ERICH
SCHMIDT
VERLAG

IT-Audit

Grundlagen
Prüfungsprozess
Best Practice

Von Dr. Stefan Beißel

2., neu bearbeitete und erweiterte Auflage

ERICH SCHMIDT VERLAG

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

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978-3-503-19124-6

1. Auflage 2015
2. Auflage 2020

Gedrucktes Werk: ISBN 978-3-503-19124-6
eBook: ISBN 978-3-503-19125-3

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706

Druck und Bindung: docupoint, Magdeburg

Vorwort zur 2. Auflage

Das IT-Audit besitzt aufgrund der fortschreitenden Digitalisierung einen immer höheren Stellenwert. Neue technologische Fortschritte und die Zunahme an Regelwerken sind ohne ein wirksames IT-Audit nur schwer zu beherrschen. In der Folge etablieren sich auch im IT-Audit ständig neue, innovative Verfahren und Techniken. Es ist daher nicht verwunderlich, dass auch die Zertifizierungsmöglichkeiten für Auditoren immer umfangreicher werden. Die 2. Auflage dieses Buchs enthält neue Kapitel und Ergänzungen, um dieser spannenden Entwicklung im IT-Audit Rechnung zu tragen.

Moderne Unternehmen nutzen technologische Fortschritte, um ihre internen Abläufe zu optimieren – z. B. sind Cloud-Lösungen in den letzten Jahren sehr populär geworden. Das IT-Audit ist gefordert, mit dieser Entwicklung standzuhalten. Es ist ein wesentlicher Faktor, um die Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit der veränderten Abläufe zu gewährleisten. Entsprechend haben sich auch im IT-Audit neue Ansätze etabliert. Mit ihrer Hilfe können Prüfungsverfahren optimiert und mit betrieblichen Abläufen besser verknüpft werden (siehe Kapitel III Abs. 2): Integrierte Prüfstellen ermöglichen eine automatisierte Prüfung während des operativen Betriebs; eingebettete Audit-Module können in Form von integrierten Softwarekomponenten Prüfungen initiieren oder unterstützen; mit der parallelen Simulation können ausgewählte Informationsverarbeitungen simuliert und geprüft werden, ohne die produktive Umgebung zu beeinträchtigen; das agile IT-Audit bedient sich der Prinzipien aus der agilen Softwareentwicklung, um die Flexibilität und Transparenz zu erhöhen und Zwischenergebnisse schneller zu erzeugen; auch Six Sigma ist im IT-Audit nützlich – es hilft, die Qualität des Audits zu erhöhen und Prüfungsfehler zu reduzieren; sogar Ansätze aus dem Lean Management lassen sich in die Welt des IT-Audits überführen – Zeit- und Ressourceneinsatz für Prüfungen werden dadurch verringert.

Die Regelwerke für das IT-Umfeld von Unternehmen werden immer umfassender und restriktiver. Neben der Datenschutz-Grundverordnung und dem IT-Sicherheitsgesetz gibt es strenge Vorgaben im Finanz- und Versicherungssektor (siehe Kapitel II Abs. 5): Die Datenschutz-Grundverordnung soll für ein einheitliches Datenschutzrecht in Europa sorgen und ist seit Mai 2018 gültig; das IT-Sicherheitsgesetz für Betreiber kritischer Infrastrukturen trat im Juli 2015 in Kraft und hat das Ziel, die Gefahr von Versorgungsstörungen zu verringern; in den Jahren 2017 und 2018 wurden detaillierte Anforderungen an die IT im Finanz- und Versicherungssektor definiert. Auch viele Standards wurden überarbeitet, z. B. der

IT-Grundschutz vom BSI im Jahr 2017. Und durch die stärkere Internationalisierung spielen Standards vom US-amerikanischen NIST eine größere Rolle.

Die zunehmende Bedeutung des IT-Audits macht sich bei Zertifizierungsorganisationen vor allem in gestiegenen Mitgliederzahlen und umfangreicheren Zertifizierungsangeboten bemerkbar (siehe Kapitel I Abs. 4.4). Beispielsweise bietet das (ISC)², das im Vergleich zum Jahr 2014 fast doppelt so viele Mitglieder besitzt, nun die Zertifizierung zum „Certified Cloud Security Professional“ an. Die GIAC hat eine ähnliche Mitgliederentwicklung zu verzeichnen und bietet sogar eine Vielzahl neuer Zertifizierungen an, sodass z. B. „Penetration Testing“ nun eine eigene Zertifizierungsdomäne darstellt.

Das IT-Audit bleibt weiterhin ein wichtiges Thema in der heutigen Industrie und ein nicht zu unterschätzender Erfolgsfaktor für fast jedes Unternehmen, bietet aber gleichzeitig auch spannende Entwicklungen gepaart mit neuen Ansätzen und Möglichkeiten für professionelle Auditoren.

Bergisch Gladbach, im Januar 2020 Stefan Beißel

Vorwort zur 1. Auflage

Informationen können einen fundamentalen Einfluss auf den Unternehmenserfolg haben. Sie sind z. B. Wettbewerbsfaktor, Machtinstrument, Alleinstellungsmerkmal oder Überlebensfaktor. Daher besitzt die IT, mit der diese Informationen gehandhabt werden, in den meisten Unternehmen einen oft unterschätzen Stellenwert.

Damit die IT wirtschaftlich effektiv genutzt wird und mit ihr verbundene Risiken reduziert werden, sollte die sichere, wirtschaftliche und ordnungsmäßige Ausübung aller IT-Aktivitäten gewährleistet werden. In vielen Unternehmen basiert die Erfüllung damit verbundener Anforderungen vornehmlich auf dem Vertrauen gegenüber zuständigen Mitarbeitern. Allerdings entstehen daraus hohe Unsicherheiten für die Stakeholder, insbesondere die Shareholder, des Unternehmens. Die Unsicherheiten ergeben sich nicht nur daraus, dass Anforderungen nicht eingehalten werden können, sondern vor allem daraus, dass sie nicht umfassend genug sind oder unbewusst und unbemerkt von ihnen abgewichen wird. Dies sollte für die Stakeholder langfristig nicht zufriedenstellend sein.

Hier kommt das IT-Audit ins Spiel, das durch die Prüfung von Sicherheit, Wirtschaftlichkeit und Ordnungsmäßigkeit eine hohe Transparenz für das Unternehmen und die Stakeholder schafft. Insbesondere können das Schutzniveau von Informationen und IT-Systemen, die Ausrichtung der IT am Geschäftsmodell des Unternehmens, der wirtschaftlich effiziente Umgang mit Ressourcen und die Befolgung von vorgeschriebenen Regularien oder erwünschten Standards und Best Practices überprüft werden.

Dieses Buch dient der Orientierung in die vielfältige Welt der IT-Audits und unterstützt die Wissensaufnahme durch die Verbindung von Theorien, Standards und Best Practices sowie praktisch orientierten Prüfungsinhalten.

Bergisch Gladbach, im November 2014 Stefan Beißel

Inhaltsverzeichnis