Revision der IT-Governance mit CoBiT

Leitfaden für die Prüfungspraxis

Von
Stefan Tönnissen

ERICH SCHMIDT VERLAG

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

Weitere Informationen zu diesem Titel finden Sie im Internet unter
ESV.info/978 3 503 13012 2

Gedrucktes Werk: ISBN 978 3 503 13012 2
eBook: ISBN 978 3 503 13013 9

Dieses Papier erfüllt die Frankfurter Forderungen
der Deutschen Bibliothek 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

Geleitwort von Prof. Dr. Hufnagel

Mit dem im Mai 2009 in Kraft getretenen BilMoG ist sowohl der Vorstand als auch der Aufsichtsrat verpflichtet, die Angemessenheit eines wirksamen internen Kontrollsystems sicherzustellen. In der Gesetzesbegründung wird explizit darauf hingewiesen, dass sich die Überwachungsfunktion nicht nur auf die Rechnungslegung bezieht, sondern auch auf die Internen Kontrollen der Informationstechnologie.

Die Unternehmen sind gegenüber dem Gesetzgeber und Wirtschaftsprüfern gefordert, diese notwendige Wirksamkeit des internen Kontrollsystems für die Informationstechnologie nachzuweisen. Doch wie kann die Wirksamkeit eines internen Kontrollsystems für die Informationstechnologie gegenüber Wirtschaftsprüfern nachgewiesen werden?

Stefan Tönnissen greift in seinem Fachbuch diese Problematik auf und zeigt einen auf dem international anerkannten Standard CoBiT basierten Prüfungskatalog aus verschiedenen Perspektiven auf. Der Standard CoBiT lehnt sich stark an COSO an und erfüllt damit die Anforderungen an ein wirksames Kontrollsystem für Informationstechnologie.

Dieser Prüfungskatalog ist in der betrieblichen Praxis als Revisor eines mittelständischen Konzerns entstanden und somit aus der Praxis für die Praxis.

Dieses Fachbuch stellt eine wertvolle Hilfe für den Revisor oder Prüfer zur Prüfung der Informationstechnologie und IT-Governance in den Unternehmen dar.

Münster, im Januar 2011

Prof. Dr. Wolfgang Hufnagel
Leiter Verbundstudiengänge Fachhochschule Münster

Vorwort

Unsere Wünsche wachsen mit den Schwierigkeiten, denen sie begegnen.

- Michel Eyquem de Montaigne -

Der Wunsch nach einem Prüfungskatalog für IT-Governance entstand bei der Aufgabe, als neuer Mitarbeiter in der Konzernrevision eines mittelständischen Konzerns die Informationstechnologie prüfen zu müssen. Es gab eine große Zahl von vorhandenen Prüfungskatalogen, Richtlinien, Prüfungsstandards und Verfahrensanweisungen. Jede davon erlaubte einen sehr speziellen Blick auf einen spezifischen Sachverhalt der Informationstechnologie.

Mir fehlten jedoch der Überblick und eine Möglichkeit, die Informationstechnologie in ihrem Lebenszyklus und ganzheitlich zu erfassen. Meine Recherchen beim Deutschen Institut für Interne Revision und bei Wirtschaftsprüfungsgesellschaften führten mich sehr schnell zu einem international anerkannten Referenzmodell zur Entwicklung und Prüfung der IT-Governance, CoBiT.

Common Objectives for Information and related Technology (CoBiT) ist 1994 entstanden durch eine Initiative von IT-Revisoren und wurde im Laufe der Jahre weiterentwickelt zu einem Rahmenmodell für IT-Governance mit 34 IT-Prozessen.

Somit findet der Prüfungsneuling als auch der erfahrende Prüfer in diesem Buch eine Anleitung vor, mit der die IT-Governance ganzheitlich und nach einem international anerkannten Standard geprüft und bewertet werden kann. Dabei wird auf die verschiedenen Perspektiven der IT-Prüfung eingegangen und ein sofort einsetzbarer Prüfungskatalog für jede Perspektive aufgezeigt.

Ein Fachbuch „Aus der Praxis – für die Praxis“ schreibt sich vielleicht von alleine, die inhaltliche Gestaltung bedarf jedoch einer umfangreichen fachlichen Diskussion mit am Thema betroffenen oder mit dem Thema vertrauten Fachleuten.

Danken möchte ich an dieser Stelle meinen Arbeitskollegen Dieter Oskamp und Ernst Sybon der Konzernrevision der Schmitz Cargobull AG. Beide Kollegen haben einen großen Anteil am Gelingen dieses Buches. Der Anspruch dieses Buches, einen

Prüfungskatalog für IT-Governance aus der Praxis für die Praxis zu erstellen, konnte nur durch den konstruktiven Dialog mit den beiden Kollegen gelingen.

Frau Brand-Noé danke ich für die Erlaubnis, die in Ihrem hervorragenden Buch „Revision des Personalbereich“ dargestellte Idee der Prüfungslandkarten in mein Buch übernehmen zu dürfen.

Des Weiteren möchte ich Herrn Prof. Dr. Hufnagel und Dipl.-Betriebswirtin Ruth Kühn M.A. von der Fachhochschule Münster für Ihre vielen Anregungen und Ideen für diese Arbeit während meiner berufsbegleitenden Studienzeit am Institut für Technische Betriebswirtschaft danken.

Zu guter Letzt möchte ich Frau Splittgerber und Frau Ludwig vom Erich Schmidt Verlag für die tolle Zusammenarbeit im Rahmen der Erstellung dieses Buches danken.

Ich wünsche Ihnen viel Erfolg bei der IT-Prüfung mit CoBiT und den in diesem Buch dargestellten Prüfungskatalogen. Mögen diese Prüfungskataloge Ihnen den Einstieg in die IT-Prüfung erleichtern und viele neue Ideen generieren.

Wettringen, im Januar 2011 Stefan Tönnissen

Inhaltsverzeichnis