Eine Veröffentlichung des ISACA Germany Chapter e.V.
Fachgruppe IT-Revision

Grundlagen der IT-Revision für den Einstieg in die Praxis

ISACA®
Trust in, and value from, information systems
Germany Chapter

dpunkt.verlag

Herausgeber:
ISACA Germany Chapter e.V.
Oberwallstrasse 24
10117 Berlin

www.isaca.de
info@isaca.de

ISACA-Fachgruppe IT-Revision (Autoren)

Autorenteam:
- Dr. Karlheinz Ahlers, CISA, KAI Consulting
- Markus Bank, CISA, Stuttgarter Straßenbahnen AG
- Axel Dors, CISA, KfW Bankengruppe
- Ingrid Dubois, dubois it-consulting gmbh
- Torsten Enk, CISA, BERLINCOUNSEL Consulting GmbH
- Jochen Hartmann, CISA, CISM, Schwarz Dienstleistung KG
- Ralf Herter, BASF Business Services GmbH
- Prof. Matthias Knoll, CISA, Hochschule Darmstadt
- Wolf-Rüdiger Mertens, CIA, CISA, CISSP, Deutsche Bundesbank
- Torsten Meyer, CISA, IBM Deutschland GmbH

Stand: Juli 2016 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe IT-Revision)

ISACA-Leitfaden

Grundlagen der IT-Revision für den Einstieg in die Praxis

ISACA®
Trust in, and value from, information systems
Germany Chapter

Vorwort

Da »Wegweiser« für Einsteiger in die IT-Revision im deutschsprachigen Raum bislang weitgehend fehlen und Literatur zum Thema IT-Revision vergleichsweise selten ist, kann die Orientierung im Rahmen des Aufbaus einer IT-Revision, etwa im Mittelstand, oder bei Einarbeitung in die Thematik entsprechend schwerfallen.

Gleichzeitig nimmt die Bedeutung der IT-Revision in den Unternehmen bedingt durch immer größere Abhängigkeit von der IT stark zu. Denn die zunehmende Komplexität der eingesetzten Architekturen und Technologien erfordert Strategien zum richtigen Umgang mit den damit verbundenen neuen Anforderungen. Zudem folgt aus stetig steigenden Compliance-Anforderungen und anderen Aspekten, etwa im speziellen Branchen- und Unternehmenskontext, sowie aufgrund immer aufwendigeren externen Prüfungen die Pflicht zu immer noch sorgfältigeren internen Vorbereitungen.

Das Ziel des Autorenteams der ISACA-Fachgruppe IT-Revision ist es daher, in Leitfadenform einen möglichst praxisnahen und kompakten Überblick sowohl über die Begriffe und Definitionen als auch über den IT-Revisionsprozess mit seinen Teilschritten und Werkzeugen bereitzustellen. Beispiele aus der Praxis sollen das Dargestellte verdeutlichen und Anleitungen sowie Templates bei Prüfungen unterstützen. Ergänzt wird der Text durch Handlungsempfehlungen und Hinweise auf weiterführende Informationen und Literatur von der ISACA und anderen Verbänden und Organisationen.

Die Information auf den folgenden Seiten erhebt keinen Anspruch auf Vollständigkeit. Ein Leitfaden zu einem Themenbereich, der kontinuierlich vielfältige Änderungen erlebt, kann in diesem Umfang niemals vollständig sein. Wir bitten daher um Ihr Feedback zu diesem Dokument, um die gesammelten Erkenntnisse im Rahmen späterer Überarbeitungen, zum weiteren Erfahrungsaustausch und für weitere Veröffentlichungen zu Ihrem Nutzen verwenden zu können.

Wir freuen uns auf Ihre Kritik, aber auch über Ihr Lob.
Sie erreichen uns unter:
leitfaden-it-revision@isaca.de

Die Autoren
Frankfurt, im Juli 2016

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

Inhaltsverzeichnis

1. Die Unternehmens-IT im Wandel – Auswirkungen auf die IT-Revision

Die Abhängigkeit vieler Unternehmen von der IT ist in den letzten Jahren in allen Branchen und unabhängig von der Unternehmensgröße deutlich gestiegen, ein Trend, der sich im Zeitalter der »digitalen Revolution« weiter verstärken wird.

Exkurs
Unternehmensbegriff

Zur Vereinfachung der weiteren Diskussion werden fortan unter dem Begriff »Unternehmen« neben juristisch selbstständigen privatwirtschaftlichen Unternehmungen (Kapitalgesellschaften, z.B. GmbH, AG; Personengesellschaften, z.B. KG, OHG, Einzelunternehmen) auch andere Organisationsformen verstanden. Unternehmen in diesem Sinne zeichnen sich durch eine festgelegte Aufbau- und Ablauforganisation (Prozesse) für den operativen Betrieb sowie Steuerungs- und Überwachungsfunktionen aus. Auch wenn verschiedene Aspekte bei gewinnorientierten Unternehmen stark abweichen, gelten bezogen auf Einsatz und Nutzung der IT sowie die Revisionsfunktionen vergleichbare Überlegungen in:

- Behörden und anderen öffentlichen Einrichtungen
- Anstalten des öffentlichen Rechts
- Gemeinnützigen bzw. nicht gewinnorientierten Organisationen (NPO)
- Vereinen und Stiftungen

Besonders betroffen sind etwa der Finanzdienstleistungsbereich, das Gesundheitswesen (»elektronische Gesundheitskarte«), die gesamte Energiewirtschaft (»Smart Grid«) und die Telekommunikationsbranche. Aber auch die Logistikbranche, der Maschinen- und Anlagenbau und viele andere Bereiche erfahren nicht zuletzt durch den Einsatz »intelligenter« Sensoren weitreichende Veränderungen (Stichworte: »Industrial Control Systems«, »Internet der Dinge«, »Cyber-physical Systems«). Bestimmte Geschäftsmodelle sind ohne IT überhaupt nicht umsetzbar, etwa Cloud-Angebote, soziale Netzwerke, Multimediaportale oder der Onlinehandel. Andererseits entstehen durch Hinzufügen von IT zu etablierten Produkten und Geschäftsmodellen vollkommen neue Konstruktionen. IT ist damit oftmals sowohl Prozessunterstützung als auch Service und Produktbestandteil. In der Regel steigen damit sowohl die Komplexität der eingesetzten IT-Anwendungen und der benötigten/eingesetzten IT-Infrastrukturen als auch der Kosten- und Effizienzdruck und die mit dem IT-Einsatz verbundenen (Sicherheits-)Risiken. Die zunehmend komplexen (regulatorischen, fachlichen oder durch den Markt bestimmten) Rahmenbedingungen erfordern eine sehr sorgfältige Begleitung durch die IT-Revision.

Viele Vorstände und Geschäftsführer fürchten neben persönlicher Haftung und finanziellen Verlusten nichts mehr als einen Vertrauensverlust bei Kunden und einen Imageverlust in der Öffentlichkeit. Denn technische Störungen oder fehlerhaft konzipierte bzw. konfigurierte Elemente in der IT können beispielsweise Unbefugten den Zugriff auf sensible Daten erleichtern. Durch solche Schwachstellen besteht die Möglichkeit, relevante Daten unbemerkt zu verändern oder bewusst zu manipulieren. Auch können durch Sicherheitsvorfälle die für einen Prozess oder ein bestimmtes Produkt notwendigen kritischen IT-Anwendungen nicht verfügbar sein.

Neben technischen Ursachen, die oft zitiert werden, verhalten sich leider häufig auch die Mitarbeiter selbst im Umgang mit IT-Anwendungen fahrlässig oder ggf. sogar vorsätzlich falsch. Die »Awareness« für die Risiken bei Einsatz und Nutzung von IT und damit auch das Bewusstsein für die Notwendigkeit von IT-Prüfungen werden neben anderen unternehmensrelevanten Elementen zu einem der wichtigsten Handlungsfelder, nicht nur innerhalb der IT-Bereiche, sondern im gesamten Unternehmen.

Aus Gesamtunternehmenssicht ist ein essenzielles Ziel, Informationssicherheit und Business Continuity zu gewährleisten und alle fachlichen Anforderungen abzudecken. Die IT-Revision unterstützt diese Bemühungen unmittelbar mit Blick auf das Business/IT-Alignment unter Nutzung eines angemessenen und wirksamen IT-Revisionsprozesses. Dessen Ergebnisse wiederum liefern für das unternehmensweite Risikomanagementsystem wertvolle Informationen.

1.1 Die Revision

Zu unterscheiden sind die externe und Interne Revision. Der wesentliche Unterschied liegt dabei in der organisatorischen Zuordnung, in den jeweils hauptsächlich maßgeblichen Prüfungsgrundlagen sowie in der Zielsetzung der Prüfungen.

Die **externe Revision** arbeitet

- im Auftrag der Unternehmensleitung oder der Aufsichtsorgane eines Unternehmens im Kontext der Zertifizierung der Internen Revision,
- als Wirtschaftsprüfer sowie
- im Auftrag der Internen Revision.

Für die externe Revision gelten teilweise zusätzliche Definitionen und Regelungen sowie ein spezielles, durch die Gesetzgebung und/oder Normungsgremien stark beeinflusstes Rahmenwerk aus Prüfungsstandards als Prüfungsgrundlage, die hier nicht weiter betrachtet werden sollen.

Die **Interne Revision** (fortan Revision) kann aus funktionaler und institutioneller Sicht betrachtet werden. Funktional führt die Revision Prüfungen mit eigenem, unabhängigem Personal durch. Im institutionellen Sinn ist Revision ein mit der Durchführung von Prüfungsaufgaben befasstes Element der Aufbauorganisation (etwa eine Abteilung oder eine Gruppe). Sie bildet die dritte Verteidigungslinie im Three-Lines-of-Defense-Modell (vgl. [Eulerich 2012] und [Ruud/Kyburz 2014]). Sie ist in der Regel der Unternehmensleitung direkt unterstellt und berichtet vorrangig an diese, in speziellen Fällen auch an das Aufsichtsorgan oder an einen in seinem Auftrag eingesetzten Prüfungsausschuss (Audit Committee). Die Revision unterstützt damit die Unternehmensleitung (Vorstand bzw. einzelne Mitglieder) bzw. die Aufsichtsorgane in ihrer Steuerungs- und Kontrollfunktion. In größeren bzw. komplexeren Organisationen kann es in den Fachbereichen zusätzliches Personal geben, das von der Abteilungsleitung benannt wird und der zentralen Revision als Ansprechpartner zur Verfügung steht, wenn sie den Fachbereich prüft. Dieses Personal übernimmt dann konsequenterweise auch eine erste Bewertung der Folgen der Prüfungsergebnisse für den Fachbereich (vgl. [Schmidt/Brand 2011, S. 11] und Abschnitt 7.4). Durch gesetzliche und regulatorische Vorgaben kann die Pflicht zur Einrichtung einer Revision und zur Wahrnehmung bestimmter Prüfungsaufgaben bestehen. In allen anderen Fällen orientiert sich die Revision primär an Unternehmensrichtlinien.

Neben der vorrangigen Unterstützung der Unternehmensleitung und der Kontrollorgane unterstützt die Revision durch Weitergabe der Revisionsergebnisse auch die Managementebene, die für die Umsetzung der Revisionsempfehlungen verantwortlich ist, und damit indirekt das gesamte Unternehmen. Im Vordergrund stehen dabei

- die Zuverlässigkeit und Vollständigkeit aller Daten des Rechnungswesens und anderer zentraler betrieblicher Funktionen,
- die Prüfung/Einschätzung der effizienten Implementierung und Ausführung aller Geschäftsprozesse,
- das Erreichen einer bestimmten Prozessleistung bzw. der angestrebten Prozessziele,
- die Sicherung des Betriebsvermögens und der Betriebskontinuität (Going-Concern-Prinzip).

In jüngster Zeit spielen oft auch Nachhaltigkeitsfragen (z.B. Umwelt, Ressourceneinsatz, Unternehmensethik) eine immer wichtigere Rolle.

Gleichzeitig grenzt sich die Revision im Sinne einer Aufgabentrennung (Segregation of Duty) gegen andere betriebliche Funktionsbereiche, insbesondere gegen das Controlling, das Qualitätsmanagement und die innerbetriebliche Beratung, ab. Sie unterstützt niemals direkt bei der Umsetzung von betrieblichen Zielen und Vorhaben (wie etwa Projekten) und ist damit nicht direkt an den Wertschöpfungsprozessen beteiligt. Dies dient der Unabhängigkeit der Revisionsfunktion.

Die **IT-Revision** ist Teil der **Revision**.

Exkurs
Abgrenzung der Revision gegen andere betriebliche Funktionen

Controlling
Das Controlling hat im Unternehmen die Aufgabe der finanziellen Planung und Steuerung, nicht einer Kontrolle im deutschen Wortsinn. Es unterstützt mit finanziellen Daten unternehmerische Entscheidungen und kann unter bestimmten Umständen der Revision Daten bereitstellen.

Unternehmensweites Risikomanagement (Enterprise Risk Management, ERM)
Zum unternehmensweiten Risikomanagement (das das IT-Risikomanagement einschließt) gehören Tätigkeiten zur Erkennung, Analyse, Bewertung, Behandlung und Kontrolle von Risiken einschließlich aller IT-Risiken. Revision und Risikomanagement sind dabei nicht voneinander abhängig. Vielmehr muss das Risikomanagement von der Revision geprüft werden.

Zwar benötigt auch die Revision ein Risikomanagement, jedoch nur, um die in ihren eigenen Revisionsprozessen liegenden Risiken angemessen zu behandeln.

Aus Sicht der Unternehmensleitung unterstützt eine effektive Revision, die idealerweise neben einer für das ERM zuständigen Organisationseinheit besteht, zwar die Fachbereiche (als erste »Verteidigungslinie« im Three-Lines-of-Defense-Modell) bei Verringerung der Risiken für das Unternehmen als Ganzes und damit auch für die Unternehmensleitung. Die Revisionstätigkeit ist jedoch niemals Maßnahme des Risikomanagements, sondern stellt neben dem Risikomanagement (als zweite »Verteidigungslinie«) die dritte »Verteidigungslinie« dar. Ob beide Verteidigungslinien, Risikomanagement und Interne Revision, wiederum Bestandteil des Internen Kontrollsystems (IKS) sind, ist nicht einheitlich definiert. Während im IDW PS 261 die Interne Revision als prozessunabhängige Überwachungsmaßnahme angesehen wird und Bestandteil des IKS ist, trennen §25a KWG und die MaRisk, AT1, das Interne Kontrollsystem und die Revision voneinander. →

Qualitätsmanagement

Das Qualitätsmanagement ist integraler Bestandteil eines Unternehmens. Es ist (auch in der IT) auf die Wirksamkeit der Prozesse (Zielerreichung, Effektivität, Effizienz) gerichtet. Im Rahmen des Qualitätsmanagements werden laufend und auf allen Ebenen innerhalb der Wertschöpfungskette Kontrollen und Messungen durchgeführt.

Inhouse-Beratung

Die Inhouse-Beratung konzipiert und optimiert neben anderen betrieblichen Funktionen auch die informationsverarbeitende Funktion. Darunter fallen insbesondere IT-Strategien, IT-Prozesse, IT-Architekturen und Technologien. Sie kann auch Implementierungsunterstützung leisten.

Definition »IT-Revision«

Die IT-Revision ist eine unabhängige und objektive Einheit zur systematischen, **risikoorientierten** und zielgerichteten **Prüfung aller informationsverarbeitenden Funktionen** im Unternehmen.

Die IT-Revision umfasst damit den gesamten IT-Lebenszyklus. Er beinhaltet alle strategischen Planungen und Entscheidungen (IT-Governance), die Entwicklung/Konzeption (Information Systems Development), die Beschaffung (Information Systems Acquisition), die Implementierung/das Change-Management (Information Systems Implementation), den Betrieb (Information Systems Operation), die Wartung (Information Systems Maintenance) und das IT-Servicemanagement.

Die Systematik der Prüfungs- und Beratungstätigkeiten der IT-Revision orientiert sich über die genannten Strukturen hinaus an den **für das Unternehmen relevanten (IT-)Risiken**. Weitere Grundlagen bilden beispielsweise ISACA- und IIA-Standards, das Information Technology Assurance Framework (ITAF) sowie die Standards für die Jahresabschlussprüfung (vgl. Kapitel 3).

Ziel der Prüfungstätigkeiten der IT-Revision ist die Verbesserung des IT-Risikomanagements und des IT-Risikomanagementprozesses sowie die Verbesserung aller von der IT abhängigen Prozesse eines Unternehmens in Bezug auf Steuerungs- und Kontrollmaßnahmen (engl. Controls) zur Risikobehandlung. Die IT-Revision unterstützt damit stets auch die Erreichung der Unternehmensziele, die Verbesserung der Unternehmenssteuerung und die Einhaltung von (internen und externen) Regelungen.

Dieses Verständnis folgt der Definition des Revisionsbegriffs der Internen Revision des Deutschen Instituts für Interne Revision e.V. (DIIR) bzw. des Institute of Internal Auditors (IIA)[1]:

»Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.«

Die organisatorische Zuordnung zur Unternehmensleitung verschafft der IT-Revision Gewicht und Respekt im Unternehmen. Wichtige Voraussetzung dafür ist, dass die Unternehmensleitung die IT-Revision ideell (»Management Commitment«) unterstützt und sie mit entsprechenden Vollmachten sowie Sach- und Personalmitteln zur Prüfung ausstattet. Eine weitere wichtige Voraussetzung ist die angemessene Form der Kommunikation mit der Unternehmensleitung und den Fachbereichen. Da viele Feststellungen der IT-Revision eher technischen Charakter haben, müssen sie so formuliert werden, dass sie verständlich sind und Ursachen und Auswirkungen nachvollzogen werden können. Dies kann etwa durch Wahl geeigneter Begriffe und Vergleiche aus der Fachdomäne der Vorstände oder auch durch Aufzeigen einer möglichen persönlichen Betroffenheit der Adressaten geschehen. Vergleichbares gilt für die Kommunikation mit den betroffenen Fachbereichen.

Eine Interne IT-Revision kann mit einer extern durchgeführten IT-Prüfung verglichen werden. Prüfungsgegenstände, Vorgehen sowie weitere Aspekte sind weitgehend mit externen IT-Prüfungen identisch. Hieraus ergibt sich auch die Notwendigkeit besonderer, IT-bezogener Fachkenntnisse der Prüfer (vgl. Kapitel 4).

Eine theoretisch denkbare Übernahme dieser prüfenden Tätigkeiten durch die Fachbereiche des Unternehmens verbietet sich (mit Ausnahme sog. Control Self-Assessments) aus mehreren Gründen:

- **Fehlendes Revisions-Spezialwissen**
  Für die Durchführung einer IT-Prüfung wird Spezialwissen benötigt, über das Fachbereiche selten verfügen. Fachbereiche wissen oftmals auch nicht, welche (technischen) Rahmenbedingungen und Vorgaben von der IT erfüllt werden müssen. Zudem müssen sich Fachbereiche mit Blick auf den Wettbewerb auf ihre Kernaufgaben konzentrieren (vgl. [Schmidt/Brand 2011, S. 3-8]).
- **Eigener Betrieb von zu prüfenden Anwendungen**
  Fachbereiche betreiben selbst teilweise zahlreiche und überaus komplexe Anwendungen (sog. »Schatten-IT«, »End-User-Computing«, »individuelle Datenverarbeitung«).

1 Vgl. *http://www.diir.de/fileadmin/fachwissen/revisionshandbuch-marisk.pdf.*

Auch sie bedürfen einer Prüfung. Eine unabhängige Prüfung ist hier jedoch nur durch eine unabhängige organisatorische Einheit sichergestellt.

- **Generell fehlende Unabhängigkeit und Objektivität**
  Das Fachbereichspersonal untersteht dem für den Fachprozess und seinen zugehörigen Anwendungen verantwortlichen Leitungspersonal[2]. Eine Prüfung durch eigenes Personal wäre also nicht unabhängig, eine objektive Berichterstattung gegenüber der Fachbereichsleitung kann so nicht gewährleistet werden.

Sonderfall »IT-Outsourcing«

Eine Sonderstellung in der Arbeit der IT-Revision nimmt das IT-Outsourcing ein. Unter IT-Outsourcing werden alle Formen der Auslagerung der IT zusammengefasst, darunter auch Cloud Computing. IT-Outsourcing kann sich auf einzelne oder alle Elemente von Informationssystemen und IT-Dienstleistungen wie beispielsweise Security Services, Entsorgung von Medien/Datenträgern und Webdienste beziehen. Im Kontext der aktuellen Cloud-Diskussion ist dabei insbesondere der Auslagerungsort von großer Bedeutung.

Für die IT-Revision gilt der Grundsatz, dass das auslagernde Unternehmen auch weiterhin die volle Verantwortung für das in den ausgelagerten Funktionen enthaltene Kontrollsystem und für die dazugehörigen Risiken trägt[3]. Die IT-Revision ist daher dafür verantwortlich, zu prüfen, ob die ausgelagerten Tätigkeiten mindestens denselben Vorgaben entsprechen, die auch im eigenen Unternehmen gelten. Der Outsourcing-Anbieter muss demzufolge entsprechende Auflagen des auslagernden Unternehmens prüfbar erfüllen.

Ob die IT-Revision beim Outsourcing-Partner Prüfungen vornehmen darf/kann, muss in der Regel vertraglich vereinbart werden oder wird durch einschlägige gesetzliche Regelungen vorgegeben (vgl. MaRisk AT 9 Tz. 6b) und 6c). Im Idealfall soll ein solches Prüfungsrecht erwirkt werden oder es sollten neutrale Dritte mit einer IT-Prüfung beauftragt werden können. Ein Verweis des Outsourcing-Anbieters auf entsprechende Prüfungsbescheinigungen (IDW PS 951, AT 801 / SSAE 16 und ISAE 3402) ist in der Regel nicht aussagekräftig genug. Vielmehr müssen die gesamten Prüfungsunterlagen vorgelegt und gesichtet und ggf. durch eigene Stichproben verifiziert werden. Auch Vor-Ort-Besuche sind statthaft und je nach Kritikalität und Komplexität der Prozesse, der Bedeutung eines Produkts und/oder spezieller IT-gestützter Funktionen empfehlenswert.

2 Als weitere Begründung kann auch IDW PS 261, RS FAIT 1, TZ 8 herangezogen werden, wonach das interne Überwachungssystem aus prozessintegrierten Maßnahmen (organisatorische oder systemseitige »Kontrollen« – durch die Fachbereiche) und prozessunabhängigen Maßnahmen (in der Verantwortung der Revision bzw. IT-Revision) besteht und somit eine Trennung unabdingbar ist.

3 Dieser Grundsatz leitet sich für rechnungslegungsrelevante Systeme oder deren IT-Infrastruktur aus den GoBD Rz 11 ab, für Systeme mit personenbezogenen Daten aus BDSG §11.

1.2 Zielsetzung der IT-Revision

Die IT-Revision ist durch ihre Ziele im Unternehmen mit einer Vielzahl von sehr unterschiedlichen Herausforderungen konfrontiert. Entsprechend muss die IT-Revision viele Themen im Blick behalten und gleichzeitig auf ihre Unabhängigkeit achten. Die IT-Revision unterstützt, analog zur Internen Revision, die Ziele des Unternehmens, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des IT-Risikomanagements sowie der zugehörigen Maßnahmen zur Risikobehandlung (als ein wesentlicher Bestandteil des IT-IKS) und der Führungs- und Überwachungsprozesse in der IT bewertet und diese verbessern hilft[4].

Zu den Unternehmenszielen mit Bezug zur IT gehören insbesondere:

- Vermeidung von Verstößen gegen Gesetze und andere Regelungen
- Langfristiger Schutz des Unternehmens vor (monetären und nicht monetären) Schäden aus und für die IT
- Erhaltung der Leistungsfähigkeit der IT und damit der Geschäftsprozesse und Geschäftsmodelle des Unternehmens
- Gewährleistung des Internen Kontrollsystems in der IT

Oberstes Ziel der IT-Revision ist es also, im Auftrag der Unternehmensleitung eine **Prüfungsaufgabe** für alle IT-relevanten Themen in allen Bereichen des Unternehmens (vgl. [Schmidt/Brand 2011, S. 4-7]) abhängig von deren jeweiligem Risikogehalt (Kritikalität für den betrachteten Geschäftsprozess/Geschäftserfolg) zu übernehmen und über die Revisionsergebnisse zur Verbesserung der Aufbau- und Ablauforganisation (Prozesse) beizutragen.

Die Aufgaben der IT-Revision entsprechen den Aufgaben der Internen Revision ergänzt um den Bezug zur IT (vgl. [Fochler et al. 2013, S. 20]):

- Prüfung der Einhaltung aller unternehmensexternen und -internen Regelungen in der und für die IT
- Prüfung der Wirtschaftlichkeit der IT
- Prüfung des Schutzes und der Sicherheit aller Informationssysteme, insbesondere der rechnungslegungsrelevanten IT-Systeme und Anwendungen

Ferner nimmt sie im Rahmen der ständigen Verbesserung (ggf. auf Initiative eines Fachbereichs) in genau abgesteckten Grenzen eine Beratungsfunktion wahr. Eine beratende Funktion erscheint, obwohl unter Unabhängigkeitsgesichtspunkten mitunter kontrovers diskutiert, durchaus sinnvoll und wichtig. Welcher Weg dabei der richtige ist, ist oftmals nicht leicht zu beantworten. Statt einer pauschalen Antwort erscheinen folgende Kriterien als Orientierungshilfe sinnvoll:

4 Vgl. *www.diir.de/fachwissen/revisionshandbuch-marisk/ziele-und-aufgabenstellung-der-internen-revision*

- Größe der (IT-)Revision: Je mehr Personal zur Verfügung steht, desto leichter kann die Beratung von der Prüfung getrennt werden.
- Es muss klar sein, dass die Beratung keine Vorgaben macht, sondern fundierte Vorschläge, die auch durch eigene Lösungen des Fachbereichs ersetzt werden können.
- Klare organisatorische Trennung von Beratung und Prüfung
- Zeitlicher Abstand der letzten Beratung zur nächsten Prüfung im betreffenden Sachgebiet, da bei der Prüfung die Neutralität gewahrt bleiben muss.
- Abstraktheit der Empfehlungen: Je methodischer die Beratung, desto geringer die Gefahr des Verlustes der Unabhängigkeit.
- Vollständige und verständliche Dokumentation aller Beratungsvorgänge und deren Ergebnisse

Wichtig sind zudem ein einheitliches Verständnis vom Begriff der IT-Revision im gesamten Unternehmen und klar definierte und dokumentierte Prozesse für die Arbeit der IT-Revision.

1.3 Nutzen der IT-Revision

Externe Einflüsse wie Gesetze, Verordnungen und verbindlich einzuhaltende (Prüfungs-)Standards sorgen für die Notwendigkeit, eine IT-Revision mit entsprechendem Fachwissen einzurichten. Aber auch die wachsende Komplexität und die immer kürzeren Entwicklungszyklen der IT-Prozesse sowie die stetig steigende Verflechtung mit Fachprozessen begründen die Notwendigkeit, die in diesem Zusammenhang stehenden Arbeiten und Ergebnisse einer Prüfung zu unterziehen. Der Mehrwert einer effektiv arbeitenden IT-Revision für die Unternehmen ist entsprechend vielfältig. Dies gilt auch dann, wenn er von den geprüften Bereichen mitunter angezweifelt wird, sich manchmal erst mit einigem Zeitversatz zeigt oder ein gewisser Mehraufwand notwendig ist, um die Erfolge quantifizieren zu können.

Ein Fehlen von IT- und IT-Revisions-Spezialwissen führt in der Praxis oft dazu, dass klassische, durch die Interne Revision initiierte, technisch geprägte Prüfungen den hohen und komplexen IT-Risiken (die auch Informations- und Informationssicherheitsrisiken umfassen) nicht mehr gerecht werden. Unternehmensinterne Messinstrumente helfen festzustellen, inwieweit eine IT-Revisionsfunktion dabei unterstützt, Abläufe angemessener und wirksamer zu gestalten. Diese tragen damit zu einer Verbesserung der Faktoren Kosten, Zeit, Qualität und Sicherheit bei.

Eine Abgrenzung von der laufenden Optimierungstätigkeit der IT-Abteilung selbst fällt in der Praxis zwar häufig schwer, ist aber möglich. Beispiele für das effektive Wirken einer IT-Revision sind:

- Ein Sinken sicherheitsrelevanter Vorfälle (Security Incidents)
- Die Initiierung eines Projekts zur Abschaltung eines teuren und schwer zu betreuenden Altsystems (sog. Legacy-System)
- Die zusätzliche und sinnvolle Aus- und Fortbildung von Mitarbeitern in sensiblen oder wissensintensiven Bereichen
- Die Erhöhung der IT-Sicherheit durch die Etablierung einer weiteren Kontrollinstanz
- Die Einhaltung von externen Compliance-Vorschriften, zu denen oft kein umfassendes Fachwissen in den Fachbereichen existiert.

Der Mehrwert der IT-Revision ergibt sich also ausgehend von einer intensiven Beschäftigung mit den Prüfungsfeststellungen durch schrittweise Veränderungen über Hinzulernen und die daraus erfolgten Korrekturen bzw. Verbesserungen (Ursachensuche, Abstellen der Fehlerquelle und Verhindern des Wiederauftretens an gleicher oder anderer Stelle). Neben einer risikoorientierten Betrachtung rücken damit auch realisierbare Chancen im betroffenen Themengebiet durch Optimierungen stärker in den Vordergrund.

2. Grundlagen: Begriffe und Definitionen

Jedes Unternehmen verfügt über mehr oder weniger individuell ausgeprägte IT-Systeme. Entsprechend heterogen sind die IT-Landschaften, die IT-Revisoren antreffen. Häufig ist es nur mit Spezialkenntnissen und Erfahrungen möglich, Zusammenhänge zwischen Anwendungen, Schnittstellen und IT-Prozessen zu erkennen und in der Prüfung zu berücksichtigen. Mitunter bleibt es auch für Revisoren mit langjähriger Prüfungserfahrung eine Herausforderung, alle Details nachzuvollziehen und zu durchdringen – etwa in komplexen SAP-Installationen.

Die nachfolgenden Abschnitte erläutern wichtige, in der IT-Revision gebräuchliche Begriffe und enthalten Hinweise auf einführende Literatur, wenn einzelne Aspekte der IT nicht ausführlich dargestellt sind. Denn für den IT-Revisor ist es oftmals hilfreich, ein Modell zu entwerfen, das die Einordnung neuer Sachverhalte erleichtert. Ziel ist es, innerhalb des Unternehmens ein einheitliches Begriffsverständnis über die genutzte IT zu erzielen.

Wird dieses einheitliche Begriffsverständnis nicht erreicht, drohen im gesamten Revisionsprozess Missverständnisse und Fehler, die zu unnötigen Schuldzuweisungen und Verzögerungen führen können.

2.1 Das Informationssystem als soziotechnisches System

Ein Informationssystem ist ein soziotechnisches System. Es besteht aus technischen (Hardware, Software, Daten), organisatorischen (Rollen und Berechtigungen) und fachlichen Komponenten (Geschäftsprozesse) und beinhaltet verschiedene zu schützende Werte unterschiedlicher Komplexität. Sein primärer Zweck ist die Be- und Verarbeitung (Erzeugen, Erheben, Lesen, Schreiben, Sperren, Löschen), Übertragung und Speicherung von Daten zum Zweck einer zielgerichteten Nutzung.

Als IT-System gilt hierbei innerhalb des Informationssystems die Kombination aus Hardware, Betriebssystem, Middleware und Software, wobei die Software auch alle hardwarenahen Teile (etwa Firmware) umfasst. Netzwerkkomponenten bestehen sowohl aus Hardware (Netzwerkkarte, Appliance) als auch aus Software (Kommunikationssoftware, Firmware, Konfigurationseinstellungen in Appliances). Für die hardwarenahen Elemente eines IT-Systems werden die Begriffe »Informationstechnik« bzw. »Informationstechnologie« oft auch synonym verwendet. Die Hardware bildet die technische Infrastruktur, die Software umfasst (parametrisierte) Anwendungen bzw. Services. In Anlehnung an COBIT 5 (vgl. [ISACA 2012, S. 15]) stellt ein IT-System damit den Enabler »technische Infrastruktur (einschließlich Netze), Anwendungen bzw. Services« im Sinne des serviceorientierten Paradigmas zur Verfügung.

Es ist jedoch nicht ausreichend, ausschließlich eher technische Aspekte der Daten- bzw. Informationsverarbeitung mithilfe eines IT-Systems zu betrachten. Es ist vielmehr notwendig, grundsätzlich alle – in COBIT 5 (vgl. [ISACA 2012, S. 15]) definierten – Enabler-Kategorien zu betrachten:

1. Infrastruktur, Anwendungen und Services
2. Prinzipien, Richtlinien und Rahmenwerke
3. Prozesse
4. Organisationsstrukturen
5. Kultur, Ethik und Verhalten
6. Informationen
7. Mitarbeiter, Fähigkeiten und Kompetenzen

Für die IT-Revision ergeben sich daraus die folgenden relevanten Elemente, die entsprechend ihren jeweiligen Inhalten gemeinsam ein Prüfungsobjekt bilden und bewertet werden müssen:

- **Hardware** – Enabler 1
- **Software** (Betriebssystem und Middleware (Dienste, wie Active Directory o.Ä., Verschlüsselung, Berechtigungs- sowie Identity und Access Management), Datenbank- und Applikationsebene, Schichtenmodell) – Enabler 1
- **Netzwerk** (Datenübertragung, Schnittstellen) – Enabler 1
- **Personal** (Fachbereich und IT) – Enabler 4, 5 und 7
- **Prozesse** (technische und fachliche, hierzu zählen auch alle Projekte) – Enabler 3
- **Daten** (Stamm-/Bewegungsdaten, Datenqualität, Klassifikation – Schutzbedarf) – Enabler 6
- **Organisatorische Regelungen** (ergänzend zu den Prozessen/Projekten) – Enabler 2

Weitere Modelle für Informationssysteme enthalten beispielsweise auch ITIL und TOGAF.

Das Institut der Deutschen Wirtschaftsprüfer (IDW) greift auf eine ähnliche Systematik zurück. Es fasst die gesamte rechnungslegungsrelevante IT-Infrastruktur, die IT-Anwendungen und die IT-gestützten Geschäftsprozesse zu einem IT-System zusammen.

Zur Vertiefung
Literatur zu IT-Grundlagen

Abts, D.; Müldner, W.: Grundkurs Wirtschaftsinformatik: Eine kompakte und praxisorientierte Einführung. 8. Aufl., Wiesbaden, 2013.

Krcmar, H.: Informationsmanagement. Berlin, Heidelberg, 2010.

Moeller, R. R.: Executive's Guide to IT Governance: Improving Systems Processes with Secure Management, COBIT, and ITIL. ISACA Bookstore, 2013.

Schwarzer, B.; Krcmar, H.: Wirtschaftsinformatik: Grundlagen betrieblicher Informationssysteme. 5. Aufl., Stuttgart, 2014.

Stenzel, J. P.; Cokins, G.; Schubert, K. D.; Hugos, M.: CIO Best Practices: Enabling Strategic Value with Information Technology. 2. Aufl., ISACA Bookstore, 2010.

Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 5. Aufl., München, 2013.

Wright, C.: Agile Governance and Audit – An Overview for Auditors and Agile Teams. ISACA Bookstore, 2014.

CISA-/CISM-/CRISC-Exam Resources, ISACA Bookstore

2.2 Wichtige Begriffe im Prüfungskontext

Die nachfolgenden Abschnitte thematisieren wichtige Aspekte im Rahmen des Prüfungskontextes, die in den weiteren Kapiteln dieses Leitfadens an unterschiedlicher Stelle wieder aufgegriffen und daher an dieser Stelle zusammengefasst werden.

2.2.1 Audit Charter

Die **Audit Charter** ist das offizielle Genehmigungsdokument für die IT-Revision sowie für externe Prüfungen. Die Unternehmensleitung oder der Prüfungsausschuss legen in der Audit Charter Zweck, Rechte und Pflichten sowohl des Prüfenden als auch des Geprüften sowie den Gültigkeitszeitraum der Charter selbst fest. Vor Verabschiedung und Inkrafttreten der Charter wird das Dokument mit allen betroffenen Bereichen abgestimmt.

Hinweis auf IT-Prüfungsstandard (ITAF)

Anforderungen an die Audit Charter sind in dem IT-Prüfungsstandard »1001 – Audit Charter« der ISACA (vgl. Abschnitt 3.1.2) definiert.

2.2.2 Prüfungsstrategie

Zu Beginn der Prüfungsplanungen soll die **Prüfungsstrategie** festgelegt werden. Dazu müssen Informationen über das Unternehmen gesammelt oder aktualisiert werden.

Die Festlegung der Prüfungsstrategie beinhaltet stets die Beurteilung von inhärenten Risiken und Kontrollrisiken, auch über die rein technische Betrachtung der IT-Systeme hinaus. Weiterhin wichtig ist deshalb das Wissen über die Geschäftstätigkeit sowie die Branchenzugehörigkeit des zu prüfenden Unternehmens einschließlich aller wesentlichen branchenspezifischen Informationen. Zudem sind die Bedürfnisse interessierter Parteien (Aufsichtsbehörden, Gesellschafter, Mitarbeiter, Kunden usw.) zu beachten. Auch sie beeinflussen die Unternehmensstrategie und damit Risiken und Chancen für die IT.

Auf Basis dieser Informationen werden die Geschäftsziele des Unternehmens bzw. der einzelnen Unternehmenseinheiten und die zu ihrer Erreichung etablierten Geschäftsprozesse sowie die sie unterstützenden IT-Systeme identifiziert. Hieraus wiederum lassen sich in den einzelnen Unternehmenseinheiten IT-Kontrollziele ableiten. Darauf aufbauend muss die IT-Revision zu den IT-Kontrollzielen diejenigen IT-Risiken identifizieren, die die Erreichung der Kontrollziele gefährden. In einem folgenden Schritt müssen geeignete Maßnahmen identifiziert werden, um diesen IT-Risiken angemessen zu begegnen. Zur Orientierung kann beispielsweise das Ergebnis der vorangegangenen Revision herangezogen werden.

Im Rahmen der Entwicklung einer Prüfungsstrategie müssen bei der Beurteilung von inhärenten Risiken schließlich folgende Gründe für das Entstehen von IT-Risiken in Betracht gezogen werden (vgl. [ISACA 2012, Ziffer 18]):

- Zunehmende Abhängigkeit der Unternehmen von der IT
- Größere Änderungsprojekte in der IT, die durch die Einführung neuer IT-Systeme und Technologien, aber auch durch die Einführung von Standardsoftware bedingt sein können
- Überlastungen in der IT und im Fachbereich aufgrund fehlender Ressourcen
- Unzureichende Pflege und Fehlbedienung der IT-Systeme aufgrund von beispielsweise unzureichendem Know-how
- Mangelhafte Ausrichtung der IT auf Geschäftsstrategien und Prozessanforderungen
- Bei länderübergreifender Organisation und Aufgabenverteilung: Sprachprobleme und kulturelle Unterschiede
- Zunehmende Regulierung (bspw. BDSG, GoBD, IT-SiG, EnWG)
- Zunehmende Bedrohungen von außen

Weitere Faktoren, die bei der Planung der Prüfungsstrategie in Betracht gezogen werden müssen, sind Wechselwirkungen der IT-Systeme und das Änderungsmanagement im Rahmen der Updates von Hardware und Software sowie deren Einfluss auf die Leistungserstellung (Business Impact).

2.2.3 Audit Universe (Prüfungsuniversum) und Prüfungsobjekte

Das Audit Universe, die **Gesamtheit aller Prüfungsobjekte**, ist die Basis der Prüfungsplanung. ISACA definiert das Audit Universe als »an inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process«[1]. Das Audit Universe muss regelmäßig aktualisiert werden, um Änderungen im Gesamtrisikoprofil des Unternehmens korrekt widerzuspiegeln. Es sollte alle Bereiche des Unternehmens abdecken und keinen »prüfungsfreien Raum« (»white spots«) lassen.

Das Audit Universe ist hierarchisch strukturiert:

1. Ebene: Mithilfe der **Prüfungsgebiete** werden die Prüfungsfelder strukturiert.
2. Ebene: **Prüfungsfelder** fassen bestimmte Prozesse und die betroffenen Organisationseinheiten zusammen. Ein Beispiel ist etwa der IT-Betrieb oder die Softwareentwicklung in Verbindung mit einer Landesgesellschaft oder einer inländischen Tochtergesellschaft. Dabei kann – je nach Unternehmen – die Organisationsstruktur Teil des Audit Universe sein oder auch nicht.
3. Ebene: **Teilprüfungsfelder** fassen zur besseren Übersicht verschiedene Prozesse zu Prozessgruppen zusammen.
4. Ebene: **Prüfungsobjekte** in Form von IT-Prozessen und zugehörigen Ressourcen sowie Fachprozessen und zugehörigen Ressourcen (IT-Systeme, Anwendungen). Aus einer risikoorientierten Betrachtung der Prüfungsobjekte folgen die Prüfungsaspekte (vgl. Abschnitt 2.2.5).

Die **Prüfungsobjekte** müssen alle wesentlichen (Fach-)Prozesse und Wertschöpfungsketten umfassen[2], systematisch gebildet und nach Risikogehalt kategorisiert werden. Dies schließt auch die funktionalen und operativen Bereiche sowie Produkte und Systeme bzw. alle zur Prozessdurchführung notwendigen Ressourcen ein.

IT-Prozesse, die die Revision prüfen sollte, sind:

- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Release & Deployment Management
- Security Management
- User Access & Privilege Management
- Licence Management
- Service Level Management
- Availability Management
- IT Service Continuity Management (einschl. Backup- und Data-Recovery-Management)
- IT Supplier Management (Management der – technischen – Vorgaben für den Einkauf)
- Facility Management für die IT-Infrastruktur (einschl. physische Sicherheit)

Die zu prüfenden Prozesse umfassen alle IT-Systeme, insbesondere jahresabschlussrelevante Systeme sowie alle für den Betrieb unverzichtbaren Systeme. Ebenso gehören alle organisatorischen Einheiten dazu, die im Rahmen der üblichen Prüfungszyklen geprüft werden (müssen). Wesentliche Bestandteile des Audit Universe sind daher die IT-Prozesse, Anwendungen und Systeme, die ausgehend von der IT-Strategie unter Beachtung der internen (Unternehmensziele und -abläufe) und externen (gesetzlichen, regulatorischen, vertraglichen) Anforderungen implementiert sind, um die Geschäftsprozesse des Unternehmens (Geschäftsbetrieb) zu unterstützen. Hinzu kommen Prozesse, Anwendungen, Dienste und Systeme, die für den Aufbau und Betrieb der IT selbst benötigt werden, und das Managementsystem, das die Implementierung und Umsetzung steuert und überwacht.

Grundsätzlich sind alle Elemente der Aufbau- und Ablauforganisation für die Aufstellung des Audit Universe zu betrachten. Es ist wesentlich, dass die Aufstellung vollständig ist. Diese Gesamtheit der Prüfungsthemen (auch als »Brutto«-Betrachtung bezeichnet) kann jedoch im Rahmen konkreter Prüfungsplanungen durch eine risikoorientierte Eingrenzung und Gewichtung auf alle tatsächlich verbleibenden Prüfungsinhalte (entsprechend als »Netto«-Betrachtung bezeichnet) reduziert werden. Im Rahmen der Durchführung einzelner Prüfungen können so zudem die einzelnen Prüfungsobjekte im Audit Universe risiko- und themenorientiert zu Prüfungsfeldern oder Teilprüfungsfeldern zusammengefasst werden.

Aus dem Inhalt des Audit Universe leiten sich dann die (Jahres-)Prüfungsplanung sowie die Planung der konkreten Prüfung(en) ab.

2.2.4 (Jahres-)Prüfungsplan

Im Prüfungsplan legt die Revision fest, welche Prüfungsobjekte bzw. Prüfungsgegenstände aus dem Audit Universe in welchem Prüfungszyklus betrachtet werden sollen.

Man unterscheidet

- mehrjährige,
- jährliche,
- unterjährige,
- rollierende

Prüfungsplanungen.

Revisionen sollen innerhalb von drei bis fünf Jahren das gesamte Audit Universe durch Prüfungen abdecken. Die **mehrjährige Prüfungsplanung** soll dies sicherstellen und im Mehrjahresprüfungsplan darstellen.

1 Vgl. *www.isaca.org/Knowledge-Center/Lists/ISACA%20Glossary%20Terms/DispForm.aspx?ID=1011.*

2 Vgl. *http://www.diir.de/fachwissen/revisionshandbuch-marisk/standardrevisionsprozess, Abschnitt 4.1.1.1.*

Im **Jahresprüfungsplan** legt die Revision fest, welche Prüfungsobjekte bzw. Prüfungsgegenstände aus dem Audit Universe im kommenden Prüfungsjahr betrachtet werden sollen. Diese sind oft durch bereits vorliegende Auditergebnisse sowie durch Nachprüfungsbedarf oder auch von der in der Regel jährlichen, unternehmensweiten Risikoanalyse mitbestimmt.

Im **unterjährigen Prüfungsplan** wird die zeitliche Anordnung der im Jahresprüfungsplan festgelegten Prüfungsobjekte bzw. Prüfungsgegenstände vorgenommen und ggf. werden kurzfristig relevante, neue Erkenntnisse (z.B. neue Risiken oder Kapazitätsänderungen bei den Prüfern) berücksichtigt.

Die **rollierende Prüfungsplanung** ist eine alternative, flexible Planungsmethode zur mehrjährigen und Jahresprüfungsplanung. Bei der **rollierenden Prüfungsplanung** wird ständig risikoorientiert neu festgelegt, welche Prüfungsobjekte bzw. Prüfungsgegenstände aus dem Audit Universe in den kommenden Prüfungen betrachtet werden sollen.

2.2.5 Prüfungsaspekte und Prüfungsziele

Prüfungsaspekte sind Aspekte, auf die ein Prüfungsobjekt hin geprüft werden soll. Entsprechend dem risikoorientierten Ansatz der Revision sind dies die Risiken, die die Erreichung der vom Unternehmen angestrebten Ziele gefährden. **Prüfungsziel** ist hierbei die Beurteilung der Prüfungsobjekte im Hinblick auf die Prüfungsaspekte.

Die häufigsten IT-bezogenen Prüfungsziele sind:

- **Angemessenheit (Eignung, Zweckmäßigkeit)**
  Die Angemessenheit bezieht sich auf alle organisatorischen, personellen und technischen Maßnahmen im Rahmen eines IT-IKS. Prüfungsaspekte sind sowohl das Design der einzelnen Maßnahmen (Steuerungs- und Kontrollmaßnahmen) als auch ihr Zusammenspiel innerhalb des IT-IKS.
- **Wirksamkeit (Funktionsfähigkeit, Effektivität)**
  Die Wirksamkeit betrifft die Frage, ob die vorgesehenen Steuerungs- und Kontrollmaßnahmen tatsächlich gewährleisten, dass das angestrebte (Prozess-)Ziel erreicht wird.
- **Rechtmäßigkeit**
  Rechtmäßigkeit impliziert die Einhaltung von Gesetzen und anderen rechtlich bindenden Vorschriften. Bei einer Prüfung der Rechtmäßigkeit wird geprüft, ob die physische und technische Beschaffenheit der IT, die Abläufe der IT sowie das IT-Management die externen Anforderungen erfüllen.
- **Ordnungsmäßigkeit (Compliance)**
  Ordnungsmäßigkeit geht über die auf die Erfüllung von gesetzlichen und anderen rechtlich bindenden Vorschriften ausgerichtete Rechtmäßigkeit hinaus. Sie umfasst zusätzlich die Erfüllung von bindenden, vertraglichen Vereinbarungen und internen Vorgaben und Regelungen. Auch wenn zwischen formeller und materieller Ordnungsmäßigkeit unterschieden werden kann, sollte sich die Revision bei der Prüfung der Compliance mit intern vorgegebenen Vorschriften nicht darauf beschränken, die buchstabengetreue Beachtung dieser Vorschriften (formelle Ordnungsmäßigkeit) zu prüfen. Vielmehr sollte sie stets auch die materielle Ordnungsmäßigkeit und damit die Angemessenheit der internen Vorschriften bewerten.
- **Sicherheit**
  Das Prüfungsziel Sicherheit betrifft in der IT den Schutz der IT-Systeme und Daten vor sämtlichen Formen der Beeinträchtigung.

  IT-Sicherheit muss die drei zentralen Ziele der Informationssicherheit erfüllen:

  - **Vertraulichkeit** (Schutz gegen Ausspähen und unbefugte Verbreitung von Daten),
  - **Integrität** (Schutz gegen Manipulation und unbefugte Veränderung von Daten und IT-Systemen) und
  - **Verfügbarkeit** (Schutz gegen unberechtigtes Vorenthalten oder Zerstören von Daten und Ausfall oder Unzugänglichkeit eines IT-Systems)

  sowie ergänzend

  - **Authentizität** (d.h. die eindeutige Zuordnung zu einem Sender, wobei dies nicht auf Personen beschränkt ist. Im Internet der Dinge (Maschine-zu-Maschine-Kommunikation) soll etwa sichergestellt sein, dass die richtige/autorisierte Maschine, der richtige/autorisierte Prozess/Service kommuniziert),
  - **Nichtabstreitbarkeit** (d.h. die Verbindlichkeit des Nachweises einer Aktivität; engl. non-repudiation).

  Die IT-Grundschutz-Kataloge des BSI oder die ISO/IEC-Reihe 27000 ff. können bei der Konkretisierung, Umsetzung und dem Management dieser Aspekte Hilfestellung leisten[3].

- **Wirtschaftlichkeit (Effizienz)**
  Die Wirtschaftlichkeit ist das Verhältnis zwischen dem Mitteleinsatz und dem erzielten Ergebnis beim Einsatz von IT-Systemen und in allen Prozessen. Auch in der IT-Prüfung ist die Wirtschaftlichkeit ein wichtiges Prüfungsziel. Deshalb sollte ein Prüfungsaspekt auch daraufhin untersucht werden, ob die Regelung und die praktische Handhabung zur Erreichung eines Ergebnisses den damit verbundenen Aufwand rechtfertigen oder ob dasselbe Ergebnis mit geringerem Aufwand ebenso erreicht werden kann.

Praxisbeispiel

»Ziel der Prüfung ist die Beurteilung der Angemessenheit (einschl. Ordnungsmäßigkeit und Sicherheit) und Wirksamkeit des User Access & Privilege Management.«

3 Zu beachten ist dabei allerdings, dass in beiden Standards die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit nicht identisch definiert sind.

2.2.6 Prüfungsarten

Im Rahmen der Planung einer konkreten Prüfung ist festzulegen, welchen Charakter die Prüfung hat (Prüfungsart). Zur Systematisierung der Prüfungsart existieren mehrere Klassifikationen. Das gemeinsame Ziel aller Prüfungsarten ist es, Risiken der im Unternehmen eingesetzten IT und den Umgang mit ihnen zu identifizieren, zu analysieren und zu beurteilen.

Die für die IT-Revision wichtigsten Prüfungsarten sind:

a. IT-Systemprüfungen
Eine IT-Systemprüfung gliedert sich gemäß Prüfungsstandard IDW PS 330 in

- Aufnahme des IT-Systems,
- IT-Aufbauprüfung (Verfahrens-/Prozessprüfung bzw. Angemessenheitsprüfung) und
- IT-Funktionsprüfung (Wirksamkeitsprüfung).

Art und Umfang der IT-Systemprüfung ergeben sich aus der Wesentlichkeit des IT-Systems sowie aus der Komplexität des IT-Systems. Ausgelagerte Bestandteile des IT-Systems müssen ebenfalls geprüft werden (vgl. [IDW PS 330, Zf. 8-13]).

Nach dem Verständnis einer IT-Systemprüfung erfolgt im Rahmen der Prüfung ein Abgleich zwischen den aus Gesetzen und sonstigen Vorgaben begründeten Anforderungen an beispielsweise eine IT-gestützte Rechnungslegung (Sollzustand der IT) und dem Istzustand im Unternehmen. Hierbei wird insbesondere die Sicherheit und Ordnungsmäßigkeit der IT beurteilt. Die IT-Systemprüfung unterscheidet dabei in Prüfungsgegenstände bzw. Prüfungsgebiete (IT-Infrastruktur, IT-Anwendungen, IT-gestützte Geschäftsprozesse, IT-Umfeld und IT-Organisation), Prüfungsziele und Prüfungskriterien. Bei den Kriterien liegt der Fokus auf der Ordnungsmäßigkeit der Rechnungslegung mithilfe der IT, insbesondere im Hinblick auf Vollständigkeit, Richtigkeit, Zeitgerechtigkeit, Nachvollziehbarkeit und Unveränderlichkeit. Im Rahmen der dafür notwendigen Sicherheit der IT werden Authentizität, Autorisierung, Vertraulichkeit, Verbindlichkeit, Integrität und Verfügbarkeit betrachtet.

b. Verfahrens-/Prozessprüfungen
Verfahrens- und Prozessprüfungen konzentrieren sich auf die Untersuchung von Abläufen und allen in ihnen relevanten Elementen sowie den dazugehörigen Steuerungs- und Kontrollmaßnahmen. Zu den relevanten Elementen zählen etwa alle Aktivitäten, Ablaufregelungen und die Organisationsstruktur (Aufbau), in die die Verfahren und Prozesse eingebunden sind.

c. Angemessenheitsprüfungen
Im Rahmen von Angemessenheitsprüfungen gemäß Definition in Abschnitt 2.2.5 wird ermittelt, ob Maßnahmen für den ihnen zugedachten Zweck sinnvoll dimensioniert und ausgerichtet sind. Betrachtet werden neben technischen und organisatorischen Fragen auch betriebswirtschaftliche und rechtliche Aspekte. Zu schwache Maßnahmen, die das zu kontrollierende Element nicht oder nicht vollständig erfassen, oder zu starke Maßnahmen gelten demnach als nicht angemessen.

Der Prüfer unterstellt dabei, dass die Maßnahmen wie geplant durchgeführt werden und wirksam sind. Das Prüfungsergebnis ist eine Aussage darüber, ob die vorgesehenen Maßnahmen geeignet sind, das Risiko angemessen zu behandeln.

d. Wirksamkeits- bzw. Funktionsprüfungen
Wirksamkeitsprüfungen (Funktionsprüfungen) gemäß Definition in Abschnitt 2.2.5 untersuchen, ob die als angemessen bewerteten Maßnahmen tatsächlich so arbeiten, wie es ihre Spezifikation vorsieht. Eine Maßnahme gilt auch als unwirksam, wenn sie leicht umgangen werden kann.

e. Erhebungsprüfungen
Eine Ausnahme bezüglich des Prüfungsziels »Beurteilung« stellen reine Erhebungsprüfungen dar, weil bei ihnen nur eine Aufnahme der relevanten IT-Systeme, Verfahren und Prozesse stattfindet und insbesondere keine Bewertung der Angemessenheit oder Wirksamkeit erfolgt. Erhebungsprüfungen dienen im Wesentlichen der Aktualisierung des Audit Universe und zur Vorbereitung der Prüfungsplanung.

f. Continuous Auditing (Continuous Auditing Approach)
Weder in der aktuellen Literatur noch bei den internationalen Berufsverbänden ISACA und IIA existieren eindeutige Begriffsdefinitionen und -abgrenzungen zwischen »Continuous Auditing« und »Continuous Monitoring«. Hierdurch werden diese beiden Begriffe häufig synonym oder widersprüchlich genutzt.

Die ISACA-Fachgruppe IT-Revision hat sich daher zur Abgrenzung auf folgende Begriffsdefinitionen verständigt:

»Continuous Auditing« ist eine kontinuierliche, manuelle oder maschinell unterstützte Überwachung des gesamten Audit Universe auf Veränderungen, die Auswirkungen auf die risikoorientierte Prüfungsplanung haben könnten.

Ergänzend hierzu beschreibt das ISACA Glossary of Terms den Begriff »Continuous Auditing Approach« (Kontinuierlicher Prüfungsansatz) als Überwachung der Systemzuverlässigkeit auf einer kontinuierlichen Basis, um selektiv Prüfungsbeweise computergestützt zu sammeln. Damit ähnelt der Begriff »Continuous Auditing Approach« dem »Continuous Monitoring«. Der wesentliche Unterschied liegt in der selektiven Nutzung der gesammelten Daten.

Exkurs
Continuous Monitoring

»Continuous Monitoring« ist eine systemorientierte, kontinuierliche, meist maschinell unterstützte und prozessintegrierte Überwachung von Prozessen mit IT-Unterstützung zur Aufdeckung von Fehlern oder Unplausibilitäten. Um die Unabhängigkeit der Internen Revision nicht zu gefährden, sollte diese kontinuierliche Überwachung nicht durch die Interne Revision durchgeführt werden.

g. IT-Assurance
Unter IT-Assurance wird eine Prüfungsform verstanden, die grundsätzlich frei gestaltbar ist (vgl. [Fröhlich et al. 2007b]). Aber auch solche Prüfungen folgen einem klaren Prüfungsprozess (Assurance-Prozess), haben einen definierten Kriterienkatalog, nach dem geprüft wird, und konzentrieren sich auf klar umrissene Prüfungsobjekte (Assurance-Objekte). Typische Beispiele sind Sonderprüfungen nach IDW PS 850 (projektbegleitende Prüfungen), ISAE 3402 und IDW PS 951 (Outsourcing-Prüfungen):

i. **Projektprüfungen (IDW PS 850)**
Bei Projektprüfungen unterscheidet man zwischen den projektbegleitenden Prüfungen (Pre-implementation Audit) und den nachgelagerten Prüfungen (Post-implementation Audit). Bei projektbegleitenden Prüfungen werden neben der Vorgehensweise selbst (Projektmanagement) auch alle Meilensteine und Ergebnisse einer Prüfung unterzogen, um möglichst frühzeitig Empfehlungen zur Verbesserung der Projektabwicklung und des in der Projektarbeit zu erstellenden Produkts geben zu können. Ziel einer nachgelagerten Prüfung ist – im Sinne einer kontinuierlichen Verbesserung und Erhöhung des Reifegrads der (Projekt-)Organisation –, Empfehlungen für die Planung und Durchführung künftiger Projekte zu geben oder beispielsweise zu prüfen, ob das im Rahmen des Projekts zu erstellende »Produkt« so erstellt wurde wie gefordert (etwa hinsichtlich Funktion, Leistung, Zeit, Budget).

ii. **Prüfung »Einführung neuer Systeme« (Sonderform von i.)**
Aufgrund hoher Dynamik im IT-Umfeld, verursacht durch neue Technologien, Verfahren und/oder Veränderungen/Weiterentwicklung der zugrunde liegenden Technik, bedarf es einer permanenten Anpassung der IT an unternehmensinterne und -externe, meist gesetzliche oder regulatorische Anforderungen. Größere Änderungen werden in der Regel im Rahmen von IT-Projekten durchgeführt. Um die Unternehmensleitung bei ihrer Überwachungsaufgabe zu unterstützen, prüft die Interne Revision alle wesentlichen Projekte insbesondere bezüglich des Projektmanagements und – in Abhängigkeit von der Höhe der Risiken in dem zu entwickelnden System – bezüglich fachlicher Aspekte (sog. Systemrisiken).

iii. **Outsourcing-Prüfungen (Kontrolle der IT-Serviceprovider)**
Häufig wird die gesamte IT oder ein Teil davon aufgrund von meist wirtschaftlichen Überlegungen an spezialisierte IT-Serviceprovider ausgelagert. Dabei ist es für das auslagernde Unternehmen bzw. seine Prüfer wichtig, zu wissen, ob das IKS des IT-Serviceproviders die spezifischen Anforderungen des Auftraggebers erfüllt. Um dies festzustellen, kann entweder das IKS unmittelbar beim IT-Serviceprovider geprüft werden oder der IT-Serviceprovider kann die Anforderungserfüllung anhand eines detaillierten Prüfungsberichts nach IDW PS 951 (als nationale Konkretisierung des ISAE3402/SSAE16) nachweisen. Für die Prüfung hat der IT-Serviceprovider eine detaillierte Beschreibung des IKS zu erstellen (Prozessaktivitäten, berücksichtigte Kriterien, Kontrollziele und implementierte Maßnahmen). Der Prüfer muss auf dieser Basis die Angemessenheit und die Wirksamkeit der implementierten Maßnahmen beurteilen (vgl. [Fröhlich/Swart 2013, S. 10]).

iv. **Prüfungen des Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 270xx**
Prüfungen in diesem Themenfeld orientieren sich neben den üblichen Prüfungsgrundsätzen eng an den Normen und den Regelungen der entsprechenden Zertifizierungsprozesse.

h. Softwareprüfung (inklusive Software Asset Management)
Auf dem in der Regel überaus großen Markt für Standardsoftware besteht die Herausforderung meist darin, anhand von verschiedenen Kriterien (technisch, preislich, funktional) die »passende« Software auszuwählen. Wenn die ausgewählte Software für die Ordnungsmäßigkeit der Rechnungslegung und andere unternehmenskritische Bereiche bedeutend ist, können **Softwarebescheinigungen** für den Auswahlprozess sehr hilfreich sein. Für die Erstellung einer solchen Bescheinigung wird eine Softwareprüfung (IDW PS 880) im Auftrag des Softwareherstellers durch einen Wirtschaftsprüfer durchgeführt. In diesem Rahmen ist festzustellen, ob die vom Softwarehersteller verwendeten Entwicklungs-, Test- und Freigabeverfahren angemessen sind. Darüber hinaus wird anhand von Tests überprüft, ob die Software über entsprechende Verarbeitungsfunktionen (etwa die Erfüllung der Ordnungsmäßigkeitsanforderungen gemäß HGB und AO im Bereich des Rechnungswesens) und über Verfahren für Zugriffsschutz und - steuerung sowie Datensicherung verfügt.

2.2.7 Prüfungsprogramm (Arbeitsprogramm)

Im Prüfungsprogramm werden anhand von externen Prüfungskriterien (insbesondere abgeleitet aus Gesetzen, aber auch aus Best-Practice-Rahmenwerken wie COBIT) und internen Prüfungsmaßstäben (z.B. Richtlinien und Verfahrensanweisungen) Prüfungsobjekte geprüft.

Ziel des Prüfungsprogramms ist es zunächst, die Prüfer bei der Durchführung der Prüfung und bei der Dokumentation der Prüfungsergebnisse bestmöglich zu unterstützen. Das zweite Ziel ist, dem Prüfungsleiter die Abnahme der Leistungen der Mitglieder des Prüfungsteams zu ermöglichen, d.h., die tatsächlich durchgeführten Prüfungshandlungen und die Ergebnisse einschließlich der Bewertungen der vorgefundenen Situation gedanklich nachzuvollziehen. Das dritte Ziel ist, dem Prüfungsleiter zu ermöglichen, aus den Prüfungsergebnissen den Prüfungsbericht abzuleiten. Die wesentlichen **Inhalte eines Prüfungsprogramms** für ein Prüfungsobjekt sind:

- Identifizierte Risiken
- Prüfungskriterien
- Prüfungsfragen
- Vorgesehene Prüfungshandlungen, durch deren Ausführung der Prüfer die Informationen gewinnen kann, die er zur Beantwortung der Fragen benötigt.
- Erwarteten Maßnahmen

2.2.8 Prüfungsunterlagen

Typische **Prüfungsunterlagen**, die bei der Prüfung eines Prüfungsobjekts herangezogen werden, können beispielsweise sein:

- Prozess- und Systemdokumente
- Alle Arten von Nachweisen für den ordnungsmäßigen Ablauf von Prozessen
- Netzwerkdiagramme
- Zutrittslisten
- Zugangslisten (Systemberechtigungen)
- Notfallkonzept
- Angaben zu den Datensicherungen
- Sitzungsprotokolle
- Teilnehmerlisten
- Freigaben
- Verträge
- Konfigurationsdaten
- Prüfberichte
- Testergebnisse
- Ablauf-, Prüf- und Freigabenachweise aus Datenbanken oder in Papierform
- Lizenzen

2.2.9 Prüfungshandlungen

Typische **Prüfungshandlungen** sind:

- Analyse von Risiken
- Sichtung von Dokumenten
- Beobachtungen von Abläufen/Prozessen
- Erläuterung von Prozessen gegenüber dem Prüfenden im Rahmen von freien Interviews oder entlang einer Checkliste
- Untersuchung/Analyse von IT-Systemen, insbesondere die Durchsicht von Configuration-Management-Datenbanken (CMDB) sowie Inventarlisten
- Aufnahme von Beständen
- Begehungen von Gebäuden (Rechenzentren, Serverräume) und (Auslands-)Standorten
- Analyse von Daten/Informationen

3. Regelwerke und ihre Einordnung

Im Rahmen von Prüfungen bzw. der Prüfungsplanung sind einerseits Gesetze, regulatorische Vorgaben, nationale und internationale Normen und Standards von Bedeutung, deren Einhaltung bei der Prüfung der Prüfungsobjekte inhaltlich geprüft werden muss. Für die Mehrheit der Unternehmen sind dies etwa die ISO/IEC-27000-Normenreihe (Informationssicherheits-Managementsystem), ISO/IEC 20000 (IT-Servicemanagement) und die damit kompatible Information Technology Infrastructure Library (ITIL), ISO 31000 (Risikomanagement), das deutsche Telekommunikationsgesetz (TKG), das Bundesdatenschutzgesetz (BDSG), die Landesdatenschutzgesetze sowie bauliche Vorschriften (etwa für Rechenzentren und vergleichbare Gebäude/Räume mit IT-Nutzung).

Zu den vielfältigen, teilweise sehr speziellen branchenspezifischen Vorgaben zählen etwa Gesetze und Normen für die IT im Gesundheitswesen oder der Payment Card Industry Data Security Standard (PCI DSS) für Unternehmen, die am kreditkartenbasierten Zahlungsverkehr teilnehmen. Für Finanzdienstleistungsunternehmen besonders relevant sind das Kreditwesengesetz (KWG), BASEL III bzw. Solvency II sowie die Mindestanforderungen an das Risikomanagement (MaRisk) und – international – der Sarbanes-Oxley Act (SOX).

Andererseits sind Standards zu beachten, die für die Prüfungsprozesse und damit für die Durchführung von Prüfungen selbst relevant sind. Hierzu zählen neben den ISACA-Standards (vgl. [ISACA 2013a, S. 31]) ITAF und COBIT insbesondere die IDW-, DIIR- und IPPF- sowie ISAE-Standards. Sie beeinflussen den Prüfungsumfang und die Prüfungsziele.

Die nachfolgende Abbildung 3–1 ordnet die wichtigsten Gesetze, Regelungen, Normen und Standards zu.

3.1 Das Information Technology Assurance Framework (ITAF)

Dieses Framework integriert als eine Art Informationsplattform für IT-Prüfung und -Assurance alle relevanten Veröffentlichungen der ISACA, des ITGI und weiterer anerkannter Organisationen zum Thema IT-Prüfung[1].

Das englische Original ist unter *www.isaca.org/itaf* verfügbar.

1 Einen sehr guten Überblick über ITAF bietet [Auf der Heyde/Hahn 2014].

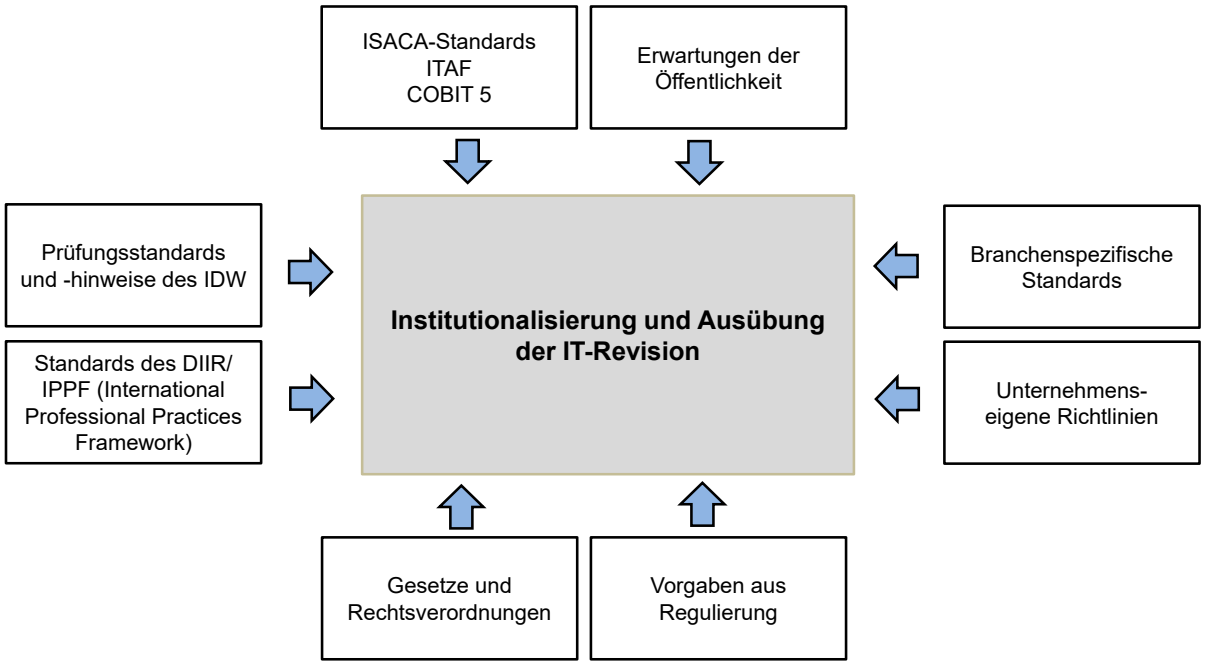

Abbildung 3–1: Institutioneller Rahmen für die IT-Revision (modifiziert nach [Amling/Bantleon 2015])

ITAF umfasst drei Kategorien von Standards (general, performance, reporting) sowie Guidelines, Werkzeuge und Techniken (vgl. Abschnitt 3.1.2 sowie [ISACA 2013a, S. 39]).

3.1.1 Ethikkodex

Der ISACA Code of Ethics verpflichtet Mitglieder sowie Inhaber eines ISACA-Zertifikats (CISA, CISM, CRISC, CGEIT) zur Einhaltung von ethischen Grundsätzen bei der Ausübung ihrer Tätigkeit. Dies beinhaltet die Befolgung der ISACA-Standards, gesetzestreues, rechtschaffenes und kompetentes Handeln und schließt eine Geheimhaltungspflicht ein (vgl. [Cascarino 2012, S. 50]).

Ein angemessener Ethikkodex umfasst auch die Betrachtung des Spannungsfelds zwischen IT-Revision und Beratung sowie die Revisionskultur im Unternehmen.

Spannungsfeld zwischen Prüfung und Beratung

Da sich die IT-Revision an verbindlichen Standards und Quasistandards und insbesondere »Best-Practice«-Ansätzen orientiert, gilt sie prinzipiell als wertvolle Quelle für den Einsatz und die Optimierung von Methoden und Prozessen in der IT-Organisation (vgl. auch Abschnitt 1.2). Ihr Grundgeschäft ist zunächst die Istanalyse. Strategie- und Prozessberatung hin zu einem Sollzustand, Ideen, Anregungen und Impulse liefern dann wichtige Hinweise für die Fachbereiche auf dem Weg zur erfolgreichen Umsetzung. Dies gilt insbesondere auch für projektbegleitende und damit meist weniger formale Prüfungen.

Allerdings muss gleichzeitig auf die Unabhängigkeit der Revisionsfunktion geachtet werden. Zwar darf die »zulässige« Bandbreite (unterstützende Beratung im Sinne der Methodik, Grundsatzfragen usw.) ausgeschöpft werden, eine konkrete Unterstützung bei Implementierungen oder bei der Wahl eines Anbieters im Rahmen des Bezugs externer Leistungen muss aber vermieden werden. Denn nur dann kann die Revision später objektiv und unabhängig prüfen, ob die Fachbereiche alle notwendigen Schritte durchgeführt und Hinweise beachtet haben.

Revisionskultur im Unternehmen

Es gilt als Kulturfrage, wie gut die Awareness für die Bedeutung und Notwendigkeit der Revisionsfunktion und den Umgang mit ihr ausgeprägt ist. Im Idealfall ist das Verhältnis zwischen der (IT-)Revision und den Fachbereichen konstruktiv und im gegenseitigen Umgang offen. So sollten die Fachbereiche die IT-Revision bei Prüfungen uneingeschränkt unterstützen und ihr alle erforderlichen Informationen bereitstellen sowie den Zugang zu notwendigen Informationen ermöglichen. Zudem sollten die Fachbereiche auch ohne ausdrücklichen Hinweis auf ihre Informationspflichten gegenüber der IT-Revision über relevante Änderungen bzw. aufgedeckte Fehler oder Mängel unverzüglich informieren (vgl. [Schmidt/Brand 2011, S. 11-12]).

Umgekehrt können Prüfungsfeststellungen einen Fachbereich positiv beeinflussen, beispielsweise wenn ein Fachbereich versucht, Änderungen umzusetzen, die Rahmenbedingungen dies vermeintlich aber nicht zulassen. In diesem Zusammenhang kann es hilfreich sein, nicht nur negative, sondern auch positive Prüfungsergebnisse in den Prüfbericht mit aufzunehmen.

Die Anzahl Mitarbeiter, der Umsatz, das Geschäftsmodell und der Stellenwert der IT, aber auch alle positiven Synergieeffekte zur betriebswirtschaftlichen Revision sind dann weitere wichtige Kennzahlen im Rahmen der Entscheidung, ob und in welchem Umfang eine eigene IT-Revision eingerichtet und wie die Zusammenarbeit mit den Fachbereichen organisiert werden soll.

3.1.2 ISACA-Standards

Zu den im Rahmen von ITAF wichtigen Elementen gehören alle **ISACA-Standards, ISACA-Guidelines (Richtlinien/Leitfäden) und ISACA-Procedures (Maßnahmen)**. Sie sind die zentrale Orientierungshilfe für IT-Prüfungen. Standards definieren verbindlich einzuhaltende Anforderungen an IT-Prüfung und Berichterstattung. Guidelines unterstützen bei der Implementierung der Standards. Procedures enthalten weitere Informationen mit Empfehlungscharakter zu konkreten Maßnahmen, die die Befolgung der Standards sicherstellen sollen.

Alle ISACA-Standards (gültig seit 01.11.2013) sind in englischer und deutscher Sprache verfügbar. Die deutsche Übersetzung kann unter *http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/Standards-for-IS-Audit-and-Assurance-German.aspx* abgerufen werden.

Allgemeine Standards (General Standards)

Die allgemeinen Standards umfassen:

- IT-Prüfungsstandard 1001 – Audit Charter
- IT-Prüfungsstandard 1002 – Organisatorische Unabhängigkeit
- IT-Prüfungsstandard 1003 – Persönliche Unabhängigkeit
- IT-Prüfungsstandard 1004 – Hinreichende Durchführbarkeit
- IT-Prüfungsstandard 1005 – Berufsübliche Sorgfalt
- IT-Prüfungsstandard 1006 – Expertise
- IT-Prüfungsstandard 1007 – Aussagen
- IT-Prüfungsstandard 1008 – Kriterien

Ausführungsstandards (Performance Standards)

Die Ausführungsstandards umfassen:

- IT-Prüfungsstandard 1201 – Auftragsplanung
- IT-Prüfungsstandard 1202 – Risikoorientierte Planung
- IT-Prüfungsstandard 1203 – Durchführung und Überwachung
- IT-Prüfungsstandard 1204 – Wesentlichkeit
- IT-Prüfungsstandard 1205 – Nachweise
- IT-Prüfungsstandard 1206 – Verwendung der Ergebnisse anderer Sachverständiger
- IT-Prüfungsstandard 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen

Berichtsstandards (Reporting Standards)

Die Berichtsstandards umfassen:

- IT-Prüfungsstandard 1401 – Berichterstattung
- IT-Prüfungsstandard 1402 – Nachschau

3.1.3 Richtlinien (Guidelines)

Die Richtlinien sind analog in allgemeine Richtlinien, Ausführungsrichtlinien und Berichtsrichtlinien unterteilt. Ihre Aufteilung und ihre Titel folgen derselben Logik und Namensgebung wie die der Standards.

3.1.4 Instrumente und Methoden (Tools and Techniques)

COBIT 5

Definition »Governance«

ISACA definiert den Begriff Governance als einen unternehmensinternen Anspruch, der »ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives«.

Governance beschreibt also alle Aktivitäten, die sicherstellen, dass die Bedürfnisse aller Anspruchsgruppen einschließlich aller Rahmenbedingungen mit dem Ziel gegeneinander abgewogen werden, die im Sinne eines gemeinsamen Interesses formulierten Unternehmensziele zu erreichen. Dabei nutzt gute Governance die Instrumente der Priorisierung ebenso wie klare Entscheidungen, um eine strategische Richtung vorzugeben. Gleichzeitig überwacht sie den Prozess der Zielerreichung und die Zielerfüllung.

Als zentrales Instrument im ITAF soll COBIT bzw. die COBIT-Produktfamilie eine ganzheitliche Governance und ein ganzheitliches Management der IT für das gesamte Unternehmen ermöglichen. Dabei werden alle funktionalen Zuständigkeitsbereiche von Unternehmen und IT lückenlos integriert und die IT-bezogenen Interessen interner und externer Anspruchsgruppen berücksichtigt. So werden Unternehmen dabei unterstützt, den Wertbeitrag der IT zu optimieren, indem sie für ein ausgeglichenes Verhältnis zwischen Nutzen, Risiken und Ressourceneinsatz sorgen (vgl. [ISACA 2012]).

Der Einsatz des COBIT-Rahmenwerks kann die Erfüllung der ISACA-Standards weitgehend unterstützen (vgl. [Cascarino 2012, S. 49]). Die ISACA-Fachgruppe »IT-Risikomanagement« beispielsweise hat 2013 einen Leitfaden zur Durchführung eines IT-Risikomanagements mithilfe von COBIT erstellt[2].

Neue Erkenntnisse aus Forschung und Praxis

Zu den weiteren Instrumenten und Methoden zählt ITAF alle verfügbaren Erkenntnisse aus Forschung und Praxis, wie sie unter *www.isaca.org/research* laufend um neue Erkenntnisse aktualisiert abrufbar sind.

3.2 COSO Internal Control Standards

Ziel des COSO Internal Control – Integrated Framework (COSO ICIF 2013)[3] ist es, jedem Unternehmen das Erreichen der folgenden Ziele zu ermöglichen:

- Wirtschaftlichkeit und Effizienz des Geschäftsbetriebs, Erreichung von Leistungszielen, Schutz von Vermögenswerten
- Zuverlässigkeit von (insbesondere rechnungslegungsrelevanten) Daten und der Berichterstattung
- Konformität mit Gesetzen und regulatorischen Vorgaben

Das Erreichen der Ziele wird durch folgende Komponenten unterstützt (vgl. [Cascarino 2012, S. 51-52]):

- Intakte Umgebung für Maßnahmen zur Risikobehandlung
- Intakter Risikobeurteilungsprozess
- Intakte operationelle Maßnahmen zur Risikobehandlung
- Intakte Informations- und Kommunikationssysteme
- Effektive Überwachung

Entsprechend werden diese Aspekte im Rahmen von IT-Prüfungen betrachtet. Das Interne Kontrollsystem kann als angemessen und wirksam bezeichnet werden, wenn alle fünf Komponenten in Bezug auf den Geschäftsbetrieb, die Finanzberichterstattung sowie die Compliance vorhanden sind (vgl. [Cascarino 2012, S. 173]).

3.3 IIA-Standards

Die vom Institute of Internal Auditors (IIA) veröffentlichten »International Standards for the Professional Practice of Internal Auditing« (Berufsstandards der Internen Revision)[4] dienen der Sicherstellung der Qualität der Internen Revision. Zusätzlich zu den verbindlichen Standards ist auch der Ethikkodex (»Code of Ethics«) zwingend zu befolgen. »Practice Advisories« stellen Ansätze zur bestmöglichen Implementierung der Standards dar. Außerdem werden »Development and Practice Aids« sowie ein »Guide to the Assessment of IT Risk (GAIT)[5]« zur Unterstützung der Entwicklung von Mitarbeitern in der Internen Revision zur Verfügung gestellt (vgl. [Cascarino 2012, S. 47-48]).

2 »IT-Risikomanagement – leicht gemacht mit COBIT«, abrufbar unter *https://isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/2012-isaca-leitfaden-it-risikomanagement_0.pdf.*

3 Vgl. *www.coso.org.*

4 Vgl. *https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20English.pdf.*

5 *www.theiia.org/guidance/technology/gait*

3.4 ISO/IEC-270xx-Familie

Der Standard ISO/IEC 27001:2013 »Information technology – Security techniques – Information security management systems – Requirements« ist ein für Unternehmen wichtiger Standard, um ein Informationssicherheits-Managementsystem zu planen, zu betreiben und kontinuierlich zu verbessern. Der Standard ISO/IEC 27002:2013 »Information technology – Security techniques – Code of practice for information security management« ist für die Umsetzung der dazugehörigen Maßnahmen von Bedeutung. Der Standard beschreibt Umsetzungsmaßnahmen für unterschiedliche Bereiche und auf unterschiedlichen Ebenen im Unternehmen, wie z.B. Management, Personal, physische Sicherheit, IT, Compliance (vgl. [Johannsen/Goeken 2011, S. 237-239]). So gibt ISO/IEC 27001 vor, was für ein gemäß Standard funktionierendes Informationssicherheits-Managementsystem (ISMS) implementiert sein muss. ISO/IEC 27002:2013 beschreibt, wie in einem Unternehmen Informationssicherheitsmaßnahmen implementiert werden können. Dabei wird unter Informationssicherheitsmanagement ein Maßnahmenbündel verstanden, das insbesondere unternehmensinterne Standards, Vorgaben und Regelungen sowie Managementprozesse umfasst (vgl. [Fröhlich et al. 2007a, S. 64]). Der Standard ISO/IEC 27005:2011 »Information technology – Security techniques – Information security risk management« schließlich befasst sich mit dem für die risikoorientierte Prüfung wichtigen Risikomanagement. Der Standard enthält eine Anleitung zur Analyse und zum Management von Informationssicherheitsrisiken und unterstützt die Erfüllung von Anforderungen des ISO/IEC-Standards 27001 zum Informationssicherheits-Managementsystem (vgl. [Fröhlich et al. 2007a, S. 39]).

Die ISACA-Fachgruppe Informationssicherheit hat im Jahr 2011 einen Leitfaden veröffentlicht, der die Anforderungen aus ISO/IEC 27001:2005 denen aus dem IDW PS 330 gegenüberstellt[6]. Zudem hat sie in diesem Jahr einen Leitfaden zur Implementierung eines ISMS nach ISO/IEC 27001:2013 veröffentlicht[7].

3.5 BSI-Standards

Das Ziel des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist es, Informationssicherheit in öffentlichen Einrichtungen, aber auch in Unternehmen, insbesondere kleinen und mittelgroßen Unternehmen (KMU), sowie in Privathaushalten zu etablieren. Um den wachsenden Anforderungen an die Sicherheit in der IT Rechnung zu tragen, wurde 1992 das Konzept des IT-Grundschutzes entwickelt und seither kontinuierlich angepasst und weiterentwickelt. Seit 2008 sind alle Empfehlungen des BSI zum Aufbau eines angemessenen Informationssicherheits-Managementsystems (ISMS) aus den vorher existierenden Dokumenten in einheitlicher Form in den BSI-Grundschutz-Standards und -Katalogen zusammengefasst. Die Grundschutz-Standards geben die Vorgehensweise vor, die Grundschutz-Kataloge beschreiben Gefährdungen (als Folge von Bedrohungen und Schwachstellen – Begriffe, die das BSI abweichend von internationalen Darstellungen so nicht direkt verwendet) und die Maßnahmen zur Behandlung der aus den Gefährdungen resultierenden Risiken.

Die IT-Grundschutz-Standards umfassen:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement

Die IT-Grundschutz-Kataloge setzen sich aus mehreren informativen Teilen sowie drei Katalogen (Baustein-, Maßnahmen-, Gefährdungskatalog) zusammen.

Die Bausteine sind sogenannten Schichten zugeordnet. Die Schichten befassen sich jeweils mit einem konkreten Bereich (übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze, Anwendungen). Die Bausteine wiederum beschäftigen sich mit einer speziellen Thematik aus dem Bereich (wie z.B. Organisation, Personal, Outsourcing, Rechenzentrum, elektrotechnische Verkabelung, Server, Laptop, Speichersysteme und -netze, TK-Anlage, Firewall, VoIP, Datenbanken, DNS, mobile Datenträger u.a.m.).

Über das Schichtenmodell und die Modellierung – die Zuordnung der Bausteine zu einer Schicht – ist ein guter Überblick und ein pragmatischer Einstieg möglich, um mit dem umfangreichen Kompendium arbeiten zu können.

In jedem Baustein sind jeweils die Gefährdungen und Maßnahmen aufgelistet, die für diesen Baustein relevant sind, also die Gefährdungen, die in dem betrachteten Bereich (Baustein) typisch bzw. möglich sind, und die Maßnahmen, die umgesetzt werden sollten.

Auch der Gefährdungs- und der Maßnahmenkatalog sind strukturiert. Der Gefährdungskatalog ist aufgeteilt in die Abschnitte G0 Elementare Gefährdungen, G1 Höhere Gewalt, G2 Organisatorische Mängel, G3 Menschliche Fehlhandlungen, G4 Technisches Versagen und G5 Vorsätzliche Handlungen. Der Maßnahmenkatalog gliedert sich in M1 Infrastruktur, M2 Organisation, M3 Personal, M4 Hardware und Software, M5 Kommunikation und M6 Notfallvorsorge.

Die IT-Grundschutz-Kataloge sowie die IT-Grundschutz-Vorgehensweise werden vom BSI zurzeit überarbeitet. Wesentliche Ursachen dafür sind neue Anforderungen und der Bedarf nach Optimierung sowie der Bedarf der Anwender an ein aktuelles, praxisnahes und attraktives Vorgehen.

6 »ISACA-Leitfaden und Nachschlagewerk IDW PS 330 – DIN ISO/IEC 27001 Referenztabelle«, abrufbar unter *https://isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_sicherheit_0.pdf*.

7 *https://isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_i_gesamt_web.pdf*

Die BSI-Standards und die IT-Grundschutz-Kataloge sowie aktuelle Informationen und vielfältige, teils umfangreiche Vorlagen und Hilfsmittel stehen auf den Webseiten des BSI kostenlos zum Download zur Verfügung[8].

3.6 ITIL

ITIL (Information Technology Infrastructure Library) ist ein sehr häufig angewandtes Rahmenwerk und kann als De-facto-Standard für das IT-Servicemanagement gelten. Es hat sich als gute Hilfestellung für die Organisation und die Definition von IT-Dienstleistungen (IT-Services) etabliert und findet inzwischen Anwendung in fast allen großen Unternehmen bzw. Bereichen, die IT-Leistungen erbringen (vgl. [Rüter et al. 2010, S. 24]). Einige Unternehmen haben auch ihre IT-Governance-Praktiken daran ausgerichtet. ITIL ist kompatibel zu ISO/IEC 20000.

3.7 ISO/IEC-20000-Familie

Seit 2011 ist ISO/IEC 20000-1 als eigenständig zertifizierbares Servicemanagementsystem etabliert, mit einem begleitenden »Code of Practice« ISO/IEC 20000-2.

Die offiziellen Bezeichnungen der beiden Standards sind:

- ISO/IEC 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements
- ISO/IEC 20000-2:2012: Information technology – Service management – Part 2: Guidance on the application of service management systems

3.8 ISO 22301:2012 Societal security – Business continuity management systems

Als DIN EN ISO 22301:2014-12 (Sicherheit und Schutz des Gemeinwesens – Business Continuity Management System – Anforderungen) ist diese Norm der Nachfolger des vom British Standards Institute herausgegebenen Standards BS-25999 und spezifiziert Anforderungen an ein wirksames Geschäftskontinuitäts-Managementsystem. Die Norm beinhaltet zertifizierbare Mindestanforderungen an die Erstellung sowie den Test von u.a.:

- Geschäftskontinuitäts-Strategie
- Geschäftskontinuitäts-Planung (Business Continuity Plan, BCP)
- Geschäftskontinuitäts-Notfall-/Ausfallszenarien (Disaster Recovery Plan, DRP)

3.9 ISO/IEC 38500:2015

ISO/IEC 38500:2015: Informationstechnik – Unternehmensführung in der Informationstechnik (Governance of IT for the organization) ist ein »High Level Standard«, der ein Fundament für eine weiter gehende Auseinandersetzung mit IT-Governance-Fragen bereitstellt. Er bietet zwar kein umfassendes IT-Governance-Referenzmodell, mit seiner Hilfe können Organisationen jedoch ein Referenzmodell definieren, das Führungskräften das Verständnis für die Bedeutung und die Umsetzungspflichten hinsichtlich rechtlicher, regulatorischer und ethischer Anforderungen veranschaulicht (vgl. [Johannsen/Goeken 2011, S. 190-195]). Das aus ISO/IEC 38500 stammende »Model for Corporate Governance of IT« bildet u.a. eine Grundlage für das COBIT-5-Framework.

8 *www.bsi.bund.de*

4. Der IT-Prüfer

4.1 Fachliche Eignung

Die Berufsbezeichnungen »IT-Prüfer« und »IT-Revisor« sind nicht geschützt. Entsprechende Qualifikationen werden auf Basis einschlägiger Informatik- oder Wirtschaftsinformatik-Ausbildungen und beruflicher Vorerfahrungen während der Ausübung der Tätigkeit erworben. Schulungen oder andere Formen der Weiterbildung zu speziellen IT-Themen sind mit Blick auf die zu fordernden technischen Kompetenzen zwingend notwendig, daneben aber auch sogenannte »Soft Skills« wie Kommunikations-, Interview- und Fragetechniken sowie Moderationstechniken. Viele IT-Revisoren spezialisieren sich wegen der stetig zunehmenden Komplexität der IT auf ein bestimmtes Gebiet oder bestimmte Anwendungen und arbeiten im Rahmen der IT-Prüfung eines komplexen IT-Systems, etwa in einem Konzern, deshalb stets im Team.

In Abhängigkeit von der Größe der Organisation und ihrer IT-Revision, der Komplexität der Geschäftsprozesse und je nach Umfang und Tiefe der Prüfung sollte der leitende Prüfer ein erfahrener Mitarbeiter mit Verantwortung für die wichtigsten Prüfmethoden und zentralen Prüfungsgebiete sein. In kleineren Organisationen übernimmt er zudem die Rolle eines mit der Abarbeitung der geplanten Arbeitspakete zuständigen Prüfers.

Die Prüfer im Prüfungsteam werden nach Qualifikations- und Erfahrungsstufen und der damit verbundenen Verantwortung unterschieden. Berufseinsteiger werden zunächst meist als »Junior IT Auditor« bezeichnet und eingesetzt, erfahrene IT-Revisoren erhalten dann etwa den Status »Senior IT Auditor«.

Der IT-Revisor ist grundsätzlich zur Verschwiegenheit gegenüber Dritten verpflichtet.

Obwohl die Frage der Unabhängigkeit nur in externen IT-Prüfungen in besonderer Weise geregelt ist und Verstöße nur dort offiziell sanktioniert werden, muss es der Anspruch aller IT-Revisoren sein, das Prüfungsobjekt so neutral wie möglich zu beurteilen. Der IT-Revisor arbeitet daher stets neutral und unabhängig und berichtet ausschließlich an den Auftraggeber. Auftraggeber externer IT-Revisoren ist in aller Regel die Unternehmensleitung oder deren Kontrollgremium. Weitere Anspruchsgruppen können Behörden, etwa die Staatsanwaltschaft, sein, wenn bei vermuteten Straftaten IT Forensic Audits durchgeführt werden. In diesem Kontext gelten dann besondere Regelungen. Auch das Management der geprüften Bereiche zählt zu den Anspruchsgruppen, da das Management für die Beseitigung der Mängel verantwortlich ist und deshalb die Prüfungsergebnisse mit ihm diskutiert werden müssen (vgl. Abschnitt 7.4).

Hinweis auf IT-Prüfungsstandard (ITAF)

Anforderungen an die Eignung von IT-Revisoren sind in den folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) definiert:

- 1002 – Organisatorische Unabhängigkeit
- 1003 – Persönliche Unabhängigkeit
- 1004 – Hinreichende Durchführbarkeit
- 1005 – Berufsübliche Sorgfalt
- 1006 – Expertise

Senior IT-Auditor in einer Wirtschaftsprüfungsgesellschaft

Was wir von Ihnen erwarten:
Als erfahrener IT-Revisor leiten Sie IT-Prüfungen in unterschiedlichen Branchen mit unterschiedlichsten Aufgabenstellungen. Sie setzen sich mit allen Themengebieten, insbesondere allen aktuellen Fragestellungen der IT-Revision, auseinander. Damit stellen Sie ein exzellentes Prüfungs- und Beratungsniveau sicher. Zu Ihren Prüfungsgebieten zählen die IT-Sicherheit, Prozesse im IT-Betrieb sowie Geschäftsprozesse mit unternehmenskritischer IT-Unterstützung, komplexe Datenanalysen, Fragen der IT-Governance und -Compliance, das IKS, IT-Risikomanagement sowie ERP-Systeme und andere zentrale Unternehmensanwendungen.

Was Sie mitbringen:
Sie verfügen über ein wirtschaftswissenschaftliches Studium oder Studium der (Wirtschafts-)Informatik oder eine vergleichbare Ausbildung mit entsprechender, mindestens fünfjähriger praktischer Erfahrung auf den Gebieten IT-Revision, IT-Sicherheit und IT-Consulting. Ihre praktischen und methodischen IT-Kenntnisse sind sehr gut. Sie zeichnen sich durch Teamgeist, Eigeninitiative, zuverlässige Arbeitsweise und großes persönliches Engagement für die von Ihnen betreuten Themen und Projekte aus. Sie besitzen ausgeprägtes analytisches Denkvermögen und können auch in schwierigen Situationen sicher kommunizieren. Aufgabentypische Zertifizierungen (z.B. CISA) sind von Vorteil, ebenso Erfahrungen mit einschlägigen ERP-Systemen. Gute englische Sprachkenntnisse setzen wir voraus.

Typische Stellenprofile umfassen die nachfolgenden Anforderungen:

IT-Revisor in einem internationalen Anwenderunternehmen

Was wir von Ihnen erwarten:
Als IT-Revisor führen Sie IT-Audits u.a. mit den Schwerpunkten Sicherheits- und Berechtigungsmanagement durch. Sie unterstützen alle Managementebenen im Konzern bei Prozessverbesserungen, auch im Rahmen von Beratungsprojekten. Zudem sind Sie für die Prüfung der Funktionsfähigkeit und Zuverlässigkeit der Internen Kontrollsysteme (in Anwendungen), die Erarbeitung risikoorientierter Prüfungsprogramme und Unterstützung bei der Prüfungsplanung verantwortlich. Sie evaluieren und präsentieren die Prüfungsergebnisse und erstellen die Prüfungsberichte. In diesem Rahmen übernehmen Sie federführend die Koordination mit den verschiedenen Fachbereichen. Sie beraten die Fachbereiche hinsichtlich revisionsspezifischer Fragestellungen, erarbeiten Verbesserungsvorschläge und begleiten und überwachen notwendige Optimierungsmaßnahmen. Zu Ihren Aufgaben gehören auch die Planung und Durchführung von Prüfungen, insbesondere Sonderprüfungen, im In- und Ausland sowie die Durchführung anspruchsvoller Compliance-Tests unter Anwendung der jeweils geltenden nationalen und internationalen gesetzlichen Vorgaben. Schließlich wirken Sie bei der Auswahl und Weiterentwicklung von Prüfungsmethoden und -strategien mit.

Was Sie mitbringen:
Sie verfügen über ein abgeschlossenes Hochschulstudium der (Wirtschafts-)Informatik oder Wirtschaftswissenschaften oder besitzen eine vergleichbare Qualifikation sowie mehrjährige IT-Audit-Erfahrung in der internationalen Industrie oder einer namhaften Prüfungsgesellschaft. Detaillierte Kenntnisse und Erfahrungen mit der Prüfung von Kontrollsystemen sowie hinsichtlich verschiedener Funktionsmodule in ERP-Systemen und in der ERP-Implementierung sind von Vorteil, ebenso Know-how im Bereich Sicherheit von Webapplikationen, mobiler Geräte, Malware und Cloud Computing. Mit BI-Software und SQL-Datenbanken können Sie sicher umgehen. Berufszertifikate (z.B. CISA, CISM, CISSP, CIA, CFE) oder nachweisbare Kenntnisse von Konzepten der IT-Governance (z.B. COBIT und ITIL) sind wünschenswert. Kenntnisse über gesetzliche Vorgaben und nationale und internationale Prüfungsstandards (IDW, COBIT, SOX) runden Ihr fachliches Profil ab. Sie verfügen zudem über eine ausgeprägte Kommunikationsstärke, eine verbindliche und belastbare Persönlichkeit mit Gespür für die Belange unterschiedlicher Unternehmensbereiche und -kulturen, präsentieren auch komplexe Sachverhalte anschaulich und verständlich, beherrschen die englische Sprache verhandlungssicher in Wort und Schrift und sind zu internationalen Dienstreisen bereit.

4.2 Das CISA-Examen

Um die eigene Qualifikation als IT-Prüfer nachweisen zu können, hat sich der Erwerb der CISA-Zertifizierung etabliert[1]. Ein solcher Certified Information Systems Auditor (CISA) muss dazu ein umfangreiches Examen erfolgreich absolvieren und bestimmte, mehrjährige Praxiserfahrungen vorweisen. Das Examen soll zeigen, dass die hinter der Zertifizierung stehenden methodischen und fachlichen Konzepte verstanden sind. Es ist daher inhaltlich breit angelegt und umfasst fünf Wissensgebiete, derzeit unterteilt in »Prüfung von Informationssystemen«, »IT-Governance und IT-Management«, »Anschaffung, Entwicklung und Implementierung von Informationssystemen«, »Betrieb, Pflege/Instandhaltung und Unterstützung von Informationssystemen« sowie »Schutz von Informationswerten«. Inhaber des CISA-Zertifikats sind verpflichtet, ethische und für IT-Prüfungen verbindliche Standards einzuhalten und sich in einem vorgegebenen Mindestmaß laufend weiterzubilden. Die Zertifizierung wird von der ISACA vergeben. Das CISA-Zertifizierungsprogramm ist von ANSI nach ISO/IEC 17024:2003 akkreditiert, was eine gewisse Vergleichbarkeit der Qualifikation einzelner IT-Prüfer untereinander erleichtert.

Weitere sinnvolle Zertifizierungen sind CISM, CRISC sowie ISO/IEC 27001 Lead Auditor. Auch für diese Zertifizierungen ist ein jeweils individuell festgelegtes Mindestmaß an Berufserfahrung (in der Regel 3 – 5 Jahre) notwendig.

1 *www.isaca.org/CISA*

5. Übersicht über die Revisionsprozesse

Aus übergeordneter, langfristiger Perspektive folgt der Revisionsprozess einem zyklischen Ablauf (vgl. Abbildung 5–1), der wiederum aus drei, jeweils linear verlaufenden Prozessen mit definiertem Anfang und Ende besteht:

- Prüfungsplanung (Kapitel 6)
- Durchführung konkreter Prüfungen (Kapitel 7)
- Nachverfolgung von Maßnahmen (Follow-up) (Kapitel 8)

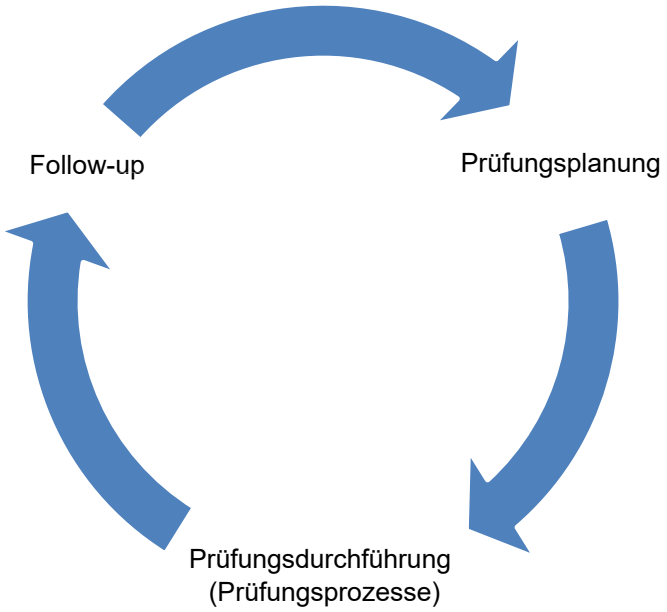

Abbildung 5–1: Revisionsprozesse

Die Prüfungsplanung gliedert sich in 4 Teilprozesse:

- Risikoanalyse (Abschnitt 6.1)
- Mehrjahresplanung (Abschnitt 6.2)
- Jahresplanung (Abschnitt 6.3)
- Unterjährige Planung/rollierende Planung (Abschnitte 6.4 und 6.5)

Die Durchführung einer konkreten Prüfung auf Basis der Prüfungsplanung lässt sich in 5 Teilprozesse unterteilen:

- Planung und Vorbereitung (Abschnitt 7.1)
- Voruntersuchung (Abschnitt 7.2)
- Prüfungsdurchführung (Field Work, Abschnitt 7.3)
- Abstimmung (Abschnitt 7.4)
- Berichterstattung und Dokumentation (Abschnitt 7.5)

Die prozessuale Darstellung des Follow-up kann sehr unterschiedlich gegliedert sein, weshalb keine einheitliche Teilprozessdarstellung wiedergegeben ist (vgl. Kapitel 8).

6. Die Prüfungsplanung

Abbildung 6–1: Prüfungsplanung

Die Revision erstellt üblicherweise im Herbst eines jeden Jahres den **Prüfungsplan** für das folgende Prüfungsjahr, der auch eine Vorausschau auf die kommenden Jahre enthält, und legt diesen der Unternehmensleitung zur Genehmigung vor (vgl. Abbildung 6–1). Gegebenenfalls kann die Unternehmensleitung Prüfungsaufträge ergänzen.

Hinweis auf IT-Prüfungsstandard (ITAF)

Anforderungen an die Prüfungsplanung sind im IT-Prüfungsstandard »1202 – Risikoorientierte Planung« der ISACA (vgl. Abschnitt 3.1.2) definiert.

Ausgangspunkt der Prüfungsplanung ist das aktualisierte Audit Universe (vgl. Abschnitt 2.2.3). Im Regelfall liegt das Audit Universe zu Beginn der Risikoanalyse bereits vor und muss ggf. lediglich (nochmals) auf Aktualität geprüft werden. Findet die Prüfungsplanung und damit auch die Risikoanalyse **erstmals** statt, wird das Audit Universe in diesem Rahmen neu erstellt.

Die nachfolgende Abbildung 6–2 zeigt beispielhaft ein Template für einen Prüfungsplan. Tabelle 6–1 zeigt die Input-Output-Beziehung im Rahmen der Prüfungsplanung sowie eine Übersicht der Aktivitäten und Werkzeuge in diesem Prozessschritt.

Mehrjahres-, Einjahres-, unterjährige Prüfungsplanung		
Input	**Einflussgrößen**	**Output**
Audit Charter	-	Mehrjahresprüfungsplan
Audit Universe (aktualisiert)		Einjahresplan
		Unterjahresplan
		rollierender Plan
Aktivitäten		**Werkzeuge/Dokumente**
Risikoanalyse		ursachenorientiert (qualitativ/quantitativ) für die Risikoanalyse
Mehrjahresplanung		wirkungsorientiert (qualitativ/quantitativ) für die Risikoanalyse
Einjahresplanung		Planungsmethoden/-werkzeuge
unterjährige Planung / rollierende Planung		Template Prüfungsplan
		Template Risikoregister/-katalog
		Office-Tools

Tabelle 6–1: Input-Output-Beziehung Prüfungsplanung

Audit-Nr.	Audit-Jahr	Audit-Typ	Audit-Standort	Audit-Land	interne Auditoren	externe Auditoren	Audit Scope	Audit-Beginn	Audit-Ende	Audit-Status

Legende

Audit-Typen:	IA	Internes Audit
	LA	Lieferantenaudit
	EA	Externes Audit
	ISO / MSA	ISO-Audit Measurement System Analysis
	Pen TA	Pen Test
	WLAN SA	WLAN Audit
	Phys Sec	Audit der physikalischen Sicherheit (Gebäude)
	Network Sec	Netzwerksicherheits-Audit
	BCM	Audit der Business Continuity

Auditstatus	- In Planung
	- durchgeführt
	- Maßnahmen vereinbart
	- Maßnahmen abgeschlossen
	- Maßnahmen zurückgezogen

Abbildung 6–2: Beispiel für einen Prüfungsplan

6.1 Risikoanalyse

Abbildung 6–3: Der Planungsprozess – Risikoanalyse

Der risikoorientierte Prüfungsansatz fordert, jedes Prüfungsobjekt im Audit Universe hinsichtlich seines Risikos individuell zu bewerten. Aufgrund dieser Risikobewertung wird festgelegt, in welchem Prüfungszyklus (wann, wie oft) das Prüfungsobjekt betrachtet werden muss.

Da in der Praxis begrenzte Zeitvorgaben und Prüferkapazitäten es häufig nicht zulassen, jedes Prüfungsobjekt einzeln einer Risikobewertung zu unterziehen, werden stattdessen die Risiken der übergeordneten (Teil-)Prüfungsfelder unter Wahrung der prüferischen Sorgfalt und Beachtung dieser Einschränkungen bewertet.

Liegen der Revision noch keine fundierten Informationen/Kenntnisse zu den (Teil-)Prüfungsfeldern vor, sodass die Bildung einer eigenen Risikoeinschätzung und damit die risikoorientierte Auswahl der Prüfungsobjekte schwierig bis unmöglich ist, empfiehlt es sich, zunächst eine Erhebungsprüfung (vgl. Abschnitt 2.2.6) zum (Teil-)Prüfungsfeld durchzuführen und deren Ergebnisse in die mehrjährige und jährliche Prüfungsplanung einfließen zu lassen.

> **Praxishinweis**
>
> Um ihre Unabhängigkeit zu wahren, muss die Revision die Risikobewertung selbst vornehmen und darf sich nicht allein auf die Risikobewertung anderer Stellen stützen.

Im Rahmen der Identifikation der Risiken eines Geschäftsprozesses lassen sich wegen der hohen IT-Durchdringung neben den Risiken, die sich originär aus dem Geschäftsprozess[1] ergeben, stets auch Risiken erfassen, die aus der IT-Nutzung resultieren[2]. Unterschieden werden dabei inhärente **IT-Risiken** und **IT-Fehlerrisiken**.

1 Zum Beispiel Adress-/Adressenausfallrisiken (einschließlich Länderrisiken), Marktpreisrisiken, Liquiditätsrisiken und Reputationsrisiken.
2 Oft auch als sogenannte operationelle Risiken bezeichnet.

Inhärente IT-Risiken existieren *trotz* bestehender Maßnahmen zur Risikobehandlung. Sie lassen sich erkennen etwa aus einer besonders großen Abhängigkeit von der IT oder bestimmtem IT-Fachwissen, treten bei allen Änderungen an bestehenden IT-Systemen oder der IT-Infrastruktur auf und ergeben sich nicht zuletzt auch durch die gewählte IT-Strategie und grundsätzliche Entscheidungen zu verwendeten Architekturen und Technologien. Inhärente Risiken der Nutzung von Informationstechnik können im Alltag jederzeit beispielsweise in Form von Störungen in den internen IT-Prozessen und deren Ressourcen sowie in Form von Störungen bei IT-Serviceprovidern, etwa als Ausfall von IT-Systemen (evtl. sogar eines ganzen Rechenzentrums), eintreten, sodass die Geschäftsbereiche ihre Geschäftsprozesse ggf. ohne oder nur mit einer eingeschränkten informationstechnischen Unterstützung abwickeln müssen, was in der Praxis zunehmend schwierig oder gar unmöglich ist. Aus diesem Grund ist auch das Kontinuitätsmanagement (Business Continuity Management) von elementarer Bedeutung.

IT-Fehlerrisiken entstehen durch Aufbau und innere Funktionsweise eines IT-Systems. So kann etwa ein Designfehler in einer Datenbank zu fehlerhaften Daten in der Anwendung führen.

Zur Bewertung der Risiken eines Prüfungsobjekts sind in Abhängigkeit der für das Unternehmen relevanten Risiken folgende Faktoren zu beachten (vgl. [Cascarino 2012, S. 80-81]):

- Datum und Ergebnisse der letzten Prüfung
- Finanzrisiken
- Reputationsrisiken
- Kritikalität
- Bedeutende Änderungen in Prozessen, Programmen, Systemen und Maßnahmen zur Risikobehandlung
- Kompetenz des Managements
- Komplexität der Transaktionen
- Liquidität
- Möglichkeiten zur Erzielung des operativen Gewinns
- Zeitkritische und/oder sachlich komplexe Managementanfragen
- Ethik und Moral der Mitarbeiter

Bei der Risikobewertung (vgl. Tabelle 6–2) der Prüfungsobjekte berücksichtigt die Revision neben den inhärenten Risiken, die originär mit dem Prüfungsobjekt verbunden sind, auch die sogenannten **Kontrollrisiken**, die die Wirksamkeit der Maßnahmen im IKS (Qualität des IKS) widerspiegeln und sich im Ergebnis der vorangegangenen Prüfung niederschlagen, sowie die seit der vorangegangenen Prüfung verstrichene Zeit, weil ein vor langer Zeit erzieltes zufriedenstellendes Ergebnis nicht zwingend auf aktuelle Verhältnisse schließen lässt.

Da die IT immer Dienstleister für fachliche Prozesse ist, leitet sich die Gewichtung identifizierter IT-Risiken immer aus der Kritikalität der fachlichen Prozesse ab (Business Impact). Die Prüfungsplanung der IT-Revision berücksichtigt daher auch die Auswirkungen der IT-Risiken auf die fachlichen Prozesse (z.B. durch Abdeckung konkreter Aspekte in »business critical processes«, sog. Pain Points).

Im Unterschied zu einer möglichen Risiko-Netto-Betrachtung von Risikocontrolling-Einheiten im Unternehmen sollte die Interne Revision immer von einer Risiko-Brutto-Betrachtung

Beispiel Risikobewertung

Prüffeld	Adressen-ausfallrisiko	Marktpreis-risiko	Liquiditäts-risiko	…	Reputations-risiko	Fehlerrisiko in IT-Prozessen	Fehlerrisiko von IT-Serviceprovidern	Gesamt-risiko
IT-Governance	entfällt	entfällt	entfällt	…	hoch	mittel	mittel	hoch
Informationssicherheit	mittel	mittel	mittel	…	mittel	hoch	mittel	hoch
…	…	…	…	…	…	…	…	…
IT-Betrieb	entfällt	entfällt	entfällt	…	mittel	hoch	mittel	hoch
IT-Entwicklung	entfällt	entfällt	entfällt	…	mittel	hoch	gering	hoch
Incident & Problem Management	entfällt	entfällt	entfällt	…	mittel	mittel	mittel	mittel
User Access & Privilige Management	entfällt	entfällt	entfällt	…	mittel	hoch	hoch	hoch
Licence Management	entfällt	entfällt	entfällt	…	gering	gering	gering	gering
IT-Systeme	mittel	gering	mittel	…	gering	mittel	mittel	mittel
…	…	…	…	…	…	…	…	…

Tabelle 6–2: Beispiel Risikobewertung

Abbildung 6–4: Der Planungsprozess – Mehrjahresplanung

ausgehen. Der Unterschied liegt in der Berücksichtigung (Netto) bzw. Nichtberücksichtigung (Brutto) von risikovermindernden (sog. »mitigierenden«) Steuerungs- und Kontrollmaßnahmen. Risikocontrolling-Einheiten berücksichtigen solche Maßnahmen in ihrer Risikoanalyse, da z.B. im Bankgewerbe abhängig von der Risikohöhe Eigenkapital vorgehalten werden muss und bei der Netto-Betrachtung das Risiko kleiner ist. Die Interne Revision hat aber die Aufgabe, die risikovermindernden Maßnahmen zu beurteilen. Daher sind stets die Brutto-Risiken bei der Prüfungsplanung (und im Prüfungsverlauf) zu betrachten.

Bei Anwendung des risikoorientierten Planungsansatzes wird stets auch berücksichtigt, dass die Ressourcen der IT-Revision knapp sind. Daher ist es grundsätzlich sinnvoll und wichtig, die zur Prüfung verfügbaren personellen, finanziellen und sachlichen Ressourcen mit entsprechender Priorität in Bereichen mit hoher Bedeutung (Kritikalität) einzusetzen. Dies sind insbesondere Bereiche, in denen IT-Risiken über die rechnungslegungsrelevanten Aspekte hinaus die größten Auswirkungen auf die Geschäftstätigkeit (Business Impact) haben.

Detaillierte Informationen zu möglichen IT-Risiken sind im COBIT-5-Framework der ISACA enthalten (vgl. Abschnitt 3.1.4).

Für die weitere Planung ist es zweckmäßig, die Bewertungen der einzelnen Risiken für ein Prüfungsobjekt bzw. (Teil-)Prüfungsfeld zu einem Risikowert zusammenzufassen.

Die gesamte Risikobewertung ist detailliert zu dokumentieren, um sie auch später jederzeit nachvollziehen zu können.

Ein Prüfungsplan auf Basis des risikoorientierten Prüfungsansatzes kann auch für ISO-9001-zertifizierte Unternehmen sinnvoll sein, da ab ISO 9001:2015 der risikoorientierte Ansatz (und damit ein funktionierender Risikomanagementprozess) eine Mindestanforderung für ein funktionierendes Qualitätsmanagementsystem (QMS) darstellt.

6.2 Mehrjahresplanung

Im Rahmen der Mehrjahresplanung (Schritt 2 in Abbildung 6–4) wird abhängig vom Ergebnis der Risikobewertung der Prüfungszyklus für Prüfungsobjekte bzw. (Teil-)Prüfungsfelder festgelegt. Prüfungsobjekte bzw. (Teil-)Prüfungsfelder mit hohen oder sehr hohen Risiken sollten mindestens jährlich geprüft werden. Für Prüfungsobjekte bzw. (Teil-)Prüfungsfelder mit geringen Risiken ist eine Prüfung in der Regel alle 3 bis 5 Jahre (je nach Ausgestaltung der Audit Charter, vgl. Abschnitt 2.2.1) ausreichend. Ziel sollte aber sein, alle Prüfungsobjekte bzw. (Teil-)Prüfungsfelder unabhängig vom Risikogehalt innerhalb des Planungszeitraums mindestens einmal prüferisch abzudecken (vgl. Beispiel in Tabelle 6–3).

Prüfungsobjekte bzw. (Teil-)Prüfungsfelder, die nicht jährlich geprüft werden müssen, sind unter Berücksichtigung der bereits durch Prüfungen erreichten Prüfungsabdeckung zeitlich einzuplanen.

Beispiel Mehrjahresplanung							
Prüffeld	Risiko	Prüfintervall	2015	2016	2017	2018	2019
IT-Governance	hoch	1 Jahr	X	X	X	X	X
Informationssicherheit	hoch	1 Jahr	X	X	X	X	X
…	…	…	…	…	…	…	…
IT-Betrieb	hoch	1 Jahr	X	X	X	X	X
IT-Entwicklung	hoch	1 Jahr	X	X	X	X	X
Incident & Problem Management	mittel	2 Jahre		X		X	
User Access & Privilige Management	hoch	1 Jahr	X	X	X	X	X
Licence Management	gering	3 Jahre	X			X	
IT-Systeme	mittel	2 Jahre	X		X		X
…	…	…	…	…	…	…	…

Tabelle 6–3: Beispiel Mehrjahresplanung

Abbildung 6–5: Der Planungsprozess – Jahresplanung

Beispiel Jahresplanung							
Planjahr:	2016						
Prüffeld	Prüfobjekte	geplanter Aufwand	1. Quartal	2. Quartal	3. Quartal	4. Quartal	Prüfer
IT-Entwicklung	Release Management Deployment Management	40 Personentage	X	X			Prüfer 1
IT-Betrieb	Service Level Management	20 Personentage			X		Prüfer 2
Informationssicherheit	Security Mannagement	20 Personentage				X	Prüfer 1
…	…	…	…	…	…	…	…

Tabelle 6–4: Beispiel Jahresplanung

6.3 Jahresplanung

Im Jahresprüfungsplan wird festgelegt, welche Prüfungsobjekte aus welchen (Teil-)Prüfungsfeldern im folgenden Prüfungsjahr geprüft werden. Ausgangspunkt der Jahresprüfungsplanung ist die Mehrjahresplanung sowie das aktualisierte Audit Universe und aktuelle Erkenntnisse. Berücksichtigung finden hier erneut auch die Kapazität und das vorhandene Know-how der Prüfer. Daher können sich bei der Jahresplanung immer wieder Abweichungen gegenüber den Mehrjahresprüfungsplänen bei den zu prüfenden (Teil-) Prüfungsfeldern ergeben (vgl. Beispiel in Tabelle 6–4).

Abbildung 6–6: Der Planungsprozess – Unterjährige Planung

Beispiel unterjährige Planung								
Planjahr:	2016							
Prüfung	Prüffeld	Prüfobjekte	geplanter Aufwand	Beginn Konzept-erstellung	Beginn Prüfungs-durchfüh-rung	Beginn Berichts-abstim-mung	Berichts-vorlage	Prüfer
03/2016	IT-Entwicklung	Release Management Deployment Management	40 Personentage	04.01.2016	18.01.2016	23.03.2016	25.04.2016	Prüfer 1
07/2016	IT-Betrieb	Service Level Management	20 Personentage	11.07.2016	25.07.2016	26.09.2016	28.10.2016	Prüfer 2
11/2016	Informations-sicherheit	Security Mannagement	20 Personentage	10.10.2016	24.10.2016	23.12.2016	30.01.2017	Prüfer 1
…	…	…	…	…	…	…	…	…

Tabelle 6–5: Beispiel unterjährige Planung

6.4 Unterjährige Planung

In der unterjährigen Planung werden die in der Jahresplanung festgelegten Prüfungsobjekte bzw. (Teil-)Prüfungsfelder bestimmten Prüfungen zugeordnet und eine konkrete zeitliche, kapazitative und an der jeweiligen Qualifikation orientierte Mitarbeitereinsatzplanung vorgenommen.

Im Rahmen der risikoorientierten Eingrenzung für geplante Prüfungen sind bestimmte Prüfungsobjekte zweckmäßig auszuwählen und ggf. weitere (Teil-)Prüfungsfelder thematisch zusammenzufassen. Dazu konzentriert sich der risikoorientierte Prüfungsansatz auf die Auswahl derjenigen Elemente mit den höchsten IT-Fehlerrisiken. Sie sind Prüfungsobjekte, die bevorzugt geprüft werden müssen.

Die unterjährige Planung erfolgt regelmäßig (z.B. monatlich oder quartalsweise) und berücksichtigt dabei auch aktuelle Erkenntnisse (z.B. IT-Sicherheitsvorfälle oder Ausfälle spezialisierter Administratoren, vgl. Tabelle 6-5).

6.5 Rollierende Planung

Bei der rollierenden Planung wird die Risikoanalyse und (Mehr-)Jahresplanung ständig im Rahmen der unterjährigen Planung durchgeführt, sodass erst einige Wochen vor Prüfungsbeginn feststeht, welches Prüfungsobjekt betrachtet wird.

7. Die konkrete Prüfung

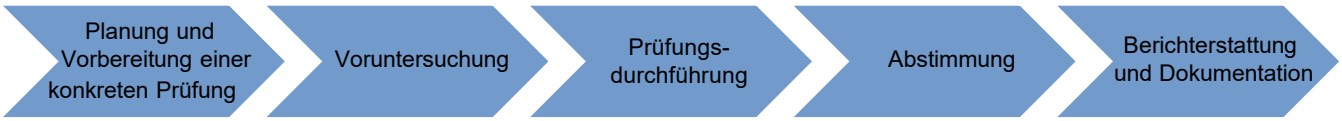

Abbildung 7–1: Prüfungsdurchführung

Eine konkrete Prüfung folgt einem sequenziellen Ablauf, der stets alle Schritte enthält. Einzelne Schritte können nicht ausgelassen, übersprungen oder vertauscht werden. Abbildung 7-1 zeigt als Orientierungshilfe die Schritte durch den Revisionsprozess von der Planung einer konkreten Prüfung über die Prüfungsvorbereitung und -durchführung bis hin zur Berichterstattung und Dokumentation.

In den nachfolgenden Abschnitten werden besonders wichtige Aspekte der einzelnen Teilprozesse (Schritte des Prüfungsprozesses) näher erläutert und in den Input-Output-Tabellen 7–1 bis 7–5 dargestellt.

7.1 Planung und Vorbereitung einer konkreten Prüfung

Der Umfang der Planung und Vorbereitung einer konkreten Prüfung hängt stark vom Umfang und vom Detaillierungsgrad der vorangegangenen Prüfungsplanung (vgl. Kapitel 6) ab.

Sind im Rahmen der Mehrjahres-, Einjahres- oder unterjährigen Planung bereits Prüfungsinhalte, das Prüfungsteam und der Zeitrahmen festgelegt worden (vgl. Kapitel 6), konzentriert sich die Planung und Vorbereitung einer konkreten Prüfung auf eine Präzisierung der Prüfungsaspekte und Prüfungsziele (vgl. Abschnitt 2.2.5) sowie auf die Festlegung der Prüfungsart je Prüfungsziel (vgl. Abschnitt 2.2.6).

Erfolgte die Prüfungsplanung bislang eher allgemein, müssen im Rahmen der Planung und Vorbereitung einer konkreten Prüfung auch die Prüfungsinhalte risikoorientiert und das Prüfungsteam sowie der Zeitrahmen genau festgelegt werden.

Die Dokumentation der Planung und Vorbereitung einer konkreten Prüfung erfolgt in der Prüfungskonzeption durch den Prüfungsauftrag. Ein weiteres Ergebnisdokument der Planung und Vorbereitung einer konkreten Prüfung ist die Prüfungsankündigung.

> **Hinweis auf IT-Prüfungsstandard (ITAF)**
>
> Anforderungen an die Planung und Vorbereitung einer konkreten Prüfung sind im IT-Prüfungsstandard »1201 – Auftragsplanung« und teilweise im IT-Prüfungsstandard »1202 – Risikoorientierte Planung« der ISACA (vgl. Abschnitt 3.1.2) definiert.

7.1.1 Prüfungskonzeption

Eine konkrete Prüfung kann sich auf unterschiedliche Geschäfts- und IT-Prozesse und die darin enthaltenen Aktivitäten und Ressourcen beziehen, beispielsweise auf produktive Anwendungen und deren Betriebsprozesse, auf Anwendungen, die sich in Entwicklung befinden, sowie deren Entwicklungsprozesse, auf Einrichtungen der IT-Infrastruktur, auf sicherheitsbezogene Maßnahmen oder auf die Effektivität und Effizienz der IT insgesamt.

Die Planungsphase einer konkreten Prüfung wird vielfach auch als Konzeptionsphase bezeichnet. In dieser Phase werden ausgehend von den Vorgaben aus der Prüfungsplanung die Prüfungsobjekte gemäß risikoorientiertem Prüfungsansatz konkretisiert.

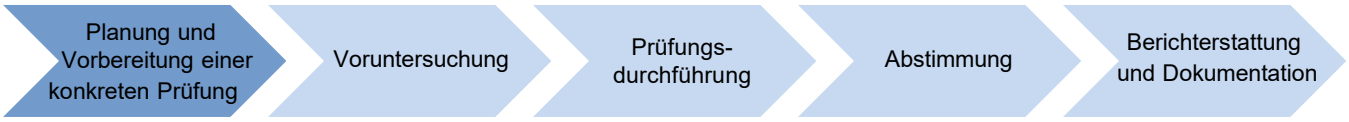

Abbildung 7–2: Prüfungsdurchführung – Planung und Vorbereitung einer konkreten Prüfung

Planung und Vorbereitung einer konkreten Prüfung		
Input	**Einflussgrößen**	**Output**
genehmigter Prüfungsplan (mehr-/einjährig/unterjährig/rollierend)	Umfang/Detailliertheit der Prüfungsplanung	Prüfungsauftrag (Prüfungskonzept)
	Qualifikation der Prüfer	Prüfungsankündigung
		konkrete Prüfungsobjekte
		Prüfungsfeld mit Prüfungsaspekten (daraus: Prüfungsart) und Prüfungszielen
		Prüfungsaufgaben
Aktivitäten		**Werkzeuge**
Prüfungskonzeption: ◗ risikoorientierte Konkretisierung der Prüfungsobjekte ◗ Präzisierung der Prüfungsaspekte, -ziele und -inhalte		Risikoanalysetools (vgl. Abschnitt 6.1) Planungswerkzeuge (vgl. Hinweise in Kapitel 6)
Zusammenstellung des Prüfungsteams		Office-Tools
Zeit- und Kapazitätsplanung (unter Beachtung der Kompetenzprofile der Prüfer) Personaleinsatzplanungs- und Projektmanagement-Tools		

Tabelle 7–1: Input-Output-Beziehung Planung und Vorbereitung einer konkreten Prüfung

Die hierfür notwendige Risikoanalyse kann z.B. folgende Unterlagen berücksichtigen:

- Ergebnisse aus vorherigen Prüfungen
- Ergebnisse der fachlichen Informationssicherheitsanalyse
- Ergebnisse aus Assessments zu operationellen Risiken (OpRisk)
- Ergebnisse aus Assessments zur Gefährdung durch (wirtschafts-)kriminelle Handlungen (Fraud-Risiken)
- Ergebnisse aus Assessments zur physischen Sicherheit (z.B. Naturkatastrophen, Einbruch, Überfall)
- Vereinbarungen zwischen IT und Fachbereich (Service Level Agreement)
- Regelungen zum Notfallbetrieb
- Berichte des IT-Security-Teams
- Berichte des Wirtschaftsprüfers und anderer externer Prüfer
- Berichte über aufgetretene OpRisk-Fälle
- Berichte über aufgedeckte kriminelle Handlungen
- Hinweise von Whistleblowern
- Hinweise aus anderen Prüfungen
- Hinweise aus dem Follow-up vorangegangener Prüfungen

Auf Basis der verfügbaren Informationen werden die Prüfungsobjekte aus der Gesamtheit der Themen zum festgelegten Prüfungsfeld eingegrenzt.

Praxisbeispiel

Der Prozess zur Beantragung und Anlage von Benutzerberechtigungen könnte in einem Unternehmen unter anderem folgende Risiken beinhalten:

- Benutzer erhalten zu weitgehende Berechtigungen
- Benutzer erhalten fehlerhafte Berechtigungen
- Benutzer erhalten unzureichende Berechtigungen

Um diese Risiken zu verringern, könnten unter anderem folgende Maßnahmen implementiert worden sein:

- Freigabe der beantragten Berechtigungen durch einen fachlich Verantwortlichen
- Konzeption und Dokumentation von notwendigen Berechtigungen für eine bestimmte Benutzerrolle

Würde in einem Unternehmen die Rolle »fachlich Verantwortliche« bei der Freigabe von Berechtigungen durch die Assistenz der Unternehmensleitung wahrgenommen, wäre zwar eine Maßnahme gegen zu weitgehende Berechtigungen implementiert, sie wäre aber sicherlich nicht angemessen. Denn die Assistenz der Unternehmensleitung wird nicht für jede Berechtigung fachlich beurteilen können, ob ein Benutzer dieses Recht tatsächlich benötigt. Würde sich die Prüfung aber nur auf Objekte mit hohen Risiken nach Berücksichtigung dieser Maßnahme beziehen (Netto-Betrachtung), könnte ggf. in der →

Prüfung nicht entdeckt werden, dass die Maßnahme »Freigabe der beantragten Berechtigungen durch fachlich Verantwortliche« das Risiko »Benutzer erhalten zu weitgehende Berechtigungen« nicht ausreichend verringert und somit nicht angemessen ist.

Für das Risiko »Benutzer erhalten fehlerhafte Berechtigungen« wurde im Unternehmen keine Maßnahme eingerichtet, da angenommen wird, dass sich die Benutzer melden, wenn etwas nicht funktioniert. Würde sich die Planung der konkreten Prüfung nur auf die eingerichteten Maßnahmen beschränken, würde in der Prüfung nicht entdeckt, dass die wesentliche Maßnahme »Test der Berechtigungen vor Vergabe an Benutzer« fehlt.

Die risikoverringernde Maßnahme »Konzeption und Dokumentation von notwendigen Berechtigungen für eine bestimmte Benutzerrolle« schließlich könnte Teil der Prüfungsobjekte »Konzeption und Entwicklung von IT-Systemen« und »Dokumentation von fachlichen Prozessen« sein, obwohl das Risiko »Benutzer erhalten unzureichende Berechtigungen« dem Prüfungsobjekt »Beantragung und Anlage von Benutzerberechtigungen« zugeordnet ist. Die Maßnahme müsste also präzisiert und richtig zugeordnet werden.

Die Risikoanalyse der potenziell zu prüfenden Objekte sollte dabei ohne Beachtung der ggf. implementierten Maßnahmen erfolgen (sog. Brutto-Betrachtung, vgl. hierzu Abschnitt 6.1).

Anschließend werden zu jedem Prüfungsobjekt die Prüfungsaspekte und Prüfungsziele bestimmt. Hierbei wird ggf. erneut eine Eingrenzung auf bestimmte oder zufällige Sachverhalte (Stichprobe) zum jeweiligen Prüfungsobjekt vorgenommen, um so die tatsächlich zu beurteilenden Sachverhalte festzulegen.

Aus den Prüfungsaspekten und Prüfungszielen leitet sich dann für jedes Prüfungsobjekt jeweils die Prüfungsart ab. Somit können in einer konkreten Prüfung mehrere Prüfungsarten genutzt werden.

Im Rahmen der Festlegung der Prüfungsaspekte und Prüfungsziele kann es aufgrund von gesetzlichen oder betrieblichen Vereinbarungen vor Ankündigung und Beginn der Prüfung notwendig sein, Abstimmungen mit dem Datenschutzbeauftragten des Unternehmens, mit Vertretern der Belegschaft (Betriebsrat, Personalvertretung) oder mit einzelnen von der Prüfung betroffenen Personen zu führen.

Bei der inhaltlichen Planung einer konkreten Prüfung ist neben den bereits vorhandenen Informationen zum jeweiligen Prüfungsobjekt und der Risikoanalyse auch das Know-how der jeweiligen Prüfer zu berücksichtigen.

Zur Festlegung des Prüfungsvorgehens gehört auch die (projektmäßige) Zeit- und Kapazitätsplanung. Hierbei werden Prüfungsaufgaben zu Arbeitspaketen gebündelt, zeitlich mit Meilensteinen eingeplant und mit Personalkapazitäten und Verantwortlichkeiten unterlegt.

Hinweis auf IT-Prüfungsstandard (ITAF)

Anforderungen bezüglich der Fähigkeiten und Kompetenzen eines Prüfers sind in den IT-Prüfungsstandards »1006 – Expertise« und »1203 – Durchführung und Überwachung« der ISACA (vgl. Abschnitt 3.1.2) definiert.

Die Ergebnisdokumentation der Planung einer konkreten Prüfung ist das Prüfungskonzept. In der Regel ist das Prüfungskonzept auch gleichzeitig der offizielle Prüfauftrag. Je nach Ausgestaltung der Kompetenzen und Prozesse im Unternehmen wird das Prüfungskonzept zur Genehmigung dem Auftraggeber (i.d.R. die Geschäftsführung oder der Leiter der Internen Revision) vorgelegt. Dies dient in erster Linie der verbindlichen Verständigung über die Inhalte der Prüfung und vereinfacht später die Berichtsabstimmung.

Die Genehmigung durch den Leiter der Internen Revision erfolgt in der Regel dann, wenn die Mehrjahresplanung und/oder der in der vorausgehenden Prüfungsplanung erstellte Prüfungsplan durch die Unternehmensleitung oder ein Aufsichtsorgan genehmigt wurde (vgl. Kapitel 6).

Aufgrund des Auftragscharakters und einer möglichen Prüfung der Internen Revision durch externe Prüfer sollte auch für einen sachverständigen Dritten aus dem Prüfungskonzept nachvollziehbar hervorgehen, was, warum, wie und mit welchem Ziel von wem und wann geprüft wird.

Daher empfiehlt sich, folgende Informationen in das Prüfungskonzept aufzunehmen:

- Darstellung des betroffenen Prüfungsfelds
- Darstellung der Risikosituation möglicher Prüfungsgegenstände und Prüfungsobjekte
- Auswahl der Prüfungsobjekte mit Begründung
- Auswahl der Prüfungsaspekte und Prüfungsziele je Prüfungsobjekt mit Begründung
- Auswahl der Prüfungsart je Prüfungsobjekt mit Begründung
- Abgrenzung der Aspekte, die ausdrücklich nicht zum Prüfungsinhalt gehören
- Darstellung wesentlicher interner und externer Prüfungsmaßstäbe (z.B. übergeordnete Arbeitsanweisungen, Gesetze, Standards – vgl. Kapitel 3)
- Darstellung wesentlicher Meilensteine bzw. Termine (z.B. Beginn der Prüfungshandlungen, Termin zur Vorlage des Berichtsentwurfs)
- Aufführung der eingeplanten Prüfer mit ihren Kapazitäten und Rollen in der Prüfung

Wegen ihres Auftragscharakters sollte das Konzept ein formales, für alle Prüfungen einheitliches Dokument sein, aus dem auch der Ersteller und das Erstellungsdatum hervorgehen.

Praxisbeispiel

Darstellung der IT-Risikosituation zu einem Nicht-IT-Prüfungsobjekt (z.B. Bilanzerstellungsprozess eines Unternehmens):

Risiken aus fehlerhaften

- Datenübernahmen/Dateneingaben,
- Abbildungen von Beständen und
- Datenaggregationen sowie
- Analysen und Reports der Daten

haben ihre Ursachen in den IT-Systemen, insbesondere durch:

- fehlerhafte Funktion der IT-Anwendung,
- fehlerhafte Übertragung von Daten aus Vorsystemen,
- unangemessene Eingabekontrollen,
- unangemessene oder zu umfangreich vergebene Berechtigungen; keine angemessene systemseitige Forcierung von Funktionstrennungen und/oder
- unangemessene Datenmodellierung.

7.1.2 Prüfungsankündigung

Der Fachbereich erhält in der Regel eine Information über die geplante Prüfung.

Eine solche Ankündigung kann telefonisch, persönlich oder schriftlich erfolgen, wobei eine schriftliche Ankündigung (auch in elektronischer Form) grundsätzlich vorzuziehen ist. Je nach Prüfungsinhalt oder -art sollte die Ankündigung zwei bis vier Wochen vor dem tatsächlichen Prüfungsbeginn im Fachbereich eingehen. Bei einigen Prüfungen kann auch eine deutlich längere Ankündigungsfrist notwendig sein, um später angemessene Prüfungsergebnisse zu erzielen. Gründe hierfür könnten aufwendige Reisevorbereitungen oder aber Personalengpässe in der geprüften Einheit sein. Dies ist insbesondere dann wichtig, wenn die geprüfte Einheit nur wenige Mitarbeiter hat, deren Anwesenheit erforderlich ist.

Bei Verdacht auf dolose Handlungen oder bei einer Kassenprüfung kann eine Prüfungsankündigung auch sehr kurzfristig oder gar nicht erfolgen. Gleiches gilt oft auch, wenn ein Prüfungsziel etwa die Beurteilung der Wirksamkeit von Regelungen zu Vertretungen oder zum Schutz von Informationen ist (bspw. abgeschlossenes Büro bei Abwesenheit und/oder Aktivierung der Bildschirmsperre).

Die Prüfungsankündigung sollte generell an die Führungsebene unterhalb der Unternehmensleitung adressiert werden. Nach Rücksprache mit der Unternehmensleitung bzw. der betroffenen Führungsebene können auch nachgeordnete Führungsebenen direkt informiert werden.

Praxishinweis

Es ist in beiderseitigem Interesse, dass der zu prüfende Fachbereich auf die Prüfungsankündigung reagiert und sinnvolle Vorbereitungsmaßnahmen ergreift, u.a. einen Ansprechpartner für die Revision benennt, der während der Prüfung verfügbar ist.

Der benannte Ansprechpartner sollte sich im Bereich gut auskennen und im Idealfall Erfahrung aus früheren Prüfungen haben.

Je nach Umfang und Intensität der Prüfung sind geeignete Besprechungsräume vorzusehen, die auch die erforderliche technische Ausstattung haben (Beamer, Netzwerk).

Wenn in der Prüfung auch Interviews vorgesehen sind, etwa mit einer Livedemonstration von Konfigurationseinstellungen an Servern, dann sind geeignete Personen für solche Interviews zu identifizieren.

Alle direkt Betroffenen sollten schließlich rechtzeitig über die bevorstehende Prüfung informiert und ggf. direkt eingeladen werden.

Die Prüfungsankündigung dient dazu, den geprüften Bereich über Gegenstand und Ziel der Prüfung vorab zu informieren, damit er benötigte Unterlagen und andere Informationen (ggf. vorab) bereitstellen kann. Je früher informiert wird, desto eher ist eine effiziente Prüfungsdurchführung sichergestellt. Folgende Informationen sind in die Prüfungsankündigung aufzunehmen:

Prüfungsankündigung		
Input	**Einflussgrößen**	**Output**
genehmigtes Prüfungskonzept	Prüfungsinhalt	Prüfungsankündigung
	Prüfungsart	
Aktivitäten		**Werkzeuge**
Erstellen der Prüfungsankündigung		Office-Tools
Information der Betroffenen (Geprüften)		

Tabelle 7–2: Input-Output-Beziehung Prüfungsankündigung

- Grund der Prüfung, z.B. gemäß Revisionsplanung, Sonderprüfung
- Beginn und geplante Dauer der Prüfung
- Bezeichnung, Gegenstand und Ziel der Prüfung
- Name(n) des/der Prüfenden, Name der Prüfungsleitung
- Benötigte Unterlagen/Informationen
- Ansprechpartner/Koordinator, ggf. auch ein (neutraler) Moderator, der Treffen zwischen Prüfern und Geprüften moderiert.
- Termin für ein Kick-off-Meeting

Eine Prüfungsankündigung könnte beispielsweise wie folgt aufgebaut sein:

Praxishinweis
Prüfungsankündigung

Sehr geehrte Damen und Herren,

entsprechend dem vom Vorstand genehmigten Revisionsplan kündigen wir die Prüfung der Berechtigungen und Berechtigungskonzepte der Anwendung <XYZ> an.

Die Prüfung beginnt am 10. Juni 2016 und dauert 4 Wochen. Sofern die Prüfung aus Ihrer Sicht aus wichtigem Grund nicht zu diesem Zeitpunkt starten oder in diesem Zeitraum durchgeführt werden kann, setzen Sie sich bitte unter Angabe einer Begründung kurzfristig mit uns in Verbindung.

Die Prüfung wird die Vorgehensweise der Anlage, Änderung und Löschung von Berechtigungen sowie die systemtechnischen Möglichkeiten zur Umsetzung des Berechtigungskonzepts umfassen. Ziel der Prüfung ist festzustellen, ob die eingerichteten Berechtigungen den beantragten und dokumentierten Rechten sowie den tatsächlichen Tätigkeitsgebieten der Mitarbeiter entsprechen.

Unsere Prüfung betrachtet dabei die folgenden Bereiche:

- Vorgehensweise der Anlage, der Änderung und der Löschung von Berechtigungen in der o.g. Anwendung
- Definition der Berechtigungen (über Profile, Rollen) in der o.g. Anwendung
- Berechtigungsstruktur und -konzepte
- Umsetzung der Funktionstrennung – unvereinbare Rechte
- Administrationsberechtigungen

Änderungen der genannten Bereiche im Rahmen der weiteren Prüfungsplanungen und der Prüfungsdurchführung sind möglich. →

Wir bitten Sie, uns vorab, spätestens zu Prüfungsbeginn, die folgenden Informationen bereitzustellen:

- Dokumentation der Berechtigungen
- Dokumentation der Customizing-Einstellungen

Setzen Sie bitte Ihre Mitarbeiter von der geplanten Prüfung in Kenntnis. Die frühzeitige Information ist förderlich, um eine effiziente Prüfungsdurchführung zu ermöglichen. Des Weiteren bitten wir Sie, uns bis 15. Mai 2016 einen Ansprechpartner für die Prüfung zu nennen, der in Abstimmung mit der Prüfungsleitung die Koordination der Aktivitäten übernimmt. Zur Vereinbarung eines Termins für das Kick-off-Meeting werden wir den von Ihnen benannten Koordinator ansprechen.

Mit freundlichen Grüßen

IT-Revisionsleitung/verantwortliche IT-Revisorin/
verantwortlicher IT-Revisor

7.2 Voruntersuchung

Mit Genehmigung des Prüfungskonzepts und Ankündigung der Prüfung sind die Planungs- und Vorbereitungsaktivitäten in der Regel noch nicht abgeschlossen.

Bevor die eigentliche Prüfung durchgeführt wird, sind im Rahmen der Voruntersuchung die Prüfungsaktivitäten zu planen und die geprüften Organisationseinheiten mittels eines Kick-off-Meetings auf die Prüfung vorzubereiten.

7.2.1 Arbeitsprogramm (Prüfungsprogramm)

Im Rahmen der Voruntersuchung sind nun auf Basis der im Konzept festgelegten Prüfungsobjekte, Prüfungsaspekte und Prüfungsziele und entsprechend der definierten Prüfungsart die einzelnen Prüfungsaktivitäten (Prüfungshandlungen) durch die Prüfer inhaltlich und zeitlich zu planen und in einem Arbeitsprogramm (Prüfungsprogramm) zu dokumentieren (vgl. Abschnitt 2.2.7).

Das Arbeitsprogramm kann je nach Organisation der IT-Revision unterschiedlich konkret ausgestaltet sein. Bei erfahrenen und eigenverantwortlich arbeitenden Prüfern kann das Arbeitsprogramm zu Beginn der Prüfungsdurchführung allein aus den Informationen des Prüfungskonzepts bestehen und erst während der Prüfung als Teil der Prüfungsdokumentation verfeinert werden. Für Personal, das erst seit kurzer Zeit in der Revision mitarbeitet, bietet sich dagegen an, konkrete Handlungsanweisungen und Fragestellungen ins Arbeitsprogramm aufzunehmen.

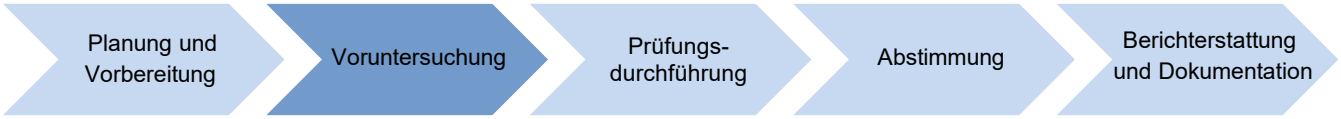

Abbildung 7–3: Prüfungsdurchführung – Voruntersuchung

Voruntersuchung		
Input	**Einflussgrößen**	**Output**
genehmigtes Prüfungskonzept	Detaillierungsgrad des Prüfungskonzepts	Arbeitsprogramm (Prüfungsprogramm)
Prüfungsankündigung	Prüfungsart	
Aktivitäten		**Werkzeuge**
Planung der Prüfungsaktivitäten und -handlungen		Planungs- und Projektmanagement-Tools
Durchführung des Kick-off-Meetings		Office-Tools
Erhebung/Aufbereitung zusätzlicher Informationen zu den Prüfungsobjekten, ggf. Vertiefung des Verständnisses der Geschäftsziele, Prozesse, IT-Systeme ggf. Vertiefung des Wissens über Fehlerrisiken und kritische Maßnahmen zur Risikobehandlung		

Tabelle 7–3: Input-Output-Beziehung Voruntersuchung

Konkrete Handlungsanweisungen und Fragestellungen in Arbeitsprogrammen sind auch dann sinnvoll, wenn mehrfach gleichartige Prüfungen (etwa die Prüfung von mehreren Filialen) durchgeführt werden und die Ergebnisse vergleichbar sein sollen.

Zur Erstellung des Arbeitsprogramms ist es in der Regel erforderlich, weitere interne und externe Informationen zu den Prüfungsobjekten zu erheben und aufzubereiten:

- Interne Informationen könnten hierbei z.B. aus Veröffentlichungen der geprüften Bereiche im Firmennetzwerk (Intranet) stammen.
- Externe Informationen sind z.B. Standards und Normen sowie Gesetze, Verordnungen oder auch Fachliteratur zum Thema.

Exkurs
Zusammenarbeit von IT- und Fachrevisoren sowie Abhängigkeiten ihrer Prüfungsergebnisse untereinander

Da heutzutage in nahezu jedem Geschäftsprozess auch IT eine entscheidende Rolle spielt, ist es unerlässlich, bei einer Angemessenheits- und Wirksamkeitsprüfung von Geschäftsprozessen auch die dabei verwendete IT zu betrachten. Hieraus ergibt sich die Notwendigkeit, bereits bei der (Mehr-) Jahresplanung, spätestens aber bei der Erstellung der Prüfungskonzeption, ein Zusammenarbeitsmodell zwischen der IT- und der Fachrevision festzulegen.

Es empfiehlt sich dabei, ausgehend von der Risikosituation in den einzelnen Geschäftsprozessen, die zu prüfenden IT-Systeme auszuwählen.

Wie tief eine Prüfung der IT-Systeme und der darunterliegenden IT-Prozesse und IT-Infrastruktur erfolgen muss, ist abhängig →

von Ergebnissen bereits erfolgter IT-Prüfungen. Idealerweise kann sich der IT-Revisor bei einer vom Geschäftsprozess ausgehenden IT-Prüfung auf die Implementierung fachlicher Funktionalitäten konzentrieren, da z.B. Netzwerkinfrastruktur oder Softwarebeschaffungs- und Betriebs- bzw. Softwareentwicklungsprozesse in separaten, speziellen Prüfungen bewertet wurden, auf die dann zurückgegriffen werden kann.

Bei der Bewertung der Geschäftsprozesse sind die Ergebnisse aus der fachlichen Prüfung und der Prüfung der IT-Systeme zusammenzuführen. Prüfer der Geschäftsprozesse können sich also auf die Ergebnisse der IT-Prozess-Prüfung stützen, d.h., sie brauchen das Design des IKS für die betrachteten IT-Prozesse nicht mehr zu prüfen und können sich darauf beschränken, aus fachlicher Sicht einzelne Prozessdurchläufe für die Anwendung nicht mehr zu prüfen und können sich darauf beschränken, aus fachlicher Sicht einzelne Prozessdurchläufe für die Anwendung zu prüfen, die ihren zu prüfenden Geschäftsprozess unterstützt.

Insgesamt ist so eine belastbare Aussage zur Angemessenheit und Wirksamkeit der Geschäftsprozesse und der dafür eingesetzten IT möglich.

Soweit in der Konzeptionsphase noch nicht bzw. nicht in der erforderlichen Detaillierungstiefe erledigt, sind bei der Erarbeitung des Prüfungsprogramms weitere Aspekte zu berücksichtigen:

- Das betriebswirtschaftliche Verständnis über die betroffenen Prozesse und IT-Systeme
- Die Geschäftsziele der betrachteten Prozesse/IT-Systeme
- Kritische Maßnahmen zur Risikobehandlung sowie möglichen IT-Fehlerrisiken

Praxishinweis

Je nach Anzahl und Know-how der eingesetzten Prüfer sowie Umfang der Prüfung kann die Entwicklung eines sehr detaillierten Zeitplans für Prüfungen als Ergänzung zum Arbeitsprogramm sinnvoll sein, hier am Beispiel einer ISO/IEC-27001-Prüfung gezeigt.

Zeitplan für Prüfungen (Auszug)
Name des Unternehmens / Logo
- vertraulich –

Datum und interne Audit-Nr:	18.-20 Juni, 2015, _A4172
Auditor-Name(n) und Rollen:	LA: Lead Auditor
Standorte / Land:	Straße, PLZ, ggf. Bezeichnung des Standortes/Werks
Audit-Teilnehmer und Rollen	… B: Beobachter
Zugrunde liegende Regelwerke/Gesetze:	ISO/IEC 27001:2013

Audit 1. Tag						
Datum	**Ort / Land**	**Zeit**	**Auditor**	**Themen**	**Dokumente**	**Verantwortlich**
18. Juni 2015	Stuttgart, Deutschland	9:00 – 10:30		**Einführungsrunde**	Unternehmensstrategie, Kundenzufriedenheit, Managementbewertung	GL, QMB, alle Prozessverantwortliche
		10:30 – 12:30	Frau A, Herr B, Herr C	**Prüfungsfeld »Governance/ Compliance – Strategie«**	Sicherheitsrichtlinie, Auditberichte, Korrektur- und Vorbeugungsmaßnahmen	ISMS- Managerin, QMB, Risk- Managerin
		12:30 – 13:15	Alle	Mittagessen		
		13:15 – 14:00	Frau A, Herr B, Herr C	**Prüfungsfeld »Governance/ Compliance – Strategie« (Forts.)**	Strategie-Handbuch, Berechtigungsprozess, Incident Management	ISMS-Managerin, QMB, Risk-Managerin
		15:00 -16:00		**Prüfungsfeld »Personal«**	Richtlinien	Personalabteilung, Bereichsleiter
				…	…	…
		16:30- 17:15		Zusammenfassung		Auditoren
		17:15-18:00		**Tages-Abschlussgespräch**		Alle
		18:00		**Audit-Ende 1. Tag**		

Teilnehmerliste

Name (in Druckbuchstaben)	Bereich/Rolle	Ort/Datum	Unterschrift

Die Prüfungsobjekte des Arbeitsprogramms bei einer Prüfung der IT-Prozesse, die auch unterstützende IT-Systeme umfassen, sollten sich an der Prüfungsart (vgl. Abschnitt 2.2.6) orientieren. Beispielhaft gliedert sich eine IT-Systemprüfung in folgende Schritte:

- Im ersten Schritt nimmt die Revision das System auf (Erhebung des Regelungsgefüges und der technischen Unterstützung).
- Im zweiten Schritt untersucht die Revision die Vorgaben, das Regelungsgefüge und deren technische Unterstützung dahingehend, ob die vorgesehenen Maßnahmen des IKS geeignet sind, die identifizierten Risiken angemessen zu behandeln.
- Im dritten Schritt prüft die Revision dann die Wirksamkeit der Maßnahmen in der praktischen Prozessabwicklung.

7.2.2 Kick-off-Meeting

Im Rahmen eines Kick-off-Meetings vor den eigentlichen Prüfungshandlungen können zwischen den Revisoren und dem/den benannten Ansprechpartner(n) der geprüften Bereiche

- das geplante Prüfungsvorgehen mit seinem zeitlichen Rahmen,
- mögliche Rahmenparameter, die die Einhaltung des geplanten Prüfungsvorgehens gefährden,
- die Erwartungen der Revision und der geprüften Bereiche (auch an die Kommunikationswege)

und weitere Themen besprochen werden, um die Informationen aus der Ankündigung zu ergänzen.

Das geplante Prüfungsvorgehen mit seinem zeitlichen Rahmen leitet sich aus dem Prüfungskonzept ab und wird den geprüften Bereichen so detailliert vorgestellt, wie es für deren Verständnis notwendig ist. In der Praxis zeigt sich hierbei, dass eine Erläuterung der Prüfungsziele und der verwendeten Revisionsbegriffe und -methoden hilfreich ist.

Mögliche Rahmenparameter, die die Einhaltung des geplanten Prüfungsvorgehens gefährden, sind z.B. aktuell laufende Änderungen am Prüfungsobjekt (z.B. Projekte zum Ablösen eines IT-Systems oder Organisationsänderungen).

Die Erwartungen der Revision an die Zusammenarbeit mit den geprüften Bereichen sowie die Erwartungen der geprüften Bereiche an die Revision sollten ebenso geklärt werden, denn eine wesentliche Voraussetzung für eine gute Durchführung einer Prüfung ist die aktive Mitwirkung der Fachbereiche.

Der Prüfende hat im Rahmen seines Prüfungsauftrags (aufgrund der Audit Charter) das Recht, alle notwendigen Dokumente und anderen Formen von Nachweisen anzufordern. Gleichzeitig ist der Fachbereich verpflichtet, diese Informationen bereitzustellen. Der Fachbereich darf jedoch Erklärungen erbitten, zu welchem Zweck angeforderte Nachweise erforderlich sind.

In allen Fällen ist unbedingt darauf zu achten, dass sich zwischen Prüfendem und Geprüftem kein Machtgefälle entwickelt, das die Prüfungen beeinträchtigt. In vielen Fällen empfiehlt es sich deshalb, allen Beteiligten – etwa im Rahmen einer kleinen Präsentation zum Kick-off-Meeting – noch einmal die im Unternehmen etablierten Regeln für die Mitwirkung in Erinnerung zu rufen.

Praxishinweis

Verhaltensregeln für den Fachbereich in der Revisionsprüfung – cum grano salis entnommen einem Originalbeispiel aus der IT-Industrie

1. Allgemeines

Richtiges Verhalten:
- Verstehe den Revisionsprozess
- Informiere im Bereich darüber, dass Prüfer kommen werden
- Sei geschäftsmäßig, freundlich, respektvoll gegenüber Prüfern und anderen geprüften Fachbereichen
- Löse erkannte Probleme (wenn möglich) schon während der Prüfung
- Stelle sicher, dass dein Arbeitsplatzrechner vollständig vorschriftsmäßig ist
- Mache die Prüfung zur ersten Priorität

Falsches Verhalten:
- Behindere den Prüfungsprozess
- Zeige Feindseligkeit gegenüber den Prüfern und anderen geprüften Fachbereichen
- Nehme direkten, unabgestimmten Kontakt zu den Prüfern auf

2. Anforderung von Informationen

Richtiges Verhalten:
- Stelle Informationen schnell zur Verfügung
- Stelle nur das Verlangte zur Verfügung
- Übergebe Informationen nur über den Ansprechpartner/Koordinator
- Stelle die vollständige Beantwortung sicher
- Frage über den Ansprechpartner/Koordinator nach, wenn die Anforderung unklar ist
- Informiere den Ansprechpartner/Koordinator, falls besondere Systemläufe zur Beantwortung der Anforderung nötig sind
- Übergib alle Informationen möglichst in einer Antwort

Falsches Verhalten:
- Verweigere Informationen
- Ändere Informationen ab (Achtung, kann in bestimmten Audits sogar strafbar sein!)

3. Interviews, Präsentationen, Vorführungen

Richtiges Verhalten:
- Stelle sicher, dass die richtigen Personen teilnehmen
- Überlege, welche Personen nicht mit den Prüfern sprechen sollten
- Stelle alle Anwesenden und Teilnehmer der Prüfung am Anfang vor
- Entwickle eine positive Einstellung zur Prüfung/zum Prüfer
- Antworte mit definitiver Aussage
- Schalte das Mobiltelefon während der Gespräche aus oder stumm →

Falsches Verhalten:
- Mache dir Gedanken, wenn Prüfer sich Notizen machen
- Spreche über Dinge, die nicht gefragt sind
- Nutze unklare Redewendungen wie »ich glaube/nehme an …«, »es sollte/müsste eigentlich …«
- Mache allgemeine Angaben, sei möglichst wenig konkret bei deinen Aussagen
- Vermittle den Eindruck, etwas sei außer Kontrolle
- Mache Aussagen zu Bereichen außerhalb deiner Zuständigkeit
- Sage wissentlich die Unwahrheit
- Nutze dein Smartphone für SMS und Chats, besonders während laufender Präsentationen
- Nutze dein Notebook/PC zu Nebentätigkeiten (Mail abrufen und bearbeiten) und führe Privatgespräche in der Prüfungsbesprechung

7.3 Prüfungsdurchführung

Unter dem Begriff Prüfungsdurchführung (Field Work) wird die Abarbeitung des im Rahmen der Vorbereitung erstellten Arbeitsprogramms verstanden.

Abhängig von der Prüfungsart sichtet der Prüfer vom zu prüfenden Bereich zur Verfügung gestellte Dokumente, führt Interviews und analysiert relevante Daten und beurteilt anschließend die gewonnenen Informationen nach den im Prüfungskonzept festgelegten Prüfungsaspekten und -zielen.

Ergebnisse aus der Beurteilung sollte der Prüfer bereits während der Prüfungsdurchführung mit den geprüften Bereichen abstimmen, um sicherzugehen, dass die spätere Aussage im Prüfungsbericht auch wirklich den Tatsachen entspricht.

Abarbeitung des Arbeitsprogramms

Vielfach erfordert die Abarbeitung des Arbeitsprogramms eine weitere Konkretisierung des Prüfungsverfahrens und der Prüfungsziele zu einzelnen Detailfragen. Diese Konkretisierung wird im Arbeitsprogramm ergänzt.

Hinweis auf IT-Prüfungsstandard (ITAF)

Weitere Anforderungen an die Abarbeitung des Arbeitsprogramms und deren Dokumentation sind in den folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) definiert:

- 1203 – Durchführung und Überwachung
- 1204 – Wesentlichkeit
- 1205 – Nachweise
- 1206 – Verwendung der Ergebnisse anderer Sachverständiger
- 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen

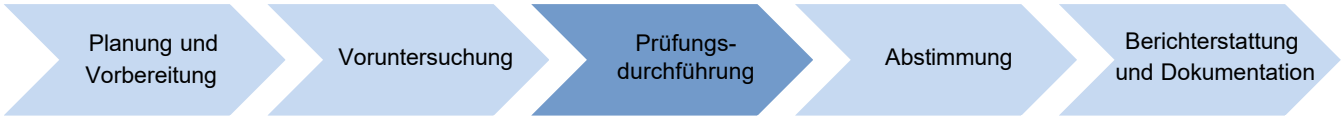

Abbildung 7–4: Prüfungsdurchführung

Prüfungsdurchführung		
Input	**Einflussgrößen**	**Output**
Arbeitsprogramm	Prüfungsart	Dokumentation der Abarbeitung des Arbeitsprogramms
Prüfungsaspekte		ggf. Präzisierung des Arbeitsprogramms
Prüfungsziele		Dokumentation der Feststellungen
Aktivitäten		**Werkzeuge**
Datenprüfungen		Vorgehens- und Referenzmodelle
Interviews		Prüfungs- und Revisionstools
Dokumentensichtungen		Data-Mining-Tools und Datenbank-Tools
Konkretisierung der Prüfungsverfahren und Prüfungsziele		Interviewtechniken
erste Beurteilungen		Checklisten
erste Abstimmungen		Office-Tools

Tabelle 7–4: Input-Output-Beziehung Prüfungsdurchführung

Die Abarbeitung des Arbeitsprogramms ist detailliert und nachvollziehbar zu dokumentieren (siehe Abschnitt 7.5). Die Abarbeitung des Arbeitsprogramms erfordert aber auch in den meisten Fällen den Einsatz von technischen und methodischen Werkzeugen, wie etwa Prüfungs-/Revisionstools oder Vorgehens- und Referenzmodelle.

Technische Werkzeuge (Prüfungs- und Revisionstools)

Insbesondere bei der Prüfung von großen Datenmengen im Bereich Stamm- und Bewegungsdaten, bei komplexen Konfigurationen, umfangreichen Protokollen in Form von Logdaten und technischen Sachverhalten kann auf einen Einsatz von Tools oft nicht verzichtet werden. Bei einfacheren Sachverhalten können auch Excel oder eine SQL-Schnittstelle ausreichend sein. Bei komplexeren Sachverhalten oder bei größeren Datenmengen sind spezielle Datenanalysetools für die Revision sinnvoll, wie etwa Audicon IDEA oder ACL Analytics[1], die auch eine entsprechende Protokollierung der durchgeführten Prüfungsschritte und Ergebnisse durchführen. Bei der Prüfung von Berechtigungen kommt vermehrt vorkonfigurierte Standardsoftware zur Anwendung, um komplizierte Zusammenhänge zu analysieren. Zur Ermittlung von Auffälligkeiten bei Massendatenanalysen kann sogenannte »Data Mining«-Software eingesetzt werden.

Methodenbasierte Werkzeuge (Vorgehensmodelle, Referenzmodelle)

Zu den methodenbasierten Werkzeugen gehören neben verschiedenen Interviewtechniken unter anderem auch Werkzeuge

- zur Bestimmung von Prozessreifegraden (z.B. COBIT-Reifegradmodell, CMMI, SPICE),
- zur Ermittlung von Stichproben sowie
- zur Ermittlung von Auffälligkeiten bei Massendatenanalysen.

Zu den methodenbasierten Werkzeugen zählen auch standardisierte Checklisten zu speziellen Themen, die vor der Anwendung kritisch hinterfragt und – wie alle generischen Werkzeuge – auf den konkreten Prüfungskontext angepasst werden müssen.

Prüfung durch Dritte

Bei Spezialthemen oder bei Prüfungen mit speziellen Methoden kann es sinnvoll sein, die Prüfung mithilfe von externem Prüfungspersonal durchführen oder zumindest von ihnen begleiten zu lassen, beispielsweise, wenn kein Mitarbeiter der IT-Revision über ausreichend detailliertes Know-how verfügt und/oder wenn die IT-Revision keine passenden Werkzeuge besitzt. Auch bei akuten Personalengpässen kann es sinnvoll sein, externes Prüfungspersonal zu beauftragen, um die Abarbeitung des Prüfungsplans nicht zu gefährden.

Zu unterscheiden ist dieses externe Prüfungspersonal im Auftrag der Internen Revision von externem Prüfungspersonal einer Wirtschaftsprüfungsgesellschaft im Rahmen der Prüfung des Jahresabschlusses. Externes Prüfungspersonal im Auftrag der Internen Revision erstellt **kein** Testat zum Jahresabschluss und ist im Rahmen dieses Prüfauftrags ausschließlich der Leitung der Revision und nicht dem Aufsichts- oder Verwaltungsrat rechenschaftspflichtig.

Ob externes Prüfungspersonal im Auftrag der Internen Revision nur ein vorgegebenes Arbeitsprogramm abarbeitet oder dieses auf Basis des Prüfungskonzepts selbst erstellt, also an der Voruntersuchung (vgl. Abschnitt 7.2) beteiligt ist, hängt von den jeweiligen Anforderungen des Auftraggebers ab. Sie legen auch fest, ob externes Prüfungspersonal selbst einen Prüfungsbericht erstellen (vgl. Abschnitt 7.5) oder nur seine Prüfungsdokumentation der Revision übergeben muss.

Bewertung der Prüfungsergebnisse

Aus der Abarbeitung des Arbeitsprogramms ergeben sich je nach Prüfungsverlauf mehr oder weniger zahlreiche und schwerwiegende Feststellungen (sog. »Findings«) sowie Empfehlungen. Feststellungen werden anhand einer prüfungsunabhängigen Skala beurteilt.

Praxishinweis
Beispiele für die Klassifizierung von Feststellungen

Ein geringer Mangel kann beispielsweise die Missachtung interner Vorschriften zu formellen Anforderungen an interne Dokumente sein, da diese Missachtung keinen relevanten wirtschaftlichen Schaden verursacht.

Schwerwiegende Mängel sind z.B. massive, regelmäßige oder bewusste Verstöße gegen gesetzliche Bestimmungen. Aber auch unerkannte Schwachstellen in wesentlichen Anwendungen oder allgemein unzureichende Maßnahmen zur Behandlung wesentlicher IT-Risiken zählen dazu. Etwa das Fehlen eines Notfall- oder Datensicherungskonzepts stellt für die Mehrheit der Unternehmen einen schwerwiegenden Mangel dar, da ein Ausfall der IT oder ein erheblicher Datenverlust die Geschäftstätigkeit stark beeinträchtigen und entsprechende monetäre Folgen haben kann.

Besondere Umsicht ist geboten, wenn bei der Beurteilung der Rechtmäßigkeit Mängel festgestellt werden. Einerseits ist die Revision im Interesse der Unternehmensleitung verpflichtet, Verstöße offenzulegen und die Beseitigung des Mangels anzuregen. Andererseits müssen stets die Unternehmensinteressen berücksichtigt werden. Das Hinzuziehen von Fachjuristen ist daher in solchen Fällen stets empfehlenswert.

Negative Feststellungen beschreiben Mängel. Sie werden in der Regel in verschiedene Klassen eingeteilt. Eine gängige Unterteilung ist:

- Geringer Mangel
- Mittlerer Mangel

1 Beide Programme zählen zu den sogenannten Computer Assisted/Aided Auditing Techniques (CAAT).

Praxisbeispiel
Feststellungen aus einer ISO/IEC-27001-Prüfung

Finding Nr.	Klassifikation	Referenz zu Norm	Kapitel	Beschreibung	Verantwortliche/r	Termin	Status (aktuell)
1	Sehr hoch	27001	A 17.1	Keine BCM-Strategie, kein BCM-Plan, kein BCM-Test	BCM-Manager	Bis Ende August 2016	Noch nicht begonnen
2	Sehr hoch	27001	A 9.4	Keine Zugangskontrolle implementiert	Net Admin	Bis Ende August 2016	Noch nicht begonnen
3	Hoch	27001	A 15.2	Nicht alle Lieferanten werden geprüft	Beschaffung	Bis Ende September 2016	Noch nicht begonnen
4	Sehr hoch	27001	A 12.3	Backup-Bänder und -DVDs werden im Serverraum aufbewahrt	Net Admin	Bis Ende Juni 2016	Noch nicht begonnen

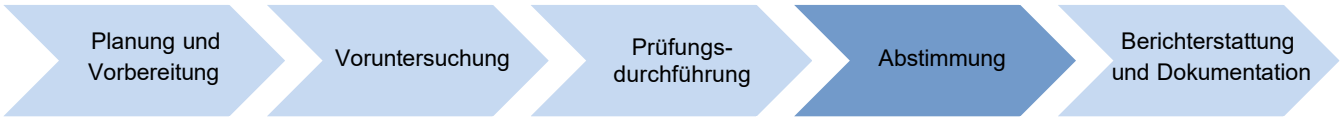

Abbildung 7–5: Prüfungsdurchführung – Abstimmung

- Wesentlicher Mangel
- Schwerwiegender Mangel
- Besonders schwerwiegender Mangel

In welche Klasse eine Feststellung fällt, hängt von verschiedenen Beurteilungskriterien ab. Diese Beurteilungskriterien beruhen auf den für das Unternehmen relevanten Risiken und sollten sowohl für das Revisionspersonal als auch für die Geprüften verbindlich, zugänglich und nachvollziehbar sein.

Wird der potenzielle wirtschaftliche Schaden als primäre Messgröße verwendet, soll darauf geachtet werden, dass Rechts- und Reputationsrisiken nicht an Gewicht verlieren.

Eine Feststellung ohne Mangel weist lediglich auf einen bestimmten Sachverhalt hin (Informationsfunktion).

Um die Feststellungen zu beheben, werden durch die Revision Maßnahmen empfohlen. Diese können auch durch den geprüften Bereich vorgeschlagen und entsprechend übernommen werden. Empfehlungen können auch zu anderen Aspekten ausgesprochen werden, die nicht Teil einer Feststellung sind, der Revision jedoch im Rahmen der Prüfung aufgefallen sind.

Da ein primäres Ziel der Internen Revision die Reduzierung möglicher Schäden für das Unternehmen ist, haben **positive Feststellungen** eine eher untergeordnete Rolle in der Prüfungsberichterstattung und werden deshalb im weiteren Verlauf nicht berücksichtigt. Ausnahmen davon beziehen sich auf Feststellungen aus vorangegangenen Prüfungen, die nun erfolgreich beseitigt worden sind.

Die Klassifikation von Feststellungen geschieht häufig in Tabellenform.

7.4 Abstimmung

Der Teilprozess zur Abstimmung der Prüfungsfeststellungen und des Prüfungsberichts gliedert sich in der Regel in drei Phasen:

- Inhaltliche Verifizierung der Feststellungen mit dem geprüften Bereich
- Revisionsinterne Abstimmung des Berichtsentwurfs
- Abstimmung des Berichtsentwurfs mit dem geprüften Bereich

Die **erste Phase** erfolgt im Regelfall bereits während der Prüfungsdurchführung oder zu deren Abschluss. Hierbei empfiehlt es sich, nur die einzelnen Feststellungen inhaltlich zu besprechen und abzusichern und eine Wertung der Feststellung seitens der Revision noch nicht zu kommunizieren.

Die **zweite Phase** beginnt nach der Prüfungsdurchführung. Das Prüfungsteam konsolidiert die einzelnen Feststellungen, bewertet sie und erstellt den ersten Berichtsentwurf. Dieser wird im Prüfungsteam und anschließend mit den zuständigen Führungskräften der Revision abgestimmt. Die Abstimmung mit den zuständigen Führungskräften der Revision ist unter anderem aus folgenden Gründen notwendig:

- Kontrolle, ob die Prüfungsziele gemäß Prüfungskonzept eingehalten wurden
- Information über firmenpolitisch kritische Feststellungen
- Qualitätssicherungsmaßnahme innerhalb der Revision

Abstimmung		
Input	**Einflussgrößen**	**Output**
Dokumentation der Feststellungen mit (ersten) Beurteilungen	-	abgestimmter Prüfungsbericht
Aktivitäten		Werkzeuge
Verifizierung der Inhalte der Prüfungsdokumentation		Berichterstellungsfunktionen in Prüfungs- und Revisionstools
revisionsinterne Abstimmung der Inhalte		Web- oder Groupware-Lösungen
Abstimmung der Inhalte mit den Geprüften		Office-Tools

Tabelle 7–5: Input-Output-Beziehung Abstimmung

Ist der Prüfungsbericht revisionsintern finalisiert, beginnt als **dritte Phase** die Abstimmung des Prüfungsberichts mit dem geprüften Bereich. Ehe die endgültige Fassung des Prüfungsberichts verteilt wird, erhält der geprüfte Fachbereich bzw. Unternehmensteil dabei die Gelegenheit, die bei der Prüfung getroffenen Feststellungen auf Vollständigkeit und sachliche Richtigkeit hinsichtlich der Darstellung des vorgefundenen Sachverhalts sowie hinsichtlich der Ursache und Auswirkung der Abweichung vom Prüfungskriterium zu prüfen und ggf. eine Richtigstellung einzufordern. Dies betrifft nicht die Bewertung der Feststellungen.

Hierbei ergibt sich zudem die Möglichkeit, Maßnahmen zur Verringerung (sog. »Mitigation«) aufgedeckter IT-Risiken inhaltlich und terminlich zu vereinbaren.

Grundsätzlich sollte der Teilprozess Abstimmung zeitlich fest definierte Meilensteine haben, um eine zeitnahe Berichterstattung gegenüber den Auftraggebern zu gewährleisten.

7.5 Berichterstattung und Dokumentation

Die Dokumentation der Durchführung einer konkreten Prüfung lässt sich in zwei Dokumentenklassen gliedern:

- Arbeitsprogramm und dessen Durchführungsdokumentation (Prüfungsdokumentation)
- Prüfungsbericht (ggf. mit Anlagen)

Hinweis auf IT-Prüfungsstandard (ITAF)

Anforderungen an die Berichterstattung und Dokumentation sind in den folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) definiert:

- 1007 – Aussagen
- 1008 – Kriterien
- 1401 – Berichterstattung

7.5.1 Prüfungsdokumentation

Für die Dokumentation können verschiedene Formen genutzt werden. Neben einfachen Formularen können auch spezielle Prüfungs- und Revisionstools eingesetzt werden, die über eine Reporting-Funktion verfügen.

Zu Nachweiszwecken und zur Sicherstellung der Nachvollziehbarkeit sollten die Prüfungsdokumente in einer für alle Beteiligten nachvollziehbaren Ordnerstruktur abgelegt werden. Insbesondere sollte darauf geachtet werden, dass eine einheitliche Nomenklatur genutzt und sprechende Verzeichnis- und Dateinamen verwendet werden, aber auch, dass auf Umlaute, Sonder- oder Leerzeichen verzichtet wird.

Praxishinweis

Alle im Rahmen der Prüfung erstellten Dokumente (einschließlich Nachweise) sind nach Abschluss der Prüfung gegen Veränderung zu schützen und langfristig zu archivieren. Für einige Branchen gelten gesetzliche Aufbewahrungsfristen (z.B. bei Banken 6 Jahre).

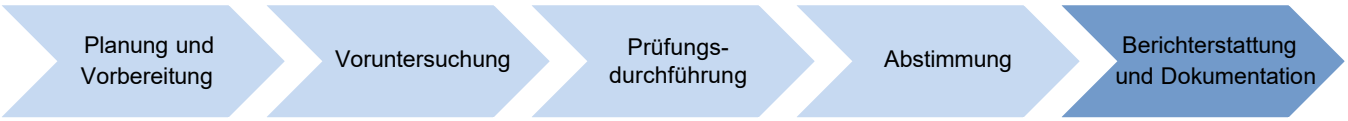

Abbildung 7–6: Prüfungsdurchführung – Berichterstattung und Dokumentation

Soweit Prüfungsziele mit der Prüfung nicht erreicht werden, sind jeweils Ursachen und Auswirkungen der Abweichung zu ermitteln und zu dokumentieren.

Für eine einfache Referenzierung aller Dokumente können geeignete bzw. im Unternehmen bereits vorhandene Web- oder Groupware-Lösungen verwendet werden.

Um Dateien rasch wiederfinden zu können, sollten sie nach einer einprägsamen Namenskonvention durchgängig und eindeutig benannt werden. Nur so sind zudem eine eindeutige Zuordnung zum Thema und eine klare Referenzierung in Arbeitsprogrammen möglich.

Praxishinweis
Ordnerstruktur

Die Ordner werden nummeriert, um stets die gleiche Struktur zu erreichen und Unterordner systematisch einordnen und leichter auffinden zu können.

Ein Ordner setzt sich also aus einer Ziffer und einem möglichst sprechenden Begriff zusammen. In den jeweiligen Ordnern werden folgende Dokumente abgelegt:

- **10_Projektmanagement:** Dokumente wie z.B. Offene-Punkte-Listen, Listen der Ansprechpartner, Planungsunterlagen für den Teameinsatz bei größeren Prüfungen usw.
- **20_Ankuendigung:** Prüfungsankündigung
- **30_Arbeitspapiere:** Neben dem Arbeitsprogramm die verarbeiteten Dokumente wie z.B. bereitgestellte Richtlinien, Verfahrens- oder Prozessbeschreibungen oder sonstige Nachweise, die für die Prüfung herangezogen werden.
- **40_Bericht:** Berichtsentwürfe und der finale Bericht sowie ggf. Freigabedokumente.
- **50_Wissen:** Dokumente, die zur Vorbereitung oder im Laufe der Bearbeitung eines Themas gefunden werden und zur Wissensanreicherung dienen können, z.B. Standards, Gesetze, Artikel oder Prüfungsleitfäden, Referenzierung von Dokumenten.

Zur Unterscheidung der jeweiligen Prüfungsaufträge wird ein übergeordneter Hauptordner eingerichtet und jedem Unterordner dann ein eindeutiges Buchstaben-Zahlenkürzel vorangestellt.

Beispiel: Kürzel »BER16« für den Hauptordner »Berechtigungsprüfung_2016«, entsprechend dann: »BER16_10_Projektmanagement« usw.

Praxishinweis
Referenzierungsschema für Dokumente

- [Prüfungskürzel]_[1. Ziffernfolge Unterordner ##]. [2. Ziffernfolge lfd. Nummer ##]_[Name]_v[#.#] Beispiel: BER16_30.01_Arbeitsprogramm_SAP-FI-Berechtigung_v0.4
- Die laufende Nummer wird für Dokumente innerhalb eines Ordners hochgezählt. Sollten Dokumente inhaltlich zusammengehören, z.B. ein Benutzerantrag in deutscher und englischer Sprache, können diese mit einem Zusatzbuchstaben versehen werden. Beispiel: BER16_30.01a_Benutzerantrag_Deu.pdf und BER16_30.01b_User_Registration_Request_Eng.pdf
- Die Versionierung sollte nur für eigenerstellte Dokumente erfolgen. Für erhaltene Dokumente sollte der original verwendete Dateiname beibehalten werden.

Die Versionen werden nach folgender Regel verwaltet:

- Hauptversion(en): #.0
- Nebenversionen: 0.#
- Die aktuellen Hauptversionen werden nicht gelöscht. Es wird ein zweiter Dateistrang eröffnet, d.h., dass dann zwei Dateien vorhanden sein können – z.B. [Dateiname]_v1.0 und [Dateiname]_v1.1.
- Alte Versionsstände können in einem Unterordner z.B. ARCHIV je Hauptordner zur Verbesserung der Übersichtlichkeit verschoben werden.

7.5.2 Prüfungsbericht

Der Zweck einer IT-Prüfung liegt letztlich darin, die (weitere) Optimierung der Unternehmensprozesse durch die jeweiligen Prozesseigner anzustoßen, und damit die wirtschaftliche Situation des Unternehmens insgesamt zu verbessern. Um diesen Zweck zu erreichen, fasst die Revision ihre Prüfungsergebnisse, d.h. insbesondere ihre Revisionsempfehlungen, im Prüfungsbericht zusammen und tritt in Dialog mit den Geprüften.

Zielsetzung

Der Prüfungsbericht sollte

- fehlerfrei,
- objektiv,
- klar verständlich,
- kurzgefasst,
- vollständig,
- konstruktiv und
- termingerecht

sein, um seine Botschaft eindeutig und verständlich zu überbringen. Da der Hauptadressat des Prüfungsberichts die Unternehmensleitung ist, sollte der Bericht in einer für diesen Adressatenkreis verständlichen Weise formuliert sein. Dies umfasst ggf. auch kurze Erklärungen technischer Fachbegrif-

fe und Akronyme. Zur Veranschaulichung und zum besseren Verständnis können auch Grafiken und Farben zum Einsatz kommen (vgl. [Cascarino 2012, S. 123-125]). Bei IT-Sachverhalten kann dies nicht immer einfach umsetzbar sein, weshalb auf diesen Punkt besondere Sorgfalt verwendet werden sollte, um die nötige Aufmerksamkeit zu erhalten (vgl. Abschnitt 1.1).

Ein überzeugender Prüfungsbericht sollte über Mängel bzw. Schwachstellen von Prüfungsobjekten und niemals über Personen (Ausnahme bei Sonderprüfungen im Zusammenhang mit Fraud) berichten.

Der Prüfungsbericht dient dazu, den Prüfungsvorgang und die Prüfungsergebnisse zu dokumentieren. Der Prüfungsbericht beinhaltet daher in strukturierter Form folgende Angaben in Bezug auf die durchgeführte IT-Prüfung:

- Angewandte IT-Audit-Richtlinien und IT-Audit-Standards sowie zu beachtende Gesetze und sonstige Vorgaben
- Geprüftes Unternehmen und seine Teile
- Empfänger
- Sperrklauseln
- Umfang, Zielsetzung, Zeitraum, Art, Ablauf, Reichweite und etwaige Abgrenzungen
- Alle Vollständigkeitserklärungen der Geprüften
  Im Rahmen *externer* Prüfungen müssen die Geprüften den Prüfern gegenüber schriftlich erklären, dass sie alle im Rahmen der Prüfung relevanten Informationen vollständig und nach bestem Wissen und Gewissen vorgelegt und keine wesentlichen Sachverhalte verschwiegen oder fehlerhaft wiedergegeben haben.
- Sonstige Angaben zum verwendeten Datenmaterial
- Zusammenfassung aller identifizierten Feststellungen
- Prüfungsbemerkungen (detaillierte Erläuterungen der Feststellungen)
- Die in der IT-Prüfung insgesamt gewonnenen Erkenntnisse, die daraus gezogenen Schlüsse, alle Empfehlungen, Vorbehalte und Einschränkungen

Bei der Entwicklung des Prüfungsberichts müssen alle relevanten Prüfungsnachweise berücksichtigt werden (vgl. [ISACA 2013a, 2401 Reporting]).

Der Prüfungsbericht wird nach inhaltlicher Abstimmung von der Leitung der (IT-)Revision freigegeben, an die geprüften Fachbereiche bzw. Unternehmensbereiche zur Durchsicht verteilt und bei der IT-Revision abgelegt. Eine Zusammenfassung dient zur Information des betroffenen Managements.

Von wesentlicher Bedeutung für die inhaltliche Ausgestaltung des Berichts ist, ob es sich um eine interne oder externe Prüfung handelt. Im Kontext dieses Leitfadens wird ausschließlich auf Berichte der Internen IT-Revision eingegangen.

Abschnitte des Prüfungsberichts

Einleitung

In der Einleitung sollen die Grundsätze und Aufgaben der Revision sowie eine Übersicht des angewendeten Revisionsprozesses kurz dargestellt werden. Zudem umfasst die Einleitung auch die Grundlagen der Prüfung, also alle maßgeblichen internen und externen Regelungen sowie den Prüfungsplan. In den einleitenden Abschnitten wird auch der Verteiler aufgeführt, an den der Prüfungsbericht gegeben wird.

Beschreibung der Prüfung

Die Beschreibung der Prüfung enthält detaillierte Informationen darüber, was genau geprüft wurde (Organisationsteile, Prozesse, Zeitraum, Stichproben, Dokumente, IT-Systeme), wann und wo die Prüfung durchgeführt wurde, welche Personen (Prüfende und Geprüfte) beteiligt waren, wo und welche Schwerpunkte gesetzt wurden und – soweit relevant – in welchen Bereichen und aus welchem Grund entgegen dem Prüfungsplan auf eine Prüfung verzichtet wurde.

Wichtig sind Beschreibungen der Prüfungsarten und der eingesetzten technischen und methodenbasierten Werkzeuge (bspw. Dokumentenprüfung von Vorgaben, Nachweisen und Ergebnissen, Interviews, Prüfung von Systemeinstellungen, genutzte Funktionalitäten von Revisionstools) und des Klassifizierungsschemas von Feststellungen sowie der erwarteten Maßnahmen.

Feststellungen (»Findings«)

Alle Feststellungen und Empfehlungen im Prüfungsbericht fokussieren grundsätzlich auf das angestrebte Prüfungsziel. Die Feststellungen sind genau und nachvollziehbar zu beschreiben hinsichtlich folgender Punkte:

- **Prüfungskriterium** (bindende externe Vorgaben, z.B. Gesetz oder sonstige Rechtsvorschriften, aufsichtsrechtliche Anforderungen, Normen und Standards, sonstige interne Vorgaben)
  Prüfungskriterien sind z.B. Kriterien für die Prüfung des Internen Kontrollsystems. Die als Kriterium verwandte Unterlage ist stets mit Titel, Versionsbezeichnung und Datum zu bezeichnen.
- **Vorgefundener Sachverhalt**, der am Prüfungskriterium gemessen als nicht zufriedenstellend zu bewerten ist.
- **Ursache der Abweichung** des vorgefundenen Sachverhalts vom Prüfungskriterium, soweit bekannt.
- **Auswirkung der Abweichung** (entstandener Schaden oder Risiko, wenn der Schaden noch nicht eingetreten ist)
- **Prüfungsbemerkungen** in Form bewertender Beanstandungen (bei Nichtbeachtung einer Regelung oder Fehlen einer Maßnahme des Internen Kontrollsystems) oder Empfehlungen (bei identifizierter Verbesserungsmöglichkeit einer Maßnahme des Internen Kontrollsystems)

Jede Feststellung ist risikoorientiert zu bewerten (vgl. Abschnitt 6.1). Die Feststellungen der Revision sollen grundsätzlich das Ziel (Reduktion eines konkreten Risikos) vorgeben. Sie können zudem – und dann idealerweise beispielhaft – eine Lösungsmöglichkeit vorstellen. Da Prüfungen in der Regel auf Stichproben basieren, sind bei der Beseitigung von Feststellungen eine Ursachenanalyse und umfassende, nachhaltige Lösungen zu fordern.

Ziel der Forderung einer detaillierten Ursachenanalyse ist, dass die gleichen Feststellungen und deren Ursachen in künftigen Prüfungen nicht erneut oder gar an anderer Stelle diskutiert werden müssen.

Weiteres Vorgehen

In diesem Abschnitt wird den Betroffenen erläutert, was geschehen soll, nachdem die Prüfung beendet ist. Die Verantwortlichen werden darauf hingewiesen, dass Feststellungen im Hinblick auf mögliche Ursachen zu analysieren und diese zu beseitigen sind. Je nach Schwere der Feststellungen und den damit verbundenen Risiken werden verschiedene Fristen gesetzt (vgl. Kapitel 8). Das Ergebnis der Ursachenanalyse und die Beseitigung der Abweichung/des Mangels sind angemessen zu dokumentieren. Bei schweren Mängeln wird bereits im Bericht eine ggf. geplante Nachprüfung angekündigt.

Zusammenfassung

Die Zusammenfassung ist für die Unternehmensleitung vorgesehen. Sie enthält eine Kurzfassung des Berichts mit Angaben zur durchgeführten Prüfung und dem Gesamtergebnis, ggf. verbunden mit Hinweisen auf besonders relevante Feststellungen, jedoch ohne dabei Details darzustellen. Die Zusammenfassung ist Bestandteil des Berichts, kann aber auch separat verteilt werden.

7.6 Supervisor-Aufgaben im Prüfungsprozess

Der Supervisor ist eine Rolle im Prüfungsprozess mit der Aufgabe, die Planung, Durchführung, Berichterstattung und das Nacharbeiten einer Prüfung zu überwachen. Die Rolle wird entweder von der Revisionsleitung (bzw. einem Mitglied der Revisionsleitung) oder, insbesondere in großen Revisionseinheiten, von einer von der Revisionsleitung beauftragten Person der mittleren Leitungsebene wahrgenommen. Die Überwachungsaufgabe des Supervisors erstreckt sich über den gesamten Prüfungsprozess.

In der Prüfungsvorbereitungsphase begutachtet der Supervisor zunächst das vom Prüfungsleiter entwickelte Prüfungskonzept bezüglich der darin festgelegten inhaltlichen (Risiken, Festlegung von Prüfungsschwerpunkten), personellen (qualitative und quantitative Anforderungen an die Personalausstattung des Prüfungsteams) und zeitlichen Planung. Die Kernfrage ist dabei, ob das Konzept auf das mit dem Prüfungsauftrag vorgegebene Ziel ausgerichtet ist und ob erwartet werden kann, dass dieses Ziel bei der Prüfungsdurchführung erreicht wird. Im nächsten Schritt überwacht der Supervisor, dass alle Vorgaben aus dem Prüfungskonzept vom Prüfungsleiter in das Arbeitsprogramm überführt wurden und dass das Arbeitsprogramm geeignet ist, das ausgewiesene Prüfungsziel zu erreichen. Hierzu gehören die hinreichend konkrete Benennung der Risiken sowie die Vorgabe geeigneter Prüfungshandlungen und Prüfungskriterien für die Mitglieder des Prüfungsteams. Als Abschluss der Prüfungsvorbereitungsphase gibt der Supervisor das Arbeitsprogramm für die Nutzung frei.

In der Prüfungsdurchführungsphase verfolgt der Supervisor den Fortschritt der Arbeit im Wesentlichen anhand der regelmäßigen, zumeist formlosen Berichterstattung des Prüfungsleiters. Soweit schwerwiegende Prüfungsfeststellungen zu treffen sind oder Prüfungsergebnisse einen unverzüglichen Handlungsbedarf im geprüften Bereich erkennen lassen (»Gefahr im Verzug«), informiert der Prüfungsleiter den Supervisor zeitnah und berät mit ihm das weitere Vorgehen. Sofern bei der Prüfungsdurchführung Schwierigkeiten oder Verzögerungen auftreten, unterstützt der Supervisor den Prüfungsleiter, beispielsweise durch die Zuweisung zusätzlichen Personals, die Verlängerung der Prüfungsdurchführungszeit oder durch die Genehmigung einer vom Prüfungsleiter vorgeschlagenen Anpassung bzw. Kürzung des Arbeitsprogramms. Außerdem kann der Supervisor am Informationsgespräch teilnehmen, das der Prüfungsleiter üblicherweise zum Abschluss der Erhebungen vor Ort mit der Leitung des geprüften Bereichs durchführt.

In der Berichterstattungsphase besteht die Aufgabe des Supervisors darin, die Qualitätssicherung für die Ergebnisdokumentation im Arbeitsprogramm und für den Prüfungsbericht durchzuführen.

Zu den Nacharbeiten einer Prüfung (vgl. Kapitel 8) gehören zunächst die Zusammenstellung der Prüfungsakte durch den Prüfungsleiter und später insbesondere das Follow-up, d.h. die Überwachung der Erledigung der Prüfungsbemerkungen. Für diese Tätigkeiten ist der Prüfungsleiter zuständig und der Supervisor führt die Qualitätssicherung durch, d.h., er kontrolliert die Ordnungsmäßigkeit der Prüfungsakte und überprüft die Angemessenheit der Bewertung der Follow-up-Maßnahmen des geprüften Bereichs durch den Prüfungsleiter.

Zusammenfassend ist somit festzuhalten, dass die – grundsätzlich zu den Leitungsaufgaben der Revision gehörende – Supervisor-Aufgabe im Wesentlichen aus einer Reihe von qualitätssichernden Tätigkeiten bezogen auf die Aktivitäten des Prüfungsleiters im Prüfungsprozess sowie aus der Unterstützung des Prüfungsleiters in kritischen Situationen besteht.

Hinweis auf IT-Prüfungsstandard (ITAF):

Anforderungen an das Follow-up sind im IT-Prüfungsstandard »1402 – Nachschau« der ISACA (vgl. Abschnitt 3.1.2) definiert.

8. Follow-up

Mit der Übergabe des Abschlussberichts und den darin enthaltenen Feststellungen und Empfehlungen ist die Prüfung noch nicht beendet. Der Zweck einer Prüfung ist erst erreicht, wenn die im Rahmen der vorausgehenden Abstimmung des Prüfungsberichts mit den geprüften Bereichen vereinbarten Maßnahmen zur Behandlung aufgedeckter IT-Risiken nachvollziehbar umgesetzt worden sind. Erst dann kann davon ausgegangen werden, dass die Mängel beseitigt wurden. Je nach Art und Grad eines Mangels und dem damit verbundenen Risiko können die Auflagen und die Fristen zur Umsetzung unterschiedlich ausfallen. In der Regel werden diese Fristen von den Prüfern in Abstimmung mit den geprüften Bereichen oder durch Auflagen einer externen Zertifizierungsstelle festgelegt.

Die Verantwortung für die zeitnahe und wirksame Reaktion auf alle Prüfungsfeststellungen liegt stets bei den Prozessverantwortlichen oder der Unternehmensleitung (im Fall der Bereitstellung notwendiger Ressourcen) und niemals bei der IT-Revision selbst.

Eine Feststellung, die einen wesentlichen oder höher eingestuften Mangel beschreibt, der dazu führt, dass ein wichtiger Prozess überhaupt nicht oder nicht korrekt bzw. nur unvollständig ablaufen kann oder dass beispielsweise gesetzliche Vorschriften verletzt werden, muss umgehend, also ohne schuldhafte Verzögerung durch die Betroffenen, beseitigt werden. Die Fristen liegen hier im Allgemeinen im Tages- bzw. Wochenbereich. Die wirksame Beseitigung dieser Mängel ist von dem Fachbereich gegenüber der Revision nachzuweisen und ggf. in einer Nachprüfung durch die Revision zu überprüfen.

Die Beseitigung eines als geringfügig eingestuften Mangels, der etwa die Dokumentation eines Prozesses oder eines IT-Systems betrifft, sollte vom Prozesseigentümer in die üblichen Planungsprozesse aufgenommen werden. Das Ergebnis kann im Rahmen einer rollierenden Prüfungsplanung für den nächsten Revisionszyklus (in der Regel innerhalb eines Jahres) vorgemerkt und dann nochmals geprüft werden.

Zur Beseitigung eines Mangels sind vom Prozesseigentümer eine Ursachenanalyse durchzuführen und ein Maßnahmenplan zu erstellen. Beides muss dokumentiert und im Rahmen der **Maßnahmenverfolgung** der IT-Revision zu dem von ihr genannten Termin vorgelegt werden (vgl. dazu auch den Punkt »Weiteres Vorgehen« in Abschnitt 7.5.2). Sie überprüft die Plausibilität der Analyseergebnisse und Eignung der Gegenmaßnahmen für ausgewählte (i.d.R. wesentliche oder höher bewertete) Mängel und bestätigt die erfolgreiche Beseitigung bzw. weist auf weiterhin bestehende IT-Risiken hin.

Bei längerfristigen Aktivitäten sollte eine regelmäßige Statusüberprüfung durch die Prozesseigentümer stattfinden. Die IT-Revision hat dabei darauf zu achten, dass die Maßnahmen zum Ziel führen und geeignet sind, die Mängel wirksam, umfassend und nachhaltig zu beseitigen. Dies ist durch den geprüften Bereich auch nachzuweisen.

Praxishinweis
Sonderfall Risikoübernahme

Für die Risiken in den Prozessen und deren Behandlung ist zunächst der jeweilige Prozesseigner verantwortlich. Möglicherweise lässt sich ein Risiko aus Sicht der betroffenen Prozesseigner aber überhaupt nicht, nicht in angemessener Frist, nicht auf geeignete Weise oder nur mit unverhältnismäßigem Aufwand reduzieren oder beseitigen. In einem solchen Fall wird dieses Risiko gemäß ISO 31000 und ISO/IEC 2700x als **Restrisiko** (Residual Risk) bezeichnet.

Dieses Restrisiko hat der Prozesseigner im Rahmen der **Risikoübernahme** der Unternehmensleitung zur Genehmigung vorzulegen.

Sofern die Revision bei einer Prüfung also ein Risiko feststellt, das nicht oder nicht mit vertretbarem Aufwand behandelt werden kann, sollte sie in einer Prüfungsbemerkung dem Prozesseigner je nach Kritikalität auferlegen oder empfehlen, die direkten Verantwortlichen und stets auch die Unternehmensleitung zeitnah über dieses Restrisiko und seine möglichen Auswirkungen umfassend zu unterrichten. In der Regel werden zeitgleich geeignete Ersatzmaßnahmen vereinbart.

Stimmt die Unternehmensleitung der Risikoübernahme zu (retain the risk by informed choice), muss dies anschließend explizit nachgewiesen werden können. Die Risikoübernahme muss von der Unternehmensleitung ausgehen und **ausschließlich** in schriftlicher Form erfolgen.

Bei Risiken aufgrund von Verstößen gegen gesetzliche Vorschriften ist dieses Vorgehen unzulässig.

Je nach Organisationsform der IT-Revision erfolgt das Follow-up (Nachverfolgung/die Überwachung der Erledigung der Prüfungsbemerkungen)

- begleitend zur Umsetzung,
- zum Fälligkeitstermin der jeweiligen Maßnahme,
- gebündelt zu festen Terminen (z.B. quartalsweise) oder
- im Rahmen von Folgeprüfungen oder speziellen Nachschauprüfungen.

Abhängig von der Gewichtung der Feststellung (und somit von dem damit verbundenen IT-Risiko) kann die Prüfung der Beseitigung eines Mangels materiell oder auf Basis einer Mitteilung erfolgen. Bei einer Nachschau der Beseitigung des Mangels führt der Prüfer gegebenenfalls weitere Prüfungshandlungen durch, um sich zu vergewissern, dass das IT-Risiko, das der Feststellung zugrunde liegt, durch entsprechende Maßnahmen tatsächlich reduziert wurde.

9. Qualitätssicherung: Prüfung der IT-Revision und ihrer Prozesse

Ist die IT-Revision im Unternehmen etabliert, ist es hilfreich, auch sie einer regelmäßigen Überprüfung zu unterziehen, um ihre Wirksamkeit, Effizienz und die kontinuierliche Verbesserung der Revisionsfunktion und ihrer Prozesse einzuschätzen und zu fördern.

Eine solche Prüfung betrachtet die aufbau- und ablauforganisatorischen Aspekte (Organisationsstruktur und Revisionsprozesse) sowie die Qualität der Ergebnisse des IT-Revisionsprozesses. Die Qualitätssicherung der IT-Revisionsfunktion beinhaltet eine Validierung sowie Verifizierung aller ihrer Elemente und beurteilt sie hinsichtlich ihrer Angemessenheit und Wirksamkeit. Meist werden mit dieser Qualitätssicherung entweder unabhängige und sachkundige Dritte beauftragt oder unparteiische interne Sachverständige mit Prüfungshintergrund aus anderen Unternehmensbereichen.

Praxishinweis
Standards zur Prüfung der IT-Revision

Im Rahmen der ständigen Qualitätssicherung und -verbesserung können genutzt werden:

- QAR-IT (ISACA Germany Chapter) – *www.isaca.de*
- DIIR-Prüfungsstandard 3 – *www.diir.de*
- IDW PS 321 – IDW-Verlag

Zusätzlich kann es lohnend sein, sich begleitend inhaltlich und methodisch mit

- COBIT 5 for Assurance (ISACA) – *www.isaca.org*

sowie

- DIN EN ISO 19011 – Leitfaden zur Auditierung von Managementsystemen (ISO 19011 Guidelines for auditing management systems)

zu befassen.

Das Ziel ist es wie bei jeder anderen Prüfung auch, durch sorgfältige, systematische und unabhängige Analyse sowie Nutzung geeigneter Qualitätssicherungsstandards und Prüfungsmethoden eventuell vorhandene Schwächen in der Gestaltung oder Ausführung der IT-Revisionsfunktion zu identifizieren und die daraus resultierenden Folgen zu beurteilen. Dies soll die kontinuierliche Verbesserung des IT-Prüfungsprozesses sicherstellen.

Dabei sinkt die Wahrscheinlichkeit, im Rahmen einer solchen Qualitätssicherung Schwachstellen zu finden, wenn zwischen den offiziellen Qualitätssicherungs-Audits eine kontinuierliche Überprüfung der eigenen Strukturen und Prozesse durch die IT-Revision selbst erfolgt (sog. Self-Assessment).

Als Hilfsmittel für Prüfung und Verbesserung der IT-Revisionsfunktion können verschiedene Standards herangezogen werden.

Ausblick auf COBIT 5 for Assurance

Die ISACA-Publikation »COBIT 5 for Assurance« baut auf dem COBIT-5-Rahmenwerk auf und ist auf Assurance fokussiert. Sie zeigt, wie COBIT 5 zur Unterstützung von IT-Assurance-Aktivitäten eingesetzt werden kann. Dieser Leitfaden soll die effiziente und effektive Entwicklung von IT-Assurance-Initiativen auf der Basis eines allgemein akzeptierten Assurance-Ansatzes ermöglichen. »COBIT 5 for Assurance« kann in Unternehmen aller Größen implementiert werden und richtet sich explizit nicht nur an große Organisationen. Die Publikation adressiert folgende Fragen bzw. Themen in Bezug auf IT-Assurance/IT-Prüfung:

- Was ist Assurance?
- In welchem Zusammenhang stehen die COBIT-5-Enabler zu dem Assurance-Prozess?
- Wie kann eine effiziente Assurance-Funktion aufgebaut und aufrechterhalten werden?
- Wie kann COBIT 5 bei der Durchführung des Assurance-Prozesses unterstützen?
- Wie sieht das COBIT-5-basierte Prüfungs-/Assurance-Programm aus (inklusive Beispiele)?
- Ist COBIT 5 mit gängigen Assurance-Standards verknüpft?

Die Publikation besteht aus drei Hauptkapiteln (vgl. [ISACA 2013b]):

- Kapitel 1 fokussiert auf das Thema »Assurance« und beschreibt, wie COBIT-5-Prinzipien auf Assurance-spezifische Anforderungen angewendet werden. Dieses Kapitel bietet die konzeptuelle Basis für die gesamte Publikation.
- Kapitel 2A fokussiert auf den Einsatz der COBIT-5-Enabler für die Governance und das Management der Assu-

rance-Funktion. Im Kapitel 2B wird gezeigt, wie Assurance der COBIT-5-Enabler erreicht werden kann.
- Im Kapitel 3 wird die Beziehung von COBIT 5 zu anderen Prüfungsstandards und -praktiken diskutiert.

»COBIT 5 for Assurance« baut zwar auf der Hauptpublikation COBIT 5 auf, erfordert jedoch nicht unbedingt Kenntnisse über die Hauptpublikation, denn die Schlüsselaspekte der COBIT-5-Publikation werden in »COBIT 5 for Assurance« wiederholt. Das Verständnis der COBIT-5-Hauptpublikation auf Basisniveau ist allerdings hilfreich für das bessere Verständnis von »COBIT 5 for Assurance« (vgl. [ISACA 2013b]).

Eine Assurance-Initiative besteht laut COBIT 5 aus den folgenden fünf Komponenten (vgl. [Fröhlich et al. 2007a, S. 10] und [ISACA 2013b]):

1. Definierte Beziehung zwischen drei Parteien:
   - dem für das Assurance-Objekt Verantwortlichen
   - dem Assurance-Geber
   - den an dem Assurance-Ergebnis interessierten Parteien
2. Spezifiziertes Assurance-Objekt
3. Kriterien, denen das Assurance-Objekt genügen muss und die von allen Parteien akzeptiert werden
4. Definierter Assurance-Prozess
5. Beurteilung, ob die Kriterien durch das Beurteilungsobjekt erfüllt werden

COBIT 5 basiert auf fünf Prinzipien. »COBIT 5 for Assurance« knüpft an diese Prinzipien an und verwendet sie Assurance-bezogen. Unterschiedliche Anspruchsgruppen können dabei voneinander abweichende Anforderungen an Assurance stellen. Aus diesem Grund gibt es mehrere Typen von Assurance-Projekten: externe, interne bzw. Compliance-Prüfungen oder Self-Assessments. Die genannten Assurance-Typen unterscheiden sich durch den Regulierungs- bzw. Standardisierungsgrad. Self-Assessments sind weniger reguliert bzw. standardisiert als interne und Compliance-Prüfungen. Den höchsten Regulierungs- und Standardisierungsgrad weisen demnach externe Prüfungen auf.

Anspruchsgruppen für Assurance können sein:

- Intern: Vorstand (Board Committee), Prüfungsausschuss, Prüfungs-, Risiko- und Compliance-Gruppen, Unternehmensleitung
- Extern: Anteilseigner/Investoren, externe Prüfer, Staat, Geschäftspartner; Kunden

Abkürzungsverzeichnis

ACL	Access Control List / Audit Command Language
AG	Aktiengesellschaft
ANSI	American National Standards Institute
AO	Abgabenordnung
AT	Attestation Standard
BCM	Business Continuity Management
BCP	Business Continuity Plan
BDSG	Bundesdatenschutzgesetz
BI	Business Intelligence
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAAT	Computer Assisted/Aided Auditing Techniques
CFE	Certified Financial Engineer/Certified Fraud Examinator
CGEIT	Certified in the Governance of Enterprise IT
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISM	Certified Information Systems Manager
CISSP	Certified Information Systems Security Professional
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRISC	Certified in Risk and Information Systems Control
DIIR	Deutsches Institut für Interne Revision e.V.
DNS	Domain Name System
DRP	Disaster Recovery Plan
EnWG	Energiewirtschaftsgesetz
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
GmbH	Gesellschaft mit beschränkter Haftung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GOBS	Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
ICIF	Internal Control – Integrated Framework
IDEA	Interactive Data Entry and Access
IDW	Institut der Deutschen Wirtschaftsprüfer e.V.
IEC	International Electrotechnical Commission
IIA	Institute of Internal Auditors
IKS	Internes Kontrollsystem
IP	Internet Protocol
IPPF	International Professional Practices Framework
ISACA	Information Systems Audit and Control Association
ISAE	International Standard of Assurance Engagements
ISMS	Informationssicherheits-Managementsystem
ISO	International Standardization Organization
IT	Informationstechnologie
IT-IKS	Internes Kontrollsystem in der IT
IT-SiG	IT-Sicherheitsgesetz
ITAF	IT Audit and Assurance Framework
ITGI	IT Governance Institute
ITIL	IT Infrastructure Library
KG	Kommanditgesellschaft
KWG	Kreditwesengesetz
LA	Lead Auditor
MaRisk	Mindestanforderungen an das Risikomanagement
NPO	Non-Profit Organization
OHG	Offene Handelsgesellschaft
OpRisk	Operationelle Risiken
PCI DSS	Payment Card Industry Data Security Standard
PLZ	Postleitzahl
PS	Prüfungsstandard
QAR-IT	Quality Assurance Review IT
QMB	Qualitätsmanagementbeauftragter
RZ	Rechenzentrum
SOX	Sarbanes-Oxley Act
SPICE	Software Process Improvement and Capability Determination
SQL	Structured Query Language
SSAE	Statement on Standards for Attestation Engagement
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TOGAF	The Open Group Architecture Framework
VoIP	Voice over IP

Abbildungsverzeichnis

Tabellenverzeichnis

Quellenverzeichnis

[Amling/Bantleon 2015] Amling, T.; Bantleon, U.: Handbuch der Internen Revision: Grundlagen, Standards, Berufsstand. 2. Aufl., Erich Schmidt, 2015.

[Auf der Heyde/Hahn 2014] Auf der Heyde, D.; Hahn, U.: Das überarbeitete ISACA IS Audit & Assurance Framework. IT-Governance 8 (2014), 19, S. 4-8.

[Cascarino 2012] Cascarino, R. E.: Auditor´s Guide to IT Auditing. 2. Aufl., John Wiley & Sons, Hoboken, New York, 2012.

[Eulerich 2012] Eulerich, M.: Das »Three Lines of Defense«-Modell. ZIR – Zeitschrift Interne Revision 47 (2012), 2, S. 55-58.

[Fochler et al. 2013] Fochler, K.; Schmidt, A.-H.; Paffrath, R.: IT-Revision 3.0 – Herausforderungen für die Interne IT-Revision. HMD – Praxis der Wirtschafsinformatik 50 (2013), 289, S. 20-30.

[Fröhlich/Swart 2013] Fröhlich, M.; Swart, C.: IT-Prüfung aus Sicht der Wirtschaftsprüfung. IT-Governance 7 (2013), 15, S. 5-11.

[Fröhlich et al. 2007a] Fröhlich, M.; Glasner, K.; Goeken, M.; Johannsen, W.: Sichten der IT-Governance. IT-Governance 1 (2007), 1, S. 3-8.

[Fröhlich et al. 2007b] Fröhlich, M.; Johannsen, W.; Wilop, K.: IT-Assurance mit COBIT. IT-Governance 1 (2007), 2, S. 10-16.

[IDW PS 330] IDW: PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie. IDW Verlag, Düsseldorf, 2002.

[ISACA 2012] ISACA: COBIT 5. 1. Aufl., Rolling Meadows, 2012.

[ISACA 2013a] ISACA: ISACA-Prüfungsstandards, 2013; *http://www.isaca.org*.

[ISACA 2013b] ISACA: COBIT 5 for Assurance. 1. Aufl., Rolling Meadows, 2013.

[Johannsen/Goeken 2011] Johannsen, W.; Goeken, M.: Referenzmodelle für IT-Governance. 2. Aufl., dpunkt.verlag, Heidelberg, 2010.

[Ruud/Kyburz 2014] Ruud, T. F.; Kyburz, A.: Gedanken zum Three Lines of Defense Modell – Was ist mit Verteidigung gemeint? Analyse des Governance-Modells aus der Sicht des Internen Audits. Der Schweizer Treuhänder 88 (2014), 9, S. 761-766.

[Rüter et al. 2010] Rüter, A.; Schröder, J.; Goldner, A.; Niebuhr, J.: IT-Governance in der Praxis. Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen. 2. Aufl., Springer-Verlag, Berlin, Heidelberg, 2010.

[Schmidt/Brand 2011] Schmidt, K.; Brand, D.: IT-Revision in der Praxis. Hanser, 2011.

Zeitschriften

ZIR – Zeitschrift Interne Revision, E. Schmidt, Berlin

Revisionspraxis PRev – Journal für Revisoren, Wirtschaftsprüfer, IT-Sicherheits- und Datenschutzbeauftragte, Richard Boorberg Verlag, Stuttgart

ISACA Journal, Bezug einzeln oder im Rahmen der Mitgliedschaft über *www.isaca.org*

IT-Governance – Fachzeitschrift des ISACA Germany Chapter e.V., dpunkt.verlag, Heidelberg

Onlinequellen

www.isaca.de – ISACA Germany Chapter e. V.

www.isaca.org – ISACA International

Glossar

Control

Unter Controls (wörtlich: »Kontrollen«, Maßnahmen) werden nach ISACA und IIA alle Steuerungs- und Überwachungsmaßnahmen innerhalb des Internen Kontrollsystems (IKS, mit den beiden Teilen Steuerungs- und Überwachungssystem) verstanden. Da ein Control auch nicht kontrollierende Eigenschaften besitzen kann, ist die Verwendung des Begriffs »Kontrolle« jedoch möglicherweise missverständlich und aus diesem Grund in Anführungszeichen gesetzt.

Für den Begriff Control werden häufig weitere Synonyme verwendet, etwa Countermeasure (ISACA), Kontrollmechanismus (GoBS) und Kontrollmaßnahme (GoBS, IDW). Die Begriffe »Kontrolle« und Maßnahme werden auch in den GoBS, den GoBD, vom DIIR und vom IDW genutzt.

Wichtige Begriffe im Prüfungskontext sind im ISACA-Glossar *(www.isaca.com/glossary)* sowie in den ISO-Normen hinterlegt. Das Englisch-Deutsch-Glossary (Stand Juli 2015) ist unter *http://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-German_mis_Ger_0715.pdf* verfügbar.

INHALTE DES STUDIENGANGS

- Grundlagen IT-Audit & Assurance
- IT-Audit, Systematik und Durchführung
- IT Risiko-Management
- Business Continuity Management
- Informationssicherheit
- IT-Compliance-Management
- Business Communication
- IT-Fraud, Forensics & Investigation
- IT-Projekt- und Qualitätsmanagement
- IT-Service Management
- Neuere Entwicklungen in IT-Audit & Assurance
- IT-Auditing im internationalen Umfeld

IT-AUDIT & ASSURANCE

BERUFSBEGLEITENDER MASTER OF SCIENCE

DATEN UND FAKTEN

Dozenten

Erfahrene Mitglieder der Fachgruppe „Akademische Aus- und Weiterbildung" von ISACA® Germany Chapter e.V.

Struktur

4 Semester + Master Thesis, berufsbegleitend, Blockmodell

Studienort

Europäische Fachhochschule Brühl

Abschluss

Master of Science (M.Sc.) IT-Audit & Assurance, 120 Credits

Studiengebühren

545 €/Monat + 300 Verwaltungsgebühr + 1500 Masterthesis

EU FH EUROPÄISCHE FACHHOCHSCHULE

Kontakt: studienberatung@eufh.de

WWW.EUFH.DE

DAGSA

Deutsche Akademie für
IT-Governance, IT-Security und IT-Audit

Beratung und Anmeldung zu den Seminaren unter **www.dagsa.eu**

Informieren Sie sich über unser vielfältiges Seminarprogramm

- Vorbereitungskurse auf die CISA- und CISM-Prüfungen
- Zertifikatskurse zum IT-Security Information Practitioner, Cyber Security Practitioner, ...
- Weiterbildungskurse im Bereich IT-Revision, COBIT, IT-Compliance, ...

Weitere Informationen finden Sie unter www.dagsa.eu

Die Akademie für IT-Governance, IT-Security und IT-Audit (DAGSA) ist eine Kooperation der Quadriga Akademie Berlin GmbH und dem ISACA Germany Chapter e. V.

DAGSA
Deutsche Akademie für
IT-Governance, IT-Security und IT-Audit

ISACA
Trust in, and value from, information systems
Germany Chapter