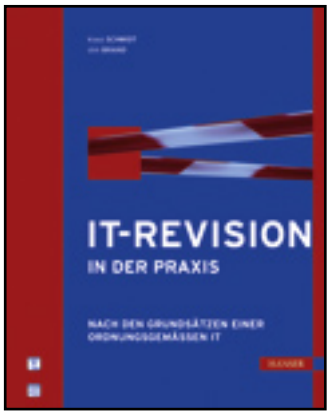
HANSER



Vorwort

Klaus Schmidt, Dirk Brand

IT-Revision in der Praxis

nach den Grundsätzen einer ordnungsgemäßen IT

ISBN: 978-3-446-41706-9

Weitere Informationen oder Bestellungen unter

http://www.hanser.de/978-3-446-41706-9

sowie im Buchhandel.

Vorwort

Die IT-Revision ist als Teil der internen Revision in den meisten größeren Unternehmen[1] ein etablierter Bestandteil der Unternehmensorganisation. Für viele im Unternehmen ist sie jedoch ein Buch mit sieben Siegeln. Zwar existiert für die funktionale Informationstechnik[2], d.h. Softwareprodukte, Netzwerktechnik usw. eine Fülle von Literatur, das Literaturangebot im Revisionsbereich hält sich jedoch in Grenzen und der Großteil der Revisionsliteratur bezieht sich eher allgemein auf die interne Revision und nicht speziell auf die IT-Revision. Das vorliegende Werk hat aus diesen Gründen zwei Intentionen:

- Zum einen soll dargestellt werden, was die IT-Revision ist, wie sie aufgebaut ist und wie sie arbeitet, um Personen einen Ein- und Überblick zu geben, die bislang noch keine Vorstellung von oder Berührung mit der IT-Revision hatten.
- Zum anderen sollen Mitarbeiter[3] der IT-Revision und andere Revisions-Insider methodische und inhaltliche Hinweise finden, die in der täglichen Revisionspraxis hilfreich sein können.

Dazu wurde das Buch in zwei Teile geteilt:

Teil I beschreibt das Wesen der IT-Revision und ihre Aufgabe: die Durchführung von Revisionsprüfungen. Nachdem in *Kapitel 1* auf die Grundlagen der IT-Revision eingegangen wurde, wird in *Kapitel 2* die Organisation von IT-Revisionsprüfungen beschrieben. Ein Punkt, der in Zusammenhang mit der Organisation steht, ist das Zusammenspiel zwischen der internen IT-Revision und externen Wirtschaftsprüfern, dies ist Thema von *Kapitel 3*. Einen Überblick über häufig verwendete Prüfungsgrundlagen bietet *Kapitel 4*, bevor in *Kapitel 5* dann die Prüfung von IT-Verfahren behandelt wird, eine der primären Aufgaben der IT-Revision. Sich dabei ergebende, besondere Prüfungsgebiete werden in *Kapitel 6*

---

[1] Wenn in diesem Buch von Unternehmen die Rede ist, sind damit in gleicher Weise auch andere Organisationen wie Behörden, Körperschaften usw. gemeint.

[2] Wenn in diesem Buch der Begriff Informationstechnik bzw. IT verwendet wird, ist damit in gleicher Weise die Kommunikationstechnik bzw. Telekommunikation (TK) gemeint. Auf vereinende Abkürzungen wie IuK oder ITK wurde weitgehend verzichtet. Sie wurden nur dort verwendet, wo es im Sinnzusammenhang notwendig erschien.

[3] Wenn bei personellen Bezeichnungen die männliche Form gewählt wurde (z.B. Mitarbeiter, Administrator), so ist damit in gleicher Weise die weibliche Form (Mitarbeiterin, Administratorin) gemeint.

vorgestellt, wobei es sich dabei angesichts der Breite von IT-Themen nur um eine kleine Auswahl handeln kann. Einer speziellen Art von IT-Revisionsprüfungen, der Prüfung nach dem CobIT-Standard, wurde mit *Kapitel 7* ein eigenes Kapitel gewidmet. *Kapitel 8* schließlich rundet den ersten Teil mit Betrachtungen zum Tooleinsatz in der IT-Revision ab.

Teil II besteht aus den Grundsätzen für eine ordnungsgemäße Informationstechnik (GoIT). Diese Grundsätze sind in Form von Anforderungen formuliert, die in sechs logisch gegliederte Bereiche („Schichten") aufgeteilt sind.

Dieser „Anforderungskatalog" soll Hilfestellungen für IT-Revisoren bei der Durchführung von IT-Revisionsprüfungen bieten. Zum einen lassen sich aus den in den Anforderungen aufgeführten Prüfungsfragen Checklisten für die Prüfungen erstellen, zum anderen wird die Argumentation gegenüber den geprüften Bereichen unterstützt (z.B. durch die Verweise auf die Vorgaben oder auf die potenziellen Folgen der Nichterfüllung).

Ergänzend zu diesem Buch haben die Autoren eine **tabellarische Arbeitshilfe** in Microsoft Excel erstellt. Um sie zu erhalten, gehen Sie wie folgt vor:

1. Rufen Sie in Ihrem Webbrowser die Adresse *http://downloads.hanser.de* auf.
2. Geben Sie im Suchfeld die ISBN dieses Buches (978-3-446-41706-9) oder einen der Autorennamen oder den Titel an.
3. Laden Sie sich die Datei mit dem Namen „GoIT.xls" herunter.

Danksagungen

Genau wie ein Film nicht nur vom Regisseur gemacht wird, ist dieses Buch nicht nur von den Autoren geschrieben worden. Daher möchten wir uns bei allen bedanken, die zum Entstehen und Gelingen dieses Buches beigetragen haben, und dies seit dem Tag, an dem ein Projekt bei einer Versicherung in Wiesbaden den Anstoß zu diesem Buch gab.

An erster Stelle ist hier unsere Lektorin Frau Metzger zu nennen, die mit viel Geduld und Mühe den Entstehungsprozess begleitete, sowie unsere Familien, die uns in dieser Zeit oft entbehren mussten. Dank sei dem Institut für interne Revision (IIR), sowie Frau Gabriele Rinke und Herrn Ralf Kapitulski von der Delta Lloyd Deutschland für so manchen guten Hinweis.

Zu erwähnen sind noch Benedikt Kisner und Patrick Kruse, die Zeit und Ressourcen zur Verfügung gestellt haben, das NETGO Systemhaus für die technische Unterstützung und Markus Olbring und Dennis Siegert für ihre Tipps und Tricks. Dirk Brand möchte ausdrücklich seinem ehemaligen Professor Herrn Dr. Kruse danken, ohne dessen Kommentare er seinen beruflichen Werdegang nicht so erfolgreich hätte gehen können.

Ebenso danken wir allen anderen, die in Gesprächen und Diskussionen einen Beitrag zu diesem Buch geleistet haben. Allen, die konstruktive Kritik geübt und Hinweise gegeben haben: Ein herzliches Dankeschön dafür!

Neuhof und Borken, im Herbst 2010

Klaus Schmidt und Dirk Brand

Die Autoren

Dipl.-Inform. Klaus Schmidt
ist Geschäftsführer der Innomenta GmbH & Co. KG, die Unternehmen in IT-Themen an der Schnittstelle zwischen Management und Technik unterstützt (IT-Revision, Security Management, Identity Management). Er ist Mitbegründer des ValueProtect-Konsortiums mit der Zielrichtung einer ganzheitlichen Sicherheit.

Zahlreiche Publikationen, Seminare, die Ausbildung von Security Managern und ein Lehrauftrag an der Hochschule Fulda ergänzten bislang seine Tätigkeit, für die er Zertifizierungen zum Information Security Manager (CISM) und zum ISO27001-Trainer erlangt hat.

Dirk Brand
ist leitender Berater bei der SILA Consulting GmbH mit den Schwerpunkten IT-Revision und Informationssicherheitsmanagement nach nationalen und internationalen Standards, sowie Mitbegründer des ValueProtect-Konsortiums mit der Zielrichtung einer ganzheitlichen Sicherheit.

Seminare zu den Themen Informationssicherheit und die Ausbildung ergänzen seine Tätigkeit, für die er Zertifizierungen zum TeleTrust Information Security Professional (T.I.S.P) und ISO27001-Trainer erlangt hat.