Autor:

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

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

ISBN 978-3-7406-0809-5 (Print)
ISBN 978-3-7406-0810-1 (E-Book)

Zur Nutzung der Broschüre

Zielsetzung der Broschüre

Interne Systemaudits gehören zum Alltag für alle Organisationen, die ein zertifiziertes Managementsystem unterhalten. Die Änderungen durch die Revision in 2022 sind berücksichtigt. In dieser Fachbroschüre erhalten Sie einleitende Informationen dazu, auf welchen Grundlagen interne Audits beruhen und welche normativen Regelwerke dabei zu berücksichtigen sind.

Aufbau

Im Kern dieser Broschüre erfahren Sie, wie Sie interne Audits nach ISO/IEC 27001 durchführen können. Zur Bildung von Auditfragen stellen wir Ihnen dazu die Textanalyse und die Turtle-Analyse vor, die beiden gebräuchlichen Methoden, mit denen Sie recht einfach passende Auditfragen generieren können.

Außerdem erhalten Sie Hinweise zu korrektem Kommunikationsverhalten in verschiedenen Auditsituationen und zur richtigen Fragetechnik, mit der Sie im Audit die für eine Bewertung notwendigen Informationen erhalten.

Der Fragenkatalog

Zu Ihrer Zeitersparnis finden Sie einen direkt verwendbaren Auditfragenkatalog für das interne Systemaudit, basierend auf den Forderungen der ISO/IEC 27001:2022, beigefügt.

Arbeitshilfen zum Download

Die im Text angeführten Klammersymbole verweisen auf Arbeitshilfen, die Sie bei der Generierung von Auditfragen unterstützen und die wir Ihnen zum Download bereitgestellt haben:

Verweismatrix „Änderungen der Normkapitel in ISO/IEC 27001, 2015–2022“

Änderungen_ Normkapitel.xlsx

In der beigefügten Arbeitshilfe sind alle Änderungen der Normkapitel 4 bis 10 von ISO/IEC 27001:2022 zu DIN EN ISO/IEC 27001:2015 in Form einer Verweismatrix zusammengefasst.

Verweismatrix „Änderungen Anhang A in ISO/IEC 27001, 2015–2022“

Änderungen_ Anhang.xlsx

In der Arbeitshilfe sind alle Änderungen von DIN EN ISO/IEC 27001:2015, Anhang A, zu ISO/IEC 27001:2022, Anhang A.1, in Form einer Verweismatrix aufgelistet

Auditfragenkatalog zum internen Systemaudit nach ISO/IEC 27001

Fragenkatalog_ 27001.docx

Der Auditfragenkatalog für das interne Systemaudit wurde für Sie auf der Grundlage der Forderungen der ISO/IEC 27001:2022 mittels Textanalyse generiert. Den Fragenkatalog können Sie an die Erfordernisse Ihrer Organisation anpassen und um firmenspezifische Belange ergänzen.

Auditfragen generieren mit Turtle-Analyse

Turtle-Analyse_ 27001.docx

Neben der Textanalyse lassen sich auch mit der Methode der Turtle-Analyse aus den Prozessen der Organisation nachvollziehbar und systematisch Auditfragen entwickeln. Über das strukturierte Formular werden alle relevanten Einflussfaktoren erfasst und zudem die Prozesse und ihre möglichen Risiken dargestellt. Sinnvollerweise werden auf diesem Formular auch Infos zu Prozesseigner, die Prozessbezeichnung und die Prozessstützen erfasst. Als Beispiel ist exemplarisch das Muster einer Turtle-Analyse für den Prozess „Interne Audits“ beigefügt.

Die Arbeitshilfen stehen für Sie zum Download bereit unter:

https://www.qm-aktuell.de/60809-2/

Passwort: **23104**

Inhalt

1 Auditprozess und seine Grundlagen

Definition Audit

Nach der ISO 9000 [1] (Normkapitel 3.13.1) ist ein Audit ein *„systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit Auditkriterien erfüllt sind“*.

ISO 19011

Zur Vorbereitung und Durchführung von internen Audits und Lieferantenaudits wurde die ISO 19011 [2] entwickelt. Das Management von Zertifizierungsaudits wird in der ISO/IEC 17021-1 [3] geregelt, die ISO 19011 kann dabei als Hilfestellung herangezogen werden.

Tabelle 1 gibt einen zusammenhängenden Überblick über die Auditarten, ihre Bezeichnungen und ihre normative Zuordnung.

Tabelle 1: Auditarten, Bezeichnungen und Anwendungsbereiche von ISO 19011 und ISO/IEC 17021

Auditarten	Internes Audit	Externes Audit	
		Lieferantenaudit (ggf. Kundenaudit)	Zertifizierungsaudit
Alternative Bezeichnungen	First-Party-Audit	Second-Party-Audit	Third-Party-Audit
Anwendungsbereich der Normen	ISO 19011	ISO/IEC 17021	

Bewertung und Verbesserung

Das Ziel eines internen Systemaudits (First-Party-Audit) besteht darin, das gesamte installierte Informationssicherheitsmanagementsystem (ISMS) eines Unternehmens nach ISO/IEC 27001 [4] systematisch zu bewerten und zu verbessern. Die Durchführung obliegt dabei meist geschulten Mitarbeitern des Unternehmens. Bei einem Systemaudit wird die gesamte Aufbau- und Ablauforganisation eines Unternehmens daraufhin überprüft, ob die Normenforderungen der ISO/IEC 27001 erfüllt sind und die eigenen Informationssicherheitsziele erreicht werden können.

Die Anforderungen an Interne Audits in der ISO/IEC 27001 unterscheiden sich im Grundsatz nicht von den Anforderungen anderer Systemnormen wie der ISO 9001 [5] oder ISO 14001. Methodisch sind ein vergleichbares Vorgehen und eine integrierte Auditdurchführung jederzeit möglich.

Informationssicherheit steigern

Wird das gesamte ISMS eines Unternehmens durch regelmäßige Audits überprüft, können Abweichungen in der Informations-, IT- und Cybersicherheit früh erkannt und rechtzeitig korrigiert werden. Dies senkt das Risiko von Daten- und Informationsverlusten und die damit verbundenen materiellen und immateriellen Schäden. Da Informationssicherheitsaudits immer auch darauf abzielen, Verbesserungsmöglichkeiten zu finden, selbst wenn der Ablauf von IT-Sicherheitsverfahren und Informationssicherheitsbelangen relativ reibungslos funktioniert, können diese regelmäßigen Überprüfungen auch dazu genutzt werden, das Sicherheitsniveau für Informationen und Daten in einem Unternehmen fortlaufend zu steigern. Der Schwerpunkt eines internen Audits liegt in der Suche nach Verbesserungspotenzial zur Weiterentwicklung des Managementsystems und der Unternehmensprozesse. Die Erfüllung der Normenforderung spielt, im Gegensatz zu einem Zertifizierungsaudit, nur eine nachrangige Rolle.

Im Rahmen der Durchführung eines internen Audits sollen Informationen durch geeignete Stichprobenverfahren in Bezug auf die Auditziele und die Auditkriterien gesammelt werden. Darin enthalten sind auch Informationen, die sich auf Schnittstellen zwischen Funktionsbereichen, Tätigkeiten und Prozessen beziehen. Um an die notwendigen Auditinformationen zu kommen, müssen verschiedene Methoden der Informationsbeschaffung genutzt werden.

Methoden der Informationsbeschaffung

Gängige Methoden der Informationsbeschaffung in einem Audit sind:

- Führen von Interviews mit Mitarbeitern,
- Beobachten von Tätigkeiten und Prozessabläufen,
- Prüfen von dokumentierter Information (Dokumente, Nachweise),
- Begehung des Standorts und Begutachtung von Informationstechnologien.

Das Interview und die Befragung von Mitarbeitern und Führungskräften der auditierten Organisation sind die wichtigsten Instrumente zur Generierung von Auditfeststellungen für den Auditor. Dazu sind die richtigen Fragen zur richtigen Zeit am richtigen Ort zu stellen.

2 Leiten und Lenken von internen Audits

Leitfaden

Die Anforderungen an interne Audits sind im Normkapitel 9.2 der ISO/IEC 27001 festgelegt. Die Beschreibung, was im Unternehmen genau zu tun ist, um die Normenforderung zu erfüllen, ist aber nicht im Detail ausgeführt. Daher hat die International Standard Organization (ISO) den „Leitfaden zur Auditierung von Managementsystemen" (ISO 19011) herausgebracht. Der Leitfaden leistet den Unternehmen Hilfestellung bei der Planung und Durchführung von internen Audits. Die Ausführungen in diesem Leitfaden sind kein Muss, aber ein *Sollte* oder *Könnte,* um die Anforderungen an interne Audits zielgerichtet für das Unternehmen festzulegen und umzusetzen.

Die Gliederung der ISO 19011 zeigt die Abbildung 1.

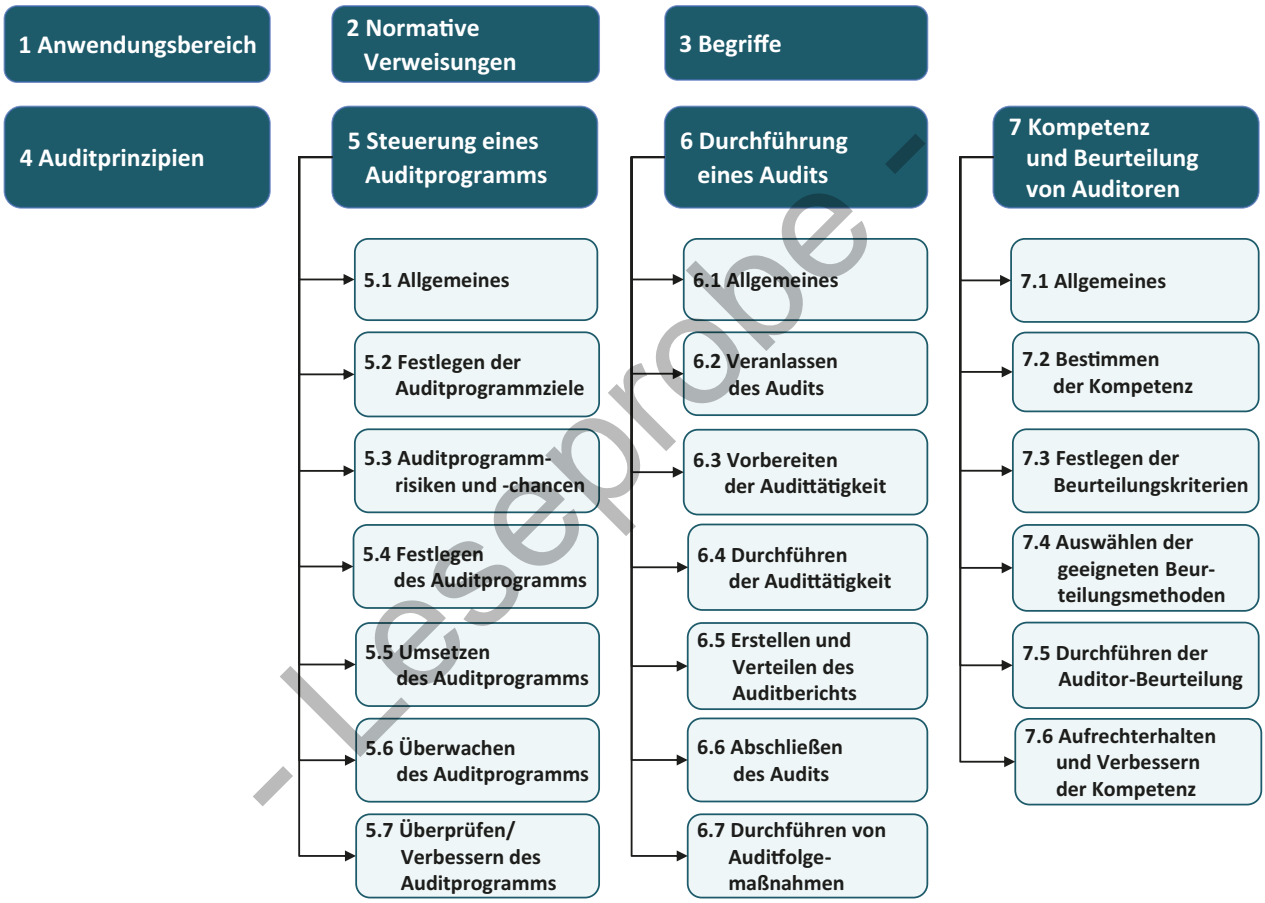


Abb. 1: Gliederung der ISO19011

Der Auditor

Das Normkapitel 4 „Auditprinzipien" beschreibt zum einen den Verhaltenskodex für den Auditor hinsichtlich der Qualität seiner Arbeit sowie die ethischen Anforderungen an seine Person und zum anderen die Grundlagen einer unabhängigen, dem Auditerfolg geschuldeten Auditdurchführung.

Auditplanung

Jede Tätigkeit, die von Erfolg gekrönt sein soll, setzt an ihren Anfang die Planung, als geistige Vorwegnahme zukünftigen Handelns, um Fehler zu vermeiden. Diesem Grundsatz folgt auch das Normkapitel 5 „Steuerung eines Auditprogramms". Zentrales Werkzeug der Planung eines Audits ist das Auditprogramm, das die Auditaktivitäten eines geplanten Zeitraums (z. B. ein Jahr) übersichtlich darstellt. Der zweite wesentliche Punkt im Normkapitel 5 ist die Analyse des Auditprozesses und des Auditprogramms mittels einer Chancen- und Risikobetrachtung, um deren Wirksamkeit abzusichern.

Auditdurchführung

Für die direkte Auditdurchführung enthält das Normkapitel 6 „Durchführung eines Audits“ die Hilfestellung für den Auditor und Auditteamleiter, die diese benötigen, um ein einzelnes Audit vor Ort wirksam zu planen und durchzuführen. In den Geltungsbereich dieses Normkapitels fällt auch die Vorbereitung auf ein Audit mit der Erstellung der Auditfrageliste und deren Anwendung in der Auditkommunikation.

Auditorkompetenz

Das letzte Normkapitel der ISO 19011 beschäftigt sich mit der Kompetenz von Auditoren und wie man diese erreichen und erhalten kann. Denn das Vertrauen in den Auditprozess und die Güte der Auditergebnisse hängt in wesentlichem Maße von der Kompetenz und der Eignung der eingesetzten Auditoren ab.

Neben den Ausführungen in den Normkapiteln 4 bis 7 bietet die ISO 19011 im Anhang A noch weitere nützliche Informationen vertiefend zum Normkapitel 6 „Durchführung eines Audits“ an. Gerade für Auditoren, die am Anfang ihrer Tätigkeit stehen, sind die Ausführungen in den Unterkapiteln des Anhangs A sehr hilfreich.

Weitere Informationen

Umfassende Informationen zur Vertiefung des Themas interne Audits finden Sie in der Fachbroschüre „Die ISO 19011 – Audits erfolgreich vorbereiten und durchführen“ [6].

3 Struktur der ISO/IEC 27001:2022

High Level Structure (HLS)

Die High Level Structure (HLS) wurde 2013 durch die ISO eingeführt, damit die Struktur von ISO-Managementsystemnormen, die Zertifizierungsgrundlage sind, einen einheitlichen Aufbau aufweisen. Mit der Revision der ISO 9001 im Jahr 2015 wurde die HLS auch für die weltweit am häufigsten zertifizierte Norm eingeführt. Weitere ISO-Normen, die als Zertifizierungsgrundlage dienen, folgten, so auch die ISO/IEC 27001:2013. Nach acht Jahren wurde die High Level Structure einer Revision unterzogen, um die wachsenden Anforderungen der Managementsysteme zur Harmonisierung weiter zu erfüllen. Im Mai 2021 wurde die neue Harmonized Structure (HS) von der ISO in Kraft gesetzt. Das bedeutet, dass ab diesem Zeitpunkt die neue HS für die Ausarbeitung neuer ISO-Managementsystemnormen und zukünftiger Überarbeitungen bestehender ISO-Managementsystemnormen Anwendung findet. Die Grundsätze der HLS bezüglich Harmonisierung von Zertifizierungsnormen werden auch in der HS beibehalten.

Neben einer einheitlichen Kapitelstruktur gibt die ISO mit identischen Textbausteinen, gemeinsamen Begriffen und Definitionen auch eine Harmonisierung der Sprache vor, die – wo immer möglich – den Kern von neuen und überarbeiteten Managementsystemnormen bilden soll und somit die Klarheit in der Aussage der Forderungen verbessert. Die einheitliche Kapitelstruktur ist von großem Vorteil bei der Zusammenführung von mehreren Managementsystemen zu einem integrierten System.

In der Kapitelstruktur hat es kleine, aber bemerkbare Änderungen gegeben. Die inhaltlichen Änderungen sind eher geringfügiger Natur und werden wohl nur von sehr normenaffinen Lesern bemerkt werden. Die Revision der ISO 27001:2022 ist die erste Norm, auf die die neue HS Anwendung findet. Welche wesentlichen Änderungen in der überarbeiteten ISO 27001 auf die HS zurückzuführen sind, wird nachfolgend erläutert.

Die Kapitelstruktur der ISO/IEC 27001 im Stand der Revision 2022 gibt Abbildung 2 wieder.

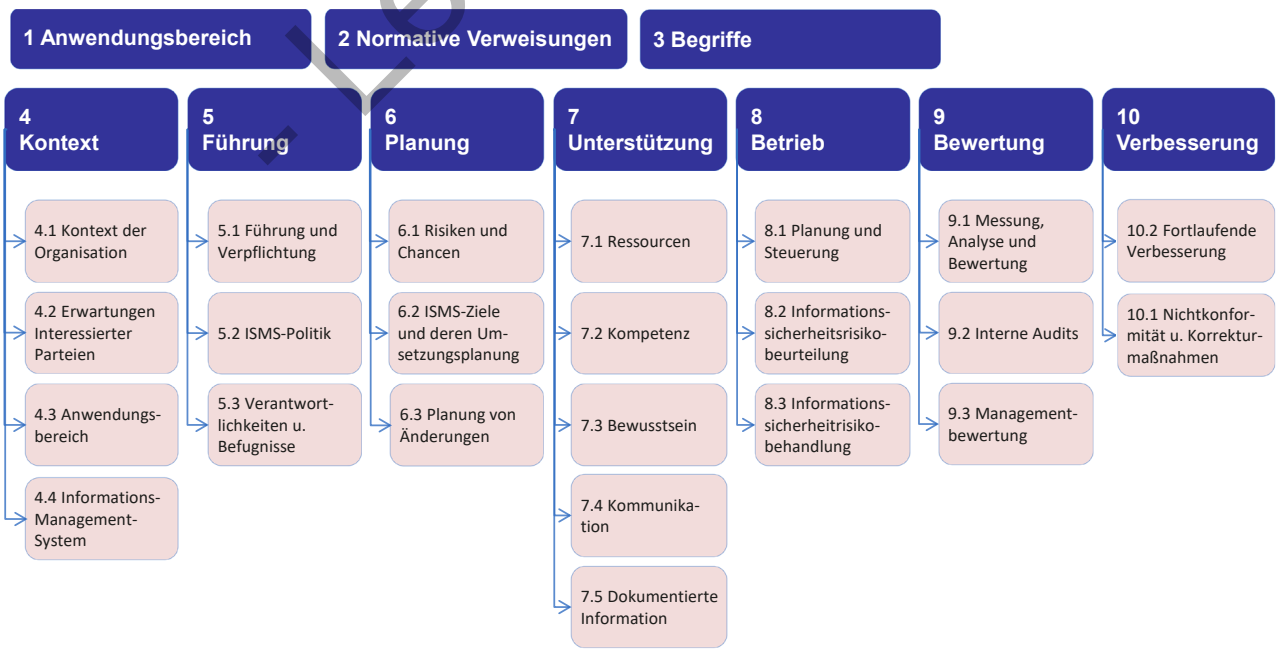


Abb. 2: HS-Struktur der ISO/IEC 27001

Risiken-Chancen-Bewertung

Das Normkapitel 4 und seine Unterkapitel bilden den Rahmen für das Informationsmanagementsystem (ISMS). Im Normkapitel 5 sind die Aufgaben

und die Verantwortung der Leitung für die Organisation und die Aufrechterhaltung sowie Wirksamkeit des ISMS niedergelegt. Das Normkapitel 6 enthält den planerischen Ansatz des Managementsystems. Die Bewertung von Risiken und Chancen soll es ermöglichen, Vorbeugemaßnahmen gezielt zu ergreifen, um negative Auswirkungen auf die Organisation zu verhindern und positive Auswirkungen zur Verbesserung zu nutzen. Ebenso dient die verbindliche Festlegung von Zielen und deren Umsetzung der Verbesserung des ISMS und seiner Prozesse.

Als neues Kapitel wird durch die HS das Normkapitel 6.3 „Planung von Änderungen" eingeführt. In der ISO 9001:2015 ist dieses Kapitel mit den gleichen Anforderungen bereits vorhanden. Es geht darum, dass Änderungen am bestehenden Managementsystem die Funktionsfähigkeit des Systems als solches nicht negativ beeinträchtigen dürfen.

Das Normkapitel 7 enthält Regelungen zur Bereitstellung der notwendigen Ressourcen, Personen und Mittel, die in einem ISMS als Erfolgsfaktor unabdingbar sind.

Umgang mit Fehlern

Das für das operative Geschäft einer Organisation wichtigste ist das Normkapitel 8. In ihm werden die Anforderungen an den Betrieb einer Organisation bezüglich der Planung und Steuerung der ISMS-Prozesse bis zur Informationssicherheitsrisikobeurteilung und Risikobehandlung vorgestellt. Zur Überwachung und Steuerung benötigen ein Managementsystem und seine Prozesse bestimmte Instrumente.

Das Normkapitel 9 stellt diese Instrumente zur Verfügung. In diesem Kapitel gibt es weitere strukturelle Neuerungen durch die Revision. Das Normkapitel 9.2 Internes Audit ist in zwei Unterkapitel untergliedert worden, die Normkapitel 9.2.1 „Allgemeines" und 9.2.2 „Programm des internen Audits". Ebenso ist das Normkapitel 9.3 „Managementbewertung" in folgende drei Unterkapitel aufgeteilt worden: Normkapitel 9.3.1 „Allgemeines", 9.3.2 „Eingaben für die Managementbewertung" und 9.3.3 „Managementbewertungsergebnisse". Inhaltlich hat es die Forderungen aus Normkapitel 9.2 und 9.3 auch schon in der alten Norm gegeben, aber sie waren aufgrund der fehlenden Unterkapitel nicht so klar strukturiert. Diese Form der Gliederung in Unterkapitel weist auch schon die ISO 9001:2015 auf.

Korrektur-Maßnahmen/ Verbesserung

Da Fehler und deren Folgen nie ganz auszuschließen sind, werden in Normkapitel 10 Forderungen zu Korrekturmaßnahmen von Fehlern und nach Instrumenten zur fortlaufenden Verbesserung gestellt. Auch dazu hat es durch die neue HS eine Veränderung gegeben. Die Reihenfolge der Normkapitel 10.1 „Nichtkonformitäten und Korrekturmaßnahmen" und 10.2 „Fortlaufende Verbesserung" ist vertauscht worden. Was auf den ersten Blick als nicht so wesentlich erscheint, ist normativ ein Paradigmenwechsel. Der Vermeidung von Fehlern durch aktive Vorbeugung wird eindeutig der Vorrang gegeben vor der Korrektur von Fehlern. Daher steht nun Normkapitel 10.1 „Fortlaufende Verbesserung" vor 10.2 „Nichtkonformität und Korrekturmaßnahmen". Daraus folgt für die Managementsysteme der Wechsel von einer Fehlerkultur, wie gut sie im Einzelnen auch immer sein mag, zu einer Vorbeugungskultur mit dem Ziel, Fehler zu vermeiden – womit auch ein neuer Auditschwerpunkt entstanden sein dürfte.

4 Besonderheiten des ISMS und Verbindungen zu anderen Managementsystemen

4.1 Allgemeines

Unternehmenswerte: Daten und Information

In der heutigen globalisierten Welt sind nicht mehr nur Betriebsmittel, Infrastruktur, Material und Waren Gegenstände, die den monetären Wert eines Unternehmens ausmachen. Software, IT-Dienstleistungen, Wissen und Informationen bestimmen heute häufig stärker den Wert eines Unternehmens. Die großen Technologiefirmen haben Börsenwerte, die die körperlichen Werte in der Bilanz um ein Vielfaches übertreffen. Auch der Erfolg eines Unternehmens hängt nicht mehr nur von der Qualität seiner Produkte, sondern in immer größeren Umfang von den zur Verfügung stehenden Daten und Informationen ab (z. B. Google). Die Mengen an nutzbaren Daten und die Möglichkeiten sowie die Geschwindigkeit ihrer Verarbeitung bestimmen immer häufiger den Markterfolg. Diese Werte zu schützen und zu mehren wird heute meist professionell durch das Assetmanagement betrieben. Die ISO/IEC 27001 leistet in diesem Kontext zur Sicherheit von Daten und IT-Systemen einen Beitrag.

Assets schützen

In der Praxis wird jede Information, unabhängig davon, ob es das gesprochene Wort, die schriftlich dokumentierte Information, Bilder und Filme oder Daten in IT-Systemen sind, als solche Information betrachtet. Wenn diese Unternehmensinterna Informationen enthalten, die dem Unternehmen Wettbewerbsvorteile verschaffen oder ggf. Wettbewerbsnachteile bedeuten können, sind es Werte (Assets), die ein Unternehmen schützen sollte. Schon die vorzeitige Information über einen geplanten Geschäftsabschluss bietet dem Wettbewerb die Möglichkeit, dieses Geschäft noch zu vereiteln. Daher ist es eine zentrale Aufgabe des ISMS, die Werte und Informationen zu erfassen (Inventarisieren), hinsichtlich ihrer Bedeutung zu klassifizieren und den Umgang mit ihnen festzulegen.

Integriertes Managementsystem

Die ISO/IEC 27001 ist in der Regel nicht die einzige zertifizierbare Managementsystemnorm in einer Organisation. In der Praxis ist sie häufig in Verbindung mit der ISO 9001 (Qualitätsmanagementsystem), der ISO 14001 (Umweltmanagementsystem) und anderen ISO-Normen in Form eines Integrierten Managementsystems (IMS) zu finden. Die Anforderungen des ISMS sind dann in einer gemeinsamen Systemdokumentation dargelegt. Die Zuordnung der ISMS-Forderungen zu den einzelnen Kapiteln eines IMS ist dank der High Level Structure (HLS) mittels gemeinsamer Kapitelstruktur ohne Schwierigkeiten möglich. Die Auditierung erfolgt dann im Kontext der anderen Managementsysteme.

Die Themen aus Anhang A bilden neben den normativen Forderungen der Normkapitel 4 bis 10 den Rahmen, der Gegenstand eines internen Audits für das ISMS ist. Die Themen in Anhang A werden dabei im Kontext der zutreffenden Normenkapitel mit auditiert. In einem IMS erfüllen die Forderungen der ISO/IEC 27001 eine Querschnittsfunktion in allen Prozessen. Es gibt keinen Managementsystemprozess, der ohne Informationen und Daten auskommt, daher ist die Sicherheit dieser Informationen und Daten auch in einem IMS allgegenwärtig.

4.2 Revision 2022 der ISO/IEC 27001, inhaltliche Änderungen

Die internationale Norm ISO/IEC 27001 bildet die Grundlage für ein Informationssicherheitsmanagementsystem. In den neun Jahren ihrer Anwendung in der Praxis ist die Bedeutung der Norm stetig gestiegen. 2021 lag sie weltweit schon auf Platz 4, wenn auch mit größerem Abstand zum drittplatzierten der zertifizierten Managementsysteme [7]. Auf den Plätze 1 bis 3 liegen die ISO 9001 (Qualitätsmanagement), die ISO 14001 (Umweltmanagement) und

die ISO 45001 (Arbeits- und Gesundheitsmanagement). Weltweit besitzen schon knapp 60.000 Unternehmen eine Zertifizierung nach ISO/IEC 27001. In Deutschland sind es immerhin schon ca. 1.300 Zertifizierungen. Damit ist bewiesen, dass das Thema Informationssicherheit für viele Unternehmen an Bedeutung gewinnt.

Cybersicherheit

Nach neun Jahren ist die ISO/IEC 27001:2013 einer Revision unterzogen worden. Im Oktober 2022 trat die erneuerte Norm in Kraft, und diese wird nach einer Übergangszeit (18 Monate nach Veröffentlichung) die alte Norm als Zertifizierungsgrundlage ersetzen. Eines ist heute schon sicher: Die Bedeutung dieser Norm wird weiter zunehmen, da elektronische Daten einschließlich ihrer Speicherung und Verarbeitung und ihres Transports die Lebensader vieler Organisationen sind. Ohne entsprechende Sicherheit ist unsere vernetzte Welt sehr verletzlich gegenüber Hackerangriffen und Datenspionage von außen. Regierungen, Organisationen und Unternehmen können ins Wanken geraten, wenn ihre Daten in falsche Hände geraten oder der Datentransfer gestört wird. Daher hat die Revision dem Thema Cybersicherheit besondere Aufmerksamkeit geschenkt. Dies geht auch schon aus dem neuen Titel „Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre" hervor (alt: Informationstechnik – IT-Sicherheitsverfahren). Die zweite inhaltliche Erweiterung der Revision betrifft das Thema des Datenschutzes, der aus guten Gründen weltweit immer stärker gesetzlichen Regulierungen unterliegt.

Für die Anwender und alle, die es in absehbarer Zeit werden wollen, stellt sich nun die Frage, was durch die Revision anders geworden ist. Auf die strukturellen Änderungen der ISO 27001:2022 aufgrund der neuen HS ist im Abschnitt 3 bereits eingegangen worden. Somit bleiben die inhaltlichen Änderungen, die auch auditrelevant sein können. Betrachtet man die operativen Normenkapitel 4 bis 10, zeigen sich zwar inhaltliche Änderungen, diese erweisen sich aber als relativ moderat. Deutlich verändert hat sich der Normanhang A. Dieser Anhang wirkt sich direkt auf die Forderung nach Normkapitel 6.1.3 c aus, die da lautet: „die nach 6.1.3 b) festgelegten Maßnahmen sind mit den Maßnahmen in Anhang A.1 zu vergleichen und zu überprüfen, so dass keine erforderlichen Maßnahmen ausgelassen wurden".

Wesentliche inhaltliche Änderungen

Nachfolgend finden Sie in Kürze die wesentlichen inhaltlichen Änderungen in den Normkapiteln 4 bis 10 der ISO 27001:2022. Die bedeutendste Änderung betrifft Normkapitel 4.4 „Informationssicherheitsmanagementsystem" mit der Forderung, die erforderlichen Prozesse und Wechselwirkungen des ISMS zu bestimmen. Damit folgt die ISO 27001 der Prozessorientierung der ISO 9001 und anderer ISO-Managementsysteme.

Eine weitere bedeutsame Änderung ist Normkapitel 6.3 „Planung von Änderungen", das neu hinzugekommen ist. Es besagt: Wenn Änderungen im oder am ISMS notwendig werden sollten, sind diese Änderungen planmäßig durchzuführen. Diese Forderung findet sich gleichlautend auch schon in der ISO 9001; sie ist daher auch nicht wirklich neu, muss jetzt aber auch im ISMS berücksichtigt werden.

An dritter Stelle kommen zwei Forderungen in Normkapitel 8.1 „Betriebliche Planung und Steuerung". In Ergänzung zur Prozessorientierung in Normkapitel 4.4 kommt zum einen die Forderung hinzu, dass es für die Prozesse des ISMS Kriterien geben muss, die zur Prozesssteuerung/Prozessüberwachung herangezogen werden können. Die andere Forderung in diesem Kapitel bezieht sich auf die Beschaffung. Die Organisation muss sicherstellen, dass neben extern bereitgestellten Prozessen auch Produkte und Dienstleistungen mit Relevanz für das ISMS kontrolliert werden, was in der Umsetzung auf eine Überprüfung der Lieferantenleistung vergleichbar mit der ISO 9001, 8.2.3 „Überprüfung der Anforderungen für Produkte und Dienstleistungen", hinausläuft.

An vierter Stelle kommt in Normkapitel 9.1 „Überwachung, Messung, Analyse und Bewertung" die Anforderung zur Bewertung der Informationssicherheitsleistung und der Wirksamkeit des ISMS als Regelaufgabe des ISMS-Controllings hinzu. Die Organisation muss die Informationssicherheitsleistung und die Wirksamkeit des Informationssicherheitsmanagementsystems bewerten.

Des Weiteren gibt es noch fünf kleinere Änderungen oder Ergänzungen in den folgenden Kapiteln:

4.2 „Verstehen der Erfordernisse und Erwartungen interessierter Parteien"

5.3 „Rollen, Verantwortlichkeiten und Befugnisse"

6.2 „Informationssicherheitsziele und Planung zu deren Erreichung"

7.4 „Kommunikation"

9.3 „Managementbewertung"

In der beigefügten Arbeitshilfe sind alle Änderungen der Normkapitel 4 bis 10 der ISO/IEC 27001:2022 im Vergleich zur DIN EN ISO/IEC 27001:2015 in Form einer Verweismatrix zusammengefasst.

Änderungen_Normkapitel.xlsx

Neue Struktur im Normanhang A

Wie bereits erwähnt, ist die Tabelle im Normanhang A im Rahmen der Revision von Grund auf neu strukturiert worden, und keine der bisherigen 114 Sicherheitsmaßnahmen ist unverändert übernommen worden. Auch die Bedeutung für das ISMS hat sich etwas verschoben. Während in der alten Norm noch von einer **umfassenden** Liste von Maßnahmenzielen die Rede ist, ist in der neuen Norm nur noch die Rede von einer **möglichen** Liste von Maßnahmenzielen. Dies bedeutet den Verzicht auf einen Anspruch auf Vollständigkeit von Maßnahmenzielen, die auf eine Organisation anzuwenden sind. Welche Maßnahmenziele explizit für sie gelten, muss die Organisation über ihre Informationssicherheitsrisikobeurteilung (Normkapitel 6.1.2) und ihre Informationssicherheitsbehandlung (Normkapitel 6.1.3) selbst ermitteln. Der Normanhang A.1 dient nur noch dem Vergleich, um zu prüfen, ob das Unternehmen auch alle für ihn wesentlichen Informationssicherheitsmaßnahmen identifiziert hat. Im speziellen Unternehmensfall kann es auch Informationssicherheitsmaßnahmen geben, die nicht im Anhang A.1 gelistet sind.

Was sind die wesentlichen Änderungen des Normanhangs A.1 Die alte ISO/IEC 27001:2013 hatte 14 Themenbereiche (Nr. 5 bis 18), die in 114 einzelne Sicherheitsmaßnahmen unterteilt waren. Die neue ISO/IEC 27001:2022 umfasst nur noch vier Themenbereiche (Nr. 5 bis 8) mit insgesamt 93 Sicherheitsmaßnahmen.

Neue Themenbereiche

Diese vier neuen Themenbereiche sind:

Titel	Sicherheitsmaßnahmen
5 Organisatorische Maßnahmen	37
6 Personelle Maßnahmen	8
7 Physische Maßnahmen	14
8 Technologische Maßnahmen	34

In Summe sind elf neue Sicherheitsmaßnahmen eingeführt worden. Eine Sicherheitsmaßnahme wurde nicht in den neuen Normanhang A übernommen (alt: A.11.2.5 Entfernen von Werten). In Tabelle 2 sind die elf neu hinzugekommenen Sicherheitsmaßnahmen aufgelistet.

sechs Schritte und deren Reihenfolge sollte jeder Auditor immer im Gedächtnis haben, wenn er auditiert.

Abfolge von Auditfragen

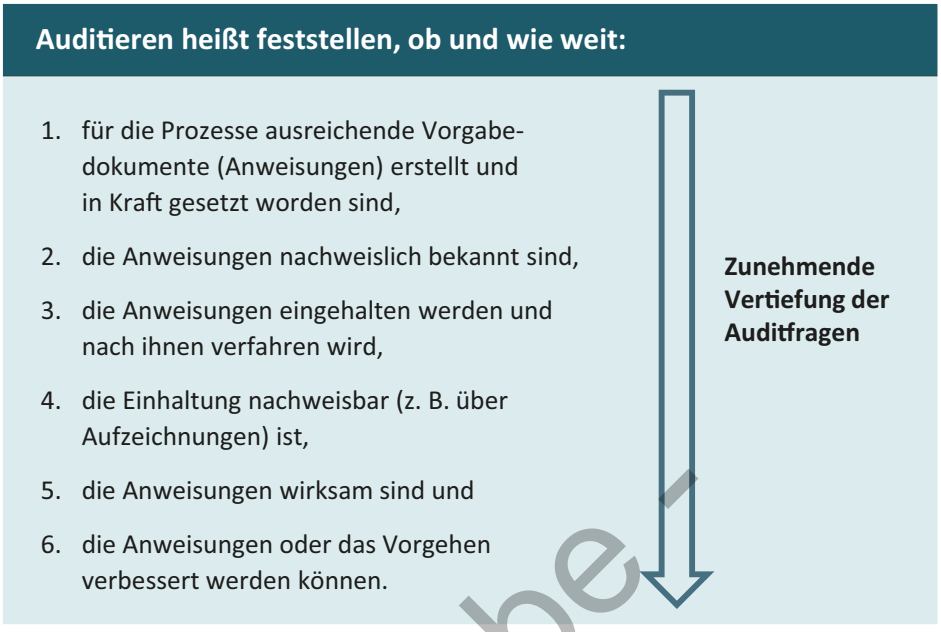


Abb. 10: Ablauf Auditkernfrage und Folgefragen

Nicht alle Auditfolgefragen befinden sich immer in der Auditfrageliste, da deren Umfang dann einfach zu lang werden würde. Meist begnügt man sich im Fragenkatalog mit der Auditkernfrage und leitet alle weiteren Fragen nach dem vorgestellten Schema daraus ab.

8 Quellen

[1] DIN EN ISO 9000:2015 – Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2015)

[2] DIN EN ISO 19011:2018 – Leitfaden zur Auditierung von Managementsystemen (ISO 19011:2018)

[3] DIN EN ISO/IEC 17021-1:2015 – Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren (ISO/IEC 17021-1:2015)

[4] ISO/IEC 27001:2022 – Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2022); (Anmerkung der Redaktion: Zum Zeitpunkt der Bearbeitung lag nur die englische Version der ISO/IEC 27001:2022 vor. Die für diesen Beitrag notwendigen Übersetzungen ins Deutsche können ggf. von der späteren offiziellen deutschen Übersetzung der DIN im Einzelfall abweichen.)

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

[6] Kallmeyer, Wolfgang: Die ISO 19011 – Audits erfolgreich vorbereiten und durchführen. www.tuev-media.de/die-iso-19011:2018

[7] ISO Survey 2021: www.iso.org/the-iso-survey.html

[8] DIN EN ISO/IEC 27002:2022 – Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

Anhang: Auditfragen zur ISO/IEC 27001

Hinweise zur Verwendung des Fragenkatalogs

Ergänzend zu dieser Broschüre ist eine Frageliste erstellt worden auf der Basis einer Textanalyse der Informationssicherheitsmanagementsystemnorm ISO/IEC 27001:2022. Der Aufbau der Frageliste orientiert sich an der Kapitelstruktur der ISO/IEC 27001. Von Normkapitel 4 „Kontext der Organisation" bis zu Normkapitel 10 „Verbesserung" ist zu jedem Kapitel eine Reihe von Fragen aus den Normforderung abgeleitet worden, um die regelkonforme Umsetzung der ISO/IEC 27001:2022 zu überprüfen. Die Auditkommunikation sollte sich aber nicht nur auf diese Fragen beschränken, sondern die Fragen sollten als Einstiegshilfe dienen, um mit weiteren Fragen den Kontext zum gewählten Auditthema weiter zu untersuchen. Erst wenn klar ist, ob die Anforderungen der Norm erfüllt sind oder nicht, kann eine fundierte Auditfeststellung, mit dem Ergebnis „konform" mit oder ohne Verbesserungspotenzial oder „nichtkonform", getroffen werden.

Nachweisbeispiele

Neben den Auditfragen enthält der Fragenkatalog noch eine Auswahl an Nachweisbeispielen zu jeder Auditfrage, die zur Feststellung des Sachverhalts, der sich aus der Auditfrage ergibt, herangezogen werden können. So kann auf die Auditfrage „Wie ist das Vorgehen zur Durchführung interner Informationssicherheitsaudits geregelt?" als Festlegung eine bestehende Prozessbeschreibung herangezogen werden. Dann gilt es zu prüfen, ob die Prozessbeschreibung hinsichtlich ihrer Regelungsinhalte die Erfüllung der Normenforderungen in Gänze widerspiegelt. Die angegebenen Nachweisbeispiele sind auf der Basis einer vieljährigen Auditorenpraxis zusammengestellt, erheben aber nicht den Anspruch, in jedem betrieblichen Einzelfall vollständig oder zutreffend zu sein.

Ergänzen und Anpassen

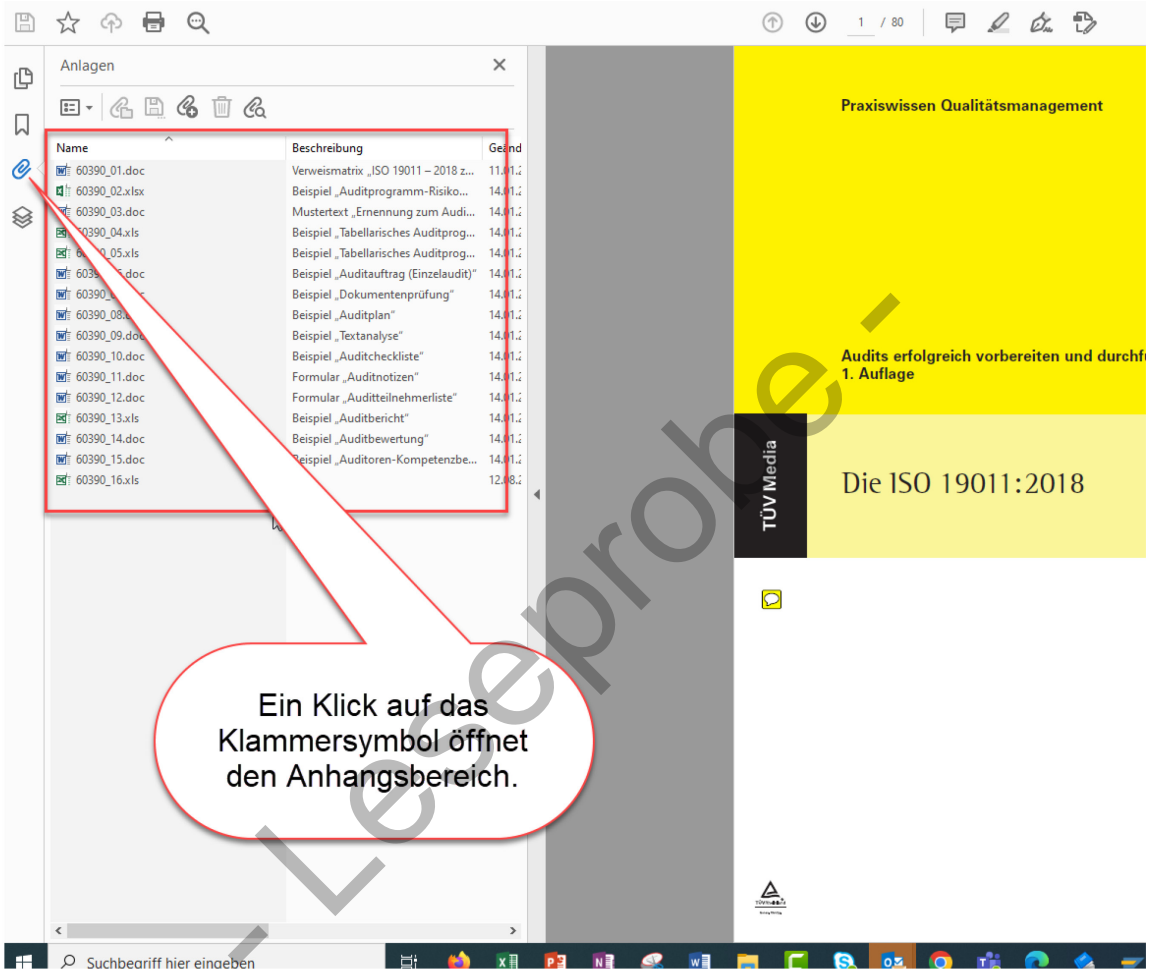
Vor Einsatz der Auditfrageliste sollte geprüft werden, ob die Auditfragen oder die Nachweisbeispiele für das Unternehmen zutreffend sind. Gegebenenfalls sind Ergänzungen und Anpassungen vorzunehmen. Der Fragenkatalog kann auch als Basis genutzt werden, um einen betriebsinternen erweiterten Fragenkatalog zu entwickeln, der mit der Auditerfahrung wächst. Dieser Fragenpool bildet dann die Grundlage für die Auswahl von individuellen Auditfragen passend für die Zielstellung des jeweiligen Einzelaudits.

Fragen zu Kern- und Unterstützungsprozessen ergänzen!

Der aus der Textanalyse und der betrieblichen Erfahrung abgeleitete Fragenkatalog enthält noch nicht die Fragen, die sich aus den Unternehmensprozessen und deren Wechselwirkung selbst ergeben. Es ist daher empfehlenswert, für die Kernprozesse und die wesentlichen Unterstützungsprozesse eine Turtle-Analyse durchzuführen (s. Abschnitt 5.4). Aus dieser Analyse lassen sich ergänzend weitere Auditfragen generieren, die dann den Normenkapiteln 4 bis 10 und ihren Unterkapiteln zugeordnet werden können. Der so erweiterte Fragenkatalog deckt dann zunehmend die Möglichkeiten bezüglich eines umfassenden internen Audits ab und kann als Einstiegshilfe und Schulungsunterlage für die Ausbildung neuer Auditoren genutzt werden.

Hinweise zum Öffnen der Datei-Anhänge

Die Arbeitshilfen sind im E-Book als Anhang eingebunden. Zum Lesen des E-Books und zum Öffnen der Anhänge empfehlen wir Ihnen ausschließlich den Acrobat Reader von Adobe.
Ein Klick auf das Klammersymbol wie auch der Klick auf die Dateinamen und -symbole im Text des E-Books öffnen den Anhangsbereich links neben dem Lesebereich:



Anzeige des E-Books in PDF-Viewern anderer Hersteller

Die Datei-Anhänge werden in den PDF-Viewern anderer Hersteller häufig auf andere Weise dargestellt. Hier müssen Sie im Zweifel prüfen, ob und wie Sie sich die Anhänge anzeigen lassen können.

Anzeige des E-Books im Browser

! Wenn Sie das E-Book aus Browsern wie z. B. Safari, Edge, Chrome oder Firefox heraus aufrufen, bieten die darin eingebundenen Viewer häufig keine Möglichkeit, die Datei-Anhänge anzuzeigen. In diesen Fällen laden Sie das E-Book bitte lokal auf Ihr Gerät herunter und öffnen es direkt aus einem installierten PDF-Viewer heraus.