Ingo Lorenz, Dirk Fox

Ein Reifegradmodell für die Datenschutzorganisation

Die Umsetzung der gesetzlichen Datenschutzanforderungen ist eine große Herausforderung in Unternehmen, die aus vielen, insbesondere internationalen Organisationseinheiten bestehen, wie z. B. Konzerne. Der Beitrag stellt ein Reifegradmodell vor, das eine strukturierte Vorgehensweise für den Aufbau und Betrieb eines Datenschutzmanagement-Systems über beliebig viele Organisationseinheiten bietet und zugleich eine differenzierte Bestimmung des erreichten Datenschutzniveaus ermöglicht.

1 Hintergrund

Die Umsetzung der gesetzlichen Anforderungen an den Datenschutz in einem Unternehmen ist unvermeidlich eine „Dauerbaustelle": Ständig werden neue Verarbeitungen personenbezogener Daten eingeführt, wird der Betrieb eingeführter Verarbeitungen modifiziert (bspw. durch den Wechsel einer On-Premise- zu einem Cloud-Lösung) oder müssen Datenschutz-Prozesse (wie z. B. die Organisation von Auskunftsersuchen) an geänderte Unternehmensstrukturen oder Zuständigkeiten angepasst werden. Dazu kommen offene Baustellen aus „Altlasten": Komplexe, gewachsene Verarbeitungen ohne effiziente Löschprozesse, Auftragsverarbeiter mit wechselnden Unterauftragnehmern und unvollständige Beschreibungen von Verarbeitungstätigkeiten.

Nicht selten beschleicht einen Datenschutzbeauftragten dabei das Gefühl, den gesetzlichen Anforderungen angesichts der unternehmensinternen Gegebenheiten unablässig „hinterherzulaufen". Der Gesamtüberblick zum Stand des Datenschutzes gerät dabei leicht aus dem Blick. Daher kann von einer umfassenden Erfüllung der gesetzlichen Anforderungen an die Verarbeitung personenbezogener Daten nach der Selbsteinschätzung vieler Datenschutzbeauftragter in der Praxis häufig keine Rede sein. Eine solche, oft obendrein von Ad-Hoc-Anforderungen „getriebene" Datenschutzorganisation entzieht sich zudem meistens einer sinnvollen Auditierung.

Diese Ausgangslage ist weder für die verantwortlichen Datenschutzbeauftragten selbst noch aus einer Compliance-Perspektive erfreulich und birgt zudem ein erhebliches Management-Risiko: Wird die Erfüllung gesetzlicher Anforderungen nicht wirksam geregelt und überprüft, kann ein Organisationsverschulden der Geschäftsleitung vorliegen. Schließlich führt Unübersichtlichkeit auch leicht dazu, dass Prioritäten falsch gewählt werden oder wichtige Maßnahmen „unter die Räder" kommen.

Einen Ausweg bietet der Aufbau eines Datenschutzmanagements in Anlehnung an die bewährten Standards der Informationssicherheit. Die einem solchen Management-System inhärente Systematik mit ihren Regel-Prozessen und der Ausrichtung an einer kontinuierlichen Verbesserung ermöglicht die Erreichung eines definierten Datenschutzniveaus. Ergänzt man das Datenschutzmanagement-System um ein Reifegradmodell (Maturity Model), kann der Aufbau auch ausgehend von einer zunächst unübersichtlichen Ausgangslage mit zahlreichen Unternehmenseinheiten systematisch nach vorgegebenen Prioritäten gestaltet werden. Dabei lässt sich zu jedem Zeitpunkt das jeweils bereits erreichte Datenschutzniveau ohne großen Aufwand detailliert bestimmen.

Ingo Lorenz

ist Konzerndatenschutzbeauftragter der Hansgrohe SE.

E-Mail: Ingo.Lorenz@hansgrohe.com

Dirk Fox

ist Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.

E-Mail: dirk.fox@secorvo.de

2 Datenschutzmanagement

Anders als im Datenschutz sind in der Informationssicherheit Managementsysteme (ISMS) inzwischen selbst bei mittelständischen Unternehmen weit verbreitet: Sowohl die Internationale Normenreihe ISO 2700x [1] als auch der BSI Grundschutz [2] verstehen Informationssicherheit nicht (mehr) als ein Bündel von Maßnahmen, sondern als einen kontinuierlichen Prozess. In einem festen, meist jährlichen Zyklus werden alle Regelungen, Maßnahmen und Prozesse der Informationssicherheit über-

prüft und erforderlichenfalls angepasst oder verbessert („Plan-Do-Check-Act" – PDCA).

In der DSGVO finden sich zahlreiche Hinweise darauf, dass der europäische Gesetzgeber sich auch für die Umsetzung des Datenschutzes ein Management-System vorstellt. So müssen viele Entscheidungen wie Datenschutzfolgenabschätzungen, Risikobewertungen oder Verarbeitungen aus berechtigtem Interesse geeignet dokumentiert werden, sind Unterauftragnehmer regelmäßig zu prüfen und berichtet der Datenschutzbeauftragte direkt an die Unternehmensleitung – Vorgaben, die für ein Management-System typisch sind.

Für die Umsetzung der gesetzlichen Anforderungen an den Datenschutz gibt es seit einigen Jahren anerkannte Methoden wie das Standard-Datenschutz-Modell (SDM) des AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder [3] oder die ISO-Standards 2770x zum Datenschutzmanagement [4]. Bei beiden Ansätzen stehen die konkreten Verarbeitungen personenbezogener Daten im Zentrum: Während das SDM in einem PDCA-Zyklus die Erfüllung von Gewährleistungszielen durch jede einzelne Verarbeitung betrachtet, liegt der Schwerpunkt des ISO 2770x auf den insbesondere technischen Maßnahmen zum Schutz der verarbeiteten Daten, eingebettet in ein bestehendes ISMS nach ISO 2700x.

Diese Ansätze sind gut geeignet, um die Umsetzung von Datenschutzanforderungen im Konkreten, also auf der Ebene einer einzelnen Verarbeitung zu gestalten oder zu auditieren. Dabei werden allerdings die Verarbeitungsprozesse selbst und weniger die Prozesse des Datenschutzmanagements betrachtet.

3 Reifegradbestimmung

In der unternehmerischen Praxis wird der Datenschutz in zunehmendem Maße als bedeutsames Compliance-Thema eingestuft, nicht zuletzt wegen des Risikos hoher Bußgeldzahlungen bei Verstößen. Aus dieser Perspektive stehen weniger die operative Erfüllung von Gewährleistungszielen durch einzelne Verarbeitungen (wie beim SDM) oder die Vollständigkeit der ergriffenen technischen Schutzmaßnahmen (wie beim ISO 2770x) im Vordergrund. Stattdessen muss der Erfüllungsgrad der gesetzlichen Anforderungen als Ganzes bewertet werden – möglicherweise sogar im internationalen Kontext.

Um eine solche Abstraktion vom Konkreten zu einer Gesamtsicht zu erreichen, orientieren sich Unternehmen bei ihren Management-Systemen schon länger an Reifegradmodellen. So werden bewährte Ansätze wie das Maturity Model von ITIL (*Information Technology Infrastructure Library*) [5] oder COBIT (*Control Objectives for Information and Related Technology*) [6] inzwischen nicht mehr nur im IT Service Management bzw. in der IT Governance angewendet, sondern bspw. auch im Informationssicherheitsmanagement [7]. Dabei werden alle Regelungsbereiche des Management-Systems hinsichtlich des Grads der Strukturierung, der konkreten Umsetzung und der systematischen Steuerung bewertet.

In diesen Reifegradmodellen wird der Stand der Umsetzung des Managementsystems mit Hilfe von meist sechs Reifegrad-Stufen bewertet, die von „kein Prozess existiert" (Reifegrad 0) bis „es gibt einen regelmäßig überprüften und kontinuierlich verbesserten Prozess" (Reifegrad 5) reichen (siehe Abb. 1).

Abb. 1 | Reifegrade 0 bis 5 nach ITIL/COBIT

Reifegrad	Merkmale
0	Kein Prozess, keine Planung
1	Planung zur Einführung eines Prozesses, keine Umsetzung
2	Prozess teilweise umgesetzt, keine systematische Dokumentation
3	Prozess vollständig umgesetzt und dokumentiert
4	Prozess wird regelmäßig auf Effektivität überprüft
5	Maßnahmen zur kontinuierlichen Verbesserung vorhanden

Um den Reifegrad eines Datenschutzmanagement-Systems zu bestimmen, muss man zunächst den PDCA-Zyklus – wie beim Informationssicherheitsstandard ISO 2700x – auf die Prozesse des Datenschutzmanagements anwenden, und nicht (nur) auf einzelne Verarbeitungstätigkeiten oder Schutzmechanismen. Dafür ist ein Perspektivwechsel erforderlich: Die Umsetzung des Datenschutzes ist darin kein (einmalig zu erreichender) stabiler Zustand mehr, sondern erfolgt durch die Einführung und Anwendung geeigneter (Management-) Prozesse, die Vorgaben, Maßnahmen und Dokumentationen einfordern und regelmäßig überprüfen. Ausgangspunkt für die Reifegradbewertung sind daher nicht die Verarbeitungstätigkeiten, sondern die Prozesse zur (unternehmensspezifischen) Umsetzung der unterschiedlichen datenschutzrechtlichen Pflichten – über alle Verarbeitungstätigkeiten hinweg. Auf diese Weise wird eine eindeutige und übersichtliche Bestimmung der Qualität des Management-Systems möglich.

Zu diesem Zweck lassen sich die gesetzlichen Datenschutzpflichten verarbeitungsübergreifend in die folgenden 13 Einzelthemen (Topics) strukturieren:

- Datenschutz-Konzeption
- Datenschutz-Richtlinien
- Datenschutzfolgenabschätzungen
- Datenschutzschulung
- Betroffenenrechte
- Informationspflichten
- Übersicht der Verarbeitungstätigkeiten
- Vorfallsmanagement
- Auftragsverarbeitungen
- Audits
- Videoüberwachung
- TOMs
- Datenlöschung

Die Reifegradbestimmung erfolgt nun für jedes dieser Topics. Einige Topics (wie die Erfüllung der Betroffenenrechte, die Informationspflichten oder die Löschung von Daten) betreffen alle Verarbeitungen personenbezogener Daten. Der Reifegrad eines solchen Topics muss dabei von allen Verarbeitungstätigkeiten erreicht sein.

Für die Bewertung eines Datenschutzmanagement-Systems hat sich in der Praxis eine Unterscheidung der in Abb. 2 gezeigten vier Reifegrade (0-3) bewährt. Ein Nebeneffekt der Nutzung von lediglich vier verschiedenen Reifegraden ist, dass sie sich durch eine einfache farbliche „Ampeldarstellung" veranschaulichen lassen.

Damit die Bestimmung des Reifegrads einheitlich über mehrere Unternehmenseinheiten vorgenommen werden kann und jederzeit nachvollziehbar ist, werden jedem Topic zunächst sinnvolle Teilaufgaben für die Umsetzung zugeordnet. Dabei sollten die

Abb. 2 | Reifegrade des Datenschutzmanagement-Systems

Reifegrad		Merkmale
0	rot	Problem erkannt
1	orange	Lösungsweg festgelegt, Umsetzung terminiert
2	gelb	Prozess definiert, Templates erstellt, Umsetzung begonnen
3	grün	Prozess etabliert, Dokumentation aktuell, regelmäßige Prüfung

einzelnen Teilaufgaben aufeinander aufbauen und sowohl vom zeitlichen als auch vom inhaltlichen Aufwand überschaubar sein.

Für das Topic „Datenschutzschulung" kann die Liste der Teilaufgaben beispielsweise die folgenden Schritte umfassen:

- Ermittlung und Gruppierung der im Datenschutz zu schulenden Aufgabenbereiche im Unternehmen,
- Ermittlung des jeweiligen Schulungsbedarfs,
- Erstellung geeigneter Schulungsunterlagen,
- Durchführung der Schulungen,
- regelmäßige Überprüfung des Schulungsbedarfs und
- regelmäßige Aktualisierung der Schulungsunterlagen.

Ergebnisse dieser Teilaufgaben sind definierte, bedarfsgerechte Anforderungen an die Schulungen und deren Zuordnung zu allen Stellen im Unternehmen – die regelmäßig (z. B. jährlich) überprüft werden. Denn die Teilaufgaben in jedem Topic unterliegen durch gesetzliche Änderungen, strategische oder organisatorische Weiterentwicklungen einem ständigen Wandel.

Für jede Teilaufgabe werden nun die Reifegrade 1-3 konkretisiert. Deren Definitionen müssen so eindeutig sein, dass keine auseinandergehenden Auffassungen darüber bestehen und sich somit wiederholbare Bewertungen vornehmen lassen [8]. Reifegrad 3 (grün) umfasst dabei immer ein regelmäßiges Review der Ergebnisse der Teilaufgabe. Dadurch wird sichergestellt, dass ein kontinuierlicher Abgleich mit gesetzlichen und internen Anforderungen erfolgt und erforderliche Änderungen in die Wege geleitet werden. Abb. 3 zeigt eine solche konkrete Definition der Reifegrade für Teilaufgaben des Topics „Datenschutzschulung".

Die Bestimmung des Reifegrades der gesamten Datenschutzorganisation wird für jede einzelne Organisationseinheit vorgenommen, indem dort für jedes Topic der erreichte Reifegrad festgestellt wird. Dabei erreicht ein Topic einen bestimmten Reifegrad, wenn alle zugehörigen Teilaufgaben mindestens denselben Reifegrad erfüllen.

Die Reifegrade der Teilaufgaben sollten in den Organisationseinheiten von geschulten Datenschutzkoordinatoren vorgenommen werden, die den Datenschutzbeauftragten bei der Umsetzung des Datenschutzes in der Organisationseinheit unterstützen. Damit die Bewertung einheitlich und wiederholbar erfolgt, sollten die Datenschutzkoordinatoren im Umgang mit dem Reifegradmodell geschult werden. Auf diese Weise kann eine differenzierte Bestimmung des Reifegrades der gesamten Datenschutzorganisation jederzeit mit begrenztem Aufwand durchgeführt werden.

4 Reifegrade als Zielvorgabe

Das beschriebene Reifegradmodell ist nicht nur geeignet, den Reifegrad der Datenschutzorganisation differenziert und zu jedem Zeitpunkt mit moderatem Aufwand zu ermitteln, sondern kann auch dafür eingesetzt werden, die Umsetzung der gesetzlichen Datenschutzanforderungen in einer oder mehreren (neuen) Organisationseinheiten zu steuern und zu begleiten. Dabei ist irrelevant, ob es sich bei der Organisationseinheit um eine Abteilung oder ein Unternehmen im Konzern handelt.

Dazu wird zunächst als Ausgangspunkt der Reifegrad für jedes Topic von den betroffenen Organisationseinheiten selbst anhand der Erfüllung der Teilaufgaben ermittelt. Das Ergebnis dieser Selbsteinschätzung wird ggf. vom Datenschutzbeauftragten des Konzerns oder Unternehmens als Gesamtverantwortlichem überprüft.

Anschließend steht mit dem Reifegrad zugleich fest, welche Teilaufgaben von den Organisationseinheiten noch erledigt werden müssen. Mit Hilfe einer Risikobewertung oder anderen Kriterien werden die zu lösenden Teilaufgaben priorisiert. Auf Vorschlag des Datenschutzbeauftragten können dann Ziel-Reifegrade von der Geschäftsleitung vorgegeben werden, die innerhalb eines vorgegebenen Zeitrahmens (bspw. eines Geschäftsjahres) von den Organisationseinheiten in jedem Topic erreicht werden sollen (siehe Abb. 4).

Dazu schätzt der Gesamtverantwortliche für die Anwendung des Reifegradmodells – beispielsweise der Konzerndatenschutzbeauftragte – den Aufwand für diese Zielerreichung ausgehend vom aktuellen Ist-Zustand und legt die Reihenfolge und Zeitpunkte der Umsetzung („Meilensteine") in einem groben zeitlichen Projektplan („Roadmap") fest (siehe Abb. 5). Dabei ist es

Abb. 3 | Definition der Reifegrade am Beispiel des Topics „Datenschutzschulung"

Topic Datenschutzschulung	Orange	Gelb	Grün
Basistraining für alle Mitarbeiter bei Eintritt	ist erstellt	wird regelmäßig für alle Neueintritte durchgeführt	wird jährlich aktualisiert
Zuordnung von Stellen zu erforderlichen Trainings	Vorgehen ist geplant	Zuordnung gemacht, Prozess für neue Stellen steht	wird jährlich auf Richtigkeit und Vollständigkeit überprüft
Office-Training	ist erstellt	wird regelmäßig für alle erforderlichen Stellen durchgeführt	Training wird jährlich aktualisiert
Fachbezogene Trainings	sind erstellt	werden regelmäßig für alle erforderlichen Stellen durchgeführt	Durchführung in vorgegebener Regelmäßigkeit ist in HR dokumentiert; Trainings werden jährlich aktualisiert

Abb. 4 | Reifegrade als Zielvorgabe

Datenschutzmanagement	aktueller Status	Status Zieltermin
Datenschutz-Konzeption	orange	grün
Datenschutz-Richtlinien	gelb	grün
Datenschutzfolgenabschätzungen	orange	gelb
Datenschutzschulung	gelb	grün
Betroffenenrechte	gelb	grün
Informationspflichten	orange	gelb
Übersicht der Verarbeitungstätigkeiten	rot	grün
Vorfallsmanagement	rot	gelb
Auftragsverarbeitungen	gelb	grün
Audits	orange	gelb
Videoüberwachung	gelb	grün
TOMs	gelb	grün
Datenlöschung	rot	gelb

sinnvoll (und für die Verantwortlichen in den Organisationseinheiten außerdem motivierend), mit wenig Aufwand erreichbare Fortschritte zeitlich vorzuziehen – „niedrig hängende Früchte" wie bspw. die Erfüllung einfacher Teilaufgaben, die unmittelbar zu einem höheren Reifegrad des gesamten zugehörigen Topics (und damit der gesamten Datenschutzorganisation) führen.

Die gewählten Zielvorgaben für die einzelnen Topics, die am Ende des Betrachtungszeitraumes erreicht sein sollen, dürfen anspruchsvoll sein, müssen aber auch realistisch erreicht werden können. Im Verlauf des vorgegebenen Umsetzungszeitraums kann der Fortschritt durch regelmäßige Bestimmungen des Reifegrades der betroffenen Organisationseinheiten überprüft werden. Die Verteilung der Reifegradziele der einzelnen Topics auf den Projektzeitraum ermöglicht es den Verantwortlichen in den Organisationseinheiten, sich bei der Umsetzung jeweils auf wenige Topics zu konzentrieren.

5 Reifegrade im Reporting

Die Anwendung eines Reifegradmodells vereinfacht es dem Datenschutzbeauftragten, den aktuellen Stand und die Fortschritte bei der Umsetzung der Datenschutzanforderungen im Unternehmen übersichtlich und transparent darzustellen. Über die Erreichung der festgelegten Reifegrad-Zielsetzungen sollte daher regelmäßig an die Geschäftsleitung berichtet werden; damit werden die auf den Datenschutz bezogenen Compliance-Risiken transparent. Zugleich ist auf diese Weise sichergestellt, dass die Erfüllung der erforderlichen Teilaufgaben in den Organisationseinheiten den angemessenen Stellenwert erhält.

Eine Visualisierung des Reifegrads der Datenschutzorganisation in den 13 Topics kann mit gängigen Diagrammformaten er-

Abb. 6 | Visualisierung der Zielerreichung (Beispiel)

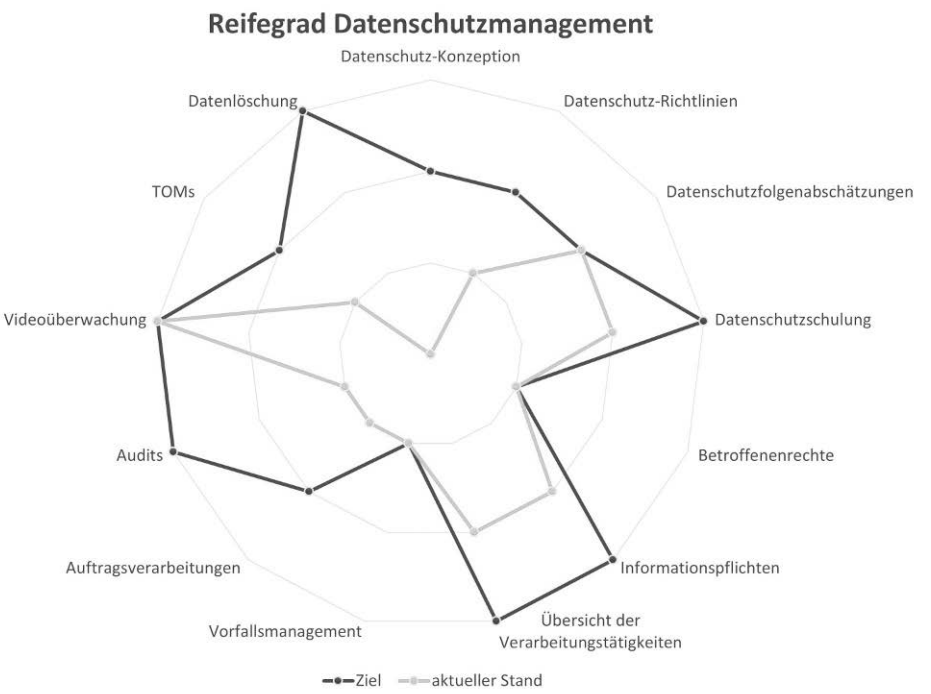

Abb. 5 | Roadmap (Beispiel)

Roadmap	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember
Datenschutz-Konzeption		orange	gelb	gelb	grün							
Datenschutz-Richtlinien									gelb	grün		
Datenschutzfolgenabschätzungen						orange	gelb					
Datenschutzschulung												
Betroffenenrechte				gelb	grün							
Informationspflichten							gelb	gelb	grün			
Übersicht der Verarbeitungstätigkeiten										orange	gelb	
Vorfallsmanagement									rot	orange	gelb	grün
Auftragsverarbeitungen												
Audits												
Videoüberwachung												
TOMs												
Datenlöschung												

folgen. Beim oft verwendeten und sehr anschaulichen „Spinnendiagramm“ ist allerdings zu beachten, dass eine hohe Zielerreichung bei benachbarten Topics leicht der Eindruck eines höheren Gesamt-Reifegrads suggerieren kann, weil das Diagramm mehr Fläche bedeckt. Dem kann in der Darstellung durch eine Änderung der Reihenfolge der Topics entgegengewirkt werden, indem bspw. einfach zu erreichende Topics und anspruchsvolle Topics abwechselnd benannt werden (Abb. 6).

6 Kontinuierliche Weiterentwicklung

Die Teilaufgaben der 13 Topics müssen selbst einer regelmäßigen Überprüfung unterzogen werden. Durch unternehmensinterne oder datenschutzrechtliche Änderungen, wie auch geänderte Auslegungen durch höchstinstanzliche Urteile, kann es erforderlich sein, die Teilaufgaben der Topics zu ändern oder zu ergänzen. Dabei kann der Reifegrad eines Topics sinken, sogar gleich um mehrere Stufen. Aufgabe des Datenschutzmanagement ist es, in einem solchen Fall geeignete Maßnahmen zu ergreifen und neue Ziel-Reifegrade zu setzen, um den Reifegrad des gesamten Datenschutzmanagement-Systems wieder zu korrigieren.

Eine wichtige Rolle spielt das Topic „Audit“ für die kontinuierliche Überprüfung: Durch regelmäßige (interne oder auch externe) Auditierungen kann sichergestellt werden, dass keine „blinden Flecken“ im Datenschutzmanagement entstehen, die dazu führen, dass der anhand der Topics und Teilaufgaben bestimmte Reifegrad nicht vom tatsächlichen Datenschutz-Niveau im Unternehmen abweicht.

Fazit

Reifegradmodelle, die im IT Management schon lange Standard sind und inzwischen auch im Informationssicherheitsmanagement eingesetzt werden, eignen sich auch für den Aufbau und die Bewertung eines Datenschutzmanagements. Sie ermöglichen eine effiziente Bestimmung des erreichten Datenschutzniveaus, eignen sich für die Definition von Zielvorgaben und erlauben zudem eine anschauliche, differenzierte und transparente Visualisierung.

Literatur

[1] Milan Burgdorf, Kai Jendrian: *ISO 27002 revisited*. DuD 5/2022, S. 301-304.
[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz-Kompendium (Edition 2023)*. 01.02.2023.
[3] AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: *Das Standard-Datenschutzmodell*. Version 3.0 vom 24.11.2022.
[4] ISO/IEC: *Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. ISO/IEC 27701:2019.
[5] ITIL Foundation: *Information Technology Infrastructure Library*, ITIL 4, 2019.
[6] ISACA: *Control Objectives for Information and Related Technology*, COBIT Framework, 2019.
[7] Diogo Proença, José Borbinha: *Information Security Management Systems – A Maturity Model based on ISO/IEC 27001*. In: Witold Abramowicz, Adrian Paschke (Hrsg.): *Business Information Systems*, Proceedings of 21st International Conference BIS 2018, Berlin, 18.-20.07.2018. LNBIP 320, Springer 2018, S. 102-114.
[8] DIN/ISO: *Leitfaden zur Auditierung von Managementsystemen*. DIN EN ISO 19011:2018, Abschnitt 6.4.8: Erarbeiten von Auditfeststellungen.

Terms and Conditions

Springer Nature journal content, brought to you courtesy of Springer Nature Customer Service Center GmbH (“Springer Nature”).
Springer Nature supports a reasonable amount of sharing of research papers by authors, subscribers and authorised users (“Users”), for small-scale personal, non-commercial use provided that all copyright, trade and service marks and other proprietary notices are maintained. By accessing, sharing, receiving or otherwise using the Springer Nature journal content you agree to these terms of use (“Terms”). For these purposes, Springer Nature considers academic use (by researchers and students) to be non-commercial.
These Terms are supplementary and will apply in addition to any applicable website terms and conditions, a relevant site licence or a personal subscription. These Terms will prevail over any conflict or ambiguity with regards to the relevant terms, a site licence or a personal subscription (to the extent of the conflict or ambiguity only). For Creative Commons-licensed articles, the terms of the Creative Commons license used will apply.
We collect and use personal data to provide access to the Springer Nature journal content. We may also use these personal data internally within ResearchGate and Springer Nature and as agreed share it, in an anonymised way, for purposes of tracking, analysis and reporting. We will not otherwise disclose your personal data outside the ResearchGate or the Springer Nature group of companies unless we have your permission as detailed in the Privacy Policy.
While Users may use the Springer Nature journal content for small scale, personal non-commercial use, it is important to note that Users may not:

1. use such content for the purpose of providing other users with access on a regular or large scale basis or as a means to circumvent access control;
2. use such content where to do so would be considered a criminal or statutory offence in any jurisdiction, or gives rise to civil liability, or is otherwise unlawful;
3. falsely or misleadingly imply or suggest endorsement, approval , sponsorship, or association unless explicitly agreed to by Springer Nature in writing;
4. use bots or other automated methods to access the content or redirect messages
5. override any security feature or exclusionary protocol; or
6. share the content in order to create substitute for Springer Nature products or services or a systematic database of Springer Nature journal content.

In line with the restriction against commercial use, Springer Nature does not permit the creation of a product or service that creates revenue, royalties, rent or income from our content or its inclusion as part of a paid for service or for other commercial gain. Springer Nature journal content cannot be used for inter-library loans and librarians may not upload Springer Nature journal content on a large scale into their, or any other, institutional repository.
These terms of use are reviewed regularly and may be amended at any time. Springer Nature is not obligated to publish any information or content on this website and may remove it or features or functionality at our sole discretion, at any time with or without notice. Springer Nature may revoke this licence to you at any time and remove access to any copies of the Springer Nature journal content which have been saved.
To the fullest extent permitted by law, Springer Nature makes no warranties, representations or guarantees to Users, either express or implied with respect to the Springer nature journal content and all parties disclaim and waive any implied warranties or warranties imposed by law, including merchantability or fitness for any particular purpose.
Please note that these rights do not automatically extend to content, data or other material published by Springer Nature that may be licensed from third parties.
If you would like to use or distribute our Springer Nature journal content to a wider audience or on a regular basis or in any other manner not expressly permitted by these Terms, please contact Springer Nature at

onlineservice@springernature.com