

Richtig planen, durchführen, dokumentieren

TÜV Media

Managementreview zur ISO/IEC 27001 im IMS

Autor:

Dr.-Ing. Wolfgang Kallmeyer
Partner der TÜV Rheinland Consulting GmbH

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7406-0918-4 (Print)
ISBN 978-3-7406-0919-1 (E-Book)

© by TÜV Media GmbH, TÜV Rheinland Group, 1. Auflage, Köln 2024
tuev-media.de

® TÜV, TUEV und TUV sind eingetragene Marken.
Eine Nutzung und Verwendung bedarf der vorherigen Zustimmung.

Die Inhalte dieses Werks wurden von Verlag und Redaktion nach bestem Wissen und Gewissen erarbeitet und zusammengestellt. Eine rechtliche Gewähr für die Richtigkeit der einzelnen Angaben kann jedoch nicht übernommen werden. Gleiches gilt auch für Websites, auf die über Hyperlinks verwiesen wird. Es wird betont, dass wir keinerlei Einfluss auf die Inhalte und Formulierungen der verlinkten Seiten haben und auch keine Verantwortung für sie übernehmen. Grundsätzlich gelten die Wortlaute der Gesetzestexte und Richtlinien sowie die einschlägige Rechtsprechung.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten in der Regel gleichermaßen für alle Geschlechter.

Über die Broschüre

Die Managementbewertung gehört zur alltäglichen Praxis für alle Organisationen, die ein zertifiziertes Managementsystem unterhalten. In dieser Broschüre erhalten Sie einleitende Informationen, auf welcher Grundlage die Managementbewertungen nach ISO/IEC 27001:2022 – Informationssicherheitsmanagementsystem (ISMS) [1] beruhen und welche normativen Anforderungen dabei zu berücksichtigen sind.

Im Kern der Broschüre erfahren Sie, wie Sie eine normenkonforme und strukturell übersichtliche Managementbewertung zur ISO/IEC 27001 durchführen können, was Inhalte der dokumentierten Bewertung sein müssen und was ggf. in andere begleitende Dokumente (Anlagen) ausgelagert werden kann.

Sie erhalten auch ergänzende Hinweise, wie Sie die Managementbewertung zum ISMS integrativ mit anderen ISO-Normen verbinden können. Als Beispiel wird dabei ein integriertes Managementsystem (IMS) nach ISO 9001 [2], ISO 14001 [3] und ISO 45001 [4] und deren Managementreview herangezogen. Dabei wird gezeigt, wie vergleichbare Forderungen integrativ bearbeitet werden können, um Redundanzen zu vermeiden und das gemeinsame Review im Umfang auf das Notwendigste zu beschränken.

Außerdem erhalten Sie eine Anleitung, in welchen Schritten und mit welchen Methoden Sie die Managementbewertung in der Praxis gestalten können. Auch werden die Freiräume beschrieben, die Sie haben, um dabei den Bedürfnissen ihrer Organisation gerecht zu werden. Der Umgang mit der Managementbewertung im Nachgang ist ebenso Thema, damit Ihre Organisation daraus den größtmöglichen Nutzen ziehen kann.

Im Ergebnis erfahren Sie, wie Sie aus einer (ungeliebten) Pflicht ein übersichtliches und akzeptiertes Führungsinstrument machen können.

Die im Text angeführten Klammersymbole verweisen auf Arbeitshilfen, die Sie bei der Erstellung und Dokumentation des Managementreviews unterstützen und die wir für Sie zum Download bereitgestellt haben. Sie können die Dokumente frei bearbeiten und an Ihre eigenen betrieblichen Anforderungen anpassen.

Verweismatrix Forderungen an die Managementbewertung

Drei Managementsysteme (ISO 9001/ISO 14001/ISO 45001) bilden die Grundlage für das Managementreview des IMS in das das Review der ISO/IEC 27001 integriert wird. Dabei erheben die vier Normen nur auf den ersten Blick gemeinsame Forderungen bezüglich des Managementreviews. Bei genauer Analyse unterscheiden sich, neben vielen Gemeinsamkeiten, die Forderungen der spezifischen Managementsysteme in einigen Punkten. Eine detaillierte Gegenüberstellung der Anforderungen gibt die Verweismatrix zur Managementbewertung.

Matrix Datenquellenplan

Um die Datenerfassung für das Managementreview übersichtlicher zu gestalten, ist es hilfreich, eine Matrix zu erstellen, aus der die Details der zu erfassenden Daten ersichtlich werden. Dazu gehören Datenquellen, Art der Daten, Verantwortlicher für die Erfassung, Aufbereitung und Bereitstellung

Zielsetzung

Arbeitshilfen zum Download



Verweismatrix.xlsx



Datenquellen.xlsx

[1] DIN EN ISO/IEC 27001:2024 – Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022)

[2] DIN EN ISO 9001:2015 – Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015)

[3] DIN EN ISO 14001:2015 – Umweltmanagementsysteme – Anforderungen mit Anleitung zur Anwendung (ISO 14001:2015)

[4] DIN EN ISO 45001:2018 – Managementsystem für Sicherheit, Gesundheit bei der Arbeit – Anforderungen mit Anleitung zur Anwendung (ISO 45001:2018)

**Management-
review.docx**

der Daten, Zeitpunkt(e) der Bereitstellung der Daten. Die Arbeitshilfe bietet dazu eine erprobte Vorlage.

Vorlage Managementreview – Word

Für die Art der Darstellung des Protokolls zum Managementreview gibt es keine Normenvorgaben. In der Praxis eingebürgert haben sich zwei Formen, die sich gängiger Microsoft-Office-Programme bedienen (Word und PowerPoint). Diese in der Broschüre vorgestellten Formen des Musterreviews eines fiktiven Unternehmens unterscheiden sich inhaltlich nicht. Sie haben jedoch aufgrund ihrer Darstellungsweise spezifische Vor- und Nachteile. Überwiegend wird das Managementreview in der hier zum Download angebotenen klassischen Form eines Word-Dokuments erstellt. Der Vorteil dieser Vorgehensweise besteht darin, dass die meisten Anwender in der Nutzung einer Textverarbeitung geübt sind.

**Management-
review.pptx**

Vorlage Managementreview – PowerPoint

Für die Art der Darstellung des Protokolls zum Managementreview gibt es keine Normenvorgaben. In der Praxis eingebürgert haben sich zwei Formen, die sich gängiger Microsoft-Office-Programme bedienen (Word und PowerPoint). Diese in der Broschüre vorgestellten Formen des Musterreviews eines fiktiven Unternehmens unterscheiden sich inhaltlich nicht. Sie haben jedoch aufgrund ihrer Darstellungsweise spezifische Vor- und Nachteile. Zunehmend wird neben Word in der Praxis das Review in der hier zum Download angebotenen Form einer PowerPoint-Präsentation erstellt. Das hat den Vorteil, dass die Ergebnisse des Reviews für Präsentationen direkt geeignet sind. Aufgrund der Folienstruktur können Themen der Bewertung auch übersichtlich voneinander abgegrenzt werden.

**Maßnahmenplan.
xlsx**

Maßnahmenplan zum Managementreview

Die im Managementreview beschlossenen ISMS-Ziele und Maßnahmen können gemeinsam mit den Zielen und Maßnahmen der drei anderen Systeme des IMS im Protokoll des Managementreviews dokumentiert werden. Um das Review vom Umfang her weiter zu begrenzen, kann die Dokumentation von Zielen und Maßnahmen in separaten Anhängen zum Protokoll erfolgen. Ein Muster eines solchen vom Managementreview losgelösten Maßnahmenplans, das Sie an Ihre Bedürfnisse anpassen können, haben wir als Excel-Dokument beigefügt.

Download

Die Arbeitshilfen stehen für Sie zum Download bereit unter:

qm-aktuell.de [Redacted]

Passwort: [Redacted]

Sie können die Dokumente frei bearbeiten und an Ihre eigenen betrieblichen Anforderungen anpassen.

Inhalt

Über die Broschüre	3
1 Zielstellungen des Managementreviews	7
1.1 Normenanforderung an das Managementreview.....	7
1.2 Managementreview aus Unternehmenssicht.....	8
1.3 Managementreview aus Zertifizierungssicht	9
1.4 Integration der ISO/IEC 27001 in ein IMS.....	10
2 Vorbereitung des Managementreviews	15
2.1 Umfang des Managementreviews	15
2.2 Ablaufschritte des Managementreviews	15
2.3 Turnus der Bewertung	16
2.4 Managementreview strukturieren	20
2.5 Datenquelle festlegen.....	22
3 Erstellung des Managementreviews	25
3.1 Organisatorische Methoden der Erstellung.....	25
3.2 Dokumentarische Anforderungen.....	26
3.3 Reviewdaten bewerten und Maßnahmen festlegen.....	30
3.4 Ergebnisse dokumentieren und Maßnahmenplan erstellen.....	32
4 Nach dem Review ist vor dem Review	35
4.1 Kommunikation der Ergebnisse des Managementreviews.....	35
4.2 Nachverfolgung des Managementreviews	36

- Leseprobe -

1 Zielstellungen des Managementreviews

1.1 Normenanforderung an das Managementreview

Die Managementbewertung nach Normkapitel 9.3 ist eine Anforderung der ISO bei all jenen Managementsystemnormen, die Grundlage einer externen Zertifizierung sind, so auch für die ISO/IEC 27001. Im Allgemeinen wird sie in vielen Organisationen auch als Managementreview bezeichnet. Diese Bezeichnung wird im Folgenden hauptsächlich verwendet, da sie sich in der Praxis eingebürgert hat. Der Begriff „Review“ steht für eine kritische Überprüfung oder Nachprüfung der Leistung und Wirksamkeit des betrachteten Managementsystems und der darin eingebetteten Organisationsprozesse.

Was sind die Grundanforderungen der ISO/IEC 27001 – Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre (ISMS) an das Managementreview? Die Formulierung zum Normkapitel 9.3 „Managementbewertung“ lautet unter 9.3.1 „Allgemeines“: *„Die oberste Leitung muss das Informationssicherheitsmanagementsystem der Organisation in geplanten Abständen bewerten, um dessen fortlaufende Eignung, Angemessenheit und Wirksamkeit sicherzustellen.“*

Wenn man diesen Satz in seinen Teilen analysiert, stellt sich zuerst die Frage, wer mit der obersten Leitung gemeint ist. Dazu gibt die ISO/IEC 27001 keine Hinweise. Aber im Leitfaden ISO 9000:2015 „Qualitätsmanagementsysteme – Grundlagen und Begriffe“ steht im Normkapitel 3 „Begriffe“ eine Definition unter 3.1.1. Als oberste Leitung wird dort definiert *„die Person oder Personen-Gruppe, die eine Organisation auf oberster Ebene führt und steuert.“* Dabei gibt es in der Praxis schon Unterschiede in der Leitungsorganisation, die sich z. B. aus der Organisationsgröße und -struktur ergeben. In einem mittelständischen Unternehmen mit nur einem Standort ist die Frage nach der obersten Leitung wohl meist einfach zu beantworten. Es ist der Geschäftsführer oder bei einer mehrköpfigen Unternehmensleitung die Geschäftsführung.

Bei einem weltumspannenden Konzern mit Tochtergesellschaften und Standorten in vielen Ländern ist die Antwort auf die Frage nach der obersten Leitung schon etwas komplexer. In der Praxis geht man dazu auf die nationalen Gesellschaften und deren Führung als oberste Leitung zurück. Im Einzelfall kann bei größeren Standorten (unselbstständige Werke einer nationalen Gesellschaft) als oberste Leitung auch die Werksleitung aufgefasst werden. Besteht die oberste Leitung aus mehr als einer Person (Führungsgremium), sollte die Verantwortung für das ISMS explizit (z. B. im Geschäftsverteilungsplan) auf eine davon übertragen werden. Gleiches gilt für die weiteren Normen des IMS.

Als Nächstes ist der Begriff „geplante Abstände“ im Sinne der Normen zu klären. Die Wortwahl weist auf eine regelmäßig wiederkehrende Aktion der obersten Leitung hin. Zur Klärung dieser Frage ist die gelebte Praxis heranzuziehen. Der maximale Abstand zwischen einem Managementreview und dem nächsten beträgt in der Regel zwölf Monate. Das ergibt sich aus der Pflicht der Zertifizierungsgesellschaften (Vorgabe der Deutschen Akkreditierungsstelle, DAkkS), jährlich ein Überwachungsaudit der zertifizierten Managementsysteme ihrer Kunden vorzunehmen. Zu den wichtigsten Prüfpunkten gehören dabei das zuletzt durchgeführte interne Audit und das aktuelle Managementreview. Zum Zeitpunkt der Prüfung durch den Zertifizierungsauditor sollte das Managementreview nicht älter als drei Monate sein.

Bleibt als letzter Punkt zu klären, was die Bewertung von Eignung, Angemessenheit und Wirksamkeit des Managementsystems bedeutet. Was genau da zu bewerten ist, findet sich nicht in der ISO/IEC 27001, sondern ist in anderen weit verbreiteten Managementsystemen (Normenhang A, A.9.3, ISO 14001

**Management-
bewertung**

**Grund-
anforderungen**

Oberste Leitung

**Komplexe
Unternehmens-
strukturen**

Geplante Abstände

**Eignung,
Angemessenheit
und Wirksamkeit**