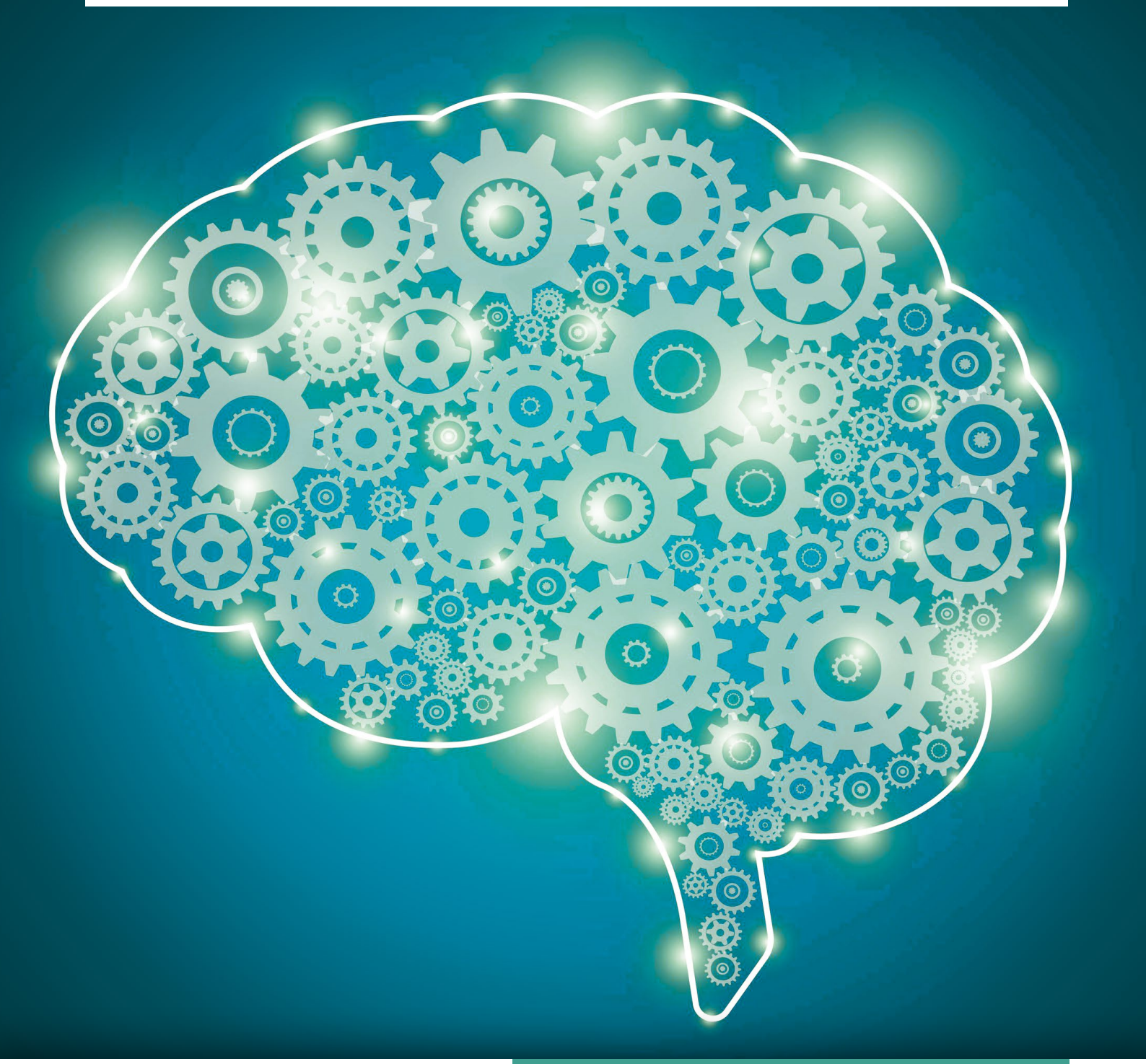
Eine Veröffentlichung des ISACA Germany Chapter e.V.
Fachgruppe IT-Revision



2., aktualisierte und überarbeitete Auflage

Grundlagen der IT-Revision für den Einstieg in die Praxis

ISACA
Germany Chapter

dpunkt.verlag

Herausgeber:

ISACA Germany Chapter e.V.
Storkower Straße 158
10407 Berlin

www.isaca.de
info@isaca.de

ISACA-Fachgruppe IT-Revision (Autoren)

Autorenteam

- Dr. Karlheinz Ahlers, CISA, 1. und 2. Auflage
- Markus Bank, CISA, 1. und 2. Auflage
- Axel Dors, CISA, 1. und 2. Auflage
- Torsten Enk, CISA, CDPSE, 1. und 2. Auflage
- Sebastian Grüneberg, CISA, CISM, 2. Auflage
- Jochen Hartmann, CISA, CISM, 1. Auflage
- Ralf Herter, 1. und 2. Auflage
- Ingrid Dubois, 1. Auflage
- Prof. Matthias Knoll, CISA, 1. und 2. Auflage
- Christian Lossos, 2. Auflage
- Wolf-Rüdiger Mertens, CIA, CISA, CISSP, 1. und 2. Auflage
- Torsten Meyer, CISA, 1. und 2. Auflage
- Patrick Schwieder, 2. Auflage
- Stefanie Schmidt, CIA, CISA, 2. Auflage
- Simon Scribelka, CISA, 2. Auflage
- Dr. Dirk Silkenbäumer, CISA, 2. Auflage

Vorstand

- Dr. Tim Sattler (Präsident)
- Thomas O. Englerth (Vizepräsident – Zertifizierungen)
- Dr. Martin Fröhlich (Vizepräsident – Finanzen und Verwaltung)
- Markus Gaulke (Vizepräsident – Weiterbildung)
- Prof. Dr. Matthias Goeken (Vizepräsident – Veröffentlichungen)
- Julia Hermann (Vizepräsidentin – Kommunikation und Marketing)
- Matthias Kraft (Vizepräsident – Fachgruppen)

Stand: September 2022 (Final nach Review und Überarbeitung durch ISACA-Fachgruppe IT-Revision)

ISACA-Leitfaden

Grundlagen der IT-Revision für den Einstieg in die Praxis

2., überarbeitete und aktualisierte Auflage

ISACA
Germany Chapter

Vorwort zur 2. Auflage

Sechs Jahre sind in der IT eine sehr lange Zeit. Vorgaben haben sich geändert, neue Themen sind hinzugekommen, die Digitalisierung ist in vielen Bereichen rasch vorangeschritten. Und nicht zuletzt hat auch die Corona-Pandemie für die IT-Revision viele neue Fragen aufgeworfen. Die Bedeutung der IT-Revision in den Unternehmen nimmt also weiterhin stark zu.

Der Anspruch des Autorenteams der ISACA-Fachgruppe IT-Revision war es daher, den vorliegenden Leitfaden hinsichtlich der Änderungen bei wichtigen Vorgaben, aber auch bei Veränderungen in den Grundlagen zu aktualisieren und anzupassen.

Selbstverständlich kann jedoch auch diese Aktualisierung keinen Anspruch auf Vollständigkeit erheben. Wir bitten daher auch in dieser Auflage um Ihr Feedback, 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:
fg-it-revision@isaca.de

Die Autoren
Frankfurt, im Juli 2022

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung genderspezifischer Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Vorwort zur 1. Auflage

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 von 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:
fg-it-revision@isaca.de

Die Autoren
Frankfurt, im Juli 2016

Inhaltsverzeichnis

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

In den letzten Jahren stieg die Abhängigkeit von der Informationstechnologie bei praktisch allen Unternehmen unabhängig von Branchenzugehörigkeit und Unternehmensgröße stark an, erkennbar etwa an[1] der steigenden Anzahl der Projekte und der immer größer werdenden Budgets für die IT. Dieser Trend wird sich in der erst am Anfang stehenden digitalen Transformation noch weiter verstärken.

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

Von der zunehmenden Digitalisierung und den damit verbundenen Änderungen in den Geschäftsmodellen besonders betroffen ist etwa der Finanzdienstleistungsbereich, das gesamte Gesundheitswesen (»elektronische Gesundheitskarte«, »E-Rezept«), die Energiewirtschaft (»Smart Grid«) und die Telekommunikationsbranche. Aber auch die Logistikbranche, der Maschinen- und Anlagenbau (Stichworte: »Industrial Control Systems«, »Internet der Dinge«, »Cyber-physische Systeme«) und viele andere Bereiche erfahren nicht zuletzt durch den Einsatz »intelligenter« Sensorik und Aktorik, künstlicher Intelligenz sowie Cloud-Nutzung mit immer neuen »As-a-Service«-Modellen weitreichende Veränderungen. Bereits heute sind zahlreiche Geschäftsmodelle ohne IT nicht mehr umsetzbar, etwa Multimedia/Streaming-Dienste wie Netflix oder Spotify, soziale Netzwerke, etwa Facebook, das neue Metaverse, Instagram und TikTok, Vermittler-Plattformen, wie Uber oder airbnb, oder der gesamte Onlinehandel. Parallel dazu entstehen durch Hinzufügen von IT zu etablierten Produkten und Geschäftsmodellen vollkommen neue Konstruktionen. Die Informationstechnologie dient damit oftmals einerseits der Prozessunterstützung und ist andererseits auch 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 Risiken.

Die aufgrund der hohen IT-Durchdringung zunehmend komplexen regulatorischen, fachlichen oder durch den Markt bestimmten Rahmenbedingungen erfordern daher eine sehr sorgfältige Begleitung durch die IT-Revision, um Lücken und Schwächen des Internen Kontrollsystems[2] sowie Haftungsrisiken für die Unternehmensleitung frühzeitig erkennen und minimieren oder vermeiden zu können.

Viele Vorstände und Geschäftsführer fürchten neben persönlicher Haftung, etwa im Kontext des Ordnungswidrigkeitengesetzes (OWiG) durch ein nicht angemessenes IKS, und finanziellen Verlusten nichts mehr als einen Vertrauensverlust bei Kunden und einen Imageverlust in der Öffentlichkeit. Denn technische Störungen oder fehlerhaft konzipierte, implementierte (Hard- und Softwarefehler, »Bugs«) oder konfigurierte Elemente in der IT können beispielsweise Unbefugten sensible Daten in die Hände spielen. Durch solche Schwachstellen besteht zudem die Möglichkeit, relevante Daten unbemerkt zu verändern oder bewusst zu manipulieren. Auch können aus einer Vielzahl von Gründen die für einen

1 Hinweise darauf lassen sich in verschiedenen Statistiken und Studien zu IT-Budgets, IT-Kosten und IT-Projekten finden, die im Statistik-Portal statista veröf-fentlicht worden sind *(de.statista.com)*.

2 Zum Internen Kontrollsystem vgl. [Bungartz 2017]. In diesem Leitfaden wird »Internes Kontrollsystem« großgeschrieben, vielfach wird jedoch auch »internes Kontrollsystem« verwendet. In Literatur und Praxis findet sich dazu keine einheitliche Regelung, beide Schreibweisen sind daher zulässig.

Prozess oder ein bestimmtes Produkt notwendigen IT-Anwendungen nicht oder nur eingeschränkt verfügbar sein. Die drei klassischen Schutzziele der Informationssicherheit Vertraulichkeit, Integrität und Verfügbarkeit sind dadurch nicht mehr gewährleistet.

Neben gezielten Angriffen und technischen Problemen, die oft zitiert werden, gelten leider häufig auch das Personal und externe Dienstleister im Umgang mit IT-Anwendungen als Ursprung von Störungen oder Ausfällen. Die Awareness für Risiken bei Einsatz und Nutzung von IT, präzise formulierte und »gelebte« Vorgaben, aber auch die Notwendigkeit von IT-Prüfungen werden daher 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 aller Aktivitäten, Informationssicherheit und Business Continuity zu gewährleisten und alle damit verbundenen direkten und indirekten fachlichen Anforderungen abzudecken. Die IT-Revision unterstützt diese Bemühungen mit Blick auf das Business-IT-Alignment unmittelbar und im Idealfall laufend, etwa durch projektbegleitende Prüfungen. Dabei nutzt sie einen angemessenen und wirksamen IT-Revisionsprozess bei gleichzeitiger Wahrung ihrer Unabhängigkeit. Als dritte Linie im Drei-Linien-Modell liefert die Revision ihre Ergebnisse aus den Revisionsprozessen nicht nur ausschließlich für die erste Linie. Es werden wertvolle Informationen auch an die in der zweiten Linie angesiedelten zentralen Funktionen wie Risikomanagement, Informationssicherheit oder Compliance weitergeleitet[3].

3 Zur Theorie des Drei-Linien-Modells siehe Exkurs zur Abgrenzung der Revision im nachfolgenden Abschnitt.

2 Grundlagen: Begriffe und Definitionen

Jedes Unternehmen verfügt über mehr oder weniger stark standardisierte oder individuell entwickelte IT-Systeme bzw. Anwendungen. Entsprechend heterogen sind die IT- und Anwendungslandschaften, 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 den Aufbau des Informationssystems als Gegenstand von IT-Prüfungen sowie in der IT-Revision gebräuchliche Begriffe. Sie enthalten zudem 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 damit 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, Systemsoftware (Betriebssystem, Middleware und hardwarenahe Softwareelemente, etwa Firmware) sowie Anwendungssoftware. 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/konfigurierte) Anwendungen bzw. Services. Eingeschlossen in die Betrachtungen sind hierbei wegen der fortschreitenden Digitalisierung dieser Bereiche zunehmend auch Maschinen- und Anlagensteuerungen für die vernetzte Fertigung im Industrie-4.0-Umfeld bzw. für Aufgaben in kritischen Infrastrukturen. In Anlehnung an COBIT 2019 (vgl. [ISACA 2019, Abschnitt 4.3, S. 21]) stellt ein IT-System damit die »Components« »Services, Infrastructure and Applications« im Sinne des serviceorientierten Paradigmas zur Verfügung. Es ist jedoch nicht ausreichend, ausschließlich eher technische Aspekte der Informationsverarbeitung mithilfe eines IT-Systems zu betrachten. Es ist vielmehr notwendig, grundsätzlich alle sieben in COBIT 2019 definierten »Components« zu betrachten (vgl. [ISACA 2019, Abschnitt 4.3, S. 21]):

1. Prozesse (Processes)
2. Organisationsstrukturen (Organizational structures)
3. Prinzipien, Richtlinien und Rahmenwerke (Principles, policies and frameworks)
4. Information (Information)
5. Kultur, Ethik und Verhalten (Culture, ethics and behaviour)
6. Mitarbeiter, Fähigkeiten und Kompetenzen (People, skills and competencies)
7. Services, Infrastruktur und Anwendungen (Services, infrastructure and applications)

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** – Component »Infrastructure«
- **Software** (hardwarenahe Software, etwa Firmware, Betriebssystem und Middleware, etwa Dienste, wie Active Directory o.Ä., Verschlüsselung, Berechtigungs- sowie Identity- und Access-Management), Datenbanken und alle fachlichen und technischen Anwendungen – Components »Services« und »Applications«

- **Netzwerk** (Datenübertragung, Schnittstellen) – Component »Infrastructure«
- **Personal** (Fachbereich und IT) – Components »People«, »Skills« und »Competencies«
- **Prozesse** (technische und fachliche, hierzu zählen auch alle **Projekte**) – Component »Processes«
- **Daten** (Stamm-/Bewegungsdaten, Datenqualität, Klassifikation – Schutzbedarf) – Component »Information«
- **Organisatorische Regelungen** (ergänzend zu den Prozessen/Projekten) – Component »Organizational Structures«

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. 9. Aufl., Wiesbaden, 2017.

Krcmar, H.: Informationsmanagement. 6. Aufl., Berlin, Heidelberg, 2015.

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

Tiemeyer, E.: Handbuch IT-Management: Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis. 7. Aufl., München, 2020.

2.2 Der Risikobegriff

Gute Revisionsarbeit folgt dem risikoorientierten Prüfungsansatz (vgl. Kapitel 5 und Abschnitt 6.2). Gleichzeitig überwacht die Revision die Arbeit des Risikomanagements (vgl. Folgeabschnitt). Der Risikobegriff nimmt daher in der Arbeit der Revision eine zentrale Stellung ein und soll aus diesem Grund kurz definiert werden.

Organisationen sind permanent verschiedensten externen als auch internen Risiken ausgesetzt und stehen deshalb in der Verantwortung, entsprechende Vorkehrungen zum Umgang mit Risiken zu treffen. Ein fortlaufend betriebenes Risikomanagement unterstützt sie dabei. Es gewährleistet innerhalb der Organisation, dass alle Beteiligten die Verantwortung für einen professionellen Umgang mit Risiken übernehmen.

Der Risikobegriff ist in Wissenschaft und Praxis auf unterschiedliche Weise definiert. Die allgemeinste Definition liefert der ISO/IEC Guide 73:2009, dem auch die ISACA in ihrem Glossar folgt[1]. Dort sind Risiken als »The combination of the probability of an event and its consequence« definiert.

Allen Definitionen gemeinsam ist auch die Einordnung des Risikos als Maß für Wagnis einerseits und Unsicherheit andererseits. So beschreibt die ISO 31000:2018 als zentrale internationale Norm für das Risikomanagement in Abschnitt 3.1 (Risiko) das Risiko als die Auswirkung von Ungewissheit auf ein erwartetes Ziel. Die Norm merkt dabei an, dass eine Abweichung positiv und/oder negativ ausfallen kann. Entsprechend können daraus sowohl Chancen (Gewinne, Nutzen) als auch Schäden (Verluste, Misserfolge) resultieren. Daran anknüpfend beschreibt die Norm, dass Risiken gewöhnlich auf Basis ihrer jeweiligen Risikoquelle (Ursache) sowie den potenziellen Folgen (Wirkung) ausgedrückt werden.

Als Maßstab zur Analyse und Bewertung von Risiken können ihre jeweilige Eintrittswahrscheinlichkeit sowie die potenziellen Auswirkungen – als Funktion oder Kombination von Eintrittswahrscheinlichkeit und Auswirkungen, nicht als einfaches mathematisches Produkt – herangezogen werden[2]. Diese Form der Risikobewertung wird in der Praxis häufig in Form von (relativ aufwendigen) Risikoszenarien sowie unter Nutzung komplexer mathematischer Modelle, aber auch einfacher, überblicksartiger Risikomatrizen vorgenommen, sodass schließlich eine Gesamtbewertung der unternehmensindividuellen Risiken erfolgen kann.

Bezogen auf Risiken im Kontext von Informationssystemen (vgl. Abschnitt 2.1) wird häufig definiert, dass eine bestimmte interne oder externe Bedrohung eine Schwachstelle in einem beliebigen Element (Asset) des Informationssystems oder in einer Gruppe dieser Assets ausnutzt und dadurch einen Schaden in der Organisation verursacht. Dieser Sicht folgt auch die Definition der Fachgruppe »Risikomanagement« des ISACA Germany Chapter[3]. Um genauer differenzieren zu können, wird zudem häufig unterschieden zwischen eher technisch geprägten Risiken und eher inhaltlich begründeten Informationssicherheitsrisiken. Auch aus diesem Grund verwendet dieser Leitfaden den zusammenfassenden neutralen Begriff »Risiko«.

2.3 Das Drei-Linien-Modell

Bei der Umsetzung einer systematischen und einheitlichen Vorgehensweise für Organisationen im Umgang mit Risiken kann das 2013 erstmals vom IIA als Three-Lines-of-

1 Vgl. ISACA-Glossar, *https://www.isaca.org/resources/glossary#glossr.*

2 Weitere Informationen zur Risikoanalyse in der online verfügbaren IT-Grundschutz-Schulung des BSI: *https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/it-grundschutzschulung_node.html.*

3 ISACA-Leitfaden »Risikomanagement«, *https://www.isaca.de/sites/default/files/attachements/2012-isaca-leitfaden-it-risikomanagement_0.pdf.*

Defense veröffentlichte und 2020 aktualisierte Three-Lines-Modell (Drei-Linien-Modell, Abbildung 2–1) wirkungsvoll unterstützen. Ein Ziel des Drei-Linien-Modells besteht darin, Strukturen und Prozesse zu identifizieren und zu etablieren, die helfen, Risiken frühzeitig zu identifizieren, zu analysieren und zu bewerten sowie in der Organisation zu kommunizieren, um bei Bedarf entsprechende Gegenmaßnahmen zu implementieren (der »Verteidigungscharakter«). Gleichzeitig soll das Modell die Unternehmenswerte schützen und aktiv dabei unterstützen, die Unternehmensziele zu erreichen (der »Schutz- und Werterhaltungscharakter«).

Beide Aspekte werden durch die Etablierung von mehreren Linien umgesetzt, die in verschiedenen Ebenen der Aufbauorganisation abgebildet werden. Dabei kann das Drei-Linien-Modell grundsätzlich branchen-, struktur- sowie größenunabhängig eingesetzt werden.

2.3.1 Erste Linie: operatives Management

Innerhalb der ersten Linie werden Risiken identifiziert, bewertet und abgeschwächt, indem Maßnahmen durch Vorgaben und Prozesse entwickelt und implementiert werden. Zudem liegt innerhalb der Linie die Verantwortung zur Gewährleistung, dass sämtliche Aktivitäten in Einklang mit den unternehmerischen Zielen und Vorgaben stehen. Sie stellt damit einen grundlegenden Bestandteil jeder Organisation dar.

2.3.2 Zweite Linie: Überwachung und Steuerung

In der zweiten Linie erfolgt eine Überwachung und Unterstützung der ersten Linie durch das unternehmensweite Risikomanagement (Enterprise Risk Management, ERM) sowie die Compliance-Funktionen. Zum unternehmensweiten Risikomanagement, das IT-Risikomanagement einschließt, gehören Tätigkeiten zur Erkennung, Analyse, Bewertung, Behandlung und Kontrolle von Risiken. Die zweite Linie ist dabei schwer-

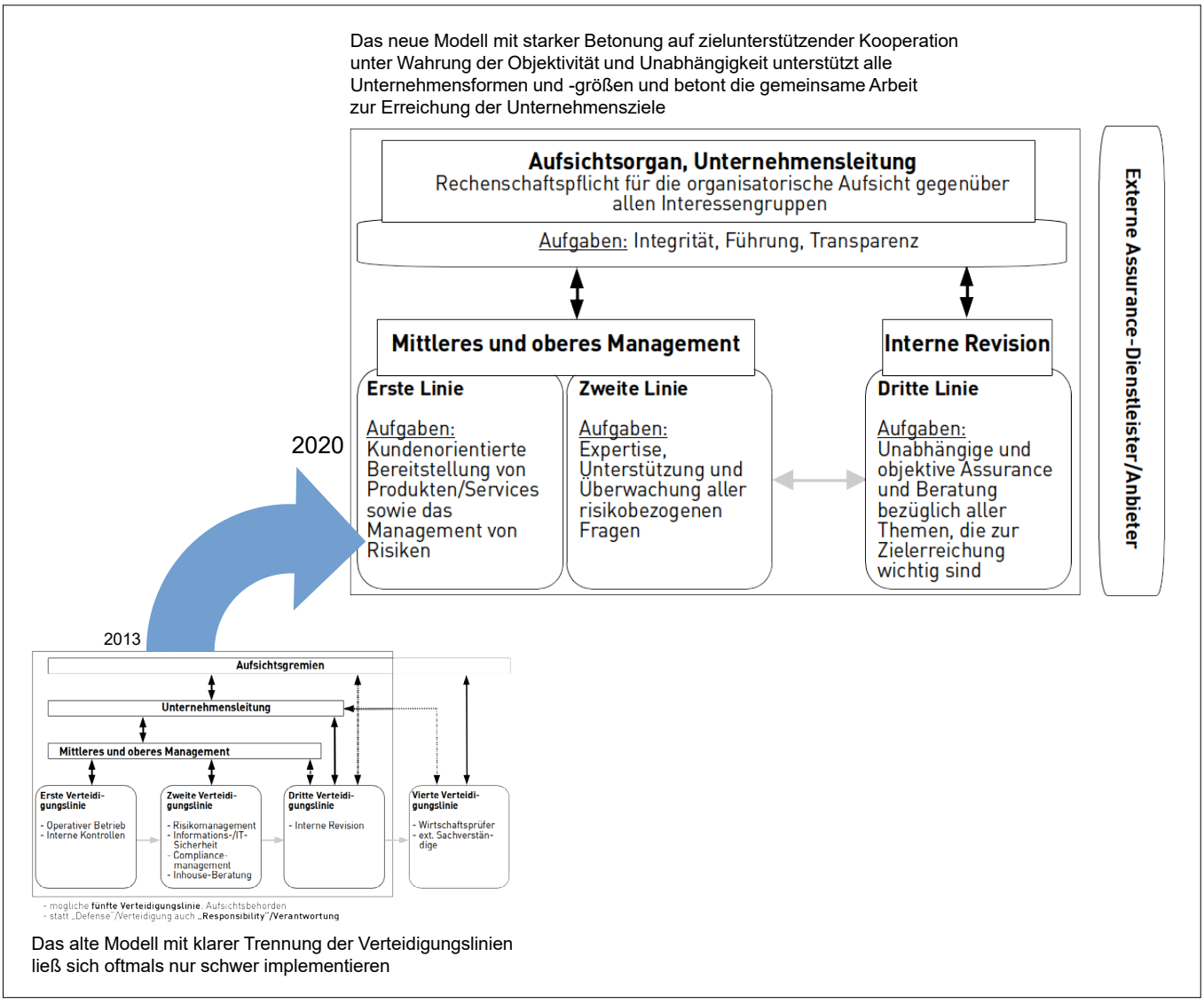


Abbildung 2–1: Das Drei-Linien-Modell in alter und aktualisierter Fassung zur Verdeutlichung der Neuerungen (siehe auch Abschnitt 2.3.5)[4]

punktmäßig methodisch tätig und entwirft Vorgaben für die Anwendung des Risikomanagements und seiner Werkzeuge in der ersten Linie. Revision, Risikomanagement und Compliance sind dabei nicht voneinander abhängig. Vielmehr muss insbesondere 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. Das Risikomanagement überwacht damit die Umsetzung von Risikomaßnahmen des operativen Managements und unterstützt die dortigen Verantwortlichen bei der Identifikation von Risiken und der Implementierung geeigneter Maßnahmen zur Behandlung von Risiken.

Dies umfasst auch die Kontrolle von finanziellen Risiken und die Finanzberichterstattung gegenüber externen Regulatoren wie beispielsweise Finanzbehörden sowie die Kontrolle der Einhaltung von fachspezifischen Vorgaben, beispielsweise im Kontext des Gesundheits- und Umweltschutzes.

Exkurs
Weitere betriebliche Funktionen der zweiten Linie

Informations-/IT-Sicherheit
Die Informationssicherheit befasst sich – aufgrund der hohen Bedeutung der IT-Funktion für die Unternehmen – mit allen Aspekten der Sicherheit von Informationen (Daten) und eingesetzten IT-Systemen (Definition siehe Abschnitt 2.1). Dabei werden alle Elemente des Informationssystems (siehe Abschnitt 2.1) einbezogen. Die im Rahmen der Informationssicherheit behandelten Aspekte umfassen nicht nur technische, sondern auch organisatorische und soziologische Themen, etwa den Aufbau von Awareness und einer Fehlerkultur oder die Beherrschung von Social-Engineering-Gefahren.

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

Qualitätsmanagement
Das Qualitätsmanagement ist integraler Bestandteil eines Unternehmens. Es ist auch in der IT auf die Wirksamkeit der Prozesse hinsichtlich Zielerreichung, Effektivität und Effizienz ausgerichtet. 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 die Entwicklung und Umsetzung von IT-Strategien, die Gestaltung von IT-Prozessen, IT-Architekturen und die Evaluation von Technologien. Sie kann auch konkrete Implementierungsunterstützung leisten.

2.3.3 Dritte Linie: unabhängige und objektive Prüfung

Obwohl durch die zweite Linie bereits Überwachungsfunktionen der operativen Kontrollen durchgeführt werden, besteht gegenüber den überwachenden Bereichen keine vollständige Unabhängigkeit. Daher verfügt das Drei-Linien-Modell über eine dritte Linie, die die Aktivitäten der ersten und zweiten Linie unabhängig und objektiv prüft (Assurance-Gedanke).

Die Interne Revision (vgl. nachfolgenden Abschnitt 2.4) unterstützt die Unternehmensführung, ggf. den Aufsichtsrat, in der Überwachung der Wirksamkeit von Governance, Risikomanagement und dem Internen Kontrollsystem.

2.3.4 Externe Akteure: Wirtschaftsprüfung, externe Prüfer und Aufsichtsbehörden

Außerhalb des betreffenden Unternehmens leisten externe Akteure ihren Beitrag zur Umsetzung des Drei-Linien-Modells. Dies geschieht beispielsweise im Rahmen von Prüfungen der drei Linien durch Wirtschaftsprüfungsgesellschaften. Besonders risikoreiche oder komplexe fachliche und technische Aspekte innerhalb einer Linie können zudem durch spezialisierte Prüfungsgesellschaften untersucht werden. Auch Aufsichtsbehörden können Prüfungen durchführen. Dies geschieht häufig in stark regulierten Branchen wie der Finanzdienstleistungsbranche. Aber auch im Rahmen bestimmter Zertifizierungsprozesse (etwa ISO 9000, ISO 27000) werden Maßnahmen in den Linien geprüft. Denn alle externen, insbesondere zusätzlichen Prüfungen geben den Stakeholdern des Unternehmens weitere Gewissheit über die Ordnungsmäßigkeit von Strukturen und Prozessen. Je nach Aufbau und Umsetzung des Risikomanagements eines Unternehmens können sowohl externe Prüfungen als auch Aufsichtsbehörden daher als zusätzliche vierte und fünfte Linie definiert werden.

2.3.5 Neuerungen in der Weiterentwicklung des Modells

In der Praxis sind die drei Linien nicht klar abgegrenzt. Zum einen können Funktionen der ersten Linie auch Vorgaben

4 Siehe hierzu das IIA-Dokument zum neuen Three-Lines-Modell (Juli 2020) unter *https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf* sowie die deutsche Übersetzung des DIIR unter *https://www.diir.de/fileadmin/fachwissen/downloads/Three-Lines-Model-Updated-German.PDF.*

zur Risikobeherrschung für andere Funktionen erlassen und dann auch überwachen (z. B. Beschaffungsrichtlinien durch eine zentrale Einkaufsabteilung), zum anderen können Funktionen der zweiten Linie in Projekten der ersten Linie eingebunden sein. Je nach Branche und/oder organisatorischer Aufstellung sowie Größe des Unternehmens können auch Teile der Revision als dritte Linie unter Wahrung ihrer Unabhängigkeit beratend und ohne dabei eine Entscheidungs- bzw. Umsetzungsverantwortung zu übernehmen, in der ersten und zweiten Linie mitwirken. Insgesamt ist eine stärkere Kommunikation und Zusammenarbeit zwischen den Linien wahrnehmbar und wird auch explizit gewünscht.

Diese in der Praxis häufig fehlende klare Abgrenzung der Linien bzw. der Wunsch nach verbesserter Unterstützung durch das Modell bei der Erreichung der Unternehmensziele trug mit zu einer Überarbeitung des Modells unter Berücksichtigung dieser Sachverhalte bei. Als wesentliche Änderung gilt die Integration eines auf sechs Prinzipien basierenden Ansatzes:

1. **Governance**: Es existieren klare Regelungen für die Gesamtübersicht über die Organisation (Integrität, Führung, Transparenz) einschließlich zentraler Strukturen und Prozesse (**Accountability**). Dies schließt auch Maßnahmen beim Management (**Actions**) sowie Überwachung und Beratung durch eine unabhängige interne Prüfungsfunktion ein (**Assurance & Advice**).
2. **Rollen der Leitungsorgane**: Die Leitungsorgane stellen klare Strukturen und Prozesse sicher und sorgen dafür, dass Verantwortung zugewiesen ist und Ressourcen für die Umsetzung notwendiger Maßnahmen verfügbar sind. Alle Ziele und Maßnahmen orientieren sich an den Stakeholder-Interessen. Zudem sorgt das Leitungsgremium für die Einrichtung einer unabhängigen internen Audit-Funktion.
3. **Management-Rollen und Rollen der ersten und zweiten Linie**: Die Rollen in der ersten und zweiten Linie können separiert oder in verschiedener Ausprägung zusammengefasst sein. Die Verantwortung für Risiken verbleibt jedoch grundsätzlich in der ersten Linie.
4. **Rollen der dritten Linie**: Für die unabhängige und objektive Tätigkeit der dritten Linie kann weitere interne oder externe Sachkunde herangezogen werden.
5. **Unabhängigkeit der dritten Linie**: Das schließt auch einen objektiven, unvoreingenommenen Blick sowie den ungehinderten Zugang zu Daten und Personen ein.
6. **Werte schaffen und erhalten**: Nur durch Zusammenarbeit, interdisziplinäres Denken und gemeinsam erzielte Ergebnisse können Werte nachhaltig generiert und erhalten werden.

In ihrer Gesamtheit heben die Prinzipien nicht mehr auf die vormals eher betonte Trennung der Linien, sondern vielmehr auf ein gemeinschaftliches, zielorientiertes, kooperatives und transparentes Miteinander ab. Damit erfüllt das Modell unter Berücksichtigung der Unabhängigkeit der Revisionsfunktion einerseits nach wie vor eine Überwachungsaufgabe, stärkt jedoch gleichzeitig die Bündelung der unterschiedlichen Kenntnisse, Erfahrungen und Fähigkeiten im Unternehmen für eine bestmögliche Zielerreichung und Risikobeherrschung.

2.4 Die Revision

2.4.1 Definition

Zu unterscheiden sind externe und Interne Revision. Die wesentlichen Unterschiede liegen dabei in der organisatorischen Zuordnung, den jeweils hauptsächlich maßgeblichen Prüfungsgrundlagen sowie in der Zielsetzung der Prüfungen.

Gemäß § 316 und § 319 Abs. 1 HGB hat der Abschlussprüfer in seiner Funktion als **externer Revisor** einen gesetzlichen Prüfungsauftrag. Neben der Richtigkeit und Ordnungsmäßigkeit des Jahresabschlusses werden auch die Angemessenheit und Wirksamkeit des Internen Kontrollsystems unter Anwendung der entsprechenden Verlautbarungen des IDW geprüft[5]. Darüber hinaus prüfen Wirtschaftsprüfungsgesellschaften sowie andere Prüfungsgesellschaften

- im Auftrag des Aufsichtsorgans des Unternehmens oder auf Anordnung von Behörden im Rahmen einer Vielzahl von (Sonder-)Prüfungen,
- im Auftrag der Unternehmensleitung oder der Aufsichtsorgane eines Unternehmens im Kontext der Zertifizierung der Internen Revision sowie
- im Auftrag der Internen Revision als Unterstützung im Kontext von Prüfungen mit einem bestimmten inhaltlichen Schwerpunkt oder bei Ressourcenengpässen der Internen Revision.

Für die externe Revision können – abhängig von den Gegebenheiten – zusätzliche Definitionen und Regelungen sowie ein spezielles, durch nationale und internationale Gesetzgebung stark beeinflusstes Rahmenwerk aus Prüfungsstandards als Prüfungsgrundlage gelten. Die damit verbundenen Aspekte sollen hier nicht weiter betrachtet werden. Ist die externe Revision jedoch unterstützend und beratend tätig, greift sie im Rahmen der Ausführung ihrer prüferischen Tätigkeiten in gleicher Weise wie die Interne Revision auf die Ergebnisse aus Normungsgremien (beispielsweise ISO) und Berufsverbänden (DIIR/IIA, ISACA) zurück (vgl. Kapitel 3).

Die **Interne Revision** (fortan Revision) kann aus aufbau- und ablauforganisatorischer Sicht betrachtet werden. Aus aufbauorganisatorischer Sicht ist die Revision ein mit der Durchführung von Prüfungsaufgaben befasstes Element der Gesamtorganisation, etwa eine funktional angeordnete Abteilung oder eine Stabsfunktion. Die Revision ist in der Regel der

5 Eine Übersicht aller Verlautbarungen (insbesondere Prüfungsstandards und Prüfungshinweise) ist unter *https://www.idw.de/idw/verlautbarungen* zu finden.

Unternehmensleitung direkt unterstellt und berichtet vorrangig an diese, in speziellen Fällen auch an das Aufsichtsorgan oder einen in seinem Auftrag eingesetzten Prüfungsausschuss (Audit Committee).

Aus ablauforganisatorischer Sicht führt die Revision im Rahmen von Prozessen und den darin enthaltenen Aktivitäten Prüfungen mit eigenem, unabhängigem Personal unter Rückgriff auf verschiedene Ressourcen durch.

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 im 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. Auch die Vorgehensweise der Revision kann durch entsprechende gesetzliche oder berufsständische Vorgaben festgelegt sein (vgl. Kapitel 3). In allen anderen Fällen orientiert sich die Revision primär an Unternehmensrichtlinien und externen Best Practices.

Neben der vorrangigen Unterstützung der Unternehmensleitung und der Kontrollorgane unterstützt die Revision durch Weitergabe der Revisionsergebnisse wie oben dargestellt auch die Managementebene in den geprüften Fachbereichen oder Projekten und damit indirekt das gesamte Unternehmen. Denn die Managementebene ist, letztlich für die Umsetzung der Revisionsempfehlungen verantwortlich.

Im Vordergrund der prüferischen Tätigkeiten stehen dabei (vgl. bereits [Hofmann 1972, S. 13ff.] sowie [Knapp 2009, S. 39, 44ff.]):

- Umfang, Angemessenheit und Wirksamkeit des Internen Kontrollsystems,
- die Zuverlässigkeit und Vollständigkeit aller Daten des Rechnungswesens und weiterer betriebswichtiger Daten anderer zentraler Funktionen,
- die Prüfung/Einschätzung der effizienten Implementierung und Ausführung aller Geschäftsprozesse sowie
- das Erreichen einer bestimmten Prozessleistung bzw. eines Leistungsniveaus (etwa in der Sicherheit oder Verfügbarkeit) und damit der angestrebten Prozessziele sowie die Sicherung des Betriebsvermögens und der Betriebskontinuität.

In jüngster Zeit spielen oft auch Nachhaltigkeitsfragen (z. B. Umwelt, Ressourceneinsatz) und Fragen der Unternehmensethik eine immer wichtigere Rolle. Gleichzeitig grenzt sich die Revision als dritte Linie des Drei-Linien-Modells im Sinne einer Aufgabentrennung (Segregation of Duty) und zur Wahrung der Unabhängigkeit gegen andere betriebliche Funktionsbereiche ab, insbesondere gegen das Risikomanagement, das Controlling und das Qualitätsmanagement (zweite Linie), aber auch gegen weitere, eher operative Funktionen wie die zunehmend bedeutsamere Informationssicherheit und gegen eher strategisch ausgerichtete Funktionen wie die innerbetriebliche Beratung. Sie unterstützt niemals direkt bei der Umsetzung von betrieblichen Zielen und Vorhaben, etwa Projekten, und ist damit nicht direkt an den Wertschöpfungsprozessen beteiligt. Dadurch ist die Unabhängigkeit der Revisionsfunktion stets sichergestellt.

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

Definition »IT-Revision«

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

Die IT-Revision deckt in ihren Prüfungen – aus funktioneller Sicht – den gesamten IT-Lebenszyklus ab. Er umfasst in Anlehnung an die CISA-Examens-Domains 2, 3 und 4 die Entwicklung/Konzeption (Information Systems Development), die Beschaffung (Information Systems Acquisition), die Implementierung/das Change Management (Information Systems Implementation), den Betrieb einschließlich Support (Information Systems Operation, Information Systems Support), die Wartung (Information Systems Maintenance) und die Außerbetriebnahme sowie das Management der IT (ganzheitliches Servicemanagement, etwa im Sinne von ITIL 4). Eingeschlossen sind auch alle Trends wie beispielsweise agiles Arbeiten, DevOps und DevSecOps sowie NoOps (Fußnote: eine mögliche Definition der drei Begriffe findet sich unter anderem unter *www.dev-insider.de*).

Zu den Aufgaben zählt auch eine Prüfung des Informationssicherheits-Managementsystems (ISMS). Auch wenn diese Form von Prüfungen mitunter als **IS-Revision** bezeichnet wird, ist sie doch **Bestandteil der IT-Revision**.

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 (englisch 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[6]:

»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 einerseits ideell (»Management Commitment«) unterstützt. Andererseits soll sie die Revision mit entsprechenden Vollmachten sowie angemessenen Sach- und Personalmitteln zur Prüfung ausstatten, insbesondere vor dem Hintergrund eines durch die zunehmende IT-Abhängigkeit stetig wachsenden Aufgabenumfangs.

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

Eine weitere wichtige Voraussetzung für eine erfolgreiche Revisionsarbeit ist zudem die »richtige« 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 auch für Nicht-IT-Fachleute 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 geschehen. Vergleichbares gilt für die Kommunikation mit den geprüften 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 selbst verbietet sich mit Ausnahme bei sogenannten 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]).
- **Eigenverantwortlicher Betrieb von zu prüfenden Anwendungen**
  Fachbereiche betreiben selbst teilweise zahlreiche und überaus komplexe Anwendungen (sog. »Schatten-IT«, »End-User-Computing«, »Individuelle Datenverarbeitung«), etwa Excel-Anwendungen oder direkt bezogene Cloud-Services. 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 seine zugehörigen Anwendungen verantwortlichen Leitungspersonal[7]. Eine Prüfung durch eigenes Personal wäre also nicht unabhängig, eine objektive Berichterstattung gegenüber der Unternehmens- und Fachbereichsleitung kann so nicht gewährleistet werden.

Sonderfall IT-Outsourcing

Eine Sonderstellung in der Arbeit der IT-Revision mit Blick auf die prüferischen Möglichkeiten und Spielräume nimmt das IT-Outsourcing ein. Unter IT-Outsourcing werden alle Formen der Auslagerung der IT an ein darauf spezialisiertes Unternehmen zusammengefasst, darunter auch Cloud Computing. Nicht immer besteht daher die Möglichkeit, Prüfungen selbst durchzuführen.

6 Deutsches Institut für Interne Revision e.V. (DIIR), laut Beschluss des DIIR-Vorstandes vom 07. Juni 2002. Im englischsprachigen Original der IIA: »Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.« Vgl. für die deutsche Übersetzung durch das DIIR den DIIR-Prüfungsstandard 3, Abschnitt 3.1, die Empfehlungen zur (Neu-)Einrichtung einer Internen Revision, *https://www.diir.de/fileadmin/fachwissen/diir_veroeffentlichungen/DIIR_Fachbeitrag_Nr._1_Empfehlungen_zur__Neu-_Einrichtung_einer_Internen_Revision.pdf* sowie das Online-Revisionshandbuch für die Interne Revision in Kreditinstituten, *https://www.diir.de/fileadmin/fachwissen/revisionshandbuch-marisk.pdf*. Vgl. zusätzlich auch [Berwanger/Kullmann 2012].

7 Als weitere Begründung kann auch IDW PS 261.RS FAIT 1, Tz. 8 herangezogen werden, nach dem 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.

IT-Outsourcing kann sich auf einzelne oder alle Elemente von Informationssystemen (siehe Abschnitt 2.1) und alle damit realisierbaren Geschäftsprozesse sowie Prozesse im Kontext der Supply Chain sowie auf weitere IT-Dienstleistungen wie beispielsweise Security Services, Entsorgung von Medien/Datenträgern und Webdienste beziehen. Im Kontext der aktuellen Cloud-Diskussion ist dabei insbesondere der Auslagerungsort sowie Fragen der Vertraulichkeit (Nutzung von Verschlüsselung) und Verfügbarkeit 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[8]. Die IT-Revision ist daher dafür verantwortlich, zu prüfen, ob die ausgelagerten Tätigkeiten mindestens die Anforderungen erfüllen, 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[9]. Im Idealfall soll ein solches Prüfungsrecht erwirkt werden, oder es sollten neutrale Dritte mit einer IT-Prüfung beauftragt werden können. Dieser Aspekt wird aktuell intensiv diskutiert, weil eine Vielzahl von Unternehmen auf Cloud-Services einiger weniger großer Anbieter mit Hyperscale-Infrastrukturen[10] zurückgreifen, die aufgrund ihrer Marktmacht eine Durchsetzung des Prüfungsrechts für einzelne Unternehmen erschweren. Häufig wird deshalb etwa eine gemeinsam durchgeführte Prüfung (Joint Audit) erwogen. Für solche gemeinsamen Prüfungen hat sich die Collaborative Cloud Audit Group (CCAG) gegründet, in der Finanzdienstleister mit Sitz in der EU Mitglied werden können.

Ein Verweis des Outsourcing-Anbieters auf entsprechende Prüfungsbescheinigungen (IDW PS 951, AT 801/SSAE 16 und ISAE 3402) ist vielfach also nicht aussagekräftig genug. Vielmehr müssen zumindest die Prüfungsberichte vorgelegt werden, wobei der Detaillierungsgrad des Berichts vertraglich vereinbart werden sollte. Im Idealfall lässt sich zwischen den Outsourcing-Partnern vereinbaren, zusätzlich die für den individuellen Outsourcing-Fall zutreffenden wichtigsten Prüfungsunterlagen für eine Einsichtnahme zur Verfügung zu stellen. Auch Vor-Ort-Besuche sind statthaft und je nach Kritikalität und Komplexität der Prozesse, der Bedeutung eines Produktes und/oder spezieller IT-gestützter Funktionen empfehlenswert. Auch hier ist es jedoch insbesondere bei Anbietern von Hyperscale Computing üblich, dass nicht die prüfenden Unternehmen, sondern die Geprüften entsprechende Vorgaben für die Prüfungsdurchführung formulieren, die zu befolgen sind.

Inwieweit Abhängigkeiten, die sich aus der Inanspruchnahme bestimmter Cloud-Leistungen möglicherweise ergeben, selbst ein besonderes Risiko für das Unternehmen nicht nur aus technischer Sicht darstellen und wie im Unternehmen darauf reagiert wird, sollte von der IT-Revision ebenfalls mit betrachtet und dokumentiert werden, um entsprechende Maßnahmen zur Risikobeherrschung (weiter-)entwickeln zu können.

2.4.2 Zielsetzung

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 zu verbessern hilft[11].

Zu den Unternehmenszielen mit Bezug zur IT gehören in Anlehnung an COSO ERM 2017[12] insbesondere:

- Vermeidung von Verstößen gegen Gesetze und andere Regelungen, die durch fehlerhafte IT entstehen, aber auch durch gezielten Einsatz von IT zur Identifikation solcher Verstöße einschließlich Beweissicherung
- 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
- Einrichtung und Betrieb eines wirksamen Internen Kontrollsystems in der IT

Oberstes Ziel der IT-Revision ist es also, im Auftrag der Unternehmensleitung eine **Prüfungsfunktion** für alle IT-relevanten Themen in allen Bereichen des Unternehmens abhängig von deren jeweiligem Risikogehalt (Kritikalität für den betrachteten Geschäftsprozess/Geschäftserfolg) zu überneh-

8 Dieser Grundsatz leitet sich für rechnungslegungsrelevante Systeme oder deren IT-Infrastruktur aus IDW RS FAIT 1 sowie den GoBD Rz. 11 ab, für Systeme mit personenbezogenen Daten zusätzlich aus BDSG §11.

9 Vgl. speziell für Kreditinstitute etwa die MaRisk AT 9 7.b und c, BAIT Modul 8 und die EBA-Guideline 2019/02 zu Auslagerungen. Vergleichbare Regelungen existieren auch für Versicherungen (VAIT) und Kapitalverwaltungsgesellschaften (KAIT).

10 Vgl. zum Begriff *https://en.wikipedia.org/wiki/Hyperscale_computing.*

11 Vgl. DIIR-Revisionsstandard NR. 3, Abschnitt 3.1 sowie *https://www.diir.de/fachwissen/revisionshandbuch-marisk.*

12 Vgl. COSO: Enterprise Risk Management Integrating with Strategy and Performance, *https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.*

men und über die Revisionsergebnisse zur Verbesserung der Aufbau- und Ablauforganisation (Prozesse) beizutragen (vgl. [Schmidt/Brand 2011, S. 4-7]).

Die Aufgaben der IT-Revision entsprechen den Aufgaben der Internen Revision[13], ergänzt um den Bezug zur IT (vgl. [Fochler et al. 2013, S. 20], allgemeine Definition (siehe vorausgehenden Abschnitt):

- Prüfung der Einhaltung aller unternehmensexterner und -interner 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 durchaus sinnvoll und wichtig, obwohl sie unter Unabhängigkeitsgesichtspunkten mitunter kontrovers diskutiert wird. Welcher Weg dabei der richtige ist, ist oftmals nicht leicht zu beantworten. Statt einer pauschalen Antwort erscheinen folgende Kriterien als Orientierungshilfe sinnvoll:

- 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.
- Es erfolgt eine klare organisatorische Trennung von Beratung und Prüfung.
- Es gibt einen zeitlichen Abstand zwischen der letzten Beratung und der nächsten Prüfung im betreffenden Sachgebiet, da bei der Prüfung die Neutralität gewahrt bleiben muss.
- Abstraktheit der Empfehlungen: Je methodischer die Beratung, desto geringer ist die Gefahr des Verlustes der Unabhängigkeit.
- Alle Beratungsvorgänge und deren Ergebnisse werden vollständig und verständlich dokumentiert.

Wichtig sind zudem ein einheitliches Verständnis der Aufgaben der IT-Revision im gesamten Unternehmen, das überall umfassend kommuniziert wird, sowie klar definierte und dokumentierte Prozesse für die Arbeit der IT-Revision, die in dieser Form auch tatsächlich angewandt werden.

2.4.3 Nutzen

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 der IT-Prozesse und ihrer beteiligten fachlichen und technischen Ressourcen, die immer kürzeren Entwicklungszyklen, der Einsatz neuartiger Vorgehensmodelle in Entwicklung und Betrieb sowie die stetig wachsende 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 Risiken (die auch IT- und Informationssicherheitsrisiken umfassen, vgl. Abschnitt 2.2) 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 aussagekräftige Berichte zu einer Prüfung, auf deren Grundlage etwa:

- die Initiierung eines Projektes zur Abschaltung eines teuren und schwer zu betreuenden Altsystems (sog. Legacy System) erfolgt,
- die zusätzliche und sinnvolle Aus- und Fortbildung von Mitarbeitern in sensiblen oder wissensintensiven Bereichen gefördert wird,
- die Wartbarkeit von Eigenentwicklungen, gerade auch bei Anwendung neuartiger Vorgehensmodelle (agil, DevOps) erhöht wird,
- die IT-Sicherheit erhöht wird, was daran erkennbar ist, dass die Anzahl und die Schwere der sicherheitsrelevanten Vorfälle (Security Incidents) durch das Etablieren einer zusätzlichen Kontrollinstanz in der zweiten Linie des Drei-Linien-Modells sinkt, sowie
- die Einhaltung von externen Compliance-Vorschriften sichergestellt wird, 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

13 Vgl. DIIR-Revisionsstandard Nr. 3, Abschnitt 3.2.

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.

2.5 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.

2.5.1 Audit-Charta

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

Hinweis auf das IT Audit and Assurance Framework (ITAF 4)

Anforderungen an die Audit-Charta sind in den IT-Prüfungsstandards »General Standard 1001 – Audit Charter« sowie »General Guidelines 2001: Audit Charter« der ISACA (vgl. Abschnitte 3.1.2 und 3.1.3) definiert.

2.5.2 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 die für Prüfungen relevanten IT-Kontrollziele ableiten. Darauf aufbauend muss die IT-Revision zu den IT-Kontrollzielen diejenigen Risiken identifizieren, die die Erreichung der Kontrollziele gefährden. Mit den erzielten Ergebnissen und unter Berücksichtigung der Prüfungsziele kann nun die Prüfungsstrategie so gestaltet werden, dass spätere Prüfungshandlungen fundierte Aussagen ermöglichen. Auf dieser Basis kann dann geprüft werden, ob geeignete Maßnahmen identifiziert wurden, um diesen Risiken angemessen zu begegnen. Zur Orientierung kann beispielsweise das Ergebnis der vorangegangenen Prüfung herangezogen werden.

Im Rahmen der Entwicklung einer Prüfungsstrategie müssen bei der Beurteilung von inhärenten Risiken schließlich folgende Ursachen für das Entstehen von Risiken in Betracht gezogen werden:

- Zunehmende Abhängigkeit aller Bereiche im Unternehmen von der IT, insbesondere auch von Cloud-Lösungen
- Größere Änderungsprojekte in der IT, die durch die Einführung neuer IT-Systeme und Technologien (etwa KI), aber auch durch die Einführung neuer oder durch Anpassung bestehender Anwendungen oder durch Cloud-Migrationsstrategien bedingt sein können
- Fehlende Ressourcen führen zu Überlastungen in der IT und im Fachbereich
- Unsicherheit oder Unvermögen im Kontext steigender Komplexität der Fragestellungen
- Unzureichende Qualifikation und Weiterbildung
- Unzureichende Pflege (bspw. Einspielen von funktionalen und Sicherheits-Updates, Anpassung wichtiger Parameter) und Fehlbedienung der IT-Systeme/Anwendungen aufgrund von unzureichendem Know-how oder fehlender Zeit
- Mangelhafte Ausrichtung der IT auf Geschäftsstrategien und Prozessanforderungen (unzureichendes Business-IT-Alignment)
- Bei länderübergreifender Organisation und Aufgabenverteilung in der IT: Sprachprobleme und kulturelle Unterschiede
- Zunehmende Regulierung (bspw. DSGVO, GoBD, IT-SiG, EnWG)
- Zunehmende Bedrohungen von außen (wachsende Cyberkriminalität)

Weitere Faktoren, die bei der Formulierung 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). Dies ist insbesondere dann wichtig und herausfordernd, wenn neue Projektmanagement- und Entwicklungsansätze, wie etwa Agile Development oder DevOps-/NoOps-Konzepte, eingesetzt werden (sollen).

2.5.3 Prüfungsuniversum und Prüfungsobjekte

Das Prüfungsuniversum (engl. Audit Universe), die **Gesamtheit aller Prüfungsobjekte**, ist die Basis der Prüfungsplanung. ISACA definiert das Prüfungsuniversum als »an inventory of audit areas that is compiled and maintained to identify areas for audit during the audit planning process«.[14] Das Prüfungsuniversum muss regelmäßig aktualisiert werden, um Änderungen im Gesamtrisikoprofil des Unternehmens korrekt widerzuspiegeln. Es sollte **alle** Bereiche des Unternehmens abdecken und keinen »prüfungsfreien Raum« lassen.

Das Prüfungsuniversum ist hierarchisch strukturiert:

1. Ebene: **Prüfungsgebiete** – Mithilfe der Prüfungsgebiete werden die Prüfungsfelder strukturiert.
2. Ebene: **Prüfungsfelder** – Sie 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 Prüfungsuniversums sein oder auch nicht.
3. Ebene: **Teilprüfungsfelder** – Sie fassen zur besseren Übersicht verschiedene Prozesse zu Prozessgruppen zusammen.
4. Ebene: **Prüfungsobjekte** – Sie umfassen IT-Prozesse und zugehörige Ressourcen sowie Fachprozesse und zugehörige Ressourcen (IT-Systeme, Anwendungen). Aus einer risikoorientierten Betrachtung der Prüfungsobjekte folgen die Prüfungsaspekte (vgl. Abschnitt 2.5.5).

Die **Prüfungsobjekte** müssen alle wesentlichen Prozesse und Wertschöpfungsketten umfassen[15], 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[16]:

- 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 Suppliers 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 und Anwendungen, dies können u.a. jahresabschlussrelevante Systeme (wie etwa ERP-Systeme) sowie alle für den Betrieb unverzichtbaren Systeme (einschließlich Maschinen- und Anlagensteuerungen) sein. Ebenso gehören alle organisatorischen Einheiten dazu, die im Rahmen der üblichen Prüfungszyklen geprüft werden (müssen). Wesentliche Bestandteile des Prüfungsuniversums 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, sowie das Managementsystem, das deren Implementierung und Umsetzung steuert und überwacht. Hierunter fallen auch die ersten beiden Linien des Drei-Linien-Modells sowie die prozessintegrierten Steuerungs- und Überwachungsmaßnahmen des Internen Kontrollsystems in der IT (IT-IKS).

Grundsätzlich sind also alle Elemente der Aufbau- und Ablauforganisation für die Aufstellung des Prüfungsuniversum 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 Prüfungsuniversum risiko- und themenorientiert zu (Teil-)Prüfungsfeldern zusammengefasst werden.

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

2.5.4 (Jahres-)Prüfungsplan

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

14 Vgl. *https://www.isaca.org/resources/glossary#glossr.*

15 Vgl. *http://www.diir.de/fileadmin/fachwissen/revisionshandbuch-marisk.pdf*, Abschnitt 4.1.1.1. Innerhalb der Geschäftsprozesse gewinnen auch Produktions- und Logistikprozesse im Kontext zunehmender IT-Durchdringung (Industrie 4.0) eine immer größere Bedeutung, weshalb sie mit einbezogen werden müssen. Von der Digitalisierung sind darüber hinaus alle administrativen Prozesse betroffen.

16 In ITIL 4 werden statt Prozessen Prinzipien, Konzepte und Praktiken definiert. Im Bereich der Servicemanagement-Praktiken entsprechen viele Praktiken den früheren Prozessen, ohne dabei prozessuale Vorgaben zu machen. Darin besteht eine wesentliche Neuerung in ITIL 4, weil so eine Flexibilisierung der Prozesse im Unternehmen leichter möglich wird. Dennoch behalten die aus ITIL v3 bekannten Prozesse weiterhin ihre Gültigkeit.

- mehrjährige,
- jährliche,
- unterjährige und
- rollierende/agile

Prüfungsplanungen.

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

Im **Jahresprüfungsplan** legt die Revision fest, welche Prüfungsobjekte bzw. Prüfungsgegenstände aus dem Prüfungsuniversum im kommenden Prüfungsjahr betrachtet werden sollen. Diese sind oft durch bereits vorliegende Audit-Ergebnisse 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 (agile) Prüfungsplanung** ist eine alternative, flexible Planungsmethode zur mehrjährigen und Jahresprüfungsplanung. Bei der rollierenden Prüfungsplanung wird (häufig unter Zuhilfenahme von spezieller Audit-Software, vermehrt auch von Machine-Learning-Methoden) ständig risikoorientiert neu festgelegt, welche Prüfungsobjekte bzw. Prüfungsgegenstände aus dem Prüfungsuniversum in den kommenden Prüfungen betrachtet werden sollen oder müssen. Solche rollierenden Prüfungsplanungen sind besonders dann anzuwenden, wenn etwa agile Methoden, DevOps-/NoOps-Konzepte und Continuous-Auditing-Ansätze (vgl. Abschnitt 2.5.6) im Unternehmen angewandt werden.

2.5.5 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[17]:

- **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 vollständig und hinreichend genau sind und damit 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.
- **Compliance**
  Compliance bezeichnet einen Zustand, in dem alle für das Unternehmen relevanten Vorgaben eingehalten werden. Compliance geht über die Erfüllung von gesetzlichen und anderen rechtlich bindenden Vorschriften hinaus. Sie umfasst zusätzlich die Erfüllung von bindenden, vertraglichen Vereinbarungen und internen Vorgaben und Regelungen. Vielfach umfassen Compliance-Handlungsfelder auch Fragen der Ordnungsmäßigkeit, wie sie etwa aus den GoBD ableitbar sind[18]. Neben der zwingend notwendigen Prüfung der Einhaltung externer Vorgaben sollte sich die Revision bei der Prüfung der Compliance mit intern vorgegebenen Vorschriften nicht darauf beschränken, die buchstabengetreue Beachtung dieser Vorschriften zu prüfen. Vielmehr sollte sie stets auch 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 (Schutz-)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-

17 Vgl. dazu auch DIIR-Revisionsstandard Nr. 4, Abschnitt 6.1, *https://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard__Nr._4_V_3.0_Sept_2019.pdf.*

18 Vgl. ISACA-Leitfaden IT-Compliance: *https://www.isaca.de/sites/default/files/attachements/leitfaden_it-compliance_grundlagen_regelwerke_umsetzung.pdf.*

Kommunikation) soll etwa sichergestellt sein, dass die richtige/autorisierte Maschine, der richtige/autorisierte Prozess/Service kommuniziert) und
- **Nichtabstreitbarkeit** (d.h. die Unwiderlegbarkeit des Nachweises einer Aktivität; engl. non-repudiation).

Unter das Prüfungsziel Sicherheit fällt auch der Schutz personenbezogener Daten gemäß Art. 1 DSGVO (Verarbeitung personenbezogener Daten und Verkehr personenbezogener Daten) mit den folgenden sechs Grundsätzen gemäß Art. 5 DSGVO:

- **Rechtmäßigkeit**
  Verarbeitung nach Treu und Glauben, Transparenz
- **Zweckbindung**
  Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke
- **Datenminimierung**
  Daten müssen »dem Zweck angemessen und erheblich sowie auf das […] notwendige Maß beschränkt sein«.
- **Richtigkeit**
  »[…] es sind alle angemessenen Maßnahmen zu treffen, damit [unrichtige] personenbezogene Daten unverzüglich gelöscht oder berichtigt werden.«
- **Speicherbegrenzung**
  Daten müssen »in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es […] erforderlich ist«.
- **Integrität und Vertraulichkeit**
  Daten müssen »in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung«.

Die IT-Grundschutzkataloge des BSI oder die ISO/IEC-Reihe 27000 ff. können bei der Konkretisierung, Umsetzung und dem Management von Sicherheitsthemen Hilfestellung leisten[19].

- **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.

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

Praxisbeispiel

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

2.5.6 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:

- **IT-Systemprüfungen**
  Eine IT-Systemprüfung ist integraler Bestandteil der Jahresabschlussprüfung. Sie wird nach dem internationalen Standard ISA 315 (Revised 2019) – Identifying and Assessing the Risks of Material Misstatement – durchgeführt. Die bislang gültigen Standards IDW PS 261 und IDW PS 330 werden hingegen nicht mehr angewandt.

  Hierdurch soll zum einen der zunehmenden Internationalisierung auch im Prüfungsumfeld Rechnung getragen werden. Zum anderen werden bislang nicht oder nur am Rand betrachtete Aspekte eines IT-Systems in die Prüfung einbezogen. Im Appendix 5 werden beispielsweise explizit auch aktuelle Technologien (»Emerging Technologies«, etwa Blockchain, künstliche Intelligenz) angesprochen.

  Art und Umfang der IT-Systemprüfung ergeben sich aus der Erfassung des IT-Umfelds und der daraus resultierenden IT-Risiken für die Rechnungslegung. Ausgelagerte Bestandteile der IT müssen ebenfalls geprüft werden (IDW PS 331 n.F.).

  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 werden 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.

Die folgenden häufig explizit genannten Prüfungsarten sind keine eigenständigen Prüfungen, sondern werden schwerpunktmäßig der Abschlussprüfung (als Teil einer IKS-/Systemprüfung) zugeordnet:

- **Verfahrens-/Prozessprüfungen (Aufbauprüfungen)**
  Verfahrens- und Prozessprüfungen als Bestandteil einer Systemprüfung 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.
- **Angemessenheitsprüfungen**
  Im Rahmen von Angemessenheitsprüfungen als Bestandteil von Aufbauprüfungen gemäß der Definition in Abschnitt 2.5.5 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.
- **Wirksamkeits- bzw. Funktionsprüfungen**
  Wirksamkeitsprüfungen (Funktionsprüfungen) untersuchen als Bestandteil einer Systemprüfung und gemäß der Definition in Abschnitt 2.5.5, 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.
- **Erhebungen**
  Eine Ausnahme bezüglich des Prüfungsziels »Beurteilung« stellen reine Erhebungen dar, weil bei ihnen nur eine Aufnahme der relevanten IT-Systeme, Verfahren und Prozesse stattfindet und insbesondere keine Bewertung der Angemessenheit oder Wirksamkeit erfolgt. Erhebungen dienen im Wesentlichen der Aktualisierung des Prüfungsuniversums und zur Vorbereitung der Prüfungsplanung.

Die folgenden Prüfungsarten sind nicht Bestandteil einer Jahresabschlussprüfung. Diese von der Abschlussprüfung unabhängigen Prüfungen sind ziemlich frei gestaltbar. Ihre Durchführung orientiert sich an den ISACA-Standards sowie am neuen Prüfungsstandard IDW PS 860 (vgl. [IDW 2018]):

a. **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 Prüfungsuniversums 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 im Gegensatz zu Continuous Auditing 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.

Für Continuous Monitoring können unter anderem Process-Mining-Werkzeuge eingesetzt werden.

b. **IT-Assurance**
   Unter IT-Assurance (Sonderprüfung) wird eine Prüfungsform verstanden, die hinsichtlich des Prüfungsgegenstandes – soweit kriterienbasiert – grundsätzlich frei gestaltbar ist. Aber auch solche Prüfungen folgen einem klaren Prüfungsprozess (Assurance-Prozess, ISAE 3000), 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) (vgl. [IDW 2008])**[20]
Bei Projektprüfungen unterscheidet man zwischen den projektbegleitenden Prüfungen (Pre-Implementation-Audit) und den nachgelagerten Prüfungen (Post-Implementation-Audit). Bei solchen 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 Reifegrades der (Projekt-)Organisation –, Empfehlungen für die Planung und Durchführung künftiger Projekte zu geben oder beispielsweise zu prüfen, ob das im Rahmen des Projektes 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 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 (einschließlich Cloud-Anbieter) 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 (was bei Nutzung von Cloud-Diensten der sog. Hyperscaler meist nicht möglich ist) oder der IT-Serviceprovider kann die Anforderungserfüllung anhand eines detaillierten Prüfungsberichts nach IDW PS 951 (als nationale Konkretisierung des ISAE 3402/SSAE 16) 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]). Speziell für Cloud-Anbieter existieren zudem Zertifizierungen wie EuroCloud »SaaS Star Audit (ECSA)«, »TÜV Trust IT« bzw. »Certified Cloud Service« des TÜV Rheinland, »SOC-2« nach Cloud Computing C5 des BSI, »Trust in Cloud« des Cloud-EcoSystem e.V. sowie die STAR-Zertifizierungen auf unterschiedlichen Leveln der Cloud Security Alliance (CSA).

iv. **Prüfungen des Information Security Management System (ISMS) nach ISO/IEC 270xx**
Der für Informationssicherheits-Managementsysteme (ISMS) maßgebliche Standard ISO/IEC 27001:2013 sieht regelmäßige »interne Audits« des ISMS vor (siehe Kapitel 9.2 der Norm). Diese internen Audits sind nicht zu verwechseln mit den offiziellen Zertifizierungs- und Re-Zertifizierungsaudits, die im Falle eines zertifizierten ISMS von einer externen prüfenden Stelle durchgeführt werden. Im Fokus einer solchen internen Prüfung des ISMS steht zum einen die im Hauptteil der Norm beschriebene Organisation des Informationssicherheits-Managementsystems (z. B. der Anwendungsbereich, die Planung zum Umgang mit Informationssicherheitsrisiken oder Maßnahmen zur kontinuierlichen Verbesserung des ISMS) und zum anderen die Wirksamkeit einzelner risikobeherrschender Maßnahmen, die sich aus dem Anhang A der Norm ergeben (z. B. die Informationssicherheitsrichtlinien, die Informationsklassifizierung oder die Zugangssteuerung).

Für Betreiber kritischer Infrastrukturen im Sinne des BSI-Gesetzes ist ein ISMS in der Regel indirekt gefordert. Betreiber kritischer Infrastrukturen müssen sich gemäß § 8a (3) BSI-Gesetz alle zwei Jahre hinsichtlich ihrer IT-Sicherheit prüfen lassen, z. B. von der Internen Revision. Wesentlicher Bestandteil dieser Prüfungen ist regelmäßig auch die Beurteilung, ob ein angemessenes ISMS etabliert ist.

c. **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, vgl. [IDW 2010]) im Auftrag des Softwareherstellers durch einen Wirtschaftsprüfer durch-

20 Siehe auch DIIR Prüfungsstandard Nr. 4.

geführt. 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) sowie über Verfahren für Zugriffsschutz und Datensicherung verfügt.

2.5.7 Prüfungsprogramm (Arbeitsprogramm)

Im Prüfungsprogramm werden anhand von externen Prüfungskriterien (insbesondere abgeleitet aus Gesetzen, aber auch 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 besteht darin, 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
- Erwartete Maßnahmen

2.5.8 Prüfungsunterlagen

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

- Prozess- und Systemdokumentation
- 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

2.5.9 Prüfungshandlungen

Typische **Prüfungshandlungen** sind:

- Analyse von Risiken
- Sichtung von Dokumenten
- Beobachtungen von Abläufen/Prozessen (nicht nur im betriebswirtschaftlichen, sondern auch im technischen Bereich)
- 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 sowie Inventarlisten – auch hier nicht nur im betriebswirtschaftlichen, sondern verstärkt auch im technischen Bereich, beispielsweise Maschinen-/Anlagensteuerungen und eingebundene weitere IoT-Geräte
- Aufnahme von Beständen
- Begehungen von Gebäuden (Rechenzentren, Serverräume, Produktionsstandorte, Steuerungs-Leitstände, sonstige Betriebsgebäude mit vernetzten Anlagen) an allen (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, ISO/IEC 20000 und die damit kompatible Information Technology Infrastructure Library (ITIL) und ISO 31000 (Risikomanagement), das deutsche Telekommunikationsgesetz (TKG), das Bundesdatenschutzgesetz (BDSG, auf Basis der EU-DSGVO 2018 novelliert), 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 Finanz- und Zahlungsdienstleistungsunternehmen besonders relevant sind das Kreditwesengesetz (KWG) und das Zahlungsdiensteaufsichtsgesetz (ZAG), BASEL III/IV bzw. Solvency II sowie die Mindestanforderungen an das Risikomanagement (MaRisk), die Bankaufsichtlichen Anforderungen an die IT (BAIT) und weitere aufsichtliche Anforderungen an die IT (KAIT, VAIT, ZAIT) des BaFin, und – international – Anforderungen in den Leitlinien der European Banking Authority (EBA) unter anderem zum »Management von IKT- und Sicherheitsrisiken« (EBA/GL/2019/04) und »Auslagerungen« (EBA/GL/2019/02) sowie 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 ITAF (aktuell in Version 4) insbesondere die IDW-, DIIR- und IPPF- sowie ISAE-Standards. Sie beeinflussen den Prüfungsumfang und die Prüfungsziele. Auch COBIT 2019, eher IT-Governance-Rahmenwerk als Prüfungsstandard, kann eine wichtige Unterstützung beispielsweise im Rahmen der Erstellung des Prüfungsplans und des Prüfungsuniversums sein[1]. Bei den nationalen Vorgaben aus der Regulierung sind aktuell insbesondere alle Vorgaben im Kontext kritischer Infrastrukturen (KRITIS) von großer Bedeutung[2].

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 und weiterer anerkannter Organisationen zum Thema IT-Prüfung[3].

Sowohl das englische Original (Version 4) als auch die deutsche Übersetzung (allerdings noch der Vorgängerversion 3) ist im ISACA-Store unter dem Suchbegriff ITAF verfügbar und für Mitglieder als PDF kostenfrei erhältlich.

ITAF 4 umfasst wie bisher auch drei Kategorien von Standards (General – 1000er-Reihe, Performance – 1200er-Reihe und Reporting – 1400er-Reihe) sowie entsprechend dazu gehörende Guidelines (2000er-, 2200er- bzw. 2400er-Reihe). Jeder Standard enthält entsprechende Statements (vgl. Abschnitt 3.1.2).

General Standards (und dazugehörige Guidelines) gelten grundsätzlich im Prüfungs- und Assurance-Kontext. Performance Standards beziehen sich auf die einzelnen Elemente und Tätigkeiten im Kontext der IT-Prüfung, Reporting Standards schließlich fokussieren auf die zu erstellenden Berichte und Nachweise sowie die darin enthaltenen Informationen und die Form der Kommunikation.

3.1.1 Ethikkodex

Der ISACA Code of Professional Ethics verpflichtet Mitglieder sowie Inhaber eines ISACA-Zertifikats (CISA, CISM, CRISC, CGEIT, CSX-P) zur Einhaltung von ethischen Grundsätzen bei der Ausübung ihrer Tätigkeit. Dies beinhaltet die Befolgung anerkannter Standards und gesetzestreues, recht-

1 Vgl. etwa den Beitrag »IS Audit Basics: Developing the IT Audit Plan Using COBIT 2019«, *https://www.isaca.org/resources/isaca-journal/issues/2019/volume-3/developing-the-it-audit-plan-using-cobit-2019.*

2 Vgl. *www.kritis.bund.de.*

3 Einen grundsätzlichen Überblick über ITAF bietet [Auf der Heyde/Hahn 2014]; zu den Neuerungen 2020 in ITAF 4 siehe den Überblick unter *https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2020/isaca-updates-it-audit-framework-itaf.*

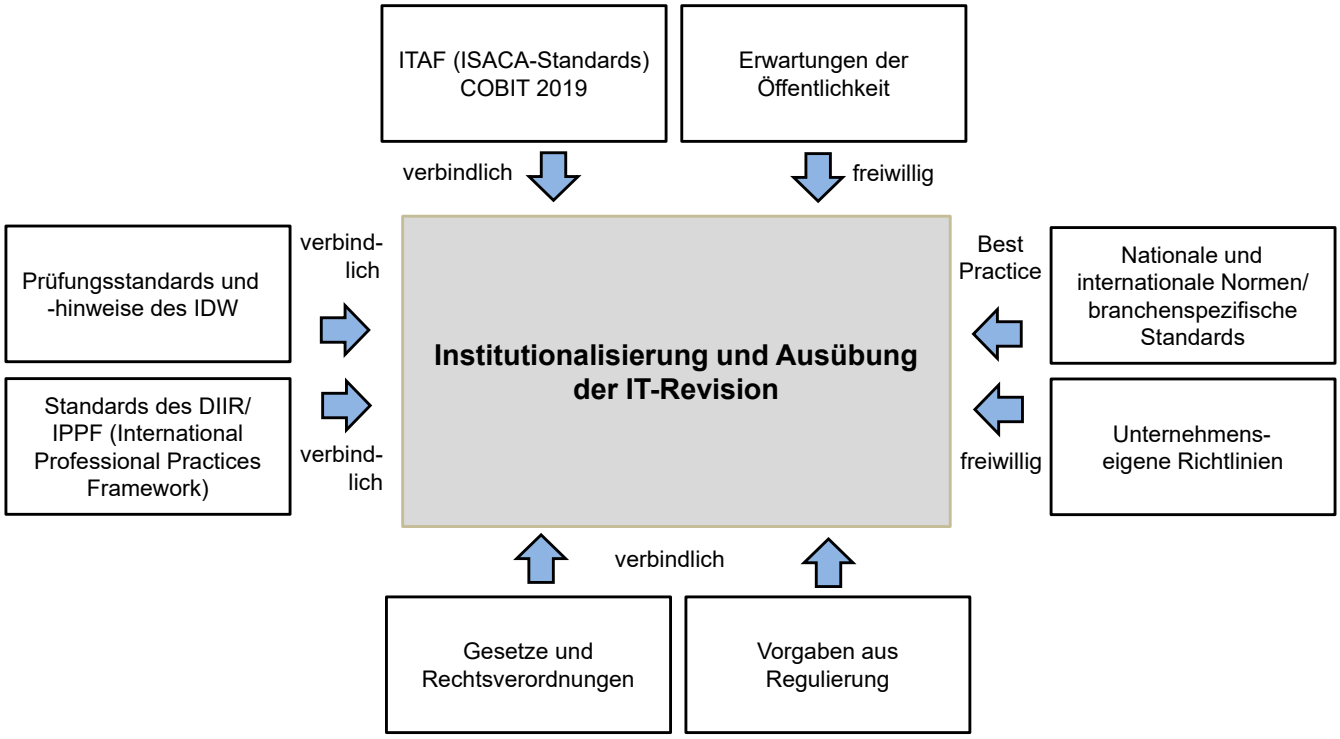


Abbildung 3–1: Institutioneller Rahmen für die IT-Revision (modifiziert nach [Amling/Bantleon 2007])

schaffenes und kompetentes Handeln und schließt eine Geheimhaltungspflicht ein[4].

Ein angemessener Ethikkodex umfasst auch die Betrachtung des Spannungsfeldes 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 für die prozessverantwortlichen Fachbereiche im Unternehmen als wertvoller Impulsgeber im Kontext des Einsatzes und der Optimierung von Methoden und Prozessen in der IT-Organisation und trägt damit zur Verbesserung ihrer organisationalen Reife bei. Das Grundgeschäft der IT-Revision ist dabei zunächst die risikoorientierte Istanalyse. Mögliche Lösungswege hin zu einem Sollzustand und die damit verbundenen Ideen, Anregungen und Impulse liefern dann im Kontext von Prüfungen oder im Rahmen von internen Beratungsaufträgen wichtige Hinweise für die Fachbereiche auf dem Weg zur erfolgreichen Umsetzung. Dies gilt in gleicher Weise für projektbegleitende und damit meist weniger formale Prüfungen, etwa im agilen Projektmanagement oder in DevOps-Organisationsformen.

Von zentraler Bedeutung dabei ist allerdings die gleichzeitige Beachtung der prüferischen Unabhängigkeit der Revisionsfunktion. Zwar darf die »zulässige« Bandbreite (unterstützende Beratung im Sinne der Methodik, Grundsatzfragen usw.) ausgeschöpft werden. Eine konkrete Unterstützung im Rahmen von Implementierungen oder bei der Wahl eines Anbieters im Rahmen des Bezugs externer Leistungen muss aber unbedingt 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 das Bewusstsein (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]).

4 Vgl. *www.isaca.org/credentialing/code-of-professional-ethics.*

Denn umgekehrt ist es das Ziel einer erfolgreichen Revision, über Prüfungsfeststellungen einen Fachbereich positiv zu beeinflussen, beispielsweise wenn ein Fachbereich versucht, Änderungen umzusetzen, die Rahmenbedingungen dies vermeintlich aber nicht zulassen. Im Kontext positiver Beeinflussung kann es zudem sehr 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 4 wichtigen Elementen gehören alle **ISACA-Standards und ISACA-Guidelines (Richtlinien/Leitfäden)**. Sie sind untergliedert in General Standards, Performance Standards und Reporting Standards. Zu jedem Standard gehört ein entsprechendes Statement. Diese Standards (mit ihren Statements) und Guidelines 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 sind Teil des in 2020 überarbeiteten IT Audit and Assurance Framework (ITAF 4).

Allgemeine Standards (General Standards)
Die allgemeinen Standards umfassen:

- IT-Prüfungsstandard 1001 – Audit Charter (Audit Charter)
- IT-Prüfungsstandard 1002 – Organisatorische Unabhängigkeit (Organizational Independence)
- IT-Prüfungsstandard 1003 – Unabhängigkeit des Prüfenden (Auditor Objectivity)
- IT-Prüfungsstandard 1004 – Hinreichende Durchführbarkeit (Reasonable Expectation)
- IT-Prüfungsstandard 1005 – Berufsübliche Sorgfalt (Due Professional Care)
- IT-Prüfungsstandard 1006 – Expertise (Proficiency)
- IT-Prüfungsstandard 1007 – Aussagen (Assertions)
- IT-Prüfungsstandard 1008 – Kriterien (Criteria)

Ausführungsstandards (Performance Standards)
Die Ausführungsstandards umfassen:

- IT-Prüfungsstandard 1201 – Risikoorientierter Planungsansatz (Risk Assessment in Planning)
- IT-Prüfungsstandard 1202 – Gesamthafte Prüfungsplanung (Audit Scheduling)
- IT-Prüfungsstandard 1203 – Durchführungsplanung (Engagement Planning)
- IT-Prüfungsstandard 1204 – Durchführung und Überwachung (Performance and Supervision)
- IT-Prüfungsstandard 1205 – Nachweise (Evidence)
- IT-Prüfungsstandard 1206 – Verwendung der Ergebnisse anderer Sachverständiger (Using the Work of Other Experts)
- IT-Prüfungsstandard 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen (Irregularities and Illegal Acts)

Berichtsstandards (Reporting Standards)
Die Berichtsstandards umfassen:

- IT-Prüfungsstandard 1401 – Berichterstattung (Reporting)
- IT-Prüfungsstandard 1402 – Nachschau (Follow-up Activities)

3.1.3 Leitlinien (Guidelines)

Die Leitlinien sind analog in allgemeine Leitlinien, Ausführungsleitlinien und Berichtsleitlinien unterteilt. Ihre Aufteilung und ihr Titel folgen derselben Logik und Namensgebung wie die der Standards, allerdings mit dem Präfix »2« statt »1«.

3.1.4 Instrumente und Methoden für die IT-Prüfung (Tools and Techniques)

Das ITAF verweist auf Whitepapers und Prüfungsprogramme sowie die COBIT-Produktreihe und weitere Ressourcen, die über die ISACA-Global-Homepage erreichbar sind. Aktuell fasst die neu gestaltete Homepage alle Ressourcen unter *www.isaca.org/resources* zusammen.

COBIT 2019
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; direction is set through prioritization and decision making; performance and compliance are monitored 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 (Bewerten, »Evaluate«). Dabei nutzt gute Governance die Instrumente der Priorisierung ebenso wie klare Entscheidungen (Anweisen, Entscheiden, »Direct«), um eine strategische Richtung vorzugeben. Gleichzeitig überwacht sie den Prozess der Zielerreichung (Überwachen, »Monitor«).

Damit grenzt COBIT 2019 »Governance« klar von »Management« ab, das unter Berücksichtigung der Governance-Vorgaben das Ziel verfolgt, die konkrete Umsetzung zu gestalten (»Management plans, builds, runs and monitors activities«).

Als zentrales Werkzeug im ITAF soll COBIT bzw. die COBIT-Produktfamilie auch in der aktuellen Fassung 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. Zu den Neuerungen in COBIT 2019 siehe [Gaulke 2019].

Der Einsatz des COBIT-Rahmenwerks kann die Erfüllung der ISACA-Standards weitgehend unterstützen (vgl. [Cascarino 2012, S. 49]). Zu jedem Standard und jeder Guideline sind daher in ITAF 4 explizit Bezüge zu COBIT 2019 angegeben. Die ISACA-Fachgruppe »IT-Risikomanagement« hat bereits 2013 ergänzend einen Leitfaden zur Durchführung eines IT-Risikomanagements mithilfe von COBIT 5 erstellt, der sinngemäß übertragen werden kann[5].

Neue Erkenntnisse aus Forschung und Praxis

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

3.2 COSO Internal Control Standards

Ziel des COSO Internal Control – Integrated Framework (COSO ICIF 2013)[6] ist es, jedem Unternehmen das Erreichen der folgenden Ziele zu ermöglichen:

- Wirtschaftlichkeit (Effizienz) des Geschäftsbetriebes, 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) 2019 in Version 7 veröffentlichten »International Standards for the Professional Practice of Internal Auditing« (IPPF; Berufsstandards der internen Revision)[7] dienen der Sicherstellung der Qualität der Internen Revision. Zusätzlich zu den verbindlichen Standards ist auch der Ethikkodex (»Code of Ethics«) zwingend zu befolgen. »Practice Guides« stellen Ansätze zur bestmöglichen Implementierung der Standards dar. Außerdem werden »Global Technology Audit Guides (GTAGs)« sowie »Guide to the Assessment of IT Risk (GAIT)[8]« zur Unterstützung der Entwicklung von Mitarbeitern in der Internen Revision zur Verfügung gestellt.

5 »IT-Risikomanagement – leicht gemacht mit COBIT«, abrufbar unter *https://www.isaca.de/sites/default/files/attachements/2012-isaca-leitfaden-it-risikomanagement_0.pdf.*

6 Vgl. *www.coso.org.*

7 Vgl. *https://iia.org.au/sf_docs/default-source/quality/ippf-standards-2017.pdf.*

8 Vgl. *https://www.theiia.org/en/standards/what-are-the-standards/recommended-guidance.*

3.4 ISO-Standards

3.4.1 ISO/IEC-270xx-Familie

Der Standard ISO/IEC 27001:2013/Corr 2:2015 »Information technology – Security techniques – Information security management systems – Requirements« (deutsche Übersetzung DIN EN ISO/IEC 27001:2017-06) ist ein für Unternehmen wichtiger Standard, um ein Informationssicherheits-Managementsystem zu planen, zu betreiben und kontinuierlich zu verbessern. Seit Juni 2017 ist auch seine deutsche Übersetzung veröffentlicht (DIN EN ISO/IEC 27001:2017-06). Der Standard ISO/IEC 27002:2013 »Information technology – Security techniques – Code of practice for information security management« ist für die Umsetzung von 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 funktionierendes Informationssicherheits-Managementsystem (ISMS) gemäß Standard implementiert sein muss. ISO/IEC 27002:2013 beschreibt, wie in einem Unternehmen Informationssicherheitsmaßnahmen implementiert werden können. Dabei wird unter Informationssicherheit ein Maßnahmenbündel verstanden, das insbesondere unternehmensinterne Standards, Vorgaben und Regelungen sowie Managementprozesse umfasst (vgl. [Fröhlich et al. 2007a, S. 64]). Der Standard ISO/IEC 27005:2018 »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.

Die ISACA-Fachgruppe Informationssicherheit hat 2013 einen Leitfaden zur Implementierung eines ISMS nach ISO/IEC 27001:2013 veröffentlicht[9].

3.4.2 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 20000-2:2019: Information technology – Service management – Part 2: Guidance on the application of service management systems

3.4.3 ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements

Diese Norm ist 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 und die laufende Verbesserung eines vollständigen Business Continuity Management System (BCMS). Es umfasst u. a.:

- Geschäftskontinuitäts-Strategie und davon abgeleitete Richtlinien (Policies)
- Geschäftskontinuitäts-Planung (Business Continuity Plan, BCP)
- Geschäftskontinuitäts-Notfall-/Ausfallszenarien (Disaster Recovery Plan, DRP)

Ziel ist es, die Widerstandsfähigkeit (»Resilience«) des Unternehmens im Notfall durch ein entsprechend ausgestaltetes BCMS laufend zu verbessern.

3.4.4 ISO/IEC 38500:2015 Information technology – Governance of IT for the organization

ISO/IEC 38500:2015: Informationstechnik – Unternehmensführung in der Informationstechnik (Governance of IT for the organization) ist ein bereits seit 2008 existierender »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]). Die Norm befindet sich aktuell im Review, was auf eine Aktualisierung hindeuten könnte.

3.5 BSI-Standards

Das Ziel des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist es, Informationssicherheit insbesondere in den als kritische Infrastrukturen definierten Sektoren[10], aber auch in öffentlichen Einrichtungen, 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-Grundschutzstandards und im BSI-Grundschutz-Kompendium zusammengefasst. Das

9 *https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf.*

10 Vgl. *www.kritis.bund.de.*

Grundschutz-Kompendium wird jährlich aktualisiert und jeweils im Februar veröffentlicht. Seit 1. Februar 2022 liegt die Edition 2022 vor, die für Zertifizierungen genutzt werden muss. Die Grundschutzstandards geben die Vorgehensweise vor, das Grundschutz-Kompendium beschreibt 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[11]:

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Standard 200-3: Risikomanagement
- BSI-Standard 100-4: Notfallmanagement

Das IT-Grundschutz-Kompendium 2022 setzt sich aus mehreren informativen Teilen (Einstieg in die Thematik und Methodik, Vorstellung der Änderungen, Hinweise zum Schichtenmodell und zur Modellierung, Beschreibung der Rollen sowie ein Glossar) und drei weiteren Abschnitten (Gefährdungen, Prozess-Bausteine und System-Bausteine) zusammen. Die Darstellungen zu den Gefährdungen und die Bausteine bilden den Hauptteil und das Herzstück des Kompendiums.

Der Abschnitt zu Gefährdungen beschreibt insgesamt 47 unterschiedliche Gefährdungen. Die Prozess- und System-Bausteine wiederum sind thematisch geordnet und entsprechend in Schichten weiter detailliert untergliedert. Die Schichten befassen sich jeweils mit einem konkreten Bereich. So unterteilen sich die Prozess-Bausteine in das Sicherheitsmanagement, organisatorische und personelle Sicherheitsaspekte, Organisation und Personal, Konzepte und Vorgehensweisen, den operativen Betrieb und die Erkennung von Vorfällen einschließlich der richtigen Reaktion darauf. Die System-Bausteine wiederum unterteilen sich in Anwendungen, einzelne IT-Systeme, industrielle IT, Vernetzungsaspekte und die sonstige Infrastruktur, die explizit auch den häuslichen Arbeitsplatz adressiert.

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

11 Stand: Februar 2022.

Die BSI-Standards und das IT-Grundschutz-Kompendium sowie aktuelle Informationen und vielfältige, teils umfangreiche Vorlagen und Hilfsmittel stehen auf den Webseiten des BSI kostenlos zum Download zur Verfügung[12].

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.

Seit Anfang 2019 erfolgt die schrittweise Einführung von ITIL 4 als Erweiterung von ITIL v3:2011. Soweit Elemente der alten Good Practices noch nicht durch aktualisierte Elemente ersetzt sind, behalten die alten Elemente ihre Gültigkeit. Eine wesentliche Neuerung ist das Ersetzen der bisherigen ITIL-Prozesse durch Practices, was eine Flexibilisierung des Modells bedeutet, da die »starre« Orientierung an Prozessen entfällt. Neu eingeführt wird auch das Service-Wert-System (»Service Value System, SVS«)[13].

12 *www.bsi.bund.de.*

13 Weiterführende Informationen unter *https://www.axelos.com/certifications/itil-service-management/what-is-itil.*

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 und damit gesamtverantwortliche Prüfer ein erfahrener, fachkundiger Mitarbeiter sein, der mit den wichtigsten Prüfmethoden bestens vertraut ist und über gute Kenntnisse der zentralen Prüfungsgebiete verfügt. 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 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, die an dieser Stelle nicht weiter vertieft werden sollen. 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 das IT Audit and Assurance Framework (ITAF 4)

Anforderungen an die Eignung von IT-Revisoren sind in den folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) sowie den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) definiert:

- 1002 – Organisatorische Unabhängigkeit
- 1003 – Unabhängigkeit des Prüfenden
- 1005 – Berufsübliche Sorgfalt
- 1006 – Expertise

Die beiden nachfolgenden Stellenprofile beschreiben beispielhaft typische Anforderungen:

IT-Revisor in einem internationalen Anwenderunternehmen (m/w/d)

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.

Senior IT-Auditor in einer Wirtschaftsprüfungsgesellschaft (m/w/d)

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 ein 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.

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«, »Beschaffung, Entwicklung und Implementierung von Informationssystemen«, »Betrieb von Informationssystemen und Business Resilience« sowie »Informationssicherheit«. Inhaber des CISA-Zertifikats sind verpflichtet, ethische und für IT-Prüfungen verbindliche Standards aus dem ITAF einzuhalten und sich in einem vorgegebenen Mindestmaß laufend weiterzubilden. Die Zertifizierung wird von der ISACA vergeben. Die CISA-Zertifizierung selbst ist von ANSI nach ISO/IEC 17024:2012 zertifiziert, was eine gewisse Vergleichbarkeit der Qualifikation einzelner IT-Prüfer untereinander gewährleistet.

Weitere sinnvolle Zertifizierungen sind CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control) 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.

4.3 Studiengänge mit Bezug zur IT-Revision

Aktuell wird an der Universität Duisburg-Essen mit dem Master BWL, Schwerpunkt Interne Revision and Corporate Governance *(https://www.ircg.msm.uni-due.de/lehre)* ein Studiengang mit Bezug zur IT-Revision angeboten.

Mit Fokus auf die IT-Forensik, ein für IT-Prüfer besonders interessantes Spezialgebiet, werden aktuell folgende Studiengänge bzw. Weiterbildungen angeboten:

- Hochschule Albstadt-Sigmaringen: Master of Science – Digitale Forensik (berufsbegleitend): *https://master-digitale-forensik.de/berufsbegleitender-onlinestudiengang*
- Technische Hochschule Deggendorf: Bachelor of Science Cyber Security
- Hochschule Fresenius: Master of Science – Wirtschaftsforensik/Analytische & Digitale Forensik (berufsbegleitend)
- Hochschule Mittweida, Universität Potsdam, Hochschule Wismar: Digitale Forensik
- SANS Forensik-Fortbildungskurse einschließlich abschließender Zertifizierung

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)

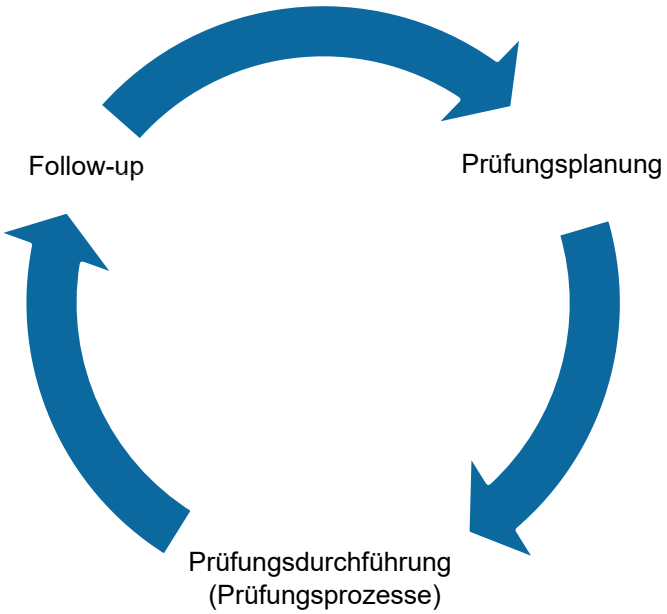


Abbildung 5–1: Revisionsprozesse

Die Prüfungsplanung gliedert sich in 5 Teilprozesse:

- Erstellung und Aktualisierung des Prüfungsuniversums (Abschnitt 6.1)
- Risikoanalyse (Abschnitt 6.2)
- Mehrjahresplanung (Abschnitt 6.3)
- Jahresplanung (Abschnitt 6.4)
- Unterjährige Planung/rollierende Planung (Abschnitte 6.5 und 6.6)

Die Durchführung einer konkreten Prüfung auf Basis der Prüfungsplanung lässt sich ebenfalls 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: Die 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 das IT Audit and Assurance Framework (ITAF 4)

Anforderungen an die Prüfungsplanung sind in den folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) sowie den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) definiert:

- IT-Prüfungsstandard 1201 – Risikoorientierter Planungsansatz
- IT-Prüfungsstandard 1202 – Gesamthafte Prüfungsplanung
- IT-Prüfungsstandard 1203 – Durchführungsplanung

Die nachfolgende Abbildung 6–2 zeigt beispielhaft ein Template für einen Prüfungsplan.

Mehrjahres-, Jahres-, unterjährige Prüfungsplanung		
Input	**Einflussgrößen**	**Output**
◗ Audit-Charta ◗ Prüfungsuniversum	◗ Aktuelle Entwicklungen im Unternehmen ◗ Veränderung der Risikosituation	◗ Aktualisiertes Prüfungsuniversum ◗ Mehrjahresprüfungsplan ◗ Jahresprüfungsplan ◗ Unterjähriger Prüfungsplan ◗ Rollierender Prüfungsplan
Aktivtäten		**Werkzeuge**
◗ Erarbeitung/Aktualisierung des Prüfungsuniversums ◗ Risikoanalyse ◗ Mehrjahresplanung ◗ Jahresplanung ◗ Unterjährige Planung/rollierende Planung		◗ Risikoanalysetools ◗ Planungswerkzeuge ◗ Templates ◗ Checklisten ◗ Office-Tools ◗ Spezialisierte Revisionssoftware

Tabelle 6–1: Input-Output-Beziehung Prüfungsplanung

1 Für eine Übersicht der geeigneten Methoden und Werkzeuge im IT-Risikomanagement vgl. [Knoll 2019, S. 184ff.].

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	Pentest
	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 Erstellung und Aktualisierung des Prüfungsuniversums

Im Regelfall liegt das Prüfungsuniversum (vgl. Abschnitt 2.5.3) zu Beginn der Prüfungsplanung bereits vor und muss ggf. lediglich (nochmals) auf Aktualität geprüft werden. Findet die Prüfungsplanung erstmals statt, wird das Prüfungsuniversum in diesem Rahmen neu erstellt. Die Aktualisierung des Prüfungsuniversums wird zweckmäßigerweise als erster Schritt in der Prüfungsplanung durchgeführt, da die Risikoanalyse und die Erstellung von Prüfungsplänen auf das Prüfungsuniversum aufbauen.

Veränderungen der Geschäftstätigkeit und der Organisation eines Unternehmens finden insbesondere im Kontext der Digitalisierung immer häufiger statt. Hierzu gehört vor allem das Anbieten neuer Dienstleistungen, was oftmals mit der Einrichtung neuer Prozesse und vielfach auch einer Veränderung der Aufbauorganisation verbunden ist. Um ungeprüfte Bereiche im Unternehmen zu vermeiden, ist es erforderlich, dass die Revision periodisch ihr Prüfungsuniversum auf Vollständigkeit kontrolliert und ggf. neue Prüfungsobjekte definiert oder bestehende entsprechend anpasst bzw. erweitert. Da viele Veränderungen unterjährig stattfinden, hat es sich bewährt, die Informationen über Veränderungen fortlaufend zu sammeln. Änderungen im Unternehmen sollte daher das Prüfungsuniversum stets auch anlassbezogen aktualisiert werden können. Als Informationsquellen für die bei der Gestaltung des Prüfungsuniversums zu berücksichtigenden Veränderungen können die unternehmensinternen Veränderungsmeldungen und – sofern im Unternehmen vorhanden – die Prozesslandkarte sowie auch das Projektportfolio dienen, da heute nahezu alle Tätigkeiten mit Unterstützung einer IT-Lösung abgewickelt und Veränderungen der IT üblicherweise als Projekt durchgeführt werden.

Abbildung 6–3: Der Planungsprozess – Aktualisierung des Prüfungsuniversums

6.2 Risikoanalyse

Abbildung 6–4: Der Planungsprozess – Risikoanalyse

Der risikoorientierte Prüfungsansatz fordert, jedes Prüfungsobjekt im Prüfungsuniversum 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 Erhebung (vgl. Abschnitt 2.5.6) 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 ergeben und rein fachlichen, etwa betriebswirtschaftlichen und rechtlichen Ursprungs sind[2], stets auch Risiken erfassen, die aus der IT-Nutzung resultieren[3]. Unterschieden werden dabei **inhärente Risiken** und **Kontrollrisiken**.

Inhärente Risiken sind stets originär mit dem Prüfungsobjekt verbunden. Sie existieren unabhängig davon, ob Maßnahmen zur Risikobehandlung ergriffen wurden. Bei IT-Systemen sind inhärente Risiken beispielsweise durch den Aufbau und die innere Funktionsweise begründet. So kann etwa ein Designfehler in einer Datenbank zu fehlerhaften Daten in der Anwendung führen. Aktuell von großer Bedeutung sind insbesondere inhärente Risiken, die zu Sicherheitsproblemen und damit Sicherheitsrisiken führen. Dies trifft etwa zu, wenn Softwarefehler in Webapplikationen unentdeckt bleiben oder wenn Fehler aufgrund fehlender Anwendung von By-Design-Grundsätzen nicht korrigierbar sind.

Inhärente Risiken des IT-Einsatzes zur Unterstützung von Geschäftsprozessen liegen in der hohen Abhängigkeit der Geschäftsprozesse von der IT, insbesondere, dass sie verfügbar ist und fehlerfrei arbeitet. Außerdem stellt jede Änderung am IT-System und der IT-Infrastruktur ein Risiko für die Geschäftsprozesse dar. Sie ergeben sich nicht zuletzt auch durch die gewählte IT-Strategie und grundsätzliche Entscheidungen zu verwendeten Architekturen und Technologien. Aus diesem Grund ist auch das Kontinuitätsmanagement (Business Continuity Management) von elementarer Bedeutung.

Kontrollrisiken wiederum entstehen durch Schwächen im Design des Internen Kontrollsystems oder im Kontext der Umsetzung von Kontrollen. Sie sind daran erkennbar, dass IT-Kontrollen versagen. Ihre Existenz spiegelt damit die Unwirksamkeit der Maßnahmen im IKS und damit die Qualität des IKS wider.

Zur Bewertung der Risiken eines Prüfungsobjekts sind in Abhängigkeit der für das Unternehmen relevanten Risiken folgende Faktoren zu beachten:

- Datum und Ergebnisse der letzten Prüfung
- Finanzrisiken
- Lieferrisiken
- Qualitätsrisiken
- Gesundheitsrisiken
- Reputationsrisiken
- Kritikalität
- Bedeutende Änderungen in Prozessen, Programmen, Systemen, Maschinen und Anlagen sowie Steuerungssystemen
- Bedeutende Änderungen in Maßnahmen zur Risikobehandlung
- Kompetenz des Managements
- Komplexität der Transaktionen
- Komplexität von Produktionsabläufen, Steuerungsprozessen und anderen durch IT immer stärker beeinflussten Prozessen
- Liquidität

2 Z. B. Adress-/Adressenausfallrisiken (einschließlich Länderrisiken), Marktpreisrisiken, Liquiditätsrisiken und Reputationsrisiken.

3 Oft auch als sog. operationelle Risiken bezeichnet.

- Möglichkeiten zur Erzielung des operativen Gewinns
- Zeitkritische und/oder sachlich komplexe Managementanfragen
- Ethik und Moral der Mitarbeiter

Bei der Risikobewertung der Prüfungsobjekte berücksichtigt die Revision auch alle Risiken, die bei vorangegangenen Prüfungen festgestellt wurden, sowie die seit der vorangegangenen Prüfung verstrichene Zeit, weil ein vor langer Zeit erzieltes zufriedenstellendes Ergebnis hinsichtlich der Risikosituation nicht zwingend auf aktuelle Verhältnisse schließen lässt.

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

Im Unterschied zu einer möglichen Netto-Risikobetrachtung von Risikocontrolling-Einheiten im Unternehmen sollte die Interne Revision immer von einer Brutto-Risikobetrachtung 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 aber hat 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 Risiken über die rechnungslegungsrelevanten Aspekte hinaus die größten Auswirkungen auf die Geschäftstätigkeit (Business Impact) haben.

Detaillierte Informationen zu möglichen Risiken sind im COBIT-2019-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 (vgl. Tabelle 6–2).

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 darstellt.

Beispiel Risikobewertung				
Prüffeld	**Reputationsrisiko**	**Fehlerrisiko in IT-Prozessen**	**Fehlerrisiko von IT-Serviceprovidern**	**Gesamtrisiko**
IT-Governance	hoch	mittel	mittel	hoch
Informationssicherheit	mittel	hoch	mittel	hoch
…	…	…	…	…
IT-Betrieb	mittel	hoch	mittel	hoch
IT-Entwicklung	mittel	hoch	gering	hoch
Incident & Problem Management	mittel	mittel	mittel	mittel
User Access & Privilege Management	mittel	hoch	hoch	hoch
Licence Management	gering	gering	gering	gering
IT-Systeme	gering	mittel	mittel	mittel
…	…	…	…	…

Tabelle 6–2: Beispiel Risikobewertung

6.3 Mehrjahresplanung

Abbildung 6–5: Der Planungsprozess – Mehrjahresplanung

Abhängig vom Ergebnis der Risikobewertung wird der Prüfungszyklus für Prüfungsobjekte bzw. (Teil-)Prüfungsfelder festgelegt (vgl. Tabelle 6–3). 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 alle 3 bis 5 Jahre (je nach Ausgestaltung der Audit-Charta, vgl. Abschnitt 2.5.1) zulässig und ausreichend. Ziel sollte aber sein, alle Prüfungsobjekte bzw. (Teil-)Prüfungsfelder unabhängig vom Risikogehalt innerhalb des Planungszeitraums (3 bis 5 Jahre) mindestens einmal prüferisch abzudecken.

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**	**2020**	**2021**	**2022**	**2023**	**2024**
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 & Privilege 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

6.4 Jahresplanung

Im Jahresprüfungsplan (vgl. Tabelle 6-4) wird festgelegt, welche Prüfungsobjekte aus welchen (Teil-)Prüfungsfeldern im folgenden Prüfungsjahr geprüft werden. Ausgangspunkt der Jahresprüfungsplanung ist die Mehrjahresplanung sowie das aktualisierte Prüfungsuniversum 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.

Abbildung 6–6: Der Planungsprozess – Jahresplanung

Beispiel Jahresplanung								
Planjahr:	**2020**							
Prüfung	**Prüffeld**	**Prüfobjekte**	**geplanter Aufwand**	**1. Quartal**	**2. Quartal**	**3. Quartal**	**4. Quartal**	**Prüfer**
03/2020	IT-Entwicklung	Release Management Deployment Management	40 Personentage	X	X			Prüfer 1
07/2020	IT-Betrieb	Service Level Management	20 Personentage			X		Prüfer 2
11/2020	Informations-sicherheit	Security Management	20 Personentage				X	Prüfer 1
…	…	…	…	…	…	…	…	

Tabelle 6–4: Beispiel Jahresplanung

6.5 Unterjährige Planung

Abbildung 6–7: Der Planungsprozess – unterjährige Planung

Beispiel unterjährige Planung								
Planjahr:	**2020**							
Prüfung	**Prüffeld**	**Prüfobjekte**	**geplanter Aufwand**	**Beginn Konzeptions-erstellung**	**Beginn Prüfungs-durchführung**	**Beginn Berichts-abstimmung**	**Berichts-vorlage**	**Prüfer**
03/2020	IT-Entwicklung	Release Management Deployment Management	40 Personentage	06.01.2020	13.01.2020	23.03.2020	24.04.2020	Prüfer 1
07/2020	IT-Betrieb	Service Level Management	20 Personentage	13.07.2020	27.07.2020	28.09.2020	26.10.2020	Prüfer 2
11/2020	Informations-sicherheit	Security Management	20 Personentage	12.10.2020	26.10.2020	21.12.2020	25.01.2021	Prüfer 1
…	…	…	…	…	…	…	…	…

Tabelle 6–5: Beispiel unterjährige Planung

In der unterjährigen Planung (vgl. Tabelle 6–5) 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).

6.6 Rollierende (agile) 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.

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

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

Planung und Vorbereitung einer konkreten Prüfung		
Input	**Einflussgrößen**	**Output**
◗ Genehmigter Prüfungsplan (mehrjährig/einjährig/unterjährig/rollierend)	◗ Umfang/Detailliertheit der Prüfungsplanung ◗ Qualifikation der Prüfer ◗ Prüferkapazitäten	◗ Prüfungsauftrag (Prüfungskonzept mit Prüfungsart und Prüfungszielen) ◗ Prüfungsankündigung ◗ Prüfungsprogramm mit konkreten Prüfungsobjekten und Prüfungsaspekten im Prüfungsfeld
Aktivtäten		**Werkzeuge**
◗ Prüfungskonzeption: - risikoorientierte Konkretisierung der Prüfungsobjekte - Präzisierung der Prüfungsaspekte, -ziele und -inhalte ◗ Zusammenstellung des Prüfungsteams ◗ Zeit- und Kapazitätsplanung (unter Beachtung der Kompetenzprofile der Prüfer)		◗ Risikoanalysetools (vgl. Abschnitt 6.2) ◗ Planungswerkzeuge (vgl. Hinweise in Kapitel 6) ◗ Office-Tools ◗ Spezialisierte Revisionssoftware

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

Prüfung auf eine Präzisierung der Prüfungsaspekte und Prüfungsziele (vgl. Abschnitt 2.5.5) sowie auf die Festlegung der Prüfungsart je Prüfungsziel (vgl. Abschnitt 2.5.6).

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.

Hinweis auf das IT Audit and Assurance Framework (ITAF 4)

Anforderungen an die Planung und Vorbereitung einer konkreten Prüfung sind im IT-Prüfungsstandard »1202 – Gesamthafte Prüfungsplanung« sowie dem IT-Prüfungsstandard »1203 – Durchführungsplanung« der ISACA (vgl. Abschnitt 3.1.2) sowie den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) definiert.

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

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.

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

- Ergebnisse aus vorherigen Prüfungen
- Ergebnisse der Informationssicherheitsanalyse
- Ergebnisse aus Assessments zu operationalen Risiken (OpRisk)
- Ergebnisse aus Assessments zu 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
- Tagesaktuelle Berichte des IT-Security-Teams oder externer Quellen (beispielsweise CERT-Bund)
- 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.

Die Risikoanalyse der potenziell zu prüfenden Objekte sollte dabei *ohne* Beachtung der ggf. implementierten Maßnahmen erfolgen (sog. Brutto-Betrachtung, vgl. hierzu Abschnitt 6.2).

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 fachlichen 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.

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.

Hinweis auf das IT Audit and Assurance Framework (ITAF 4)

Anforderungen bezüglich der Fähigkeiten und Kompetenzen eines Prüfers sind in den IT-Prüfungsstandards »1006 – Expertise« und »1204 – Durchführung und Überwachung« der ISACA (vgl. Abschnitt 3.1.2) sowie den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) definiert.

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.

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 die Leitung 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 Prüfungsfeldes
- 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, regulatorische Vorgaben, Normen, Standards – vgl. Kapitel 3)
- Darstellung wesentlicher Meilensteine/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 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,
- unangemessene Datenmodellierung sowie
- nicht ordnungsgemäßer Betrieb von Anwendung und Infrastruktur.

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 Berechtigungen oder 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 – abgesehen von Prüfungen aufgrund des Verdachts doloser Handlungen – 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 informie-

Prüfungsankündigung		
Input	**Einflussgrößen**	**Output**
◗ Genehmigtes Prüfungskonzept	◗ Prüfungsinhalt ◗ Prüfungsart	◗ Prüfungsankündigung
Aktivtäten	**Werkzeuge**	
◗ Erstellen der Prüfungsankündigung ◗ Information der Betroffenen (Geprüften)	◗ Office-Tools ◗ Spezialisierte Revisionssoftware	

Tabelle 7–2: Input-Output-Beziehung Prüfungsankündigung

ren, 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:

- Grund der Prüfung, z. B. gemäß Revisionsplanung, Sonderprüfung
- Beginn und geplante Prüfungsdauer
- 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,

aus dem beschlossenen Revisionsplan für 2023 kündigen wir die Revisionsprüfung »Berechtigungen – Benutzeranlage und -verwaltung ausgewählter Anwendungen« an.

Die Durchführung der Prüfung findet im 2. Quartal statt. Sofern die Prüfung aus Ihrer Sicht nicht in diesem Zeitraum starten oder durchgeführt werden kann, setzen Sie sich bitte umgehend mit dem Prüfungsleiter in Verbindung.

Schwerpunkt der Prüfung ist die Vorgehensweise bei der Anlage, der Änderung und der Löschung von Zugangs- und Zugriffsberechtigungen. Dabei werden auch die Aufgaben der Key-User im Rahmen der Berechtigungsverwaltung sowie die Dokumentationen der dabei durchgeführten Tätigkeiten betrachtet. Ziel der Prüfung ist, festzustellen, ob die Berechtigungsverwaltung innerhalb des Unternehmens bzw. in den einzelnen Organisationseinheiten zeitnah und auf Basis von Richtlinien, Dienstvorschriften und Best Practices nach definierten Prozessen erfolgt. →

Bitte stellen Sie uns vorab Unterlagen per E-Mail zum Prüfungsgebiet zur Verfügung, u. a. geltende Richtlinien, Regelungen, Handbücher oder Dokumente.

Im Rahmen des Kick-off-Termins wird sich das Prüfungsteam bei Ihnen vorstellen, die Zielsetzung der Prüfung, das geplante Vorgehen und die Erwartungen mit Ihnen erörtern. Zur Vereinbarung des Kick-off-Termins wird sich das Prüfungsteam mit Ihnen in Verbindung setzen.

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 werden kann, sind im Rahmen der Voruntersuchung die Prüfungshandlungen sowie alle dazu notwendigen ergänzenden Schritte 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 Prüfungshandlungen und die dazu notwendigen ergänzenden Schritte durch die Prüfer inhaltlich und zeitlich zu planen und in einem Arbeitsprogramm (Prüfungsprogramm) zu dokumentieren (vgl. Abschnitt 2.5.7).

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 ◗ Prüfungsankündigung	◗ Detaillierungsgrad des Prüfungskonzeptes ◗ Prüfungsart	◗ Prüfungsprogramm (Arbeitsprogramm)
Aktivtäten		**Werkzeuge**
◗ Planung der Prüfungshandlungen sowie aller dazu notwendigen ergänzenden Schritte ◗ Durchführung des Kick-off-Meetings ◗ 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		◗ Planungs- und Projektmanagement-Tools ◗ Office-Tools ◗ Spezialisierte Revisionssoftware

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 die 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 des Prüfungskonzepts, 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 darunter liegenden IT-Prozesse und IT-Infrastruktur notwendig ist, 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 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 mögliche 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.

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

Datum und interne Audit-Nr: 18.-20 Juni, 2020, _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/Corr2:2015

Audit 1. Tag

Datum	Ort/Land	Zeit	Auditor	Themen	Dokumente	Verant-wortlich
18. Juni 2020	Stuttgart, Deutschland	9:00 – 10:30		*Einführungsrunde*	Unternehmensstrategie, Kundenzufriedenheit, Managementbewertung	GL, QMB, alle Prozessverant-wortlichen
		10:30 – 12:30	Frau A, Herr B, Herr C	*Prüfungsfeld »Governance/ Compliance – Strategie«*	Sicherheitsrichtlinie, Auditberichte, Korrektur- und vorbeugende Maßnahmen	ISMS-Manage-rin, 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-Manage-rin, QMB, Risk-Managerin
		15:00 – 16:00		*Prüfungsfeld »Personal«*	Richtlinien	Personalabtei-lung, Bereichs-leiter
				...	…	…
		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 2.5.6) 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 dessen 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-Charta) das Recht, alle notwendige Dokumente und andere 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
   - Nimm 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« 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.

7.3.1 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.

Die Abarbeitung des Arbeitsprogramms ist detailliert und nachvollziehbar zu dokumentieren (siehe Abschnitt 7.5).

Abbildung 7–4: Prüfungsdurchführung

Prüfungsdurchführung		
Input	**Einflussgrößen**	**Output**
◗ Prüfungsprogramm (Arbeitsprogramm)	◗ Prüfungsart ◗ Prüfungsziele	◗ Dokumentation der Abarbeitung des Arbeitsprogramms ◗ ggf. Präzisierung des Arbeitsprogramms ◗ Dokumentation der Feststellungen
Aktivtäten		**Werkzeuge**
◗ Datenprüfungen ◗ Interviews ◗ Dokumentensichtungen ◗ Konkretisierung der Prüfungsverfahren und Prüfungsziele ◗ erste Beurteilungen ◗ erste Abstimmungen		◗ Vorgehens- und Referenzmodelle ◗ Prüfungs- und Revisionstools ◗ Data-Mining-Tools und Datenbanktools ◗ Interviewtechniken ◗ Checklisten ◗ Office-Tools ◗ spezialisierte Revisionssoftware

Tabelle 7–4: Input-Output-Beziehung Prüfungsdurchführung

Hinweis auf das IT Audit and Assurance Framework (ITAF 4)

Weitere Anforderungen an die Abarbeitung des Arbeitsprogramms und deren Dokumentation sind in folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) sowie den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) definiert:

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

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.

7.3.2 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 kann auch Excel oder eine SQL-Schnittstelle ausreichend sein. Bei komplexeren Sachverhalten oder bei größeren Datenmengen sind spezielle Datenanalysetools für die Revision sinnvoll[1], wie etwa Audicon IDEA, audimex oder Galvanize Analytics, 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 Data-Mining-Software eingesetzt werden[2].

7.3.3 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),
- 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.

7.3.4 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 erstellt (vgl. Abschnitt 7.5) oder seine Prüfungsdokumentation der Revision übergeben muss.

7.3.5 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.

Negative Feststellungen beschreiben Mängel. Sie werden in der Regel in verschiedene Klassen eingeteilt. Beispielsweise macht die IDW-PS-400er-Reihe hierzu Vorgaben. Die BaFin hingegen unterscheidet von F0, keine Mängel, bis F4, schwergewichtige Mängel. Einige Banken verwenden hingegen eine davon abweichende Systematik auf Basis der Erläuterungen zur »Abstufung der Mängel zu MaRisk, BT 2.4«:

- Geringer Mangel
- Mittlerer Mangel
- Wesentlicher Mangel
- Schwerwiegender Mangel
- Besonders schwerwiegender Mangel

1 Diese Programme zählen zu den sog. Computer Assisted/Aided Auditing Techniques (CAAT).

2 Zur Datenanalyse ist ein Leitfaden der ISACA erschienen: *https://www.isaca.de/veroeffentlichungen/datenanalyse.*

Bei schwerwiegenden und besonders schwerwiegenden Mängeln muss die Revision gemäß MaRisk unverzüglich der Geschäftsleitung einen Bericht vorlegen.

Ebenso ist die Verwendung einer dreistufigen Gliederung der Feststellung/Mängel möglich:

- Geringer Mangel
- Größerer Mangel
- Wesentlicher Mangel

Vielfach wird die Bedeutung einer Feststellung auch mit dem Empfängerkreis des Berichtsinhalts verknüpft. So kann etwa zwischen Feststellungen unterschieden werden, die lediglich an die Unternehmensleitung weitergegeben werden, und solchen, die auch oder in besonderen Fällen (Fraud) sogar exklusiv an die Aufsichtsorgane übermittelt werden.

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.

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.

Besonders schwerwiegende Mängel sind z. B. massive, regelmäßige oder bewusste Verstöße gegen gesetzliche Bestimmungen, darunter fallen dolose Handlungen. Aber auch unerkannte Schwachstellen in wesentlichen Anwendungen oder allgemein unzureichende Maßnahmen zur Behandlung wesentlicher Risiken zählen dazu. Etwa das Fehlen eines Notfall- oder Datensicherungskonzeptes 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.

Die Klassifikation von Feststellungen geschieht häufig in Tabellenform (vgl. beispielhaft Tabelle 7–5).

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 2020	Noch nicht begonnen
2	Sehr hoch	27001	A 9.4	Keine Zugangskontrolle implementiert	Net Admin	Bis Ende August 2020	Noch nicht begonnen
3	Hoch	27001	A 15.2	Nicht alle Lieferanten werden geprüft	Beschaffung	Bis Ende September 2020	Noch nicht begonnen
4	Sehr hoch	27001	A 12.3	Backup-Bänder und -DVDs werden im Serverraum aufbewahrt	Net Admin	Bis Ende Juni 2020	Noch nicht begonnen

Tabelle 7–5: Praxisbeispiel für Feststellungen aus einer Prüfung

7.4 Abstimmung

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

1. Inhaltliche Verifizierung der Feststellungen mit dem geprüften Bereich
2. Revisionsinterne Abstimmung des Berichtsentwurfs
3. Abstimmung des Berichtsentwurfs mit dem geprüften Bereich

Die **erste Phase** (inhaltliche Verifizierung der Feststellungen mit dem geprüften Bereich) 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.

Abbildung 7–5: Prüfungsdurchführung – Abstimmung

Abstimmung		
Input	**Einflussgrößen**	**Output**
◗ Dokumentation der Feststellungen ggf. mit (ersten) Beurteilungen	◗ ---	◗ Abgestimmte Feststellungen ◗ Abgestimmter Prüfungsbericht
Aktivtäten		**Werkzeuge**
◗ Verifizierung der Inhalte der Prüfungsdokumentation ◗ Revisionsinterne Abstimmung der Inhalte ◗ Abstimmung der Inhalte mit den Geprüften		◗ Interviewtechniken ◗ Office-Tools ◗ Spezialisierte Revisionssoftware ◗ Web- oder Groupware-Lösungen

Tabelle 7–6: Input-Output-Beziehung Abstimmung

Die **zweite Phase** (revisionsinterne Abstimmung des Berichtsentwurfs) 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. Eventuell erfordert der Prozess auch die Freigabe einer unabhängigen – revisionsinternen – Qualitätsstelle. Die interne Abstimmung ist unter anderem aus folgenden Gründen notwendig:

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

Ist der Prüfungsbericht revisionsintern finalisiert, beginnt als **dritte Phase** (Abstimmung des Berichtsentwurfs mit dem geprüften Bereich) 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 allerdings nicht die Bewertung der Feststellungen.

Hierbei ergibt sich zudem die Möglichkeit, Maßnahmen zur Verringerung (sog. »Mitigation«) aufgedeckter 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, Arbeitspapiere)
- Prüfungsbericht (ggf. mit Anlagen)

Hinweis auf das IT Audit and Assurance Framework (ITAF 4)

Anforderungen an die Berichterstattung und Dokumentation sind in folgenden IT-Prüfungsstandards der ISACA (vgl. Abschnitt 3.1.2) sowie den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) 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.

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

Praxishinweis

Alle im Rahmen der Prüfung erstellten Dokumente (einschließlich Nachweisen) 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).

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 einem einprägsamen Muster durchgängig und eindeutig benannt werden. Nur so sind zudem eine eindeutige Zuordnung zum Thema und eine klare Referenzierung in Arbeitsprogrammen möglich.

Abbildung 7-6: Prüfungsdurchführung – Berichterstattung und Dokumentation

Praxishinweis
Referenzierungsschema für Dokumente bei Ablage im Dateisystem

- [Referenznummer Basisordner ##].[laufende Dokumentenreferenz ##]_[pbc oder wp für die Art des Dokuments]_[Dateiname]_[Versionsnummer #.#]
  Beispiel für die Dateibenennung des Prüfprogramms im Ordner A2 gemäß der nachfolgenden Ordnerstruktur: A2.01_wp_Arbeitsprogramm_Beschaffung_v0.4
- Die laufende Nummer – im Beispiel »01« – 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: A2.01a_pbc_Benutzerantrag_Deu.pdf und A2.01b_pbc_User_Registration_Request_Eng.pdf
- Die Versionierung sollte nur für eigenerstellte Dokumente erfolgen. Für erhaltene Dokumente sollte der Originaldateiname beibehalten werden.
- Um Arbeitsdokumente von erhaltenen Prüfungsnachweisen unterscheiden zu können, hat es sich in der Praxis bewährt, nach der Referenz »pbc« für »prepared by client« oder »wp« für »working paper« in den Dateinahmen mit aufzunehmen.

Die Versionen werden nach folgender Regel verwaltet:

- Hauptversion(en): #.m
- Nebenversionen: n.#
- 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.

Praxishinweis

Auch wenn vielfach Daten noch direkt im Dateisystem abgelegt werden, erlauben es aktuelle Kollaborationssysteme wie beispielsweise Microsoft Sharepoint, Dateien unterschiedlicher Typen über die Metadaten in Bibliotheken zu verwalten, was zahlreiche Vorteile mit sich bringt (beispielsweise differenziertere Zugriffsregelungen und Protokollierungen) Eine Benennung bzw. Referenzierung der Dateien ist in dem Fall nicht notwendig, setzt aber ein durchgängiges Schema für die Metadaten voraus. Diese können z. B. die automatische Versionierung, die Kategorie wie Arbeitsdokument oder Prüfungsnachweis, der Status der Datei wie Entwurf oder Final sein. Benutzer, Erstellungsdatum oder auch das Datum der letzten Änderung werden durch derartige Systeme automatisch je Datei erfasst.

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 abgelegt:

/ A_Prüfungsvorbereitung
  / A1_Ankündigung
  / A2_Prüfprogramm
  / A3_Kick-off
  / A4_Zeitplan & Räume
/ B_Prüfungsdurchführung
  / B1_Interviewdokumentation
  / B2_Kommunikation
  / B3_Erhaltene Unterlagen
/ C_Berichterstattung
  / C1_Berichtsentwurf intern
  / C2_Review & Abstimmung
  / C3_Durchsprache Bereiche & Stäbe
  / C4_Schlussbesprechung
  / C5_Finaler Bericht
/ D_Wissen
/ Z_Archiv

- A_Prüfungsvorbereitung: Dokumente wie z. B. Prüfungsankündigung, Prüfprogramm, Offene-Punkte-Listen, Listen der Ansprechpartner, Planungsunterlagen für den Teameinsatz bei größeren Prüfungen usw.
- B_Prüfungsdurchführung: Neben der Interviewdokumentation und Kommunikation die verarbeiteten Dokumente wie z. B. bereitgestellte Richtlinien, Verfahrens- oder Prozessbeschreibungen oder sonstige Nachweise, die für die Prüfung herangezogen werden.
- C_Berichterstattung: Berichtsentwürfe und der finale Bericht sowie ggf. Freigabedokumente
- D_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.

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 – insbesondere mit Blick auf die Feststellungen –

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

sein, um seine Botschaft eindeutig 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 Fachbegriffe 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.

Ein überzeugender Prüfungsbericht sollte über Mängel bzw. Schwachstellen von Prüfungsobjekten und nicht über Personen berichten. Ausnahmen sind etwa bei Sonderprüfungen im Zusammenhang mit Fraud und anderen Prüfungen aufgrund eines auf eine konkrete Person oder Personengruppe bezogenen Verdachts denkbar.

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 2013, 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 nennen.

- **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 6.2). 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). Es wird gefordert, dass das Ergebnis der Ursachenanalyse und die Beseitigung der Abweichung/des Mangels nachzuweisen sind. 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.

8 Follow-up

Unter Follow-up wird die Nachverfolgung/die Überwachung der Erledigung von Prüfungsbemerkungen verstanden. Idealerweise erfolgt diese Nachverfolgung softwaregestützt.

Hinweis auf das IT Audit and Assurance Framework (ITAF)

Anforderungen an das Follow-up sind im IT-Prüfungsstandard »1402 – Nachschau« der ISACA (vgl. Abschnitt 3.1.2) sowie in den korrespondierenden Guidelines (vgl. Abschnitt 3.1.3) definiert.

Mit Übergabe der finalen Fassung des Prüfungsberichts 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 es Prüfungsberichtes mit den geprüften Bereichen vereinbarten Maßnahmen zur Behandlung aufgedeckter Risiken nachvollziehbar umgesetzt worden sind. Erst dann kann davon ausgegangen werden, dass die Mängel beseitigt wurden. Je nach Art und Grad einer Feststellung 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 und zusätzlich im Fall der Bereitstellung notwendiger Ressourcen bei der Unternehmensleitung, 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 Feststellung ist von dem Fachbereich gegenüber der Revision nachzuweisen, ggf. in einer Nachprüfung durch die Revision.

Die Beseitigung einer als geringfügig eingestuften Feststellung, die 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 einer Feststellung 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 und Eignung der Analyse und der Gegenmaßnahmen für ausgewählte (i.d.R. als wesentlich bewertete) Mängel und bestätigt die erfolgreiche Beseitigung bzw. weist auf weiter bestehende 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 Feststellungen wirksam, umfassend und nachhaltig zu beseitigen. Dies ist durch den geprüften Bereich auch nachzuweisen.

Je nach Organisationsform der IT-Revision erfolgt das Follow-up

- 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 Risiko kann die Prüfung der Beseitigung einer Feststellung materiell oder auf Basis einer Mitteilung erfolgen. Bei einer Nachschau der Beseitigung der Feststellung führt der Prüfer ggf. weitere Prüfungshandlungen durch, um sich zu vergewissern, dass das Risiko, das der Feststellung zugrunde liegt, durch entsprechende Maßnahmen tatsächlich reduziert wurde.

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 31000:2018 und ISO/Guide 73:2009 als **Restrisiko** (Residual Risk, Abschnitt 3.8.1.6) bezeichnet.

Dieses Restrisiko hat der Prozesseigner im Rahmen seiner **Risikoübernahme** in einer Genehmigungsvorlage darzustellen und 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.

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

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.

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.

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

- ISO 19011:2018 – Leitfaden zur Auditierung von Managementsystemen (Guidelines for auditing management systems)

zu befassen.

COBIT 5 for Assurance

In der COBIT-2019-Produktfamilie existiert noch keine aktualisierte Veröffentlichung zu Assurance-Aspekten. Die ISACA-Publikation »COBIT 5 for Assurance« kann daher noch immer uneingeschränkt genutzt werden. Sie 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 2013]):

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

»COBIT 5 for Assurance« baut auf der Hauptpublikation COBIT 5 auf. »COBIT 5 for Assurance« erfordert jedoch nicht unbedingt Kenntnisse der 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 des »COBIT 5 for Assurance« (vgl. [ISACA 2013]).

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

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

10 Ausblick

10.1 Ein Blick in die Zukunft der IT-Revision

Die Welt der IT und somit auch die Welt der IT-Revision hat sich in den letzten Jahren stark verändert: von fast ausschließlichen On-Premises-Systemlandschaften hin zu Cloud-Dienstleistungen, häufig durch Hyperscaler bereitgestellt. Manuell gepflegte Excel-Sheets werden von KI-Lösungen verdrängt, die beispielsweise in der Lage sind, durch fortwährendes Lernen ohne menschliche Mitwirkung in Millisekunden Entscheidungen zu treffen. Der Wandel ist unaufhaltsam und erfasst jeden Tag neue Bereiche. In regulierten Branchen ist er den Vorgaben stets voraus. Dass auch in der neuen Welt die Ziele und Vorgaben der Unternehmen sowie zentrale Aspekte der Informationssicherheit und des Datenschutzes eingehalten werden müssen, stellt insbesondere die IT-Revision und alle im Drei-Linien-Modell zusammenarbeitenden Parteien damit jeden Tag vor neue Herausforderungen.

Jede Einführung einer neuen Technologie bedeutet für die Unternehmen Veränderung auf vielen Ebenen. Sie muss zum einen vorgabenkonform erfolgen und mögliche spätere Anpassungen in relevanten Vorgaben vorausdenken. Sie darf zum anderen keine neuen wesentlichen Risiken in die Unternehmen tragen, sonst besteht die Gefahr, dass größere, meist zeit- und kostenintensive Nachjustierungen notwendig werden oder gar wesentliche Feststellungen Ergebnis einer Prüfung sind.

Gerade mit Blick auf eine zunehmende Regulatorik in fast allen Branchen ist eine fortlaufende Zusammenarbeit mit den Regulierungsbehörden von beidseitigem Interesse, denn beide Partner verfolgen das gleiche Ziel der fortlaufenden Verbesserung des Unternehmens.

Damit sich ein Unternehmen weiterentwickeln kann, muss kontinuierlich in geringe Fluktuation, ein motivierendes Arbeitsumfeld und die Aus- und Weiterbildung des Personals investiert werden. Nur auf diesem Weg ist sichergestellt, dass das benötigte Wissen zum benötigten Zeitpunkt im Unternehmen verfügbar ist und zielorientiert angewandt wird. Das gilt auch für die IT-Revision.

Nur dann ist die IT-Revision auch künftig in der Lage, den technologischen Fortschritt zu beobachten und zu bewerten. Hierzu sollen Unternehmen Prozesse für die IT-Revision etablieren, mit denen neue Entwicklungen im oder für den Revisionskontext am Markt identifiziert, hinsichtlich der Risiken und Chancen bewertet und – bei Eignung – in die eigenen Arbeitsprozesse integriert werden können, etwa der Einsatz von Softwarerobotern oder künstlicher Intelligenz. Häufig wird für die Innovationsverfolgung und -koordination eine zentral angeordnete Organisationseinheit eingerichtet, die von allen Abteilungen, einschließlich der Revision, fachlich unterstützt wird.

Ein zur Technologieidentifikation und -bewertung passender Prozess, dessen Schritte 1 und 2 modifiziert auch in der IT-Revision Anwendung finden könnten, kann beispielsweise aus drei Schritten bestehen:

Schritt 1: Identifikation
Eine regelmäßige Sondierung des Marktes durch ein interdisziplinäres, ggf. sogar unternehmensübergreifendes Analystenteam mit hoher Branchen- und Berufserfahrung oder durch beauftragte Analysen von spezialisierten Marktforschungsunternehmen gibt Aufschluss über aktuelle Trends und wie deren weitere Entwicklung aussehen könnte. Hieraus lassen sich einerseits mögliche Business Cases für ein Unternehmen entwickeln, andererseits frühzeitig Risiken und Chancen aus der Revisionsperspektive erkennen.

Schritt 2: Bewertung
Anhand der in Schritt 1 gesammelten Daten kann das Team unter beratender Hinzuziehung der IT-Revision und Beachtung ihres Unabhängigkeitsgebots bewerten,

- welchen wirtschaftlichen Nutzen das Unternehmen daraus generieren kann,
- welcher Aufwand für Einführung und Betrieb einschließlich einer dauerhaften Fortführung entstehen würde und
- ggf. welche regulatorischen Anforderungen in diesem Kontext bestehen oder bald verabschiedet werden könnten.

Schritt 3: Integration
Nach Abschluss der Schritte 1 und 2 und der unternehmerischen Entscheidung, die Technologie im Unternehmen einzuführen, soll auf etablierte und weitgehend standardisierte Prozesse des Change-, System- und Servicemanagements zurückgegriffen werden.

Die IT-Revision hat durch dieses Vorgehen den Vorteil, von Anfang an beobachtend und unter Wahrung ihrer Unabhängigkeit beratend mitwirken zu können. Parallel kann so für Prüfungen zwingend benötigtes Erfahrungswissen aufgebaut werden.

Für die IT-Revision bedeutet dies vor allem, Wissen aufzubauen und zu versuchen, Entwicklungen im Sinne der bestmöglichen Risikobeherrschung frühzeitig zu erkennen.

10.2 Prüfungen unter Pandemiebedingungen

10.2.1 Veränderte Bedingungen

Die Fähigkeit, Entwicklungen vorauszusehen und mit Erfahrungswissen eine bestmögliche und frühzeitige Risikobeherrschung anzustreben, hilft nicht zuletzt bei der Beherrschung einer vollkommen neuartigen Situation (ein sog. »schwarzer Schwan«), wie sie zu Beginn des Jahres 2020 durch das neuartige SARS-CoV2-Virus entstanden ist.

Die von diesem Virus ausgelöste Corona-Pandemie führte zu weltweiten Auswirkungen auf die Unternehmen und ihre Umwelt und damit auch auf die Arbeit der Internen Revision. Die vielfach durch Vor-Ort-Prüfungen und direkte Kommunikation zwischen Prüfenden und Geprüften geprägte Arbeit wurde »über Nacht« vollständig verändert. Insbesondere Prüfungshandlungen wie Aufnahme von Beständen und Begehungen von Gebäuden, teilweise verbunden mit Reisen zu anderen Standorten, sind in gewohnter Form nicht möglich. Denn für die Prüfenden entstehen gesundheitliche Risiken, wenn sie an entfernte Unternehmensstandorte reisen, oftmals können in solchen Situationen auch Risiken im Kontext einer erschwerten Rückkehr entstehen. Manches muss also ruhen, manches kann durch den Einsatz von teilweise etablierten, teilweise neuartigen Technologien, die jetzt im Prüfungskontext eingesetzt werden, weitergeführt werden. Der Jahresprüfungsplan wird sich dadurch in den meisten Fällen verändern, weil Prüfungen entfallen und/oder hinzukommen.

Mit der Unternehmensleitung sollte besprochen werden, welche Sicherheit und Gewissheit sie von der IT-Prüfungsfunktion erwartet. Dieses Vorgehen kann eine bedarfsgerechte Akzeptanz der Prüfungsthemen unterstützen. Zudem muss geklärt werden, ob und in welcher Weise das bislang bestehende Vorgehensmodell modifiziert werden muss und welche Prüfungstools eingesetzt werden sollen oder müssen – und welche in keinem Fall verwendet werden dürfen.

Die fehlende Möglichkeit der Interaktion zwischen Prüfer und Geprüftem in Form eines realen Treffens ist eine der Hauptherausforderungen. Sie kann zu Unsicherheiten und Fragen führen, wenn die Beteiligten sich nicht »live« sehen können. Gestik und Mimik fehlen in der Kommunikation. Gespräche und Interviews, die sonst »vor Ort« stattgefunden hätten, sind über Telefonkonferenz-Werkzeuge jedoch gut substituierbar, teilweise auch, indem ein Kamerabild der Beteiligten hinzugenommen wird. Problematisch wird es hingegen, wenn keine virtuellen Meeting-Plattformen eingesetzt werden können oder wenn die Vermittlung von Gestik und Mimik trotz des Einsatzes solcher Systeme eingeschränkt ist, etwa wegen schlechter Verbindungsqualität.

10.2.2 Methoden der Remote-Prüfung

Sämtliche Methoden, die eine Prüfung aus der Ferne (Remote) ermöglichen, kommen zum Einsatz. Zentral dabei ist, dass die gesamte Revision in konsistenter Form auf die veränderte Situation reagiert, Methoden also einheitlich und unabhängig vom Prüfungsteam angewandt werden. Das wichtigste Werkzeug ist dabei die Arbeit mit einer virtuellen Meeting-Plattform wie zum Beispiel Microsoft Teams, Skype, WebEx etc. Die Einhaltung gesetzlicher Vorgaben (z. B. Datenschutz) und IT-Sicherheitsanforderungen (z. B. Wahrung der Vertraulichkeit) ist vorab zu prüfen. Mit dem geprüften Bereich kann ein Interview über diese Plattform geführt werden. Der Austausch mit dem Geprüften findet über das gegenseitige Teilen von Bildschirminhalten statt.

Wenn Prozesse erläutert werden, erstellt der Prüfer in Absprache mit dem Geprüften entsprechende Screenshots vom Bildschirm mit einem Snippingtool. Diese werden im Nachgang vom Prüfer ggf. noch textlich erläutert und dienen als Prüfungsdokumentation.

Für das Ziehen von Stichproben beantragt der Prüfer entsprechende Systemzugänge mit einer reinen Leseberechtigung. Er ist dann in der Lage, die Stichprobe selbstständig zu ziehen. Sollte ein Systemzugang nicht möglich sein, hat der Prüfer die Option, die Stichprobe live vom Administrator ziehen zu lassen, wenn der Administrator während des Vorgangs seinen Bildschirm teilt. Der Vorgang wird anhand von Screenshots entsprechend dokumentiert. Die Datenextrakte sind dann unmittelbar an den Prüfer zu senden.

Problematisch kann es zudem werden, wenn Vor-Ort-Begehungen notwendig sind, etwa im Kontext der Prüfung von Rechenzentren. Um die sonst übliche Begehung nicht für einen längeren Zeitraum aussetzen oder verschieben zu müssen, kann unter Umständen und unter Beachtung aller datenschutzrelevanten Vorschriften sowie in Abwägung mit zentralen Informationssicherheitszielen eine kamerabasierte Begehung erwogen werden. Dabei handelt ein Team, das vor Ort arbeitet, auf Anweisung des Prüfenden und nutzt hierzu eine hochwertige Kamera-Ausrüstung. Die Prüfenden sind so in der Lage, durch »Lenkung« des Teams bestimmte Aspekte zu begutachten, etwa auch über Nahaufnahmen. Eine andere Möglichkeit besteht in der Anforderung von Bildaufnahmen. Auch zu ihrer Erstellung könnten Dritte beauftragt werden, die aus ganz anderen Gründen an den zu prüfenden Standort reisen müssen. Sie sind damit häufig neutraler als das unmittelbar vor Ort tätige Personal. Nur wenn die Wahrung der

Vertraulichkeit höher wiegt als die Erstellung eines Prüfungsnachweises, sollte auf solche Methoden verzichtet werden.

In jedem Fall bieten Fragebögen/Checklisten entsprechende Unterstützung unter Beachtung ihrer Limitationen, wie etwa eine suggerierte Vollständigkeit.

Viele andere Prüfungshandlungen, wie eine Kontrolle des Patch-Managements, die Durchführung von Penetrationstests und Vulnerability-Scans oder die Prüfung von Konfigurationen, können meist problemlos aus der Ferne durchgeführt werden. Allerdings setzt dies die Einrichtung von bislang ggf. nicht vorhandenen Fernzugängen voraus, eine Maßnahme, die selbst wiederum ein Risiko darstellen kann.

Eine Risikobetrachtung ist also auch hier stets zwingend notwendig, und zwar sowohl aus Sicht des Unternehmens als auch der Prüfenden. Risiken für das Unternehmen können entstehen, wenn Prüfungen verschoben werden, sie können aber auch durch die Hinzunahme von neuen Technologien oder Prüfungshandlungen entstehen, die aus der Ferne durchgeführt werden.

Grundsätzlich gilt, dass ausgefallene Prüfungen zu einem späteren Zeitpunkt, meist innerhalb einer üblichen 3-Jahres-Frist, nachgeholt werden müssen. Aktuell planen viele Unternehmen daher ihre Prüfungen neu. Andererseits können mitunter auch Teile einer Prüfung sofort durchgeführt werden, andere wiederum werden auf einen späteren Zeitpunkt verschoben. Beispielsweise kann die im Kontext von Jahresabschlussprüfungen durchgeführte dokumentenbasierte Aufbauprüfung wie geplant durchgeführt werden. Die gesprächsbasierte Funktionsprüfung jedoch wird auf einen späteren Zeitpunkt verlegt.

Insgesamt erfordert die Durchführung der Prüfungshandlungen aus der Ferne eine klare Prüfungsstruktur und eine transparente Interviewführung in den virtuellen Besprechungen. Hier kann eine Regieanweisung, wie nachfolgend beschrieben, als Interviewleitfaden dienen.

10.2.3 Playbook

Unter einem Playbook wird einer Regieanweisung zur Strukturierung der virtuellen Besprechung verstanden. Es kann aufbauend auf den folgenden Hinweisen individuell für den jeweiligen Prüfungskontext erstellt werden, beispielsweise mit Festlegung von Zeitlimits, Teilnehmerkreis und anderen wichtigen Eckpunkten:

1. Die Prüfer zeigen sich im Videomodus, um Gestik und Mimik einsetzen zu können.
2. Zu Beginn präsentiert sich das Prüferteam kurz, anschließend stellen sich alle Teilnehmer vor.
3. Anschließend wird ein Chatmoderator bestimmt, der Wortmeldungen und Kommentare überwacht.
4. Zur Dokumentation aller prüfungsrelevanten Elemente, insbesondere Prozessbeschreibungen, wird darum gebeten, den Bildschirm zu teilen, damit Prüfungsnachweise anhand von Screenshots erstellt werden können.
5. Interviewfragen und benötigte Prüfungsnachweise werden visualisiert.
6. Das Meeting schließt mit einer kurzen Zusammenfassung und einem Ausblick der nächsten Schritte.

10.2.4 Nach der Pandemie ist vor der Pandemie

Ein Teil der gewonnenen Erfahrungen und Arbeitsweisen kann – und wird – sich sicherlich zum Vorteil der Unternehmen dauerhaft etablieren und erhöht so die Resilienz der Organisation für künftige Fälle dieser Art.

Digitalisierung muss und wird auch in die (IT-)Revision verstärkt Einzug halten. Insbesondere ein noch deutlich verstärktes, interdisziplinäres kollaboratives Arbeiten unter Nutzung entsprechender Werkzeuge lässt die Unternehmen künftig ähnliche Situationen leichter bewältigen. Und es bleibt zu vermuten, dass eine solche Situation wie die aktuelle nicht die letzte Situation gewesen ist – wenn auch (hoffentlich) nicht in dieser Dimension.

Abkürzungsverzeichnis

ACL	Access Control List / Audit Command Language
AG	Aktiengesellschaft
ANSI	American National Standards Institution
AT	Attestation Standard
AO	Abgabenordnung
BAIT	Bankaufsichtliche Anforderungen an die IT
BCM	Business Continuity Management
BCMS	Business Continuity Management System
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
CCAG	Collaborative Cloud Audit Group
CERT	Computer Emergency Response Team
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
CSA	Cloud Security Alliance
CSDC	Computer Science and Digital Communications
DIIR	Deutsches Institut für Interne Revision e.V.
DRP	Disaster Recovery Plan
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
EnWG	Energiewirtschaftsgesetz
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
GAIT	Guide to the Assessment of IT Risk
GmbH	Gesellschaft mit beschränkter Haftung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
GTAG	Global Technology Audit Guide
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
IKT	Informations- und Kommunikationstechnologie
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
KAIT	Kapitalverwaltungsaufsichtliche Anforderungen an die IT
KG	Kommanditgesellschaft
KI	Künstliche Intelligenz
KWG	Kreditwesengesetz
LA	Lead Auditor
MaRisk	Mindestanforderungen an das Risikomanagement
NPO	Non-Profit Organization
OHG	Offene Handelsgesellschaft
OpRisk	Operationelle Risiken
OWG	Ordnungswidrigkeitengesetz
PCI DSS	Payment Card Industry Data Security Standard
PLZ	Postleitzahl
PS	Prüfstandard

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
SVS	Service Value System
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TOGAF	The Open Group Architecture Framework
VAIT	Versicherungsaufsichtliche Anforderungen an die IT
VoIP	Voice over IP
ZAG	Zahlungsdiensteaufsichtsgesetz
ZAIT	Zahlungsdiensteaufsichtliche Anforderungen an die IT

Glossar

Wichtige Begriffe im Prüfungskontext sind im laufend aktualisierten ISACA-Glossar sowie in den ISO-Normen hinterlegt. Die jeweils aktuelle Version des ISACA-Glossars ist unter *https://www.isaca.org/resources/glossary#glossr* verfügbar.

Abbildungsverzeichnis

Tabellenverzeichnis

Quellenverzeichnis

Bücher

[AK 2006] AK IT-Revision / AK IT-Revision in Kreditinstituten (Hrsg.): IT-Revision. Erich Schmidt, 2006.

[Amling/Bantleon 2007] Amling, T.; Bantleon, U.: Handbuch der Internen Revision: Grundlagen, Standards, Berufsstand. Erich Schmidt, 2007.

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

[Berwanger/Kullmann 2012] Berwanger, J.; Kullmann, S.: Interne Revision – Funktion, Rechtsgrundlagen und Compliance. 2. Aufl., Springer Gabler, 2012.

[Bungartz 2017] Bungartz, O.: Handbuch Interne Kontrollsysteme (IKS): Steuerung und Überwachung von Unternehmen. Erich Schmidt Verlag, 5. Aufl., 2017.

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

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

[Fröhlich/Swart 2013] Fröhlich, M.; Swart, C.: IT-Prüfungen 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.

[Gaulke 2019] Gaulke, M.: COBIT 2019 – das neue IT-Governance-Modell für die Unternehmens-IT. IT-Governance 29 (2019), S. 3-9.

[Hofmann 1972] Hofmann, R.: Aufgaben und Bedeutung der Internen Revision. Westdeutscher Verlag (Springer Fachmedien Wiesbaden), 1972.

[IDW 2002] Institut der Wirtschaftsprüfer: Abschlussprüfung bei Einsatz von Informationstechnologie. IDW Verlag, 2002.

[IDW 2008] Institut der Wirtschaftsprüfer: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie. IDW Verlag, 2008.

[IDW 2010] Institut der Wirtschaftsprüfer: Die Prüfung von Softwareprodukten. IDW Verlag, 2010.

[IDW 2018] Institut der Wirtschaftsprüfer: IT-Prüfung außerhalb der Abschlussprüfung. IDW Verlag, 2018.

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

[ISACA 2019] COBIT 2019 – Introduction and Methodolgy, Rolling Meadows, 2019.

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

[Knapp 2009] Knapp, E.: Interne Revision und Corporate Governance. 2. Aufl., Erich-Schmidt-Verlag, 2009

[Knoll 2019] Knoll, M.: Praxisorientiertes IT-Risikomanagement. 2. Aufl., dpunkt.verlag, 2019.

[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. Carl Hanser Verlag, 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

Online-Quellen

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

www.isaca.org – Global ISACA Website

www.bsi.bund.de – Bundesamt für Sicherheit in der Informationstechnik

ISACA
Germany Chapter

Ihr Partner für Weiterbildung:
Der ISACA Germany Chapter e. V.

Der deutsche Berufsverband der IT-Revisoren, IT-Sicherheitsmanager sowie IT-Governance-Experten fördert Ihre berufliche Weiterentwicklung durch Examensvorbereitungskurse auf die internationalen Berufszertifizierungen CISA, CISM, CRISC und CDPSE.

Unterstützend bieten wir Ihnen ein thematisch breit gefächertes Zertifikatsprogramm basierend auf dem Rahmenwerk COBIT 2019.

Unser komplettes Kursangebot können Sie auf unserer Webseite **www.isaca.de/seminare** einsehen. Neben Präsenzseminaren bieten wir alle Kurse auch als **Online-Seminare** an.
Für sämtliche Kurse erhalten Sie einen anerkannten Berufsfortbildungsnachweis (sog. CPE-Stunden).