DIN

Wolfgang Böhmer | Knut Haufe | Sebastian Klipper
Thomas Lohre | Rainer Rumpel | Bernhard C. Witt

Managementsysteme für Informationssicherheit (ISMS) mit DIN EN ISO/IEC 27001 betreiben und verbessern

Beuth

Managementsysteme für Informationssicherheit (ISMS) mit DIN EN ISO/IEC 27001 betreiben und verbessern

DIN

Wolfgang Böhmer | Knut Haufe | Sebastian Klipper
Thomas Lohre | Rainer Rumpel | Bernhard C. Witt

Managementsysteme für Informationssicherheit (ISMS) mit DIN EN ISO/IEC 27001 betreiben und verbessern

1. Auflage 2018

Herausgeber:
DIN Deutsches Institut für Normung e. V.

Beuth Verlag GmbH · Berlin · Wien · Zürich

Herausgeber: DIN Deutsches Institut für Normung e. V.

Berlin · Wien · Zürich
Am DIN-Platz
Burggrafenstraße 6
10787 Berlin

Telefon: +49 30 2601-0
Telefax: +49 30 2601-1260
Internet: www.beuth.de
E-Mail: kundenservice@beuth.de

Titelbild: © dotshock, Benutzung unter Lizenz von shutterstock.com
Satz: Meta Systems Publishing & Printservices GmbH, Wustermark
Druck: Medienhaus Plump, Rheinbreitbach
Gedruckt auf säurefreiem, alterungsbeständigem Papier nach DIN EN ISO 9706

ISBN 978-3-410-26032-5
ISBN 978-3-410-26033-2 (E-Book)

Inhalt

ISMS einrichten – warum?

1 Einleitung

Dieses Buch soll Ihnen wertvolle Hinweise, Tipps und Beispiele geben, anhand derer es Ihnen leichter fallen sollte, ein **Managementsystem für Informationssicherheit auf der Grundlage der DIN EN ISO/IEC 27001 erfolgreich zu betreiben und fortlaufend zu verbessern**. Gerade wenn Sie zum ersten Mal damit befasst sind,

- sich in die Welt der Normen und Standards zur Informationssicherheit einzuarbeiten und hierfür nach einem geeigneten Überblick suchen,
- wie ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet sein sollte, damit dieses optimal auf Ihre Anforderungen (z. B. hinsichtlich neuer Vorgaben aus dem IT-Sicherheitsgesetz) abgestimmt ist,
- was insbesondere beim laufenden Betrieb eines ISMS berücksichtigt werden sollte und
- worauf bei der fortlaufenden Verbesserung eines ISMS geachtet werden sollte,

dürfte Ihnen dieses Werk merklich weiterhelfen.

Aber auch wenn Sie sich bereits mit diesen Themen auseinandergesetzt haben, dürften Ihnen die Ausführungen der Autoren dabei helfen, Ihr ISMS zielgenauer und wirkungsvoller zu gestalten. Selbst für „alte Hasen“ gibt es nach der letzten Neufassung der DIN EN ISO/IEC 27001 noch vieles zu entdecken. Da für zunehmend mehr Sektoren inzwischen eine Zertifizierung auf Basis der DIN EN ISO/IEC 27001 vorgeschrieben ist, dürfte Ihnen dieses Buch zudem dabei helfen, diese Herausforderung erfolgreich meistern zu können.

HINWEIS

Die einzelnen Kapitel dieses Werkes stammen ausschließlich von Mitarbeitern aus dem Arbeitskreis „Anforderungen, Dienste und Richtlinien für IT-Sicherheitssysteme“ (AK 1) des DIN-Arbeitsausschusses zu „IT-Sicherheitsverfahren“ (DIN NA 043-01-27), die sowohl aus ihrer jeweiligen beruflichen Praxis als auch aus ihrer Tätigkeit im Rahmen der Normung sehr genau wissen, worauf es bei einem ISMS ankommt. Profitieren Sie von den reichhaltigen Erfahrungen der Autoren.

1.1 Abgrenzung

Der Fokus dieses Buches liegt in der fortlaufenden Verbesserung des ISMS und der zugehörigen Prozesse aus den klassischen **Check- und Act-Phasen**. Die Einführung eines ISMS und die zugehörigen Prozesse aus den klassischen Plan- und Do-Phasen spielen dagegen in diesem Werk nur eine untergeordnete Rolle. Das Buch setzt insoweit voraus, dass bereits ein ISMS eingerichtet wurde und dieses ISMS nun zertifizierungsfähig ausgerichtet oder auf Basis der neuen Fassung der DIN EN ISO/IEC 27001 praxistauglich betrieben und fortlaufend verbessert werden soll.

HINWEIS

Ein ISMS ist eingerichtet, wenn aus der DIN EN ISO/IEC 27001 die Abschnitte 4 bis 6 erfolgreich abgeschlossen wurden. **Dieses Werk konzentriert sich daher auf die Abschnitte 7 bis 10 der DIN EN ISO/IEC 27001**. Das betrifft damit die Phasen Do, Check und Act aus dem PDCA-Zyklus.

Im Rahmen eines ISMS wird Informationssicherheit adressiert und nicht IT-Sicherheit. Informationen sind die „Primary Assets“ eines ISMS und damit das primäre Schutzgut.

> Informationen können auf vielfältige Weise gespeichert werden: sowohl in digitaler Form (z. B. Dateien, die auf elektronischen oder optischen Medien gespeichert sind), in materieller Form (z. B. auf Papier) als auch in nichtmaterieller Form als Fachwissen der Mitarbeiter. Informationen dürfen auf unterschiedliche Weise übermittelt werden, wie z. B. per Post, elektronisch oder durch mündliche Kommunikation.
>
> (Abschnitt 3.2.2 der DIN EN ISO/IEC 27000)

Daher ist die **Ausrichtung auf Informationssicherheit** weitgehender als eine Ausrichtung auf IT-Sicherheit, denn diese fokussiert sich auf die digitale Form von Informationen und ist insoweit eine (im mathematischen Sinne: echte!) Teilmenge der Informationssicherheit.

Unter Informationssicherheit wird wiederum die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen verstanden (nach Abschnitt 2.33 der DIN EN ISO/IEC 27000).

In diesem Buch wird beschrieben, was beim **Management eines ISMS** wichtig ist, um den Betrieb und die fortlaufende Verbesserung des ISMS optimal gestalten zu können, und nicht, welche Maßnahmen zur Gewährleistung von Informationssicherheit sinnvoll oder geboten sind.

1.2 Zum Nutzen eines ISMS

> Die Planung und Umsetzung des ISMS einer Organisation wird beeinflusst durch die Anforderungen und Ziele der Organisation, den Sicherheitsbedarf, die angewandten Geschäftsprozesse und die Größe und Struktur der Organisation. Die Planung und der Betrieb eines ISMS erfordern es, den Interessen und Anforderungen an die Informationssicherheit aller Stakeholder der Organisation, einschließlich Kunden, Lieferanten, Geschäftspartnern, Anteilseignern und anderen betroffenen Dritten, Rechnung zu tragen.
>
> (Abschnitt 3.4 der DIN EN ISO/IEC 27000)

Ein ISMS ist daher ein systematischer, zielgesteuerter und risikobasierter Ansatz zum Management von Informationssicherheit. Dabei werden alle relevanten Anforderungen berücksichtigt, die auf den sogenannten Kontext eines ISMS einwirken. Im Rahmen der DIN EN ISO/IEC 27001 werden hierzu alle Einflussfaktoren in den Aktivitäten zu den Abschnitten 4.1 und 4.2 systematisch ausgewertet und damit in das ISMS einbezogen.

> Ein ISMS ist ein systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit der Organisation, um Geschäftsziele zu erreichen. Es basiert auf einer Risikobeurteilung und dem Risikoakzeptanzniveau der Organisation und dient dazu, die Risiken wirksam zu behandeln und zu handhaben. Eine Anforderungsanalyse für den Schutz von Informationswerten und die Anwendung angemessener Maßnahmen, um den Schutz dieser Informationswerte bedarfsgerecht sicherzustellen, trägt zu der erfolgreichen Umsetzung eines ISMS bei.
>
> (Abschnitt 3.2.1 der DIN EN ISO/IEC 27000)

Ein ISMS trägt daher entscheidend dazu bei festzustellen, welche Informationssicherheitsrisiken tatsächlich zu adressieren sind und welche begründet beibehalten werden können. Das ist effektiv und effizient zugleich. Aufwendun-

gen für überflüssige oder minderwertige Maßnahmen können auf diese Weise eingespart werden. Relevante Informationssicherheitsrisiken werden dagegen erkannt und können so adäquat behandelt werden. Dies entlastet wiederum die Geschäftsführung bei ihrer Organhaftung.

Durch den systematischen Ansatz und die zielorientierte Ableitung von Maßnahmen auf Basis des risikobasierten Ansatzes werden zugleich interne Prozesse fortlaufend verbessert und damit zielgenauer. Zugleich erhöht sich das Niveau erreichter Informationssicherheit (inkl. IT-Sicherheit) und das Niveau erreichten Datenschutzes quasi automatisch. Vorausgesetzt, das ISMS wird sinnvoll gesteuert. Dieses Buch soll Ihnen dabei helfen, Ihr ISMS in diesem Sinne zielgerecht zu steuern.

1.3 Struktur dieses Buches

Dieses Buch gliedert sich in zwei Teile:

1) Im **ersten Teil** wird die Frage beantwortet, **warum ein ISMS eingerichtet** werden sollte. Dieser Teil dient der Hinführung zum Hauptteil.
   a) Dazu wird zunächst der „rechtliche Rahmen“ dargestellt, welche Vorschriften zum Management von Informationssicherheit beachtet werden sollten und wo es sogar eine Verpflichtung zur Einrichtung eines ISMS gibt.
   b) Anschließend werden „Hintergründe zur Normung“ benannt, wie Normungstätigkeiten durchgeführt werden und was die zahlreichen Abkürzungen im Normungswesen bedeuten.
   c) Daraufhin wird ein detaillierter „Überblick über die Normungsfamilie ISO/IEC 2700x“ gegeben, zu dessen Zweck die zahlreichen Standards zu den IT-Sicherheitsverfahren geeignet eingruppiert werden.
   d) Schließlich wird im ersten Teil näher vorgestellt, was „integrierte Managementsysteme“ sind.
2) Im **zweiten Teil**, dem eigentlichen Hauptteil dieses Werkes, wird ausgeführt, **was nach der Einrichtung eines ISMS zu tun** ist.
   a) Zuerst wird genauer beleuchtet, wie die „Betriebsdokumentation eines ISMS“ aussehen sollte und die Dokumentenpyramide vorgestellt.
   b) Daraufhin wird im Kapitel „Ressourcen bereitstellen und Kompetenz gewährleisten“ ausgeführt, was beim Ressourcenmanagement für ein ISMS zu beachten ist und welche Rollen es bei einem ISMS-Betrieb üblicherweise gibt, welche Aufgaben diese zu erfüllen haben und welche

Anforderungen infolgedessen die Träger dieser Rollen mitbringen sollten.

c) Im Kapitel „Bewusstsein schaffen und Kommunikation verbessern“ wird aufgezeigt, was unter dem Begriff Bewusstsein zu verstehen ist, welche Randbedingungen für Kommunikation besteht und wie auf dieser Grundlage eine Sicherheitskultur ausgebildet werden kann.

d) Wie im Rahmen des ISMS das „Risikomanagement“ ausgestaltet werden kann, wird im gleichnamigen Kapitel beschrieben. Hierbei wird dargestellt, was bei der Informationssicherheitsrisikobeurteilung einerseits und bei der Informationssicherheitsrisikobehandlung andererseits beachtet werden sollte. Zudem wird weiter ausgeführt, welche Aspekte im Rahmen der Überwachung der Informationssicherheitsrisiken eine Rolle spielen.

e) Im Kapitel „ISMS bewerten“ werden bestehende Reifegradmodelle vorgestellt sowie Anforderungen und Werkzeuge zum Messen und Bewerten benannt.

f) Schließlich wird in dem Kapitel „ISMS verbessern“ aufgezeigt, was bei der fortwährenden Verbesserung eines ISMS relevant ist und wie insbesondere mit Nichtkonformitäten umzugehen ist.

Die einzelnen Kapitel lassen sich im Rahmen der DIN EN ISO/IEC 27001 und in der Darstellung des klassischen PDCA-Zyklus einordnen (siehe Tabelle 1).

Tabelle 1: Einordnung der Buchkapitel zur DIN EN ISO/IEC 27001 und zum PDCA-Zyklus

Buchkapitel	Referenz DIN EN ISO/IEC 27001	PDCA-Phase
Rechtlicher Rahmen	Abschnitte 4.1 und 4.2	Plan
Hintergründe zur Normung	---	---
Überblick über die Normungsfamilie ISO/IEC 2700x	---	---
Integrierte Managementsysteme	Abschnitt 4.4	Plan
Betriebsdokumentation eines ISMS	Abschnitt 7.5	Do

Buchkapitel	Referenz DIN EN ISO/IEC 27001	PDCA-Phase
Ressourcen bereitstellen und Kompetenz gewährleisten	Abschnitte 7.1 und 7.2 (in Verbindung mit 6.2)	Do
Bewusstsein schaffen und Kommunikation verbessern	Abschnitte 7.3 und 7.4	Do
Risikomanagement	Abschnitte 8.2 (in Verbindung mit 6.1.2) und 8.3 (in Verbindung mit 6.1.3)	Check
ISMS bewerten	Abschnitt 9 (in Verbindung mit 6.1.1 und 6.2)	Check
ISMS verbessern	Abschnitt 10 (in Verbindung mit 9)	Act

Ergänzend zu diesem Buch liefert die ISO/IEC 27003 weitere Hinweise, wie die Angaben aus der DIN EN ISO/IEC 27001 zu interpretieren sind. Diese wurde 2017 veröffentlicht. Eine deutsche Übersetzung wird aber noch etwas Zeit beanspruchen.

Eine Hilfestellung zur Überwachung, Messung, Analyse und Bewertung eines ISMS liefert die ISO/IEC 27004, seit 2016 veröffentlicht, aber ebenfalls noch nicht in deutscher Übersetzung erhältlich. Hinweise zur Durchführung des Risikomanagements im Rahmen der DIN EN ISO/IEC 27001 stellt die ISO/IEC 27005 zur Verfügung, Hinweise zur Planung und Durchführung interner Audits die ISO/IEC 27007 und Hinweise zur Prüfung getroffener Maßnahmen die ISO/IEC TS 27008 (alle drei befinden sich derzeit in Überarbeitung). Hilfestellungen zur integrierten Umsetzung von ISMS und ITIL (hinsichtlich der zertifizierungsfähigen Variante nach der ISO/IEC 20000-1) gibt die ISO/IEC 27013. Aspekte zur Steuerung der Informationssicherheit beschreibt wiederum die ISO/IEC 27014 und ökonomische Aspekte die ISO/IEC TR 27016.

Die Autoren dieses Buches wünschen Ihnen viel Erfolg bei der Umsetzung der gewonnenen Erkenntnisse!

2 Rechtlicher Rahmen

Wenn ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet und betrieben werden soll, dann sind dabei insbesondere rechtliche Vorschriften zum Management von Informationssicherheit zu beachten. Im Rahmen der DIN EN ISO/IEC 27001 stellen solche Vorschriften wiederum Anforderungen dar, die einen starken Einfluss darauf haben, wie das ISMS ausgerichtet ist. Für bestimmte Sektoren bestehen sogar rechtliche Verpflichtungen zur Einrichtung eines ISMS.

2.1 Vorschriften zum Management von Informationssicherheit

Zunehmend wird auf der Grundlage rechtlicher Vorschriften von Unternehmen verlangt, so etwas wie ein ISMS einzurichten und zu betreiben. Dies geschieht über drei Varianten:

1) Der Gesetzgeber orientiert sich an internationalen Standards, wie der DIN EN ISO/IEC 27001, und fordert hier ggf. zusätzlich die Umsetzung sektorspezifischer Erweiterungen ein.
2) Der Gesetzgeber orientiert sich vor allem im Behördenkontext an deutschen Standards und Rahmenwerke, wie die Standards und IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
3) Der Gesetzgeber legt einzelne Aspekte ausdrücklich fest ohne Bezug auf internationale oder nationale Standards und fordert von den entsprechend verpflichteten Stellen eine geeignete Umsetzung.

Lange Zeit war die dritte Variante die vorherrschende Vorgehensweise, die sich in zahlreichen Rechtsvorschriften (vor allem bei der Gewährleistung von Grundrechten) wiederfand, insbesondere

– **zum Datenschutz und zum Schutz der Telekommunikation** (z. B. §§ 4d Abs. 5, 9, 11, 31 und 42a BDSG, §§ 93 Abs. 3, 100, 107 und 109 TKG und §§ 13 und 15a TMG u. v. a. m.).

Flankiert wurde dies durch Rechtsvorschriften

– **zur Sorgfalt eines ordentlichen Geschäftsmannes** (z. B. § 347 Abs. 1 HGB, § 93 Abs. 1 AktG, § 43 Abs. 1 GmbHG, § 34 Abs. 1 GenG) – zur frühzeitigen Erkennung fortbestandsgefährdender Risiken (z. B. nach § 91 Abs. 2 AktG) und zur Gewährleistung ausreichender Verkehrssicherheit durch Malwareschutz und manipulationsfester Datensicherung (z. B. nach den GoBD),
– **zur Haftung** (z. B. § 130 OWiG, § 276 BGB u. v. a. m.)

– **und zum Umgang mit Schadensfolgen** (z. B. §§ 254, 823 und 1004 BGB, §§ 97 und 100 UrhG u. v. a. m.).

HINWEIS

Neben diesen allgemeinen Vorschriften zum Management von Informationssicherheit sind beim Betrieb eines ISMS **datenschutzrechtliche und mitbestimmungsrechtliche Vorgaben** zu beachten, da ein ISMS durchaus der Verhaltenskontrolle dient, und bestehende **Meldepflichten** umzusetzen. Diese Anforderungen finden über Abschnitt 4.2 der DIN EN ISO/IEC 27001 Eingang in die Gestaltung des ISMS und beeinflussen dessen Ausrichtung und Betrieb entscheidend mit.

Infolge der Rechtsprechung zur Vorratsdatenspeicherung einerseits (durch Aufnahme des § 109a TKG) und im Zuge des **IT-Sicherheitsgesetzes** andererseits kamen für Betreiber kritischer Infrastrukturen weitere Verpflichtungen hinzu (wie §§ 8a und 8b BSIG und § 11 Abs. 1b EnWG). Ferner hat mittlerweile der Datenschutz mit der Verabschiedung der **EU-Datenschutz-Grundverordnung** (EU-Verordnung 2016/679) eine andere Ausprägung erhalten (hier vor allem durch Art. 24, 25, 32 und 33 der EU-DS-GVO), die entsprechende bisherige Datenschutzbestimmungen verdrängen.

Die neuere Rechtsetzung orientiert sich immer stärker an allgemein anerkannten Standards, wie der DIN EN ISO/IEC 27001, oder legt eine Umsetzung rechtlicher Anforderungen durch Erfüllung eines allgemein anerkannten Standards zumindest faktisch nahe.

2.2 Rechtliche Verpflichtungen zur Einrichtung eines ISMS

Für hochregulierte Branchen besteht in den jeweiligen Ausführungsbestimmungen eine explizite Verpflichtung zur Einrichtung eines ISMS (entweder nach der DIN EN ISO/IEC 27001 oder nach den IT-Grundschutz-Katalogen):

1) **Energiesektor**: Gemäß § 11 Abs. 1a EnWG wurde von der zuständigen Aufsichtsbehörde, der Bundesnetzagentur (BNetzA), ein verbindlicher „IT-Sicherheitskatalog“ vorgeschrieben, der in der aktuellen Fassung vom August 2015 unter anderem ausführt:

– „Kernforderung des vorliegenden Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems gemäß DIN ISO/IEC 27001“ (Seite 3)