HANSER

Leseprobe

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.

1 Grundlagen der IT-Revision

Dieses Kapitel soll Sie in die Welt der IT-Revision einführen. Dazu ist zunächst zu klären, was unter Revision zu verstehen ist, und damit auch, was eine Revisionsabteilung tut und welche Ziele und Aufgaben sie besitzt. Ebenfalls zu den Grundlagen gehört die Frage, wie eine solche IT-Revision im Unternehmen eingebettet ist und wo Berührungspunkte mit anderen Abteilungen bzw. Bereichen existieren.

1.1 Das Wesen der IT-Revision

Befragt man das beliebte Online-Lexikon Wikipedia nach dem Stichwort „Revision“, so bekommt man die Auskunft, dass sich der Begriff aus dem Verb *revidieren* ergibt, das sich aus dem lateinischen „re“ (Rückschau oder Überprüfung) und „videre“ (ansehen) zusammensetzt. Schon aus dem Begriff „IT-Revision“ ergeben sich damit drei wichtige Eigenschaften:

- *Die IT-Revision konzentriert sich auf Dinge der Informationstechnik.*
  Sie beschäftigt sich mit Dingen, die im Zusammenhang mit der Gestaltung, dem Betreiben, dem Management oder der Nutzung der Informationstechnik stehen. Diese Dinge können sehr unterschiedlicher Natur sein, z.B. Vorgänge (Migration eines Software-Systems) oder Objekte (z.B. ein Rechenzentrum).
- *Die IT-Revision schaut sich diese Dinge im Unternehmen an und prüft sie.*
  Das Anschauen besteht zunächst darin, den bestehenden Zustand festzustellen. In einem zweiten Schritt wird geprüft, ob dieser Zustand die Vorgaben erfüllt bzw. einhält, die von externen Instanzen (Gesetzgeber, Aufsichtsbehörden usw.) oder vom Unternehmen selbst gestellt werden. Diese Prüfung ist die zentrale Tätigkeit der Revision.
- *Die IT-Revision schaut sich die Dinge nachträglich an.*
  Im Fokus der IT-Revision liegen die Dinge, die bereits geschehen sind und damit ein Faktum darstellen, und nicht Dinge, die geschehen werden oder könnten[1].

[1] Damit ist die Prüfung bzw. Untersuchung zukünftiger Dinge gemeint, nicht das Ausblenden zukünftiger Entwicklungen, denn die IT-Revision macht sich sehr wohl Gedanken darüber, was aufgrund des bestehenden Zustandes in Zukunft geschehen könnte.

Bisher noch unbeantwortet ist die Frage, warum es die Revision überhaupt gibt. Die oben erwähnten Vorgaben werden schließlich an die Fachbereiche gestellt und müssen von ihnen erfüllt bzw. eingehalten werden. Doch da beginnen die Probleme: Nicht selten wissen die Fachbereiche gar nicht, welche Vorgaben sie erfüllen müssen. Das gilt insbesondere dann, wenn Fachbereiche IT-Themen bearbeiten und nicht mit den Anforderungen an die Informationsverarbeitung vertraut sind.

Praxistipp

Veranstalten Sie kurze Info-Workshops in den Fachbereichen und erläutern Sie den Fokus der bestehenden Soll-Vorgaben für die IT. Als Teilnehmer kommen alle Personen in Frage, die im Fachbereich mit IT-Aufgaben betraut sind.

Selbst wenn die Vorgaben bekannt sind, heißt das nicht, dass sie auch erfüllt werden, denn das primäre Interesse der Fachbereiche liegt woanders. Um die Konformitäten zu kontrollieren, wird daher eine von der Linie unabhängige Instanz wie die Revision benötigt.

1.1.1 Ziele der IT-Revision

Welche Zwecke verfolgt nun die IT-Revision? In der Regel sind es folgende Zielsetzungen, die sich die IT-Revision selbst gibt oder die vom Top-Management[2] vorgegeben werden:

Schutz des Unternehmens vor Bestrafung

Eines der primären Ziele der Revisionstätigkeit liegt darin sicherzustellen, dass das Unternehmen nicht dafür belangt werden kann, dass gesetzliche oder aufsichtsrechtliche Vorgaben nicht eingehalten werden. Dies gilt insbesondere für strafrechtlich relevante Handlungen, die beispielsweise durch Missbrauch der Informationstechnik vorgenommen werden.

Schutz des Unternehmens vor Schäden

Es ist Aufgabe der Managementebene, das Unternehmen vor Schäden zu schützen. Jedes größere Unternehmen sollte dazu ein Risiko- und Sicherheitsmanagement einrichten. Große Kapitalgesellschaften sind dazu durch das Gesetz der Kontrolle und Transparenz im Unternehmensbereich (KonTraG) sogar gesetzlich verpflichtet.

Die IT-Revision kann ein solches Sicherheitsmanagement unterstützen, indem sie prüft, ob es in den Fachbereichen Abweichungen von den internen und externen Sicherheitsrichtlinien gibt, die zu Schäden im Unternehmen führen können. Ziel ist es, die Entstehung der Schäden rechtzeitig mit entsprechenden Maßnahmen zu verhindern.

Die Betrachtung ist allerdings begrenzt auf die Abweichungen von den Richtlinien. Schädliche Entwicklungen, die andere Ursachen haben, können von der IT-Revision nicht er-

[2] Unter dem „Top-Management“ wird hier und im Folgenden die oberste Leitungsebene verstanden, z.B. Vorstand einer AG, Geschäftsführung einer GmbH usw.

kannt werden. Deshalb kann das Unternehmen nicht auf ein Sicherheitsmanagement verzichten und sich alleine auf die IT-Revision verlassen.

Berücksichtigung von berechtigten Interessen Dritter

Unter dem berechtigten Interesse von Dritten sind alle Verpflichtungen gegenüber Geschäftspartnern, Kunden, Lieferanten, der Öffentlichkeit usw. zusammengefasst. Diese sind in der Regel vertraglich festgelegt, anderweitig vereinbart oder ergeben sich aus allgemeinen Grundsätzen.

Auf der einen Seite wird in Prüfungen der IT-Revision kontrolliert, ob die bestehende Situation im geprüften Bereich gegen Verträge und Vereinbarungen verstößt. Auf der anderen Seite wird gleichzeitig geprüft, ob die betrachteten Dritten (Vertragspartner etc.) ihrerseits in der bestehenden Situation den vereinbarten Pflichten nachkommen.

Auch die Vereinbarungen selbst sind meist Bestandteil der Prüfung. So wird untersucht, ob die Verträge bzw. Vereinbarungen Passagen enthalten, die gegen das berechtigte Interesse des Unternehmens gerichtet oder gar für das Unternehmen nicht hinnehmbar sind. In diesem Fall wird also nicht nur gegen die Vorgaben (Vertrag/Vereinbarung) geprüft, die Vorgabe selbst wird gegen das Unternehmensinteresse und allgemeine Vertragsgrundsätze geprüft.

Identifizierung von Gefährdungen und Risiken

Ähnlich wie beim Schutz vor Schäden obliegt auch die Identifizierung von Gefährdungen und Risiken der Managementebene innerhalb des Risiko- und Sicherheitsmanagements. Es ist jedoch gängige Praxis, durch risikoorientierte Prüfungen der Revision die Ergebnisse des Risiko- und Sicherheitsmanagements zu verifizieren. Nicht selten sind die Ergebnisse der Revision sogar die einzige Risikoidentifikation.

Bei der risikoorientierten Revisionsprüfung wird der bestehende Zustand dahingehend untersucht, welche Risiken sich für das Unternehmen aus diesem Zustand ergeben. Grundlage für die Prüfung sind beispielsweise allgemeine Sicherheitsstandards, Normen, branchenübliche Maßstäbe oder Best-Practice-Ansätze (siehe dazu auch Kapitel 4).

Erkennung von Schwachstellen und Lücken

Neben risikobehafteten Umständen in der bestehenden Situation kann es auch Schwachstellen und Lücken geben, die nicht direkt ein Risiko für das Unternehmen darstellen. Beispielsweise könnten Änderungen in der IT sehr umständlich und bürokratisch sein. Dies ist nicht unmittelbar ein Risiko, beeinträchtigt aber die Performance, die Wirtschaftlichkeit und die Fehleranfälligkeit des Änderungsprozesses.

Die Erkennung solcher Schwachstellen und Lücken wird daher bei der Revisionsprüfung erwartet. Bei einem Revisionsergebnis „Keine Mängel“ geht das Top-Management meist davon aus, dass nicht nur keine Verstöße gegen Gesetze und Vorschriften vorliegen, sondern beim Prüfobjekt auch keine Ungereimtheiten, Auffälligkeiten, Schwachstellen oder Lücken gefunden wurden, die es zu beheben gilt.

Die Suche nach den Ursachen von gefundenen Schwachstellen und Lücken gehört nicht zwingend zum Aufgabenspektrum der IT-Revision, sie kann aber in vielen Fällen von der IT-Revision übernommen werden. Es kommt zum einen darauf an, wie die IT-Revision im Unternehmen gesehen wird und welchen Auftrag sie vom Top-Management bekommt, zum anderen müssen für eine Ursachenermittlung die notwendigen Ressourcen und das benötigte Know-how vorhanden sein.

Erhaltung der Leistungsfähigkeit des Unternehmens

Das Ziel der Erhaltung der Leistungsfähigkeit des Unternehmens ist eng mit dem Ziel des Erkennens von Schwachstellen und Lücken verbunden. Nicht selten ist eine Revisionsprüfung die erste Betrachtung des bestehenden Zustands bei einem Prüfobjekt. Die unabhängige, systematische und an Soll-Vorgaben orientierte Prüfung bringt oft Dinge ans Tageslicht, die lange Zeit nicht auffallen, weil man zu sehr auf das normale Tagesgeschäft konzentriert ist.

Die Entdeckung von Fakten, die ein IT-Objekt, einen IT-Prozess oder einen IT-relevanten Managementbereich ineffektiv, unnötig kompliziert, langsam, teuer oder unpassend machen, hilft dem Unternehmen, behindernde Faktoren bei der IT-gestützten Leistungserbringung zu erkennen und auszuräumen. Damit wird die Leistungsfähigkeit des Unternehmens erhalten oder sogar verbessert.

Gewährleistung des internen Kontrollsystems

Das interne Kontrollsystem (IKS) soll sicherstellen, dass bestimmte Dinge im Unternehmen so gestaltet sind bzw. so ablaufen, wie sie vom Unternehmen geplant wurden. Die Revision ist nun sozusagen die „Kontrolle des Kontrollsystems“, denn auch in das IKS können sich Schwachstellen und Lücken einschleichen.

Daher werden die in den Prozessen verankerten Kontrollen, die Kontrollmethodik und das Kontrollvorgehen in den Revisionsprüfungen berücksichtigt. Dies geschieht entweder, indem man eine eigene Revisionsprüfung ansetzt, die explizit das jeweilige IKS untersucht, oder bei jeder Prozessrevisionsprüfung wird das IKS mit untersucht.

Unterstützung und Entlastung des Top-Managements

Die Verantwortung für die Einhaltung von Rechtsvorschriften liegt beim Top-Management (Vorstand, Geschäftsführung). Angesichts der Vielzahl von Vorgaben und der Komplexität der heutigen Informationstechnik ist das Top-Management jedoch selbst nicht in der Lage zu beurteilen, ob das Unternehmen den geltenden Bestimmungen entspricht.

In dieser Situation schafft die IT-Revision die Informationsgrundlage, mit der das Top-Management diese Beurteilung vornehmen kann. Das Top-Management sollte daher von der IT-Revision ungeschönte und interessensfreie Informationen bekommen. Und die IT-Revision leistet noch mehr: Indem sie Verbesserungsvorschläge macht, sorgt sie mit dafür, dass die Prozesse ihren Anforderungen genügen. Nicht selten kommt es dabei jedoch zu Diskussionen und Auseinandersetzungen mit den Fachbereichen.

Empfehlung von Verbesserungen

Neben der Aufdeckung von Mängeln ist die Empfehlung von Verbesserungen ein wichtiger Bestandteil der Revisionsarbeit. Die geprüften Bereiche werden mit dem Prüfungsergebnis nicht alleine gelassen, vielmehr bekommen sie von der IT-Revision auch Hinweise, wie die Situation so verbessert werden kann, dass keine oder zumindest keine schwerwiegenden Mängel mehr existieren.

Dazu empfiehlt die IT-Revision die Durchführung von geeigneten Maßnahmen, um eine Situation zu schaffen, in der die Anforderungen erfüllt werden, die für das Prüfobjekt existieren. Bei der Empfehlung von Maßnahmen sollte jedoch nicht anmaßend vorgegangen werden.

Beurteilung von IT-relevanten Themen im Unternehmen

Die IT-Revision ist für das Management eine gute Informationsquelle. Die Revisoren sind kompetent, nicht in das Interessensgeflecht der operativen Unternehmensorganisation („Linie“) verstrickt und haben einen guten Über- und Einblick, was die Informationstechnik des Unternehmens betrifft.

Daher wird die Meinung der IT-Revision meist geschätzt, wenn es um Planungen oder Projekte in der IT geht. Die IT-Revision kann über bestehende Soll-Vorgaben informieren und Gutachten zu IT-relevanten Sachverhalten erstellen, wenn es um die Erfüllung der Soll-Vorgaben geht. Auch die Integration von Informationstechnik in das Unternehmen kann von der IT-Revision beurteilt werden.

Es ist jedoch nicht Aufgabe der Revision, sich am operativen Geschäft des Unternehmens zu beteiligen, d.h. an Planungen oder ihrer Umsetzung inhaltlich mitzuarbeiten. Sie wird sich daher stets auf eine beratende Funktion zurückziehen.

Von der IT-Revision kann auch eine „zweite Meinung“ eingeholt werden, die unabhängig von der operativen Unternehmensorganisation („Linie“) ist, da die IT-Revision selbst keine Managementfunktion hat und keine Entscheidungen in den Fachbereichen trifft. Ob und inwieweit die IT-Revision genutzt wird, um schon im Vorfeld spätere Mängel zu verhindern, ist von Unternehmen zu Unternehmen sehr unterschiedlich.

1.1.2 Externe Revision

Die Revision kann grob in externe und interne Revision unterschieden werden. Die externe Revision prüft regelmäßig von außen, ob das Unternehmen den gesetzlichen und behördlichen Bestimmungen entspricht. Diese Prüfung wird von Wirtschaftsprüfern vorgenommen. Sie ist auch zuständig, wenn das Top-Management oder die Revision selbst geprüft werden soll.

Wozu aber die Doppelarbeit? Kann der externe Prüfer nicht einfach die Ergebnisse der internen IT-Revision übernehmen? In der Tat werden die Ergebnisse der internen IT-Revision nicht unberücksichtigt bleiben, aber sie einfach zu übernehmen, ist jedoch aus mehreren Gründen nicht statthaft:

- *Die Zielsetzungen sind verschieden.*
  Die Zielsetzungen der internen IT-Revision (siehe Abschnitt 1.1.1) und die Zielsetzungen der externen Revision sind nicht deckungsgleich. Ziele wie die Erhaltung der Leistungsfähigkeit des Unternehmens oder der Schutz vor verkraftbaren Schäden haben für die externe Revision keine Bedeutung. Daher wären die internen Revisionsberichte für die externe Revision nur eingeschränkt aussagekräftig.
- *Die Prüfungsgrundlagen sind verschieden.*
  Nicht nur die Zielsetzungen, auch die zugrunde gelegten Soll-Vorgaben (Prüfungsgrundlagen) sind unterschiedlich. Interne Richtlinien des Unternehmens haben für die externe Revision keine Bedeutung, auch aus diesem Grund sind die internen Revisionsberichte für die externe Revision nicht direkt verwertbar.
- *Die Prüfungsergebnisse sind nicht unabhängig.*
  Der plausibelste und wichtigste Grund besteht darin, dass die Revisionsergebnisse der externen Revision völlig unabhängig vom geprüften Unternehmen sein müssen. Die internen Revisoren besitzen zwar im Unternehmen eine unabhängige Stellung und arbeiten losgelöst von der Linie, sie werden aber nach wie vor vom eigenen Unternehmen bezahlt.

Mehr zur externen Revision und dem Zusammenspiel mit der internen Revision findet sich in Kapitel 3.

1.1.3 Interne Revisionsarten

Die interne Revision wird in mehrere Revisionsbereiche unterteilt, die sich dadurch unterscheiden, dass sie jeweils andere Prüfobjekte untersuchen, andere Prüfungsgrundlagen verwenden und teilweise verschiedene Prüfungsaspekte betrachten. Die Revisionsmethodik bleibt dabei gleich.

- *Kaufmännische Revision*
  Im Zentrum der kaufmännischen bzw. betriebswirtschaftlichen Revision stehen die Geschäftsprozesse des Unternehmens, unterteilt in die Kernprozesse und die wertschöpfungsbegleitenden, betriebswirtschaftlichen Prozesse.
- *IT-Revision*
  Wie bereits weiter oben beschrieben, konzentriert sich die IT-Revision auf die Beschaffenheit, den Betrieb, das Management und die Nutzung der Informationstechnik. Da die Geschäftsprozesse moderner Unternehmen intensiv durch die IT unterstützt werden, hat die IT-Revision an Bedeutung gewonnen.
- *Technische Revision*
  Die technische Revision prüft technische Einrichtungen im Unternehmen wie Fahrzeuge, Maschinen oder bauliche Einrichtungen. Besonderes Augenmerk liegt dabei auf der Betriebssicherheit der Prüfobjekte.

In einigen Bereichen gibt es noch speziell ausgeprägte, branchenspezifische Revisionsarten, die jedoch hier nicht näher beleuchtet werden sollen.

1.2 Mit der IT-Revision verwandte Funktionen

Mit den Tätigkeiten Erheben, Prüfen, Kontrollieren, Empfehlen und Beraten steht die IT-Revision nicht alleine im Unternehmen. Es gibt mehrere Funktionsbereiche im Unternehmen, die ähnliche Zielsetzungen besitzen.

Im Unterschied zu diesen anderen Funktionsbereichen ist die IT-Revision nicht in das operative Geschäft involviert. Sie trifft keine geschäftlichen Entscheidungen und beeinflusst nicht direkt die Planungen und Vorgehensweisen. Sie ist nicht in der Pflicht, die bestehende Situation in den geprüften Bereichen zu verbessern, und ist aufgrund der fehlenden Weisungsbefugnis[3] dazu auch nicht in der Lage. Die Steuerung des Zustands der Prüfobjekte liegt in der Verantwortung des jeweiligen Fachbereichs.

Externe Soll-Vorgaben wie Gesetze sind für das Unternehmen verpflichtend und können nicht umgangen werden. Wie in Abschnitt 1.4 gezeigt wird, ist es mit der Prüfung auf Gesetzeskonformität jedoch nicht getan. Für die Prüfung weiterer Prüfungsaspekte werden interne Vorgaben benötigt. Durch eine geschickte Auswahl bzw. eine Minimierung der Vorgaben kann beeinflusst werden, ob die Prüfungsergebnisse besser oder schlechter ausfallen.

Die IT-Revision ist nicht verantwortlich dafür, welche Vorgaben vom Management für die einzelnen Bereiche festgelegt werden. Es ist jedoch vielfach sinnvoll, dass ihre Beratungsfunktion auch bei der Auswahl der Vorgaben in Anspruch genommen wird. Erstellt das Unternehmen eigene Richtlinien und Standards, so ist es möglich, die IT-Revision im Erstellungsprozess zu konsultieren. Schließlich ist es auch möglich, eine Revisionsprüfung dahingehend durchzuführen, dass festgestellt wird, ob die Vorgaben ausreichend sind bzw. die richtigen Vorgaben gewählt wurden.

IT-Controlling

Das IT-Controlling ist eine Überwachungs- bzw. Kontrollinstanz im operativen Management, die folgende Aufgaben besitzt:

- Überwachung der IT-Kosten (Budget- und Investitionskontrolle, Leistungsverrechnung)
- Überwachung der effektiven Gestaltung und Entwicklung der IT (Zielerfüllung, Projektpriorisierung)
- Kontrolle der Ausrichtung an der IT- und Unternehmensstrategie (Verfolgen der Übereinstimmung zwischen IT-Entscheidungen und der Strategie)

Aus der Aufstellung ist ersichtlich, dass die Aufgaben des IT-Controllings etwas anders gelagert sind als die der IT-Revision. Beispielsweise liegt die kostengerechte Leistungsverrechnung nicht im Fokus der Revisionsbetrachtung. Dennoch sind IT-Controller wichtige Ansprechpartner für die IT-Revision.

---

[3] Eine Ausnahme wäre eine Situation, in der eine akute Gefahr erkannt wird. Für diesen Fall sollte die Revision die Vollmacht besitzen, gefahrabwendende Schritte anordnen zu können.

IT-Qualitätsmanagement

Ziel des IT-Qualitätsmanagements ist die Steuerung und Verbesserung der IT-Qualität, vor allem die Qualität der erbrachten IT-Dienste für die Fachbereiche. In der Qualitätsplanung wird festgelegt, was unter dieser Qualität zu verstehen ist und welche Ausprägung sie besitzen soll oder muss. In der Qualitätssicherung werden Maßnahmen wie Qualitätsprüfungen ergriffen, um diese Qualität zu erreichen und zu erhalten. Die Prüfung der Konformität zu bestehenden Richtlinien gehört nicht zu den Aufgaben des IT-Qualitätsmanagements.

IT-Risiko- und IT-Sicherheitsmanagement

Wie der Name schon sagt, ist diese Funktion ein umfangreicher Managementbereich, der den Schutz gegen IT-Risiken wie Ausfall, Manipulation oder Ausspähung organisiert. Da die Sicherheit auch ein wichtiger Prüfungsaspekt der IT-Revision ist, gibt es hier eine inhaltliche Schnittmenge. Die Analyse der IT-Risiko- bzw. -Sicherheitssituation ist jedoch nur ein Teilbereich des IT-Sicherheitsmanagements. Das Prüfspektrum der IT-Revision geht weit über den Aspekt Sicherheit hinaus.

IT-Governance

Die Funktion der IT-Governance ist der auf die Informationstechnik bezogene Ansatz der Corporate Governance. Im Mittelpunkt der IT-Governance steht das Zusammenspiel zwischen dem Gesamtunternehmen und dem IT-Bereich:

- Die Eignung der IT, die Geschäftstätigkeit adäquat zu unterstützen (Business-IT-Alignment)
- Die Konformität der IT mit der Unternehmensstrategie
- Die Ermittlung der Anforderungen und Erwartungen an die IT und das Verfolgen ihrer Erfüllung

Entsprechend diesen Schwerpunkten ist die Funktion der IT-Governance im strategischen Management angesiedelt (z.B. IT-Vorstand, CIO[4]). Im Gegensatz zur Revision ist die IT-Governance keine prüfende, sondern eine führende Funktion, d.h. sie stellt keine Nachbetrachtungen an wie die Revision, sondern agiert „mitten im Geschehen“.

IT-Compliance

Ziel der IT-Compliance ist die Erfüllung der Soll-Vorgaben, die an die IT des Unternehmens gestellt werden. Das klingt deckungsgleich zur IT-Revision. Doch die IT-Compliance ist meist eine Funktion und kein Bereich, der als eigenständige Organisationseinheit in der Aufbauorganisation des Unternehmens verankert ist.

---

4 Chief Information Officer

Datenschutz

Diese Funktion kümmert sich um den Schutz personenbezogener Daten. Ziel ist die Wahrung des informationellen Selbstbestimmungsrechtes. Die Funktion wird in den meisten Fällen von einem vom Unternehmen bestellten Datenschutzbeauftragten wahrgenommen.

Der Datenschutzbeauftragte prüft, ob die Erhebung, Speicherung, Verarbeitung und Nutzung personenbezogener Daten konform zu den geltenden Datenschutzbestimmungen (z.B. BDSG, siehe dazu Kapitel 4) erfolgt. Er erstellt datenschutzrechtliche Gutachten und gibt Empfehlungen an die Fachbereiche. Damit ähnelt seine Tätigkeit strukturell der Arbeit der IT-Revision, er wird jedoch in der Regel auf Anforderung tätig und beschränkt sich, wie beschrieben, auf personenbezogene Daten.

1.3 Die IT-Revision im Unternehmen

1.3.1 Position im Unternehmen

Für die Aufbauorganisation stellt sich die Frage, an welcher Stelle im Unternehmensgefüge die IT-Revision anzusiedeln ist. Da es um die Informationstechnik geht, könnte der erste Gedanke sein, die IT-Revision in den IT-Bereich einzugliedern. In diesem Fall wäre der IT-Leiter bzw. der IT-Vorstand der Vorgesetzte des Revisionsleiters. Es liegt auf der Hand, dass sich eine solche Platzierung in der Linie verbietet.

In der Regel wird die Revision direkt unter dem Top-Management platziert. Damit ist die IT-Revision unabhängig und nur dem Top-Management gegenüber verantwortlich. Eine Ausnahme bildet der Fall, dass bei einer Revisionsprüfung entdeckt wird, dass schwerwiegende Verstöße mit Wissen bzw. Billigung oder sogar auf Veranlassung des Top-Managements stattfinden. In diesem Fall könnte das Top-Management die Verstöße vertuschen, wenn die Revision nur das Top-Management informiert. Daher muss in diesen Fällen auch eine externe Information (je nachdem Aufsichtsrat, Aufsichtsbehörde usw.) erfolgen.

In großen Umgebungen kann es zusätzlich zur zentralen Revision noch Revisionsbeauftragte in den Fachbereichen geben, die von der Leitung des Bereichs benannt werden. Sie sind zum einen Ansprechpartner für die zentrale Revision, zum anderen wirken sie in den Fachbereich hinein. Die Bewertungen liegen weiterhin bei der zentralen Revision, daher müssen die Revisionsbeauftragten nicht unabhängig von der Linie sein.

1.3.2 Befugnisse

Die Position direkt unter dem Top-Management besitzt neben der Unabhängigkeit von der Linie einen entscheidenden Vorteil: Die Revision gewinnt dadurch an Gewicht und Respekt im Unternehmen. Voraussetzung ist, dass das Top-Management hinter der Revision steht. Das bedeutet:

1. Das Top-Management nimmt die Revision ernst und betrachtet sie nicht als Alibi-Veranstaltung. Handelt das Top-Management nach der Devise: „Es muss was geschehen, aber es darf nichts passieren“, dann wird eine sachgerechte Arbeit für die Revision sehr schwierig.
2. Das Top-Management gibt der Revision Rückendeckung. Hält das Top-Management bei Konflikten mit den Fachbereichen immer zum Fachbereich, dann wird die Autorität der Revision untergraben, und sie wird nicht mehr ernst genommen. Ähnliches gilt, wenn ständig beschwichtigt wird („Dann verlegen Sie doch die Prüfung in den Herbst, damit endlich Ruhe ist“).
3. Die Revision wird personell, finanziell, mit Sachmitteln und Vollmachten ausreichend ausgestattet.

Folgende Punkte sollten beachtet werden:

- Der Auftrag für Revisionsprüfungen sollte immer vom Top-Management kommen.
- Die Fachbereiche sollten gehalten sein, die Revision bei Prüfungen uneingeschränkt zu unterstützen. Vom Fachbereich angeführte Gründe, warum eine Prüfung nicht durchgeführt werden kann, sind in der Regel als Mangel zu werten (z.B. mangelnde Verfügbarkeit von Personen).
- Die Fachbereiche sollten gehalten sein, alle erforderlichen Unterlagen und Informationen unverzüglich und vollständig zur Verfügung zu stellen, z.B. Unterlagen, Einblick in Prozesse, Zutritt zu Räumen, Revisionszugriff auf Systeme.
- Die Revision sollte das Recht zum Zugang zu allen Informationen erhalten, die für die Prüfungen benötigt werden. Das sollte auch für vertrauliche Informationen gelten. Es sollte keine prüfungsfreien Räume (im Sinne von ungeprüften Prüfobjekten) geben.
- Alle Fachbereiche sollten eine Informationspflicht gegenüber der Revision haben (d.h. von sich aus die Revision informieren), wenn
  - dem Fachbereich schwerwiegende Mängel bekannt werden,
  - im Fachbereich ein Verdacht für ein Fehlverhalten besteht,
  - Änderungen am internen Kontrollsystem (IKS) vorgenommen werden.
- Die Revision sollte ein Weisungsrecht besitzen, wenn Gefahr im Verzug ist, wenn also beispielsweise begründeter Verdacht besteht, dass ein Fehlverhalten verschleiert oder ein Beweismittel vernichtet werden könnte.

Praxistipp

Immer wieder sträuben sich Fachbereiche gegen Prüfungen mit Argumenten wie „Wir haben gerade eine besonders hohe Belastung durch das Tagesgeschäft“ oder „Die Person, die Auskunft geben kann, ist gerade im Urlaub“. Die oben genannten Rahmenbedingungen sollten daher schriftlich dokumentiert und vom Top-Management unterschrieben werden. Zusätzlich sollten die Punkte vom Top-Management in deutlicher Form an die Fachbereiche kommuniziert werden.

1.3.3 Mitarbeiter

Die Revision lebt von dem Wissen und den Fähigkeiten ihrer Mitarbeiter. Daher sollte das Unternehmen in eigenem Interesse darauf achten, die Revision personell entsprechend auszustatten. Die Revision wird zwar von den Fachbereichen oft als lästiges Übel gesehen, für das Top-Management ist sie aber eine wichtige Informationsquelle.

Revisionsleitung

Natürlich muss der Revisionsleiter die Revision methodisch und inhaltlich organisieren können. Doch daneben muss er vor allem unternehmenspolitisch beschlagen sein, denn er wird oft in der Kritik der Fachbereiche stehen, besonders dann, wenn diese sich ungerecht behandelt und bewertet fühlen. Das erfordert ein gutes Standing[5] im Unternehmen.

Er muss das „Ohr am Unternehmen haben", mitbekommen, was sich tut, wo akute Probleme entstehen, die in einer Sonderprüfung untersucht werden sollten. Er sollte einen guten Draht zum Top-Management haben und die Revision als Unterstützung des Top-Managements begreifen. Er muss loyal zum Unternehmen sein, aber auch das Rückgrat besitzen, um bei besonders schwerwiegenden, strafrechtlich relevanten Mängeln konsequent zu handeln.

Revisoren

Mit den Revisoren steht und fällt die Güte der IT-Revision. Daher ist es wichtig, schon bei der Personalauswahl gezielt Revisoren zu gewinnen, die über die benötigten bzw. wünschenswerten Qualifikationen verfügen:

- *Revisionswissen*
  Unter Revisionswissen wird hier das Wissen um die Vorbereitung und Durchführung von Revisionsprüfungen verstanden. Der Revisor muss den Aufbau und Ablauf von Revisionsprüfungen kennen und die Prüfungsmethoden beherrschen. Er muss in der Lage sein, die Prüfungsgrundlagen zu bestimmen, die Prüfungsfragen auszuwählen, den bestehenden Zustand des Prüfobjekts zu ermitteln und anschließend zu bewerten.
- *Organisationswissen*
  Ein allgemeines Wissen um die IT-Organisation ist bei annähernd jeder IT-Revisionsprüfung notwendig. Der Revisor muss wissen, welche Bereiche das IT-Management umfasst, welche IT-Prozesse es gibt und wie die IT technisch gestaltet werden kann.
  Das Wissen um die konkrete Ausprägung im eigenen Unternehmen erleichtert dabei die Arbeit des Revisors.
- *Anforderungswissen*
  Die IT-Revision prüft immer gegen bestehende Soll-Vorgaben, die in Form von Anforderungen in den Prüfungsgrundlagen (siehe Kapitel 4) vorgegeben sind. Der Revisor muss die relevanten Prüfungsgrundlagen zumindest in ihrer Existenz kennen. Wichtige

[5] Eine Mischung aus Rückgrat, Ruf, Respekt und Durchsetzungsfähigkeit.

Prüfungsgrundlagen sollte er inhaltlich erschlossen haben und anwenden können. Er muss die Absicht erkennen, die hinter den Anforderungen steht und somit wissen, worauf es bei den Prüfungen ankommt.

- *Psychologische Robustheit*
  Zu den wichtigen sogenannten „Soft Skills" gehört eine gewisse psychologische Robustheit, oder einfacher gesagt: ein dickes Fell. Es kommt öfter vor, dass es widerspenstige Fachbereiche gibt, die sich durch Revisionsprüfungen in die Mangel genommen fühlen und nicht mitarbeiten wollen. Der Revisor muss auch mit solch schwierigen Situationen umgehen können und darf sich nicht persönlich angegriffen fühlen.
- *Erfahrung*
  Besonders für die Erkennung und Feststellung von Mängeln innerhalb der Bewertung des bestehenden Zustandes ist es notwendig, einen gewissen Spürsinn zu entwickeln und zu erahnen, wo „der Hase im Pfeffer liegt". Dabei hilft der Faktor Erfahrung. Wer bereits viele Prüfungen durchgeführt hat, der bemerkt schnell, wenn der Fachbereich etwas zu verbergen hat. Auch hier hilft die Erfahrung im eigenen Unternehmen, denn dann kennt man die Abteilungen und Personen, die kritisch sein können. Revisoren mit viel Erfahrung kennen zudem die Tricks der Fachbereiche, um sich in Revisionsprüfungen gut zu verkaufen.
- *Engagement und Charakter*
  Zwar sind Revisionsprüfungen nach einem festen Schema organisiert, dennoch hängt die Qualität der Ergebnisse davon ab, wie engagiert der Revisor in der Prüfung agiert. Wichtig ist vor allem eine gewisse Hartnäckigkeit, d.h. der Revisor darf sich nicht gleich mit dem zufriedengeben, was ihm der Fachbereich anbietet.
  Besonders in Interviews erlebt man es oft, dass die Interviewten von den Fragen ablenken und andere, unwichtige Details beschreiben oder durch lange „Referate" die Interviewzeit verkürzen wollen. Engagement bedeutet daher auch, die Führung in der Prüfung zu behalten. Ein weiterer Punkt ist in diesem Zusammenhang die Fähigkeit des Revisors, eigenständig zu arbeiten und seine Tätigkeit zu organisieren.
- *Unabhängigkeit*
  Revisoren dürfen nicht in betriebliche Abläufe eingebunden sein, die sie als Revisor zu prüfen haben. Im Hinblick auf eine Prüfung darf kein Interessenkonflikt entstehen, z.B. weil der Revisor privat oder nebenberuflich[6] eng mit einem Unternehmen verbunden ist, das in ein Prüfobjekt des Revisors involviert ist, weil er (wenn er aus dem Unternehmen kommt) noch Verpflichtungen gegenüber seiner alten Abteilung hat oder weil er aufgrund einer Liebesbeziehung befangen ist.
  Revisoren dürfen nicht voreingenommen sein. Sie dürfen sich von persönlichen Sympathien/Antipathien, Zu- oder Abneigungen nicht leiten lassen und müssen möglichst objektiv bleiben. Sie dürfen sich nicht „um den Finger wickeln lassen", müssen Charme-Attacken widerstehen und dürfen sich nicht einschüchtern lassen.

6 Die Prüfung von nebenberuflichen Tätigkeiten ist bei Revisoren besonders wichtig.

- *Integrität*
  Revisoren dürfen nicht bestechlich sein. Bei einigen Unternehmen werden daher auch die Revisoren überprüft. Ist das polizeiliche Führungszeugnis in Ordnung? Steckt der Revisor in finanziellen Schwierigkeiten? Ist er erpressbar? Wurden bei einer Sicherheitsüberprüfung (Hintergrund-Check) Auffälligkeiten festgestellt?
  Der Revisor muss loyal zum Unternehmen sein. Eine Selbstverständlichkeit sollte die Verschwiegenheit der Revisoren sein. Das gilt gegenüber anderen Unternehmen, der Presse, Kollegen und selbst gegenüber der eigenen Familie.

1.3.4 Qualitätssicherung und Leistungsmessung

Die im vorhergehenden Abschnitt genannten Eigenschaften sind Voraussetzungen (Kompetenzen), die erfüllt sein sollten, damit die Revisionsleistung erbracht werden kann. Diese Voraussetzungen müssen zunächst definiert und eingefordert werden.

Wie kann aber auch die Güte der Revisionsleistung festgestellt werden? Wie kann die Qualität beurteilt, erhalten und verbessert werden?

Anwendung von Qualitätskennzahlen

Bei diesem Verfahren werden mehrere Kennzahlen definiert, mit deren Hilfe die Qualität eingeschätzt werden kann. Solche Kennzahlen können sein:

- Die durchschnittliche Dauer einer Revisionsprüfung.
- Die zeitliche Belastung für den Fachbereich (z.B. durch Interviews).
- Das zur Verfügung gestellte Zeit- und Kostenbudget für die Weiterbildung der Revisoren (und das Verhältnis zu dem, was davon in Anspruch genommen wurde).

Diese Kennzahlen werden fortlaufend (bei jeder Prüfung) erhoben und über die Zeit verfolgt, sodass sich eine zeitliche Entwicklung erkennen lässt. Wichtig ist, dass die Kennzahlen in einer objektiven[7] Größe angegeben werden können und unabhängig vom Inhalt der Prüfungen sind.

Vergleich mit externen Prüfungen

Eine weitere Möglichkeit besteht darin, einen Vergleich zu externen Prüfungen zu ziehen. Dies ist natürlich nur dann möglich, wenn es um das gleiche Prüfobjekt und einen vergleichbaren Prüfungsumfang geht. War der Zeitaufwand größer? Wurden weniger oder mehr Mängel gefunden? Wurden die gleichen Soll-Vorgaben zugrunde gelegt? Diese oder ähnliche Fragen würde man sich bei diesem Verfahren stellen.

Selbstbeurteilung

Das Verfahren mit Qualitätskennzahlen hat den wesentlichen Nachteil, dass Qualitätsfaktoren unberücksichtigt bleiben, die nicht in einer objektiven Kennzahl erfasst werden kön-

[7] Objektiv im Sinne einer Größe, die sich über mehrere Prüfungen hinweg vergleichen lässt

nen. In diesem Fall hilft die Selbstbeurteilung weiter. Jeder Revisor hält bei jeder Prüfung fest, welche Schwierigkeiten es bei der Durchführung der Revisionsarbeit gab.

In regelmäßigen Abständen setzt sich dann das Revisionsteam zusammen, diskutiert diese Schwierigkeiten und sucht nach Verbesserungen. Bisweilen reicht schon der Austausch von Tipps, um die Arbeit zu verbessern. In anderen Fällen sind strukturelle Änderungen (z.B. im Revisionsprozess, der Personalausstattung usw.) oder Unternehmensentscheidungen (z.B. im Streit mit der Linie, für Befugnisse usw.) nötig.

Beurteilung durch die geprüften Bereiche

Das Problem der Selbstbeurteilung ist, dass so mancher verbesserungswürdige Punkt den Revisoren selbst nicht auffällt („Blinder Fleck"). Daher sollten auch die geprüften Bereiche die Revisionsarbeit beurteilen.

Am Ende einer jeden Revisionsprüfung sollte deshalb eine Rückmeldung des geprüften Bereichs erfolgen. Die Gefahr einer solchen Beurteilung liegt darin, dass bei einem schlechten Prüfungsergebnis (viele Mängel) der Fachbereich nun „Rache" nehmen könnte und die Prüfung schlecht bewertet. Daher sollte darauf geachtet werden, dass der Fachbereich in seiner Wertung keine allgemeinen Meinungsäußerungen abgibt, sondern konkret angibt, wo es unter Berücksichtigung der Vorgaben für die Revision Anlass zur Kritik gibt.

Beurteilung durch das Top-Management

Auch das Top-Management als Auftraggeber der Prüfungen und Empfänger der Revisionsberichte[8] sollte die Dienstleistungsqualität (Performance) der Revision beurteilen. Doch hier wird es schwierig, denn ein Auftraggeber hat immer bestimmte Erwartungen an das Ergebnis. Das können konkrete oder diffuse, explizite und implizite, ausgesprochene und nicht ausgesprochene Erwartungen sein. In der Praxis ergibt sich vom Prüfungsauftrag bis zur Auswertung des Prüfungsergebnisses ein Kreislauf, wie in Abbildung 1.1 zu sehen ist.

Der Top-Manager wird immer bewerten, ob das, was er vom Prüfungsergebnis wahrnimmt, mit dem übereinstimmt, was er im Prüfungsauftrag von der Revision wollte. Letzteres wird in Form von Anforderungen an die Revisionsdienstleistung definiert und als Soll-Zustand formuliert. Beispiel: „Die Prüfungsberichte sollen übersichtlich gestaltet sein".

Die Bewertung kann nun erfolgen, indem der Manager die Anforderung auf einer Skala von „viel besser als erwartet" bis „viel schlechter als erwartet" einschätzt. Das Problem hierbei ist, dass der Grund für die Bewertung nicht klar wird. Lag es bei einer guten Bewertung daran, dass der Manager vorher der Revision nichts zugetraut hat? Wo lag der Grund bei einer schlechten Bewertung? War die IT-Revision nicht in der Lage, das Ergebnis zu liefern? Hat der Manager das Ergebnis nur nicht wahrgenommen oder hatte er zu hohe, unrealistische Erwartungen?

---

[8] Als „Kunden" der Revision kommen auch der Aufsichtsrat, das Audit Committee, Aufsichtsbehörden und externe Prüfer in Betracht.

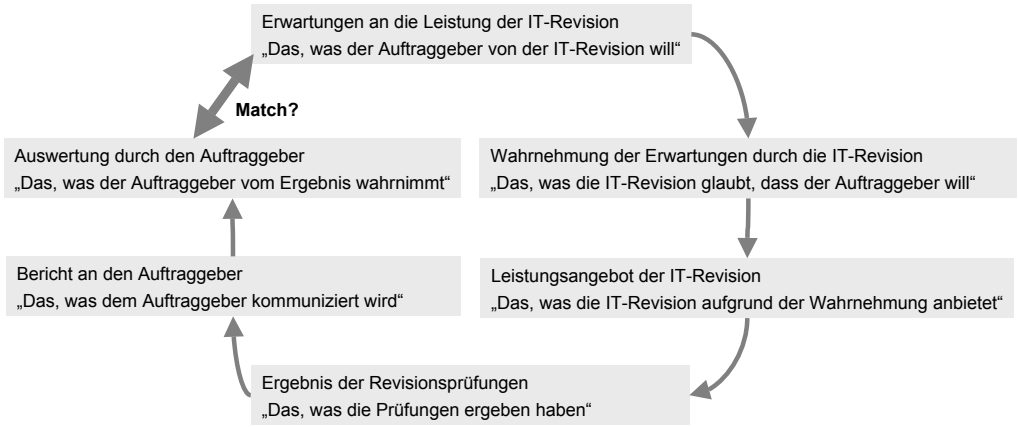

Abbildung 1.1 Erbringung der Revisionsdienstleistung und Erwartungserfüllung

Ein etwas ausführlicheres Verfahren beurteilt daher zunächst die Anforderungen und gibt erst dann die Ist-Einschätzung. Dazu werden drei Schritte durchgeführt:

1. **Anforderung beurteilen** (Stimmt der jeweilige Top-Manager der Anforderung zu? Ist sie für ihn relevant und wichtig?). Für diese Einschätzung gibt es entsprechende Skalierungsverfahren mit mehreren Stufen[9]. Beispiel mit vier Stufen: Stimme in vollem Umfang zu / Stimme in hohem Maße zu / Stimme in geringem Maße zu / Stimme überhaupt nicht zu.
2. **Ist-Einschätzung**. Anforderung als erfüllt formulieren („Die Prüfungsberichte sind übersichtlich gestaltet“) und mit dem gleichen Skalierungsverfahren bewerten.
3. **Ist-Wert vom Soll-Wert abziehen**. Positives Ergebnis = Erwartungen werden übertroffen, 0 = Erwartungen werden erfüllt, negatives Ergebnis = Erwartungen werden nicht erfüllt.

Praxistipp

Beachten Sie, dass die Beurteilung der Anforderungen subjektiv erfolgt. Positive Werte können daher auch dadurch erreicht werden, dass einfach die Anforderungen „heruntergewertet“ werden. Vergleichen Sie die Anforderungsbewertungen verschiedener Personen. Weichen sie stark ab? Aus welchem Grund?

Zusätzlich zu solchen formalisierten Verfahren ist es in der Praxis am besten, in persönlichen Gesprächen die Erwartungen und Leistungen gegenseitig abzugleichen. Kennt die IT-Revision die Erwartungen des Auftraggebers und nimmt sie diese richtig wahr? Sind die Erwartungen des Auftraggebers realistisch und angemessen oder verlangt er etwas, was die IT-Revision nicht leisten kann oder darf?

Dazu listet der Auftraggeber die Erwartungen auf und gibt an, wie wichtig jede Erwartung aus seiner Sicht ist und warum das so ist. Auch die IT-Revision gibt an, wie wichtig die

[9] Gebräuchlich sind Verfahren mit 2 bis 7 Stufen.

Erwartungen aus ihrer Sicht sind. Abweichungen werden diskutiert, und es wird versucht, sich gegenseitig besser zu verstehen.

Um sicher zu sein, dass die IT-Revision angesichts der Erwartungen die richtigen Leistungen ausführt, muss der Auftraggeber näher spezifizieren, woran er merken würde, dass die Leistung den Erwartungen entspricht. Das bedeutet, dass der Auftraggeber die Leistungen hinsichtlich Geschwindigkeit, Detailliertheit, Treffen der Zielsetzung, richtige Vorgehensweise, Methode oder Kosten spezifiziert. Im Gegenzug gibt die IT-Revision die Leistungen an, die sie erbringen kann. Abweichungen werden wieder diskutiert und daraus Vorgaben entwickelt, die in der Praxis kontrolliert werden.

Wichtig ist auch die Frage, ob die erbrachte Leistung beim Auftraggeber ankommt. Die Revisoren sollten kommunikationstechnisch geschult sein, um die Ergebnisse richtig präsentieren zu können und gleichzeitig zu erfahren, was der Auftraggeber will und meint. Wird die erbrachte Leistung an den Auftraggeber kommuniziert? Nimmt er sie wahr? Kann er sie verstehen und gebrauchen? Bekommt er von verschiedenen Revisoren unterschiedliche Informationen? Wird betont, worauf es ankommt?

1.3.5 Sicherheit der Revisionsabteilung

Es liegt auf der Hand, dass die Revision eine sensible Abteilung darstellt, da sie nicht nur im Zuge ihrer Prüfungen Dinge erfährt, die vertraulich zu behandeln sind, sondern auch selbst durch die Feststellungen von Mängeln sensible Informationen produziert und austauscht.

Die Abteilung ist daher entsprechend zu sichern. Das beginnt bei den Räumlichkeiten der IT-Revision. Im Idealfall verfügt die Revision über eigene Räume, die von den anderen Büros räumlich getrennt sind (je nach Größe der Revision ein eigenes Büro, ein eigener Flur oder eine eigene Büroetage). Die Räume sollten weder für den Publikumsverkehr noch für die außerhalb der Revision tätigen Mitarbeiter des Unternehmens frei zugänglich sein.

Gibt es keine Einzelbüros, dann muss jeder Revisor für die Sicherheit seines Arbeitsplatzes sorgen. In der Praxis bedeutet das, die Schränke verschlossen zu halten, den Schreibtisch beim Verlassen des Arbeitsplatzes zu verschließen, sensible Unterlagen nicht offen auf dem Schreibtisch liegen zu lassen und den Computer beim Verlassen des Arbeitsplatzes zu sperren.

Ein Großraumbüro ist aus den geschilderten Gründen für die Revisionsabteilung eher nicht geeignet. Ist es trotzdem unumgänglich, dann sollte der Revisionsbereich möglichst in einer Ecke der Etage liegen und mit höheren Schränken und Sichtblenden optisch und akustisch (Telefongespräche) abgetrennt werden.

Auch in der Kommunikation ist einiges zu beachten. Sensible Informationen sollten nicht unversiegelt mit der normalen Hauspost versendet werden, bei elektronischer Kommunikation (z.B. E-Mail) sollten sensible Informationen vor der Übertragung verschlüsselt werden.

Alle Dokumente, bei denen die Bewahrung der Ursprünglichkeit wichtig ist, müssen vor nachträglicher Veränderung geschützt werden (z.B. nicht änderbares Format oder Schreibschutz) bzw. es muss sichergestellt werden, dass nachträgliche Veränderungen erkennbar sind (z.B. durch eine digitale Signatur).

Nicht mehr benötigte Unterlagen, die sensible Informationen enthalten, sollten sicher vernichtet oder über einen sicheren Kanal (eigene Sammelstellen für sensible Dokumente) entsorgt werden.

1.4 Prüfungsaspekte

Die Prüfungsaspekte geben an, worauf ein Prüfobjekt geprüft werden soll. Sie werden im Zuge der Prüfungsvorbereitung vor oder während der Erstellung des Prüfungsauftrags festgelegt. Aus den Prüfungsaspekten ergeben sich die Zielsetzungen für die Prüfung und letztlich auch die Prüfungsfragen, die in der Prüfung zu stellen sind.

Es gibt eine Vielzahl von denkbaren Prüfungsaspekten. Zudem können Prüfungsaspekte in andere Prüfungsaspekte integriert werden. So kann bei Buchführungssystemen die Nachvollziehbarkeit in die Ordnungsmäßigkeit integriert werden, da die Soll-Vorgabe der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS, siehe Kapitel 4) die Nachvollziehbarkeit fordert. Die im Folgenden beschriebenen Aspekte sind diejenigen, die man häufig bei Revisionsprüfungen findet.

1.4.1 Rechtmäßigkeit

Die fundamentalste Forderung an ein Prüfobjekt ist die Forderung, dass die geltenden Gesetze und rechtlichen Vorschriften und Bestimmungen eingehalten werden. Das Prüfobjekt wird daher fast immer auf die Rechtmäßigkeit hin geprüft.

Bezogen auf die Informationstechnik des Unternehmens bedeutet die Rechtmäßigkeit, dass

- ... die physische Beschaffenheit der IT den geltenden Normen und Vorschriften entspricht. Das betrifft die bauliche Beschaffenheit von IT-relevanten Bauwerken, Gebäuden und Räumen (Vorschriften der Bauordnung, Brandschutz, Klimatisierung etc.).
- ... die technische Beschaffenheit der IT den geltenden Normen und Vorschriften entspricht. Das betrifft die technische Beschaffenheit von ITK-Netzwerken sowie von IT-Hardware- und Software-Komponenten (Funkentstörung, Schutzerdung, EMV-Verhalten etc.).
- ... Abläufe in der IT den gültigen Gesetzen und Bestimmungen entsprechen. Das betrifft die Planung/Entwicklung, die Implementierung, den Betrieb, die Änderung/Migration und die Entfernung/Entsorgung (Roll-Off) von IT-Komponenten und deren Inhalte/Daten (Datenschutz, Archivierung etc.).
- ... das IT-Management gesetzlichen Vorgaben und rechtlichen Bestimmungen entspricht (Corporate Governance, Verfahrensmanagement, Risikomanagement etc.)

Es ist dabei zu prüfen, ob der bestehende Zustand zulässig und gesetzeskonform ist. Falls nicht, ist zu prüfen, gegen welche Bestimmungen verstoßen wird und als wie gravierend dieser Verstoß für das Unternehmen anzusehen ist. Ein Gesetzesverstoß ist in der Regel ein schwerwiegender Mangel.

1.4.2 Ordnungsmäßigkeit

Die Prüfung auf Ordnungsmäßigkeit geht in die gleiche Richtung wie die Prüfung auf Rechtmäßigkeit, ist jedoch weiter gefasst. Nun wird nicht mehr nur auf Konformität mit Gesetzen geprüft, sondern generell auf Konformität mit Soll-Vorgaben, die von externen Instanzen (Gesetzgeber, Aufsichtsbehörde, Vertragspartner[10], Kunden) oder vom Unternehmen selbst an die IT im Unternehmen gestellt werden (z.B. aufsichtsrechtliche Vorschriften, Policies, interne Richtlinien und Anweisungen, Betriebsvereinbarungen, Sicherheitsstandards etc.).

Die Prüfung auf Ordnungsmäßigkeit schließt die Prüfung auf Rechtmäßigkeit mit ein, daher taucht meist der Prüfungsaspekt der Rechtmäßigkeit in Prüfungen nicht mehr explizit auf. Es wird zwischen der formellen und der materiellen (inhaltlichen) Ordnungsmäßigkeit unterschieden:

Die **formelle Ordnungsmäßigkeit** ist gegeben, wenn sichergestellt ist, dass die relevanten Soll-Vorgaben für die Form (das „Wie“) unabhängig vom Einzelfall eingehalten werden. Beispiel: Im Unternehmen existiert eine Einkaufsrichtlinie für die IT, die für Beschaffungen über 10.000 € eine Ausschreibung vorschreibt. Die Vorgabe konzentriert sich auf den Beschaffungsprozess, unabhängig davon, was beschafft wird. Bei der Beschaffung eines großen Servers wird damit nicht verhindert, dass ein falscher Server beschafft wird.

Die **materielle Ordnungsmäßigkeit** ist gegeben, wenn sichergestellt ist, dass die relevanten Soll-Vorgaben für den Inhalt (das „Was“) im Einzelfall eingehalten werden. Beispiel: In der bereits genannten Einkaufsrichtlinie wird vorgeschrieben, dass IT-Einrichtungen gemäß ihrer funktionalen Spezifikation beschafft werden müssen. Die Vorgabe konzentriert sich auf den Inhalt der Beschaffung – unabhängig davon, wie beschafft wird. Bei der Beschaffung eines großen Servers wird damit nicht verhindert, dass ein zu teurer Server beschafft wird.

Damit wird klar, dass in der Praxis nur eine Kombination aus formeller und materieller Ordnungsmäßigkeit sinnvolle Ergebnisse liefert. Leider wird dies bei der Erstellung der Soll-Vorgaben nicht immer berücksichtigt. Zumindest die internen Soll-Vorgaben können jedoch wiederum Prüfobjekte darstellen, die von der IT-Revision geprüft werden. Damit kann die IT-Revision solche Schwächen aufdecken und kommunizieren.

[10] Verträge sind dabei auch Versicherungspolicen, Wartungsverträge, Service Level Agreements (SLAs) oder Leasingvereinbarungen.

1.4.3 Sicherheit

Ein wichtiger Prüfungsaspekt ist die Sicherheit oder etwas konkreter: die Sicherheit der Informationstechnik im Unternehmen. Der Grund dafür liegt in der Verletzbarkeit der Informationstechnik und den weitreichenden Folgen, die sich daraus für das Unternehmen ergeben können. In modernen Unternehmen sind die Geschäftsprozesse in der Wertschöpfungskette größtenteils IT-gestützt und damit von der IT abhängig.

Durch einen Ausfall oder Missbrauch entsteht für das Unternehmen mitunter ein erhebliches Risiko für Ertrag und Bestand. Aufgabe der IT-Revision ist es deshalb, dazu beizutragen, dass die mit der IT verbundenen Risiken minimiert oder ganz verhindert werden[11].

Es gibt viele Modelle, wie Risiken eingeteilt werden können. So unterscheidet man beispielsweise zwischen:

- *Grundrisiken*
  Das sind Risiken, die naturgegeben vorhanden sind oder bereits dann entstehen, wenn das Unternehmen die Geschäftstätigkeit aufnimmt. Sie sind untrennbar mit dem Unternehmen verbunden, die Ursache lässt sich nicht beseitigen. Ein Beispiel dazu sind Elementarrisiken wie Blitzschlag, Erdbeben, Brand oder Überschwemmung.
- *Ungewollt entstehende Risiken*
  Darunter werden Risiken verstanden, deren Ursache in einem Versehen, einer Fahrlässigkeit oder einem Irrtum liegen. Hierzu gehört das oft gebrauchte „menschliche Versagen“, von Mensch oder Maschine veranlasste Fehler oder auch Verschleiß.
- *Gewollt entstehende Risiken*
  Liegt dem Risiko ein Vorsatz zugrunde, dann hat man es mit einem gewollt entstehenden Risiko zu tun. Beispiele sind Manipulation, Ausspähung, Sabotage oder Diebstahl.

Man kann Risiken auch danach einteilen, an welcher Stelle das Risiko entsteht. In diesem Fall könnte man beispielsweise folgende Einteilung wählen:

- *Erkennungsrisiken*
  Darunter wird das Risiko verstanden, dass Brände, Fehler, Manipulationen etc. nicht oder nicht rechtzeitig erkannt bzw. bemerkt werden. Die IT-Revision würde in diesem Fall fragen, welche Ereignisse welche Meldungen auslösen (z.B. löst ein Brand einen Brandmelder aus).
- *Kontrollrisiken*
  Das sind Risiken, die dadurch entstehen, dass Kontrollen nicht vorhanden sind oder nicht greifen. Kontrollen können sehr unterschiedlicher Art sein: Es gibt Applikationskontrollen in Software-Systemen (z.B. Eingabeprüfungen), Nutzungskontrollen (mit Plausibilitätsprüfungen) oder IT-Verfahrenskontrollen (z.B. im Change-Management).
- *Entscheidungsrisiken*
  Risiken, die durch falsche, unvollständige oder zu späte/zu frühe Entscheidungen entstehen , können als Entscheidungsrisiken zusammengefasst werden.

---

[11] Alle Risiken zu verhindern, würde absolute Sicherheit bedeuten. Dies ist in der Praxis nicht möglich.

Weitere, mögliche Einteilungen:

- *Nach der Struktur des gesamten IT-Bereichs*
  Risiken in der Gestaltung der IT (technische Risiken), im Ablauf der IT (Prozessrisiken) und im Management der IT (Steuerungs- und Führungsrisiken).
- *Nach den Auswirkungen der Risiken*
  Risiken für Leib und Leben, finanzielle Risiken, Imagerisiken etc.

IT-Sicherheit äußert sich in drei grundlegenden **Sicherheitskriterien:**

- *Verfügbarkeit:* Schutz vor Verlust, Ausfall, Unterbrechung, Fehler und Störungen.
- *Vertraulichkeit:* Schutz vor Missbrauch, Ausspähung, unbefugter Verbreitung und unberechtigtem Zugriff.
- *Integrität:* Schutz vor Manipulation, Verfälschung und Betrug.

Es gibt nationale und internationale Sicherheitsstandards wie die IT-Grundschutzkataloge des BSI[12] oder die ISO[13]-Standardfamilie 2700x, die beschreiben, wie diese Sicherheitskriterien in der IT konkretisiert und umgesetzt sowie gemanagt werden können. Daneben erstellen viele Unternehmen (insbesondere große Unternehmen) eigene Sicherheitsrichtlinien für die Informationstechnik („IT Security Policies“).

In den Revisionsprüfungen der IT-Revision ist zunächst die Ordnungsmäßigkeit des Prüfobjekts hinsichtlich der Soll-Vorgaben für die IT-Sicherheit zu prüfen. Im Zentrum stehen dabei meist die internen Sicherheitsrichtlinien des Unternehmens, da die externen Sicherheitsstandards nicht unbedingt zwingend anzuwenden sind[14].

In einem zweiten Schritt gilt es zu prüfen, an welcher Stelle welche Risiken für das Unternehmen bestehen oder entstehen können.

1.4.4 Zweckmäßigkeit/Funktionsfähigkeit

Es liegt im Interesse des Unternehmens, nicht nur sicherzustellen, dass keine Strafen oder Risiken drohen, sondern auch zu untersuchen, ob das jeweilige Prüfobjekt seiner Bestimmung gerecht wird. Ein Maß dafür ist die Zweckmäßigkeit, die durch folgende Eigenschaften gekennzeichnet ist:

- *Funktionserfüllung*
  Die IT liefert termingerecht die geplanten/erwarteten Ergebnisse. Die Ergebnisse sind inhaltlich richtig und vollständig.
- *Effektivität*
  Die IT ist dazu geeignet, den ihr zugedachten Zweck zu erfüllen.

---

12 Bundesamt für Sicherheit in der Informationstechnik

13 International Organization for Standardization

14 Es sei denn, das Unternehmen oder eine übergeordnete Instanz (Muttergesellschaft, Holding o.Ä.) erklärt sie für das Unternehmen als verbindlich.

- *Ziel- und Strategiekonformität*
  Die IT stimmt mit der IT- und Geschäftsstrategie überein und unterstützt die Erfüllung der an sie gestellten Ziele.

In den Revisionsprüfungen der IT-Revision muss zunächst geklärt werden, wie die geplante Funktion beschaffen ist, welchem Zweck sie dienen soll und welche Ziele festgelegt wurden. Anschließend wird der bestehende Zustand erhoben, d.h. wie die Funktion aktuell beschaffen ist. Schließlich werden die vorhandenen Ziel- und Funktionsabweichungen festgestellt und Verbesserungsvorschläge vorgelegt. Die Funktionsprüfung wird auch als „Operational Auditing[15]“ bezeichnet

1.4.5 Wirtschaftlichkeit

Es geht in Revisionsprüfungen auch um das Aufspüren von Nachteilen für das Unternehmen. Auch wenn das Prüfobjekt ordnungsgemäß, sicher und zweckmäßig arbeitet, heißt das nicht, dass sich das Management entspannt zurücklehnen kann. Die Einhaltung dieser Prüfungsaspekte kann mit einem unverhältnismäßig hohen Aufwand erkauft worden sein oder das Anforderungsniveau ist so niedrig, dass Ressourcen verschwendet werden.

Aus diesen Gründen ist auch die Wirtschaftlichkeit ein wichtiger Prüfungsaspekt, der jedoch in vielen Fällen aus Zeitgründen nicht in jeder Prüfung zum Zuge kommt.

Unter dem betriebswirtschaftlichen Begriff der Wirtschaftlichkeit wird das Verhältnis zwischen dem Mitteleinsatz und dem damit erzielten Ergebnis (Erfolg) verstanden. Je höher der Mitteleinsatz für ein bestimmtes Ergebnis, desto geringer bzw. schlechter wird die Wirtschaftlichkeit.

In den Revisionsprüfungen der IT-Revision werden zunächst die Kennzahlen für das Ergebnis erhoben, z.B. Mengengerüste an Daten, die vom Prüfobjekt verarbeitet werden. In einem zweiten Schritt wird ermittelt, wie das Prüfobjekt dimensioniert ist und welcher initiale und laufende Aufwand damit verbunden war und ist. Damit ergibt sich, ob das Prüfobjekt hinsichtlich seiner Funktion und der erzielten Ergebnisse angemessen ist und wirtschaftlich arbeitet.

Beispiel: Ein IT-System der mittleren Datentechnik als reines E-Mail-System einzusetzen, um in der Bürokommunikation ein E-Mail-Aufkommen von täglich 1.000 E-Mails[16] zu bewältigen, kann sicher als unwirtschaftlich gelten und würde von der internen Revision zu Recht bemängelt, sofern keine gewichtigen Gründe für diese Dimensionierung vorliegen.

---

[15] Der Begriff stammt ursprünglich von der Untersuchung der Geschäftstätigkeit hinsichtlich Effektivität und Effizienz.

[16] Hier wird von „normalen“ E-Mails durchschnittlicher Größe und Komplexität ausgegangen.

1.4.6 Kontrollierbarkeit und Nachvollziehbarkeit

Ein Prüfungsaspekt, der besonders für die IT-Revision selbst von Bedeutung ist, stellt die Kontrollierbarkeit und die damit verwandte Nachvollziehbarkeit dar.

Für die Kontrollierbarkeit ist die Transparenz des Prüfobjekts entscheidend. Die Transparenz ist gegeben, wenn die Beschaffenheit des Prüfobjekts zeitnah (d.h. ohne unverhältnismäßig großen Aufwand) vollständig, klar und eindeutig ermittelt werden kann. Dies sollte möglich sein, ohne auf spezielle Personen angewiesen zu sein.

Um kontrollieren zu können, werden schließlich noch Richtwerte benötigt, deren Einhaltung bzw. Übereinstimmung geprüft werden kann.

Um eine Nachvollziehbarkeit einer Handlung, einer Systemeigenschaft, eines Entscheidungsprozesses etc. zu erreichen, gibt es hauptsächlich zwei Methoden:

- *Die Momentaufnahme (Snapshot)*
  Der Zustand wird in regelmäßigen oder unregelmäßigen Abständen in seiner Gesamtheit festgehalten. Das hat den Nachteil, dass Zustände zwischen den Momentaufnahmen nicht eindeutig festgestellt werden können.
- *Das Protokoll*
  Jede Veränderung an dem Zustand wird protokolliert. So lässt sich aus dem Ausgangszustand zu Beginn der Protokollierung der Zustand zu einem bestimmten Zeitpunkt rekonstruieren. Der Nachteil liegt in der Kompliziertheit und dem hohen Aufwand, der für eine solche Rekonstruktion getrieben werden muss.

Die Nachvollziehbarkeit ist wichtig, um Ereignisse und deren Entstehung nachweisen können. In den Revisionsprüfungen von IT-Verfahren und IT-Systemen wird daher auch geprüft, ob das Prüfobjekt über eine Protokollierung (Logging) verfügt.