Knoll, Matthias

Article — Published Version

Rezension „IT-Audit“

HMD Praxis der Wirtschaftsinformatik

Provided in Cooperation with:
Springer Nature

Suggested Citation: Knoll, Matthias (2021) : Rezension „IT-Audit“, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 58, Iss. 2, pp. 447-449, https://doi.org/10.1365/s40702-021-00708-0

This Version is available at:
https://hdl.handle.net/10419/287682

HMD (2021) 58:447–449
https://doi.org/10.1365/s40702-021-00708-0

REZENSIONEN

Rezension „IT-Audit“

Matthias Knoll

Angenommen: 2. Februar 2021 / Online publiziert: 10. Februar 2021

Stefan Beißel **IT-Audit – Grundlagen, Prüfungsprozess, Best Practice**
ISBN 978-3-503-19124-6, Erich Schmidt Verlag, 2. Aufl., Berlin 2020, 313 S., 44,95 €

Angesichts der vergleichsweise knappen verfügbaren Literatur kommt einem Übersichtswerk zum Thema IT-Audit große Bedeutung zu. Entsprechend hoch sind daher die Erwartungen, verspricht das Buch bereits im Untertitel nicht nur Grundlagen zu vermitteln, sondern mit „Best Practices“ auch und gerade für die Praxis relevant zu sein.

Der englische Fachbegriff „Audit“ wird im Sprachgebrauch einschlägiger Literatur ohne exakte Fokussierung auf ein Fachgebiet recht allgemein im Sinne einer Überprüfung oder Inspektion angewandt, wie der Autor im einleitenden Satz zu den Grundlagen korrekt schreibt. Denn „Audit“ wird etwa im Kontext von Zertifizierungen und überall dort verwandt, wo die Einhaltung spezifischer Regelungen bestätigt werden soll. Dies gilt auch für die IT, ein Beispiel ist das ISO-27001-Audit.

Das Präfix „IT-“ könnte nun suggerieren, dass der Begriff „Audit“ im Kontext der IT einer ebenso allgemeinen Verwendung unterliegt. Doch es ist hier durchaus üblich, ein IT-Audit mit dem deutschen Begriff der IT-Prüfung gleichzusetzen. IT-Prüfungen unterscheiden sich jedoch in vielerlei Hinsicht von den oben angesprochenen *Über*prüfungen und Inspektionen. IT-Prüfungen werden von Revisionen, Wirtschaftsprüfungsgesellschaften und weiteren, in diesem Kontext tätigen Spezialisten durchgeführt, was mit einem bestimmten Sprachgebrauch verbunden ist.

Wer also IT-Prüfungen durchführt oder in dieses Themengebiet einsteigen möchte, erwartet eine bestimmte Begrifflichkeit.

M. Knoll (✉)
Hochschule Darmstadt, Darmstadt, Deutschland
E-Mail: matthias.knoll@h-da.de

Genau hier liegt das Hauptproblem des vorliegenden Buches. Zwar ist das Buch sehr breit aufgestellt, der inhaltlich sehr interessante Stoff wird aber stellenweise durch Verwendung von Begriffen, die im IT-Prüfungs-Kontext eher selten oder überhaupt nicht genutzt werden, abschnittsweise schwer lesbar.

In insgesamt vier Kapiteln, die wiederum in Unterabschnitte aufgeteilt sind, werden Grundlagen, die etwa ein Viertel des Gesamtumfangs einnehmen, sowie die zentralen Schritte im Prüfungsprozess (Vorbereitung, Durchführung, Abschluss) diskutiert.

Möglicherweise hat der Autor mit seiner Begriffswahl versucht, alle Facetten des Audit-Begriffs gleichermaßen abzubilden. Trotz Gemeinsamkeiten kann dies jedoch nur bedingt gelingen. Für Einsteiger könnte eine Lektüre daher irritierend sein, insbesondere, wenn sie aus ihrem beruflichen Umfeld parallel mit anderen Begriffen vertraut gemacht worden sind.

So spricht Abschnitt 2.2 etwa vom „Prüfungsvollzug“ und beschreibt damit 1st-, 2nd-, 3rd-Party IT-Audits sowie Joint IT-Audits. Im Sprachgebrauch der IT-Prüfung werden diese Begriffe jedoch zurückhaltend genutzt.

Der Prüfungsumfang wiederum wird in Abschnitt 2.3 als Vorgabe definiert, was geprüft werden soll, also Daten, Applikationen, Netzwerke, Personen, Projekte und vieles mehr. Das ist sicherlich nicht falsch. Doch sind vor dem Hintergrund des risikoorientierten Prüfungsansatzes, der auf S. 39 eher „nebenbei“ erwähnt wird, jedoch im Kontext von IT-Prüfungen von zentraler Bedeutung ist und prominenter herausgestellt werden sollte, nicht vielmehr Prüfungsgegenstände bzw. -objekte gemeint, die in einem Prüfungsuniversum zusammengefasst sind?

Ebenso ungewöhnlich ist es, den Prüfungsprozess mit seinen Prozessschritten unter die Überschrift „Lebenszyklus“ zu stellen.

Auch im nachfolgenden Kapitel 2 (Vorbereitung) findet sich Verbesserungspotential. So darf man durchaus erwarten, dass ein im Jahr 2020 erscheinendes Buch bereits auf COBIT 2019 verweist. Im Kontext der Planung fehlt zudem ein prominenter Hinweis auf die nicht unwichtige Prüfungsstrategie.

Warum Abschnitt 4 (Prüfungsstandards) und Abschnitt 5 (Regelwerke) in dieser Form getrennt sind, lässt sich vielleicht noch mit der Relevanz und Verbindlichkeit dieser Prüfungsstandards erklären, doch auch andere Vorgaben haben bindende Wirkung, wenngleich diese Bindung anders motiviert ist. Der Abschnitt 4 spricht zudem einzelne Prüfungsstandards an, die im Kontext der IT-Prüfung bestenfalls am Rand oder für bestimmte Branchen relevant sind.

Gut und sehr praxisnah sind in diesem Kapitel hingegen „Prüfungsfragen“, die eine erste Orientierung ermöglichen und als Einstieg in die Planung von Prüfungshandlungen genutzt werden können.

Der Abschnitt 7 ist der Prüfungsumgebung gewidmet. Bei ihrer Festlegung ist nach Meinung des Autors eine Eingrenzung in Betracht zu ziehen. Relevante werden also von nicht-relevanten Sachverhalten abgegrenzt. Durch diese Eingrenzung werden nach seiner Auffassung Prüfungsnotwendigkeiten außerhalb des Relevanzbereichs beseitigt. Eine Eingrenzung kann demnach aus Kosten-Nutzen-Aspekten heraus sinnvoll sein. Im Folgenden werden technische und organisatorische Eingrenzungen diskutiert. Im Kontext der technischen Eingrenzung werden Tokenisierung, Punkt-zu-Punkt-Verschlüsselung und Netzwerksegmentierung erwähnt. Die

organisatorische Eingrenzung fokussiert auf Outsourcing, Prozessorientierung und Unternehmensaufteilung. Es ist fraglos richtig, dass im Kontext von IT-Prüfungen nicht alle Aspekte gleichzeitig betrachtet werden können, eine Prioritätensetzung daher notwendig und sinnvoll ist. Doch die hier angewandten Überlegungen könnten sich für Einsteiger in die IT-Prüfung eher schwer erschließen. So könnte dieser Abschnitt den Eindruck erwecken, was sicher nicht beabsichtigt ist, dass diese Aspekte (Tokenisierung, Verschlüsselung, Outsourcing usw.) nicht geprüft werden müssten.

In Abschnitt 8 werden Technologietrends angesprochen. Die Darstellungen enthalten zwar nützliche Hinweise für die Planung und Durchführung einer IT-Prüfung, bleiben aber eher an der Oberfläche. Zudem hätte hier ergänzend das aktuelle und vieldiskutierte Thema Künstliche Intelligenz adressiert werden können.

Mit Blick auf die angekündigten Best Practices sehr hilfreich für die Praxis sind hingegen die Kapitel 3 und 4. Kapitel 3 widmet sich der Prüfungsdurchführung und enthält viele konkrete Tipps für den Prüfungsalltag. Das Kapitel widmet sich auch aktuellen Themen wie dem agilen Audit, Six Sigma im Audit oder dem Lean Audit.

Das sehr kurze Kapitel 4 stellt die wichtigsten Aspekte im Kontext der Berichterstattung und des Follow-up vor und rundet damit das Buch ab.

Ein Gesamtfazit fällt schwer. Einerseits enthält das Buch viele wertvolle Informationen, die auch und gerade für Einsteiger hilfreich sind, andererseits könnte die im Kontext der IT-Prüfung ungewohnte Verwendung wichtiger Fachbegriffe insbesondere in den ersten beiden Kapiteln irritieren. Auch sollte der risikoorientierte Prüfungsansatz stärker in den Vordergrund gerückt und die Formulierung mancher Textstelle zur Vermeidung von Missverständnissen optimiert werden. Vielleicht lassen sich die angesprochenen Punkte in einer 3. Auflage durch stärkere Fokussierung auf IT-Prüfungen berücksichtigen? Es würde sich mit Blick auf die zunehmende Bedeutung und die steigende Komplexität dieses Fachgebiets in jedem Fall lohnen.

Funding Open Access funding enabled and organized by Projekt DEAL.