Holger Reibold

Audit Ready IT

IT-Audits bestehen mit Prozessen, Kontrollen und Evidence – ohne neue Tools und ohne Systemumbau

BRAIN-MEDIA.DE

Holger Reibold

Audit Ready IT

IT-Audits bestehen mit Prozessen, Kontrollen und Evidence – ohne neue Tools und ohne Systemumbau

BRAIN-MEDIA.DE

ISBN: 978-3-95444-329-1

Cover: Niklas Junge / Pixabay

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. 52c – 66113 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

Auditoren prüfen keine Systeme – sie prüfen Kontrollen und Evidence.

Diese Erkenntnis ist zugleich einfach und überraschend. Viele IT-Organisationen investieren enorme Zeit und Ressourcen in technische Verbesserungen, neue Tools oder komplexe Sicherheitsarchitekturen, wenn ein Audit bevorsteht. Server werden neu konfiguriert, Monitoring-Systeme erweitert, zusätzliche Software beschafft oder bestehende Prozesse hastig umgebaut. Dennoch endet das Audit nicht selten mit kritischen Findings, offenen Punkten oder umfangreichen Nacharbeiten.

Der Grund dafür liegt selten in der technischen Qualität der Systeme. In den meisten Fällen liegt er vielmehr darin, dass Kontrollen nicht nachvollziehbar sind oder ihre Umsetzung nicht durch belastbare Nachweise belegt werden kann. Auditoren bewerten nicht primär, wie modern oder komplex eine IT-Landschaft ist. Sie prüfen, ob Risiken erkannt werden, ob Kontrollen existieren und ob deren Wirksamkeit nachvollziehbar dokumentiert ist. Kurz gesagt: Ohne Evidence existiert eine Kontrolle aus Sicht des Audits nicht.

Genau an diesem Punkt setzt dieses Buch an. Es verfolgt einen pragmatischen Ansatz, den man als Evidence Engineering bezeichnen kann: die systematische Gestaltung von Prozessen, Kontrollen und

Nachweisen, sodass Evidence nicht erst kurz vor einem Audit gesucht werden muss, sondern automatisch im täglichen IT-Betrieb entsteht.

Parallel dazu nimmt der regulatorische Druck auf Unternehmen weltweit zu. Standards wie ISO 27001, Frameworks wie SOC 2 sowie regulatorische Anforderungen wie NIS2 oder DORA erhöhen die Erwartungen an IT-Organisationen erheblich. Gleichzeitig wächst die Abhängigkeit von digitalen Prozessen, Cloud-Plattformen und komplexen IT-Landschaften. Audits werden dadurch nicht nur häufiger, sondern auch strukturierter und umfassender. Für viele Organisationen bedeutet das: Audits sind kein seltenes Ereignis mehr, sondern ein wiederkehrender Bestandteil des Betriebs.

Trotz dieser Entwicklung sind Audits in vielen IT-Abteilungen noch immer mit erheblichem Stress verbunden. Kurz vor der Prüfung beginnen hektische Aktivitäten: Dokumente werden zusammengestellt, Prozesse werden nachträglich beschrieben und Verantwortlichkeiten geklärt. Häufig entsteht der Eindruck, dass ein Audit ein außergewöhnliches Projekt sei, das besondere technische Maßnahmen erfordert.

In der Praxis zeigt sich jedoch immer wieder, dass dieser Ansatz selten zum gewünschten Ergebnis führt. Neue Software löst nur selten das eigentliche Problem. Wenn Prozesse unklar sind, Verantwortlichkeiten fehlen oder Evidence nicht systematisch entsteht, wird auch das modernste Tool keine Auditfähigkeit herstellen.

Dieses Buch verfolgt daher einen anderen Ansatz: Auditfähigkeit ohne Systemumbau.

Der Schwerpunkt liegt nicht auf Technologie, sondern auf Struktur, Nachvollziehbarkeit und organisatorischer Klarheit. Ziel ist es zu zeigen, wie Organisationen ihre bestehenden Systeme, Prozesse und Werkzeuge so nutzen können, dass Kontrollen transparent werden und Evidence automatisch entsteht. Dabei geht es nicht um zusätzliche Bürokratie, sondern um eine bessere Nutzung der bereits vorhandenen Abläufe.

Die Zielgruppe dieses Buches sind Menschen, die in der Praxis Verantwortung für IT-Systeme und deren Governance tragen: CIOs und IT-Leiter, Security-Verantwortliche, Compliance-Manager, interne Auditoren sowie IT-Architekten und Administratoren. Ebenso richtet es sich an Beraterinnen und Berater im Bereich IT-Governance, die Organisationen auf Audits vorbereiten.

Der Nutzen dieses Buches liegt in einer klaren und anwendungsorientierten Perspektive auf Audit Readiness. Es zeigt, wie Kontrollen strukturiert werden können, wie Evidence systematisch entsteht und wie bestehende Werkzeuge sinnvoll genutzt werden. Darüber hinaus behandelt es auch die organisatorischen und menschlichen Aspekte von Audits – von der Vorbereitung bis zur Kommunikation während eines Audit-Interviews.

Auditfähigkeit ist letztlich kein Zustand, der durch ein einzelnes Projekt erreicht wird. Sie entsteht durch nachvollziehbare Prozesse, klare Verantwortlichkeiten und eine Kultur der Transparenz. Wenn diese Elemente vorhanden sind, verlieren Audits ihren Ausnahmecharakter und werden zu einem normalen Bestandteil eines gut geführten IT-Betriebs.

Dieses Buch soll dabei helfen, genau diesen Zustand zu erreichen.

Herzlichst

Holger Reibold

P.S.: Über die Verlags-Website stehen verschiedene Downloads kostenlos bereit. Weitere Ergänzungen wie eine editierbare Matrix sind Teil von KaaS.

1 Audits als Realität moderner IT

Audits prufen selten Technik – sie prufen, ob eine Organisation ihre IT im Griff hat.

In vielen IT-Abteilungen gelten Audits noch immer als Ausnahmezustand. Während der normale Betrieb darauf ausgerichtet ist, Systeme stabil zu halten, Probleme schnell zu lösen und neue Anforderungen umzusetzen, bringt ein Audit eine völlig andere Perspektive in die Organisation. Plötzlich stehen nicht mehr Verfügbarkeit, Performance oder Innovation im Vordergrund, sondern Nachvollziehbarkeit, Dokumentation und formale Kontrollen.

Diese unterschiedliche Sichtweise führt häufig zu Spannungen. IT-Teams sind darauf trainiert, technische Probleme effizient zu lösen. Auditoren hingegen interessieren sich weniger dafür, wie elegant eine technische Lösung ist, sondern vielmehr dafür, ob Prozesse definiert wurden, ob Kontrollen existieren und ob deren Durchführung nachweisbar ist. Für viele IT-Verantwortliche wirkt diese Herangehensweise zunächst fremd oder sogar bürokratisch. Die unterschiedlichen Perspektiven von IT-Teams und Auditoren lassen sich vereinfacht wie folgt darstellen:

Unterschiedliche Perspektiven von IT-Teams und Auditoren: Während IT-Organisationen Systeme und technische Lösungen in den Mittelpunkt stellen, betrachten Audits primär Risiken, Kontrollen und deren Nachweisbarkeit.

Hinzu kommt, dass Audits selten im Alltag der IT stattfinden, sondern in zeitlich klar abgegrenzten Phasen. Wochen oder Monate vor einem geplanten Audit beginnt oft eine intensive Vorbereitungsphase. Dokumente werden gesucht, Prozesse werden beschrieben und Verantwortlichkeiten werden geklärt. In dieser Situation entsteht leicht der Eindruck, dass ein Audit ein außergewöhnliches Ereignis sei, das nur mit zusätzlicher Technik oder neuen Tools bewältigt werden kann.

Genau hier liegt jedoch ein grundlegendes Missverständnis. Audits bewerten nicht primär die technische Qualität eines Systems, sondern die Struktur und Nachvollziehbarkeit der Organisation dahinter. Ein System kann technisch hervorragend umgesetzt sein und dennoch im Audit schlecht abschneiden, wenn Kontrollen nicht dokumentiert sind oder Evidente fehlt.

Dieses Kapitel beleuchtet deshalb zunächst die Realität moderner IT-Audits. Es zeigt, warum Audits für IT-Teams häufig belastend wirken, welche typischen Situationen in der Vorbereitung entstehen und warum viele Organisationen reflexartig zu technischen Lösungen greifen. Gleichzeitig wird erklärt, wie Auditoren tatsächlich denken und warum es oft zu Konflikten zwischen IT-Abteilungen und Compliance-Funktionen kommt.

Wer versteht, welche Logik hinter einem Audit steht, kann viele dieser Spannungen auflösen. Audits verlieren dann ihren Ausnahmecharakter und werden zu einem nachvollziehbaren Bestandteil eines professionell geführten IT-Betriebs.

1.1 Warum Audits für IT-Teams belastend sind

Für viele IT-Abteilungen sind Audits mit erheblichem Stress verbunden. Obwohl Audits in vielen Organisationen regelmäßig stattfinden, werden sie im Arbeitsalltag häufig als außergewöhnliches Ereignis wahrgenommen. Der Grund dafür liegt weniger in der technischen

Prüfung selbst, sondern vielmehr in der Art und Weise, wie Audits organisiert und vorbereitet werden.

IT-Teams arbeiten in der Regel unter starkem operativem Druck. Systeme müssen stabil laufen, Störungen müssen schnell behoben werden und neue Anforderungen aus Fachbereichen oder Management werden kontinuierlich umgesetzt. In dieser Umgebung zählen Geschwindigkeit, technische Kompetenz und pragmatische Problemlösung. Wenn ein System ausfällt, erwartet niemand eine ausführliche Dokumentation des Reparaturprozesses – entscheidend ist, dass der Betrieb möglichst schnell wiederhergestellt wird.

Ein Audit stellt diese Arbeitslogik plötzlich auf den Kopf. Anstelle von Geschwindigkeit und technischer Effizienz stehen nun Nachvollziehbarkeit, Dokumentation und formale Kontrollen im Mittelpunkt. Auditoren möchten verstehen, wie Entscheidungen getroffen werden, wer bestimmte Aktivitäten freigibt und ob Prozesse wiederholbar und überprüfbar sind. Für viele IT-Spezialisten wirkt diese Perspektive zunächst ungewohnt oder sogar unnötig bürokratisch.

Ein weiterer Stressfaktor ist der Zeitpunkt, zu dem Audits häufig wahrgenommen werden. In vielen Organisationen beginnt die intensive Beschäftigung mit Audit-Anforderungen erst wenige Wochen vor der eigentlichen Prüfung. Dokumente müssen kurzfristig zusammengestellt werden, Prozesse werden nachträglich beschrieben und Verantwortlichkeiten werden plötzlich hinterfragt. Diese kurzfristige Vorbereitung erzeugt zusätzlichen Druck und verstärkt den Eindruck, dass Audits vor allem zusätzliche Arbeit verursachen.

Hinzu kommt, dass viele IT-Teams den Eindruck haben, im Audit beurteilt zu werden. Wenn Auditoren kritische Fragen stellen oder bestimmte Nachweise verlangen, wird dies leicht als Kritik an der eigenen technischen Arbeit interpretiert. In Wirklichkeit prüfen Auditoren jedoch nicht die Fähigkeiten einzelner Administratoren oder Entwickler. Sie prüfen, ob die Organisation in der Lage ist, Risiken zu erkennen, Kontrollen zu definieren und deren Umsetzung nachvollziehbar zu dokumentieren.

Ein weiterer Grund für die Belastung liegt in der unterschiedlichen Sprache von IT und Audit. Technische Teams denken in Systemen, Architekturen und Konfigurationen. Auditoren sprechen hingegen von Kontrollen, Risiken und Wirksamkeit. Diese unterschiedlichen Perspektiven können leicht zu Missverständnissen führen. Ein Administrator, der ein Problem technisch hervorragend gelöst hat, kann Schwierigkeiten haben zu verstehen, warum ein Auditor zusätzlich einen dokumentierten Nachweis verlangt.

Schließlich spielt auch die Komplexität moderner IT-Landschaften eine Rolle. Viele Organisationen betreiben heute hybride Infrastrukturen aus lokalen Systemen, Cloud-Plattformen und zahlreichen SaaS-Diensten. Verantwortlichkeiten sind verteilt, Prozesse sind nicht immer eindeutig dokumentiert und neue Systeme werden kontinuierlich eingeführt. In einem solchen Umfeld fällt es schwer, jederzeit einen vollständigen Überblick über alle relevanten Kontrollen und Nachweise zu behalten.

All diese Faktoren tragen dazu bei, dass Audits in vielen IT-Abteilungen als belastend wahrgenommen werden. Dabei ist der eigentliche Zweck eines Audits nicht, zusätzliche Arbeit zu erzeugen, sondern Transparenz über Risiken und Kontrollen zu schaffen. Wenn Organisationen ihre Prozesse so gestalten, dass Kontrollen und Evidence im Alltag entstehen, verliert das Audit seinen Ausnahmecharakter und wird zu einem normalen Bestandteil eines gut strukturierten IT-Betriebs.

1.2 Typische Situationen vor einem Audit

In vielen Organisationen beginnt die intensive Auseinandersetzung mit einem Audit erst dann, wenn der Termin bereits feststeht. Wochen oder Monate vor der Prüfung entsteht eine Phase erhöhter Aktivität, in der versucht wird, alle relevanten Informationen, Dokumente und Nachweise zusammenzustellen. Diese Phase ist häufig von Hektik geprägt, da viele Themen zuvor nicht systematisch vorbereitet wurden.

Eine typische Situation ist die kurzfristige Suche nach Dokumentation. Prozesse existieren zwar im Alltag, sind jedoch selten vollständig beschrieben. Administratoren wissen aus Erfahrung, wie bestimmte Aufgaben durchgeführt werden, doch es gibt keine formalen Prozessbeschreibungen oder Richtlinien. Sobald ein Auditor nach einer dokumentierten Kontrolle fragt, beginnt die mühsame Rekonstruktion dessen, was eigentlich schon lange praktiziert wird. Der

typische Ablauf einer Auditvorbereitung lässt sich vereinfacht wie folgt darstellen:

Typischer Ablauf der Auditvorbereitung in vielen Organisationen: Kurz vor einem Audit entsteht häufig eine Phase intensiver Dokumentations- und Evidence-Suche, während im normalen Betrieb nur wenig strukturierte Vorbereitung erfolgt.

Ähnlich verhält es sich mit Nachweisen. In vielen Fällen werden Kontrollen im Alltag tatsächlich durchgeführt, etwa bei der Vergabe von Benutzerrechten, bei Systemänderungen oder bei Backup-

Stichwortverzeichnis

F

G

I

J

K

L

M

N

O

R

S

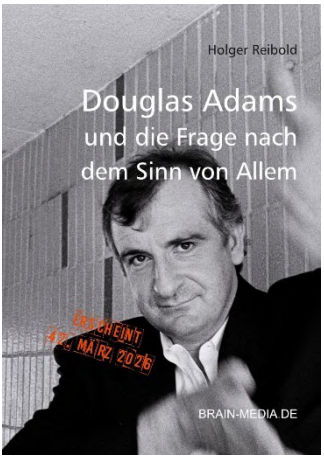
T

V

W

Z

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

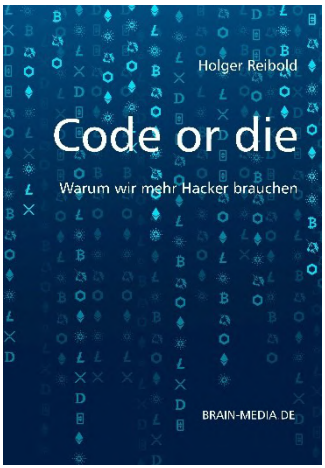
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 19,99 EUR

Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 24,99 EUR

Brain-Media KaaS

Individual

Business

Enterprise

– die E-Book-Flatrate –

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt Plus+ eine Renaissance.

Abonnementen erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können über 30 verfügbare E-Books herunterladen – dazu editierbare Checklisten, Vorlagen, Beispiele etc. Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die E-Books verwenden kein DRM!

Und das alles zum **unschlagbaren Sonderpreis**!