



DRUM PRÜFE, WER SICH TECHNISCH BINDET, OB TRANSPARENZ SICH IN DER TECHNIK FINDET

Die interne IT-Revision auf dem Weg zur Management Support-Funktion

Von Klaus Schmidt

Das Thema IT-Revision wird in vielen Unternehmen immer noch als lästiges Übel gesehen. Die interne IT-Revision wird nicht selten als Vorauskommando betrachtet, das dafür sorgen soll, dass es bei externen Prüfungen keine großen Probleme gibt. Dazu wird die Rechtmäßigkeit, die Ordnungsmäßigkeit und die Sicherheit der Informationstechnik und ihrer Anwendung geprüft. Doch die interne IT-Revision kann noch mehr: Mit entsprechendem Know-how ausgerüstet, ist sie als eine von der Linie unabhängige Instanz sehr gut geeignet, um dem Management ein ungeschöntes Bild vom Zustand der aktuellen IT (Technik, Organisation, Management, Prozesse) zu geben und dort, abseits von gesetzlichen Anforderungen, Schwächen aufzudecken, zu deren Behebung sie beratend zur Seite steht. Dazu wird vor allem eines benötigt: Transparenz.

Keine Frage: Die Kontrolle der Ordnungsmäßigkeit und Sicherheit im Unternehmen bildet den Kern der internen Revisionstätigkeit, schließlich ist der Schutz des Unternehmens vor negativen Auswirkungen (Bestrafung, Schäden, finanzielle Einbußen, usw.) ein Hauptziel der Prüfungsaufträge für die Revision. Für Unternehmen, die sich als kontinuierlich verbessernde Organisationen begreifen, reicht dies jedoch nicht aus. Aus diesem Grund sollen durch risikoorientierte Prüfungen der IT-Revision die Ergebnisse des IT-Risiko- und Sicherheitsmanagements verifiziert oder eigenständig IT-Risiken identifiziert werden. Ungereimtheiten, Auffälligkeiten, Schwächen und



Zur Person

Klaus Schmidt ist seit 2001 Geschäftsführer der Innomenta GmbH & Co. KG, die Unternehmen in den Themen IT-Revision und Informationssicherheit unterstützt.

Nach dem Studium der angewandten Informatik und Mathematik stieg er in das Consulting ein und übernahm nach einiger Zeit den Bereich Risk Management einer Unternehmensberatung in Heidelberg.

Er ist zertifizierter Security Manager, Buchautor, Seminarleiter des Management Circle, hat einen Lehrauftrag an der Hochschule Fulda und verfügt über zahlreiche Veröffentlichungen in den oben genannten Fachgebieten.

Lücken sollen gefunden und kommuniziert werden, auch wenn sie kein Risiko bilden. Das Management möchte eine interessensfreie Einschätzung, wie gut die eigene IT im Vergleich zu anderen Unternehmen, dem Branchendurchschnitt, Standards oder Best-Practice Ansätzen ist und wo Verbesserungspotenziale zur Erhaltung und Erhöhung der Leistungsfähigkeit des Unternehmens liegen. Ebenso wird eine Aussage erwartet, welche Kontrollen in Technik und Prozessen verankert sind und wie wirksam und effizient das von ihnen gebildete interne Kontrollsystem (IKS) arbeitet.

Neue Prüfkriterien

Um die o.a. Aussagen zu gewinnen, ist es notwendig, das Spektrum der Revisionsprüfungen zu vergrößern. Es kommen weitere Prüfungskriterien hinzu, die darauf abzielen, die IT-Revision zu nutzen, um die IT intern zu bewerten. Dies sind insbesondere:

- **Zweckmäßigkeit**

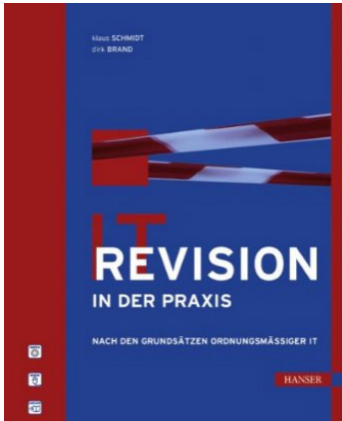
Die Zweckmäßigkeit gibt an, inwieweit die Prüfobjekte ihrer Bestimmung gerecht werden. Sie besteht aus der Funktionserfüllung (Die IT liefert termingerecht inhaltlich richtige und vollständige Ergebnisse), der Effektivität (Die IT ist dazu geeignet, den ihr zugeordneten Zweck zu erfüllen) und der Ziel- und Strategiekonformität (Die IT stimmt mit der IT- und Geschäftsstrategie überein und unterstützt die Erfüllung der an sie gestellten Ziele).

- **Wirtschaftlichkeit**

Auch wenn das Prüfobjekt ordnungsgemäß, sicher und zweckmäßig arbeitet, so kann die Einhaltung dieser Kriterien mit einem unverhältnismäßig hohen Aufwand erkauft worden sein oder das Anforderungsniveau ist so niedrig, dass Ressourcen verschwendet werden. Die Wirtschaftlichkeit als Verhältnis zwischen dem Mitteleinsatz und dem damit erzielten Ergebnis gibt entsprechend Auskunft darüber, wie rationell die Ergebnisse von der IT erbracht werden.

- **Kontrollierbarkeit**

Die Kontrollierbarkeit sagt aus, inwieweit die Statik (Struktur, Merkmale) und die Dynamik (Abläufe) eines Prüfobjekts nachvollzogen und mit festgelegten Vorgaben verglichen werden können. Sie bildet die Grundlage für die Prüfbarkeit der anderen genannten Kriterien.



Mehr zum Thema IT-Revision findet sich im neuesten Buch von Klaus Schmidt, das den Titel „IT-Revision in der Praxis“ trägt und im Hanser-Verlag erscheinen wird.

Darin findet sich mit den Grundsätzen einer ordnungsgemäßen IT (GoIT) auch eine Anforderungssammlung für die Revisionspraxis.

- **Konformität**

Immer mehr rücken Standards wie ISO27001, COBIT oder ITIL in den Fokus der Unternehmens-IT. Mit der Erfüllung von Standards soll eine gewisse Reife der IT erreicht und auch ausgewiesen werden. Die Prüfung, ob die IT die Standards erfüllt, die sie erfüllen soll, kann durch die IT-Revision erfolgen. Die Konformität mit den Standards kann dabei explizit als Prüfungsauftrag formuliert werden oder die Standards werden als Unternehmensrichtlinie erklärt und stellen damit Prüfungsgrundlagen für die IT-Revision dar.

Bei jedem dieser Kriterien ist zu definieren, auf welche Weise (Metrik, Vorgehen) es gemessen werden soll. Nach der Ermittlung des aktuellen Zustands gibt die IT-Revision eine Einschätzung des Reifegrades, eine Übersicht der Defizite und entsprechende Verbesserungsvorschläge. Dazu kann sie bestehende Standards wie COBIT oder ITIL heranziehen.

Ohne Transparenz ist alles nichts

Besonders für die Beurteilung der Wirtschaftlichkeit und Kontrollierbarkeit ist die Transparenz der IT entscheidend. Der Begriff wird in der IT doppeldeutig gebraucht: Neben der für die IT-Revision wichtigen Bedeutung, dass die Beschaffenheit eines Prüfobjekts (IT-Architektur, IT-Prozesse, usw.) ohne spezielle Mittel (z.B. Spezialwissen von einzelnen Personen) vollständig, klar und eindeutig ermittelt werden kann, bezeichnet er auch IT-Funktionen, die für bestimmte IT-Objekte nicht „sichtbar“ sind (z.B. ist eine Verschlüsselung auf Netzwerkebene für die IT-Anwendungen transparent). Das Erreichen von Transparenz in der IT ist ein wichtiges Qualitätsmerkmal der IT und sollte eine grundsätzliche und durch die IT-Revision zu prüfende Anforderung des Managements an die Unternehmens-IT sein. Je nach betrachtetem Objekt bzw. Aspekt unterscheidet man dabei zwischen Organisations-, Struktur-, Leistungs-, Prozess- und Kostentransparenz.

Prüfung der Organisationstransparenz

Die Beurteilung der Organisationstransparenz beginnt beim Organisationsmodell der IT. Ist vollständig, klar und eindeutig definiert und dokumentiert, welche Verantwortlichkeiten und Zuständigkeiten in der IT benötigt werden bzw. bestehen sollen und welche in der Praxis tatsächlich bestehen? Der Autor erlebte einmal den Fall, dass einige Zuständigkeiten nur auf dem Papier existierten, um einem Prozessmodell Genüge

zu tun, dass neu eingeführt wurde. Ist zudem vollständig, klar und eindeutig definiert und dokumentiert, was die Verantwortlichkeiten und Zuständigkeiten beinhalten? Wird dies gepflegt? Wie wird sichergestellt, dass es so gelebt wird, wie es definiert wurde? Ist dokumentiert, welche Personen welche Verantwortlichkeiten und Zuständigkeiten besitzen (Stellenübersicht, Rollenbeschreibungen, usw.)? Ist kenntlich gemacht, welche Verantwortlichkeiten und Zuständigkeiten einer Funktionstrennung unterliegen müssen? Dies sind einige Fragen, mit denen die IT-Revision prüfen kann, inwieweit die Organisationstransparenz gegeben ist oder nicht.

Prüfung der Strukturtransparenz

Eine moderne Unternehmens-IT besteht, besonders in Großunternehmen, in technischer Hinsicht in den meisten Fällen in einer mehrschichtigen, heterogenen und meist verteilten IT-Architektur, in der eine Vielzahl von technischen Konzepten anzutreffen ist. Und obwohl man meinen mag, dass Transparenz hier oberstes Gebot ist, sieht die Praxis in manchen Fällen ganz anders aus: In einem Handelsunternehmen fiel dem Autor im Zuge einer Inventarisierung auf, dass nicht transparent war, welche IT-Anwendungen auf welchen Servern betrieben wurden und in welchen Netzen und geografischen Standorten die für diese Anwendungen relevanten Server zu finden sind. In einem Telekommunikationsunternehmen forderte der Autor bei einer Business Impact-Analyse die Netzwerkübersicht an. Am Ende lagen fünf (!) inkonsistente Netzwerkübersichten auf dem Tisch und auf die Frage, wie denn die Realität nun tatsächlich aussähe, herrschte zunächst betretenes Schweigen.

Mit neuen Konzepten wie z.B. die Virtualisierung von Servern oder die Zerteilung monolithischer Anwendungen in kleine, universale Funktionsblöcke (z.B. Webservices) wird die Herstellung der Strukturtransparenz indes nicht gerade leichter. Hier kann die IT-Revision folgende Prüfungsfragen stellen: Welche IT-Objekte sind vorhanden? Welche IT-Objekte werden innerhalb von welchen IT-Verfahren durch die Organisationseinheiten genutzt? Wie sind die Objekte auf den Architekturebenen (Physik, Netzwerk, System, Anwendung/Dienst, Inhalt) verschaltet? Wie ist dies dokumentiert? Wie wird sichergestellt, dass Dokumentationen aktuell, konsistent und inhaltlich korrekt sind?

Prüfung der Leistungstransparenz

Eine IT-Leistung ist eine von der Unternehmens-IT erbrachte Funktion. Diese Funktion kann eine Fachaufgabe erfüllen bzw. unterstützen oder sich wiederum auf die IT beziehen (z.B. Verschlüsselung einer elektronischen Kommunikation). Jede Leistung hat

Leistungsparameter, welche die Leistung in Art, Umfang, Höhe usw. definieren (z.B. Stärke oder Geschwindigkeit der angesprochenen Verschlüsselung). Da die Erbringung einer Leistung in einer bestimmten Ausprägung Kosten verursacht (eine schnellere Verschlüsselung kostet auch mehr), werden die Leistungsempfänger (z.B. eine Fachabteilung) nur die Leistungen beziehen wollen, die sie für ihre Aufgaben benötigen (Beachtung der Wirtschaftlichkeit).

Daraus ergeben sich für die IT-Revision folgende Prüfungsfragen: Gibt es einen Überblick über die Leistungen, die von der IT erbracht werden? Welche Ausprägungen existieren für die einzelnen Leistungen? Ist ersichtlich, welche Leistungen sinnvoll (evtl. auch synergetisch) miteinander kombinierbar sind? Wie wird ermittelt, protokolliert und kommuniziert, welche Leistungen von den Leistungsempfängern bezogen werden? Kann vollständig, klar und eindeutig nachvollzogen werden, wie die einzelnen Leistungen erstellt werden und welche Organisationseinheiten, Prozesse und IT-Objekte daran beteiligt sind? Oder andersherum: Ist zu jeder IT-Leistung transparent, von welchen Organisationseinheiten, Prozessen und IT-Objekten sie abhängt (dies ist auch für die IT-Sicherheit von Bedeutung)?

Prüfung der Prozesstransparenz

Transparenz schaffen hilft, IT-Schwächen aufzudecken, bevor es die Betriebsprüfung tut



Die IT eines Unternehmens besteht neben der eigentlichen Informationstechnik (Server, Netze, usw.) aus der schon angesprochenen IT-Organisation, dem IT-Management und den IT-Prozessen. Letztere lassen sich analog zum IT-Lebenszyklus grob in Planungs-/ Implementierungs-, Betriebs-, Störungs- und Änderungsprozesse einteilen. Die Prozesstransparenz wird in diesen Prozessen besonders für das Prüfungskriterium der Sicherheit benötigt.

Folgende Prüfungsfragen kann die IT-Revision in diesem Zusammenhang stellen: Existiert eine Prozesshierarchie für die IT-Prozesse und ist vermerkt, wie die Prozesse zusammenspielen (Prozessein-, aus- und Übergänge)? Ist für jeden Prozess dokumentiert,

Folgende Prüfungsfragen kann die IT-Revision in diesem Zusammenhang stellen: Existiert eine Prozesshierarchie für die IT-Prozesse und ist vermerkt, wie die Prozesse zusammenspielen (Prozessein-, aus- und Übergänge)? Ist für jeden Prozess dokumentiert,

welche Instanzen (Organisationseinheiten, externe Partner, o.ä.) am Prozess beteiligt sind und aus welchen Prozessschritten in welcher Abfolge er besteht? Ist ersichtlich, an welchen Stellen Alternativen bestehen, Entscheidungen getroffen werden, Zuarbeit benötigt wird, usw.? Sind die Verantwortlichkeiten für einzelne Schritte bzw. Prozess-teile eindeutig festgelegt?

Prüfung der Kostentransparenz

Bei der Leistungstransparenz wurde der Kostenaspekt bereits kurz erwähnt. Er ist für die Prüfung der Wirtschaftlichkeit von besonderer Bedeutung und ist ein wichtiger Faktor für die Erfolgsmessung. In der Praxis kommen verschiedene Kostenmodelle, -verfahren und -philosophien (z.B. Prozesskostenrechnung, TCO, o.ä.) zum Einsatz, die bei der Prüfung der Kostentransparenz adäquat berücksichtigt werden müssen. Eine grundsätzliche Forderung der Kostentransparenz ist es, dass die Kostenherkunft nachvollziehbar sein muss. Die Kostenquellen und die kostenbestimmenden Faktoren (Kostentreiber) müssen identifiziert sein. Dazu gehören neben den Kosten des Regelbetriebs auch außergewöhnliche Kosten wie die Kosten von Störungen und Ausfällen.

Für die IT-Revision ergeben sich folgende Prüfungsfragen: Sind die Kosten für jede erbrachte IT-Leistung nachvollziehbar, d.h. ist ihre Zusammensetzung und ihre Herkunft (Kostenquellen, Kostentreiber) bekannt? Sind die Kosten in Höhe und Struktur plausibel, halten sie einem Fremdvergleich stand? Wie fließt die Betrachtung des Kostenaspekts in IT-Planungen ein? Wie werden die Kosten erhoben und wie kontrolliert? Wie werden die Kosten, sowie die Kostensituation und deren Entwicklung dokumentiert? Gibt es ein Kostenmanagement für die Unternehmens-IT, das die Kosten in ihrer Entwicklung überwacht und, soweit möglich, die Kostensituation kontinuierlich verbessert (KVP)?

Fazit

Die IT-Revision kann neben ihrer klassischen Aufgabe der Prüfung von Ordnungsmäßigkeit und Sicherheit mit der Prüfung weiterer Kriterien auch einen wichtigen Beitrag zur Erhöhung von Qualität, Reife und Wirtschaftlichkeit der IT liefern. Ein entscheidender Faktor für die Prüfbarkeit dieser Kriterien ist angesichts der steigenden Komplexität in der IT die Erzielung einer aufwandsminimierten Transparenz in der Technik, den Prozessen und der Organisation der IT.