Holger Reibold

ISMS erfolgreich implementieren

Praxisleitfaden für Unternehmen nach ISO/IEC 27001

BRAIN-MEDIA.DE

Holger Reibold

ISMS erfolgreich implementieren

Praxisleitfaden für Unternehmen nach ISO/IEC 27001

BRAIN-MEDIA.DE

ISBN: 978-3-95444-331-4

Cover: pixabay / LTapsaH

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. 52c – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

Die Digitalisierung hat Unternehmen in den vergangenen Jahren grundlegend verändert. Geschäftsprozesse, Kommunikation, Produktion und Dienstleistungen basieren heute nahezu vollständig auf digitalen Systemen und vernetzten Infrastrukturen. Informationen sind dabei zu einem der wertvollsten Vermögenswerte moderner Organisationen geworden. Gleichzeitig hat sich die Bedrohungslage im Bereich der Cybersecurity erheblich verschärft. Angriffe durch Cyberkriminelle, gezielte Industriespionage, Ransomware-Kampagnen oder Fehlkonfigurationen in Cloud-Systemen können innerhalb kürzester Zeit erhebliche wirtschaftliche Schäden verursachen.

Informationssicherheit ist daher längst nicht mehr ausschließlich eine technische Aufgabe der IT-Abteilung. Sie ist zu einem zentralen Bestandteil der Unternehmensstrategie geworden. Geschäftsleitungen, Aufsichtsgremien und Führungskräfte stehen zunehmend in der Verantwortung, angemessene Sicherheitsmaßnahmen zu etablieren und Risiken systematisch zu steuern. Ein strukturiertes Informationssicherheitsmanagement schafft dabei die Grundlage, um Sicherheitsrisiken nicht nur reaktiv zu behandeln, sondern proaktiv zu steuern.

Ein Informationssicherheitsmanagementsystem (ISMS) ermöglicht es Organisationen, Informationssicherheit ganzheitlich zu betrachten: von strategischen Zielen über organisatorische Prozesse bis hin

zu technischen Kontrollen. Es schafft Transparenz über Risiken, fördert klare Verantwortlichkeiten und sorgt dafür, dass Sicherheitsmaßnahmen kontinuierlich überprüft und verbessert werden.

In einer zunehmend vernetzten und datengetriebenen Wirtschaft wird Informationssicherheit damit zu einem entscheidenden Wettbewerbsfaktor. Unternehmen, die ihre Informationswerte effektiv schützen, stärken nicht nur ihre Resilienz gegenüber Cyberangriffen, sondern gewinnen auch das Vertrauen von Kunden, Partnern und Aufsichtsbehörden.

Managementsysteme in der digitalen Transformation

Managementsysteme haben sich in vielen Bereichen als effektives Instrument zur strukturierten Unternehmensführung etabliert. Ob Qualitätsmanagement nach ISO 9001, Umweltmanagement nach ISO 14001 oder Arbeitsschutzmanagement nach ISO 45001 – standardisierte Managementsysteme helfen Organisationen dabei, komplexe Anforderungen systematisch umzusetzen und kontinuierlich zu verbessern.

Das Informationssicherheitsmanagement folgt diesem bewährten Ansatz. Die internationale Norm ISO/IEC 27001 definiert Anforderungen für ein Informationssicherheitsmanagementsystem, das Risiken identifiziert, bewertet und durch geeignete Maßnahmen reduziert. Gleichzeitig sorgt der Managementsystemansatz dafür, dass

Sicherheitsmaßnahmen nicht isoliert betrachtet werden, sondern fest in die Geschäftsprozesse integriert sind.

Mit der aktuellen Version ISO/IEC 27001:2022 wurde die Norm weiterentwickelt und stärker an moderne IT-Landschaften angepasst. Insbesondere die Struktur der Sicherheitsmaßnahmen im Annex A wurde überarbeitet und auf 93 Maßnahmen in vier Themenbereiche reduziert: organisatorische, personelle, physische und technologische Maßnahmen. Diese Neustrukturierung erleichtert die Umsetzung in der Praxis und ermöglicht eine bessere Integration moderner Technologien wie Cloud-Infrastrukturen oder Künstlicher Intelligenz.

Gleichzeitig stehen Unternehmen zunehmend unter regulatorischem Druck. Neue europäische Vorgaben wie die NIS-2-Richtlinie, die DORA-Verordnung für den Finanzsektor oder der EU AI Act stellen zusätzliche Anforderungen an Governance, Risikomanagement und Sicherheitskontrollen. Ein ISMS nach ISO/IEC 27001 kann dabei als strukturelles Fundament dienen, um viele dieser Anforderungen effizient umzusetzen.

Zielsetzung und Nutzen dieses Buches

Dieses Buch verfolgt das Ziel, Organisationen bei der praktischen Einführung eines Informationssicherheitsmanagementsystems zu unterstützen. Während zahlreiche Veröffentlichungen die Anforderungen der ISO/IEC 27001 beschreiben, fehlt es in vielen Fällen an einer klaren Anleitung für die konkrete Umsetzung im

Unternehmensalltag. Der vorliegende Praxisleitfaden richtet sich daher bewusst an Leser, die ein ISMS nicht nur verstehen, sondern tatsächlich implementieren möchten. Der Fokus liegt auf der Frage: Wie lässt sich ein Informationssicherheitsmanagementsystem Schritt für Schritt in einer Organisation etablieren und dauerhaft betreiben?

Das vorliegende Buch verbindet dabei mehrere Perspektiven:

- Normative Anforderungen der ISO/IEC 27001:2022
- Praktische Umsetzungsschritte in Unternehmen
- Organisatorische und technische Maßnahmen zur Risikoreduzierung
- Erfahrungswerte aus Audits und Implementierungsprojekten

Das Ziel ist es, eine verständliche und zugleich praxisnahe Anleitung bereitzustellen, die sowohl strategische Aspekte der Informationssicherheit als auch operative Umsetzungsschritte berücksichtigt.

Zielgruppen dieses Buches

Der Leitfaden richtet sich an verschiedene Rollen innerhalb einer Organisation, die Verantwortung für Informationssicherheit tragen oder an der Einführung eines ISMS beteiligt sind.

Dazu gehören insbesondere:

- Chief Information Security Officer (CISO)
- Informationssicherheitsbeauftragte (ISB)
- IT-Leiter und IT-Architekten
- Compliance- und Risikomanager
- Datenschutzbeauftragte
- Berater und Auditoren im Bereich Informationssicherheit

Auch Führungskräfte und Entscheidungsträger können von den Inhalten profitieren, da ein ISMS immer eine enge Zusammenarbeit zwischen Management, Fachbereichen und IT erfordert.

Nutzung dieses Buches als Implementierungsleitfaden

Der Aufbau dieses Buches folgt der Logik eines typischen Implementierungsprojekts für ein Informationssicherheitsmanagementsystem. Leser können den Leitfaden entweder vollständig durcharbeiten oder gezielt einzelne Kapitel zur Unterstützung konkreter Projektphasen nutzen.

Der Inhalt orientiert sich am PDCA-Zyklus (Plan – Do – Check – Act), der auch das methodische Fundament der ISO/IEC 27001 bildet. Dadurch entsteht eine klare Struktur, die den gesamten Lebenszyklus eines ISMS abbildet – von der Planung über die Umsetzung bis hin zur kontinuierlichen Verbesserung.

Aufbau und Struktur des Leitfadens

Der Leitfaden ist so aufgebaut, dass er den typischen Phasen einer ISMS-Einführung folgt. Zunächst werden Grundlagen, organisatorische Rahmenbedingungen und regulatorische Anforderungen erläutert. Anschließend wird der Fokus auf Risikoanalyse, Sicherheitsmaßnahmen und organisatorische Prozesse gelegt. In den späteren Kapiteln stehen Monitoring, Audits und kontinuierliche Verbesserung im Mittelpunkt. Diese Struktur ermöglicht es den Lesern, die Einführung eines ISMS systematisch zu planen und umzusetzen.

Der PDCA-Zyklus als methodisches Grundprinzip

Das zentrale methodische Fundament eines Informationssicherheitsmanagementsystems ist der PDCA-Zyklus:

- Plan – Planung des ISMS, Definition des Geltungsbereichs und Durchführung der Risikoanalyse
- Do – Implementierung von Sicherheitsmaßnahmen und Prozessen
- Check – Überwachung der Wirksamkeit, interne Audits und Managementbewertungen
- Act – kontinuierliche Verbesserung des Systems

Dieser iterative Ansatz stellt sicher, dass Informationssicherheit nicht als einmaliges Projekt verstanden wird, sondern als kontinuierlicher Verbesserungsprozess.

Überblick über ISO/IEC 27001:2022 und Annex A

Die internationale Norm ISO/IEC 27001 definiert die Anforderungen an ein Informationssicherheitsmanagementsystem. Sie legt fest, welche organisatorischen Prozesse notwendig sind, um Informationsrisiken systematisch zu identifizieren und zu behandeln. Der Annex A der Norm enthält eine Sammlung von Sicherheitsmaßnahmen, die Organisationen bei der Umsetzung geeigneter Schutzfunktionen unterstützen. In der Version 2022 wurden diese Kontrollen neu strukturiert und in vier Kategorien gegliedert:

- Organisational Controls
- People Controls
- Physical Controls
- Technological Controls

Diese Struktur bildet auch die Grundlage für die Darstellung der Sicherheitsmaßnahmen in diesem Buch.

Zusammenhang mit NIS-2, DORA und EU AI Act

Neben der ISO/IEC 27001 spielen regulatorische Anforderungen eine zunehmend wichtige Rolle im Bereich der Informationssicherheit. Insbesondere in Europa wurden in den letzten Jahren mehrere bedeutende Regelwerke verabschiedet.

Die NIS-2-Richtlinie verpflichtet viele Unternehmen zu einem höheren Sicherheitsniveau und zu Meldepflichten bei Sicherheitsvorfällen. Die DORA-Verordnung adressiert speziell den Finanzsektor und stellt Anforderungen an digitale operationelle Resilienz. Der EU AI Act wiederum schafft einen regulatorischen Rahmen für den sicheren Einsatz von Künstlicher Intelligenz. Ein ISMS nach ISO/IEC 27001 kann als strukturelle Grundlage dienen, um viele dieser Anforderungen effizient zu erfüllen.

Einführung der Running Case Study

Um die praktische Umsetzung der Inhalte zu verdeutlichen, wird in diesem Buch eine durchgehende Fallstudie verwendet. Sie begleitet die Leser durch alle Kapitel und zeigt exemplarisch, wie die einzelnen Schritte der ISMS-Einführung in einem realistischen Unternehmensumfeld aussehen können.

Als Beispiel dient die Musterfirma GmbH, ein mittelständisches Unternehmen mit rund 250 Mitarbeitern. Das Unternehmen betreibt eine hybride IT-Infrastruktur, die sowohl Cloud-Dienste als auch

klassische On-Premises-Systeme umfasst. Die Kundenstruktur ist international ausgerichtet und umfasst überwiegend Unternehmen innerhalb der Europäischen Union.

Aufgrund wachsender regulatorischer Anforderungen und steigender Kundenanforderungen hat sich die Geschäftsleitung der Musterfirma GmbH dazu entschlossen, ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 einzuführen und eine entsprechende Zertifizierung anzustreben.

Die Fallstudie zeigt Schritt für Schritt, wie das Unternehmen den Geltungsbereich des ISMS definiert, Risiken bewertet, Sicherheitsmaßnahmen implementiert und sich schließlich auf ein Zertifizierungsaudit vorbereitet. Dieses Beispielunternehmen wird in den folgenden Kapiteln immer wieder aufgegriffen, um theoretische Konzepte anhand konkreter Umsetzungsszenarien zu veranschaulichen.

Informationssicherheit ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess. Dieses Buch soll dabei unterstützen, ein ISMS strukturiert, pragmatisch und nachhaltig umzusetzen. Ich wünsche Ihnen viele hilfreiche Erkenntnisse und viel Erfolg bei der Einführung Ihres Informationssicherheitsmanagementsystems.

Herzlichst

Holger Reibold

1 Einführung

Informationssicherheit schützt Daten, Systeme und Geschäftsprozesse vor Verlust, Manipulation und Missbrauch.

Die zunehmende Digitalisierung von Geschäftsprozessen, Kommunikationsstrukturen und Wertschöpfungsketten hat Informationen zu einem der wichtigsten Vermögenswerte moderner Organisationen gemacht. Unternehmen speichern, verarbeiten und übertragen täglich große Mengen sensibler Daten – von Kundendaten über Geschäftsgeheimnisse bis hin zu kritischen Betriebsinformationen. Gleichzeitig wächst die Abhängigkeit von IT-Systemen, Cloud-Diensten und vernetzten Infrastrukturen stetig.

Mit dieser Entwicklung steigt auch die Bedeutung eines wirksamen Schutzes von Informationen. Cyberangriffe, technische Ausfälle oder menschliche Fehler können erhebliche wirtschaftliche Schäden verursachen und das Vertrauen von Kunden, Partnern und Behörden nachhaltig beeinträchtigen. Informationssicherheit ist daher längst nicht mehr ausschließlich ein technisches Thema der IT-Abteilung, sondern eine zentrale Managementaufgabe.

Ein strukturierter Ansatz zur Steuerung von Informationssicherheitsrisiken wird durch ein Informationssicherheitsmanagementsystem (ISMS) ermöglicht. Ein ISMS definiert organisatorische, technische

und prozessuale Maßnahmen, um Informationen systematisch zu schützen und Sicherheitsrisiken kontrollierbar zu machen. Dabei steht nicht nur der Schutz einzelner Systeme im Mittelpunkt, sondern ein ganzheitlicher Managementansatz, der Governance, Risikomanagement, Sicherheitskontrollen sowie kontinuierliche Überwachung und Verbesserung miteinander verbindet.

Die internationale Norm ISO/IEC 27001:2022 bildet hierfür einen weltweit anerkannten Standard. Sie beschreibt Anforderungen an ein Informationssicherheitsmanagementsystem und stellt mit dem überarbeiteten Annex A eine strukturierte Sammlung von Sicherheitskontrollen bereit. Gleichzeitig müssen Organisationen die aktuelle Bedrohungslage berücksichtigen. Angriffe wie Ransomware, Schwachstellen in Lieferketten, Fehlkonfigurationen in Cloud-Umgebungen oder neue Angriffsszenarien durch künstliche Intelligenz zeigen, dass Informationssicherheit ein dynamisches und kontinuierlich weiterzuentwickelndes Handlungsfeld ist.

Dieses Kapitel führt in die grundlegenden Konzepte der Informationssicherheit ein und erläutert die Struktur der ISO/IEC 27001 sowie die zentralen Bausteine eines modernen Informationssicherheitsmanagementsystems.

1.1 Grundlagen der Informationssicherheit

Informationssicherheit umfasst alle organisatorischen, technischen und personellen Maßnahmen, die darauf abzielen, Informationen vor

unbefugtem Zugriff, Manipulation, Verlust oder Zerstörung zu schützen. Dabei stehen nicht nur digitale Daten im Fokus, sondern grundsätzlich alle Formen von Informationen – unabhängig davon, ob sie elektronisch gespeichert, auf Papier dokumentiert oder in Gesprächen weitergegeben werden.

Das zentrale Ziel der Informationssicherheit wird häufig durch das sogenannte CIA-Triad-Modell beschrieben. Dieses Modell definiert drei grundlegende Schutzziele, die für den sicheren Umgang mit Informationen entscheidend sind:

- Vertraulichkeit (Confidentiality) bedeutet, dass Informationen nur von autorisierten Personen eingesehen werden dürfen. Unbefugte Zugriffe müssen verhindert werden. Maßnahmen wie Zugriffskontrollen, Verschlüsselung oder Berechtigungskonzepte dienen dazu, die Vertraulichkeit von Daten sicherzustellen.
- Integrität (Integrity) beschreibt die Unversehrtheit und Korrektheit von Informationen. Daten dürfen nicht unbemerkt verändert oder manipuliert werden. Technische Mechanismen wie Hashwerte, digitale Signaturen oder Versionskontrollen helfen dabei, die Integrität von Informationen zu gewährleisten.
- Verfügbarkeit (Availability) stellt sicher, dass Informationen und Systeme zum benötigten Zeitpunkt verfügbar sind. Geschäftsprozesse müssen zuverlässig funktionieren, auch bei technischen Störungen oder Sicherheitsvorfällen.

Redundante Systeme, Backups und Notfallkonzepte sind typische Maßnahmen zur Sicherstellung der Verfügbarkeit.

Neben diesen drei klassischen Schutzzielen werden in modernen Sicherheitskonzepten häufig zusätzliche Aspekte berücksichtigt. Dazu gehören beispielsweise Authentizität, also die eindeutige Zuordnung von Identitäten, sowie Nachvollziehbarkeit oder Nichtabstreitbarkeit, die sicherstellen, dass Aktionen eindeutig dokumentiert und überprüfbar sind.

Ein wesentliches Element der Informationssicherheit ist das Risikomanagement. Risiken entstehen immer dann, wenn Bedrohungen auf vorhandene Schwachstellen treffen und dadurch potenziell Schaden verursachen können. Ein Cyberangriff auf ein unzureichend abgesichertes System ist ein typisches Beispiel. Ziel eines Informationssicherheitsmanagements ist es daher, solche Risiken systematisch zu identifizieren, zu bewerten und durch geeignete Maßnahmen zu reduzieren.

Dabei ist Informationssicherheit immer ein Zusammenspiel aus Menschen, Prozessen und Technologie. Technische Schutzmaßnahmen allein reichen nicht aus, wenn organisatorische Regeln fehlen oder Mitarbeiter nicht ausreichend sensibilisiert sind. Umgekehrt bleiben organisatorische Vorgaben wirkungslos, wenn technische Systeme nicht angemessen abgesichert sind. Ein wirksames Sicherheitskonzept berücksichtigt daher alle drei Dimensionen gleichermaßen.

Ein weiterer wichtiger Grundsatz lautet: Informationssicherheit ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Bedrohungen entwickeln sich ständig weiter, neue Technologien entstehen und organisatorische Rahmenbedingungen verändern sich. Sicherheitsmaßnahmen müssen deshalb regelmäßig überprüft und angepasst werden.

Ein Informationssicherheitsmanagementsystem bietet hierfür den strukturellen Rahmen. Es sorgt dafür, dass Sicherheitsmaßnahmen systematisch geplant, umgesetzt, überwacht und kontinuierlich verbessert werden. Auf diese Weise wird Informationssicherheit zu einem festen Bestandteil der Unternehmensführung und trägt langfristig zur Stabilität und Resilienz einer Organisation bei.

1.2 Ziele und Nutzen eines ISMS

Ein Informationssicherheitsmanagementsystem verfolgt das Ziel, den Schutz von Informationen systematisch und nachhaltig in einer Organisation zu verankern. Anders als einzelne technische Sicherheitsmaßnahmen stellt ein ISMS einen ganzheitlichen Managementansatz dar, der organisatorische Strukturen, Prozesse, technische Kontrollen sowie das Verhalten von Mitarbeitern gleichermaßen berücksichtigt.

Das zentrale Ziel eines ISMS besteht darin, Informationssicherheitsrisiken zu identifizieren, zu bewerten und durch geeignete Maßnahmen zu steuern. Unternehmen sind heute einer Vielzahl

unterschiedlicher Bedrohungen ausgesetzt, die von gezielten Cyberangriffen über interne Fehlhandlungen bis hin zu technischen Störungen reichen können. Ein strukturiertes Informationssicherheitsmanagement hilft Organisationen dabei, diese Risiken frühzeitig zu erkennen, ihre Auswirkungen zu bewerten und geeignete Gegenmaßnahmen zu definieren.

Ein weiterer wichtiger Nutzen eines ISMS liegt in der Schaffung von Transparenz über Informationswerte und kritische Geschäftsprozesse. In vielen Unternehmen existieren zahlreiche IT-Systeme, Anwendungen und Datenbestände, deren Bedeutung für den Geschäftsbetrieb nicht immer vollständig dokumentiert ist. Durch die Einführung eines ISMS werden Informationswerte systematisch identifiziert, klassifiziert und hinsichtlich ihres Schutzbedarfs bewertet. Dadurch wird deutlich, welche Systeme und Daten für den Unternehmenserfolg besonders kritisch sind und entsprechend geschützt werden müssen.

Darüber hinaus trägt ein Informationssicherheitsmanagementsystem wesentlich zur Stärkung der organisatorischen Resilienz bei. Sicherheitsvorfälle lassen sich trotz umfangreicher Schutzmaßnahmen nie vollständig ausschließen. Entscheidend ist daher, wie schnell und strukturiert eine Organisation auf solche Ereignisse reagieren kann. Ein ISMS etabliert klare Prozesse für Incident Management, Notfallplanung und Wiederherstellungsmaßnahmen. Dadurch wird sichergestellt, dass Sicherheitsvorfälle kontrolliert behandelt werden und

der Geschäftsbetrieb möglichst schnell wieder aufgenommen werden kann.

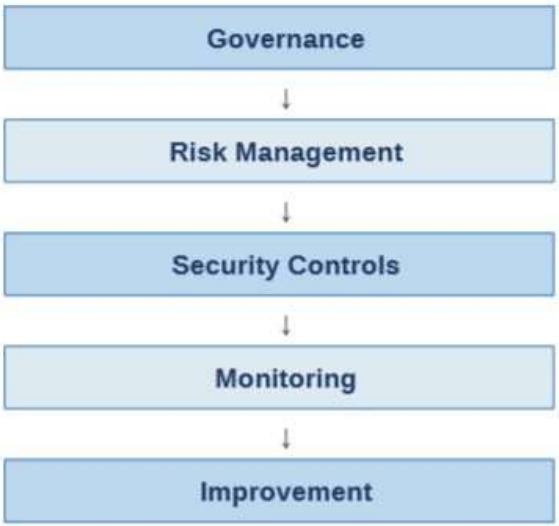
Ein weiterer wesentlicher Vorteil eines ISMS ist die Unterstützung bei der Einhaltung regulatorischer Anforderungen. Unternehmen unterliegen heute zahlreichen gesetzlichen und vertraglichen Vorgaben im Bereich der Informationssicherheit und des Datenschutzes. Dazu gehören beispielsweise branchenspezifische Sicherheitsstandards, gesetzliche Meldepflichten bei Sicherheitsvorfällen oder europäische Regelwerke wie die NIS-2-Richtlinie. Ein ISMS nach ISO/IEC 27001 bietet einen strukturierten Rahmen, um solche Anforderungen effizient umzusetzen und entsprechende Nachweise gegenüber Aufsichtsbehörden, Kunden oder Partnern zu erbringen.

Neben der Erfüllung regulatorischer Anforderungen kann ein funktionierendes ISMS auch wirtschaftliche Vorteile bringen. Sicherheitsvorfälle können erhebliche Kosten verursachen, etwa durch Produktionsausfälle, Datenverluste oder Reputationsschäden. Durch ein systematisches Sicherheitsmanagement lassen sich solche Risiken deutlich reduzieren. Gleichzeitig stärkt eine zertifizierte Informationssicherheitsstrategie das Vertrauen von Kunden, Geschäftspartnern und Investoren.

Nicht zuletzt trägt ein ISMS auch zur Entwicklung einer nachhaltigen Sicherheitskultur innerhalb der Organisation bei. Mitarbeiter werden durch Schulungen und Awareness-Programme für Sicherheitsrisiken sensibilisiert und lernen, verantwortungsvoll mit Informationen und

IT-Systemen umzugehen. Informationssicherheit wird damit zu einem festen Bestandteil des Arbeitsalltags.

Dementsprechend lässt sich festhalten, dass ein Informationssicherheitsmanagementsystem weit mehr ist als eine Sammlung technischer Sicherheitsmaßnahmen. Es schafft einen strukturierten Rahmen, um Informationsrisiken systematisch zu steuern, regulatorische Anforderungen zu erfüllen und die langfristige Stabilität sowie Wettbewerbsfähigkeit einer Organisation zu sichern.



Die grundlegende Architektur eines Informationssicherheitsmanagementsystems. Ein ISMS verbindet Governance, Risikomanagement, Sicherheitsmaßnahmen sowie kontinuierliche Überwachung und Verbesserung in einem strukturierten Managementprozess.

1.3 Aufbau der ISO/IEC 27001:2022

Die internationale Norm ISO/IEC 27001 bildet den weltweit anerkannten Standard für die Einführung, Umsetzung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS). Sie definiert Anforderungen, mit denen Organisationen Informationssicherheitsrisiken systematisch steuern und ein angemessenes Sicherheitsniveau für ihre Informationen und IT-Systeme gewährleisten können. Die aktuelle Version der Norm, ISO/IEC 27001:2022, stellt eine Weiterentwicklung der vorherigen Ausgabe dar und berücksichtigt neue technologische Entwicklungen sowie moderne Bedrohungsszenarien.

Der Aufbau der ISO/IEC 27001 folgt der sogenannten High Level Structure (HLS), die für viele moderne ISO-Managementsystemnormen verwendet wird. Diese einheitliche Struktur erleichtert die Integration verschiedener Managementsysteme innerhalb einer Organisation, beispielsweise mit Qualitätsmanagement (ISO 9001) oder Umweltmanagement (ISO 14001). Durch diese gemeinsame Struktur können Organisationen Synergien nutzen und Managementprozesse effizient miteinander verbinden. Die Norm selbst ist in mehrere Hauptkapitel unterteilt, die den gesamten Lebenszyklus eines Informationssicherheitsmanagementsystems abbilden. Zu den zentralen Kapiteln gehören insbesondere:

- **Kontext der Organisation** (Clause 4): In diesem Abschnitt wird festgelegt, dass Organisationen ihr Umfeld analysieren

und relevante interne sowie externe Anforderungen identifizieren müssen. Dazu gehören beispielsweise gesetzliche Vorgaben, Kundenanforderungen oder branchenspezifische Standards.

- **Führung und Verpflichtung** (Clause 5): Dieses Kapitel betont die Verantwortung der Unternehmensleitung. Das Management muss sicherstellen, dass Informationssicherheit in der Organisation verankert ist, ausreichende Ressourcen bereitgestellt werden und klare Verantwortlichkeiten definiert sind.
- **Planung** (Clause 6): Die Planung umfasst insbesondere die Durchführung einer Risikoanalyse sowie die Definition von Maßnahmen zur Behandlung identifizierter Risiken. Ziel ist es, Sicherheitsmaßnahmen auf Grundlage eines strukturierten Risikomanagements auszuwählen.
- **Unterstützung** (Clause 7): Hier werden Anforderungen an Ressourcen, Kompetenzen, Schulungen, Kommunikation und Dokumentation beschrieben. Diese Faktoren sind entscheidend, um ein ISMS dauerhaft und effektiv betreiben zu können.
- **Betrieb** (Clause 8): In diesem Abschnitt wird die operative Umsetzung der Sicherheitsmaßnahmen beschrieben. Organisationen müssen sicherstellen, dass geplante Prozesse umgesetzt und Risiken kontinuierlich überwacht werden.
- **Bewertung der Leistung** (Clause 9): Dieses Kapitel behandelt die Überwachung, Messung und Bewertung der Wirksamkeit

des ISMS. Interne Audits sowie Managementbewertungen spielen hierbei eine zentrale Rolle.

- **Verbesserung** (Clause 10): Der letzte Abschnitt der Norm beschreibt Anforderungen an die kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems. Sicherheitsvorfälle, Auditergebnisse und neue Risiken dienen dabei als Grundlage für Verbesserungsmaßnahmen.

Beispielhafte Governance-Struktur eines Informationssicherheitsmanagementsystems. Die Verantwortung für Informationssicherheit beginnt auf Managementebene und wird über den CISO sowie das Security-Team bis in IT und Fachbereiche operationalisiert.

Neben diesen Anforderungen enthält die Norm einen zusätzlichen Teil, den sogenannten Annex A, der eine Sammlung von

Stichwortverzeichnis

G

H

I

K

L

M

N

O

P

R

S

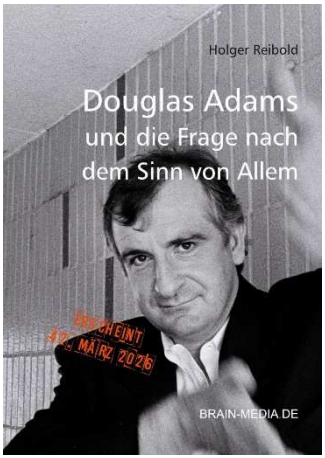
T

U

V

Z

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

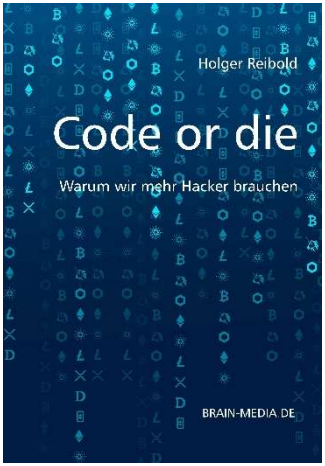
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

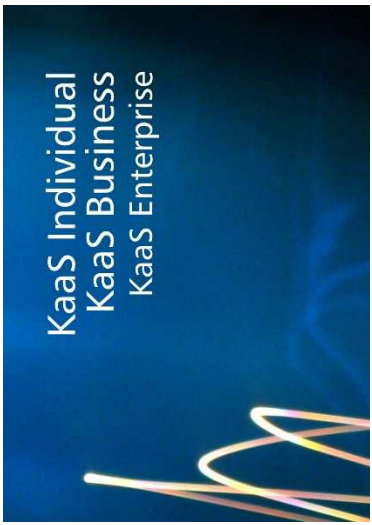
Preis: 19,99 EUR

Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 24,99 EUR



Brain-Media KaaS

Individual

Business

Enterprise

– die E-Book-Flatrate –

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt Plus+ eine Renaissance.

Abonnementen erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können über 30 verfügbare E-Books herunterladen – dazu editierbare Checklisten, Vorlagen, Beispiele etc. Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die E-Books verwenden kein DRM!

Und das alles zum **unschlagbaren Sonderpreis**!