Technische Revision

Leitfaden für ein risikoorientiertes Prüfen von technischen Themen in Unternehmen

DIIR-Arbeitskreis Technical Auditing

Version 1.0 (März 2022)

DIIR Deutsches Institut für Interne Revision e.V.

Vorwort

Die Nichteinhaltung von Gesetzen, Normen und Vorgaben sowie nicht erkannte Risiken können in Unternehmen zu Compliance-Fällen, Imageverlusten, hohen Fehlerkosten oder auch Unfällen führen. Unternehmen müssen Risiken erkennen, um diese mit angemessenen Mitteln zu managen und Schäden entsprechend abzuwehren.

Der DIIR-Arbeitskreis (AK) Technical Auditing hat diesen Leitfaden mit seinen Mitgliedern aus verschiedenen Unternehmen erstellt, um die vielfältigen Erfahrungen zusammenzutragen. Er soll aufzeigen, in welchen Bereichen Risiken auftreten können und wie sie sich systematisch erkennen sowie möglichst effizient und nachhaltig reduzieren lassen. Die enthaltenen Erfahrungen dienen sowohl einer existierenden Revision zur Weiterentwicklung als auch dem Neuaufbau einer (technischen) Revision. Der Leitfaden bietet keinen Anspruch auf Vollständigkeit, da speziell technische Risikoauslöser einem schnellen Wandel unterliegen und sich von Unternehmen zu Unternehmen stark unterscheiden. Hierzu sind in den Unternehmen eine stetige Anpassung und ein thematisches Nachschärfen notwendig.

Den Mitgliedern dieses Arbeitskreises, die an diesem Dokument mitgewirkt haben, wird hiermit großer Dank und Anerkennung ausgesprochen! Ebenso bedanken wir uns für die Unterstützung des DIIR, der diesem Arbeitskreis stets mit Rat und Tat zur Seite steht und die Arbeit an dem Leitfaden durch wichtige Beiträge bereichert hat.

Folgende Mitglieder haben am Leitfaden mitgewirkt:

Dr. Maik Adelt	Bayer AG	maik.adelt@bayer.com
Felix Tölke	BMW AG	felix.toelke@bmw.de
Dr. Marco Meibohm	BMW AG	marco.meibohm@bmw.de
Adrian Neuhart	Borealis AG	adrian.neuhart@borealisgroup.com
Britta Becker	Deloitte Wirtschaftsprüfungsgesellschaft	brbecker@deloitte.de
Stefan Mittler	Deutsche Bahn AG	stefan.mittler@deutschebahn.com
Thorsten Menden	Deutsche Post DHL AG	thorsten.menden@dpdhl.com
Dr. Christian Sames	Osram GmbH	christian.sames@ams-osram.com
Dirk Meissner	Robert Bosch GmbH	dirk.meissner@bosch.com
Michael Vogt	Robert Bosch GmbH	michael.vogt@de.bosch.com
Frank Fautz	Robert Bosch GmbH	frank.fautz3@de.bosch.com

Stefan Gorny	Robert Bosch GmbH	stefan.gorny@de.bosch.com
Thomas Nething	Robert Bosch GmbH	thomas.nething2@de.bosch.com
Ulrich Treche	Salzgitter AG	treche.u@salzgitter-ag.de
Grozdan Sljivic-Matanovic	Schwarz-Gruppe	grozdan.sljivic-matanovic@kauf-land.com
Frank Schöne	Stadtwerke Köln GmbH	f.schoene@StadtWerkeKoeln.de
Thomas Tiemann	Vaillant GmbH	thomas.tiemann@vaillant-group.com
Hendrik Jacobi	Volkswagen AG	hendrik.jacobi@volkswagen.de
Johannes Köttler	ZF AG	johannes.koettler@zf.com

Anregungen zur Aktualisierung des Leitfadens nimmt die AK-Leitung gerne entgegen:

- Thomas Nething (Leiter des Arbeitskreises)
- Stefan Gorny (stellvertretender Leiter des Arbeitskreises)

Inhalt

1 Einleitung, Motivation, Ziele

Die Interne Revision beschäftigt sich mit wirtschaftlichen und rechtlichen Risiken für ein Unternehmen und den hieraus entstehenden potenziellen Schäden für die Gesellschafter. Traditionell stehen deshalb vor allem kaufmännische Themen im Vordergrund. Da bei Unternehmen, die technische Produkte herstellen, technische Dienstleistungen erbringen oder bei denen technische Verfahren zur Leistungserbringung eingesetzt werden, viele der wirtschaftlichen Risiken ihren Ursprung in der Technik haben, ist eine Revision bereits dort anzusetzen. Die meisten Unternehmen, insbesondere aus dem verarbeitenden Gewerbe, der Rohstoffgewinnung, der Energieerzeugung und -verteilung, aber auch Dienstleister wie Verkehrsbetriebe oder der Handel haben die Notwendigkeit erkannt und ihr Prüfungsuniversum um technische Themen erweitert.

Die technisch begründete Risikolage hat sich bei einem Großteil der Unternehmen in den letzten Jahren deutlich verschärft. Prominente Beispiele dafür sind Rückrufaktionen von Produkten, Schadensersatzforderungen, Produkthaftungsfälle oder Bußgelder. Unternehmensintern manifestieren sich technische Risikoauslöser vor allem in hohen Fehlerkosten, Rekursionen oder gescheiterten Entwicklungsvorhaben. Drei Faktoren sind hier maßgeblich:

- Erstens die immer komplexer werdenden Produkte. In vielen Industrien waren mechanische Produkte die Vergangenheit, mechatronische sind die Gegenwart und vernetzte Erzeugnisse werden die Zukunft sein.
- Zweitens treiben neue Technologien wie z. B. Künstliche Intelligenz (KI) sowohl die Erzeugnisse als auch die Verfahren ihrer Entstehung voran. Dadurch werden sowohl neue Produkte oder Funktionen möglich als auch Bestehendes weiter verfeinert, folglich etwa leistungsfähiger, umweltfreundlicher, leichter und kostengünstiger gemacht.
- Drittens werden die Anforderungen an Erzeugnisse oder Dienstleistungen und deren Erbringung immer höher: Kunden erwarten immer mehr, abgegebene Kundenversprechen nehmen zu, Kunden- und Lieferantenaudits untersuchen den Leistungsprozess. Gleichzeitig nimmt die Regelungsdichte durch Gesetze, Standards und Normen ebenfalls zu und nicht zuletzt stellt die Gesellschaft immer höhere, (noch) nicht kodifizierte Erwartungen an Sicherheit und Umweltfreundlichkeit. Unbeherrschte Komplexität oder eine Nichterfüllung von Anforderungen führen zu erheblichen bis hin zu unternehmensbedrohenden Schäden.

Dieser Leitfaden hilft Verantwortlichen und interessierten Mitarbeitern der Internen Revision, eine technische Revisionsfunktion aufzubauen oder diese weiterzuentwickeln. Er gibt

Anregungen, stellt Fragen und zeigt zu Teilen auch Lösungsansätze auf. Ein fertiges Konzept zur Umsetzung ist er jedoch nicht. Dieses ist von dem Verantwortlichen, der die Ausgangssituation und die Zielsetzung kennt, spezifisch für sein Unternehmen auszuprägen.

Der Leitfaden folgt in seinem Aufbau chronologisch dem Prüfprozess. Er startet mit der *Erstellung des technischen Prüfungsuniversums* (Kapitel 2), beschreibt die *Planung und Priorisierung der Prüfungsthemen* (Kapitel 4), die *Planung der konkreten Prüfungen* (Kapitel 5) sowie schließlich die *Prüfungsvorbereitung und -durchführung* (Kapitel 7 und 8). Eingeschoben finden sich an logisch passenden Stellen Kapitel zur *Organisation* und den *Kompetenzen* sowie zu den *Prüfungsarten* (Kapitel 3 und 6).

2 Technisches Prüfungsuniversum

Das Prüfungsuniversum der technischen Revision ist eine Teilmenge des gesamten Prüfungsuniversums eines Unternehmens. Prüfungsthemen und Prüfungsobjekte werden nach den gleichen Grundsätzen aus einer Risikobetrachtung heraus abgeleitet.

Die Prüfungsthemen adressieren eine breite Spanne wie die Sicherstellung von wirtschaftlichem Erfolg, Vermögensschutz, Compliance und Reputation. Je nach Industrie liegen diese z. B. in der Produktplanung, den Entwicklungs- und Produktionsprozessen, dem Qualitätsmanagement sowie in weiteren Unterstützungs- und Zentralfunktionen.

Im Prüfungsuniversum sind alle Organisationseinheiten, Standorte und Prozesse enthalten (s. Kapitel 4.3 *Planung der Prüfungsthemen*). Die Prüfungen laufen entweder als Prozessprüfungen oder als Standortprüfungen (z. B. Forschungs-, Entwicklungs- oder Produktionsstandorte) ab (s. Kapitel 6 *Prüfungsarten*).

Zunehmend rücken Themen der Environmental, Social and Corporate Governance (ESG) in den Fokus, die das nachhaltige Agieren in allen Unternehmensbereichen sicherstellen (z. B. Recyclingfähigkeit der Produkte, ressourcenschonende Fertigung oder globale Arbeitsbedingungen). Negative Einflüsse auf die Umwelt (z. B. Emissionen) werden in fortlaufendem Maß von der Gesellschaft nicht mehr akzeptiert. Wichtig hierbei ist es auch, die Umsetzung öffentlich kommunizierter Unternehmensziele zu verfolgen.

Je nach Verteilung der Zuständigkeiten innerhalb der Revisionsabteilung lassen sich zum Betrachtungsumfang der technischen Revision auch die Logistik, die Immobilienbereitstellung oder der Einkauf von Rohmaterialien, Hilfsstoffen, technischen Güter und Dienstleistungen eingliedern. Teilweise ist mit anderen Bereichen der Internen Revision (z. B. kaufmännische Revision, IT-Revision) abzustimmen, wie Schnittstellenbereiche (z. B. Produktionscontrolling, IoT, Cyber Security) zugeordnet werden.

Abbildung 1 hat keinen Anspruch auf Vollständigkeit, gibt jedoch einen Überblick über die ständige Veränderung des technischen Prüfungsuniversums.

Jedes Unternehmen hat ein unterschiedlich ausgeprägtes Risikoinventar, welches es zu ermitteln und stets zu aktualisieren gilt.

Darüber hinaus richten Unternehmen Abteilungen ein, um eine funktionale Verantwortung (2. Linie) in relevanten Themengebieten umzusetzen. Auf diese Weise ergibt sich ein Bezug zur Internen Revision (3. Linie), die im Rahmen ihrer Prüfungen die Wirksamkeit des Risikomanagements und der internen Kontrollsysteme in Angemessenheit, Effektivität und Wirksamkeit bewertet.

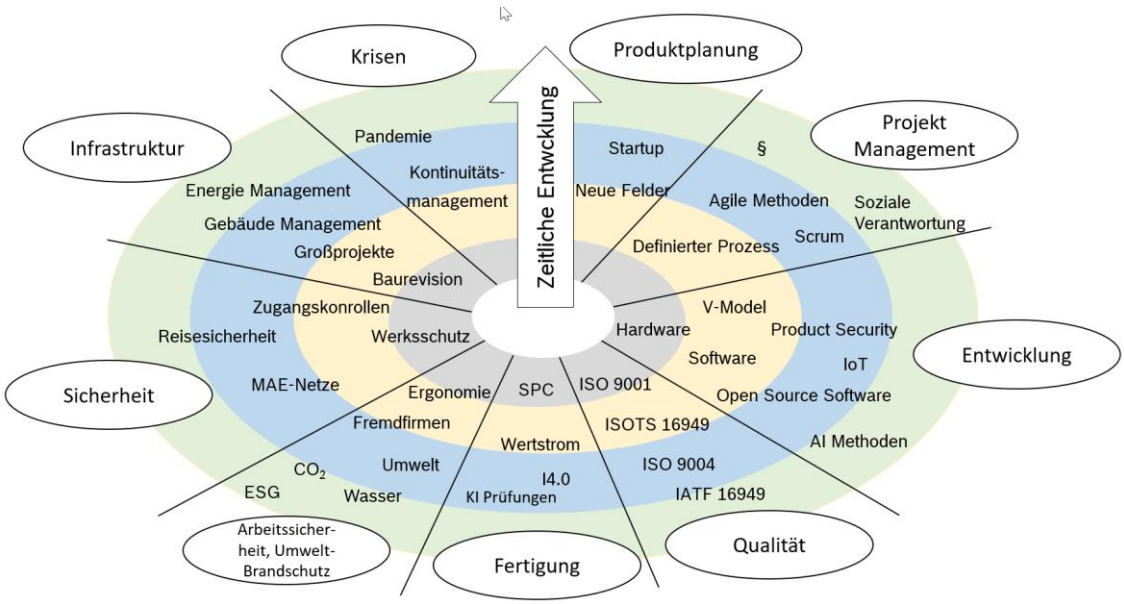


Abb. 1: Volatilität des technischen Prüfungsuniversums

Das Prüfungsuniversum (siehe Abb. 1) der technischen Revision umfasst sowohl Prüfungsthemen, die in der 1. Linie angesiedelt sind, als auch solche in der funktionalen Verantwortung der 2. Linie angesiedelt sind.

Zur Erläuterung dient das folgende Beispiel: Die für funktionale Verantwortung bei „Environmental, Health and Safety (EHS)“ zuständige Zentralstelle legt Regeln für den Brandschutz in Produktionswerken fest und überprüft diese im Rahmen ihrer Verantwortung. Die technische Revision prüft ebenfalls den Brandschutz im Rahmen ihrer Audits (z. B. Brandschutz in einem Produktionswerk). Daneben prüft die technische Revision aufgrund ihrer eigenen Risikobewertung die Zentralstelle, die für das Regelwerk von EHS zuständig ist. Dabei betrachtet sie im Rahmen ihres Audits unter anderem die Effektivität des EHS-Kontrollsystems (z. B. Qualifikation der Auditoren oder die zugehörige KPI-Erfassung).

Welche Prüfungsthemen und -objekte der funktionalen Verantwortung in das Prüfungsuniversum der technischen Revision aufgenommen werden, ist unternehmensspezifisch festzulegen. Eine Arbeitsaufteilung zwischen der Abteilung für funktionale Verantwortung und der Revision ist zulässig und im Sinne der Vermeidung von redundanten Prüfungen sowie möglichst breiter Risikoabdeckung sogar geboten (Alligned Assurance).

Durch externe und interne Einflüsse verändert sich die Risikolage eines Unternehmens über die Zeit. Die technischen Prüfungsthemen sollten die derzeitige sowie die vorhersehbare künftige Risikolage möglichst vollumfänglich abdecken. Beispiele für externe Einflüsse sind geänderte gesetzliche oder gesellschaftliche Rahmenbedingungen, angepasste oder neue Normen, eine sich ändernde Wettbewerbssituation oder sich ändernde marktseitige Anforderungen. Beispiele für interne Einflüsse sind die Änderung des Produkt- oder Technologieportfolios (z. B. IoT, KI), neue Geschäftsmodelle, neue Vertriebswege oder auch hinzugekommene Standorte.

Das überarbeitete technische Prüfungsuniversum ist eine Eingangsgröße für die Jahresplanung der Prüfungen, für die Personalplanung sowie das Kompetenzmanagement.

3 Organisation und Kompetenzen

Es ist gängige Praxis und hat sich bewährt, dass die Revision insgesamt sowohl direkt der Unternehmensleitung unterstellt ist als auch dem Überwachungsorgan bzw. sogar den Gesellschaftern berichtet. Entsprechend sei an dieser Stelle lediglich noch der Hinweis gegeben, wie wichtig der technische Berichtskanal zum Überwachungsorgan ist. Das Überwachungsorgan hat zwei institutionelle Fenster in das Unternehmen: die Unternehmensleitung und die Revision. Aus unseren Erfahrungen ist es überwiegend Praxis, dass bei den zwischen Leitung und Überwachungsorgan diskutierten Themen die technischen nicht immer an erster Stelle stehen. Folglich kommt der technischen Revision die besondere Bedeutung zu, das Überwachungsorgan über die technische Leistungs- und Zukunftsfähigkeit des Unternehmens zu informieren.

Ferner ist die organisatorische Abgrenzung der Revision als 3. Linie im Drei-Linien-Modell zur 2. Linie sicherzustellen. Wo es Überschneidungen von Aufgaben gibt, z. B. bei Audits in der 1. Linie, sollte eine inhaltliche und zeitliche Abstimmung erfolgen, um Redundanzen zu vermeiden.

Dieses Kapitel widmet sich im Folgenden der organisatorischen Einbindung der technischen in die Gesamtrevision sowie der Identifikation und Besetzung der erforderlichen Kompetenzen.

3.1 Technische Revision als Teil der Gesamtrevision

In größeren Unternehmen stellt sich die Frage nach der Aufbauorganisation einer Revision. Aus der Organisationslehre sind unterschiedliche Ansätze bekannt. Die wichtigsten drei werden hier kurz vorgestellt:

- Weit verbreitet ist die funktionale Organisation. Eine technische Abteilung steht hier i. d. R. neben einer kaufmännischen und ggf. einer IT-Abteilung.[1]

[1] Ob IT als Teildisziplin der Technik in der technischen Abteilung anzusiedeln ist, richtet sich i. W. nach den Produkten – stark IT haltige Produkte legen das nahe – und danach, inwieweit die IT-Infrastruktur insgesamt im Risikofokus steht.

- Ist das Unternehmen in stark diversifizierte Unternehmensbereiche unterteilt, so kommt auch in der Revision eine Organisation nach Unternehmensbereichen in Betracht.
- Die dritte Option ist eine Aufteilung nach Wertschöpfungsprozessen (z. B. Verkauf und Marketing, Produktentstehung sowie Leistungserbringung).

Nur in der ersten Variante ist die technische Revision eine eigenständige Abteilung. In den beiden anderen ist sie Teil einer funktionsübergreifenden Einheit, z. B. als technische Gruppe.

Entscheidungsleitend für die Wahl der Aufbauorganisation der Internen Revision ist ein Blick auf die vorherrschenden Prüfungsarten (vgl. hierzu Abb. 2 und Abb. 2.1). Hier werden mit gutem Grund i. d. R. mehrere Prüfungsarten parallel gefahren, etwa Organisations-, Prozess- und Funktionsaudits. Offensichtlich unterstützt eine funktionale Aufbauorganisation Funktionsaudits, da dort die Abstimmung zwischen den Revisionsabteilungen entfällt. Dasselbe gilt auch für die beiden anderen Schnittpunkte entlang der Hauptdiagonalen der Matrix aus Organisation und Prüfungsarten. Überwiegt folglich eine Prüfungsart gegenüber den anderen, kann das ein Hinweis auf eine passende Aufbauorganisation sein. In sämtlichen anderen Konstellationen abseits der Hauptdiagonalen fällt dem jeweiligen Prüfungsleiter die wichtige Aufgabe zu, aus den gegebenen Kompetenzen im Prüfungsteam die bestmögliche Gemeinschaftsleistung herauszuholen.

Es gibt einen Grund, welcher eindeutig für eine funktionale Organisation spricht. Die meisten Mitarbeiter haben durch ihre Ausbildung und berufliche Praxis eine funktionale Heimat. Sie passen entsprechend leichter in eine funktionale als in eine andere Organisation. Auch der Erhalt und der Ausbau von Kompetenz, einer Kernaufgabe jeder Linienorganisation, ist in einer technischen Abteilung besonders vorteilhaft.

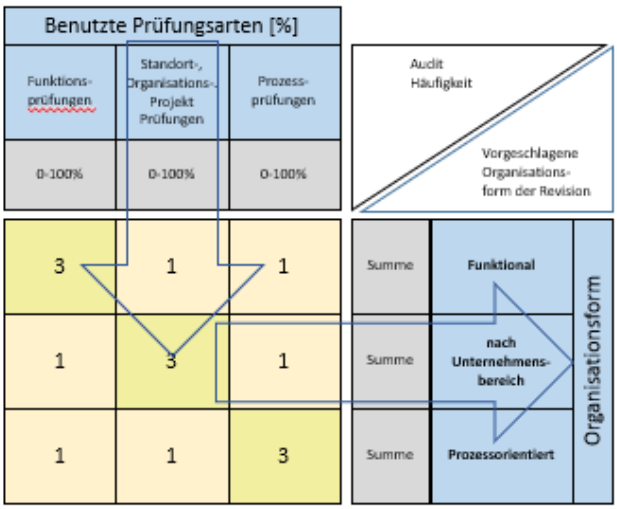


Abb. 2: Bewertungsmatrix zur Entscheidung über die Organisationsform der Revision

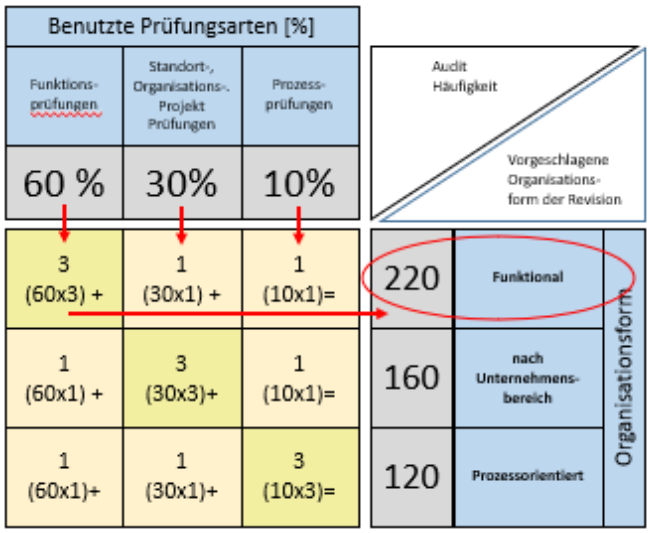


Abb. 2.1: Beispiel zum Zusammenhang von Aufbauorganisation der Internen Revision und typischen Prüfungsarten. Die Ziffern in der Matrix stellen beispielhaft den Zusammenhang zwischen Prüfungsart und Organisationsform dar.

3.2 Identifikation und Besetzung von Kompetenzen

Bei der Besetzung von Prüferstellen stehen drei Kompetenzpfeiler im Vordergrund (vgl. Abb. 3): die technisch fachliche Kompetenz, die Fähigkeit, Risiken aufzudecken und einzuschätzen sowie die Beherrschung von Prüfungstechniken. Eine weiter aufgefächerte Darstellung einschließlich definierter Kompetenzstufen ist im Internal Audit Competency Framework des IIA zu finden (DIIR, 2020).

Technisch fachliche Kompetenz ist jeweils von dem Bewerber in den gesuchten Technikfeldern mitzubringen. Dies ist wichtig, um mit den Geprüften auf Augenhöhe zu kommunizieren und fachlich fundiert, anstatt lediglich formal zu prüfen. Generalisten mit punktuellem Tiefgang sind aufgrund ihrer breiteren Einsetzbarkeit zu bevorzugen. In Unternehmen

mit raschem technologischem Wandel wird eine regelmäßige Weiterbildung und Nachbesetzung dieser Kompetenz erforderlich, ein Spezifikum der technischen Revision. Oft bringen gerade jüngere Mitarbeiter aktuelles Technologiewissen in die Revision ein.

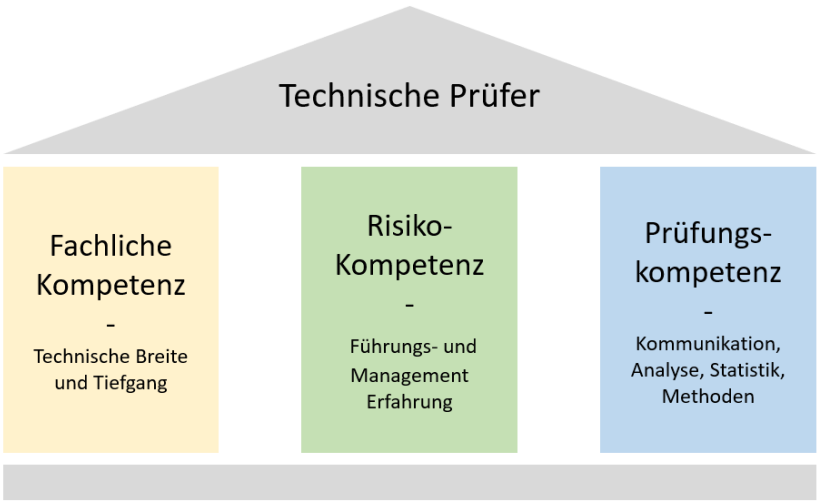


Abb. 1: Die drei Kompetenzsäulen von technischen Prüfern

Zur Identifikation des zur akquirierenden Technologiewissens ist eine regelmäßige Abstimmung mit den „frühen“ Entwicklungsabteilungen (etwa Forschung und Vorausentwicklung) vorzunehmen. Hilfreich sind dafür abgestimmte Technologie- und Produkt-Roadmaps, aus welchen auch die Relevanz fürs Gesamtunternehmen hervorgeht.

Der zweite Kompetenzpfeiler beinhaltet die Fähigkeit, Risiken zu entdecken, sie richtig einzuschätzen und angemessene Vorschläge zur Risikominderung zu tätigen. Dies ist häufig bei erfahrenen Führungskräften anzutreffen. Sie haben es gelernt, an den richtigen Stellen tief zu bohren, und bringen aus ihrer operativen Erfahrung pragmatische Lösungsansätze ein. Eine breite fachliche, idealerweise auch über die rein technische hinausgehende Basis ist dafür hilfreich.

Der dritte Kompetenzpfeiler, die Prüfungstechniken, ist oft bei Fachkräften aus dem Qualitätswesen ausgeprägt. Anders als das Technikwissen sind Prüfungstechniken keine notwendige Einstellungsvoraussetzung, sondern können in der Revision erlernt werden. Dabei sind insbesondere Interviewführung, statistische und datenanalytische Fähigkeiten zu vermitteln. Während die einschlägigen Qualifizierungsprogramme, wie z. B. die Ausbildung

zum Certified Internal Auditor[2] insgesamt stärker kaufmännisch ausgerichtet sind, so können von den vermittelten Prüfungstechniken auch technische Prüfer profitieren.

Diese drei Kompetenzen werden aus den genannten Gründen selten in einer Person in Maximalausprägung angetroffen. In größeren Teams wird folglich durch geeignete personelle Mischung die Gesamtkompetenz sichergestellt. Dies führt i. d. R. auch zu einer Differenzierung bei den Verweildauern von Auditoren in der Revision. Langjährige Mitarbeiter erhalten das Prüfungs- und Risiko-Know-how, wohingegen eine gewollte Rotation hilft, um mit der technischen und insbesondere der informationstechnischen Entwicklung Schritt zu halten, wenn Weiterbildung allein das nicht oder nicht mehr leistet.

Die Prüfungsformen verändern sich (siehe Abb. 4) und fachlich kompetente Mitarbeiter für die Revision zu gewinnen ist nicht immer einfach, da kompetente Mitarbeiter oft lieber selbst entwickeln oder produzieren als deren Entstehungsprozess zu auditieren. Entscheidend ist, dass sie ihre Kenntnisse in der Breite des Unternehmens anwenden können und mit fachfremden Aufgaben möglichst wenig belastet werden. Ferner sollte die Revision ein professionelles Personalmarketing betreiben und dabei vor allem an einem innovativen, zukunftsgerichteten Image arbeiten. Ein von dem Unternehmen garantiertes Rückkehrprogramm in die Linie untermauert dies. Sollte es dennoch nicht möglich sein, den fachlichen Bedarf durch Einstellung zu decken, sei es, dass dieser Bedarf zu punktuell ist, um eine ganze Stelle zu rechtfertigen, sei es, dass sich tatsächlich kein geeigneter und/oder gewillter Kandidat findet, sind interne oder externe Gast-Auditoren hinzuzuziehen.

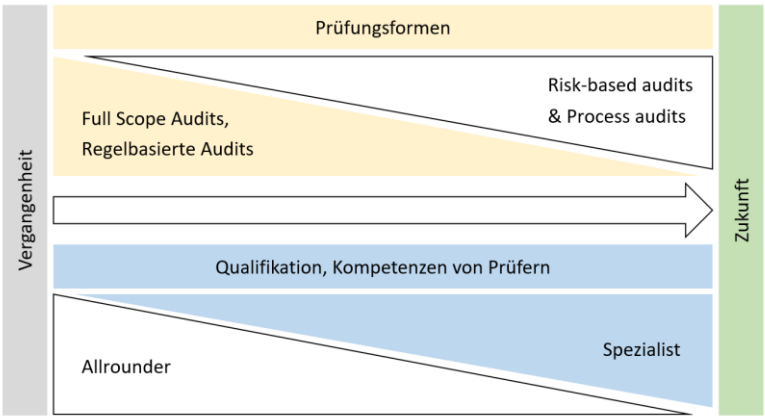


Abb. 4: Der Wandel der Prüfungsformen bedingt auch einen Wandel der Kompetenzen der Prüfer.

[2] Der Certified Internal Auditor (CIA) ist die global anerkannte und einheitliche Berufszertifizierung für Interne Revisoren. CIAs haben ihre Professionalität und Kompetenz nachgewiesen. Mit der Zertifizierung wird auch gegenüber externen Prüfern und Aufsichtsbehörden ein hohes Ansehen erreicht.

4 Planung und Priorisierung der Prüfungsthemen

4.1 Risikokategorien

Aus dem Prüfungsuniversum leiten sich unterschiedliche Risikokategorien ab. Relevante Risiken werden eingeordnet und in Clustern zusammengefasst (vgl. Abb. 5).

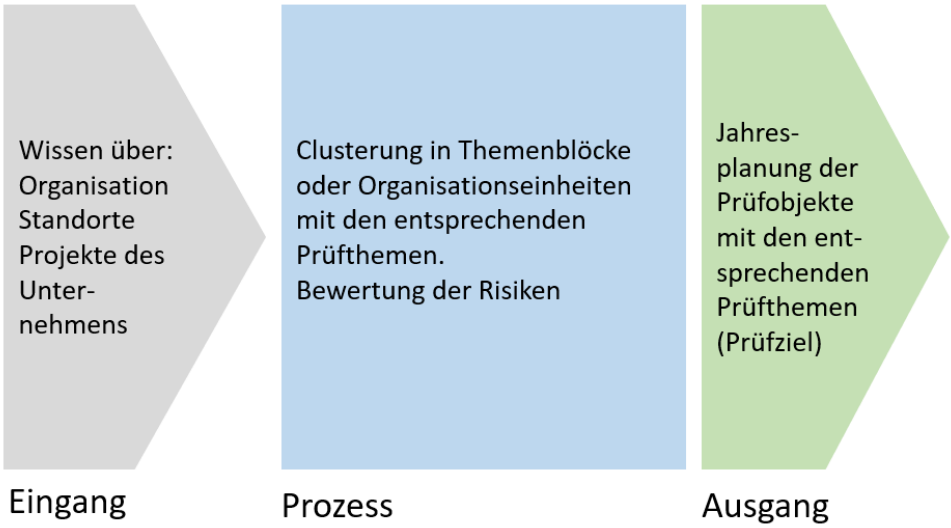


Abb. 5: Planung und Priorisierung der Prüfungsthemen im Rahmen der Jahresplanung

Relevante Cluster für die technische Revision können folgendes umfassen (exemplarisch):

- *Produktbezogene Risiken:* Das Produkt trifft nicht den Kundenbedarf oder die Kundenanforderungen, Wettbewerbsprodukte bieten ein besseres Preis-Leistungsverhältnis oder Zusatznutzen, Sicherheitsrisiken verbunden mit Rückruf und/oder Imageverlust, Produkthaftung/Produktsicherheit, Mängel in der Dienstleistungserbringung, versteckte Qualitätsmängel und ggf. Folgeschäden beim Abnehmer,
- *Opportunitätsrisiken:* Innovationsschwäche, nicht erkannte Markt- oder Technologietrends, Überregulierung, unklare Verantwortungen,
- *Risiken in Fertigung und Logistik:* Nacharbeitskosten, Qualitätsmängel, fehlende Produktivität, veralteter Maschinenpark, hoher Instandhaltungsaufwand, Stillstandskosten, Engpässe durch zu lange Logistikketten, steigende Transportkosten,

- *Risiken des Standortumfelds:* Erreichbarkeit, Risiko für Elementarschäden wie Feuer, Wasser oder seismische Aktivität, Diebstahl und Beschädigung,
- *Informationsmanagement:* Informationsbeschaffung, Verarbeitung, ineffektive Software, fehlerhafter Aufbau bzw. Architektur von Systemen der Informationstechnologie, Integrität, Vertraulichkeit und Verfügbarkeit der Informationsverarbeitung, Digitalisierung und Datenschutz,
- *Umweltmanagement:* Unklare Regelung der Verantwortung, Aufgaben und Kompetenzen, fehlende Gesetzeskenntnisse und fehlende Kontrolle auf deren Einhaltung, Emissionsschäden, Imageschäden (z. B. durch negative CO2-Bilanz, unzureichende technische Schutzmaßnahmen),
- *Arbeitsschutz:* Unzureichende Schutzkleidung, Verstoß gegen Gefahrstoffverordnung, ungesicherte Maschinen und Anlagen, unzureichend qualifiziertes Personal, unzureichende Organisation des Arbeits- und Gesundheitsschutzes sowie mangelnde oder unklare Verantwortlichkeiten, mangelnde Ein- bzw. Unterweisung, fehlende arbeitsmedizinische Betreuung.

Es handelt sich dabei um generische Risikokategorien. Es ist im hohen Maße von individuellen Organisationen und ihrem Kontext sowie rechtlichen Rahmenbedingungen abhängig, welche Risikokategorien definiert und verwendet werden.

4.2 Bewertung der Risikolage als Basis für die Priorisierung der Prüfungsthemen

Eine effektive Revisionsarbeit erfolgt, wenn Risiken transparent sind und systematisch priorisiert werden. Es gilt, Risiken umfänglich zu erfassen und blinde Flecken auf der Risikolandkarte zu vermeiden. Gleichzeitig sind die Auswirkungen der Risiken in einem sinnvollen Verhältnis zu dem Aufwand einer Prüfung zu betrachten.

Die Gewinnung und Verarbeitung von Informationen stellt ein Kernelement für die risikoorientierte Bewertung der Prüfungsthemen dar. Dafür sind sämtliche verfügbaren Quellen zu nutzen.

Interne Informationsquellen für die Identifikation sind bspw. die Unternehmensleitung, die Strategische Planung, das Produktmanagement, die Forschung und Vorausentwicklung, die Entwicklung an sich, die Produktion, die Qualitätssicherung, das Risikomanagement, Compliance oder die Rechtsabteilung. Um die effektive Nutzung interner Informationsquellen sicherzustellen, ist durch die technische Revision ein regelmäßiger und strukturierter Austausch mit relevanten internen Hinweisgebern zu etablieren. Ferner ist die Einbindung

in die Ad-hoc-Kommunikation von größeren Störfällen, Qualitätsbeanstandungen, Produktrückrufen, Haftungs- und Compliance-Fällen als hilfreich zu betrachten. Dies schließt auch die Information über wesentliche „Beinahe-Fälle“ mit ein.

Externe Informationsquellen sind bspw. Wettbewerber, Lieferanten, Kunden, auf technische Rechtsgebiete spezialisierte Kanzleien, Fachverbände wie IIA und DIIR, Veröffentlichungen oder Kongresse sowie gesetzliche Vorschriften, Normen, Standards oder gesellschaftliche Anforderungen. Bei Letzteren ist insbesondere auf steigende Anforderungen zur Nachhaltigkeit hinzuweisen.

Zusätzlich ist die technische Revision gut beraten, die Entwicklung von Key Performance Indicators (KPIs) in den technischen Prozessen sowie von wirtschaftlichen KPIs mit technischen Treibern (z. B. Fehlerkosten) zu beobachten. Werden diese nicht von den entsprechenden Stellen im Unternehmen erhoben, sind ggf. eigene Aktivitäten zu unternehmen. Auch etwaige Korrelationen von KPIs aus sequenziellen Prozessen (z. B. aus der Entwicklung und Fertigung) stellen einen Frühindikator für Risiken dar.

Wie bereits erwähnt, verändert sich das Risikoinventar eines Unternehmens mit dem Geschäftsauftrag über die Zeit hinweg. Das Regelwerk des Unternehmens folgte diesen Veränderungen i. d. R. nach, sodass es einerseits zu überregulierten und andererseits zu nicht regulierten Prozessgebieten kommt. Diese Über- und Unterregulierung ist temporär, sofern das Regelwerk das Risikoinventar wieder einholt. Daneben gibt es Prozessgebiete, die innerhalb des Unternehmens geregelt sind, von denen jedoch kein bedeutsames Risiko ausgeht (strukturell überreguliert) und solche, die aus verschiedenen Gründen ungeregelt geblieben sind (strukturell unterreguliert).

In Abb. 6 wird verdeutlicht, wie es durch Veränderungen in der Risikolage und der damit verbundenen Verschiebung des Risikoinventars eines Unternehmens zu einer temporären Unter- oder Überregulierung von Risiken kommt. Dabei ist davon auszugehen, dass die strukturellen Anteile mit der generellen Einschätzung des Risikoinventars zusammenhängen. Die temporären Anteile rühren von der Verschiebung des Risikoinventars her, während Prozesse, Vorgaben und vorgesehene Kontrollen temporär, bis zu deren Anpassung, bestehen bleiben.

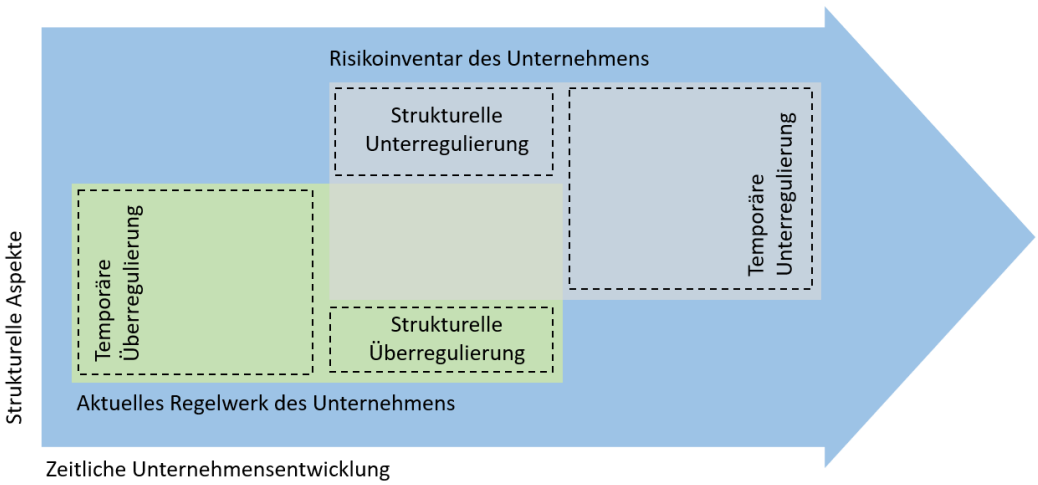


Abb. 6: Unternehmensentwicklung und Regulierung

Die Revision leistet einen wesentlichen Beitrag dazu, die Abdeckung des Risikoinventars durch das bestehende Regelwerk sicherzustellen und eine sich verändernde Risikolage rechtzeitig zu erkennen. Gleichzeitig ist das eigene Prüfungsuniversum fortlaufend weiterzuentwickeln.

Mindestens einmal jährlich, je nach Dynamik der eigenen Unternehmensentwicklung und des Umfeldes ggf. öfter, hat auf Grundlage sämtlicher zusammengetragener Informationen und Hinweise eine Neubewertung der Risikolage zu erfolgen. Daraus abgeleitet können sich die Prioritäten im vorhandenen, technischen Prüfungsuniversum verschieben oder neue Themen aufgenommen und veraltete eliminiert werden.

Von der Revision als dritte Linie wird erwartet, dass sie u. a. Risiken entdeckt, welche der ersten und zweiten Linie nicht auffallen. Dazu gehört ebenfalls, Effizienzpotenziale durch Vereinfachung oder Ausdünnen des vorhandenen Regelwerks aufzuzeigen.

Es ist sinnvoll, die identifizierten Risiken bzw. Prüfungsthemen hinsichtlich Schadenspotenzial und Eintrittswahrscheinlichkeit zu bewerten. Diese Bewertung ist durch Experteneinschätzung (qualitativ), durch Scoring Modelle oder durch quantitative Messung vorzunehmen. Eine aktuelle Bewertung der Prüfungsthemen ist die Eingangsgröße für eine Jahresplanung der Prüfungen und für die benötigten Ressourcen. Kompetenzlücken sind zu identifizieren und zu besetzen, sofern notwendig temporär mit kompetenten Gastauditoren.

4.3 Planung der Prüfungsthemen

Das folgende Kapitel beschäftigt sich mit der risikobasierten Jahresplanung. Die Planung einzelner Prüfungen wird ab Kapitel 5 näher erläutert.

Der zentrale Fokus der Revisionsaktivitäten liegt in der Identifikation der Risiken und Chancen durch die Prüfungs- und Beratungstätigkeiten. Hierzu gibt der IIA-Standard 2010 (The Institute of Internal Auditors, 2017) eindeutige Vorgaben: „Der Leiter der Internen Revision muss einen risikoorientierten Plan erstellen, um die Prioritäten der Internen Revision im Einklang mit den Organisationszielen festzulegen“. Um die Erfolgswahrscheinlichkeit bei der Erstellung eines risikobasierten Prüfungsplans zu erhöhen, wird die Verwendung eines formalen Ansatzes empfohlen.

Darüber hinaus erörtert der Leiter der Internen Revision den Prüfungsplan mit den zuständigen Gremien des Überwachungsorgans und der Unternehmensleitung, um eine Abstimmung zwischen den Prioritäten verschiedener Stakeholder zu schaffen und eine Freigabe des Prüfungsplans zu erreichen.

4.4 Fallbeispiele für die Priorisierung von Prüfungsthemen

Im Folgenden werden beispielhafte und schematische Ansätze vorgestellt, um die Prüfungsthemen für eine Prüfungsplanung zu priorisieren.

4.4.1 Fallbeispiel 1: Priorisierung von Prüfungsthemen bei einem Chemieunternehmen

Im Fallbeispiel eines internationalen Unternehmens der Petrochemie fällt die Interne Revision und die Lenkung des gruppenweiten Risikomanagements in der Funktion des Internal Audit und Risiko-Management zusammen. Das Unternehmen ist Innovationsführer mit hohen Anforderungen an Produkt- und Prozesssicherheit, Arbeitssicherheit und Umweltschutz: Hier sind Fragestellungen der technischen Revision wiederkehrende Prüfungsthemen für das Team, welches aus Mitarbeitern mit kaufmännischem und ingenieurwissenschaftlichem Hintergrund besteht.

Das unternehmensweite Risikomanagement erfolgt durch einen quartalsweisen Austausch der sogenannten Risiko Coaches, einem Team aus Vertretern jedes Geschäftsbereichs, unter Moderation der Internen Revision. In den quartalsweisen Meetings werden die be-

deutsamsten, unternehmensweiten Risiken hinsichtlich finanzieller Auswirkungen und Eintrittswahrscheinlichkeit quantifiziert, zu Risikoclustern aggregiert und auf einer Risikolandkarte visualisiert. Grundsätzlich unterscheidet das unternehmensweite Risikomanagement folgende unternehmensspezifische Risikokategorien: Strategische Risiken, Reputationsrisiken, finanzielle und Marktrisiken, operative und taktische Risiken sowie Risiken der Compliance mit rechtlichen und regulatorischen Anforderungen.

Durch die Einbindung in das unternehmensweite Risikomanagement hat die Interne Revision einen stets aktuellen und belastbaren Überblick über das Risikoportfolio. Diese Interaktion und dieses Wissen beeinflussen auch den jährlichen Prozess der Priorisierung der Prüffelder, welcher in der Zusammenschau von vier Säulen erfolgt (vgl. Abb. 7).

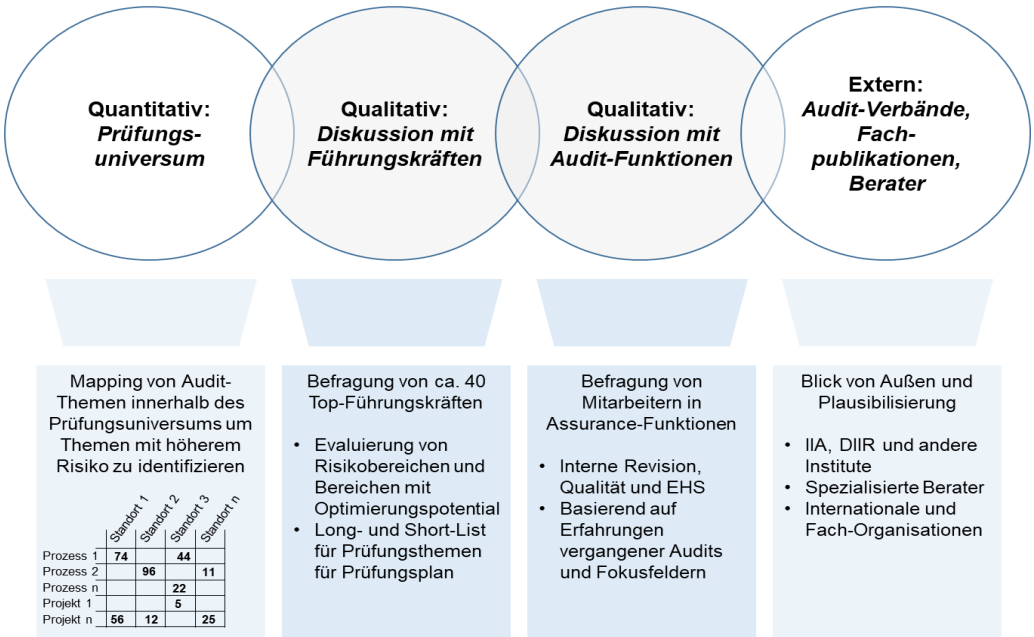


Abb. 7: Exemplarische Priorisierung der Prüfungsthemen für die Prüfungsplanung bei einem internationalen Chemieunternehmen

Die erste Säule ist ein quantitatives Prüfungsuniversum, in welchem Risikokriterien für zu prüfende Einheiten gewichtet werden. Das Prüfungsuniversum bietet einen vollständigen Überblick über zu prüfende Einheiten, welche z. B. Standorte, Prozesse oder Projekte sind. Zu den Risikokriterien zählen bspw. der Umsatz, geplante und tatsächliche Projektkosten, der Reifegrad von internen Kontrollen oder die Anzahl der Kundenbeschwerden,

welche in einem Scoring-Modell[3] gewichtet werden. Im Ergebnis entsteht daraus eine Matrix aus zu prüfenden Einheiten und aggregierten Risiken.

Die zweite Säule basiert auf einer strukturierten Befragung einer größeren Zahl von Führungskräften und Experten im Unternehmen mittels Interviews. Dadurch werden wiederholt genannte Risikothemen und Gebiete mit Optimierungspotenzial eruiert.

Die dritte Säule reflektiert die Eingaben und die Bewertung von Mitarbeitern der Internen Revision und der im Unternehmen bestehenden Prüfungs- und Unterstützungsfunktionen der 2. Linie, in diesem Fall der Bereiche Arbeits-, Gesundheitsschutz, Sicherheit und Umweltschutz bzw. EHS sowie des gruppenweiten Qualitätsmanagements.

In der vierten Säule komplementiert eine externe Perspektive durch Studium von Fachpublikationen und Konferenzen die interne Sicht.

Die eigentliche Priorisierung der Prüfungsthemen erfolgt in einer qualitativen Betrachtung sämtlicher vier Säulen durch den Leiter der Internen Revision, wobei ein Feedback und eine Vollständigkeitsprüfung durch das Prüfungsteam erfolgt. Bei der Priorisierung der Prüfthemen wird darauf geachtet, dass sämtliche Business Units sowie die Risikokategorien vollumfänglich seitens des unternehmensweiten Risikomanagements berücksichtigt sind. Die Priorisierung der Prüfthemen ist folglich ein iterativer Prozess und ergibt im Ergebnis einen konsolidierten Prüfungsplan, welcher durch Vorstand und Prüfungsausschuss bestätigt wird. Zur Vermeidung von Redundanzen und Mehrfachbelastungen einzelner Standorte erfolgt zudem eine quartalsweise Abstimmung des Prüfungsplans im Hinblick auf Terminierung, Abgrenzung des Scopes und Planung der Gastauditoren z. B. in Form eines „Audit Coordination Forum“ mit den Funktionen EHS, Qualitätsmanagement und Operation.

Die Prüfungsplanung erfolgt auf Jahresbasis. Sollte sich die Risikolandschaft verändern, bspw. durch Mergers & Acquisitions (M&A)-Aktivitäten oder durch Zwischenfälle in der Produktion, werden begründete Ad-hoc-Prüfungs-Engagements im Prüfungsplan ergänzt bzw. für spätere Zeiten geplante Prüfungen priorisiert oder vorgezogen. Um unterjährig einen optimalen Grad an Flexibilität zu gewährleisten, besteht die Möglichkeit, geplante Prüfungen des laufenden Jahres z. B. in ein sogenanntes Quartal 5 (erstes Quartal im Folgejahr) zu verschieben.

[3] Das Scoring-Modell wird im Glossar (Anhang) näher erläutert.

4.4.2 Fallbeispiel 2: Priorisierung von Prüffeldern bei einem Industrieunternehmen

Dieses Fallbeispiel stammt aus einem internationalen Industrieunternehmen mit verschiedenen Geschäftseinheiten.

Wie bereits oben beschrieben, werden Informationen aus verschiedenen Quellen für das Audit Universe zusammengetragen. Es werden vorhandene Daten z. B. aus dem Risikomanagement, dem Arbeits- und Umweltschutzmanagement sowie dem Qualitätsmanagement verwendet. Des Weiteren werden einmal jährlich mit den verschiedenen Zentralabteilungen und den Leitungen der Geschäftseinheiten in sogenannten „Strategischen Dialogen“ die möglichen Risiken und deren Veränderungen diskutiert.

Die auf diese Art und Weise gewonnenen Prüfungsthemen werden in verschiedene Bereiche, die Buckets genannt werden, sortiert und separat priorisiert.

- Bucket 1: **Risiken der Geschäftseinheiten**
  Die Priorisierung erfolgt über die Risikoeinschätzung der Geschäftseinheiten und deren Untergliederung.
- Bucket 2: **Übergeordnete Risiken**
  Hier sind hauptsächlich Prozessrisiken und einheitenübergreifende Risiken enthalten.
- Bucket 3: **Risiko-Bewusstsein**
  Um potenziellen blinden Flecken durch Fokussierung auf bekannte oder angenommene Risiken entgegen zu wirken, werden Geschäftseinheiten bzw. Standorte nach dem Zufallsprinzip ausgewählt. Dies kann sämtliche Einheiten betreffen, die nicht bereits über Bucket 1 oder 2 ausgewählt und in den letzten 24 Monaten nicht geprüft wurden.

Die Anzahl der Prüfungen pro Bucket wird bedarfsgerecht festgelegt und ist ein Teil der Priorisierung. In diesem Beispiel sind die Prüfungen i. d. R. in Bucket 1 und die wenigsten in Bucket 3 verankert.

Die Priorisierung innerhalb von Bucket 1 und 2 erfolgt separat nach einem Scoring-Modell. Die Details unterscheiden sich dabei zwischen Bucket 1 und 2.

5 Planung der Prüfungen

In Kapitel 4 wurde die Priorisierung von Prüfungsthemen beschrieben. Dabei ging es darum, innerhalb eines Unternehmens Schwerpunkte für technische Prüfungen innerhalb eines Jahres festzulegen (z. B. Fokus auf Entwicklung, Fertigung, Qualität, Arbeitssicherheit, Brandschutz, Umweltschutz).

In Kapitel 7 wird die Vorbereitung der einzelnen Prüfung beschrieben. Dazu gehört die Konkretisierung der Zielsetzung und die Feinplanung von zeitlichem Ablauf und Ressourcen.

Dieses Kapitel beschäftigt sich mit der Planung sämtlicher Prüfungen innerhalb eines Jahres (vgl. Abb. 8).

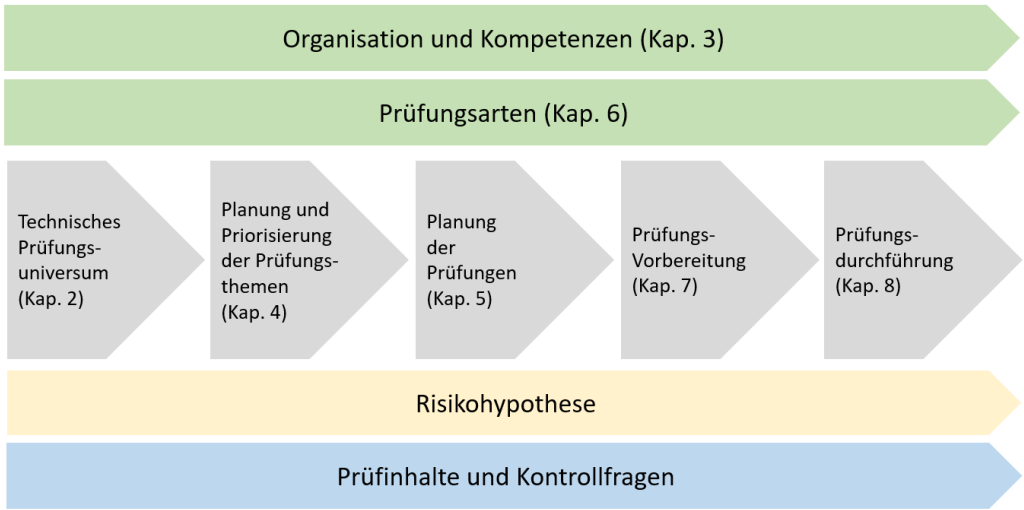


Abb. 8: Ablauf von Prüfungen

5.1 Terminliche Planung von Prüfungen

Es existieren unterschiedliche Möglichkeiten für die Planung von Prüfungen:

- Ein Jahr lässt sich in verschiedene Prüfzyklen einteilen und entsprechend werden eindeutige Termine für den Start und das Ende einer Prüfung definiert.

- Für jede Prüfung werden eine geplante Dauer und ein Zeitraum im Jahr definiert.
- Freie Kapazitäten von Prüfern werden, sofern vorhanden, verwendet und die nächste passende Prüfung fixiert.

Eine Vor- und Nachbereitungszeit ist in jedem Fall zu berücksichtigen. Führendes Kriterium im Rahmen der terminlichen Planung ist nicht die Kapazität an Prüfern oder die Zeit, sondern stets die Abdeckung der Prüfungsthemen. Unter Umständen sind Kapazitätslücken z. B. durch Gastprüfer auszugleichen.

Da die Einsatzplanung flexibel und anpassungsfähig zu gestalten ist (um z. B. auf weitere potenziell erkannte Risiken, Zeitverzögerungen durch die zu prüfende Einheit, Ausfall von Prüfern, Prüfungsverschiebungen zu reagieren), lässt sie sich revolvierend für einen Zeitraum von z. B. drei Monaten durchführen und bei neuen Erkenntnissen über den tatsächlichen Verlauf der Prüfung unverzüglich zu aktualisieren.

Gegebenenfalls ist bei der Planung ebenso zu berücksichtigen, dass sich in Folge besonderer Ereignisse (z. B. durch die Corona-Pandemie seit 2020) eine Verlagerung der Prüfungsaktivitäten aus der Prüfungsdurchführung bereits in die Prüfungsvorbereitung ergibt. Die eingeschränkten Reisetätigkeiten sowie die verstärkten Remote-Prüfungen haben zur Folge, dass bereits bei der Prüfungsvorbereitung Unterlagen intensiver aufzubereiten sind und bereits mit konkreteren Fragen in die Prüfungsdurchführung gestartet wird.

5.2 Planung von Prüfungsziel und -umfang

Ausgangspunkt einer Prüfungstätigkeit ist u. a. die Betrachtung der Hauptwertschöpfungsprozesse. Bei einem produzierenden Unternehmen für Industrie- oder Gebrauchsgüter sind dies typischerweise die Produktplanung einschließlich Marktbearbeitung, die Entwicklung und die Produktion. Die Informationen, die in jedem Hauptprozess anfallen, sind die Eingangsgrößen für die Planung (wo ist das größte Risiko bei einer Produktgruppe?), die Vorbereitung (was konkret soll in dieser Produktgruppe geprüft werden?) und die Durchführung der Prüfung. Der Umfang der Datenerhebung nimmt über drei Prüfungsphasen erheblich zu. Erfahrungsgemäß stehen zum Zeitpunkt der Planung der Prüfungen lediglich allgemeinverfügbare Daten zur Verfügung. Dagegen ist ab der Ankündigung einer Prüfung in einem bestimmten Bereich der gesamte Datenbestand für die Vorbereitung und Durchführung nutzbar.

Die Zuordnung der einzelnen Zielsetzungen orientiert sich z. B. an folgenden Kriterien:

- Feststellungen bei bereits durchgeführten bzw. vergleichbaren Prüfungen,
- Risikoaspekte (Art des Geschäftes, vorliegende Informationen und Einschätzungen),

- Compliance-Risiko-Analyse,
- Ordnungsmäßigkeitserwägungen (z. B. 3-Jahres-Rhythmus),
- andere durchgeführte Prüfungen (z. B. ISO TS Audits, Kundenaudits, Versicherungsprüfungen).

Bereits in der Planung der Prüfungen sind jeweils eine grobe Risikohypothese zu formulieren sowie Gesetzesvorgaben und das interne Regelwerk zu berücksichtigen. Hierzu ein paar Beispiele:

- Failure Mode and Effect Analysis (FMEA): Sie wurde nicht komplett durchgeführt, mögliche Abweichungen haben sich nicht ergeben, folglich besteht die Möglichkeit von Produktfehlern und damit verbundenen Rückrufen.
- Sonderfreigaben: Eine Validierung wurde durch die Entwicklung nicht durchgeführt. Die Lebensdauer des Produkts wird potenziell eingeschränkt oder das Resultat sind erhöhte Fehlerkosten.
- Prüfmittelüberwachung: Ein defektes Prüfmittel ist im Einsatz und erkennt fehlerhafte Produkte in der Schlussprüfung nicht. Folglich gelangen fehlerhafte Produkte ins Feld.

Für jeden Auditfokus sind vor jeder Prüfung die Prüffragen auf Vollständigkeit hin zu prüfen oder entsprechend zu erstellen. Hierzu ebenso ein paar Beispiele:

- FMEA: Ist die FMEA für jede Produktgruppe erstellt worden, wurden die Bewertungskriterien richtig verwendet, die FMEA anhand von Beanstandungen überarbeitet und Maßnahmen entsprechend umgesetzt?
- Sonderfreigabe: Wurde durch die Entwicklung eine Validierung vorgenommen, ist die Sonderfreigabe zeitlich oder mengenmäßig begrenzt, ist eine Nachverfolgung der gelieferten Produkte nachvollziehbar?
- Prüfmittelüberwachung: Sind Prüfmittel in der Fertigung registriert, liegt eine nachvollziehbare Prüffrist vor, werden Prüfmittel termingerecht eingezogen sowie überprüft und bei Abweichungen eine Risikoabschätzung durchgeführt?

5.3 Planung von Prüfungsressourcen

Um eine Prüfung erfolgreich durchzuführen, benötigt es eine entsprechende fachliche und prozessuale Kompetenz der Prüfer. (Siehe hierzu auch Kapitel 3 *Organisation und Kompetenzen*.)

Für die Prüfungsplanung ist es wichtig, anhand des Prüfungsziels die richtigen Prüfer auszuwählen. Idealerweise geschieht dies mithilfe einer Matrix, welche für sämtliche Prüfer die Kompetenzausprägung in den Prüfungsthemen enthält.

Weiterhin ist es sinnvoll, hinter die Prüfungsthemen auch die entsprechende Zeit für dieses Thema zu definieren. Hier weitere Beispiele:

- FMEA: Kontrollfrage benötigt einen Aufwand von fünf Manntagen.
- Sonderfreigabe: Kontrollfrage benötigt einen Aufwand von drei Manntagen.
- Prüfmittelüberwachung: Kontrollfragen benötigen einen Aufwand von vier Manntagen.

5.4 Definition Fokus

Unterstützend oder ergänzend zu den Hauptprozessen fallen mehrere Support- oder Nebenprozesse in den Fokus der technischen Revision. Supportprozesse haben i. d. R. einen Bezug zu bestimmten Hauptprozessen (z. B. Projektmanagement zur Entwicklung, Qualität und Instandhaltung zur Produktion). Es bietet sich folglich an, sie je nach Risikorelevanz mit dem Hauptprozess gemeinsam zu auditieren. Für die Datenerhebung gilt der bereits beschriebene Prozess.

Nebenprozesse wie Bauwesen, Standortsicherheit oder EHS haben keinen unmittelbaren Bezug zur eigentlichen Leistungserbringung. Da sie dennoch zur Sicherstellung der Legalität und Vermeidung des Imageverlustes wichtige Revisionsthemen sind, ist auch hier eine strukturierte Datenanalyse und -Auswertung von großer Bedeutung.

Eingangs ist zu überlegen, welche Daten risikorelevant sind (typisch sind dies u. a. Produkt- und Technologieportfolios, Projektlisten, Qualitätsbewertungen, Entwicklungsbudgets, Ausbringung, Beanstandungen und vieles mehr). Bei der Beschaffung der Daten macht es einen großen Unterschied, ob sie mit erheblichem Aufwand manuell erstellt werden, oder auf Knopfdruck abrufbar sind. Im Unterschied zu kaufmännischen Funktionen, bei welchen Daten aus Gründen der Prozessautomation und Berichtspflicht in hohem Maße standardisiert und in Enterprise Resource Planning (ERP)-Systemen zentral gespeichert sind, ist in den technischen Abteilungen oftmals eine Heterogenität anzutreffen, die eine automatische Datenerhebung und den Einsatz von Tools zur Analyse erschwert. Dennoch sind durch die technische Revision zusammen mit den zentralen Funktionen auch im Sinne von Fokusvergrößerung und kontinuierlichem Auditieren auf eine stärkere Standardisierung und Zentralisierung technischer Daten zu drängen und die automatische Erhebung und Verarbeitung stetig auszubauen.

6 Prüfungsarten

6.1 Gründe für verschiedene Prüfungsarten

Ziel einer jeder Prüfungshandlung ist es, Risiken zu erkennen und diese zu bewerten, damit sie mit angemessenen Maßnahmen reduziert oder, wenn möglich, beseitigt werden. Dafür gibt es unterschiedliche Auditarten, die je nach Zielrichtung, geprüfter Einheit und Ressourceneinsatz, ein angemessenes, effizientes und effektives Prüfen erlauben.

6.2 Bekannte Prüfungsarten

Die folgende Aufzählung enthält verschiedene Prüfungsarten, welche im AK bekannt sind. Sie hat keinen Anspruch auf Vollständigkeit. Sortierkriterium ist der Fokus im Detailgrad von tief bis breit. Beispiele für Auditarten aus einem Industrieunternehmen mit ihren Zielen sowie Vor- und Nachteilen finden sich im Anhang 10.1.

- Spezialprüfung (aktueller Vorfall),
- Prozessprüfung,
- Wiederholungsprüfung,
- Projekt-Prüfung,
- Governance Prüfung,
- Prüfung von Gemeinschaftsunternehmen,
- vollständige Prüfung,
- beratende Prüfung,
- Standortprüfung,
- Cluster-Prüfungen,
- Sensibilisierungs-Prüfung,
- Kurzprüfung.

Wie bereits aus dem Namen hervorgeht, gehören zu dem Operationsgebiet der Internen Revision nur Organisationseinheiten des eigenen Unternehmens sowie seiner Töchter und

gegebenenfalls Gemeinschaftsunternehmen. Lieferantenaudits sind typischerweise Aufgabe des Einkaufs oder der Qualitätssicherung. Akquisitionsziele werden im Rahmen von Due-Diligence-Prüfungen durch die fachlich zuständigen Abteilungen auditiert. Die Interne Revision beschränkt sich in beiden Fällen darauf, die damit verbundenen Sorgfaltspflichten zu überwachen.

Verschiedene Prüfungsarten lassen sich zudem miteinander kombinieren, z. B. kann eine Spezialprüfung in einem Gemeinschaftsunternehmen stattfinden. Häufig anzutreffende Kombinationen sind in Abbildung 9 dargestellt.

Mögliche Kombinationen von Prüfungsarten	Spezialprüfung (aktueller Vorfall)	Prozessprüfung	Wiederholungsprüfung	Projekt-Prüfung (DIIR4 Standard)	Governance Prüfung	Prüfung von Gemeinschaftsunternehmen	vollständige Prüfung	beratende Prüfung	Standortprüfung	Cluster-Prüfungen	Sensibilisierungs-Prüfung
Spezialprüfung (aktueller Vorfall)						X	X		X		
Prozessprüfung			X		X	X		X			X
Wiederholungsprüfung				X	X	X	X		X	X	
Projekt-Prüfung (*DIIR4 Standard*)						X					
Governance Prüfung								X			X
Prüfung von Gemeinschaftsunternehmen								X	X	X	X
vollständige Prüfung								X	X		X
beratende Prüfung									X	X	
Standortprüfung											X
Cluster-Prüfungen											X
Sensibilisierungs-Prüfung											

sym.

Abb. 9: Kombinierbarkeit von Prüfungsarten

7 Prüfungsvorbereitung

Die Vorbereitung einer Prüfung ist in den Internationalen Grundlagen für die berufliche Praxis (IPPF) in der 2200er Standardserie (The Institute of Internal Auditors, 2017) aufgeführt. Die zugehörigen Implementierungsleitlinien helfen Internen Revisoren die Standards anzuwenden.

Ergänzend hierzu können auch die Kriterien 26 bis 32 des DIIR Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ (DIIR, 2017) herangezogen werden.

Die wesentlichen Prüfungsschritte sind in Abbildung 10 dargestellt.

Abb. 10: Zeitliche Abfolge einer Prüfung

Die zeitliche Abfolge ist hier nicht als starr anzusehen. Beispielsweise kann nach der Analyse eine Anpassung der Ressourcenplanung erforderlich werden, oder diese wird erst nach der Analyse durchgeführt, nachdem man initial mit einem kleinen Team gestartet ist.

Im Rahmen der einzelnen Schritte sind die für technische Prüfungen typischen Besonderheiten zu beachten, welche im Folgenden erläutert werden.

7.1 Ressourcenplanung

Den Prüfobjekten des genehmigten Prüfungsplans werden Ressourcen und Verantwortlichkeiten nachvollziehbar zugeordnet. Bei fehlendem Fachwissen sind erforderliche Weiterbildungen und/oder Co-Sourcing (z. B. externe Prüfer, Dolmetscher) zu berücksichtigen.

Der Einsatz von Fremdkräften ist mit einer Geheimhaltungsverpflichtung abzusichern. Der Zeitaufwand der Prüfung ist zu ermitteln und in einem Terminplan mit Meilensteinen darzustellen. Die bekannten Planungstechniken wie Terminplan, Checklisten für Prüfungsvorbereitung und (Auslands-)Reiseplanung erleichtern das strukturierte Vorgehen.

Besonderheiten der technischen Revision

Kennzeichnend für die technische Revision ist insbesondere der starke Bezug zu dem Produkt und die damit zumindest für materielle Produkte und Dienstleitungen oft verbundene Notwendigkeit zur Inaugenscheinnahme vor Ort.

Ein Beispiel: Die Prüfung des Prozesses zur Arbeitsmittelüberwachung kann den Abgleich inventarisierter Anlagen mit dem tatsächlichen Bestand bis hin zur Kontrolle von Prüfplaketten erforderlich machen.

Folglich ist abzuwägen, ob eine Prüfung ganz oder teilweise vor Ort zu erfolgen hat, oder als Remote-Prüfung durchzuführen ist. Hierbei ist zwischen Effizienz (Reisekosten, Gefährdungsvermeidung etc.) und Effektivität (kann ein Risiko aus der Ferne ausreichend bewertet werden?) abzuwägen und ggf. der Einsatz technischer Hilfsmittel wie Videokonferenzen, Videointerviews, Einsatz von Drohnen und durch den Prüfer gesteuerte Kamerarundgänge von Mitarbeitern vor Ort oder der Einsatz lokaler Dienstleister in die Planung mit einzubeziehen. Entsprechende Systeme und Dienstleistungen für Remote-Prüfungen werden auch von Gutachtern eingesetzt und sind vermehrt am Markt verfügbar. Hierbei ist eine datenschutzkonforme Umsetzung sicherzustellen und entsprechend mit dem für das Prüfobjekt zuständigen Datenschutzbeauftragten und ggf. dem Betriebsrat abzustimmen. Diese Aufgabe kann auch der zu prüfende Bereich übernehmen.

Weiterhin besteht die Möglichkeit, dass das Thema Arbeitssicherheit bei technischen Prüfungen (Begehung von gefährlichen bzw. gefährdeten Bereichen) eine Rolle spielt und gegebenenfalls in der Planung zu berücksichtigen ist.

Je nach Organisation des Unternehmens muss auch eine terminliche Koordination mit anderen Audit-Aktivitäten erfolgen. Dies können Audits der 2. Linie sein, aber auch Zertifizierungen, Kunden- und Behördenaudits. Insbesondere bei größeren Internen Revisionen ist die Koordination der Prüfungsthemen sämtlicher Revisionsabteilungen nicht außer Acht zu lassen, die idealerweise in einer gemeinsamen Prüfung mündet.

7.2 Analyse

Zu Beginn einer Prüfung wird der Prüfungsgegenstand analysiert. Hierzu sind Informationen über das Prüfobjekt einzuholen und erforderliche Prüfmethoden zu definieren. Auf Basis der Risikoanalyse des Prüfungsobjektes werden die Ziele der genehmigten Prüfung auf Vollständigkeit geprüft und ggf. erweitert bzw. konkretisiert. Der Prüfungsansatz, die geplante Struktur und die Vorgehensweise werden entsprechend definiert.

Besonderheiten der technischen Revision

Als Input kommen u. a. in Frage und sind entsprechend zu beschaffen und auszuwerten:

- Produkt- und Technologieportfolios,
- Projektlisten,
- Produktionsberichte,
- KPIs z. B. zu Ausschuss, Termintreue, Beständen etc.,
- F&E-Berichte,
- Qualitätsbewertungen,
- Entwicklungsbudgets,
- Ausbringung,
- Beanstandungen, Stör- und Unfallmeldungen,
- Kundenbefragungen,
- Marktanalysen,
- Ergebnisse vorangegangener Revisionen, Audits, Zertifizierungen etc. und die daraus ergangenen Maßnahmen und Auflagen,
- lokale Besonderheiten bezüglich vorhandener Funktionen (z. B. Entwicklung, Produktion), eingesetzter Technologien, Wertschöpfungstiefe (Auslagerungen an Dritte, hier ist dann ggf. ein anderer Prüfungsansatz erforderlich: Lieferantenauswahl/-überwachung).

Bei technischen Prüfungen spielen potenziell lokale Sollvorgaben eine Rolle. Sie sind in diesen Fällen vorab zu ermitteln und zu berücksichtigen. Beispiele hierfür sind lokale Umweltschutzauflagen oder die nationale Arbeitsschutzgesetzgebung.

Für die Informationsbeschaffung ist eine Datenanalyse sinnvoll, um bspw. eine relevante Stichprobe (mit entsprechender Aussagewahrscheinlichkeit) zu bestimmen. Ein Beispiel sind Auswertungen zur Fristeinhaltung jeglicher Art (Qualifikationen, medizinische Untersuchungen, Instandhaltungsfristen, Liefertermine, Meilensteine). Die ermittelten Fälle mit Abweichungen werden als relevante Stichprobe näher untersucht und die Ursachen ermittelt.

Relevante Stichproben lassen sich entweder statistisch repräsentativ ziehen, falls der Untersuchungsumfang nicht den Rahmen sprengt, oder begründet, z. B. beim Vorliegen bestimmter Verdachtsmomente.

In jedem Fall ist als Ergebnis der Analyse eine Art Risikohypothese zu formulieren. Im Rahmen dessen ist von den erhobenen Fakten auszugehen und ein potenzielles Risiko zu konstruieren. Beispielsweise könnte die Tatsache, dass ein Produkt nur an einem Standort gefertigt wird, ein Risiko für die Liefersicherheit bedeuten. Entsprechend würden Prüfungsthemen wie Kontinuitätsmanagement und Brandschutz ins Prüfprogramm mit aufgenommen werden. Hypothesen sind ein wichtiges Instrument für einen effektiven, risikobasierten Einsatz von Prüfressourcen.

Standorte sind ggf. mit mehreren Produktgruppen, Fertigungslinien, Gebäuden etc. ausgestattet. Nachdem Ziele und Fokus der Prüfung feststehen, ist zu entscheiden, welche Objekte konkret geprüft werden. Um im Beispiel von Kapitel 5 *Planung der Prüfungen* zu bleiben, wären folgende Fragen zu beantworten:

- FMEA: Welche Produktgruppen sind zu prüfen?
- Sonderfreigabe: Welche Produkte sind im Fokus zu betrachten?
- Prüfmittelüberwachung: Welche Fertigungslinie ist zu überprüfen?

Dazu sind während der Prüfung erhobene Daten oder Hinweise von Abteilungen der 2. Linie hilfreich. Notfalls findet die finale Festlegung nach Sammlung zusätzlicher Informationen vor Ort statt.

7.3 Ankündigung

Mit ausreichendem[4] Vorlauf wird dem zu prüfenden Bereich die Prüfung angekündigt (Ausnahmen z. B. Sonderprüfungen). Hierbei sind die wesentlichen Kernpunkte der Prüfung (Prüfungsschwerpunkte, Meilensteine) zu erwähnen.

[4] Welcher Zeitraum hier als angemessen definiert wird, ist unternehmensspezifisch festzulegen.

7.4 Erstkontakt zum Prüfobjekt

In einem gemeinsamen Gespräch wird die Prüfungskonzeption erläutert und Zuständigkeiten, Ansprechpartner sowie der terminliche Ablauf abgestimmt.

Besonderheiten der technischen Revision

Zur Ankündigung und Vorbereitung des Kick-offs gehören auch die

- Kontaktaufnahme mit der verantwortlichen Stelle der geprüften Organisationseinheit,
- Abstimmung der Termine für das Auftaktgespräch mit dem verantwortlichen Management,
- Festlegung der Ansprechpartner der geprüften Stelle durch das verantwortliche Management,
- Absicherung der Präsenz wichtiger Auskunftspersonen der geprüften Stelle während der Prüfung,
- Klärung länderspezifischer Auflagen hinsichtlich des Umgangs mit Datenträgern (Einreise, Ausreise), Foto- sowie Videoaufnahmen und
- Abstimmung mit dem betrieblichen Datenschutzbeauftragten (und ggf. Chief Information Security Officer und/oder Betriebsrat) bei beabsichtigter Auswertung personenbezogener Daten.

Auf diese Art und Weise werden ein zeitlicher Leerlauf und Störeinflüsse während der örtlichen Prüfung minimiert. Ferner wird den Einheiten die Möglichkeit gegeben, spezielle Prüfungsanregungen oder besondere Prüfungswünsche im Rahmen der vorgesehenen Prüfung anzumelden. Neben den materiellen Aspekten sind des Weiteren organisatorische Fragen zu klären, z. B. räumliche Unterbringung, Nutzung organisatorischer Hilfsmittel, Zugangsberechtigung zur IT, Zugriff auf Unterlagen und Systemablagen (Gruppenlaufwerke, SharePoints etc.), Arbeitsschutzunterweisungen vor Ort sowie ergänzende Arbeitsschutzausrüstung.

7.5 Freigabe des Prüfprogramms

Aufbauend auf der Erstkonzeption und den Ergebnissen aus dem Kick-off-Meeting werden die Ziele und der Umfang der Prüfung erneut überprüft und ggf. angepasst. Anschließend erfolgt eine detaillierte Erstellung des Prüfprogramms. Diese beinhaltet eine thematische und prozessorientierte Gliederung der Prüfung. Die Prüfungsansätze und Fragestellungen

der geplanten Methodik (Gespräch, Stichprobe, Aufnahme von Unterlagen) werden möglichst präzise formuliert. Die Dokumentation der Ausgestaltung der Stichprobenanalyse hat ebenfalls bereits im Arbeitsprogramm zu erfolgen.

Das Prüfprogramm endet mit der Bewertung der Ordnungsmäßigkeit und Angemessenheit der Prozesse und mit der Beurteilung ihrer Umsetzung. Es schließt mit der Darstellung des Gesamtergebnisses des Prüfungsauftrages.

Das Prüfprogramm wird gemäß dem Freigabeprozess genehmigt. Üblicherweise dient dazu ein Prüfungsvorbereitungsgespräch zwischen dem Prüferteam und Vorgesetzten. Wesentliche Änderungen eines bereits genehmigten Prüfprogramms während der Prüfung, z. B. durch neue Erkenntnisse vor Ort, sollten möglich sein, sind jedoch mit dem Vorgesetzten abzustimmen. Die Änderungen sowie deren Genehmigungen sind zu dokumentieren.

8 Prüfungsdurchführung

Wie bei jeder Revisionsprüfung sollte die Zusammenarbeit zwischen Fachbereich und Revision kooperativ erfolgen. Der Fachbereich ermöglicht dies durch eine Auswahl kompetenter Gesprächspartner sowie die rechtzeitige Zurverfügungstellung geeigneter und aktueller Unterlagen.

Die geprüften Bereiche sind durch die Revisoren frühzeitig über die zu prüfenden Themen zu informieren und zielorientiert vorzubereiten. In den Interviews sind die relevanten Punkte kritisch zu hinterfragen und die Sachverhalte anschließend objektiv darzustellen.

Insofern bieten sich nach wie vor die klassischen Revisionstools, wie Interviews, Dokumentenprüfungen, risikoorientierte Stichproben und Einzelbetrachtungen kritischer Fälle in Abhängigkeit der Prüfungsthemen (z. B. im Rahmen von einzelfallbezogenen oder deliktischen Sonderprüfungen) ergänzend an.

Das physische Prüfen vor Ort ist ein Kennzeichen der technischen Revisionstätigkeit. Dies gilt insbesondere für den Produktionsprozess und seine Nebenprozesse. Traditionell geschieht dies in Rundgängen des technischen Prüfers zusammen mit den Fachleuten des zu auditierenden Bereichs. Kommentierte Fotos dienen der Dokumentation des Gesehenen. In Zeiten restriktiverer Reisebestimmungen gibt es gute Erfahrungen, diese Rundgänge z. B. durch einen kameratragenden Mitarbeiter vor Ort, der von dem Prüfer ferngesteuert wird, zu ersetzen. Erste Anbieter entsprechender Systeme sind auf dem Markt.

Im Anhang sind unter 10.2 Beispiele für technische Prüfungsthemen und zugehörige Prüfkonzepte aufgeführt.

Der seit Längerem bestehende Trend in der Revision, vermehrt Methoden der strukturierten Datenanalyse einzusetzen, hat auch in der technischen Revision seinen Niederschlag gefunden. In Anbetracht der in den technischen Bereichen vorhandenen großen Datenmengen in einer Vielzahl unterschiedlicher IT-Systeme ist es vermehrt geboten, prüfungsbezogene Aussagen auf Grundlage einer breiten Datenbasis zu treffen und demzufolge die in den betrachteten Prozessen entstehenden Datenmengen entlang der Wertschöpfungskette möglichst umfassend einzubeziehen. Um prüferisch valide und aussagekräftige Schlüsse auf Daten einer Grundgesamtheit zu ziehen und damit zur Gesamtaussage des Prüfergebnisses zu kommen, reichen reine Stichprobenbetrachtungen oftmals nicht mehr aus, sodass sich dies für eine Vielzahl der Themen nur durch eine strukturierte Datenanalyse realisieren lässt.

Da in vielen technischen Bereichen die zu prüfenden Prozesse und Prozessketten durch eine Vielzahl von unterschiedlichen IT-Systemen abgebildet sind, kommt der Datenzusammenführung und deren aussagekräftige Verknüpfung eine große, auch zeitlich einzuplanende, Bedeutung zu. Im Ergebnis muss ein belastbares Fundament für die folgenden Analysen entstehen. Bedarfsweise haben Abstimmungen mit den geprüften Fachbereichen oder Systemstellen zu erfolgen, um dies abzusichern.

In der Prüfungsplanung und -vorbereitung aufgestellte Hypothesen sowie während der Prüfung entwickelte Ansätze aus Erkenntnissen der Prozessaufnahmen, Interviews und Einzelfalluntersuchungen sind gegen die Datengrundlage zu spiegeln und damit entweder zu bestätigen oder zu widerlegen. Ferner besteht die Möglichkeit, standardisierte Prüflogiken/-skripte (z. B. Freigaben an Wochenenden, Red Flags etc.) auf den gesamten Datenbestand anzuwenden und auf diese Weise repräsentative Aussagen zu treffen. Die Analyse lässt sich mittels klassischer Revisionstools wie bspw. ACL und IDEA durchführen. Ferner bieten sich eine Vielzahl von Tools zur Massendatenanalyse wie u. a. KNIME, SPSS, MatLab oder programmierte Skripte in Python an. Die gesetzlichen und betrieblichen Anforderungen des Datenschutzes und ggf. der betrieblichen Mitbestimmung sind im gesamten Vorgehen stets im Auge zu behalten und zu berücksichtigen.

Die Auflistung unter 10.3 im Anhang gibt einen beispielhaften Überblick zu Prüfungsthemen, welche in der technischen Revision mit datenanalytischen Bestandteilen geprüft werden.

Im Rahmen der standardisierten Umsetzungsverfolgung adressierter Revisionsmaßnahmen (Follow-up) können insbesondere die im Rahmen der Datenanalysen zu dem Prüfungszeitpunkt erarbeiteten Analyselogiken und -skripte auf einen aktualisierten Datenbestand angewendet werden, um die Wirksamkeit in einem breiten Umfang zu prüfen.

8.1 Revisionsberichterstattung und Follow-up

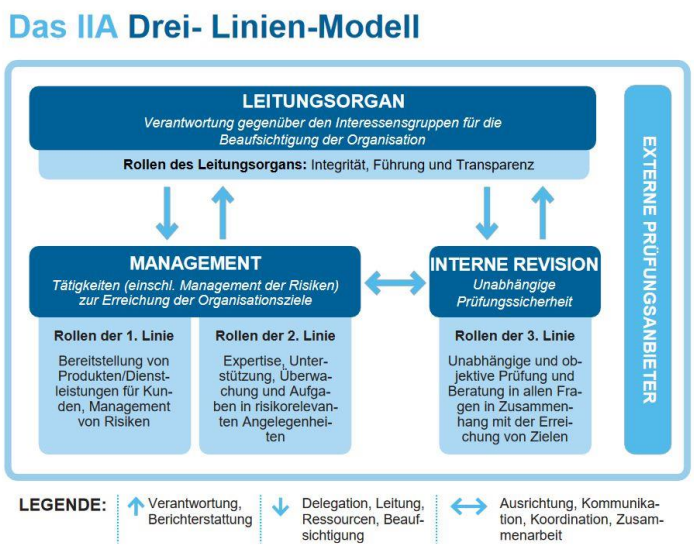
Die in technischen Prüfungen erlangten Erkenntnisse und der resultierende Handlungsbedarf werden üblicherweise im Rahmen der jeweils revisionsspezifisch festgelegten Verfahren im Einklang mit den einschlägigen Anforderungen der IIA-Standards mit den geprüften Fachbereichen abgestimmt und unternehmensintern berichtet. Die Prüfergebnisse dienen dabei zudem als wichtige Informationsquelle für die Risikoanalysen und Programmplanungen der Folgejahre.

9 Glossar

Ablauforganisation	Gemäß Eisenführ (Einführung in die Betriebswirtschaftslehre) umfasst die „Ablauforganisation […] die Regelung von Prozessen, d. h. die zeitliche und räumliche Abfolge einzelner Vorgänge“.
Audit-Plan vs. Prüfprogramm	IIA Internationale Standards für die berufliche Praxis der Internen Revision 2017 beschreibt den Begriff der Planung, welcher auch im Leitfaden Anwendung findet: „Der Leiter der Internen Revision muss einen risikoorientierten Prüfungsplan erstellen, um die Prioritäten der Internen Revision im Einklang mit den Organisationszielen festzulegen. Zur Entwicklung des risikoorientierten Prüfungsplans berät sich der Leiter der Internen Revision mit leitenden Führungskräften und Geschäftsleitung bzw. Überwachungsorgan und gewinnt ein Verständnis von den Strategien der Organisation, bedeutenden Geschäftszielen, damit verbundenen Risiken und den Risikomanagementprozessen. Der Leiter der Internen Revision muss den Plan regelmäßig überprüfen und erforderlichenfalls anpassen, wenn sich Änderungen des Geschäftes, der Risiken, der Abläufe, Programme, Systeme oder Kontrollen der Organisation ergeben." Gemäß ISO 19011:2011 definiert der Auditplan die Beschreibung der Tätigkeiten und Festlegungen für ein Audit. Es handelt sich hier um die detaillierte Planung für ein einzelnes Audit. Das Prüfprogramm (bei anderen Unternehmen auch Auditprogramm genannt) stellt gemäß ISO 19011:2011 Festlegungen für einen Satz von einem oder mehreren Audits dar, die für einen bestimmten Zeitraum geplant und auf einen spezifischen Zweck ausgerichtet sind. Die Verwendung der Begriffe ist nicht konform mit den geltenden ISO Definitionen.
Auditscope/Umfang des Auftrages	Der Auditscope stellt den Umfang der Prüfung dar. Er muss angemessen sein, um die festgelegten Prüfziele zu erfüllen.

Drei-Linien-Modell

Mithilfe des *Drei-Linien-Modells* des Institute of Internal Auditors aus Juli 2020 kann die eigene Governance-Struktur kritisch hinterfragt werden, um damit Stärken und Verbesserungspotenziale herauszuarbeiten.



Das Leitungsorgan delegiert nach Abstimmung der vorrangigen Zielsetzungen und Aktivitäten mit den Stakeholdergruppen seine Aufgabenverantwortung und stellt dem mit der Umsetzung dieser Aufgaben betrauten Management die notwendigen Ressourcen zur Verfügung, um die Ziele der Organisation zu erreichen.

Die Verantwortung des vom Vorstand so beauftragten Managements zur Erreichung der Organisationsziele umfasst sowohl die erste als auch die zweite Linie. Hauptaufgaben der ersten Linie sind die Schaffung geeigneter Strukturen und Prozesse sowie die Lenkung der operativen Funktionen. Dies umfasst auch die Einhaltung von gesetzlichen und regulatorischen Vorgaben und interne Kontrollen. Die Zentralbereiche in der zweiten Linie haben Regelungs-, Kontroll- und Berichtsfunktionen. Sie leisten aktiv Unterstützung für das Leitungsorgan und die operative Organisation durch besondere Fachkenntnisse. Mithilfe von Analysen und Berichten sorgen sie für einen kontinuierlichen Verbesserungsprozess, die Angemessenheit des Risikomanagements und eine angemessene Berichterstattung an den Vorstand über die Situation bei den Konzernunternehmen bezogen auf das zu verantwortende Fachgebiet.

Das Modell sieht vor, dass vom Leitungsorgan eine prozessunabhängige und objektive Interne Revision geschaffen wird, die dieses bei der Überwachung des mit der Aufgabe der Zielerreichung betrauten Managements unterstützt.

Die Unabhängigkeit der dritten Linie vom Management soll einen ungehinderten Zugang zu Ressourcen und Informationen gewährleisten, um die eigenen Funktionen frei von Behinderungen und Voreingenom-

	menheit erfüllen zu können. Sie darf nicht in den Arbeitsablauf der ersten und zweiten Linie integriert sein und ist auch nicht für das Ergebnis der überwachten Prozesse verantwortlich. Management und Interne Revision sind separat rechenschaftspflichtig gegenüber dem Leitungsorgan. Allerdings ist eine kooperative Zusammenarbeit aller drei Linien erforderlich, um Redundanzen oder Lücken zu vermeiden.
Enterprise Resource Planning (ERP)	Das ERP ist die Aufgabe des Unternehmens, Ressourcen (Kapital, Personal, Material) zu planen, zu steuern und zu verwalten. Dies wird in der Praxis mit ERP-Systemen durchgeführt.
Environment, Health and Safety (EHS)	Die Abkürzung EHS steht für die englischen Worte Environment, Health and Safety (auf Deutsch**:** Umweltschutz, Gesundheitsschutz und Arbeitsschutz) und ist damit der nachfolgend genannten Position Environmental, Social and Corporate Governance (ESG) sehr nahe.
Environmental, Social and Governance (ESG)	„Als Standard nachhaltiger Anlagen hat sich die Begrifflichkeit ESG etabliert. Diese drei Buchstaben beschreiben drei nachhaltigkeitsbezogene Verantwortungsbereiche von Unternehmen: 1) Das „E“ für Environment steht hierbei z. B. für Umweltverschmutzung oder -gefährdung, Treibhausgasemissionen oder Energieeffizienzthemen. 2) Social („S“) beinhaltet Aspekte wie Arbeitssicherheit und Gesundheitsschutz, Diversity oder gesellschaftliches Engagement (Corporate Social Responsibility). 3) Unter Governance („G“) wird eine nachhaltige Unternehmensführung verstanden. Hierzu zählen z. B. Themen wie Unternehmenswerte oder Steuerungs- und Kontrollprozesse (Corporate Governance). Verschiedene Nachhaltigkeitsratings basieren auf der Analyse dieser Kriterien.” (*Gabler Wirtschaftslexikon, online*)
Failure Mode and Effect Analysis (FMEA)	FMEA steht für Fehlermöglichkeits- und Einflussanalyse, welche eine System- und Risikoanalyse darstellt. Sie dient dazu, frühzeitig Quellen für mögliche Fehler bezüglich eines Produkts oder Prozesses zu identifizieren und möglichst zu minimieren. Es gibt methodisch unterschiedliche Ansätze bei der Anwendung der FMEA (z. B. präventiv, korrektiv, produkt- oder prozessbezogen).
Internes Kontrollsystem (IKS)	„Das interne Kontrollsystem (IKS) ist ein Teilsystem des Systems zur Überwachung einer Unternehmung, das die Gesamtheit der Mechanismen zur Kontrolle enthält." (*Gabler Wirtschaftslexikon, online*) Instrumente sind z. B. die Funktionstrennung, Vier-Augen-Prinzip, Organisationsplan, Kontenplan, programmierte Abläufe (IT-unterstützter Work-Flow) mit zwangsläufigen maschinellen Kontrollen sowie Stechuhren.

Key Performance Indicator (KPI)	„Der Begriff bezeichnet Kennzahlen, mit denen die Leistung von Aktivitäten in Unternehmen ermittelt werden kann. Welche KPIs betrachtet werden sollten, um Erfolg oder Misserfolg zu messen, hängt vom Unternehmen, der jeweiligen Maßnahme und deren Zielen ab.”
Mergers & Acquisitions (M&A)	Mit dem Begriff wird i. d. R. eine Fusion oder eine Verschmelzung zweier Unternehmen zu einer rechtlichen und wirtschaftlichen Einheit (Merger) bzw. der Erwerb von Unternehmenseinheiten oder eines ganzen Unternehmens (Acquisition) bezeichnet. M&A steht für alle Vorgänge im Zusammenhang mit der Übertragung und Belastung von Eigentumsrechten an Unternehmen einschließlich der Konzernbildung, der Umstrukturierung von Konzernen, der Verschmelzung und Umwandlung im Rechtssinne, dem Squeeze Out, der Finanzierung des Unternehmenserwerbs, der Gründung von Gemeinschaftsunternehmen sowie der Übernahme von Unternehmen. (Gabler Wirtschaftslexikon, online)
Prüfungsziel-/objective, Auftragsziele	Das Prüfungsziel ist das für die individuelle Prüfung festgelegte Ziel. Dieses wird im Rahmen der Auditvorbereitung anhand von prüfspezifischen Risiken festgelegt. Dabei sind Wahrscheinlichkeiten für Fehler, dolose Handlungen, Regelverstöße oder sonstige Risikopotenziale zu berücksichtigen.
Risikoinventar	Ein Risikoinventar ist eine Auflistung von Risiken in einem relevanten Bereich.
Risikolandkarte	Ein Mittel zur Darstellung von identifizierten Risiken und ihrer Bewertung hinsichtlich von Eintrittswahrscheinlichkeit und Auftreten ist die Risikolandkarte.
Scoring-Modell	Ziel des Scorings-Modells ist eine quantifizierte Priorisierung für Prüfungsthemen. Dazu werden z. B. drei Kriterien betrachtet: Finanzieller Schaden, Außenwirkung und Reifegrad.

Kriterium	Beschreibung	Bewertung
Finanzieller Schaden	z. B. Fehlerkosten	Von 1 bis 5: geringer bis existenzbedrohender Schaden
Außenwirkung	z. B. Imageverlust	Von 1 bis 5: nicht wahrnehmbar bis unternehmensweiter Imageschaden
Reifegrad	z. B. stabile Prozesse	Von 1 bis 5: etablierte Einheit mit hohem Reifegrad bis neue Einheit

Beispiel 1:
Neuanlauf eines neuen Produkts an einem neuen Fertigungsstandort: Hohes Qualitätsrisiko (4), Imageverlust (4), neue Mitarbeiter und nicht etablierte Prozesse (5) ➔ 4 x 4 x 5 = 80

Beispiel 2:
Anlauf eines modifizierten Produkts an einem Standort mit bekannt

	hoher Qualität: Kaum Qualitätsrisiko (2), kaum Imageverlust (2), eingelernte Mitarbeiter und stabile Prozesse (1) ➔ 2 x 2 x 1 = 4
Scrum	Gemäß *scrumguides.org* ist Scrum ein Rahmenansatz zur Entwicklung und Erhaltung komplexer Produkte. Der Scrumansatz basiert auf einer konsistenten „definition of Scrum“, spezifischen Rollen, Ereignissen und Artefakten sowie die verbindenden Regeln. Der Scrumansatz wurde entwickelt von Ken Schwaber und Jeff Sutherland.

10 Anhang

10.1 Beispiele für Prüfungsarten

Prüfungsart	**Ziel**	**Vorteile**	**Nachteile**
Spezialprüfung (aktueller Vorfall)	Ursachenanalyse nach Auftreten eines Vorfalls oder nach Hinweis des Managements, um Verbreitung und Wiederholung zu vermeiden	Gezielter Fokus, Übertragung auf andere Bereiche, Vermeidung von Wiederholfehlern	Suche nach Verursachern, Verschleierung
Prozessprüfung	Erkennen von prozessualen Schwachstellen in einem begrenzten Gebiet (z. B. Entwicklung, Fertigung, Prozesskette end-to-end)	Prüfung mit Tiefgang von zuvor definierten Prozessen	Allgemeine Schwachstellen werden nicht erkannt, fundierte Kenntnisse über den Prozess muss im Vorfeld vorhanden sein
Wiederholungsprüfung	Untersuchung der Risiken aus einer vorangegangenen Prüfung sowie der Wirksamkeit der Maßnahmen	Bekannter Scope, Erkennen der Wirksamkeit von umgesetzten Maßnahmen, Zeitaufwand für Prüfungshandlung kann gut ermittelt werden	Reduzierter Prüfumfang und somit kein Überblick über weitere Risiken außerhalb des Prüfungsauftrages
Projektprüfung	Prüfung von Projekten von hoher Bedeutung	Bei begleitender Prüfung über längeren Zeitraum können Risiken zeitnah entschärft werden.	Hoher Personaleinsatz
Governance Prüfung	Prüfung der 2. Line mit Fokus Unternehmensregeln und deren Durchsetzung (PDCA)	Schwachstellen in funktionaler Governance werden erkannt.	Risiken in der Umsetzung in 1. Linie werden nicht erkannt.
Prüfung von Gemeinschaftsunternehmen	Besonderer Fokus auf Risiken wie die Erreichung technischer Synergien	Vergleichende Risikobetrachtung, Lernen von fremden Vorgehensweisen	Erhöhter Aufwand durch fremde Vorgehensweise und ggf.

Prüfungsart	Ziel	Vorteile	Nachteile
			eingeschränktes Prüfrecht
Vollständige Prüfung	Komplette Risikoabdeckung besonders bei neuen Einheiten	Erkennung der Hauptrisiken, Ansätze für Vertiefungsprüfungen, Risikovergleich zwischen Einheiten	Reduzierte Prüftiefe und Schnittstellenanalyse, hoher Aufwand
Beratende Prüfung	Hilfestellung beim Aufbau eines technischen Risikomanagements besonders bei neuen Einheiten oder im PMI	Hinweise zu guten Praktiken und zur Anwendung der Unternehmensregeln	Viel Hilfestellung und Erklärung führt zu reduziertem Prüfumfang.
Standortprüfung	Breiter, risikobasierter Scope auf technische Funktionen an einem Standort (z. B. Werk)	Vergleichbarkeit von Standorten, Erfassung von Standortfunktionen (z. B. Werkssicherheit), objektive Erstbewertung	Reduzierte Prüftiefe, keine End-to-end-Prüfung, reduzierte Schnittstellenbetrachtung, hoher Zeitaufwand
Cluster-Prüfungen	Kleine Einheiten mit ähnlichem Inhalt werden gemeinsam oder repräsentativ geprüft, erkannte Risiken müssen gesamtheitlich gemindert werden.	Reduzierter Aufwand durch Übertragung von Maßnahmen auf nichtgeprüfte Einheiten	Cluster können fehlerhaft und Maßnahmen nicht einfach übertragbar sein.
Sensibilisierungs-Prüfung	Zufällige Auswahl der Einheiten, um Sensibilität hoch zu halten, auch in kürzeren Abständen und bei kleineren Einheiten	Breites Erkennen von Schwachstellen auch ohne konkreten Anlass, Vergleichbarkeit der Ergebnisse	Reduzierte Prüftiefe
Kurzprüfung	Fokus auf Themen, um ggf. frühzeitige Richtungsänderung zu bewirken	Reduzierter Zeit- und Personalaufwand durch Fokus auf wenige, wesentliche Themen	Keine vollständige Risikoabdeckung

10.2 Beispiele für technische Prüfungsthemen

Themenbereich	**Aspekt**	**Prüfungshandlungen**
Betriebliches Kontinuitätsmanagement (BCM)	Lange Wiederherstellungszeit nach Notfall	Durchsicht der Notfallpläne
Energiemanagement	Anstieg der Energiekosten	Wirkungsgrad
	Stromausfälle	Notstrom, alternative Medien
Teilefertigung	Wertstromplanung, Technisches Risikomanagement (FMEA), Prüfungsplanung, Ermittlung und Freigabe von Prozessparametern/ Toleranzen, Software in der Fertigung, Prüfmittel-Management, Fähigkeiten von Fertigungs- und Prüfeinrichtungen, Produktionslenkungsplan, Fertigungsaufzeichnungen, Statistische Prozess-Kontrolle, Schutz vor elektrostatischer Entladung	Dokumentendurchsicht Bewertungen Maschinendaten prüfen an MAE Eingriffsgrenzen in der Fertigung Versionierung System vorhanden, Maßnahmen bei defekten Prüfmitteln, Zeitraum Vorhanden und in Fertigung umgesetzt Eingriffsgrenzen, Fähigkeiten, Frequenzen eingehalten System vorhanden und in der Praxis umgesetzt
Montage	Häufige Störfälle	Begehung Gespräche vor Ort
	Kunden-Auftragsverluste	Gespräche in benachbarten Bereichen (Vertrieb, Service etc.)
	Mangelnde Planerfüllung	KPI, BDE
	Verlängerte Rüstzeiten	Analyse Fehl-, Blind-, Schein- und Wirkleistung
	Losgrößen	Analyse Fehl-, Blind-, Schein- und Wirkleistung
	Ausschuss	Analyse Fehl-, Blind-, Schein- und Wirkleistung

Themenbereich	Aspekt	Prüfungshandlungen
	Lieferengpässe	Make or Buy?
	Fluktuation	Betriebliches Verbesserungswesen
	Ineffizienter Produktionsprozess	Analyse der Verlässlichkeit und Genauigkeit des Planungsprozesses Analyse von manuellen Anpassungen von Produktionsaufträgen
Forschung und Entwicklung	Reduziertes Patentvolumen	Innovationskultur? Anreize? Partnerschaften (Hochschulen)?
	Ablauf von relevanten Patenten	Produkt-Lebenszyklus
	Forschungs-/Entwicklungs-Projektmanagement	Analyse Soll (Plan) und Ist: Produktentstehungsprozess, Projektaufbau und -steuerung: Projekt-Budgetierung, Zeitlicher Projektverlauf, Eskalationsmechanismen → Fokus: Kosten – Qualität – Zeit, Reifegradabsicherung (u. a. Teilfreigaben einzelner Gewerke und Integration zu dem Gesamtgewerk, sicherheitsrelevante Freigaben, Entwicklungsfreigaben gem. Entwicklungszielen
	Produktsicherheit und -konformität	Einhaltung marktspezifischer gesetzlicher Anforderungen zur Produkthaftung und -konformität (Conformity of Production, In-Service Conformity)
Instandhaltung	Instandhaltungsstau	Analyse der Instandhaltungsstrategie Analyse der Instandhaltungsverwaltung Durchsicht der Instandhaltungsdokumentationen Analyse der verschobenen bzw. abgelehnten Ersatzinvestitionen

Themenbereich	Aspekt	Prüfungshandlungen
Lager	Schwund, große Inventur- und Bestandsdifferenzen	List-To-Floor und Floor-To-List Stichproben Begehung der Läger und Beobachtung der Absicherung Analyse der Ausbuchungen von Bestandsdifferenzen
Logistik	Verstöße gegen Ladungssscherungsrecht	Unterweisungen
	Verfügbarkeiten	Substitution Straße/Schiene/Wasser
Qualitätssicherung	Anstieg Reklamationsvolumen	KPI, ext. Audits von Kunden und Zertifizierern
	Kunden-Auftragsverluste	KPI
	Vormaterialgüter	Alternative Lieferanten, Lieferanten-Audits durch die QS
	Produktentwicklung	Prozesse zur Absicherung innerhalb der Produktentstehung
	Produktion	Prozesse zur Sicherstellung der Conformity of Production
	Feldbeobachtung	Prozesse zur Sicherstellung der In-Service Conformity, Überwachung. Feldaktionen, Rückrufe
Standortsicherheit	Beispiele der Standortsicherheit sind: • Gefährdungsbeurteilung (z. B. Festlegung besonders schützenswerter Bereiche), • Sicherheitskonzept (z. B. Festlegung Schutzziele und zugehörige Maßnahmen), • organisatorische Gegebenheiten (z. B. Aufgaben des Werkschutzdienstes), • bauliche Gegebenheiten (z. B. Einfriedung), • technische Gegebenheiten (z. B. Videoüberwachung),	Durchgeführt, sinnvoll, umgesetzt Vorort, wirksam nach Stichprobe. Ablauf eines Besuches Vorort. Freischaltung von neuen Mitarbeitern und prüfen von Mitarbeitern die das Unternehmen verlassen haben. Vorlage von Schlüsselsystemen und deren regelmäßigen Inventur. Prozess und Maßnahmen bei Verlust von Zentralschlüsseln. Prozess bei der Einfahrt und dem Verlassen von LKW. Sinnhaftigkeit und Robustheit des Prozesses und seine Umsetzung.

Themenbereich	Aspekt	Prüfungshandlungen
	• Zutrittskontrolle, • Berechtigungsverwaltung Zutrittskontrollsystem, • Handhabung Besucher und Fremdfirmen, • Schlüsselmanagement und • Reisesicherheit	
Umweltschutz	Gestiegene gesetzliche Anforderungen, u. a. Betreiberverantwortung	Schulungen und Unterweisungen, Anpassung von Arbeits- und Verfahrensanweisungen sowie Prozessbeschreibungen
	Tatsächliche Schäden an Wasser, Boden und/oder Luft	Externe Auditberichte von Zertifizierern
Betriebliches Kontinuitätsmanagement (BCM)	Lange Wiederherstellungszeit nach Notfall	Durchsicht der Notfallpläne

10.3 Beispiele für Datenanalyse bei technischen Prüfungen

Beispiele für Prüfungsthemen und -scope

Prüfung von Verschraubungsdaten, die in der Fertigung generiert wurden und u. a. gesetzliche Dokumentationspflichten begründen, u. a. Drehmomente

Systematische Prüfung von Unter- und Hauptfreigaben der verschiedenen Gewerke in der Technischen Entwicklung im Rahmen des Produktentstehungsprozesses bis zur finalen Verbaufreigabe.

Prüfung des Umgangs mit Abweicherlaubnissen (Anzahl, Ursachen, Verlängerungshäufigkeiten, Tracking/ Monitoring), die während des Entwicklungs- und Produktionsprozesses bis zu dem „End of Service“ generiert wurden (Abweichungen gegenüber Zeichnung, Spezifikation, Qualität etc.)

Datenkonsistenz von technischen Prospektdaten (technische Spezifikation, Verbräuche, etc.) von der Entwicklung über mehrere Schnittstellen/IT-Systeme bis hin zur Aufnahme in die Verkaufsprospekte und in öffentlich zugängliche Internetkonfiguratoren

Systematische Analyse von Bestandsbuchungen in der Materialwirtschaft (Lagerbestände etc.)

- Termineinhaltung (Soll vs. Ist-Termine für Instandhaltung, Maschinenwartung, Prüfungen, …)
- Qualifikation (Termineinhaltung, Inhalte, Pflege von Solls in den Datensätzen)
- Übereinstimmung (Konsistenz) von Daten, falls diese in unterschiedlichen Systemen redundant vorhanden sind
- Tauglichkeit und Qualifikation der Mitarbeiter (Anforderungen hinterlegt, Solltermine vorhanden, Ist-Termine vorhanden, sind die Solltermine übereinstimmend mit den Vorgaben. Beispiel: letzter Ist-Termin bei jährlicher Überprüfung ab dem 50. Lebensjahr gibt rechnerisch den nächsten Solltermin abhängig vom Alter)

11 Literaturhinweise

DIIR. (2017). *DIIR Revisionsstandard Nr. 3.* Frankfurt am Main: DIIR.

DIIR. (2020). *Internal Audit Competency Framework*. Retrieved from https://www.diir.de/fachwissen/internal-audit-competency-framework/

The Institute of Internal Auditors. (2017). *Internationale Standards für die berufliche Praxis der Internen Revision 2017.* Frankfurt am Main: DIIR.

12 Abkürzungsverzeichnis

AK	Arbeitskreis
DIIR	Deutsches Institut für Interne Revision e. V.
ERP	Enterprise Resource Planning
ESG	Environmental, Social and Corporate Governance
EHS	Environment, Health and Safety
FMEA	Failure Mode and Effect Analysis
F&E	Forschung und Entwicklung
IIA	Institute of Internal Auditors
IKS	Internes Kontrollsystem
IoT	Internet of Things
KI	Künstliche Intelligenz
KPI	Key Performance Indikatoren
M&A	Mergers und Acquisitions
MAE	Maschinen und Einrichtungen
SPC	Statistische Prozess Kontrolle
TA	Technical Auditing

Herausgeber

Dieser Leitfaden wurde herausgegeben vom DIIR – Deutsches Institut für Interne Revision e.V.

Veröffentlichung am 8. März 2022 auf **www.diir.de**.

DIIR – Deutsches Institute für Interne Revision e.V.
Theodor-Heuss-Allee 108
60486 Frankfurt am Main