Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz SS 2024

10. Juni 2024

Standards zur Informationssicherheit

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

Themen

1. Abgrenzung Datenschutz und Informationssicherheit
2. Standards zur Informationssicherheit
   - VdS – Schadenverhütung GmbH
   - CISIS12 – IT-Sicherheitscluster e. V.
   - IT-Grundschutz – Bundesamts für Sicherheit in der Informationstechnik (BSI)
   - ISO 27001 – Internationale Norm für Informationssicherheitsmanagement
   - NIST 800-53 – National Institute of Standards and Technology

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.

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/standard/27001
- National Institute of Standards and Technology (NIST)
  https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

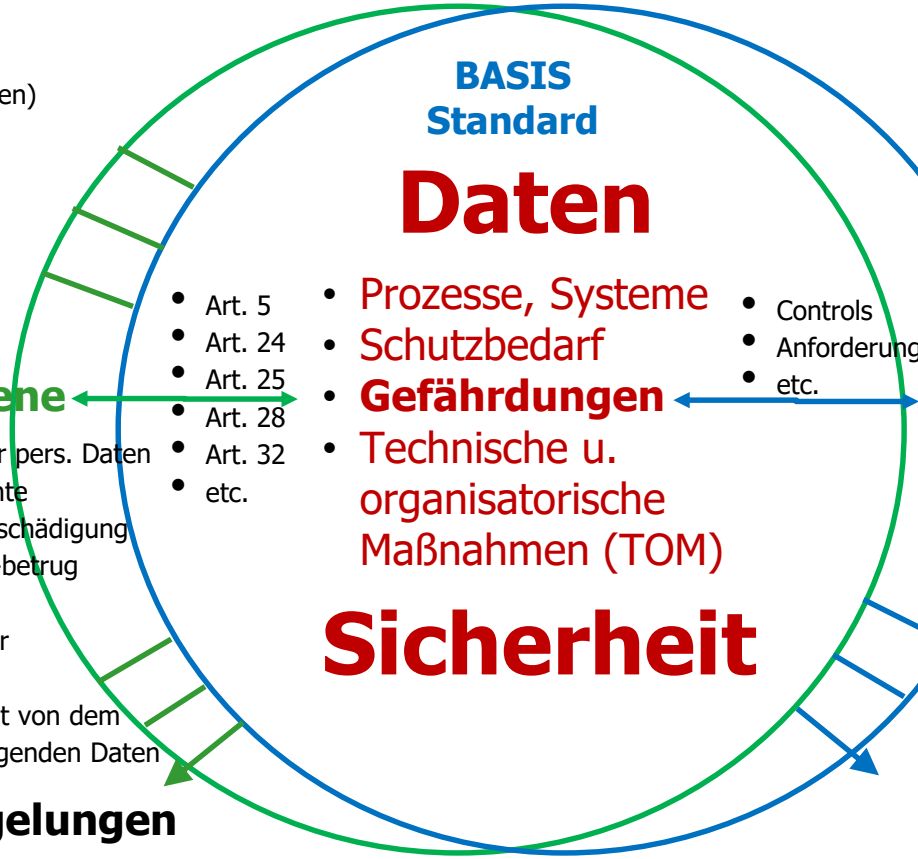
Datenschutz- und Informationssicherheit

Kombination – **Synthese**

Datenschutz DSGVO
Datenschutzanforderungen

Organisation

Informationssicherheit
ISMS



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.

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

- Controls
- Anforderungen
- etc.

Assets/Werte

Ziele

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

Risiken Organisation

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

Spezifische Regelungen

- ISO 27002
- ISO 27005
- BSIG (Kritische Infrastruktur)
- etc.

Datenschutz- und Informationssicherheitsmanagement

Kombination – **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 Technik-gestaltung und Voreinstellungen - Technische und organisatorische Sicherheitsmaßnahmen - Dokumentation der Daten-verarbeitungsprozesse - 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

Risikoanalyse – Gefährdungen

Mit welchen Maßnahmen schütze ich meine Daten?

Personen
- Mitarbeiter/innen

Infrastruktur
- Eingangsbereich
- Flur, Warteräume, Keller
- Öffentlicher Bereich
- Hausanschluss, Mülltonne

Technik
- Server, SAN, Firewall
- PC am Arbeitsplatz
- Mobile Systeme (iPhone)
- Öffentliche Netze (WLAN)
- Netzanschlussdosen
- IT-Systeme im Homeoffice

Dienste
- E-Mail, Web
- Webanwendungen
- Messanger

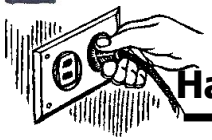
Homeoffice

Firma/Behörde
- Geschäftsverteilungsplan
- Organigramm
- Internetauftritt (Webseite)

Simulation

Experte

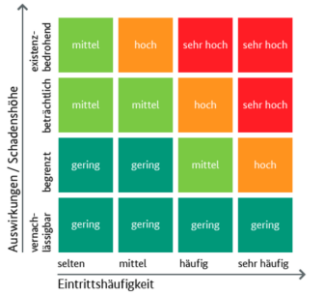
Daten



Hausanschluss

Quelle: https://pixabay.com/

Gefährdungen – Risiken – Maßnahmen



DATEN – ASSETS
z. B. Geschäftsdaten

↓

Anforderungen/Schutzbedarf
z. B. ISO 27001

Gefährdungen
(Bedrohung, Schwachstelle)
z. B. Vireninfizierung mit Ransomeware

↓

Risiko hoch = **Eintrittswahrscheinlichkeit/Schadenshöhe** = **Risiko gering**

Maßnahmen (TOM)

z. B. Antivirenschutzsoftware

↓

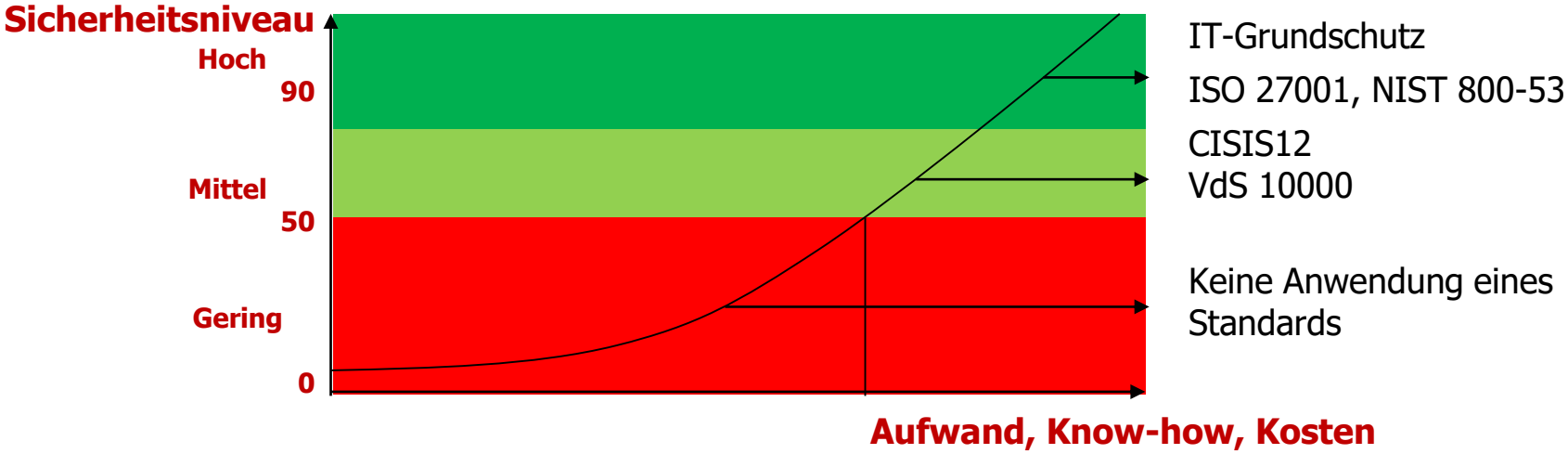
Ziel: **Informationssicherheit** und Datenschutz sollen gewährleistet werden!

- 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** und den **Schutz der Daten**

Sicherheitskonzept – Informationssicherheitsmanagementsystem (ISMS)

Orientierung an anerkannten Richtlinien und Standards:

- Informationssicherheit **ohne Anwendung** eines Standards
- **VdS Richtlinien 10000** für KMU – VdS Schadenverhütung GmbH
- **CISIS12** (ehemals ISIS12) – IT-Sicherheitscluster e. V.
- **IT-Grundschutz** – Bundesamts für Sicherheit in der Informationstechnik (BSI)
- **ISO 27001** und ISO 27002 – Internationale Norm für Informationssicherheitsmanagement
- **NIST 800-53** – National Institute of Standards and Technology



Informationssicherheit ohne Anwendung eines Standards

- Ggf. **selbst definiertes Regelwerk für Informations-sicherheit** (ISMS) entwickelt?
- **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 **Sicherheitsvorfälle** ist hoch!
- **Finanzieller** Schaden kann die Grenzen der **verfügbaren Mittel** übersteigen – hohes Risiko!

Quelle: https://pixabay.com

VdS 10000 – Inhalt

Schadenverhütung GmbH – **V**ertrauen **d**urch **S**icherheit

- 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 – Vertrauen durch Sicherheit

- 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

VdS 10000 : 2018-12 (02)
Informationssicherheitsmanagementsystem für kleine und mittlere Unternehmen (KMU), Anforderungen

VdS 10000en : 2018-12 (02)
Information security management systems for small and medium sized enterprises (SMEs), Requirements

VdS 10000QC : Online
VdS Quick-Check für das Informationssicherheits-Management in kleinen und mittelständischen Unternehmen (VdS 10000)

VdS 10001 : 2022-02 (03)
VdS Quick-Audit, Verfahren

VdS 10002 : 2019-11 (02)
Zertifizierung von Managementsystemen für KMU (Informationssicherheit und Datenschutz), Verfahren

VdS 10003 : 2018-12 (01)
Richtlinien für die Anerkennung von Beratern für Cyber-Security

VdS 10005 : 2021-07 (01)
Mindestanforderungen an die Informationssicherheit von Klein- und Kleinstunternehmen, Anforderungen

VdS 10006 : 2023-09 (02)
Testierung der Informationssicherheit von Klein- und Kleinstunternehmen, Verfahren

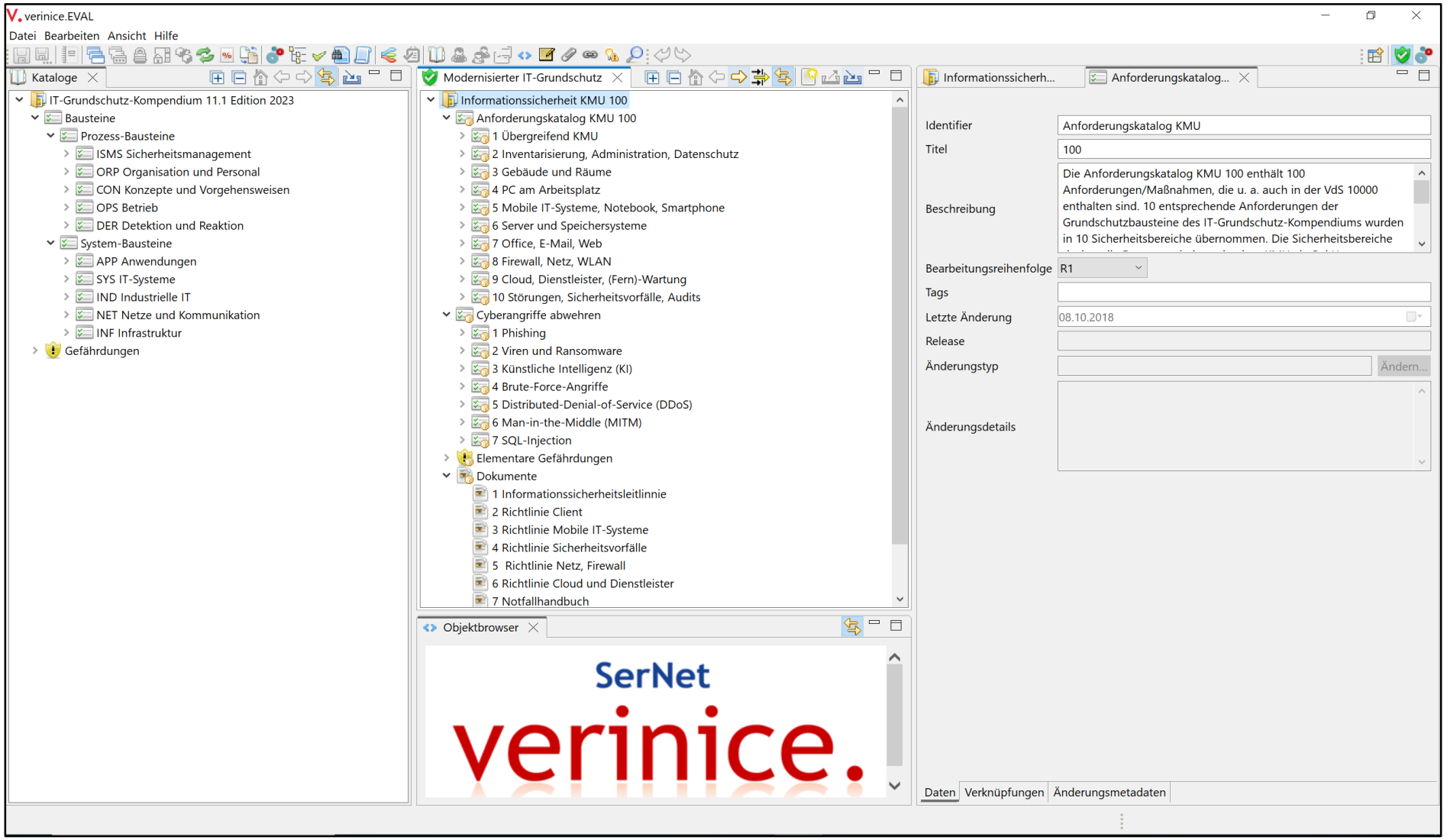
VdS 10010 : 2022-07 (02)
VdS-Richtlinien zur Umsetzung der DSGVO, Anforderungen

VdS 10012 : 2018-01 (01)
VdS-Richtlinien zur Umsetzung der DSGVO, Zertifizierung von Datenschutzmanagementsystemen, Verfahren

Quelle: https://shop.vds.de

ISMS-Tool zur Festlegung und Umsetzung der TOMs

Informationsverbund KMU mit 100 Anforderungen/Maßnahmen auf Basis von VdS 10000

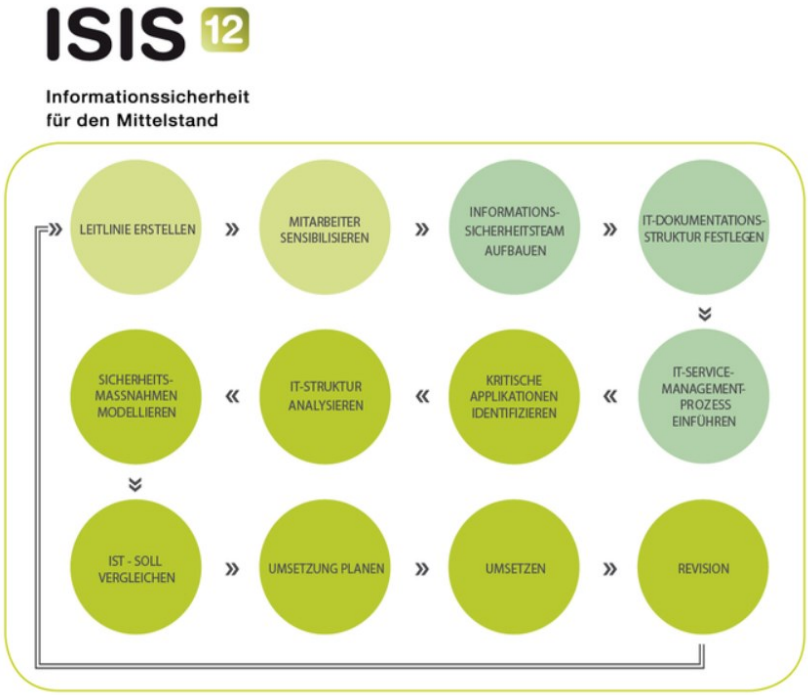


Quelle: Heiko Behrendt, Informationsverbund KMU 100

CISIS 12 Version 3.0

IT-Sicherheitscluster e.V. (Regensburg)

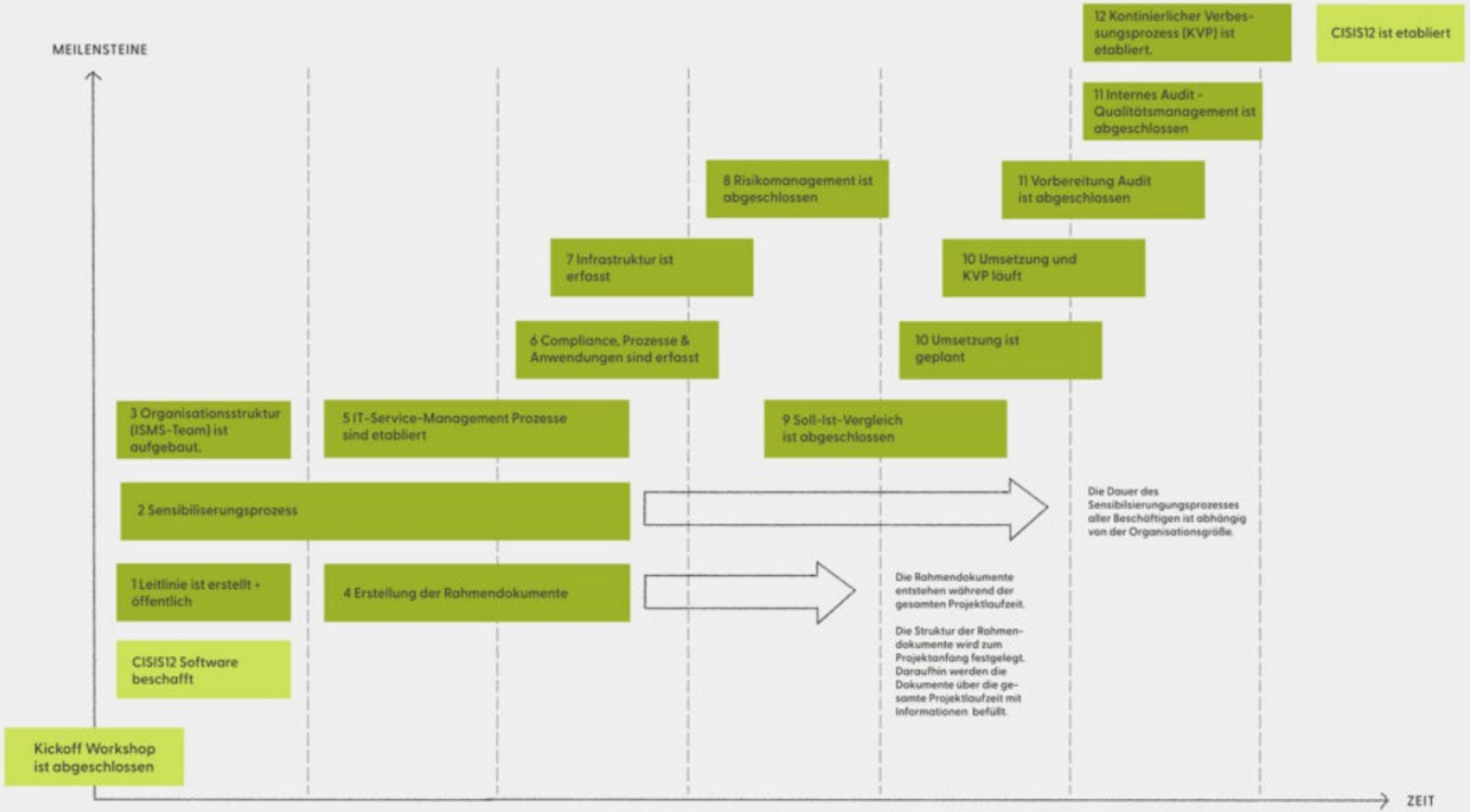
- **C**ompliance-**I**nformations-**SI**cherheits-Management-**S**ystem in 12 Schritten
- CISIS12 in der Version 3.0 ist eine **Weiterentwicklung** und Erweiterung des Informationsmanagementsystems ISIS12.
- Der Schwerpunkt liegt auf dem Thema **Compliance**.
- Der Standard besteht aus einer **Norm**, 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** möglichst unkompliziert und 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

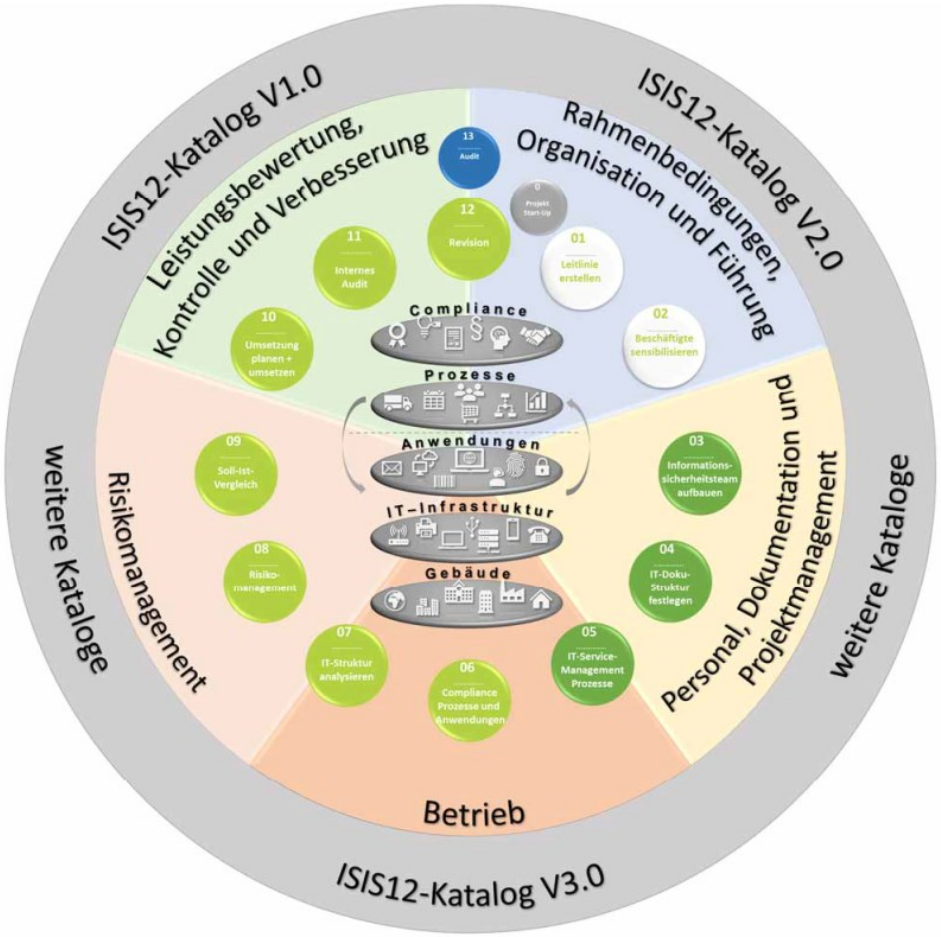


Abbildung 2: ISIS-Vorgehensmodell und Managementsystemmodell V3.0

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

Norm, Handbuch, Katalog, Tools

CISIS12 - Distribution (Norm, Handbuch, Katalog und Extended

170,00 €

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 1.1 (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.

Wichtiger Hinweis:

Der Erwerb berechtigt nicht zur gewerblichen Beratung bzw. zum Anbieten von CISIS12-Beratungsdienstleistungen. Wenn Sie Beratungsdienstleistungen anbieten möchten, bitten wir Sie, sich mit uns in Verbindung zu setzen. Informationen hier: https://cisis12.de.

MwSt (19%):	32,30 €
Summe:	202,30 €

Für Kommunen und den öffentlich-rechtlichen Bereich kostenlos!

- Tool M24S – https://m24s.info/
- Tool ISIS12 – https://www.simple-webapps.de/isis12/demo/i-app.php (Demoversion)

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.

IT-Grundschutzstandard

BSI-Standard – Leitfäden und Kompendium

BSI-Standards zur Informationssicherheit

Informationssicherheit und IT-Grundschutz

BSI-Standard 200-1

Managementsysteme für Informationssicherheit (ISMS)

BSI-Standard 200-2

IT-Grundschutz-Methodik

BSI-Standard 200-3

Risikoanalyse auf der Basis von IT-Grundschutz

BSI-Standard 200-4

Business Continuity Management

IT-Grundschutz-Kompendium

Kapitel 1	Vorspann
Kapitel 2	Schichtenmodell und Modellierung

Elementare Gefährdungen

Schichten

Prozess-Bausteine:

- ISMS (Sicherheitsmanagement)
- ORP (Organisation & Personal)
- CON (Konzepte & Vorgehensweise)
- OPS (Betrieb)
- DER (Detektion & Reaktion)

System-Bausteine:

- IND (Industrielle IT)
- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netze & Kommunikation)
- INF (Infrastruktur)

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

IT-Grundschutz-Prozess – Methode

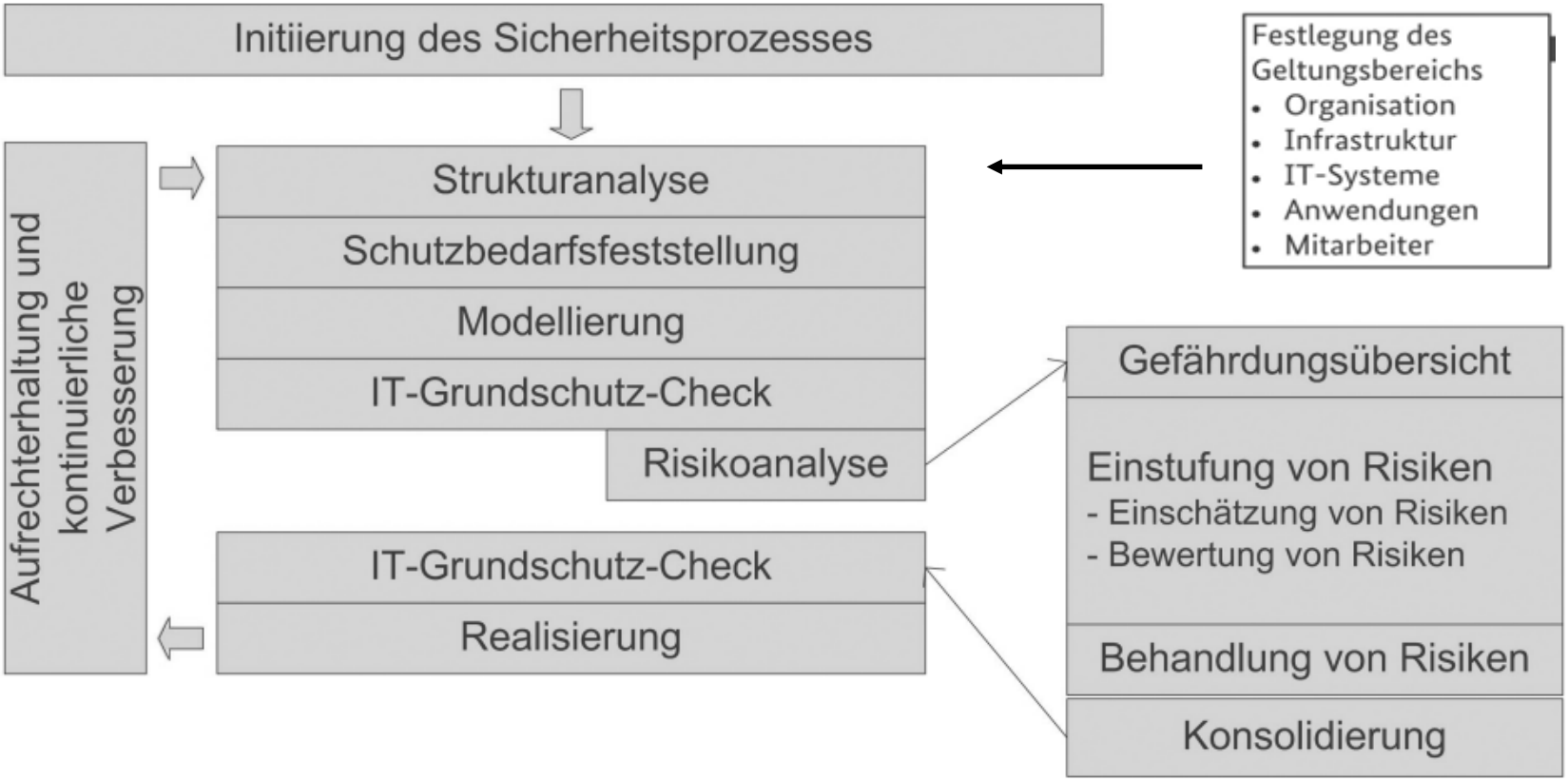
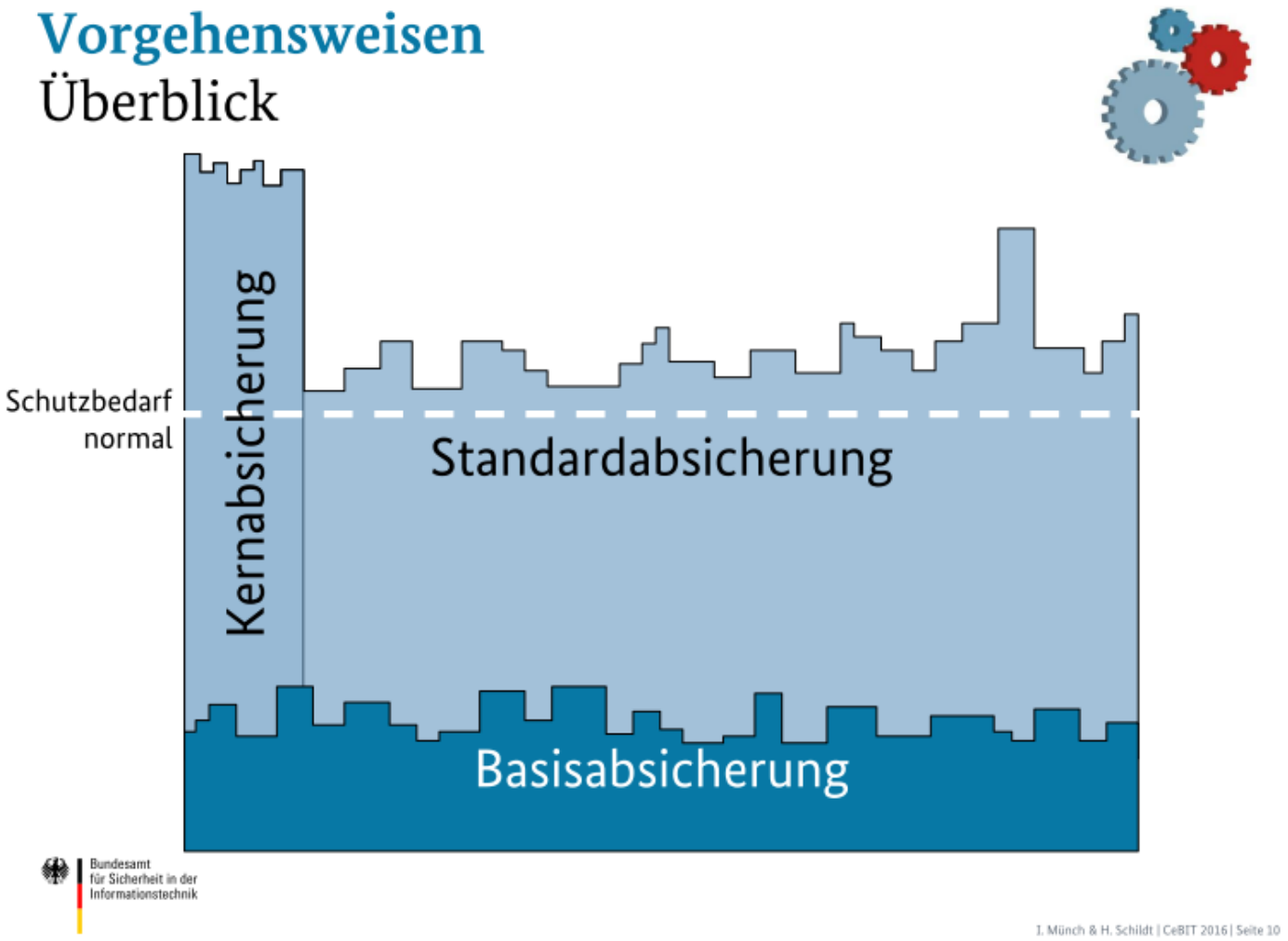


Abbildung 32: Integration der Risikoanalyse in den IT-Grundschutz-Prozess

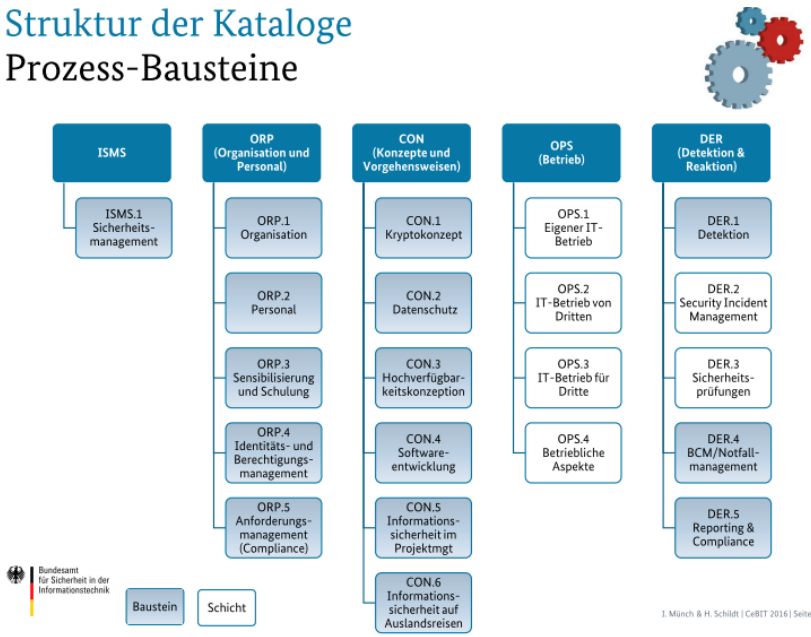
Quelle: https://www.bsi.bund.de

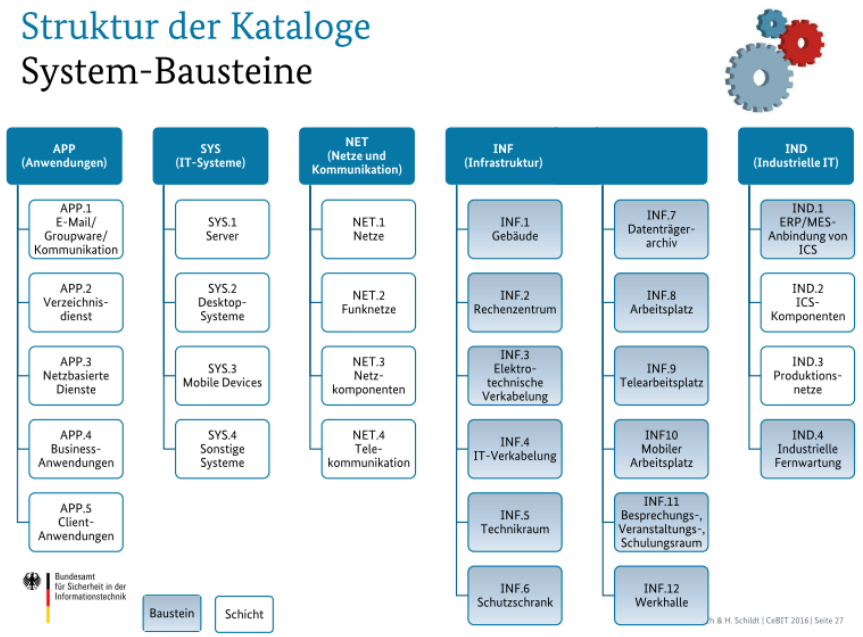
Stufenmodell



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

IT-Grundschutz-Kompendium



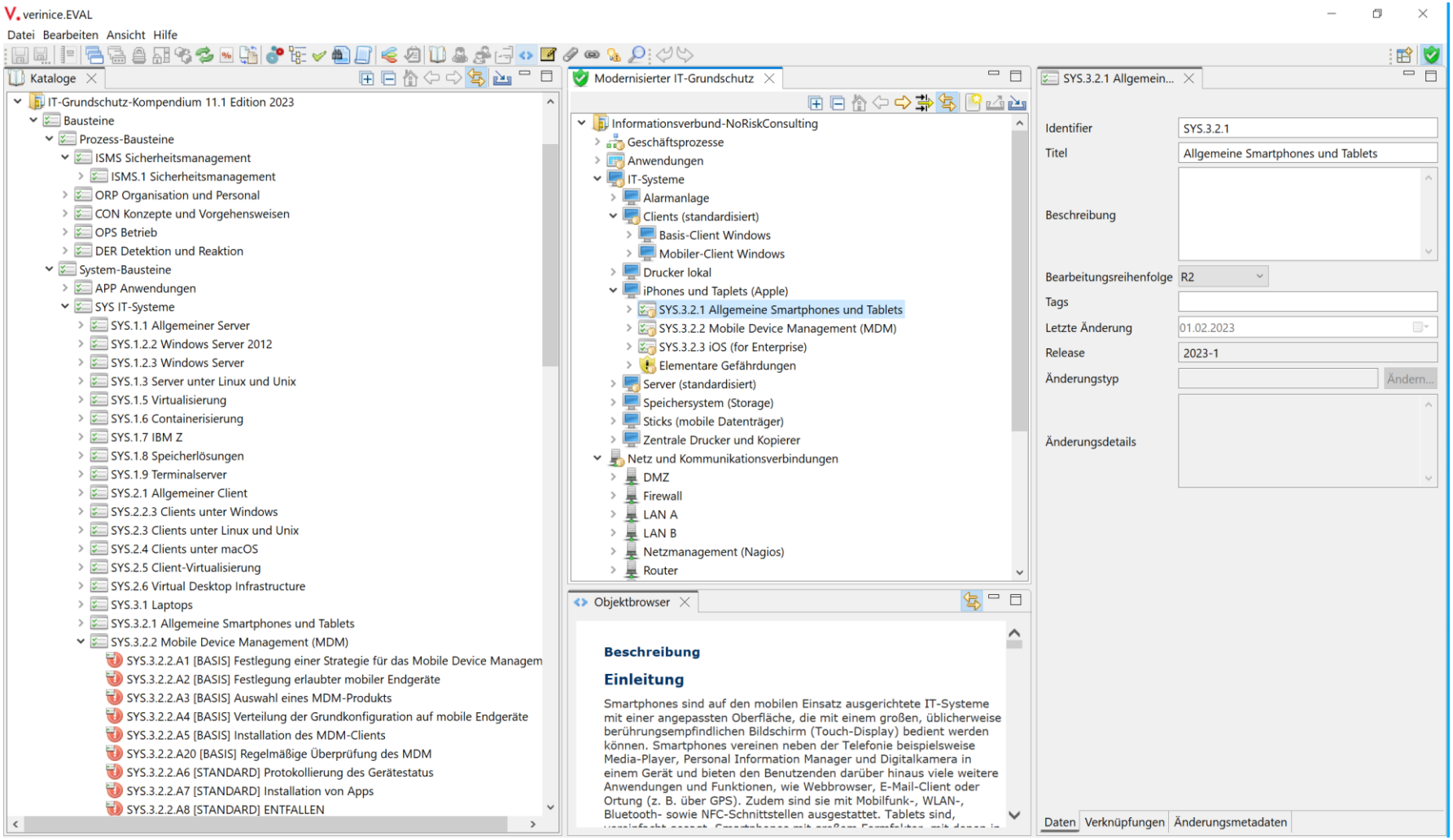


Quelle: https://www.bsi.bund.de

- Über **100 Bausteine** mit Anforderungen bzw. Maßnahmen
- Die Bausteine werden **jährlich** vom BSI aktualisiert (IT-Grundschutz-Kompendium-Edition)
- Die Bausteine und **Anforderungen/Maßnahmen** werden ausführlich beschrieben
- Das IT-Grundschutz-Kompendium lässt sich **vollständig in Tools** integrieren

ISMS-Tool zur Festlegung und Umsetzung der TOMs

Informationsverbund Muster-Firma NoRiskConsulting – IT-Grundschutz-Standard

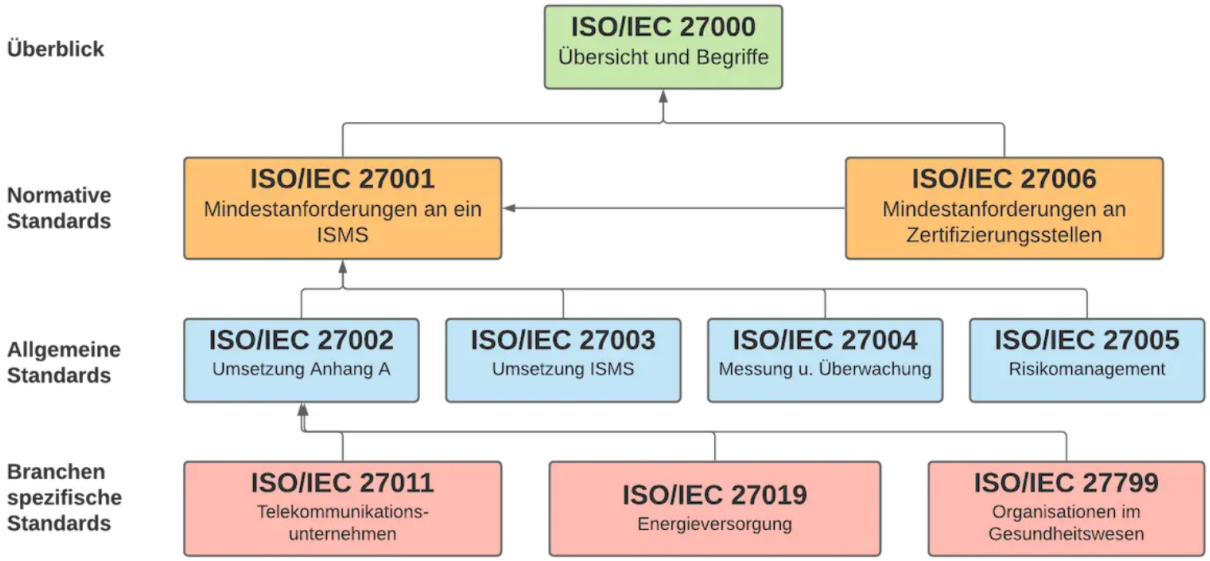


Quelle: Heiko Behrendt, Informationsverbund Muster-Firma NoRiskConsulting

ISO/IEC 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

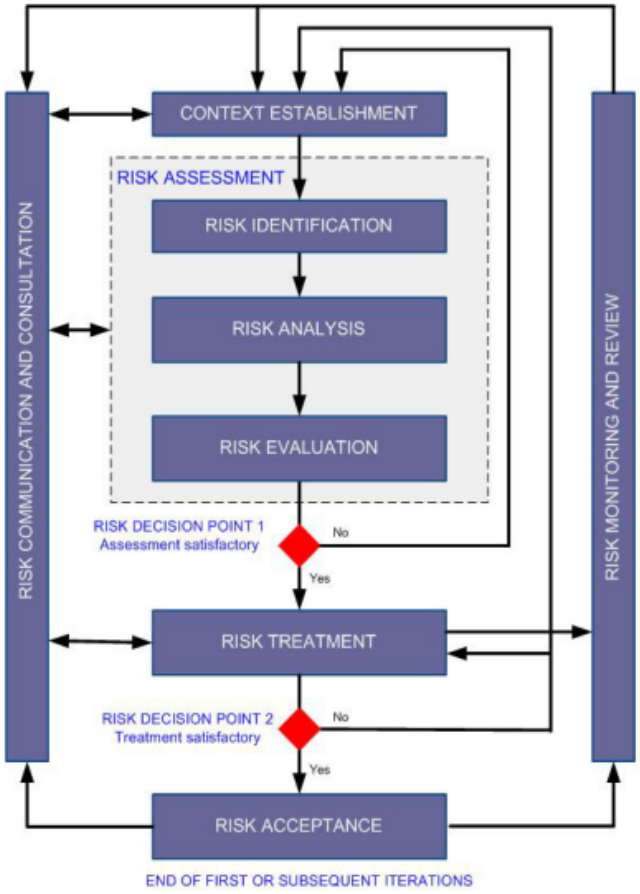
ISO/IEC 27001

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/IEC 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/IEC 27002 – Umsetzung Controls

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

Inhalt

Seite

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

Security und Privacy Controls for Information Systems and Organizations

Table of Contents

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

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	Nein
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 SS 2024

10. Juni 2024

Vielen Dank für Ihre Aufmerksamkeit!

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