Fragen finden und im internen Audit richtig einsetzen
1. Auflage

TÜV Media

Der Auditfragenkatalog zur ISO/IEC 27001

TÜVRheinland
Genau. Richtig.

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 978-3-7406-0708-1 (Print)
ISBN 978-3-7406-0709-8 (E-Book)

Zur Nutzung der Broschüre

Zielsetzung der Broschüre

Interne Systemaudits gehören zum Alltag für alle Organisationen, die ein zertifiziertes Managementsystem unterhalten. 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, 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:

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 27001:2015 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:

www.tuev-media.de/download/[redacted]

Passwort: [redacted]

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 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- und IT-Sicherheit 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.

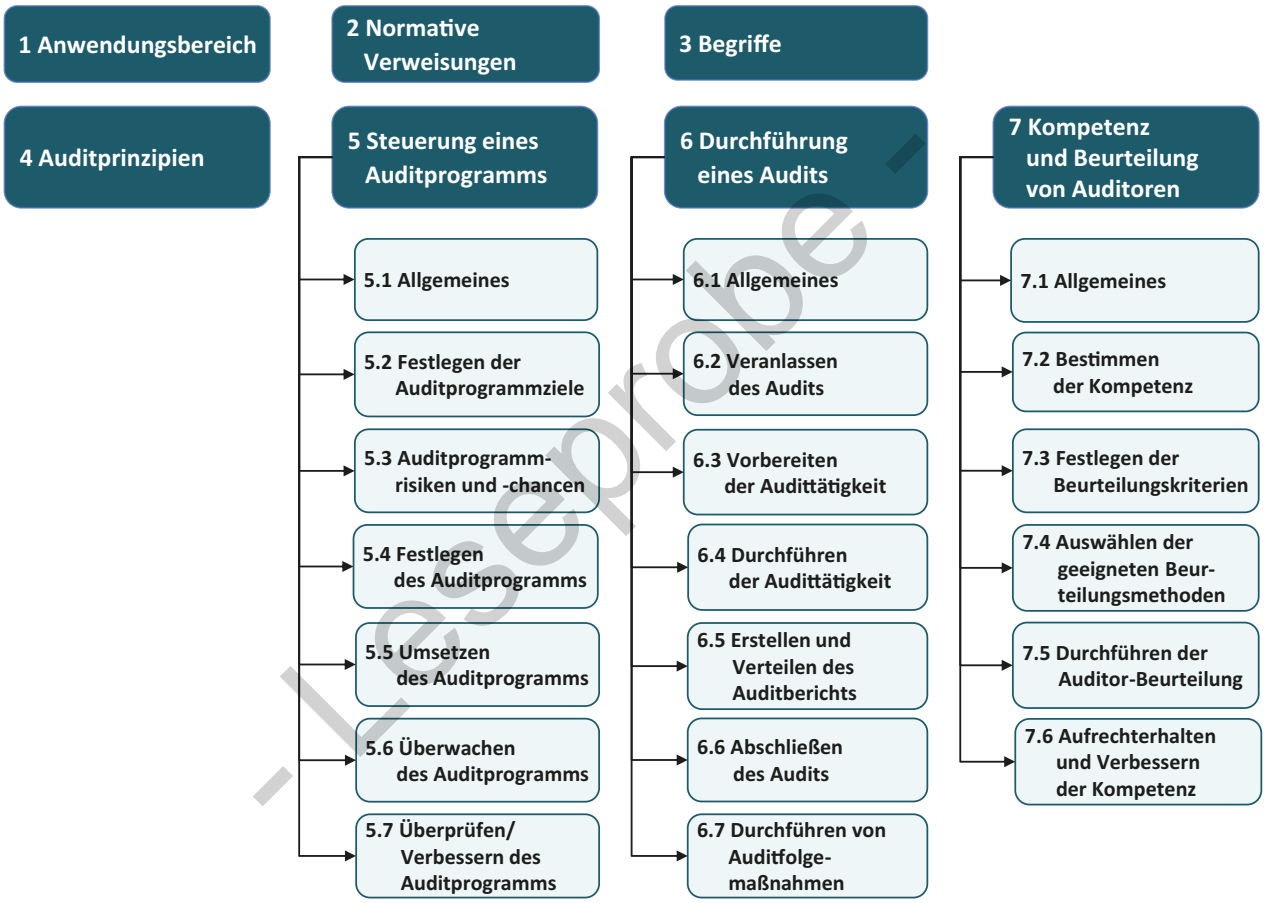

Abb. 1: Gliederung der ISO19011

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“ [5].

3 Struktur der ISO/IEC 27001

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, folgen heute dieser Struktur, so auch die ISO/IEC 27001.

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.

Die Kapitelstruktur der ISO/IEC 27001 gibt Abbildung 2 wieder.

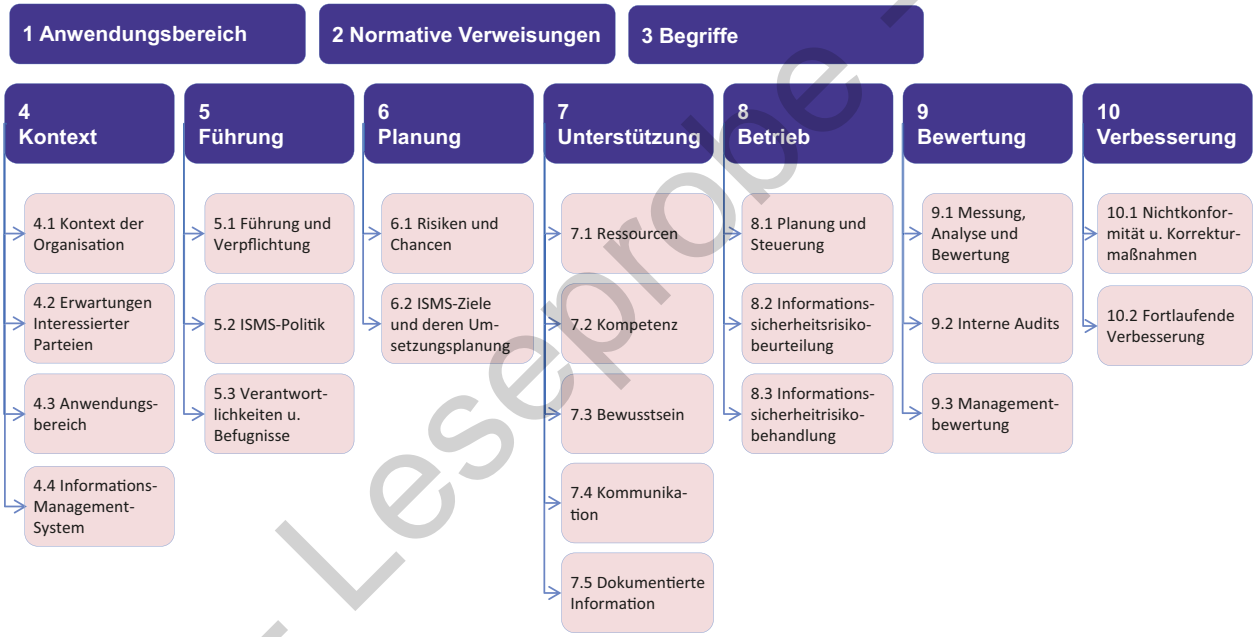

Abb. 2: HLS-Struktur der ISO/IEC 27001

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. 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. Da Fehler und deren Folgen nie ganz auszuschließen sind, werden in Normkapitel 10 Forderungen zu Korrekturmaßnahmen von Fehlern aufgestellt. Neben Anleitungen zur Beseitigung von Fehlern enthält dieses Kapitel aber auch die Forderung nach Instrumenten zur fortlaufenden Verbesserung.

4 Besonderheiten des ISMS und Verbindungen zu anderen Managementsystemen

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.

Maßnahmen nach Anhang A

Zu welchen operativen Themen ein Unternehmen ISMS-Maßnahmen und Regelungen einführen und aufrechterhalten muss, ist im normativen Anhang A beispielhaft aufgeführt. Welche Themen dies sind und wie diese den Normenkapitel 4 bis 10 zuzuordnen sind, zeigt Tabelle 2.

Tabelle 2: Zuordnung Themen Anhang A zu Normkapiteln

Themen aus Anhang A		Normen-kapitel
A.5	Vorgaben der Leitung zur Informationssicherheit	5.1
A.6	Organisation (Aufbau- und Ablauforganisation) zur Informationssicherheit (intern und extern)	5.3
A.7	Informationssicherheitskriterien für das Personal	8.1
A.8	Verwaltung der Informationssicherheitswerte (Asset-Management),	8.1
A.9	Zugangs- und Berechtigungssteuerung zu Informationen und IT-Systemen	8.1
A.10	Verschlüsselung von Informationen (Kryptografie)	8.1
A. 11	Physische und umgebungsbezogene Sicherheitsvorgaben	8.1
A.12	Betriebs- und Datensicherheit	8.1
A.13	Kommunikations- und Netzwerksicherheitsmanagement	8.1
A.14	Beschaffung, Entwicklung und Installation von IT/DV-Systemen	8.1
A.15	Beziehungen zu Lieferanten und Dienstleistern	8.1
A.16	Handhabung von Informationssicherheitsvorfällen	8.1
A.17	Informationssicherheitsaspekte beim Business Continuity Management	8.1
A.18	Compliance- und vertragliche Anforderungen	9.1

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.

5 Methoden zur Generierung von Auditfragen

5.1 Allgemeines

Vorbereitung

Eine gute Vorbereitung ist unabdingbar für die Durchführung eines erfolgreichen Audits. Man kann aber schnell zu viel des Guten tun, und dann stehen Aufwand und Nutzen nicht mehr im rechten Verhältnis. Dies passiert häufig neuen Auditoren bei der Vorbereitung der Auditfrageliste.

Auditfrageliste

Die Auditfrageliste ist das wichtigste Arbeitsdokument für den Auditor. Die Frageliste soll dem Auditor als Leitfaden dienen. Sie sollte nicht so umfassend sein, dass der Auditor sich darin verstrickt. Das erhöht nur die Vorbereitungszeit, verbessert aber nicht die Qualität des Audits, weil die meisten Fragen überhaupt nicht gestellt werden. Trotzdem muss auch unter Zeitgesichtspunkten nach relevanten Details gefragt werden, die nötig sind, um den Auditumfang angemessen abzudecken.

Element zur Strukturierung des Audits

Da Managementsystemnormen, wie auch die ISO/IEC 27001, hinsichtlich der Themenfülle sehr umfangreich sind, ist eine strukturierte Frageliste hilfreich. Das heißt jedoch nicht, dass sie als Abfrageliste verstanden werden soll, sondern als Element zur Strukturierung eines Audits. Sie spiegelt wider, wie wichtig ein Auditor das Audit nimmt, und hinterlässt somit einen positiven Eindruck bei den Auditierten. Eine angemessene Vorbereitungszeit zahlt sich daher aus, da das Audit durch den Fragenkatalog einen roten Faden hat, der den Auditor zum Ziel lenkt.

Erfahrene Auditoren formulieren die Auditfragen im Sinne einer Aufwandsminimierung aber nicht mehr vollständig aus, sondern begnügen sich mit Stichworten, anhand deren man das Audit durchführt.

Leitfaden

Die Frageliste dient dem Auditor als Leitfaden, sie umfasst aber nicht die gesamte Auditkommunikation.

In den Normen finden wir keine konkreten Hinweise darauf, wie eine solche Frageliste zu erstellen ist und was deren Inhalte sein sollen. Für das Erstellen muss der Auditor entscheiden, welche Quellen er für seine Fragen benutzen möchte. Neben den Normen und rechtlichen Vorgaben können noch weitere wichtige Quellen herangezogen werden (siehe Abb. 3).

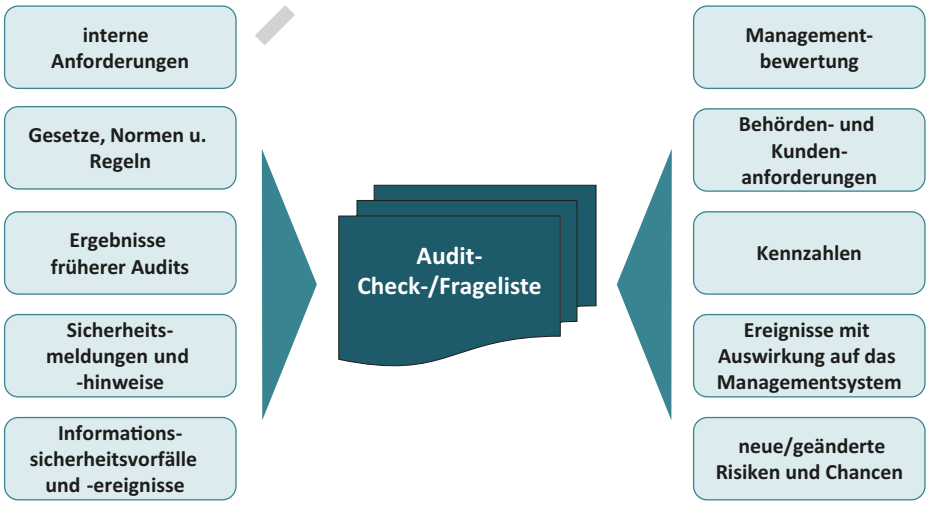

Abb. 3: Informationsquellen für Auditfragen

Letztes Audit nicht vergessen!

So sollten bei der Erstellung der Frageliste ebenso die Ergebnisse früherer Audits berücksichtigt werden. Jeder gute Auditor verifiziert, ob Abweichungen des letzten Audits oder angenommene Verbesserungsvorschläge

auch dauerhaft wirksam umgesetzt worden sind. Auch wie mit festgelegten Maßnahmen aus dem letzten Management-Review verfahren worden ist, gehört zu den möglichen Auditfragestellungen. Weitere Fragestellungen zur Informationssicherheit können sich ergeben aus:

- der Prozessleistungsbewertung durch Kennzahlen sowie der Kontrolle der Einhaltung von Sicherheitsvorgaben,
- neuen Kundenanforderungen, z. B. aufgrund neuer Sicherheitsprozeduren oder technischer Innovationen,
- neuen rechtlichen Anforderungen, z. B. infolge veränderter gesetzlicher Vorgaben (z. B. DSGVO),
- internen Anforderungen, z. B. aus geänderten oder neuen Prozessen und IT-Strukturen,
- aktuellen Sicherheitsproblemen in Prozessen oder IT-Systemen,
- weiteren Themenstellungen zu wesentlichen betrieblichen oder branchenbezogenen Ereignissen.

Gesamtheitlichkeit

Die Quellen, aus denen sich Auditfragen ergeben können, sind vielfältiger Natur. Ein ISMS ist für ein Unternehmen in der Regel mehr als nur die Umsetzung von Normenforderungen. Es ist die Festlegung aller betrieblichen Abläufe und Verantwortlichkeiten zum Thema Informationssicherheit.

Methoden

Um Auditfragen herzuleiten, sind heute zwei Methoden gebräuchlich. Dies ist zum einen die Textanalyse der Norm und zum anderen die Prozessanalyse mittels eines Turtle-Diagramms. Wir müssen uns aber nicht zwingend für ein Verfahren entscheiden; es können auch beide Verfahren kombiniert verwendet werden. Im Folgenden werden Ihnen beide Methoden vorstellt.

5.2 Textanalyse der Norm

Analyse der Normforderungen

In der Textanalyse werden die Auditfragen aus den Forderungen der Norm, z. B. der DIN EN ISO/IEC 27001 und ihrer Umsetzung in die betriebliche Praxis, entwickelt. In den folgenden vier Schritten kann daraus eine Frageliste erstellt werden:

Planungsschritte

1. Textanalyse, d. h., die Norm wird abschnittsweise gelesen und die darin enthaltenen Anforderungen werden je Textzeile markiert.
2. Aus diesen Anforderungen (z. B.: „muss festgelegt, muss durchgeführt, muss erstellt werden", ...) wird eine Maßnahme für den Aufbau des ISMS abgeleitet. Aus den Anforderungen entstehen Kernfragen (z. B. „Gibt es einen Auditplan? Wie ist festgelegt, dass ...?").
3. Aus den ISM-Maßnahmen, insbesondere aus den Vorgabedokumenten des aufgebauten ISMS, entstehen weitere Kernfragen.
4. Aus den Kernfragen werden detaillierte Fragen unter Berücksichtigung des Personals, der Organisationseinheiten oder Tätigkeiten des Unternehmens ausformuliert und in einer Auditfrageliste zusammengefasst und strukturiert.

Diese Planungsschritte zeigen, dass die einzelnen Anforderungen der Norm die Grundlage für die Erstellung einer Frageliste für ein Systemaudit bilden. Die Frageliste muss sowohl die Anforderungen der Norm als auch die daraus resultierenden unternehmensspezifischen ISM-Maßnahmen berücksichtigen.

Schematisch lässt sich die Erstellung einer Frageliste darstellen wie in Abbildung 4 gezeigt.

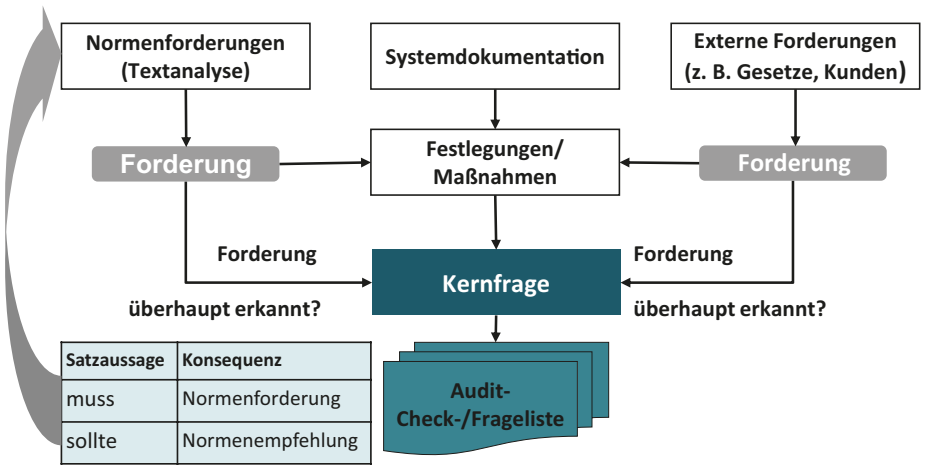

Abb. 4: Herleitung von Auditfragen – Textanalyse (1)

Regelwerksforderungen

Aus den Forderungen der Regelwerke (Normen, Gesetze) lassen sich dann detaillierte Fragen ableiten, indem man überprüft, ob die Regelwerksforderung in der ISM-Systemdokumentation berücksichtigt ist. In einem guten ISMS sollte dies der Fall sein. Dann ist zu hinterfragen, ob die Umsetzung am Arbeitsplatz so erfolgt, wie es die Vorgaben der Systemdokumentation vorsehen. Ein guter Auditor sollte dabei auch überprüfen, ob es eine hinreichende Nachweisführung gibt.

Zwei Beispiele für abgeleitete Auditfragen aus der ISO/IEC 27001 sind Abbildung 5 zu entnehmen.

Aus Normenforderung	**Aus ISMS-System** Inhalt von Anweisungen/ Anordnungen	**Auditfrage**
Welches sind die geforderten/empfohlenen einzelnen Anforderungen?	Welches Verfahren oder welche Methode wird angewendet?	Wie wird der Sachverhalt in der Umsetzung sichergestellt?
Beispiele zur Herleitung von Auditfragen aus der Textanalyse		
Beispiel 1 Informationssicherheitsziele und Planung zu deren Erreichung (Kap. 6.2)	Verfahren zur Zieledefinition und Umsetzungsplanung der Ziele	Wie werden Ziele zum ISMS festgelegt und deren Umsetzung abgesichert?
Beispiel 2 Informationssicherheitsrisikobehandlung (Kap. 8.3)	Plan zur Informationssicherheitsrisikobehandlung und Nachweisführung	Wie ist das Vorgehen bei der Informationssicherheitsrisikobehandlung, und wie lässt es sich nachweisen?

Abb. 5: Herleitung von Auditfragen – Textanalyse (2)

Fragelisten zur Durchführung von Audits entstehen aus der Analyse der Anforderungen der entsprechenden Regelwerke (Normen, Gesetze, etc.) und den betriebsinternen Vorgabedokumenten.

5.3 Frageliste zur ISO/IEC 27001

Fragenkatalog_ 27001.docx

Eine mittels Textanalyse der ISO/IEC 27001 entwickelte Frageliste für das interne Systemaudit ist zur weiteren Nutzung beigefügt. Im Anhang 1 dieser Broschüre ist Sie zudem vollständig abgedruckt. Der Aufbau der Frageliste orientiert sich an der Kapitelstruktur der ISO/IEC 27001. 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. Die Liste ist noch um spezifische das Unternehmen betreffende Auditfragen oder Nachweisbeispiele zu ergänzen.

Um die sich aus den Kernprozesse und den wesentlichen Unterstützungsprozessen ergebenden Wechselwirkung zu berücksichtigen, bietet es sich an weitere Auditfragen mittels ein Turtle-Analyse (s. Abschnitt 5.4) zu generieren und im Fragenkatalog zu integrieren. 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.

5.4 Turtle-Methode

Wechselwirkungen zwischen Prozessen analysieren

Neben der Textanalyse von Normen wird in der Praxis eine zweite systematische Möglichkeit zur Generierung von Auditfragen genutzt, die Turtle-Methode. Die ISO 9001 (Normkapitel 0.3) definiert den prozessorientierten Ansatz, d. h., die Prozesse einer Organisation bilden ein Netzwerk, in dem die einzelnen Prozesse untereinander interagieren. Dieser prozessorientierte Ansatz ist im Grundsatz auf alle ISO-Managementsysteme übertragbar, auch auf die ISO/IEC 27001.

Managementsysteme als Prozesslandschaft

Heutige Managementsysteme, insbesondere integrierte Systeme (IMS), sind in der Regel prozessbezogen aufgebaut, weil so die Wechselwirkungen der Wertschöpfungsprozesse untereinander wie auch mit den Unterstützungs- und Führungsprozessen berücksichtigt werden können. Im Rahmen einer Textanalyse werden die Normenforderungen zwar vollständig erfasst, aber die Wechselwirkung der Forderungen in den Prozessen bleibt unberücksichtigt, das bedeutet z. B., die Lenkung dokumentierter Information als Unterstützungsprozess findet in fast allen Prozessen der Organisation statt. Die Anforderungen an die Lenkung finden sich in der ISO/IEC 27001 aber nur im Normkapitel 7.5. Es gibt eine ganze Reihe von Prozessen in ISO-basierten Managementsystemen, die solche übergreifenden Querschnittsfunktionen für die anderen Prozesse haben. Zu nennen sind für die ISO/IEC 27001 z. B.:

- Risiken und Chancen – Allgemeines (Normkapitel 6.1.1)
- Dokumentierte Information (Normkapitel 7.5)
- Kompetenz (Normkapitel 7.2)
- Interne Audits (Normkapitel 9.2)
- Nichtkonformitäten und Korrekturmaßnahmen (Normkapitel 10.2)

Diese übergreifenden Prozesse finden an vielen Stellen des ISMS Anwendung und sollten im Audit auch an vielen Stellen geprüft werden und nicht nur an einer Stelle.

Prozessübergreifend arbeiten

Bei einem nach der Nachweisnorm ISO/IEC 27001 durchgeführten Audit sollte daher der Prozessbezug der Auditfrageliste mittels der Turtle-Methode Berücksichtigung finden. In der Praxis sollte für die wesentlichen Prozesse (meist die Kernprozesse) ergänzend zur Textanalyse auch eine Turtle-Analyse durchgeführt werden. Damit ist gewährleistet, dass die einzelnen ISMS-Forderungen prozessübergreifend erfasst werden und für jeden Prozess