

IT-Audit

Grundlagen
Prüfungsprozess
Best Practice

Von Dr. Stefan Beißel

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 15845 4](http://ESV.info/978_3_503_15845_4)

Gedrucktes Werk: ISBN 978 3 503 15845 4

eBook: ISBN 978 3 503 15846 1

Alle Rechte vorbehalten

© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2015

www.ESV.info

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: Hubert & Co., Göttingen

Vorwort

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 unterschätzten 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

KAPITEL I: GRUNDLAGEN	11
1	Definition des IT-Audits..... 11
2	Kategorien des IT-Audits 12
2.1	Kategorisierungsansätze 12
2.2	Prüfungsvollzug 13
2.3	Prüfungsumfang..... 18
2.4	Prüfungsaspekt..... 22
2.5	Prüfungsort..... 24
2.6	Prüfungszeit 27
2.7	Prüfungsanlass 30
3	Lebenszyklus des IT-Audits 34
3.1	Übersicht..... 34
3.2	Initiierung..... 34
3.3	Planung 35
3.4	Datenerhebung 35
3.5	Datenauswertung 36
3.6	Berichterstattung..... 36
3.7	Follow-up..... 37
4	Auditor..... 37
4.1	Rolle..... 37
4.2	Anforderungen 38
4.3	Aufgaben..... 42
4.4	Zertifizierungen 43
5	Stakeholder..... 56
6	Kontrollmaßnahmen 61
7	Nachweise..... 63
7.1	Kennzahlen 63
7.2	Indikatoren..... 64
7.3	Beweise..... 65
7.4	Indizien 66
KAPITEL II: VORBEREITUNG.....	67
1	Prüfungsauftrag 67
2	Prüfungsausschuss..... 68
3	Planung..... 69
3.1	Grundlagen..... 69

3.2	Planungsprozedur.....	76
4	Prüfungsstandards.....	77
4.1	Grundlagen.....	77
4.2	IDW	78
4.3	IFAC	79
4.4	IIA.....	80
4.5	ISACA	81
5	Regelwerke.....	82
5.1	Grundlagen.....	82
5.2	Gesetze.....	84
5.3	Standards.....	89
5.4	Best Practices.....	94
6	Prüfungskatalog.....	100
6.1	Überblick	100
6.2	Daten.....	102
6.3	Applikationen.....	118
6.4	Systeme.....	133
6.5	Netzwerke	146
6.6	Immobilien.....	156
6.7	Umwelt.....	165
6.8	Inventar	173
6.9	Prozesse	180
6.10	Projekte	188
6.11	Investitionen.....	194
6.12	Personen.....	200
7	Prüfungsumgebung.....	209
7.1	Grundlagen.....	209
7.2	Technische Eingrenzung.....	210
7.3	Organisatorische Eingrenzung.....	215
8	Technologietrends	217
8.1	Grundlagen.....	217
8.2	Cloud Computing.....	217
8.3	Soziale Netzwerke	220
8.4	Mobilität.....	223
8.5	Big Data	227
8.6	DevOps	230
KAPITEL III: DURCHFÜHRUNG		233
1	Erhebung	233
1.1	Inhaltsanalyse.....	233
1.2	Befragung.....	234
1.3	Beobachtung	236

2	Verfahren und Techniken	238
2.1	Stichprobenverfahren	238
2.2	Forensik	246
2.3	Computergestützte Audit-Techniken	247
2.4	Fuzzy Matching	249
3	Auswertung	250
3.1	Validierung	250
3.2	Ziffernverteilung	251
3.3	Hypothesentest	252
3.4	Feststellungen	254
4	Betrugserkennung	255
KAPITEL IV: ABSCHLUSS		259
1	Berichterstattung	259
2	Follow-up	261
LITERATUR		263
CHECKLISTE		269
INDEX		275