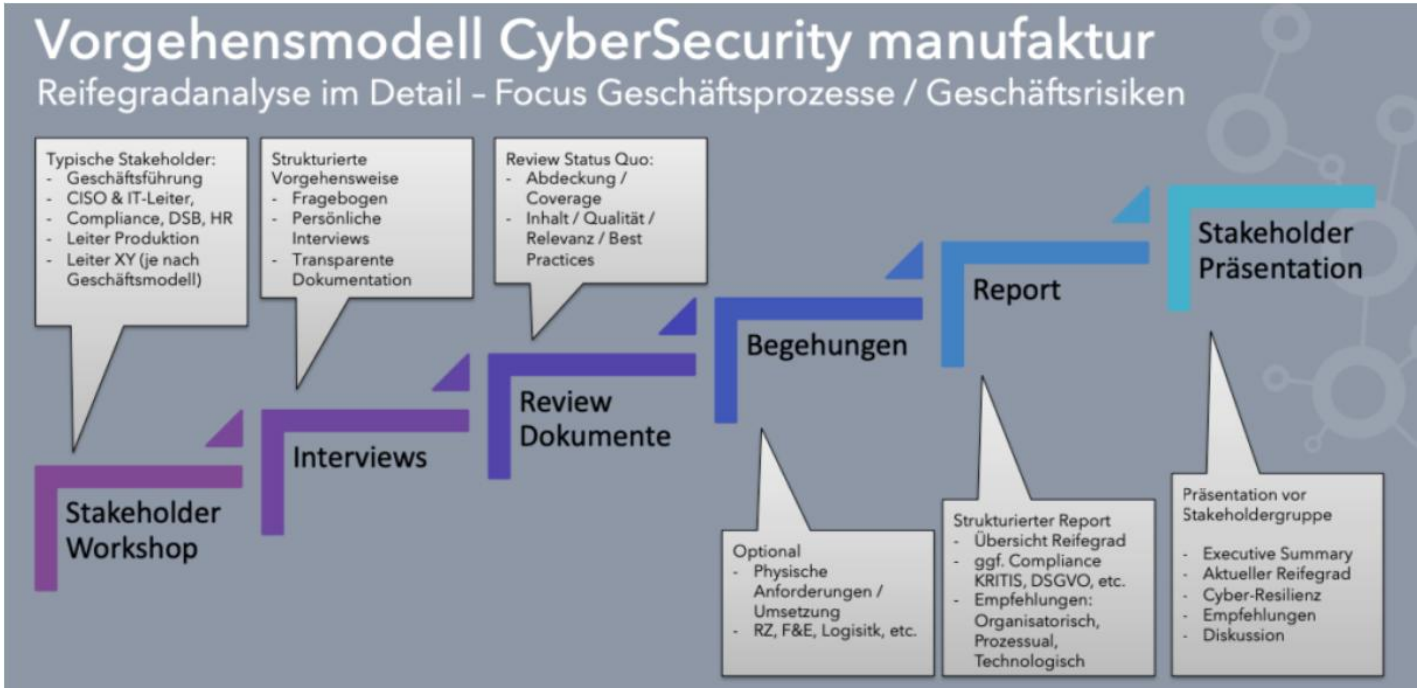
Abhängig von der **Größe** der Organisation:

- Mindestens ein „**Datenverantwortlicher**“ (Behörden- oder Abteilungsleiter, Geschäftsführer)
- Datenschutzbeauftragter
- Informationssicherheitsbeauftragter
- Leiter IT-Abteilung
- Ggf. Koordinatoren in den Fachabteilungen
- Ggf. Leiter Revisionsabteilung
- Ggf. Personal- bzw. Betriebsrat
- Ggf. DSB von Auftragsverarbeiter
- …

Quelle: https://pixabay.com

Durchführung eines Sicherheitschecks

1. Vorbereitung Sicherheitscheck (Bestandsaufnahme, Scope)
2. Sicherheitscheck vor Ort – Gefährdungen, Risiken und Maßnahmen verifizieren
3. Ergebnis – Bewertung
4. Sicherheitsniveau erhöhen, anpassen



Quelle: https://cybersecurity-manufaktur.com/

Risiken aus Gefährdungen ableiten und bewerten?

Datenschutz

Risiken Betroffene (ErwG. 75 DSGVO)

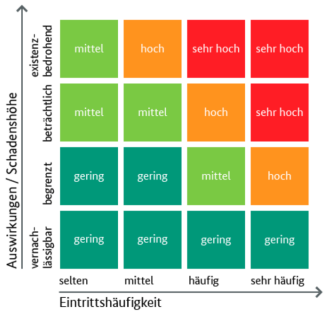
- Verlust der Kontrolle über pers. Daten
- Einschränkung ihrer Rechte
- Diskriminierung oder Rufschädigung
- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- Unbefugte Aufhebung der Pseudonymisierung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

Informationssicherheit

Risiken des Unternehmens

- Systemausfall, Viren, Hackerangriffe
- Betriebsunterbrechung
- Wettbewerber Konkurrenz
- Rechtliche Veränderungen
- Inflation
- Terrorismus
- Neue Technologien
- Naturkatastrophen
- Reputationsverlust
- Finanzieller Schaden

Gefährdung – Risiko – Maßnahme(n)



DATEN – ASSETS

z. B. Geschäftsdaten

↓

Anforderungen/Schutzbedarf

Informationssicherheitsstandard

Gefährdung ⟷ **Maßnahme(n)**

z. B. Vireninfizierung mit Ransomware | **z. B. Antivirenschutzsoftware**

↓ | ↓

Risiko hoch = Eintrittswahrscheinlichkeit / Schadenshöhe = Risiko gering

---

Ziel: Informationssicherheit und Datenschutz sollen gewährleistet werden!

- Aus den **festgestellten** Gefährdungen werden die Risiken ermittelt
- Die **Maßnahmenauswahl**/-gewichtung ergibt sich jeweils aus der **Risikokritikalität**
- Je höher die **Schadensauswirkung**, desto **belastbarer** müssen die Maßnahmen sein
- Die Maßnahmen dokumentieren die **Umsetzung der Anforderungen des Standards** und den Schutz der Daten

Schadenskalkulation – Worst-Case!

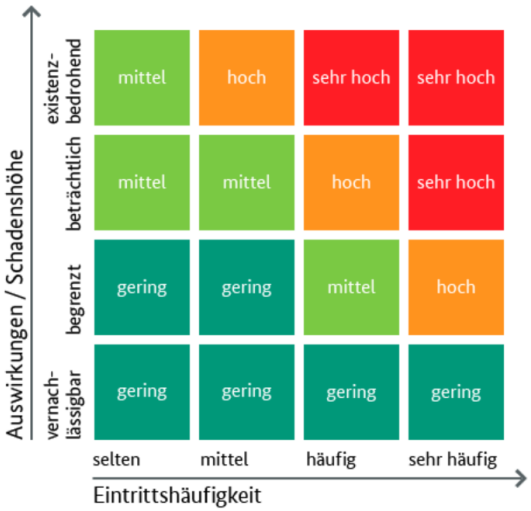
1. Welcher finanzielle **Schaden** ist für das Unternehmen **kritisch**?
2. Wie wahrscheinlich ist der **Eintritt** eines Schadens?

	1.000 €
	10.000 €
	50.000 €
	100.000 €
Zahlungsunfähig?!	**200.000 €**
	500.000 €

Beispiel Schadenskalkulation

1.	**Lösegeld** bei Ransomware-Angriff	200.000 €
2.	**Verschlüsselte** Speichermedien – ca. 30 Tage ohne IT	150.000 €
3.	**Forensische** Untersuchung durch Experten/Firma	50.000 €
4.	**Virenentfernung** durch Neuinstallation aller IT-Systeme	100.000 €
Gesamt:		**500.000 €**
Ggf. vollständiger Datenverlust		**???.??? €**

Der **Schutzbedarf** der Daten / Assets und somit die Auswahl der technischen und organisatorischen Maßnahmen **(TOM)** steht in Abhängigkeit zur **Eintrittswahrscheinlichkeit** und **Schwere** des **Schadens** für das Unternehmen und des Betroffenen!



Quelle: https://www.bsi.bund.de/

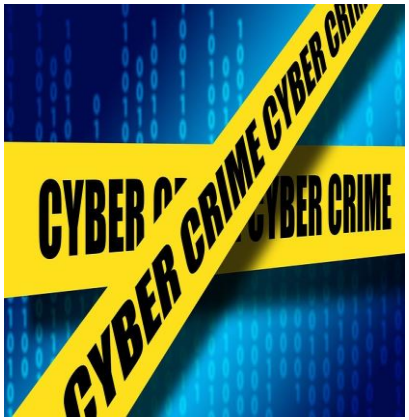
Standards zur Informationssicherheit und zum Datenschutz

VdS	Informationssicherheitsmanagementsystem für **kleine und mittlere Unternehmen** (KMU)	Verband der Sachversicherer e.V. Schadenverhütung GmbH
CISIS12	Compliance Informationssicherheitsmanagement System in **12 Schritten**	IT-Sicherheitscluster e.V.
IT-Grundschutz	Informationssicherheits-Managementsystem – **BSI-Standards 201 – 204 und IT-Grundschutzkompendium**	Bundesamt für Sicherheit in der Informationstechnik (BSI)
ISO 27001 Normativ, Basis	Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – **Anforderungen**	Internationale Organisation für Normung (ISO)
ISO 27002 Leitfaden	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – **Informationssicherheitsmaßnahmen**	
ISO 27017 Erweiterung	Anwendungsleitfaden für **Informationssicherheitsmaßnahmen** basierend auf ISO 27002 für **Cloud Dienste**	
ISO 27018 Erweiterung	Leitfaden zum **Schutz personenbezogener Daten** in öffentlichen **Cloud-Diensten** als Auftragsdatenverarbeitung	
ISO 27701 Normativ, Basis	Informationssicherheit, Cybersicherheit und Datenschutz – Datenschutzmanagementsysteme – **Anforderungen**	
ISO 29134 Erweiterung	Leitlinien für die **Datenschutz-Folgenabschätzung**	
NIST 800-53	Informationssicherheitsstandard (USA)	National Institute of Standards and Technology (NIST)

Datenschutz und Informationssicherheit ohne Standard

Kein ausreichender Schutz der Daten!

- **Geringes Sicherheitsniveau**, weil die Festlegung der erforderlichen Maßnahmen durch eine **Risikoanalyse** i.d.R. nicht gewährleistet wird!
- Keine **Transparenz** der umgesetzten Maßnahmen!
- **Gefährdungen bzw. Schwachstellen** in den Bereichen Gebäude, Räume, IT-Systeme Netze und Anwendungen sind nicht vollständig bekannt!
- Umgesetzte Maßnahmen ohne **Regelwerk** (Soll) sind nicht prüffähig!
- Eintrittswahrscheinlichkeit für **Datenschutz-** und **Sicherheitsvorfälle** ist hoch!
- **Finanzieller** Schaden kann die Grenzen der **verfügbaren Mittel** übersteigen!



Quelle: https://pixabay.com

Umsetzung eines Informationssicherheitsstandards

Vorteile!

- Die **Anforderungen** des **Standards** legen ein nachvollziehbares **Schutzniveau** fest.
- Ein nach Vorgaben zu implementierendes **Informationssicherheits-Managementsystem** (ISMS) schütz die Informationen vor unbefugtem Zugriff, Verlust oder Veränderung.
- Mit den im Standard definierten **Verfahren zur Analyse und Bewertung** von Gefährdungen und Risiken werden geeignete **Maßnahmen** zur Eindämmung vorgeschlagen.
- Standards unterstützen Unternehmen und öffentliche Stellen dabei, relevante **Gesetze** wie die **DSGVO** oder das **NIS-2-Umsetzungsgesetz** einzuhalten.
- Ein ISMS mit der **Umsetzung von Datenschutzanforderungen** sollte Zielsetzung der **Unternehmensstrategie** sein.
- Ein ISMS fördert die kontinuierliche **Verbesserung** der Informationssicherheit durch regelmäßige **Überprüfung/Audits** und Anpassung der Sicherheitsmaßnahmen.
- Die Einführung eines ISMS trägt zur **Strukturierung** und Verbesserung von **Geschäfts-prozessen** bei.
- Die Umsetzung eines Standards schärft das **Bewusstsein** für Datenschutz und Informationssicherheit im Unternehmen.
- Eine **Zertifizierung des ISMS** erhöht das Vertrauen von Kunden, Partnern und anderen Stakeholdern in den Umgang mit Informationen.

VdS 10000 – Inhalt

Schadenverhütung GmbH, Institut für Unternehmenssicherheit

- Organisation der Informationssicherheit
- Leitlinie zur Informationssicherheit (IS-Leitlinie)
- Richtlinien zur Informationssicherheit (IS-Richtlinien)
- Mitarbeiter
- Wissen
- Identifizieren kritischer IT-Ressourcen
- IT-Systeme
- Netzwerke und Verbindungen
- Mobile Datenträger
- Umgebung
- IT-Outsourcing und Cloud Computing
- Zugänge und Zugriffsrechte
- Datensicherung und Archivierung
- Störungen und Ausfälle
- Sicherheitsvorfälle
- Risikoanalyse, Risikobehandlung (Anhang)

41 Seiten

VdS-Richtlinien für die Informationsverarbeitung

Informationssicherheits-managementsystem für kleine und mittlere Unternehmen (KMU)

Anforderungen

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

Inhalt

VdS 10010 – Inhalt

Schadenverhütung GmbH, Institut für Unternehmenssicherheit

- Organisation des Datenschutzes
- Leitlinie zum Datenschutz (DS-Leitlinie)
- Richtlinien zum Datenschutz (S-Richtlinien)
- Mitarbeiter
- Wissen
- Analyse
- Verarbeitung
- Informationssicherheit
- Auftragsverarbeitung
- Datenschutzvorfälle
- Datenmanagement
- Risikoanalyse, Risikobehandlung (Anhang)

34 Seiten

VdS-Richtlinien für die Informationsverarbeitung

Datenschutzmanagementsystem für kleine und mittlere Unternehmen (KMU) zur Umsetzung der DSGVO

Anforderungen

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

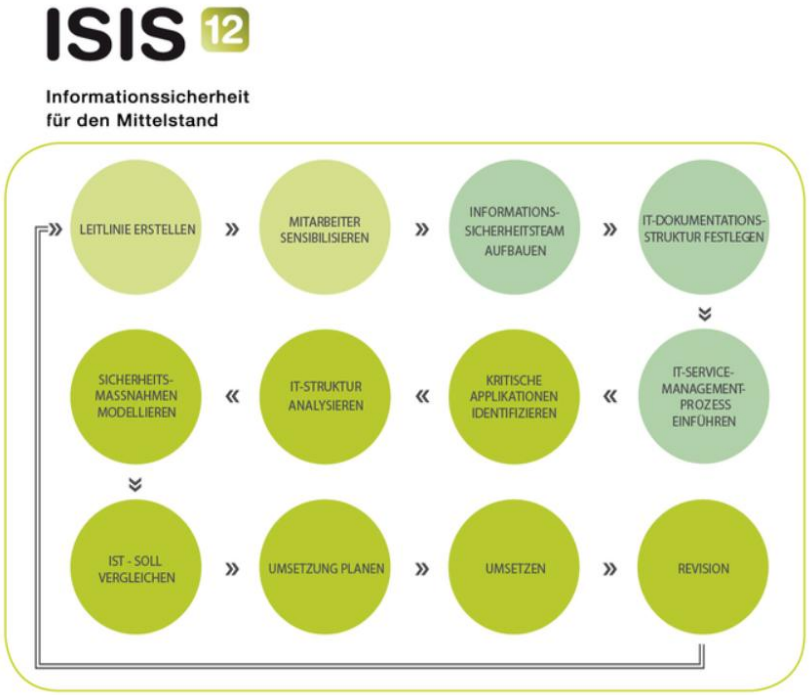
Um eine Beeinträchtigung des Textverständnisses zu vermeiden, verwendet VdS Schadenverhütung durchweg das generische Maskulinum. Eine Bevorzugung oder anderweitige Wertung des männlichen, weiblichen oder sonstigen Geschlechts geht damit ausdrücklich nicht einher.

Inhalt

CISIS 12 Version 3.0

IT-Sicherheitscluster e.V. (Regensburg)

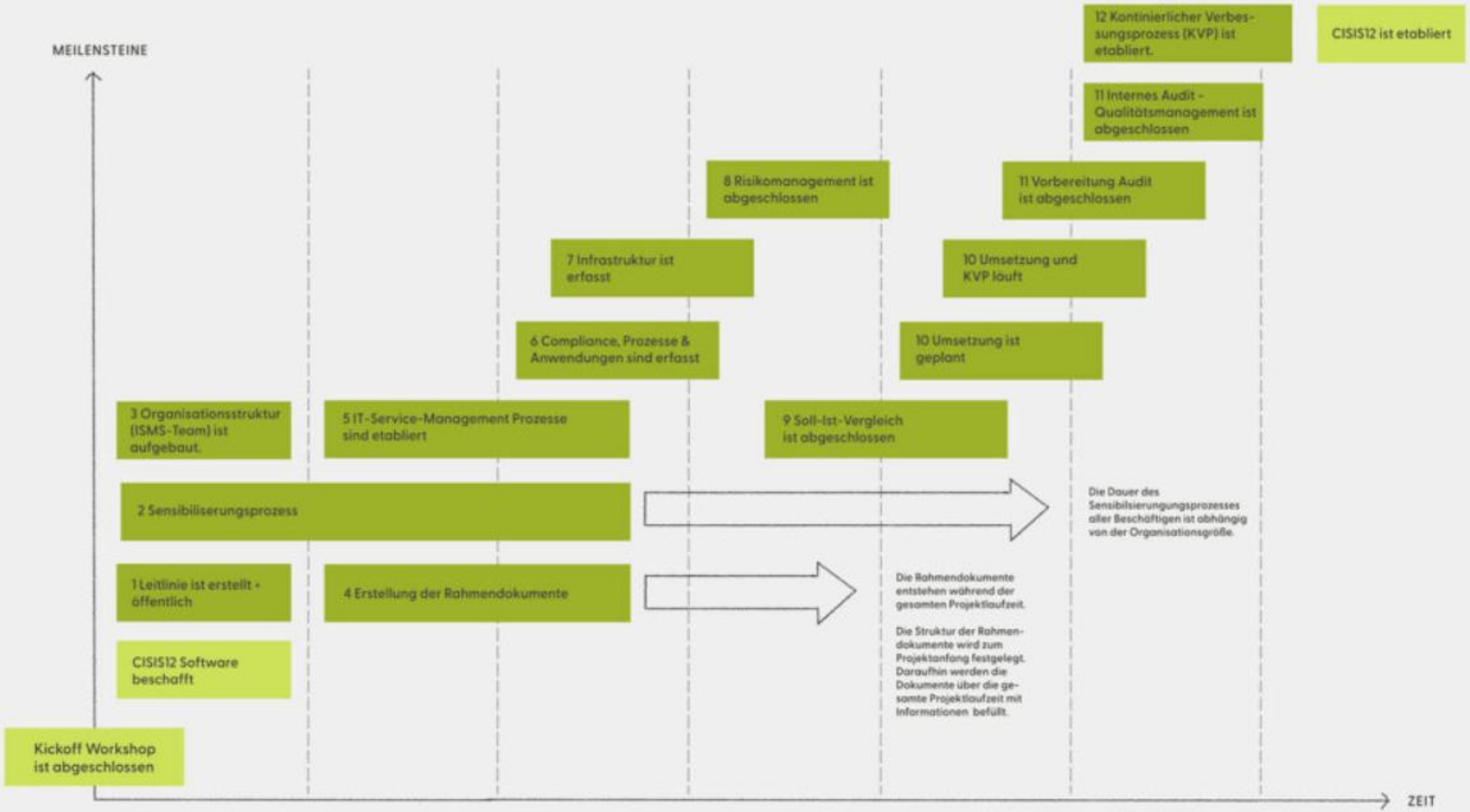
- **C**ompliance-**I**nformations-**SI**cherheits-Management-**S**ystem in 12 Schritten.
- CISIS12 in der Version 3.0 ist eine **Weiterentwicklung** und Erweiterung des Informationsmanagementsystems ISIS12.
- Der Schwerpunkt liegt auf dem Thema **Compliance**.
- Der **Standard** besteht aus einer **Norm**, einem **Maßnahmenkatalog** sowie einem **Handbuch** als Grundlage für die Umsetzung.
- CISIS12 ist speziell für die Anforderungen von **KMUs** sowie **Kommunen** entwickelt.
- Der Standard verfolgt das Ziel, ein ISMS in **zwölf Schritten** mit **geringem Aufwand** einzuführen.



Quelle: https://www.it-sicherheitscluster.de/

CISIS12

Beispielhafter CISIS12-Ablaufplan



GEMEINSAME PRINZIPIEN AUFBAUEN

1 Leitlinie erstellen
2 Beschäftigte sensibilisieren

RAHMEN-BEDINGUNGEN AUFBAUEN

3 Informationssicherheit steam aufbauen
4 IT-Doku-Struktur festlegen
5 IT-Service-Management Prozesse

ANALYSE

6 Compliance, Prozesse und Anwendungen
7 IT-Struktur analysieren

PROBLEM-IDENTIFIZIERUNG

8 Risikomanagement
9 Soll-Ist-Vergleich

SYNTHESE PROBLEMLÖSUNGEN, STRATEGIE + UMSETZUNG

10 Umsetzung planen und umsetzen

ÜBERPRÜFUNG, BEWERTUNG UND VERBESSERUNG

11 Internes Audit - Qualitätsmanagment
12 Revision - kontinuierlicher Verbesserungsprozess

CISIS12 – Vorgehensmodell

- CISIS12 ist nach der Struktur des **IT-Grundschutzstandards vereinfacht** aufgebaut
- Es werden **87 Bausteine** mit über **900 Maßnahmen** in einem Katalog beschrieben
- Die **Umsetzung** erfolgt in **3 Schritten**:
  - Erstellung der **Leitlinie** und **Dokumentation** (Konzepte, Richtlinien)
  - **Analyse** und **Strukturierung** der Datenverarbeitung (**IT-Verbund**) mit Zuordnung der Bausteine und **Soll-Ist-Prüfung** der Maßnahmen
  - **Kontrolle** und Bewertung des ISMS

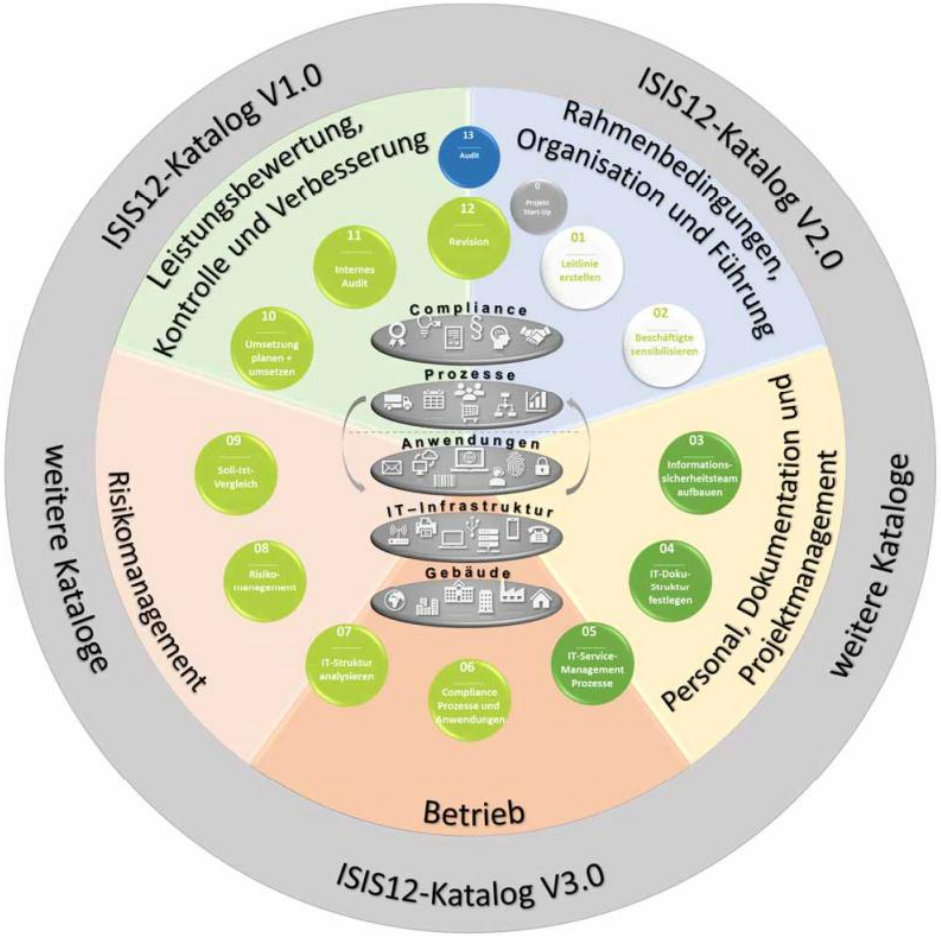


Abbildung 2: ISIS-Vorgehensmodell und Managementsystemmodell V3.0

Quelle: https://www.it-sicherheitscluster.de/

CISIS12 - Distribution (Norm, Handbuch, Katalog, Extended)

CISIS12®-Norm Version 1.0 (PDF) Die CISIS12®-Norm beschreibt die Vorgaben und Mindestanforderungen zum Aufbau und zur Aufrechterhaltung des Informationssicherheitsmanagementsystems in strukturierter und abstrakter Weise. Durch die Abstrahierung der Normenbeschreibung von CISIS12® ist diese universell anpassbar an Organisationsart und Organisationsgröße. Die CISIS12®-Norm enthält umfangreiche Verweise auf Regelwerke, BSI-Standards, ISO/IEC-2700x-Normen sowie auf ISIS12-Vorgängervorgehensmodelle.

CISIS12®-Handbuch Version 1.0 (PDF) Das CISIS12-Handbuch enthält alle grundlegenden Informationen. Der gesamte Workflow wird beschrieben und mit Kontrollfragen abgerundet. Diese ermöglichen eine objektive Bewertung der Umsetzung.

CISIS12®-Katalog Version 1.1 (PDF) Der CISIS12®-Katalog enthält die konkreten Maßnahmen zur Umsetzung. In der ersten Version enthält er 87 Bausteine mit verknüpften Maßnahmen. Jeder Baustein ist detailliert beschrieben. Eine Einteilung der Maßnahmen in „MUSS“, „SOLL“ und „KANN“ schafft Übersichtlichkeit und hilft bei der Priorisierung. Mit der Veröffentlichung des Katalogs 1.1 wurde der Katalog 1.0 redaktionell überarbeitet. Es wurden keine weiteren Bausteine und Maßnahmen aufgenommen. Es gibt keine Änderungen im Zertifizierungsprozess.

CISIS12®-Extended Katalog Version 1.0 (PDF) – zusätzliche Bausteine und Maßnahmen Der CISIS12®-Extended Katalog enthält zusätzliche Bausteine und Maßnahmen, um höheren Sicherheitsanforderungen gerecht zu werden. Diese können bei Bedarf hinzugenommen werden und im Bedarfsfall im Audit als zusätzliche Bausteine hinzugezogen werden.

CISIS12®-Kreuzreferenztabelle Version 1.0 (PDF)
Die CISIS12®-Kreuzreferenztabelle stellt eine Zuordnung zwischen den CISIS12-Bausteinen/Maßnahmen und dem BSI-Kompendium und zur ISO/IEC-27001:2022 Norm her.

Die SWI GmbH bindet einen Software-Anbieter exklusiv. Dieser verpflichtet sich, die stets die aktuellen Anforderungen des CISIS12®-Standards in die Software zu integrieren. Dies ist M24S. Darüber hinaus pflegen wir weitere Partnerschaften. Unsere Softwarepartner erhalten vertragsmäßig auch immer die aktuellste Version von ISIS12/CISIS12®; sind jedoch nicht verpflichtet diese umzusetzen. Hier werden weitere Partner aufgelistet.

M24S®
Management Systems Solutions

M24S® ist ein Werkzeug zum Aufbau und Etablierung von Managementsystemen. Hierbei handelt es sich um ein branchenunabhängiges Werkzeug mit dem unterschiedliche Managementsysteme (z.B. CISIS12®, ISO 27001, BSI, usw.) aufgebaut und nachhaltig betrieben werden können. M24S® unterstützt bei den wesentlichen Funktionen und hat folgenden modularen Aufbau.

Quelle: https://www.it-sicherheitscluster.de/

IT-Grundschutzstandard

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Ziel des **IT-Grundschutzes** ist es, einen **angemessenen Schutz für alle Informationen** einer Organisation zu erreichen.
- Durch die Kombination von **organisatorischen, personellen, infrastrukturellen und technischen** Sicherheitsanforderungen kann ein nachvollziehbares Sicherheitsniveau für den Schutz der **Daten bzw. Assets** erreicht werden.
- Im **IT-Grundschutz-Kompendium** werden standardisierte Sicherheitsanforderungen für **Geschäftsprozesse**, **Anwendungen**, **IT-Systeme**, **Kommunikationsverbindungen** und **Räume** in **IT-Grundschutz-Bausteinen** beschrieben.
- Darüber hinaus können die Anforderungen des IT-Grundschutz-Kompendiums in einem **Stufenmodel** als **Basis-**, **Standard-** oder **Kernabsicherung** umgesetzt werden.
- Nach der Festlegung des **Informationsverbunds** (Scope) können die IT-Grundschutz-Bausteine **objektbezogen** den schützenswerten Bereichen – **Infrastruktur**, **Technik**, **Netz**, **Fachanwendungen** – zugeordnet werden.
- Die **Bausteine** des IT-Grundschutz-Kompendiums bilden den **Stand der Technik** ab, basierend auf den Erkenntnissen zum Zeitpunkt der Veröffentlichung.
- Der IT-Grundschutz ist ein **anerkannter Informationssicherheitsstandard** und konform mit der **ISO 27001**. Eine **Zertifizierung** ist möglich.

Unser Leitbild

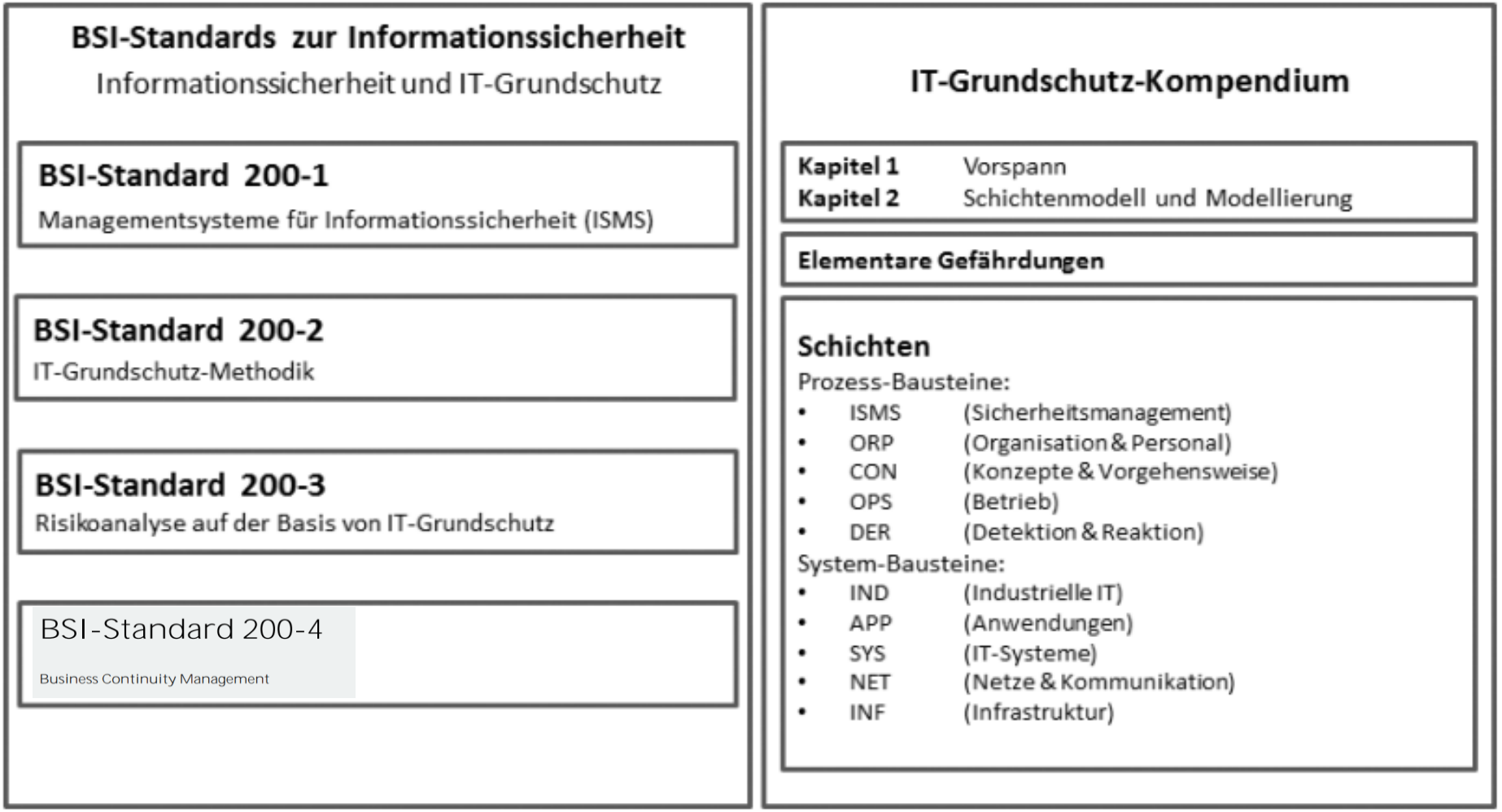
Das BSI als die Cybersicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Was wollen wir erreichen?

Das BSI ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Unser Ziel ist der sichere Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft. Mit unserer Unterstützung soll Informationssicherheit als Voraussetzung der Digitalisierung verstanden und eigenverantwortlich umgesetzt werden. Wir wollen bewirken, dass Sicherheitsaspekte schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden. Denn Informationssicherheit und Digitalisierung gehören untrennbar zusammen.

IT-Grundschutzstandard

BSI-Standard – Leitfäden und Kompendium



Quelle: https://www.bsi.bund.de

IT-Grundschutz-Prozess – Methode

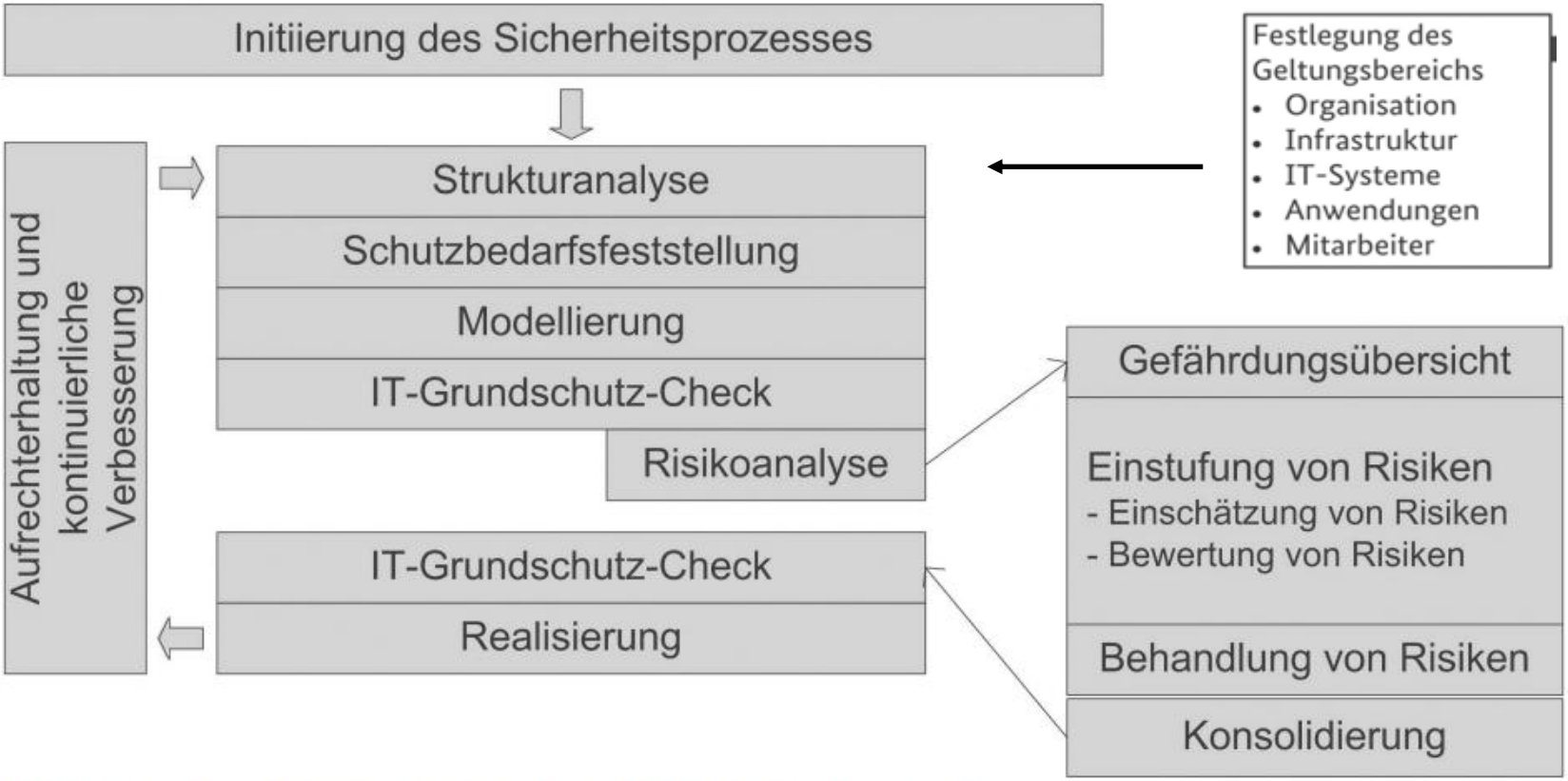
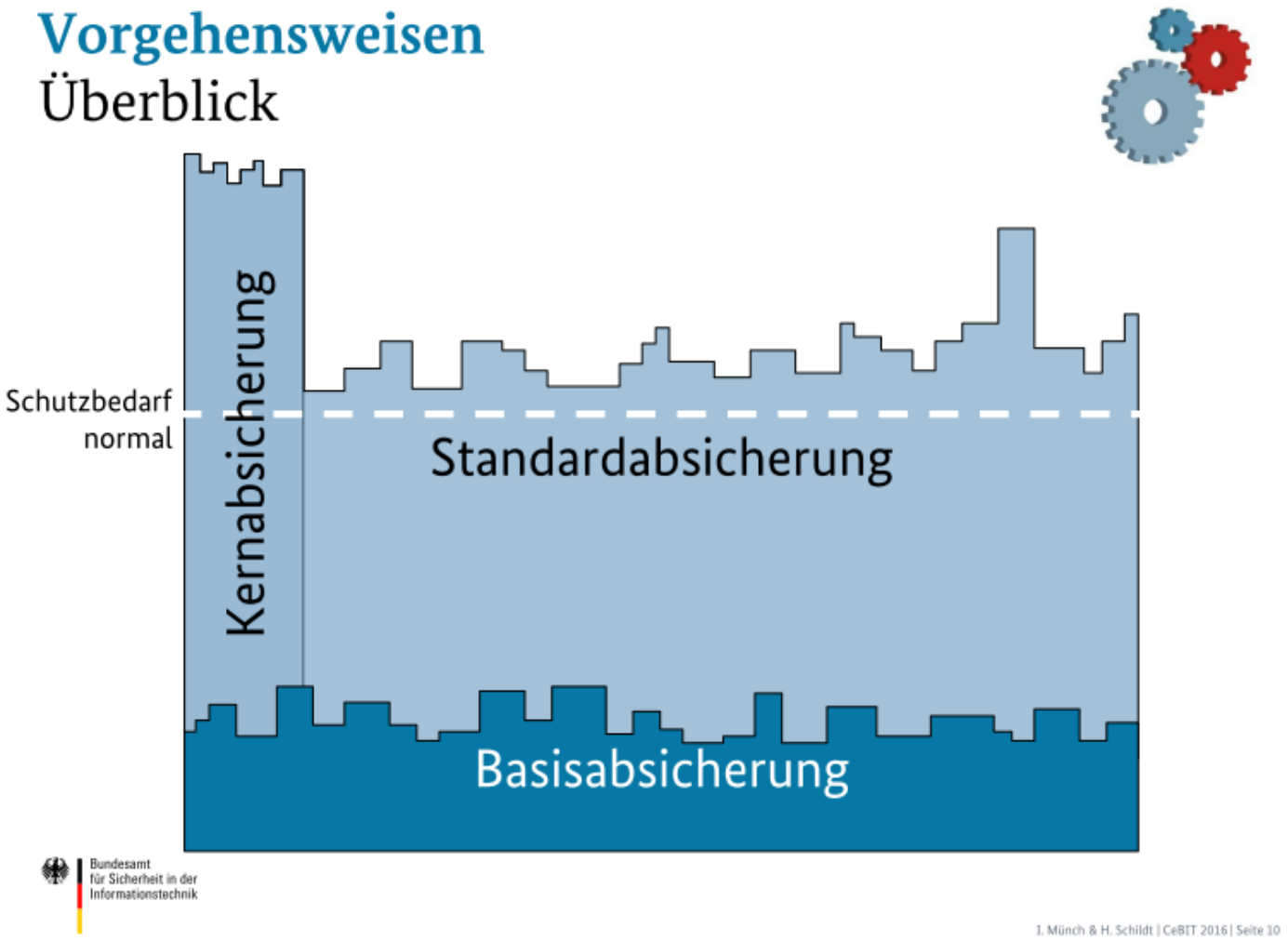


Abbildung 32: Integration der Risikoanalyse in den IT-Grundschutz-Prozess

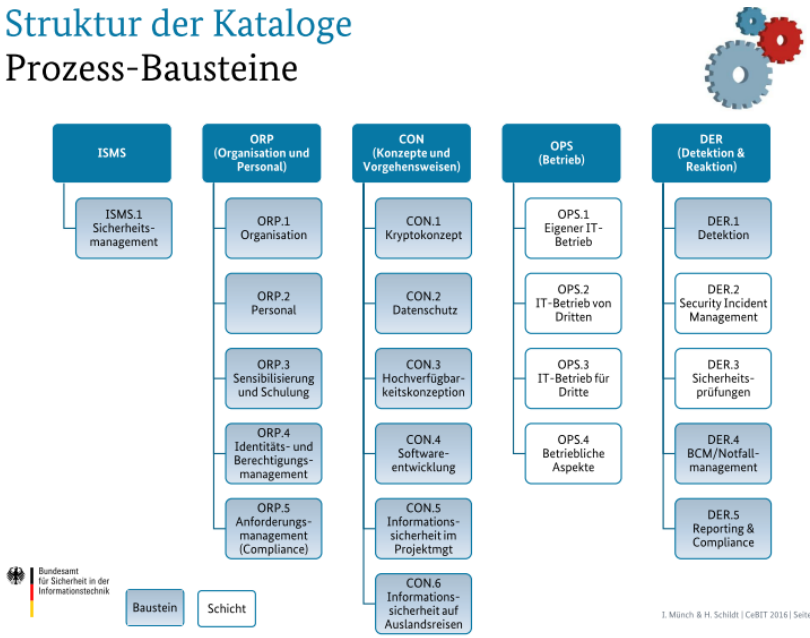
Quelle: https://www.bsi.bund.de

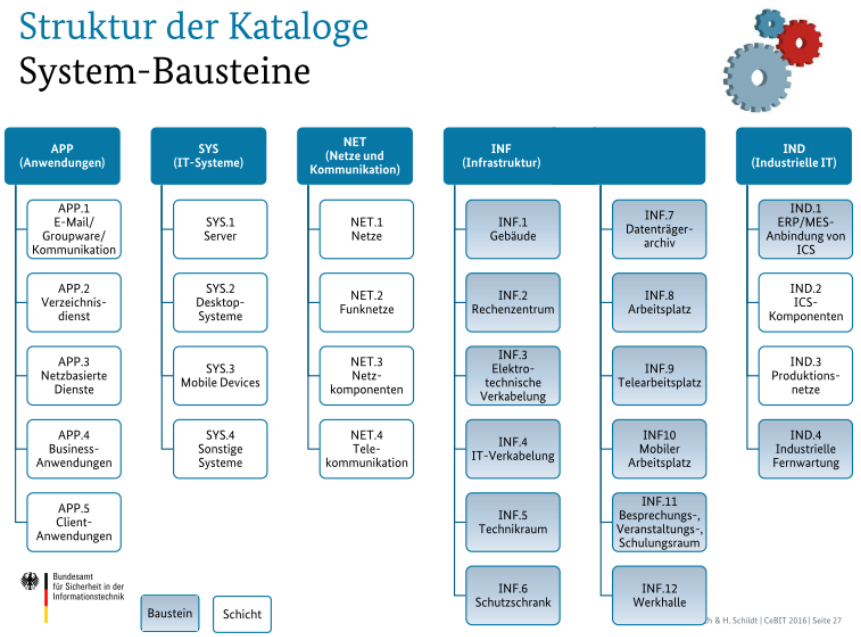
Stufenmodell



Quelle: https://www.bsi.bund.de

IT-Grundschutz-Kompendium





Quelle: https://www.bsi.bund.de

- Über **100 Bausteine** mit Anforderungen bzw. Maßnahmen
- Die Bausteine und **Anforderungen/Maßnahmen** werden ausführlich beschrieben
- Das IT-Grundschutz-Kompendium lässt sich **vollständig in Tools** integrieren

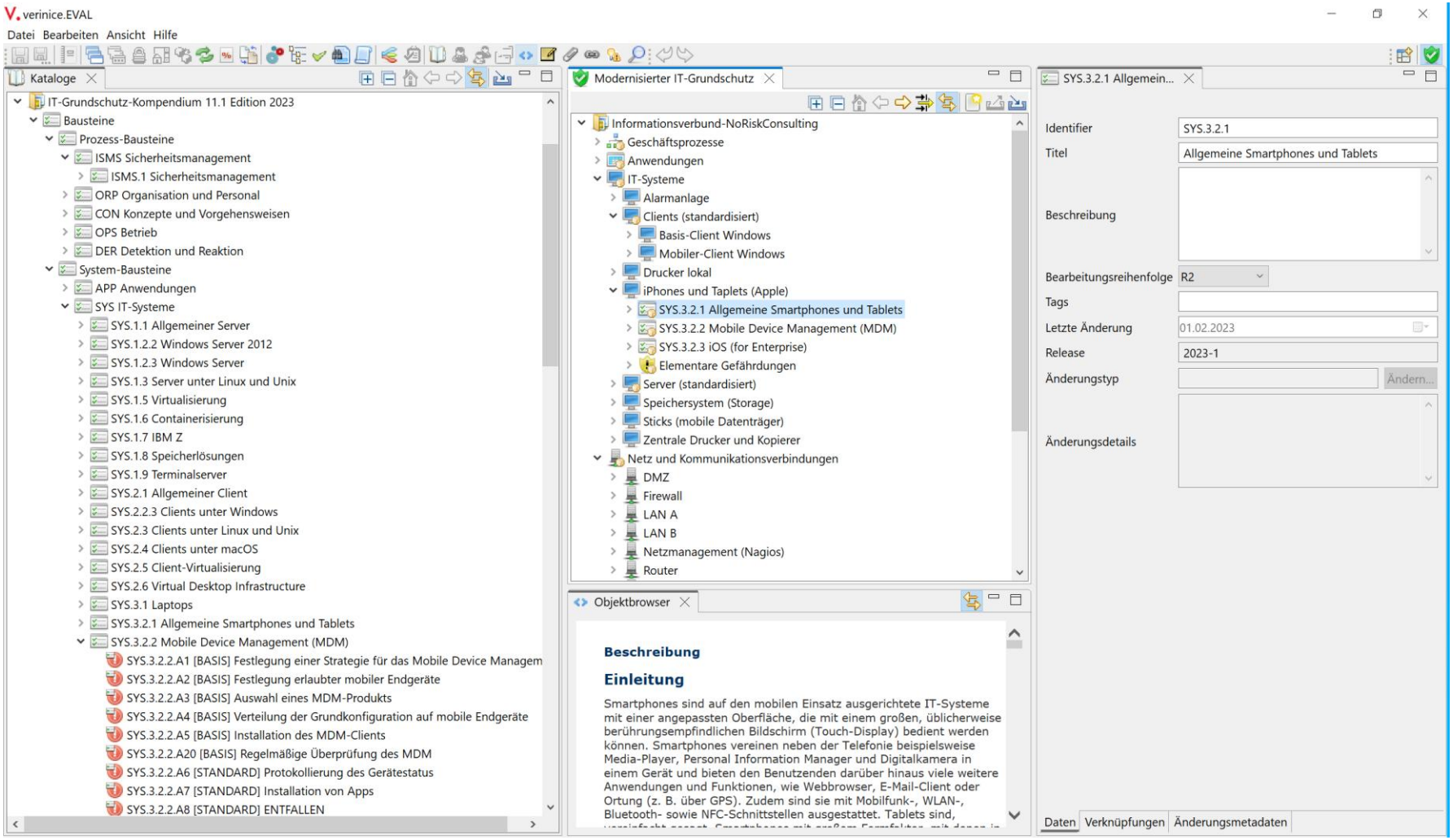
Grundschutz++

Neuer Grundschutz ab 2026

- Der Grundschutz++ orientiert sich an der **ISO 27001:2022.**
- Bausteine im **Grundschutzkompendium** werden durch **Praktiken** ersetzt.
- Die **Grundschutzmethodik** (Strukturanalyse, Schutzbedarfsfestlegung, Bausteinzuordnung, Basissicherheitscheck und Ergänzende Risikoanalyse) wird durch eine vereinfachte Vorgehensweise im Rahmen des PDCA-Zyklus ersetzt.
- Es werden sogenannte **Anforderungspakte** (Profile) für die praktische Umsetzung erstellt.
- **Alle Praktiken** des **Bereichs ISMS** sind dem IT-Verbund zuzuordnen.
- **Übergangsfristen** zur Anwendung Grundschutz++ laufen voraussichtlich bis **2031**.
- Wann **Tools**, z. B. Verinice, HiScout, fuentis, DocSetMinder, verfügbar sind, ist noch unklar.
- Es werden sogenannte **Anforderungspakte** (Profile) für die praktische Umsetzung erstellt.
- Der **Leitfaden** „Methodik Grundschutz++" beschreibt die Umsetzung des Grundschutzes++.
- Um die Anwendbarkeit weiter zu erleichtern, werden die **Absicherungsstufen Basis, Standard und erhöhter Schutzbedarf** durch flexible **Leistungszahlen** in Verbindung mit dynamischen **Schwellwerten** ersetzt.
- Die mit dem **WiBA-Weg** in die Basis-Absicherung erprobten **Checklisten** haben sich in der Praxis bewährt und werden **fester Bestandteil** des Grundschutz++.

ISMS-Tool zur Festlegung und Umsetzung der TOMs

IT-Grundschutz-Standard – Informationsverbund Beispiel: Muster-Firma NoRiskConsulting

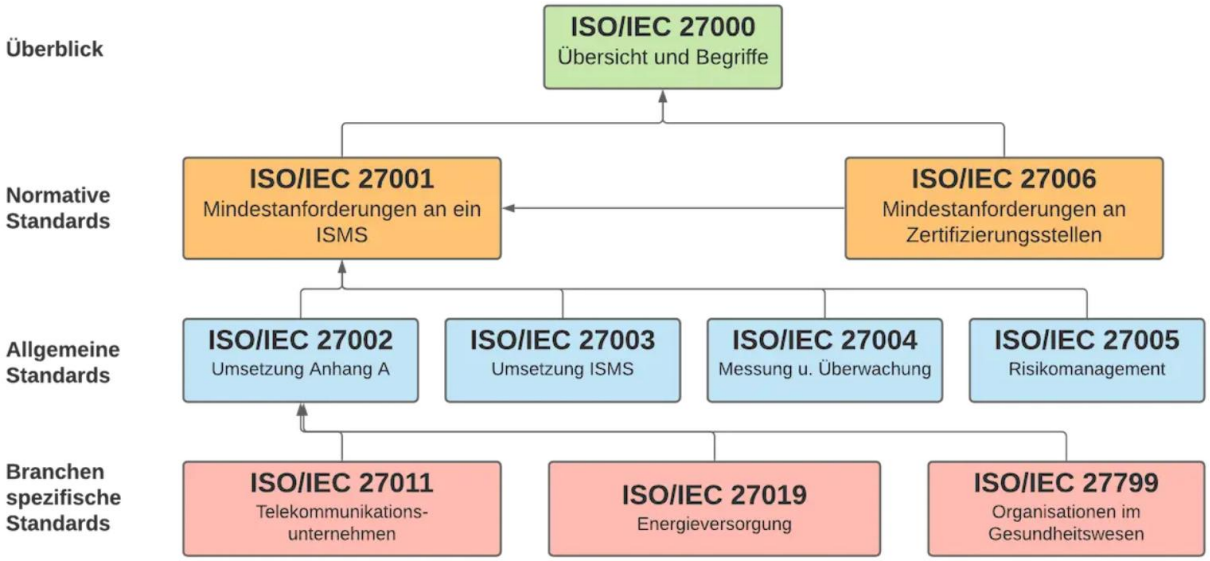


Quelle: Heiko Behrendt

ISO 27001

Internationale Norm für Informationssicherheit

- Die **ISO 27001:2022** bzw. die **Normenreihe** der ISO 27000 beinhalten **international bewährte und anerkannte Anforderungen** und Leitlinien an ein **Managementsystem für die Informationssicherheit (ISMS)**. Sie ist die **Basis** für die Zertifizierung des ISMS.
- Das ISMS dient dazu, die übergeordneten **Schutzziele** der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen zu gewährleisten.
- Im **Anhang** der Norm werden **93 Controls** aufgeführt, die umzusetzen sind.



Quelle: https://de.wikipedia.org/wiki/ISO/IEC_27001

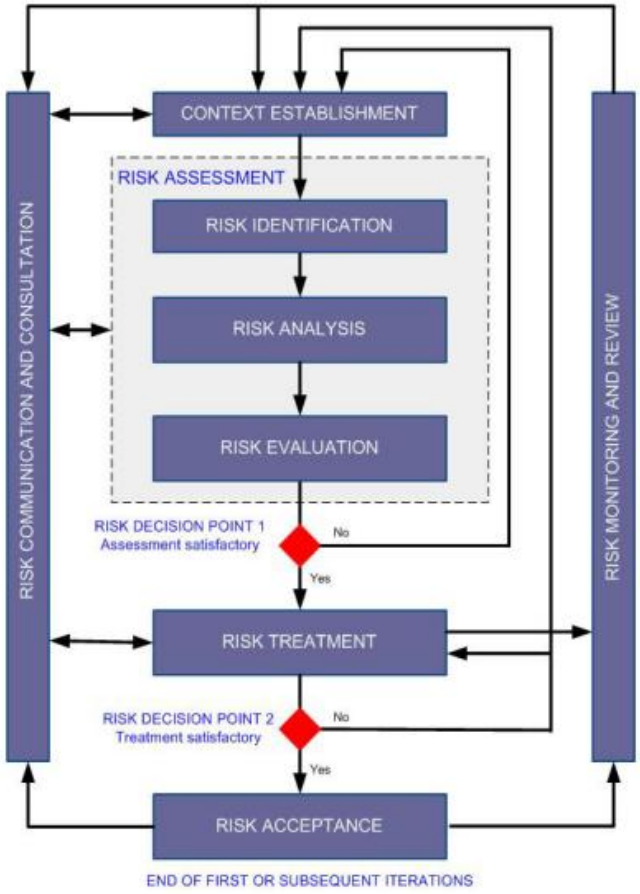
ISO 27001

Prozess bei der Umsetzung der ISO 27001 (Methode)

1. Durchführung einer **Gap-Analyse**, Abweichungen zur ISO 27001 ermitteln
2. Umfang des ISMS bzw. **Scope** abgrenzen/festlegen
3. Erstellung einer **Informationssicherheitsrichtlinie**
4. **Schwerpunkt:** Durchführung der **Risikoanalyse,** ggf. **Anwendung der ISO 27005 Risikomanagement**
5. **Prüfung**, ob die **Controls** der ISO 27001 ausreichend umgesetzt sind (Soll-Ist) und Risiken reduzieren
6. Entwicklung einer **Dokumentation** über alle umzusetzenden Controls mit **Umsetzungsstand**
7. Erstellung eines **Risikobehandlungsplans** mit **Risikoakzeptanz (Restrisiken)**
8. Erstellung der Dokumentation für die **Steuerung** des **ISMS**
9. Umsetzung eines Konzepts für die **Sensibilisierung** der **Beschäftigten**

Standard ISO 27005

Risikomanagement-Prozess



Quelle: ISO/IEC 27005:2011

ISO 27001

Inhalt

DIN EN ISO/IEC 27001:2024-01
EN ISO/IEC 27001:2023 (D)

Anhang A
(normativ)

Verweisung auf Informationssicherheitsmaßnahmen

Die in Tabelle A.1 aufgeführten Informationssicherheitsmaßnahmen[N1] sind aus denjenigen, die in ISO/IEC 27002:2022 [1], Abschnitt 5 bis Abschnitt 8, genannt sind, direkt abgeleitet, daran ausgerichtet und müssen im Kontext mit 6.1.3 angewendet werden.

Tabelle A.1 — Informationssicherheitsmaßnahmen

5	Organisatorische Maßnahmen	
5.1	Informationssicherheitspolitik und -richtlinien	**Maßnahme** Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.
5.2	Informationssicherheitsrollen und -verantwortlichkeiten	**Maßnahme** Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.
5.3	Aufgabentrennung	**Maßnahme** Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.
5.4	Verantwortlichkeiten der Leitung	**Maßnahme** Die Leitung muss vom gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik, und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.
5.5	Kontakt mit Behörden	**Maßnahme** Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.
5.6	Kontakt mit speziellen Interessensgruppen	**Maßnahme** Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.
5.7	Informationen über die Bedrohungslage	**Maßnahme** Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.
5.8	Informationssicherheit im Projektmanagement	**Maßnahme** Die Informationssicherheit muss in das Projektmanagement integriert werden.
5.9	Inventar der Informationen und anderen damit verbundenen Werte	**Maßnahme** Ein Inventar der Informationen und anderen damit verbundenen Werte, einschließlich der Eigentümer, muss erstellt und gepflegt werden.

ISO 27002 – Leitfaden für die ISO 27001

DIN EN ISO/IEC 27002:2024-01
EN ISO/IEC 27002:2022 (D)

Inhalt

Seite

ISO 27017 und ISO 27018

Erweiterungen für Datenschutz und Informationssicherheit

- **ISO 27017 Informationssicherheitsmaßnahmen für Cloud-Dienste** (Zertifizierung)
  - **Anwendungsbereich:** Die Norm richtet sich an **Cloud Service Provider** und **Cloud Service Kunden**.
  - **Ziel:** Sie dient dazu, die **Informationssicherheit in der Cloud** zu verbessern und das Risiko von Sicherheitsvorfällen zu reduzieren.
  - **Verwendung:** Die Norm kann in Verbindung mit der **ISO 27001** verwendet werden, um ein umfassendes ISMS unter Einbeziehung von **Informationssicherheit** bei Clouddiensten zu implementieren.
- **ISO 27018 Schutz pb Daten in öffentlichen Cloud-Diensten als Auftragsdaten-verarbeitung** (Zertifizierung)
  - **Anwendungsbereich:** Die Norm richtet sich an **Cloud-Anbieter**, die **personenbezogene Daten** verarbeiten.
  - **Ziel:** Sie konzentriert sich auf den **Schutz von personenbezogenen Daten**.
  - **Verwendung:** Die Norm kann in Verbindung mit der **ISO 27001** verwendet werden, um ein umfassendes ISMS unter Einbeziehung von **Datenschutz** bei Clouddiensten zu implementieren.

ISO 27701 und ISO 29134

Erweiterungen für Datenschutz und Informationssicherheit

- **ISO 27701 Datenschutz-Managementsysteme** (Zertifizierung)
  - **Anwendungsbereich:** Für alle **Organisationen** anwendbar, die ein **Datenschutzmanagementsystem** implementieren.
  - **Ziel:** Die ISO 27701:2025 legt **Anforderungen** für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines **Datenschutzmanagementsystems** fest.
  - **Verwendung:** Die Norm kann für das **Datenschutzmanagement** ab 2025 allein (neu) oder gemeinsam mit der ISO 27001 Informationssicherheitsmanagement zertifiziert werden.
- **ISO 29134 Leitlinie für die Datenschutz-Folgenabschätzung**
  - **Anwendungsbereich:** Für alle Organisationen anwendbar, die personenbezogene Daten verarbeiten.
  - **Ziel: Leitlinie,** die einen Prozess zur Datenschutzfolgeabschätzung und eine Struktur und Inhalte eines PIA-Berichts beschreibt.
  - **Verwendung:** Umsetzung einer **Datenschutz-Folgenabschätzung.**

ISO 27701

Inhalt

Tabellen

NIST 800-53 (NIST = National Institute of Standards and Technology – USA)

Security und Privacy Controls for Information Systems and Organizations

- Die NIST 800-53 ist ein **Informations-sicherheitsstandard**, der einen Katalog von Datenschutz- und Sicherheits-maßnahmen für Informationssysteme bereitstellt.
- Der **Standard** wird vom **National Institute of Standards and Technology (NIST)** herausgegeben.
- Das NIST entwickelt und veröffentlicht **Standards, Richtlinien** und andere **Publikationen** zum Schutz von Informationen der Behörden und Unternehmen in den USA.

Table of Contents

Quelle: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

VERÖFFENTLICHUNGEN

NIST SP 800-53 Rev. 5

Sicherheits- und Datenschutzmaßnahmen für Informationssysteme und Organisationen

Veröffentlichungsdatum: September 2020 (einschließlich Aktualisierungen vom 10. Dezember 2020)

Ersetzt: SP 800-53 Rev. 5 (23.09.2020)

Planungshinweis (27.08.2025):

Am 27. August 2025 veröffentlichte das NIST eine kleinere Version von SP 800-53 (Version 5.2.0), die Folgendes beinhaltet:

- Neue Steuerung/Steuerungsverbesserungen: SA-15(13), SA-24, SI-02(07)
- Änderungen an bestehenden Kontrollen: SI-07(12)
- Aktualisierungen der Kontrolldiskussion: SA-04, SA-05, SA-08, SA-08(14), SI-02, SI-02(05)
- Aktualisierungen der zugehörigen Bedienelemente: Alle -01-Bedienelemente, AU-02, AU-03, CA-07, IR-04, IR-06, IR-08, SA-15, SI-02, SI-07

Eine Liste aller Änderungen im Patch-Release finden Sie unter Zusatzmaterial.

***

Zusammenfassung der ergänzenden Dateien:

- **Analyse der Aktualisierungen zwischen 800-53 Rev. 5 und Rev. 4** (Aktualisiert am 01.07.2022).
  Beschreibt die Änderungen an den einzelnen Steuerungselementen und deren Verbesserungen, bietet eine kurze Zusammenfassung der Änderungen und beinhaltet eine Bewertung ihrer Bedeutung. *Hinweis: Dieser Vergleich wurde von der MITRE Corporation im Auftrag des Direktors des Nationalen Nachrichtendienstes (DNI) erstellt und wird mit Genehmigung des DNI veröffentlicht.*

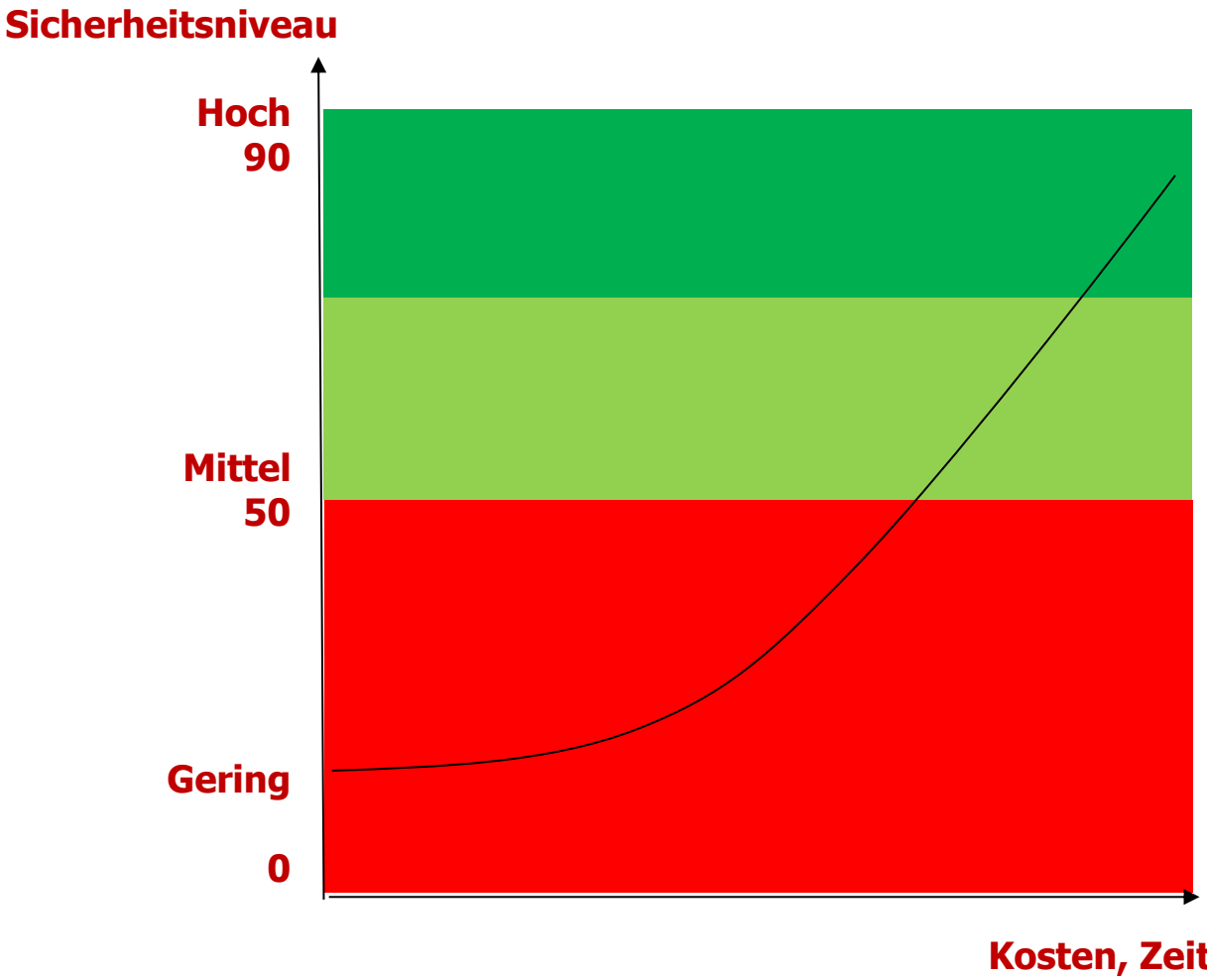
DOKUMENTATION

Veröffentlichung:
https://doi.org/10.6028/NIST.SP.800-53r5
Download-URL

Zusatzmaterial:
SP 800-53 Version 5.2.0
Zusammenfassung der Änderungen SP 800-53 Version 5.2.0 (pdf)
Analyse der Aktualisierungen zwischen 800-53 Rev. 5 und Rev. 4, von MITRE Corp. für ODNI (xlsx)
Zuordnung: Anhang J Datenschutzeinstellungen (Rev. 4) zu Rev. 5 (xlsx)
Zuordnungen: Cybersecurity Framework und Privacy Framework zu Rev. 5 (xlsx)
Konvertierungstabelle: 800-53 Rev. 5 zu ISO/IEC 27001:2022 (OLIR)
OSCAL-Version der Rev. 5-Steuerung
Vorlage für einen Index der Zusammenarbeit (xlsx)
Vorlage für einen Kontrollkollaborationsindex (docx)
Blogbeitrag

Quelle: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Sicherheitsniveau zu Kosten, Zeit, Aufwand, Know-how



IT-Grundschutz
ISO 27001 + ISO 27701
NIST 800-53

CISIS12
VdS 10000 + 10010

Keine Anwendung eines Standards

Datenschutz und Informationssicherheit	Kein Standard	VdS-Richtlinien	CISIS12	IT-Grundschutz	ISO 27001	NIST 800-53
Zielgruppe	-	KMU	KMU	Kleine u. große Unternehmen	Große Unternehmen	Große Unternehmen
Sicherheitsniveau	Niedrig	Mittel	Hoch	Hoch	Hoch	Hoch
Aufwand, Ressourcen	Niedrig	Niedrig	Mittel	Mittel bis sehr Hoch Stufenmodell	Mittel bis Hoch Je nach Scope	Mittel bis Hoch Je nach Scope
Maßnahmen/Controls	-	Prosatext	Ca. 900	über 1000	93	über 1000
Maßnahmen objektbezogen	-	Nein	Ja	Ja	Nein	Nein
Leitfäden	-	Generisch überschaubar	Pragmatisch umfangreich	Pragmatisch umfangreich	Generisch umfangreich	Generisch umfangreich
Datenschutzmanagement – DSGVO	-	10010	Nein	Nein	ISO 27701 ISO 27018	Privacy Framework
Schwierigkeitsgrad in der Umsetzung	-	Niedrig	Mittel bis Hoch	Mittel bis Hoch	Sehr Hoch	Sehr Hoch
Tool-Unterstützung	-	wenige	wenige	Ja	Ja	?
Prüffähigkeit (Soll-Ist)	-	Niedrig	Gut	Sehr gut	Gut	Gut
Ergebnis – Wirkung – Ziel	?	Niedrig	Gut	Sehr gut	Mittel	Mittel
Zertifizierung international anerkannt	Nein	Nein	Nein	Ja	Ja	Nein

Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz

22. Juni 2026

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
Experte für Datenschutz und Informationssicherheit
ISO 27001, ISO 27701 Lead-Auditor, Fachbegutachter der DAkkS
0179 2184795 - mail@heiko-behrendt.de - https://www.heiko-behrendt.de