Datenschutz-Audit

Recht – Organisation – Prozess – IT

Pachinger/Beham (Hrsg.)

Fachmedien Recht und Wirtschaft | dfv Mediengruppe | Frankfurt am Main

HINWEIS/DISCLAIMER:

Die Aufbereitung der einzelnen Kontrollbereiche, Kontrollgruppen und Kontrollen basiert auf den bisherigen Erfahrungen der Herausgeber und Autoren bei der Durchführung von Datenschutz-Audits nach der aktuellen Rechtslage. Die Methodik wurde in Anlehnung an Audits von Managementsystemen entwickelt. Die aus den Verpflichtungen der DSGVO „abgeleiteten" Kontrollen/Maßnahmen sind Möglichkeiten, die Erfüllung der Anforderungen der DSGVO und des BDSG nachzuweisen („Good Practice"). Keinesfalls wird damit gesagt, dass diese Kontrollen/Maßnahmen die ausschließlich relevanten bzw notwendigen sind, um die Erfüllung der Vorgaben der DSGVO und des DSG vollständig nachzuweisen; das vorliegende Werk stellt auch keine Rechts- oder Security-Beratung dar und ersetzt nicht die rechtliche Beratung im Einzelfall. Zu beachten ist daher, dass Datenschutz- und Aufsichtsbehörden oder auch Gerichte im Einzelfall andere oder weitere Nachweise verlangen können. Die Herausgeber und Autoren übernehmen daher keine Haftung für die korrekte Erfüllung von Vorgaben der DSGVO und des BDSG.

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

ISBN 978-3-8005-1798-5

dfv Mediengruppe

© 2022 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main

www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Druck: WIRmachenDRUCK GmbH, Backnang

Printed in Germany

2. Grundlagen eines Audits

2.1 Einleitung

Der Begriff „Audit“ hat seinen Ursprung im Lateinischen:

„audito“ – das Hörensagen, Gerede, Gerücht; aber auch die Anhörung
„audire“ – anhören, hören, vernehmen

Ein Audit hat heutzutage jedoch nichts mit den obenstehenden Begriffen zu tun. Ein modernes Audit sollte partnerschaftlich zwischen Auditor und den befragten Personen erfolgen und sicherlich kein „Verhör“ darstellen. Eine passendere Definition findet sich in „ISO 19011:2011 Leitfaden zur Auditierung von Managementsystemen“.[15] Demnach ist ein Audit ein:

„… systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiven Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind.“

Vereinfacht formuliert ist ein Audit daher die Prüfung einer Entität hinsichtlich deren Einhaltung von normierten Anforderungen. Der ISO-Standard wurde ursprünglich für Managementsystem-Prüfungen wie Qualitätsmanagement (ISO 9001) oder Umweltmanagement (ISO 14001) entwickelt und beschreibt Anforderungen und Abläufe eines Audits. Zusätzlich definiert der ISO-Standard die Ansprüche an Auditoren. Er eignet sich jedoch auch für andere (Management-)Systeme, in unserem Fall für Datenschutz.

Ziel eines Datenschutz-Audits ist es, die Einhaltung der gesetzlichen Bestimmungen im Bereich des Datenschutzes zu überprüfen, Schwächen zu identifizieren und Maßnahmen zu planen sowie einzuführen, um diese Schwächen zu beseitigen.

Ein weiterer ISO-Standard mit Auditrelevanz ist „ISO/IEC 17021-1:2015 Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“.[16] Dieser stellt die Voraussetzungen für Organisationen, die Managementzertifizierungen nach ISO durchführen dürfen, dar.

15 ISO 19011:2011 Leitfaden zur Auditierung von Managementsystemen – kurz ISO 19011 (2011) 7.

16 ISO/IEC 17021-1:2015 Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren, kurz ISO 17021.

Die beiden genannten Standards (ISO 19011, ISO 17021) werden von der ISO bewusst allgemein gehalten und gelten nicht für ein bestimmtes Managementsystem. Diese Standards können vielmehr auch für andere Standards gelten oder aber als Anforderungskataloge – wie bspw ein **Control Framework** – als Auditbasis dienen.

Audits sind ein wesentlicher Bestandteil von Managementsystemen, da durch sie regelmäßig die Anforderungen an und die Wirksamkeit (Effektivität) von Prozessen und Verfahren überprüft werden. Folgende Standards verpflichten Organisationen zu regelmäßigen Audits:

- Qualitätsmanagement
- Umweltmanagement
- Informationssicherheitsmanagement

Ebenso können Audits, die die Konformität anderer Anforderungskataloge erfüllen, nach der in ISO 17021 und ISO 19011 beschriebenen Methodik vollzogen werden. In unserem Werk wird ein **Control Framework** für **Datenschutz** beschrieben, das einen solchen Anforderungskatalog darstellt.

Dieses Kapitel zeigt die **Voraussetzungen** für ein **Datenschutz-Audit** auf und beschreibt die Planung, die Durchführung und das Reporting eines Audits nach der ISO-Management Auditmethodik.

2.2 Begriffsdefinition

2.2.1 Handelnde Parteien eines Audits

Audits werden durch einen Auditauftraggeber veranlasst. Typische Auditauftraggeber für Datenschutz-Audits sind die Unternehmensleitung, die Compliance Abteilung, die Rechtsabteilung, der Datenschutzbeauftragte des Unternehmens oder auch Geschäftskunden. Die „auditierte Organisation“ – **Auditee**[17] – ist die Entität (Unternehmen, Bereich, Standort), die im Scope des Audits steht. Die Personen (Management und Mitarbeiter des Auditee, Kunden oder Lieferanten), die vom Auditor befragt oder deren Handlungen beobachtet werden, bezeichnen wir in diesem Werk als *Auskunftspersonen*.

Der **Auditor** ist jene Person, die das Audit durchführt. Größere Audits werden von einem Auditteam vollzogen. Dieses besteht aus mehreren Auditoren, die oft durch **Fachexperten** unterstützt werden. Der Fachexperte muss kein ausgebildeter Auditor sein, vielmehr benötigt er spezifisches Wissen

17 Der englische Begriff für die „auditierte Organisation“ – „Auditee“ – hat im Bereich Audit eine hohe Verbreitung und Akzeptanz. In diesem Werk wird somit der Begriff „Auditee“ verwendet.

über die Organisation, Branche, Kultur, Technik oder Sprache und ergänzt dadurch die Auditoren. Das Auditteam wird durch einen **Auditteamleiter** (Lead Auditor) geführt. Dieser hat die Gesamtverantwortung für das Audit.

Checkliste: Aufgaben und Verantwortungen im Auditteam

Der **Auditteamleiter** nimmt die folgenden Aufgaben und Verantwortungen wahr:

- Leitung und hauptverantwortliche Durchführung des Audits
- Auditvorbereitung, Erstellung des Auditplans in Abstimmung mit dem Auditee
- Aufzeichnung und Bewertung der Auditfeststellungen in Zusammenarbeit mit dem Auditteam
- Durchführung von Nachaudits bei Abweichungen zum Standard
- Erstellung des Auditberichts
- Präsentation der Auditergebnisse

Der **Auditor** hat folgende Aufgaben und Verantwortungen:

- Vorbereitung auf das Audit: Lesen von Leitlinien, Verfahrensbeschreibungen und Nachweisen
- Mitwirkung bei der Vorbegutachtung
- Allein- oder mitwirkungsverantwortliche Durchführung von Teilaudits
- Aufzeichnung seiner Auditfeststellungen
- Mitwirkung bei der Bewertung von Auditfeststellungen (Auditteam Abstimmung)
- Mitwirkung bei der Berichterstattung und Präsentation

Dem **Experten** sind die folgenden Aufgaben und Verantwortungen zugewiesen:

- Vorbereitung auf das Audit
- Lesen von Leitlinien, Verfahrensbeschreibungen und Nachweisen
- Fachlich unterstützende Mitwirkung beim Audit
- Aufzeichnung seiner Auditfeststellungen
- Mitwirkung bei der Abstimmung im Auditteam

Abbildung 2: Aufgaben und Verantwortung im Auditteam

Ein Betreuer – Guide – ist meist ein Mitarbeiter des Auditee, der sich um die organisatorischen Themen des Audits kümmert. Er kümmert sich um die Logistik sowie die zeitliche und räumliche Planung. Während des Audits führt er die Auditoren durch die Organisation (Werksgelände, Bürogebäude, Standorte) und reagiert auf Änderungen (meist Verspätungen) im Ablauf. Er

sollte nicht zugleich Auskunftsperson im Zuge des Audits sein, also nicht für inhaltliche Themen des Audits als Gesprächspartner dienen.

2.2.2 Auditkriterien und -ergebnisse

2.2.2.1 Auditkriterien

Ein Audit sollte immer reproduzierbare Ergebnisse liefern. Das heißt, Auditor A sollte idealerweise zum selben Ergebnis kommen wie Auditor B. Voraussetzung dafür ist natürlich dasselbe fachliche Wissen beider Auditoren. Wesentlich ist hier, dass Audits auf einer einheitlichen Basis erfolgen müssen. *Auditkriterien* stellen Verfahren, Vorgehensweisen und Anforderungen dar, die als Referenz zur Prüfung der Auditnachweise verwendet werden. Standards wie ISO 9001 (Qualitätsmanagement), ISO 27001 (Informationssicherheitsmanagement) oder auch das COBIT Framework (Governance und Management-Framework für IT) stellen Auditkriterien dar. Für den Bereich Datenschutz stellen die Kontrollen[18] aus diesem Buch eine mögliche Auditbasis dar. Die beschriebenen Kontrollbereiche, Kontrollgruppen und Kontrollen können in Summe als Datenschutz-Auditkriterien herangezogen werden.

2.2.2.2 Auditnachweise

Der Auditor sollte sich während des Audits ein objektives Bild über die Wirksamkeit von Verfahren, Vorgehensweisen und Maßnahmen machen. Dazu sind Auditnachweise erforderlich. Auditnachweise sind Dokumente, Aufzeichnungen oder auch Beobachtungen, die die Einhaltung der oben genannten Kriterien aufzeigen können.

2.2.2.3 Auditfeststellungen

Werden die Kriterien hingegen nicht eingehalten, so wird die Nichteinhaltung in einer Auditfeststellung dokumentiert. ISO 19011 definiert Auditfeststellungen als *„... Ergebnis aus der Bewertung der gesammelten Auditnachweise ... in Hinblick auf Auditkriterien“*[19].

Nach dieser Definition kann auch das Einhalten der oben genannten Kriterien in Auditfeststellungen dokumentiert werden. Meist wird jedoch nur die Nichtkonformität, also ein Verstoß gegen ein vorgegebenes Verfahren, in einer Auditfeststellung dokumentiert.

---

18 Vgl Kapitel Kontrollen 3.1.3.
19 ISO 19011: Leitfaden zur Auditierung von Managementsystemen, S. 8.

2.2.2.4 Auditschlussfolgerung

Nach Abschluss des Audits wird der Auditor die *Auditschlussfolgerungen* dokumentieren. Dieses Ergebnis des Audits berücksichtigt die Auditziele (zB Einhaltung von Anforderungen der DSGVO) und schließt alle Auditfeststellungen mit ein. In der Praxis werden bei Erstaudits nicht alle Auditziele erreicht. Die Abweichungen sind in Form von Auditfeststellungen dokumentiert.

2.2.3 Auditvarianten

Audits können in verschiedene Varianten eingeteilt werden.[20] *Interne Audits*, bei denen meist das Management des Unternehmens der Auditauftraggeber ist, stellen *Erstparteiaudits* (First Party Audits) dar. Der Auditor ist ein Mitarbeiter des Unternehmens. Er sollte jedoch aus Unabhängigkeitsgründen nicht Teil des auditierten Bereiches sein. In manchen Fällen, bei denen diese Unabhängigkeit nicht gewährleistet ist, keine Ressourcen für Audits verfügbar sind oder schlicht einfach das Wissen für Audits innerhalb der Organisation fehlt, können interne Audits auch durch externe Auditoren erfolgen. Hier ist aber die klare Abgrenzung zu einem tatsächlichen externen Audit zu treffen.

Externe Audits werden meist von externen Interessierten, also Geschäftskunden, durchgeführt. Diese *Zweitparteiaudits* (*Second Party Audits*) werden beispielsweise regelmäßig von Automobilherstellern bei deren Zulieferern in den Themenbereichen Qualitätsmanagement oder Informationssicherheitsmanagement durchgeführt. Ein Dilemma stellt dies für Unternehmen dar, bei denen verschiedene Geschäftskunden dasselbe Themengebiet durch ein Zweitparteien-Audit begutachten lassen. Jedes der Audits blockiert die Mitarbeiter bei deren täglichen Aufgaben. Man spricht hier von „Audit-Tourismus“.

Abhilfe dagegen schaffen *Drittparteiaudits* (Third Party Audit), bei denen eine unabhängige Organisation das Audit durchführt. Das Auditergebnis wird daraufhin vom Auditee an die jeweiligen Geschäftskunden übermittelt.

Eine erweiterte Art von Drittparteiaudits sind *Zertifizierungsaudits*. Diese werden durch eine bevollmächtigte (akkreditierte) Stelle durchgeführt. Bei positivem Auditergebnis wird ein Zertifikat ausgestellt. Dieses Zertifikat dient dem Auditee als Nachweis der Konformität. Auch Datenschutz-Audits können in Form von Zertifizierungsaudits erfolgen. Das Ergebnis ist ein „Datenschutzzertifikat“ (siehe Kapitel 8).

---

20 Vgl ISO 19011: Leitfaden zur Auditierung von Managementsystemen, S. 7 und EN ISO/IEC 17021-1: Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren (2015).

2.3 Grundsätze eines Audits

Um das Vertrauen in das Audit, die Auditoren und somit auch in die Auditergebnisse sicherzustellen, sollte ein Audit gewissen Grundsätzen folgen.[21]

- Unabhängigkeit: der Auditor ist vom Auditee in keiner Weise abhängig; auch bei internen Audits sollte dies durch entsprechende Befugnisse und Rechte sichergestellt sein
- Objektivität: der Auditor lässt sich nicht durch Faktoren wie Sympathie, Hörensagen, unbestätigte Informationen beeinflussen
- Sachlichkeit: die Ergebnisse des Audits werden vom Auditor richtig, genau und verständlich dokumentiert
- Kompetenz: der Auditor verfügt über das entsprechende Fachwissen, arbeitet sorgfältig und hat ein gutes Urteilsvermögen
- Integrität: der Auditor erbringt seine Arbeit ehrlich und hält die rechtlichen Anforderungen beim Audit ein
- Vertraulichkeit/Verschwiegenheit: der Auditor schützt die erhaltenen Informationen in angemessener Weise und gibt diese nicht an Unberechtigte weiter
- Methodischer Ansatz: der Auditor führt Audits nach einem vordefinierten Schema durch und dokumentiert nachvollziehbar den Auditverlauf

2.4 Planung eines Audits

Zuerst sollte das Ziel des Audits definiert werden. Das übliche Ziel eines Datenschutz-Audits ist es, die gesetzliche Konformität in Hinblick auf die rechtlichen Vorgaben nachzuweisen. Aber auch weitere Ziele sind denkbar, wie eine Attestierung des Datenschutzmanagements nach ISAE 3000 (siehe Kapitel 8.1). Der Auditor muss die erforderlichen Ressourcen, die für das Audit benötigt werden, definieren. Des Weiteren sammelt der Auditor Informationen über den Auditee, um dessen Geschäftsfeld und die damit verbundenen Datenrisiken grob abschätzen zu können. Mit diesen Informationen kann der Auditor den Scope des Audits einschätzen. Bereits bei der Planung sollte der Auditteamleiter sein Team entsprechend den benötigten Qualifikationen zusammensetzen. Das Ergebnis der Planung ist ein Auditprogramm, das zeigt, wer wann und wo während des Audits involviert sein muss, welche Anforderungen betrachtet werden und wie lange das Audit dauert.

21 Vgl ISO 17021, ISO 19011, ISACA IT-Prüfungsstandards.

Checkliste: Auditplanung

Folgende Informationen sollten bei der Auditplanung erhoben werden:

- Namen der Kontaktpersonen
- Guides
- Dolmetscher (falls notwendig)
- Zahl der Mitarbeiter/Schichten
- Zahl der Standorte
- Größe des Betriebes
- Komplexität des Unternehmens
- Zu berücksichtigende Gesetzgebung
- Größe des Auditteams
- Qualifikation der Teammitglieder
- Verfügbarkeit von Einrichtungen
- Gesundheits- und Sicherheitsvoraussetzungen
- Benötigte Ausrüstung für spezielle Bereiche
- Zugang zu Hochsicherheitsbereichen
- Sicherheitsüberprüfung (Vertraulichkeitsüberprüfung der Auditoren durch den Auditee)
- Benötigte Vertraulichkeitsvereinbarungen

Abbildung 3: Checkliste zur Auditplanung

2.4.1 Auditprogramm

Ein Auditprogramm legt über einen bestimmten Zeitraum die Audittätigkeiten der Organisation fest.

> *„Ein Aspekt des Auditprogramms ist die Festlegung, welche Zielsetzung mit den Audits generell verfolgt werden soll.“*[22]

Ein Auditprogramm kann verschiedene Themengebiete oder -bereiche umfassen. Beispielsweise Qualitätsmanagement, Informationssicherheit und auch Datenschutz. Das Auditprogramm gibt somit eine Übersicht über Auditthemen, Unternehmensbereiche und Standorte.

> *„Das Auditprogramm sollte Informationen und Ressourcen erfassen, die erforderlich sind, um die Audits innerhalb des festgelegten Zeitrahmens wirksam und effizient zu organisieren und durchzuführen.“*[23]

Folgende Themen sollte ein Auditprogramm jedenfalls beinhalten:[24]

22 *Gietl/Lobinger,* Leitfaden für Qualitätsauditoren, S. 60.
23 ISO 19011: Leitfaden zur Auditierung von Managementsystemen, S. 14.
24 Vgl ISO 19011: Leitfaden zur Auditierung von Managementsystemen, S. 14.

- Ziele für das Auditprogramm/Audit
- Antworten zu wann/wo/wie lange das Audit stattfindet und was die Zielsetzung ist
- Auditkriterien
- Auditmethode
- Auditteam
- Ressourcen

Beispiele für Ziele eines Auditprogramms

- Koordinierung und Vereinheitlichung von Audits für mehrere Managementsysteme
- Aufdeckung/Nutzung von Synergieeffekten zur Reduzierung des Auditaufwands
- Evaluierung der Erfüllung von gesetzlichen Anforderungen
- Identifizierung von Verbesserungsmöglichkeiten des Auditprogramm-Managementsystems

Beispiele für Ziele einzelner Audits

- Bewertung der Effizienz des Managementsystems
- Identifizierung von Verbesserungsmöglichkeiten
- Evaluierung der Erfüllung von gesetzlichen Anforderungen
- Evaluierung der Zielerfüllung

Abbildung 4: Ziele von Auditprogrammen und Audits

Ein Auditprogramm kann auch über mehrere Jahre hinweg geplant und abgewickelt werden. Gerade bei umfangreicheren Auditprogrammen und wenig Ressourcen kann dies eine praktikable Vorgangsweise sein. Im Sinne eines risikobasierten Ansatzes wird hier zuerst identifiziert, welche Punkte im Auditprogramm für den Auditee besonders wesentlich sind bzw wo auch die Risiken am höchsten sind. Diese Punkte sollten bereits initial auditiert werden. Ein Auditprogramm kann auch Audits verschiedener Bereiche und Auditkriterien beinhalten.

Aus dem Auditprogramm werden für einzelne zusammenhängende Audits Auditpläne abgeleitet. Diese beinhalten das Programm einzelner oder weniger aufeinander folgender Audittage. Sie dienen dem Auditee zur Vorbereitung, sodass Auskunftspersonen anwesend sind und Bereiche besichtigt werden können. Dem Auditor dienen die Auditpläne zur Ressourcenplanung und zur Identifikation der benötigen Auditexpertise und während des Audits vor allem für das Zeitmanagement.