

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.

Daten

• Prozesse, Systeme
• Schutzbedarf
• Gefährdungen
• Technische u. organisatorische Maßnahmen (TOM)

Sicherheit

- Art. 5
- Art. 24
- Art. 25
- Art. 28
- Art. 32
- etc.

• Prozesse, Systeme
• Schutzbedarf
• Gefährdungen
• Technische u. organisatorische Maßnahmen (TOM)

- Controls
- Anforderungen
- 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	
Z W E C K	<ul style="list-style-type: none"> - Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten - Schutz des informationellen Selbstbestimmungsrechts der betroffenen Personen 	<ul style="list-style-type: none"> - Schutz der Prozesse und der Informationen des Unternehmens bzw. der Behörde - Festlegung von Assets/Werten 	
	Datenschutzrecht	Datensicherheit	Informationssicherheit
K E R N E L E M E N T E	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> - Risikoanalyse - Schutzbedürftigkeit - Datenschutz durch Technikgestaltung und Voreinstellungen - Technische und organisatorische Sicherheitsmaßnahmen - Dokumentation der Datenverarbeitungsprozesse - Überwachung und Audits 	<ul style="list-style-type: none"> - 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
§	<ul style="list-style-type: none"> - Datenschutzvorschriften müssen Behörden und Unternehmen beachten! 	<ul style="list-style-type: none"> - Keine gesetzliche Vorschrift 	

Datenschutz auf der Basis eines Standards zur Informationssicherheit



Datenschutz- u. Informationssicherheitsmanagement

Basis: DISM-Team

Abhängig von der **Größe** der Organisation:

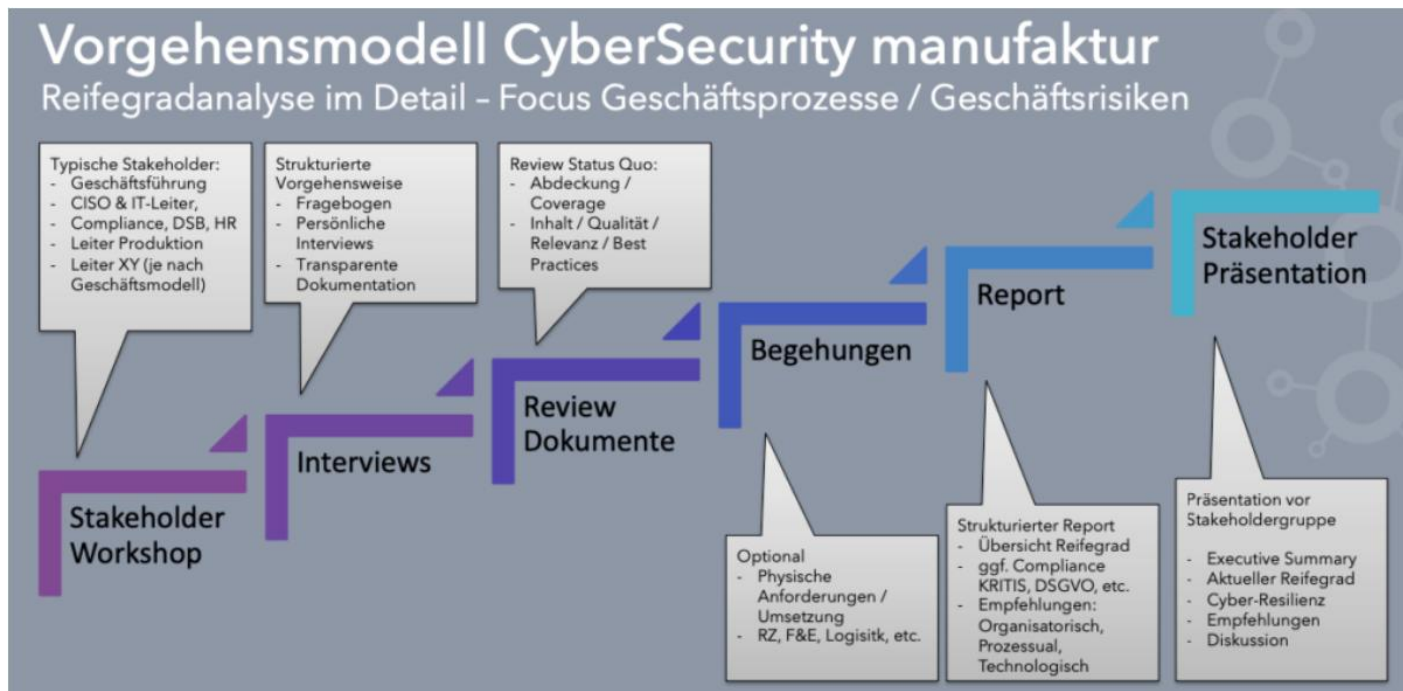
- Mindestens ein „**Datenverantwortlicher**“
(Behörden- oder Abteilungsleiter,
Geschäftsführer)
- Datenschutzbeauftragter
- Informationssicherheitsbeauftragter
- Leiter IT-Abteilung
- Ggf. Koordinatoren in den Fachabteilungen
- Ggf. Leiter Revisionsabteilung
- Ggf. Personal- bzw. Betriebsrat
- Ggf. DSB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

Schadenskalkulation – Worst-Case!

1. Welcher finanzielle Schaden ist für das Unternehmen kritisch ?	1.000 €
	10.000 €
2. Wie wahrscheinlich ist der Eintritt eines Schadens?	50.000 €
	100.000 €
	<hr/>
Zahlungsunfähig?!	200.000 €
	500.000 €

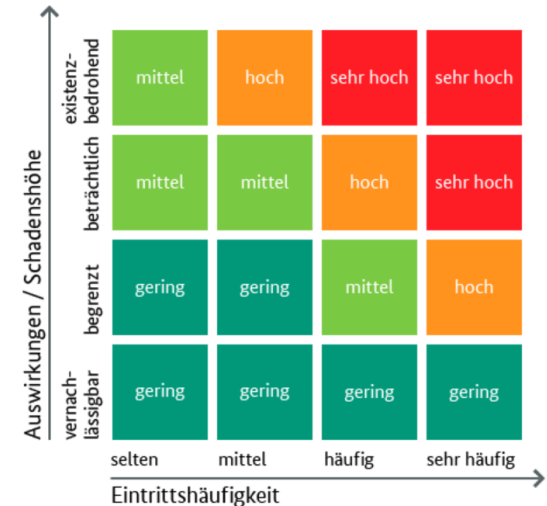
Beispiel Schadenskalkulation

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/>

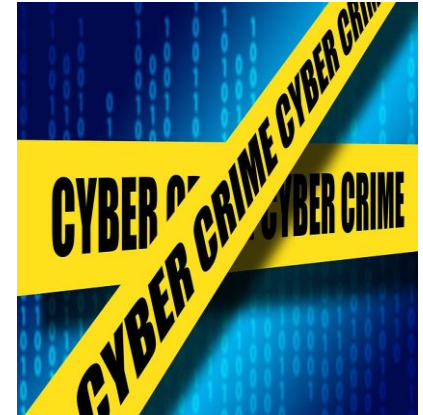
Standards zur Informationssicherheit und zum Datenschutz

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 prüfbar!
- 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) schützt 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 Datenschutzerfordernungen** 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 **Geschäftsprozessen** 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)

Heiko Behrendt

VdS 10000 : 2018-12 (02)

Informationssicherheitsmanagementsystem
für kleine und mittlere Unternehmen (KMU)

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

1	Allgemeines	6
1.1	Anwendungshinweise	6
1.2	Anwendungs- und Geltungsbereich	6
1.3	Gültigkeit	6
2	Normative Verweise	7
3	Begriffe	7
4	Organisation der Informationssicherheit	12
4.1	Verantwortlichkeiten	12
4.1.1	Zuweisung und Dokumentation	12
4.1.2	Funktionstrennungen	12
4.1.3	Zeitliche Ressourcen	12
4.1.4	Delegieren von Aufgaben	13
4.2	Topmanagement	13
4.3	Informationssicherheitsbeauftragter (ISB)	13
4.4	Informationssicherheitsteam (IST)	13
4.5	IT-Verantwortliche	14
4.6	Administratoren	14
4.7	Vorgesetzte	14
4.8	Mitarbeiter	14
4.9	Projektverantwortliche	14
4.10	Externe	15
5	Leitlinie zur Informationssicherheit (IS-Leitlinie)	15
5.1	Allgemeine Anforderungen	15
5.2	Inhalte	15
6	Richtlinien zur Informationssicherheit (IS-Richtlinien)	15
6.1	Allgemeine Anforderungen	15
6.2	Inhalte	16
6.3	Regelungen für Nutzer	16
6.4	Weitere Regelungen	17

7	Mitarbeiter	17
7.1	Vor Aufnahme der Tätigkeit.....	17
7.2	Aufnahme der Tätigkeit.....	17
7.3	Beendigung oder Wechsel der Tätigkeit.....	18
8	Wissen	18
8.1	Aktualität des Wissens.....	18
8.2	Schulung und Sensibilisierung.....	18
9	Identifizieren kritischer IT-Ressourcen	19
9.1	Prozesse.....	19
9.2	Informationen.....	19
9.3	IT-Ressourcen.....	20
10	IT-Systeme	21
10.1	Inventarisierung.....	21
10.2	Lebenszyklus.....	21
10.2.1	Inbetriebnahme und Änderung.....	21
10.2.2	Ausmusterung und Wiederverwendung.....	22
10.3	Basisschutz.....	22
10.3.1	Software.....	22
10.3.2	Beschränkung des Netzwerkverkehrs.....	22
10.3.3	Protokollierung.....	23
10.3.4	Externe Schnittstellen und Laufwerke.....	23
10.3.5	Schadsoftware.....	23
10.3.6	Starten von fremden Medien.....	23
10.3.7	Authentifizierung.....	24
10.3.8	Zugänge und Zugriffe.....	24
10.4	Zusätzliche Maßnahmen für mobile IT-Systeme.....	24
10.4.1	IS-Richtlinie.....	24
10.4.2	Schutz der Informationen.....	25
10.4.3	Verlust.....	25
10.5	Zusätzliche Maßnahmen für kritische IT-Systeme.....	25
10.5.1	Risikoanalyse und -behandlung.....	25
10.5.2	Notbetriebsniveau.....	25
10.5.3	Robustheit.....	26
10.5.4	Externe Schnittstellen und Laufwerke.....	26
10.5.5	Änderungsmanagement.....	26
10.5.6	Dokumentation.....	26
10.5.7	Datensicherung.....	26
10.5.8	Überwachung.....	26
10.5.9	Ersatzsysteme und -verfahren.....	27
10.5.10	Kritische Individualsoftware.....	27
11	Netzwerke und Verbindungen	27
11.1	Netzwerkplan.....	27
11.2	Aktive Netzwerkkomponenten.....	27
11.3	Netzübergänge.....	27
11.4	Basisschutz.....	28
11.4.1	Netzwerkanschlüsse.....	28
11.4.2	Segmentierung.....	28
11.4.3	Fernzugang.....	29
11.4.4	Netzwerkkopplung.....	29
11.5	Zusätzliche Maßnahmen für kritische Verbindungen.....	29

12	Mobile Datenträger	29
12.1	IS-Richtlinie.....	29
12.2	Schutz der Informationen.....	30
12.3	Zusätzliche Maßnahmen für kritische mobile Datenträger.....	30
13	Umgebung	30
13.1	Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen.....	30
13.2	Datenleitungen.....	30
13.3	Zusätzliche Maßnahmen für kritische IT-Systeme.....	31
14	IT-Outsourcing und Cloud Computing	31
14.1	IS-Richtlinie.....	31
14.2	Vorbereitung.....	31
14.3	Vertragsgestaltung.....	31
14.4	Zusätzliche Maßnahmen für kritische IT-Ressourcen.....	32
15	Zugänge und Zugriffsrechte	33
15.1	Verwaltung.....	33
15.2	Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen.....	33
16	Datensicherung und Archivierung	33
16.1	IS-Richtlinie.....	33
16.2	Archivierung.....	34
16.3	Verfahren.....	34
16.4	Weiterentwicklung.....	34
16.5	Basisschutz.....	34
16.5.1	Speicherorte.....	35
16.5.2	Server.....	35
16.5.3	Aktive Netzwerkkomponenten.....	35
16.5.4	Mobile IT-Systeme.....	35
16.6	Zusätzliche Maßnahmen für kritische IT-Systeme.....	35
16.6.1	Risikoanalyse.....	35
16.6.2	Verfahren.....	35
17	Störungen und Ausfälle	35
17.1	IS-Richtlinie.....	36
17.2	Reaktion.....	36
17.3	Zusätzliche Maßnahmen für kritische IT-Systeme.....	36
17.3.1	Wiederanlaufpläne.....	37
17.3.2	Abhängigkeiten.....	37
18	Sicherheitsvorfälle	37
18.1	IS-Richtlinie.....	37
18.2	Erkennen.....	38
18.3	Reaktion.....	38
Anhang A	Anhang	39
A.1	Verfahren.....	39
A.2	Risikoanalyse und -behandlung.....	39
A.2.1	Risikoanalyse.....	39
A.2.2	Risikobehandlung.....	39
A.2.3	Wiederholung und Anpassung.....	40
Anhang B	Register der Änderungen gegenüber der Vorgängerversion VdS 3473 : 2015-07 (01)	41

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)

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

1	Allgemeines	6
1.1	Geltungsbereich	6
1.2	Anwendungshinweise	6
1.3	Gültigkeit	7
2	Normative Verweise	7
3	Begriffe	7
4	Organisation des Datenschutzes	10
4.1	Verantwortlichkeiten	10
4.1.1	Zuweisung und Dokumentation	10
4.1.2	Funktionstrennungen	10
4.1.3	Ressourcen	11
4.1.4	Delegieren von Aufgaben	11
4.2	Topmanagement	11
4.3	Datenschutzmanager (DSM)	11
4.4	Datenschutzbeauftragter (DSB)	12
4.5	Datenschutzteam (DST)	12
4.6	Eigentümer einer Verarbeitung	13
4.7	Vorgesetzte	13
4.8	Mitarbeiter	13
4.9	Projektverantwortliche	13
4.10	Auftragsverarbeiter	13

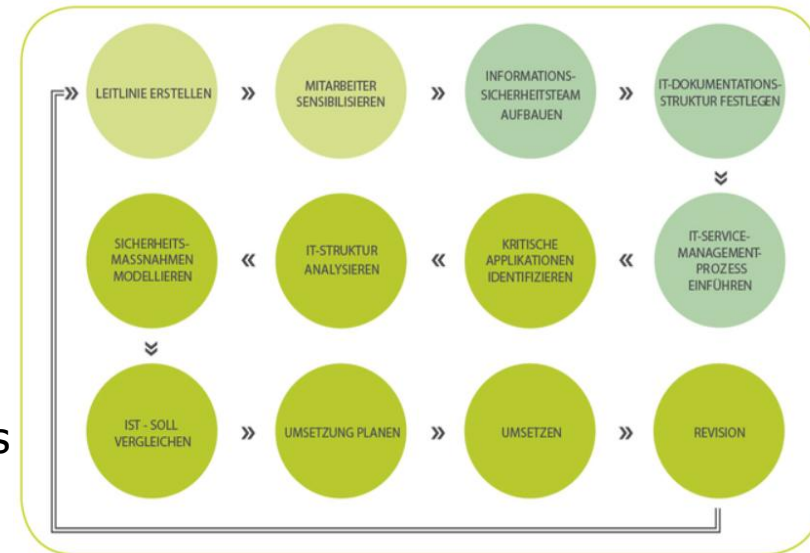
CISIS 12 Version 3.0

IT-Sicherheitscluster e.V. (Regensburg)

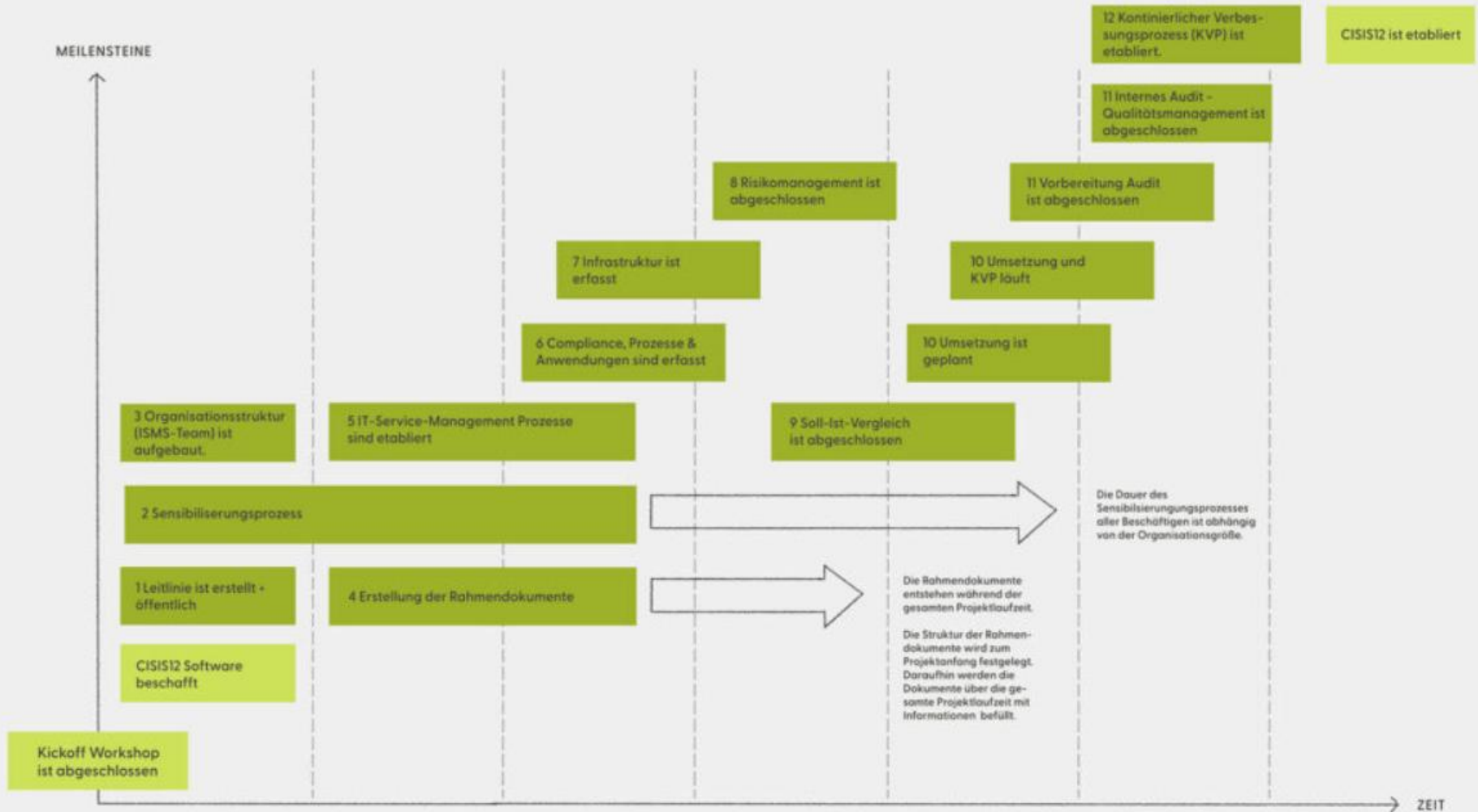
- **C**ompliance-**I**nformations-**S**icherheits-**M**anagement-**S**ystem in 12 Schritten.
- CISIS12 in der Version 3.0 ist eine **Weiterentwicklung** und Erweiterung des Informationsmanagementsystems ISIS12.
- Der Schwerpunkt liegt auf dem Thema **Compliance**.
- Der **Standard** besteht aus einer **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.

ISIS 12

Informationssicherheit
für den Mittelstand



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



GEMEINSAME PRINZIPIEN AUFBAUEN

- 1 Leitlinie erstellen
- 2 Beschäftigte sensibilisieren

RAHMEN-BEDINGUNGEN AUFBAUEN

- 3 Informationssicherheit steuern 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 - Qualitätsmanagement
- 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

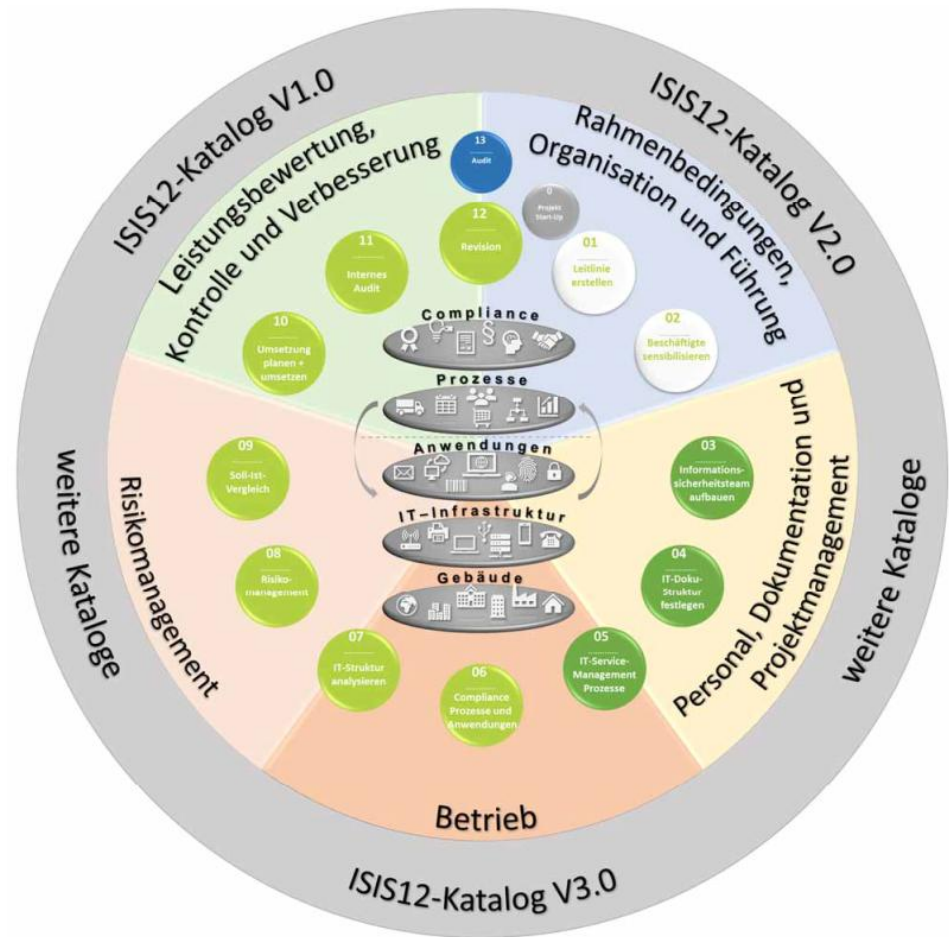


Abbildung 2: ISIS-Vorgehensmodell und Managementsystemmodell V3.0

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®-Kreuzreferenztable Version 1.0 (PDF)

Die CISIS12®-Kreuzreferenztable 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® 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 **Stufenmodell** 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

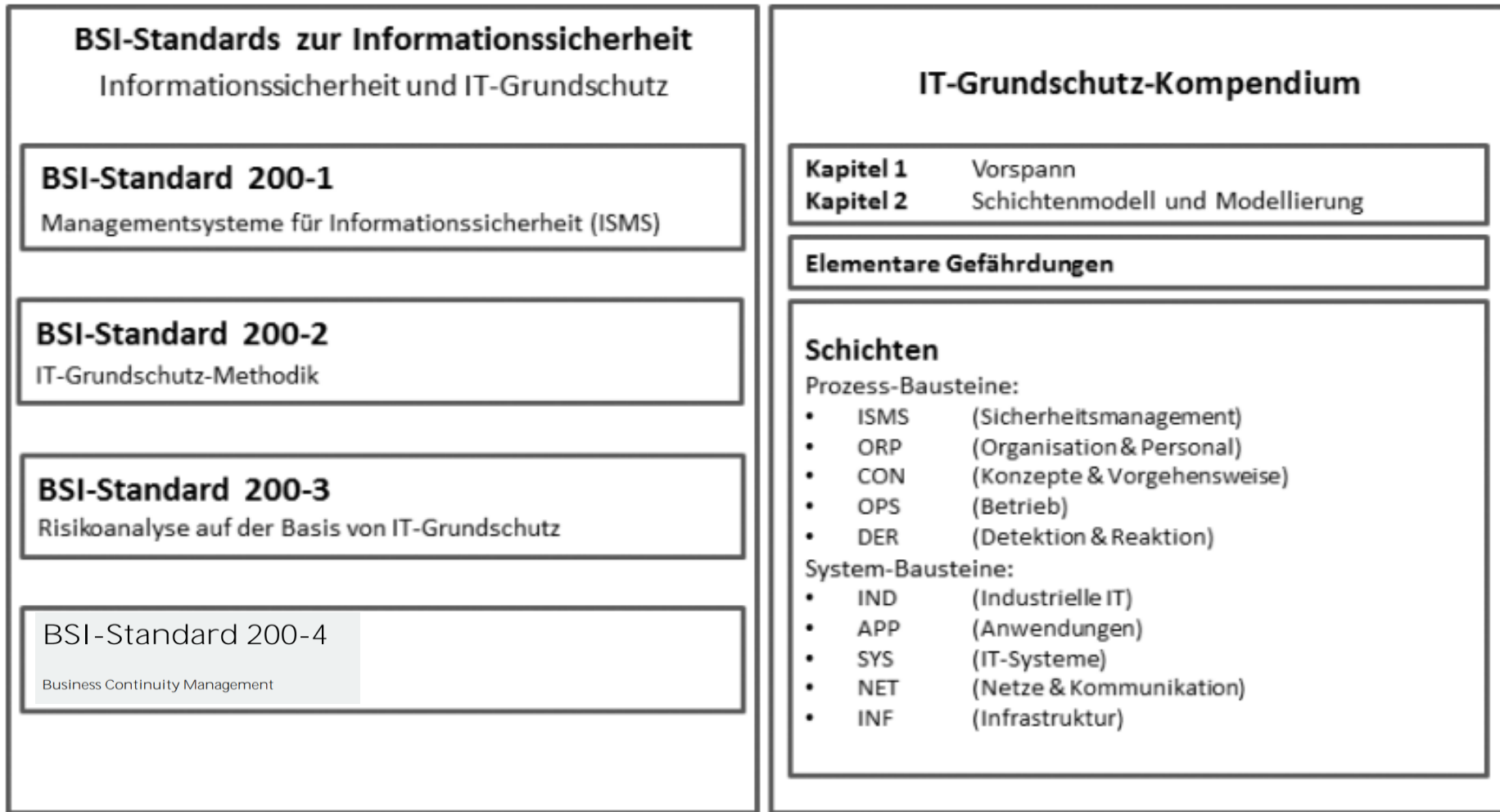
Das BSI als die Cybersicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

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

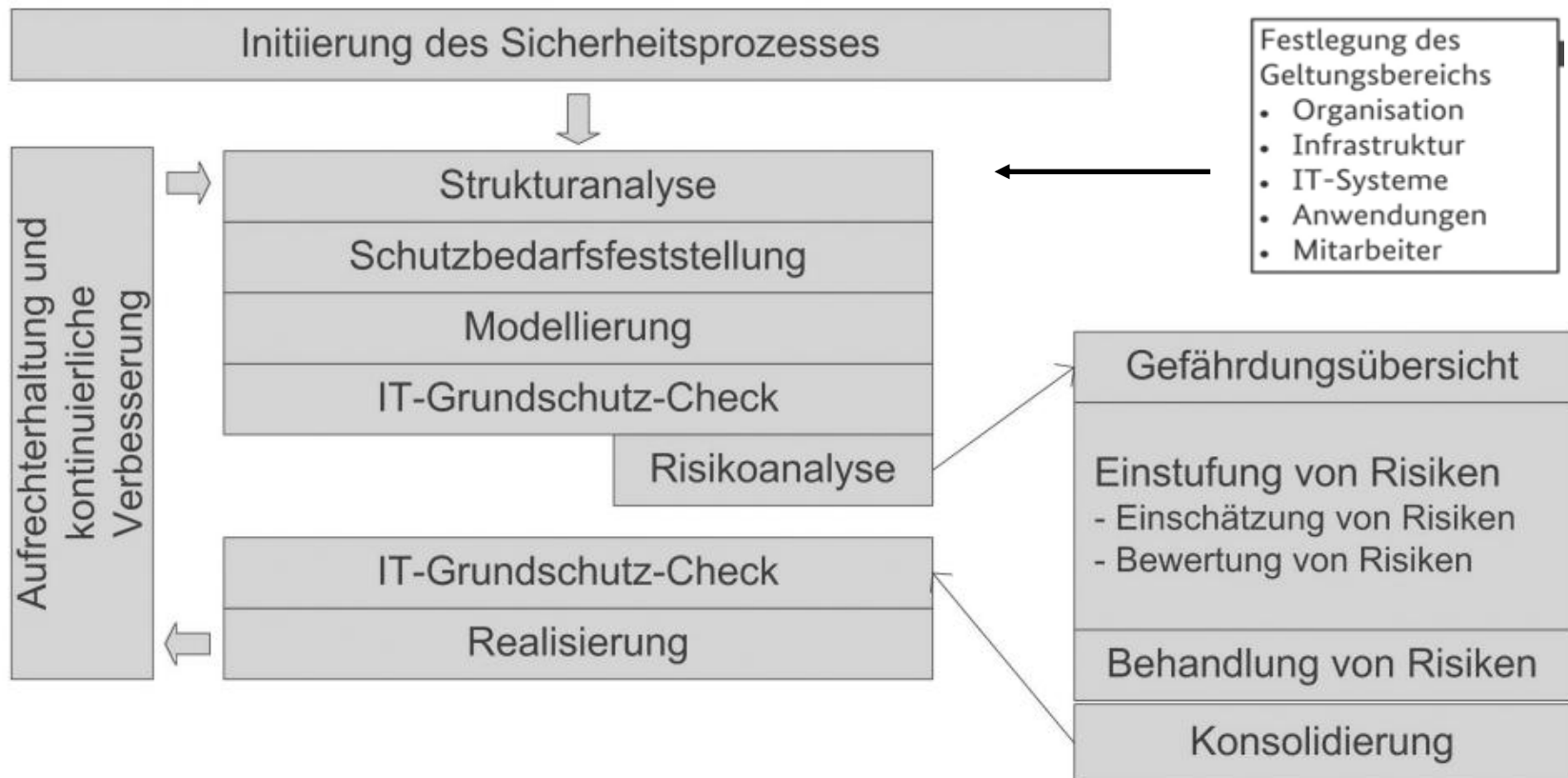
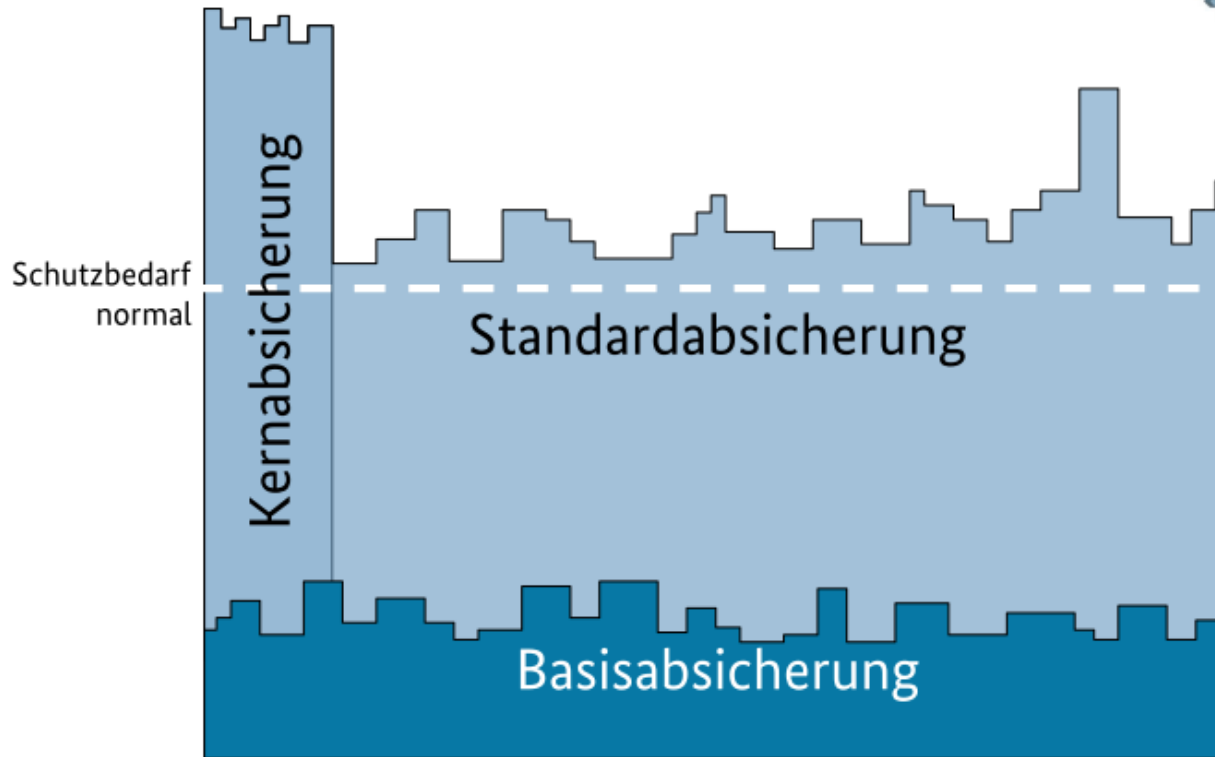


Abbildung 32: Integration der Risikoanalyse in den IT-Grundschutz-Prozess

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

Stufenmodell

Vorgehensweisen Überblick

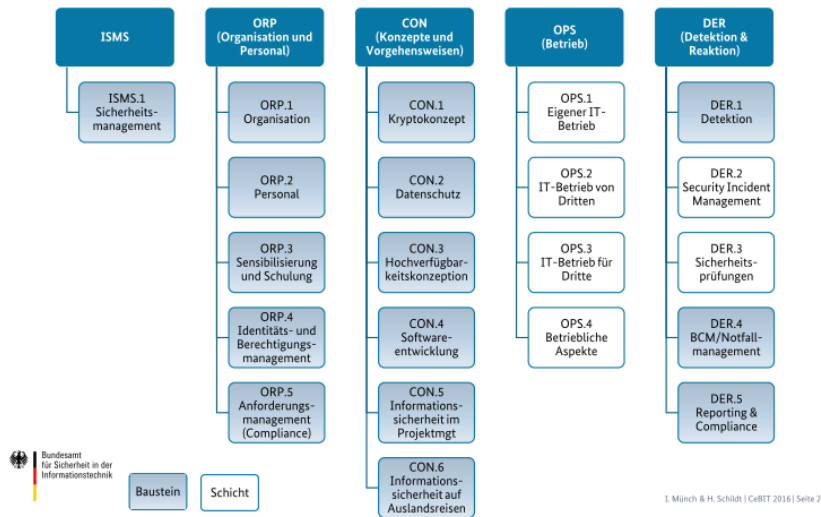


I. Münch & H. Schildt | CeBIT 2016 | Seite 10

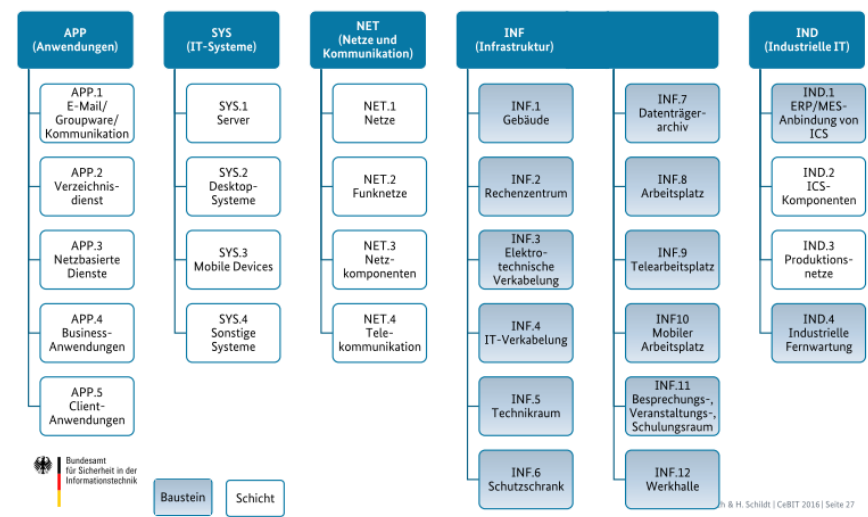
Quelle: <https://www.bsi.bund.de>

IT-Grundschutz-Kompendium

Struktur der Kataloge Prozess-Bausteine



Struktur der Kataloge System-Bausteine



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, Bausteinzuzuordnung, 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

The screenshot displays the verinice.EVAL software interface, which is used for defining and implementing Technical Organizational Measures (TOMs) based on the IT-Grundschutz standard. The interface is divided into several panes:

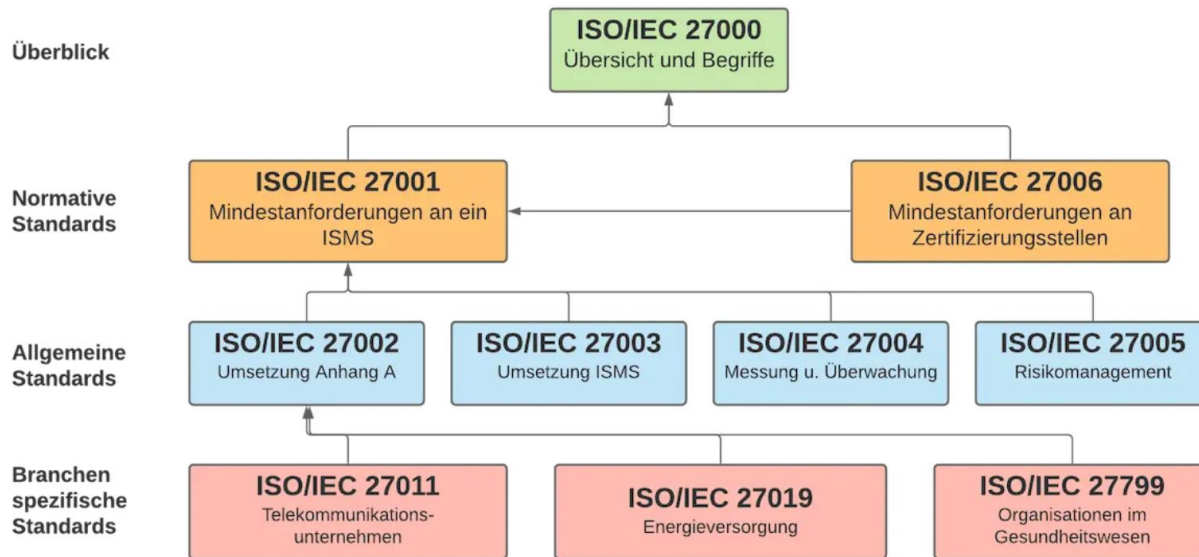
- Kataloge (Catalogs):** Shows a hierarchical tree of the IT-Grundschutz-Kompendium 11.1 Edition 2023, with 'SYS IT-Systeme' expanded to show various system categories like 'Allgemeiner Server', 'Windows Server', and 'Allgemeine Smartphones und Tablets'.
- Modernisierter IT-Grundschutz:** Displays the specific configuration for 'Informationsverbund-NoRiskConsulting'. The 'IT-Systeme' category is expanded, and 'SYS.3.2.1 Allgemeine Smartphones und Tablets' is selected.
- Objektbrowser (Object Browser):** Provides a detailed description and introduction for the selected TOM. The description states: 'Smartphones sind auf den mobilen Einsatz ausgerichtete IT-Systeme mit einer angepassten Oberfläche, die mit einem großen, üblicherweise berührungsempfindlichen Bildschirm (Touch-Display) bedient werden können. Smartphones vereinen neben der Telefonie beispielsweise Media-Player, Personal Information Manager und Digitalkamera in einem Gerät und bieten den Benutzenden darüber hinaus viele weitere Anwendungen und Funktionen, wie Webbrowser, E-Mail-Client oder Ortung (z. B. über GPS). Zudem sind sie mit Mobilfunk-, WLAN-, Bluetooth- sowie NFC-Schnittstellen ausgestattet. Tablets sind, vereinfacht gesagt, Smartphones mit großer Formfaktor...'.
- SYS.3.2.1 Allgemeine...:** A configuration pane for the selected TOM, showing fields for 'Identifier' (SYS.3.2.1), 'Titel' (Allgemeine Smartphones und Tablets), 'Beschreibung', 'Bearbeitungsreihenfolge' (R2), 'Tags', 'Letzte Änderung' (01.02.2023), 'Release' (2023-1), and 'Änderungstyp'.

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.



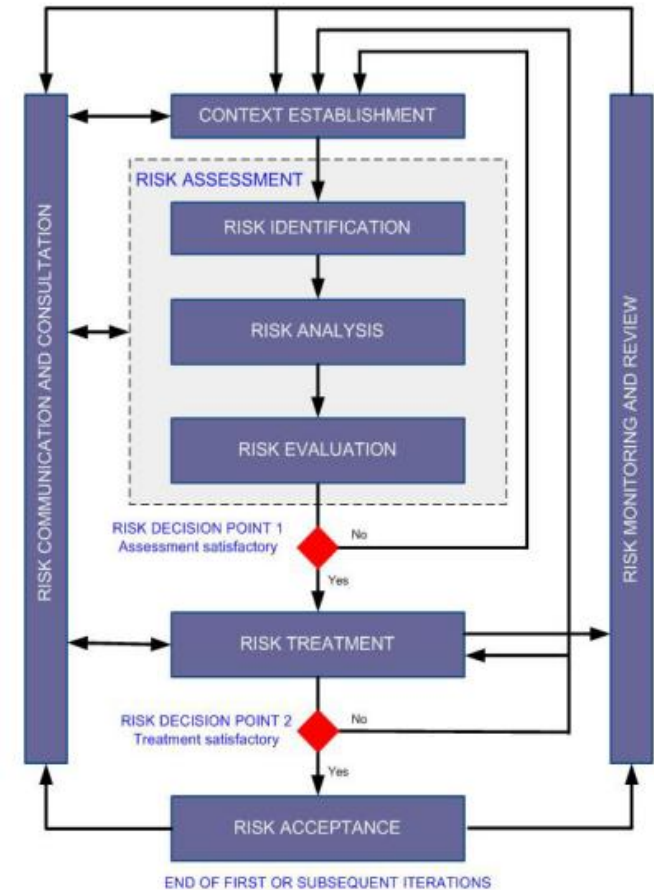
Quelle: https://de.wikipedia.org/wiki/ISO/IEC_27001

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



ISO 27001

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

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

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Kontext der Organisation	7
4.1 Verstehen der Organisation und ihres Kontextes	7
4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien	7
4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	8
4.4 Informationssicherheitsmanagementsystem	8
5 Führung	8
5.1 Führung und Verpflichtung	8
5.2 Politik	9
5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	9
6 Planung	9
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	9
6.1.1 Allgemeines	9
6.1.2 Informationssicherheitsrisikobeurteilung	10
6.1.3 Informationssicherheitsrisikobehandlung	10
6.2 Informationssicherheitsziele und Planung zu deren Erreichung	11
6.3 Planung von Änderungen	12
7 Unterstützung	12
7.1 Ressourcen	12
7.2 Kompetenz	12
7.3 Bewusstsein	12
7.4 Kommunikation	13
7.5 Dokumentierte Information	13
7.5.1 Allgemeines	13
7.5.2 Erstellen und Aktualisieren	13
7.5.3 Steuerung dokumentierter Information	13
8 Betrieb	14
8.1 Betriebliche Planung und Steuerung	14
8.2 Informationssicherheitsrisikobeurteilung	14
8.3 Informationssicherheitsrisikobehandlung	14
9 Bewertung der Leistung	14
9.1 Überwachung, Messung, Analyse und Bewertung	14
9.2 Internes Audit	15
9.2.1 Allgemeines	15
9.2.2 Internes Auditprogramm	15
9.3 Managementbewertung	16
9.3.1 Allgemeines	16
9.3.2 Eingaben für die Managementbewertung	16
9.3.3 Ergebnisse der Managementbewertung	16
10 Verbesserung	16
10.1 Fortlaufende Verbesserung	16
10.2 Nichtkonformität und Korrekturmaßnahmen	16
Anhang A (normativ) Verweisung auf Informationssicherheitsmaßnahmen	18
Literaturhinweise	27

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	Maßnahme
5.1	Informationssicherheitspolitik und -richtlinien	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	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.
5.3	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.
5.4	Verantwortlichkeiten der Leitung	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	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.
5.6	Kontakt mit speziellen Interessensgruppen	Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.
5.7	Informationen über die Bedrohungslage	Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.
5.8	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss in das Projektmanagement integriert werden.
5.9	Inventar der Informationen und anderen damit verbundenen Werte	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)

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

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	10
2 Normative Verweisungen	10
3 Begriffe und Abkürzungen	10
3.1 Begriffe	10
3.2 Abkürzungen	16
4 Aufbau dieses Dokuments	17
4.1 Abschnitte	17
4.2 Themen und Attribute	18
4.3 Maßnahmengestaltung	19
5 Organisatorische Maßnahmen	20
5.1 Informationssicherheitspolitik und -richtlinien	20
5.2 Informationssicherheitsrollen und -verantwortlichkeiten	22
5.3 Aufgabentrennung	23
5.4 Verantwortlichkeiten der Leitung	25
5.5 Kontakt mit Behörden	26
5.6 Kontakt mit speziellen Interessengruppen	27
5.7 Informationen über die Bedrohungslage	27
5.8 Informationssicherheit im Projektmanagement	29
5.9 Inventar der Informationen und anderer damit verbundener Werte	31
5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	33
5.11 Rückgabe von Werten	35
5.12 Klassifizierung von Informationen	36
5.13 Kennzeichnung von Informationen	38
5.14 Informationsübermittlung	39
5.15 Zugangssteuerung	42
5.16 Identitätsmanagement	45
5.17 Authentisierungsinformationen	46
5.18 Zugangsrechte	49
5.19 Informationssicherheit in Lieferantenbeziehungen	51
5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen	53
5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette	56
5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	58
5.23 Informationssicherheit für die Nutzung von Cloud-Diensten	60
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	63
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse	65
5.26 Reaktion auf Informationssicherheitsvorfälle	66
5.27 Erkenntnisse aus Informationssicherheitsvorfällen	67
5.28 Sammeln von Beweismaterial	68
5.29 Informationssicherheit bei Störungen	69
5.30 IKT-Bereitschaft für Business-Continuity	70
5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	71
5.32 Geistige Eigentumsrechte	73
5.33 Schutz von Aufzeichnungen	75
5.34 Datenschutz und Schutz personenbezogener Daten (pbd)	77
5.35 Unabhängige Überprüfung der Informationssicherheit	78
5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	79
5.37 Dokumentierte Betriebsabläufe	80
6 Personenbezogene Maßnahmen	82
6.1 Sicherheitsüberprüfung	82
6.2 Beschäftigungs- und Vertragsbedingungen	83
6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung	85
6.4 Maßregelungsprozess	87
6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	88
6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen	89
6.7 Remote-Arbeit	90
6.8 Meldung von Informationssicherheitsereignissen	92
7 Physische Maßnahmen	93
7.1 Physische Sicherheitsperimeter	93
7.2 Physischer Zutritt	94
7.3 Sichern von Büros, Räumen und Einrichtungen	96
7.4 Physische Sicherheitsüberwachung	97
7.5 Schutz vor physischen und umweltbedingten Bedrohungen	98
7.6 Arbeiten in Sicherheitsbereichen	100
7.7 Aufgeräumte Arbeitsumgebung und Bildschirmsperren	101
7.8 Platzierung und Schutz von Geräten und Betriebsmitteln	102
7.9 Sicherheit von Werten außerhalb der Räumlichkeiten	103
7.10 Speichermedien	104
7.11 Versorgungseinrichtungen	106
7.12 Sicherheit der Verkabelung	107
7.13 Instandhaltung von Geräten und Betriebsmitteln	108
7.14 Sichere Entsorgung und Wiederverwendung von Geräten und Betriebsmitteln	109
8 Technologische Maßnahmen	111
8.1 Endpunktgeräte des Benutzers	111
8.2 Privilegierte Zugangsrechte	113
8.3 Informationszugangsbeschränkung	115
8.4 Zugriff auf den Quellcode	117
8.5 Sichere Authentisierung	118
8.6 Kapazitätssteuerung	120
8.7 Schutz gegen Schadsoftware	122
8.8 Handhabung von technischen Schwachstellen	124
8.9 Konfigurationsmanagement	128
8.10 Löschung von Informationen	130
8.11 Datenmaskierung	132
8.12 Verhinderung von Datenlecks	134
8.13 Sicherung von Informationen	135
8.14 Redundanz von informationsverarbeitenden Einrichtungen	137
8.15 Protokollierung	138
8.16 Überwachung von Aktivitäten	142
8.17 Uhrensynchronisation	144
8.18 Gebrauch von Hilfsprogrammen mit privilegierten Rechten	145
8.19 Installation von Software auf Systemen in Betrieb	146
8.20 Netzwerksicherheit	148
8.21 Sicherheit von Netzwerkdiensten	149
8.22 Trennung von Netzwerken	150
8.23 Webfilterung	152
8.24 Verwendung von Kryptographie	153

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 Auftragsdatenverarbeitung** (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

	Seite			
Europäisches Vorwort	5	B.1	Hinweis zur Umsetzung für verantwortliche Stellen	38
Vorwort	6	B.1.1	Allgemeines	38
Einleitung	7	B.1.2	Bedingungen für die Erhebung und Verarbeitung	38
1 Anwendungsbereich	8	B.1.3	Verpflichtungen gegenüber betroffenen Personen	43
2 Normative Verweisungen	8	B.1.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	48
3 Begriffe und Abkürzungen	8	B.1.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten	51
4 Kontext der Organisation	12	B.2	Hinweis zur Umsetzung für Auftragsverarbeiter	53
4.1 Verstehen der Organisation und ihres Kontextes	12	B.2.1	Allgemeines	53
4.2 Verstehen der Erfordernisse und Erwartungen der interessierten Parteien	13	B.2.2	Bedingungen für die Erhebung und Verarbeitung	53
4.3 Festlegung des Anwendungsbereichs des Datenschutz-Managementsystems	13	B.2.3	Verpflichtungen gegenüber betroffenen Personen	55
4.4 Datenschutz-Managementsystem	14	B.2.4	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	56
5 Führung	14	B.2.5	Weitergabe, Übertragung und Offenlegung von personenbezogenen Daten	57
5.1 Führung und Verpflichtung	14	B.3	Hinweis zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter	60
5.2 Datenschutzpolitik	14	B.3.1	Zielsetzung	60
5.3 Rollen, Verantwortlichkeiten und Befugnisse	15	B.3.2	Allgemeines	61
6 Planung	15	B.3.3	Informationssicherheitspolitik und -richtlinien	61
6.1 Maßnahmen zum Umgang mit Risiken und Chancen	15	B.3.4	Informationssicherheitsrollen und -verantwortlichkeiten	61
6.1.1 Allgemeines	15	B.3.5	Klassifizierung von Informationen	62
6.1.2 Datenschutz-Risikobeurteilung	16	B.3.6	Kennzeichnung von Informationen	62
6.1.3 Datenschutz-Risikobehandlung	16	B.3.7	Informationsübermittlung	62
6.2 Datenschutzziele und Planung zu deren Erreichung	18	B.3.8	Identitätsmanagement	63
6.3 Planung von Änderungen	18	B.3.9	Zugangsrechte	63
7 Unterstützung	19	B.3.10	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	64
7.1 Ressourcen	19	B.3.11	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	64
7.2 Kompetenz	19	B.3.12	Reaktion auf Informationssicherheitsvorfälle	64
7.3 Bewusstsein	19	B.3.13	Juristische, gesetzliche, regulatorische und vertragliche Anforderungen	66
7.4 Kommunikation	19	B.3.14	Schutz von Aufzeichnungen	67
7.5 Dokumentierte Information	19	B.3.15	Unabhängige Überprüfung der Informationssicherheit	67
7.5.1 Allgemeines	19	B.3.16	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	67
7.5.2 Erstellen und Aktualisieren dokumentierter Information	20	B.3.17	Informationssicherheitsbewusstsein, -ausbildung und -schulung	68
7.5.3 Lenkung dokumentierter Information	20	B.3.18	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	68
8 Betrieb	20	B.3.19	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	69
8.1 Betriebliche Planung und Steuerung	20	B.3.20	Speichermedien	69
8.2 Datenschutz-Risikobeurteilung	21	B.3.21	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	70
8.3 Datenschutz-Risikobehandlung	21	B.3.22	Endpunktgeräte des Benutzers	70
9 Leistungsbewertung	21	B.3.23	Sichere Authentifizierung	70
9.1 Überwachung, Messung, Analyse und Bewertung	21	B.3.24	Sicherung von Informationen	70
9.2 Internes Audit	21	B.3.25	Protokollierung	71
9.2.1 Allgemeines	21	B.3.26	Verwendung von Kryptographie	72
9.2.2 Internes Auditprogramm	22	B.3.27	Lebenszyklus einer sicheren Entwicklung	73
9.3 Managementbewertung	22	B.3.28	Anforderungen an die Anwendungssicherheit	73
9.3.1 Allgemeines	22	B.3.29	Sichere Systemarchitektur und Entwicklungsgrundsätze	74
9.3.2 Eingaben für die Managementbewertung	22	B.3.30	Ausgegliederte Entwicklung	74
9.3.3 Ergebnisse der Managementbewertung	23	B.3.31	Testdaten	74
10 Verbesserung	23	Anhang C (informativ) Zuordnung zu ISO/IEC 29100		75
10.1 Fortlaufende Verbesserung	23	Anhang D (informativ) Zuordnung zur Datenschutz-Grundverordnung		78
10.2 Nichtkonformität und Korrekturmaßnahmen	23	Anhang E (informativ) Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151		82
11 Weitere Informationen zu Anhängen	23	Anhang F (informativ) Übereinstimmung mit ISO/IEC 27701:2019		85
Anhang A (normativ) DSMS-Referenzmaßnahmenziele und -Maßnahmen für verantwortliche Stellen und Auftragsverarbeiter	25	Literaturhinweise		93
Anhang B (normativ) Hinweis zur Umsetzung für verantwortliche Stellen und Auftragsverarbeiter	38			

Tabellen

Tabelle A.1 — Maßnahmenziele und Maßnahmen für verantwortliche Stellen	25
Tabelle A.2 — Maßnahmenziele und Maßnahmen für Auftragsverarbeiter	29

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 Sicherheitsmaßnahmen 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.

NIST SP 800-53, REV. 5


SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

Table of Contents

CHAPTER ONE INTRODUCTION.....	1
1.1 PURPOSE AND APPLICABILITY.....	2
1.2 TARGET AUDIENCE.....	3
1.3 ORGANIZATIONAL RESPONSIBILITIES.....	3
1.4 RELATIONSHIP TO OTHER PUBLICATIONS.....	5
1.5 REVISIONS AND EXTENSIONS.....	5
1.6 PUBLICATION ORGANIZATION.....	5
CHAPTER TWO THE FUNDAMENTALS.....	7
2.1 REQUIREMENTS AND CONTROLS.....	7
2.2 CONTROL STRUCTURE AND ORGANIZATION.....	8
2.3 CONTROL IMPLEMENTATION APPROACHES.....	11
2.4 SECURITY AND PRIVACY CONTROLS.....	13
2.5 TRUSTWORTHINESS AND ASSURANCE.....	14
CHAPTER THREE THE CONTROLS.....	16
3.1 ACCESS CONTROL.....	18
3.2 AWARENESS AND TRAINING.....	59
3.3 AUDIT AND ACCOUNTABILITY.....	65
3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING.....	83
3.5 CONFIGURATION MANAGEMENT.....	96
3.6 CONTINGENCY PLANNING.....	115
3.7 IDENTIFICATION AND AUTHENTICATION.....	131
3.8 INCIDENT RESPONSE.....	149
3.9 MAINTENANCE.....	162
3.10 MEDIA PROTECTION.....	171
3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION.....	179
3.12 PLANNING.....	194
3.13 PROGRAM MANAGEMENT.....	203
3.14 PERSONNEL SECURITY.....	222
3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY.....	229
3.16 RISK ASSESSMENT.....	238
3.17 SYSTEM AND SERVICES ACQUISITION.....	249
3.18 SYSTEM AND COMMUNICATIONS PROTECTION.....	292
3.19 SYSTEM AND INFORMATION INTEGRITY.....	332
3.20 SUPPLY CHAIN RISK MANAGEMENT.....	363
REFERENCES	374
APPENDIX A GLOSSARY.....	394
APPENDIX B ACRONYMS.....	424
APPENDIX C CONTROL SUMMARIES.....	428

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 \(xlsx\)](#)

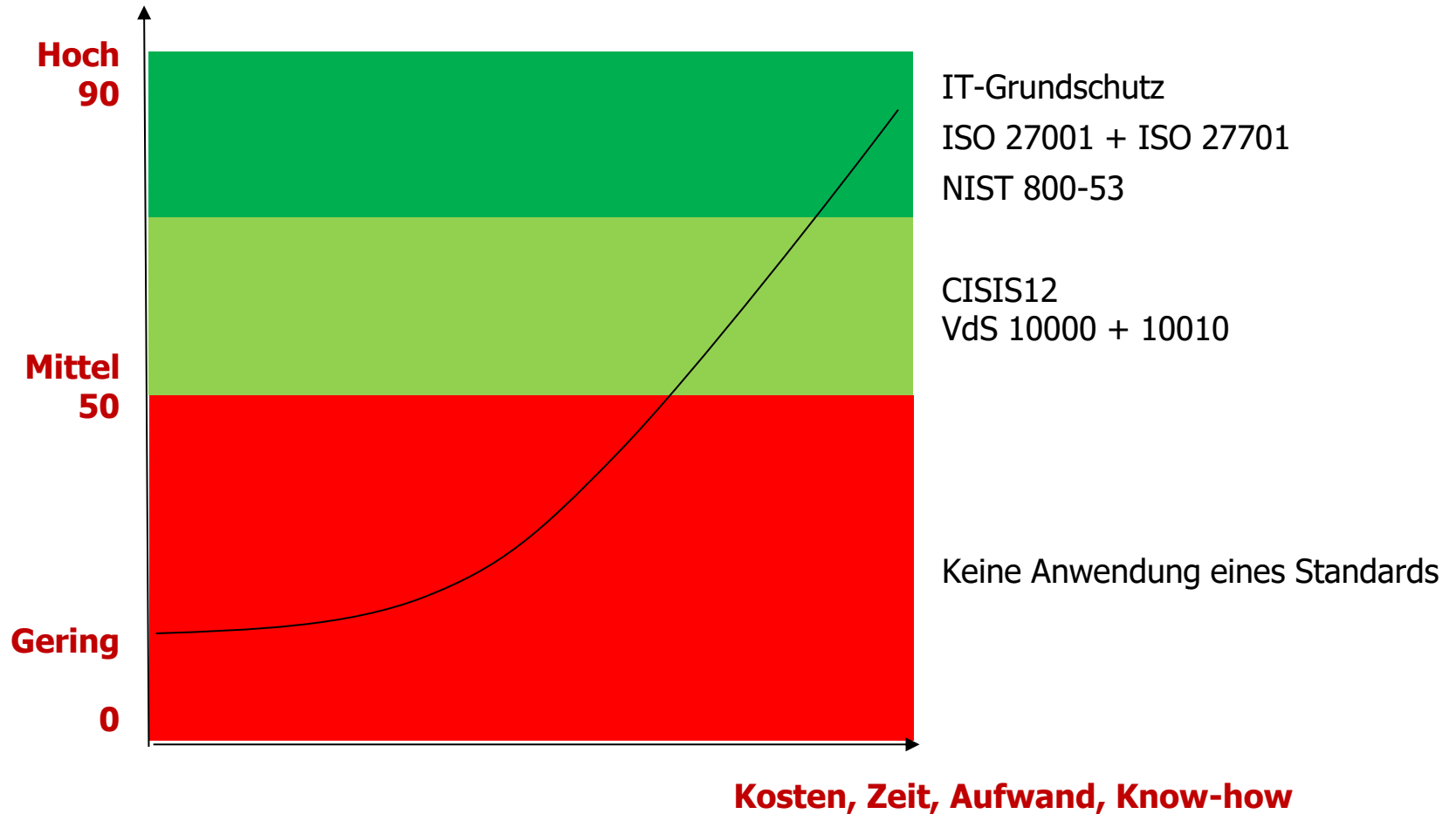
[Vorlage für einen Kontrollkollaborationsindex \(docx\)](#)

[Blogbeitrag](#)

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

Sicherheitsniveau zu Kosten, Zeit, Aufwand, Know-how

Sicherheitsniveau



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>