

Die minimalen Informatik-Kontrollen im Rahmen einer Abschlussprüfung

Von Hans Mäder

(Freie Übersetzung des Artikels «The Minimum IT Controls to Assess in a Financial Audit» von Tommie W. Singleton)

Bestimmte Bereiche der Informations- und Kommunikationstechnologie (IT) – die generellen IT-Kontrollen – betreffen beinahe alle Abschlussprüfungen, einfach weil die Informatik-Systeme heute allgegenwärtig und für die finanzielle Berichterstattung relevant sind. Fehlerhafte IT-Prozesse können durch ihren wesentlichen Einfluss auf die Verarbeitung der Finanzinformationen zu einer wesentlichen Falschaussage in der Jahresrechnung führen.

Aber nicht alle Informatik-Prozesse sind automatisch relevant für die Abschlussprüfung und es ist nicht ganz einfach, unter all den IT-Risiken jene herauszufiltern, welche für die externe Revision wesentlich sind. Unerfahrene IT-Revisionen, vor allem solche mit einem IT-Hintergrund, neigen dazu, den Blickwinkel des Audit auf nicht finanzrelevante IT-Probleme auszuweiten.

Kategorisierung der IT eines Unternehmens

Bei der korrekten Ausrichtung eines IT-Audit für die Abschlussprüfer ist zunächst relevant, wie hoch die Abhängigkeit einer Unternehmung von ihrer IT-Abteilung ist. Je grösser diese Abhängigkeit, desto höher muss auch der Reifegrad der IT-Umgebung sein. Der Einfachheit halber beschränkt sich das hier vorgestellte Modell auf drei Kategorien: tief, mittel und hoch. Offensichtlich fallen Unternehmen nicht einfach in die eine oder andere Kategorie, sondern sind je nach IT-Bereich ein bisschen von Allem. Trotzdem: Mit ausreichender Berufserfahrung lassen sich die Firmen einer Kategorie zuweisen.

Diese Typisierung erleichtert einem Revisionsexperten die Entscheidung, ob ein spezialisierter IT-Auditor beizuziehen ist. Das Modell beschreibt anhand verschiedener Eigenschaften den Reifegrad der IT-Umgebung:

	1: Tief	2: Mittel	3: Hoch
Anzahl Server	1	2–3	>3
Netzwerk	Peer to Peer	Domäne	Mehrere Domänen
Anzahl Benutzer	1–15	16–30	>30
Finanzrelevante Programme	Standard-Programme	Konfiguriertes ERP	Komplexes ERP
Standorte	1	3	>3
Automatisierte Kontrollen	keine	wenige standardisiert	viele, selbst programmiert
IT-Entwicklung	kaum	moderat	stürmisch
Anzahl online-Transaktionen	wenige	viele	sehr viele verschiedene

Unternehmen mit einem tiefen Reifegrad stützen sich nur wenig auf ihre IT-Systeme, die Abhängigkeit von der Informatik ist gering. Folglich müssen auch keine IT-Prüfer beigezogen werden. In allen übrigen Fällen hingegen ist der Beizug eines Spezialisten (beispielsweise eines CISA) empfehlenswert.

Fünf relevante IT-Kontrollen

Für die Abschlussprüfer sind fünf IT-Kontrollen relevant, die von der Fachwelt als die sogenannten «generellen IT-Kontrollen» bezeichnet werden:

- Die unternehmensweiten Kontrollen
- Änderungsmanagement
- Informationssicherheit
- Datensicherung und -rettung
- Outsourcing

Der IT-Prüfer verschafft sich im ersten Schritt ein ausreichendes Verständnis der für das Rechnungswesen relevanten IT-Systeme. Dazu gehört auch die Prüfung der Governance, der Strategien, der Abläufe und selbstverständlich des Risiko-Managements – immer mit Bezug auf die Informatiksysteme. Gleichzeitig erarbeitet sich der Prüfer auch einen Überblick über die IT-relevanten Instrumente der Internen Kontrolle (IKS). Die Resultate der Prüfungen unterstützen den Revisor bei der risikoorientierten Prüfungsplanung. Um den Revisor bei der Einschätzung des Kontrollrisikos zu unterstützen (gemäss PS 400), muss sich der IT-Auditor auch ein ausreichendes Verständnis der generellen IT-Kontrollen erarbeiten. Die notwendigen Prüfungshandlungen sind in Fachstandards wie COBIT beschrieben und sollen an dieser Stelle nicht weiter vertieft werden. Zu beachten ist ferner, dass die obenstehenden Kontrollen auch Teil der IKS-Prüfung gemäss PS 890 sind, wobei dieser Prüfungsstandard zusätzlich eine hinreichende Dokumentation verlangt.