



DIIR

Revisionshandbuch

für die Interne Revision
in Kreditinstituten

DIIR Arbeitskreis MaRisk

Stand: Februar 2026

I. Vorwort

Der DIIR-Arbeitskreis MaRisk hat ein Revisionshandbuch für die Interne Revision in Kreditinstituten erstellt. Grundlage für die im Arbeitskreis verabschiedeten Dokumente sind Regelungen in den Instituten der Mitglieder, die auf den Mindestanforderungen an das Risikomanagement in Kreditinstitute der BaFin (MaRisk) und den Global Internal Audit Standards des IIA (GIAS) basieren. Zielsetzung war es, alle Themen der Revisionsorganisation (auch über die Mindestanforderungen der MaRisk hinaus) in möglichst breit anwendbarer Form darzustellen. Das Handbuch soll dabei auch Anregungen für die Neufassung oder Weiterentwicklung der in Kreditinstituten vorhandenen Revisionshandbücher geben.

Der Anspruch, eine jederzeitige Aktualität mit Blick auf veränderte oder weiterentwickelte Rahmenbedingungen zu gewährleisten, wird jedoch nicht erhoben.

Das gesamte Revisionshandbuch wurde zuletzt im Februar 2026, unter Berücksichtigung der 2024 veröffentlichten GIAS, des Bankenrichtlinienumsetzungs- und Bürokratieentlastungsgesetz (BRUBEG) und der Anforderungen aus dem Digital Operational Resilience Act (DORA), aktualisiert. Wesentliche Änderungen ergaben sich in Kapitel 1 „Ziele, Aufgaben und Strukturen der Internen Revision“ (Schärfung Unabhängigkeit der Internen Revision, Ausführungen zur Revisionsstrategie), in Kapitel 8 „Prüfung von Auslagerungen und IKT-Drittdienstleistungen“ (DORA), in Kapitel 11 „Digitalisierung der Prüfungsprozesse“ (Einsatz von KI in der Internen Revision), in Kapitel 12 „Qualitätssicherung und -verbesserung in der Internen Revision“ (GIAS) und in Kapitel 13 „Leistungsmessung der Internen Revision“ (Ableitung von KPIs aus der Revisionsstrategie). Daneben wurden einzelne Kapitel aufgrund des besseren inhaltlichen Zusammenhangs umgegliedert.

Anmerkungen oder Anregungen für Ergänzungen und Weiterentwicklungen können gerne an die Arbeitskreisleitung [Jürgen Rohrmann](#) und [Bernd Hombach](#) gesendet werden.

II. Inhaltsverzeichnis

I.	Vorwort.....	2
II.	Inhaltsverzeichnis	3
III.	Abbildungsverzeichnis	5
1	Ziele, Aufgaben und Strukturen der Internen Revision	7
2	Externe Rahmenbedingungen	24
3	Standardrevisionsprozess.....	34
4	Begleitung wesentlicher Projekte	75
5	Einbindung der Internen Revision in die Anpassungsprozesse gem. AT 8 MaRisk	80
6	Beratung	83
7	Continuous Auditing/ Continuous-Risk Assessment.....	92
8	Prüfung von Auslagerungen und IKT-Drittdienstleistungen	104
9	Sonderprüfungen zur Aufklärung von Fraud	121
10	Interne Revision im Rahmen von agilen Strukturen (inkl. agile Prüfungsmethodik).....	133
11	Digitalisierung der Prüfungsprozesse	140
12	Qualitätssicherung und -verbesserung in der Internen Revision	151
13	Leistungsmessung der Internen Revision.....	160
14	Gewinnung und Weiterentwicklung von Mitarbeitenden und Fit & Proper- Anforderungen	174
15	Konzernrevision	188
16	Internes Kontrollsystem	202
17	Schnittstelle mit Aufsichtsbehörden, externen Prüfern und der Zweiten Linie	217

18	Nachhaltigkeit in der Revisionsfunktion	224
IV.	Autoren	229

III. Abbildungsverzeichnis

Abb. 1: COSO-Internal Control 2013.....	29
Abb. 2: COSO-Enterprise Risk Management (2004)	30
Abb. 3: COSO: Implications from the strategy	31
Abb. 4: COSO: Enterprise Risk Management (Framework 2017).....	31
Abb. 5: Gegenüberstellung Struktur bisheriges IPPF und Struktur neues IPPF	32
Abb. 6: Prüfungsziele	46
Abb. 7: Berichtspflichten der Internen Revision und rechtliche Grundlagen	69
Abb. 8: Bestandteile der Berichterstattung an Geschäftsleitung und Aufsichtsorgan gemäß § 25c KWG in Verbindung mit BT 2.4 Tz 4 MaRisk.....	70
Abb. 9: Weitere mögliche Berichtsinhalte für die Quartalsberichterstattung	71
Abb. 10: Zusammenfassende Übersicht der Berichtspflichten.....	74
Abb. 11: Der Wert der Internen Revision	83
Abb. 12: Bestandteile des Continuous Auditing	95
Abb. 13: Zusammenspiel von Prüfuniversum, Continuous Auditing und Jahresprüfplan	102
Abb. 14: Notwendigkeit eigener Prüfungshandlungen	107
Abb. 15: Traditional vs. Agile Internal Audit	136
Abb. 16: Elemente des Qualitätsmanagements	152
Abb. 17: KPIs zum Revisionsprozess	168
Abb. 18: KPIs zur Mitarbeitendenperspektive	169
Abb. 19: KPIs zur Finanzperspektive	170

Abb. 20: KPIs zur Stakeholder-Perspektive	171
Abb. 21: Ziele für die Revisionsleitung	173
Abb. 22: Übersicht über die Prüfungsarten aus Konzernsicht.....	194
Abb. 23: Informationsflüsse zwischen den Internen Revisionen der Tochtergesellschaften und der Konzernrevision.....	198
Abb. 24: Mögliche Rollen der Internen Revision der Muttergesellschaft und deren Auswirkung auf die Berichterstattung	200
Abb. 25: Das IIA - Drei Linien-Modell	218

1 Ziele, Aufgaben und Strukturen der Internen Revision

1.1 Ziele der Internen Revision

Nachfolgende Ausführungen sind im Sinne einer Präambel zu verstehen. Konkretisierungen ergeben sich in den jeweiligen nachfolgenden Abschnitten.

Die Ziele der Internen Revision orientieren sich an deren Selbstverständnis und der Erwartungshaltung der Stakeholder.

Die Global Internal Audit Standards (GIAS) beschreiben die Zielsetzung der Internen Revision in Domain 1: Die Interne Revision stärkt die Fähigkeit der Organisation, Werte zu schaffen, zu schützen und zu erhalten, indem sie dem Leitungs- und Überwachungsorgan sowie dem Management unabhängige, risikobasierte und objektive Prüfungssicherheit, Beratung und vorausschauende Erkenntnisse liefert.

Domain 1 der GIAS enthält auch drei Kriterien in Bezug auf die Wirksamkeit der Internen Revision:

- Die Prüfungen werden von kompetenten Revisorinnen und Revisoren entsprechend der Regelungen der GIAS durchgeführt.
- Die Interne Revision ist organisatorisch unabhängig und der Geschäftsleitung direkt unterstellt.
- Interne Revisorinnen und Revisoren sind frei von persönlicher unangemessener Einflussnahme und haben sich zu objektiver Beurteilung verpflichtet.

1.2 Ethik und Professionalität in der Internen Revision

Der Rahmen für die Arbeit der Internen Revision wird in den fünf Prinzipien der Domain 2 der GIAS festgelegt. Diese ersetzen den bisherigen Ethikkodex und die Standards zur Fachkompetenz.

- Integrität: Die Interne Revision handelt nach den moralischen und ethischen Grundsätzen der Standards – auch gegen mögliche Widerstände
- Objektivität: Entscheidungen werden unbeeinflusst getroffen und potenzielle Interessenkonflikte werden offengelegt.
- Kompetenz: Die Interne Revision verfügt über die erforderlichen Kenntnisse und Fähigkeiten und sorgt für kontinuierliche Weiterbildung.

- Berufsbliche Sorgfalt: Die Prüfungen werden mit professioneller Skepsis und Gründlichkeit durchgeführt.
- Vertraulichkeit: Sensible Informationen werden geschützt und nur für den vorgesehenen Zweck genutzt.

Die GIAS betonen, dass diese Prinzipien den Rahmen für alle Prüfungs- und Beratungsleistungen bilden. Sie sind für eine wirksame Revisionstätigkeit unverzichtbar. Insgesamt wird von der Internen Revision ein präventiver und proaktiver Prüfungs- und Beratungsansatz erwartet, um Mehrwerte zu generieren. Die Interne Revision prüft nicht nur die Unternehmens-, Risiko- und Kontrollkultur, sondern ist selbst ein zentraler Einfluss- und Orientierungsfaktor. Durch ihre Beratungs- und Prüfungsschwerpunkte, die Gewichtung von Feststellungen sowie den Umgang mit Mängeln transportiert sie die Erwartungshaltung der Geschäftsleitung und stellt damit selbst einen wichtigen Orientierungspunkt für die Geschäftsbereiche dar.

Für Kreditinstitute nehmen die MaRisk (Mindestanforderungen an das Risikomanagement der Kreditinstitute) als norminterpretierende Verwaltungsvorschrift zu § 25a KWG eine wesentliche ziel- und aufgabensteuernde Funktion ein. Ergänzend wirken, insbesondere bei direkt von der EZB beaufsichtigten Instituten bzw. Institutsgruppen, die europäischen Regelungen, insbesondere Veröffentlichungen der EBA sowie internationale Regelungen, wie z. B. Veröffentlichungen des Basel Committee on Banking Supervision (BCBS) und des Financial Stability Boards (FSB). Die Erweiterung des Normenrahmens für Institute, die besonders groß sind oder deren Geschäftsaktivitäten durch besondere Komplexität, Internationalität oder eine besondere Risikoexponierung gekennzeichnet sind, ergibt sich aus AT 1 Nr. 3 MaRisk.

Sofern die Interne Revision die GIAS gemeinsam mit den regulatorischen Vorgaben (hier: MaRisk) anwendet, sollte sie auf die Anwendung der Vorgaben hinweisen. Sollten Unterschiede zwischen den GIAS und den regulatorischen Anforderungen bestehen, sollte sich die Interne Revision an den jeweils restriktiveren Vorgaben ausrichten.

Die Ziele und die organisatorische Verankerung der Internen Revision (Befugnisse, Aufgaben und Verantwortlichkeiten) werden in ihrer Geschäftsordnung (auch „Audit Charter“ oder „Rahmenbedingungen der Internen Revision“) operationalisiert und konkretisiert und bestimmen den von der Geschäftsleitung gesetzten Rahmen für das Tätigkeitsfeld der Internen Revision (siehe dazu auch GIAS Standard 6.2). Es empfiehlt sich, hierbei auch das Aufsichtsorgan zu einzubeziehen.

Falls auch Leistungen für externe Dritte erbracht werden sollen, ist dies in der Geschäftsordnung zu fixieren. Originäre Tätigkeitsfelder dürfen hierdurch nicht geschwächt werden.

Die Folgen einer etwaigen Ressourcenbeschränkung (z. B. Personal, Sachmittel) hat die Leitung der Internen Revision an die Geschäftsleitung und das Aufsichtsorgan zu kommunizieren (GIAS Standards 8.2 und 10.2).

Die periodenbezogene Konkretisierung ihrer Aufgabenstellung erfolgt durch die Genehmigung des Prüfungsplans der Internen Revision durch die Geschäftsleitung (BT 2.3 Tz. 5 MaRisk). Ergänzend sollte das Aufsichtsorgan über den genehmigten Prüfungsplan in Kenntnis gesetzt werden (GIAS Standard 9.4). Aufgrund der Besonderheiten der deutschen Unternehmensverfassung, in der das Aufsichtsorgan im Kern eine Überwachungsfunktion wahrnimmt, kann der betreffende Standard, der eigentlich zusätzlich zur Kenntnisnahme eine Genehmigung vorsieht, nicht vollständig angewendet werden.

Gemäß BT 2.3 Tz. 1 MaRisk muss die Tätigkeit der Internen Revision auf einem umfassenden und jährlich fortzuschreibenden Prüfungsplan basieren. Die Prüfungsplanung hat risikoorientiert zu erfolgen. Die Aktivitäten und Prozesse des Instituts sind, auch wenn diese ausgelagert sind, in angemessenen Abständen, grundsätzlich innerhalb von drei Jahren, zu prüfen. Wenn besondere Risiken bestehen, ist jährlich zu prüfen. Bei unter Risikogesichtspunkten nicht wesentlichen Aktivitäten und Prozessen kann ein Turnus von fünf Jahren angemessen sein¹. Die Risikoeinstufung der Aktivitäten und Prozesse ist regelmäßig zu überprüfen.

Die BaFin hat in den Erläuterungen zu BT 2.3 Tz. 1 MaRisk jedoch klargestellt, dass ein Abweichen vom dreijährigen Turnus für unter Risikogesichtspunkten nicht wesentliche Aktivitäten und Prozesse nicht mit einem weitgehenden Verzicht auf Revisionsprüfungen in diesen Bereichen verbunden sein kann. Auch diese sind in die Prüfungsplanung zu integrieren und in angemessenen Abständen zu prüfen. Die Genehmigung des Jahresprüfungsplans durch die Geschäftsleitung ist die formelle Beauftragung der Internen Revision.

Zur Sicherstellung der Berücksichtigung aller gesetzlich oder aufsichtsrechtlich vorgeschriebenen Prüfobjekte sollten diese systematisch erfasst werden. In Abhängigkeit des verwendeten Ansatzes (funktions-, prozess- oder aufgabenorientiert) kann man die Prüfobjekte strukturieren.

Als zentrale Prüfobjekte definieren sowohl die MaRisk als auch das GIAS das Risikomanagement und das interne Kontrollsystem (AT 4.4.3 Tz. 3 MaRisk).

Aus den Erläuterungen der GIAS ist sowohl die Ziel- als auch die Komponentendimension des COSO-Enterprise Risk Management (ERM) 2004 als auch die Hervorhebung der Bedeutung von Vision, Mission, Grundwerte und Risikokultur des COSO ERM 2019

¹ Vgl. BaFin, Protokoll zur virtuellen Sitzung des Fachgremiums MaRisk am 01.03.2023.

zu erkennen. Hieraus leiten sich auch die klassischen Tätigkeitsfelder einer Internen Revision Financial Auditing, Compliance Auditing und Operational Auditing ab. Die verpflichtenden Fraud-, IT- und strategiebezogenen Prüfungshandlungen (GIAS Standard 13.2) sind hierbei als Spezialfall des Compliance Auditing bzw. des Operational Auditing einzuordnen.

Bei der Durchführung ihrer Aufgaben hat die Interne Revision die Anforderungen an die „Organisatorische Unabhängigkeit der Internen Revision“ (siehe Abschnitt 1.4.1) und die „Persönliche Unabhängigkeit und Objektivität der Revisionsmitarbeiter“ (siehe Abschnitt 1.4.2) zu beachten.

Weitere Grenzen der eigenen Prüfungstätigkeit ergeben sich, wenn die Interne Revision für Prüfobjekte nicht über das entsprechende Fachwissen verfügt. In diesem Fall kann neben dem Outsourcing der betreffenden Internen Revisionstätigkeit auch ein befristeter Einkauf von Fachkompetenz in die Interne Revision (Co-Sourcing) sinnvoll sein.

Konkretisierungen zu einzelnen Prüfobjekten ergeben sich sowohl aus den Topical Requirements (z. B. Topical Requirements zur Cybersicherheit, zum Drittparteien-Risiko und zum Verhalten in Organisationen) als auch aus den DIIR-Revisionsstandards (z. B. Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision“ und Nr. 4 „Prüfung von Projekten“).

Bei Kreditinstituten ergeben sich Prüfobjekte auch direkt aus dem Aufsichtsrecht; z. B. aus der CRR (z. B. Artikel 191 CRR: mindestens jährliche Prüfung der Ratingsysteme des Instituts).

Weitere Anforderungen bzw. Anregungen können sich aus Veröffentlichungen der EBA (Leitlinien, Technische Standards und Empfehlungen), z. B. Leitlinien zur Internen Governance (EBA/GL/2021/05) und BCBS-Veröffentlichungen, z. B. „The internal audit function in banks“, ergeben.

Weitere Tätigkeitsfelder/Prüfungsobjekte können sich aufgrund von Verbandsempfehlungen, durch Vorgaben der jeweiligen Sicherungseinrichtungen bzw. aus Versicherungsbedingungen, z. B. Vertrauensschadensversicherungen, ergeben. Daneben sollten die Einlagerungsverträge sowie andere Verträge dahingehend untersucht werden, welche spezifischen Prüfungshandlungen und Berichtspflichten von der Internen Revision erwartet werden.

Zur Prüfungstätigkeit gehört sowohl nach dem allgemeinen Verständnis als auch nach BT 2.5 Tz. 1 MaRisk die Überwachung der fristgerechten Beseitigung von Mängeln (Follow-up).

Die Behebung von Mängeln sollte zeitnah individuell validiert werden. Je nach Schweregrad der Feststellungen, kann die Intensität der Validierung angepasst werden, z. B. Plausibilisierung für geringere Mängel, substantielle Prüfungshandlungen für schwerwiegende Mängel (vgl. Abschnitt 3.5). Ggf. ist eine Nachschauprüfung anzusetzen.

Neben der Prüfungstätigkeit ist allgemein und aufsichtsrechtlich anerkannt, dass eine Interne Revision auch Beratungsleistungen erbringen kann (siehe Definition des IIA/DIIR; BT 2.2 Tz. 2 MaRisk). Es besteht aber keine Verpflichtung einer Internen Revision Beratungsdienstleistungen zu erbringen. Ob eine Interne Revision grundsätzlich Beratungsdienstleistungen erbringen soll, ergibt sich aus deren Geschäftsordnung (Audit Charter) und ist damit Entscheidung der Geschäftsleitung (GIAS Standard 6.1).

Für Beratungsleistungen sind in der Geschäftsordnung bzw. im Revisionshandbuch die Erwartungshaltung der Stakeholder sowie der organisatorische Rahmen (Grundsätze, Abgrenzung, Aufgabefelder, Prozessablauf, Kompetenzen etc.) zu fixieren. Hierbei können/sollten die beratungsbezogenen Regelungen der GIAS, berücksichtigt werden (vertiefend zur Beratung Abschnitt 6).

Für Kreditinstitute ergeben sich aus den MaRisk weitere Aufgabenstellungen. Im Falle wesentlicher Projekte ist eine Projektbegleitung notwendig (BT 2.1 Tz. 2 MaRisk). Dies muss nicht zwingend in Form einer Prüfungstätigkeit und nicht zwingend kontinuierlich erfolgen. Das konkrete Vorgehen wird sich an Wesentlichkeitsüberlegungen ausrichten (vertiefend Abschnitt 4).

Aufsichtsrechtlich wird weiterhin eine Einbindung der Internen Revision im Rahmen ihrer Aufgaben, insbesondere in folgende Prozesse, gefordert:

- Erläuterung zu AT 4.2 Tz. 1 MaRisk: Strategien
- AT 8.1 Tz. 5 MaRisk: Neu-Produkt-Prozess
- AT 8.2 Tz. 1 MaRisk: Änderungen betrieblicher Prozesse oder Strukturen
- AT 9 Tz. 2 MaRisk: Auslagerung

Als weitere Aufgabenstellung ergibt sich aus den GIAS und aus den MaRisk eine eigenständige Qualitätsmanagementaufgabe für die Interne Revision bezogen auf die Revisionsprozesse (BT 2.3 Tz. 3 MaRisk; GIAS Standard 8.3).

Hinsichtlich der Anforderungen an die Qualitätssicherung und -verbesserung sollte auf die Anforderungen der GIAS abgestellt werden. Der Standard empfiehlt u. a. Produktivitätsuntersuchungen, Analysen der Kosteneffizienz, Beurteilung der Beziehungen zu Geschäftsleitung und anderen Stakeholdern und andere Leistungsmessungen der Internen Revision (siehe auch GIAS Standard 12.2). Jährlich sollte eine Selbstbeurteilung auf Basis des DIIR-Standards Nr. 3 erfolgen.

Regelmäßig (mindestens alle fünf Jahre) muss eine externe Beurteilung der Qualität erfolgen (GIAS Standard 8.4). Die Leitung der Internen Revision muss die Ergebnisse der Beurteilung mit der Geschäftsleitung und dem Überwachungsorgan besprechen. Hinsichtlich der mindestens alle fünf Jahre durchzuführenden externen Qualitätsbeurteilung ist zu entscheiden, ob eine vollständige externe Beurteilung oder eine Selbstbeurteilung mit unabhängiger Bestätigung durchgeführt wird. Die Leitung der Internen Revision muss die Form und Häufigkeit externer Beurteilungen sowie die Fachkenntnis und Unabhängigkeit des externen Beurteilers einschließlich möglicher Interessenkonflikte mit der Geschäftsleitung und dem Überwachungsorgan besprechen.

Das Überwachungsorgan wird für seine Überwachungsverantwortung in Bezug auf die Wirksamkeit der Internen Revision über § 107 Abs. 3 S. 2 AktG nochmals explizit in die Pflicht genommen. Über § 324 HGB („Prüfungsausschuss“) erfolgte die Übertragung auf kapitalmarktorientierte Kapitalgesellschaften im Sinne des § 264d HGB. Eine entsprechende aufsichtsrechtliche Verpflichtung ergibt sich aus § 25d Abs. 9 Nr. 2 KWG.

Zur Wahrnehmung seiner Überwachungsfunktion wird erwartet, dass sich das Aufsichtsorgan mit den Aspekten „Prüfungsplan“, „Prüfungsmethoden“ und „Ressourcenausstattung“ der Internen Revision auseinandersetzt. Das Aufsichtsorgan wird zukünftig stärker leitende Mitarbeitenden in Kernfunktionen im Rahmen seiner Überwachungstätigkeit konsultieren. Die Informationsfunktion der Internen Revision für das Aufsichtsorgan gewinnt weiter an Bedeutung. Aufsichtsrechtlich wurde bezüglich der Internen Revision folgende explizite Regelung getroffen:

- § 25c Abs. 4a lit. h KWG: Direkter Zugang des Leiters der Internen Revision zum Aufsichtsorgan
- § 25d Abs. 9 S. 3 KWG: Auskunftsrecht des Vorsitzenden des Prüfungsausschusses
- AT 4.4.3 Tz. 2 MaRisk: Auskunftsrecht des Vorsitzenden des Aufsichtsorgans

Obiger Informationsprozess, insbesondere die Einbeziehung der Geschäftsleitung, ist in den jeweiligen Geschäfts- und Informationsordnungen der Geschäftsleitung, des Aufsichtsorgans oder des Prüfungsausschusses zu regeln.

Veränderungen in der Position der Leitung der Internen Revision sind vom Aufsichtsorgan in seiner Überwachung besonders zu berücksichtigen (AT 4.4.3 Tz. 6 MaRisk).

Hintergrund ist, dass das Aufsichtsorgan die Möglichkeit haben soll, mit der Leitung der Internen Revision die Gründe für sein Ausscheiden zu erörtern. Für die Information an das Aufsichtsorgan ist daher eine verantwortliche Stelle festzulegen und ein geeigneter Prozess einzurichten.

1.3 Struktur und Berichtslinien

1.3.1 Struktur der Revision

Die Gestaltung der Aufbauorganisation der Internen Revision ist eine der wesentlichen Aufgaben in Verantwortung der Leitung der Internen Revision. Sie sollte sich an der Struktur, den Zielen und der Strategie des Unternehmens orientieren und eine effektive und effiziente Erfüllung aller Aufgaben der Internen Revision gewährleisten. Bei der konkreten Gestaltung der Aufbauorganisation können die nachfolgend beispielhaft genannten, grundsätzlich möglichen Ansätze zur Organisation einer Internen Revision in Betracht gezogen werden:

- Orientierung an Geschäftsfeldern (Vorstandsbereichen) der Bank (z. B. Privatkunden, Firmenkunden, Investmentbanking, IT, etc.)
- Orientierung an Risikoarten (z. B. Kredit-, Markt-, Operationelle Risiken, etc.)
- Orientierung an Prozessen (z. B. Marktprozesse, Back-Office-Prozesse, Steuerungsprozesse, Infrastrukturprozesse, etc.)
- Kompetenzzentren/Fachgruppen (z. B. Kredit, Handel, IT, Allgemeine Revision, etc.)
- Pooling von Prüfern (Pooling in einer oder nach wenigen Fachgebieten unterteilten Gruppen und einzelprüfungsbezogene Bildung von Prüfungsteams)
- Bündelung von revisionsinternen Grundsatz-/Steuerungs-/Qualitätsmanagement- und Supportaufgaben

Für die Festlegung der Struktur ist auch die Größe der Revisionseinheit insgesamt ein wesentliches Kriterium, wodurch Mischformen der o. a. möglichen Ausprägungen sinnvoll sein können.

1.3.2 Zentrale/dezentrale Organisation

Bei einem Institut, das aus mehreren rechtlichen Einheiten besteht und/oder in unterschiedlichen Lokationen/Ländern vertreten ist, stellt sich zusätzlich die Frage, inwieweit eine dezentrale Organisation der Revision sinnvoll oder sogar aufsichtsrechtlich gefordert ist. Hierfür sind aufbauorganisatorische Grundlagen für eine Konzernrevision und die Revisionsabteilungen der nachgeordneten Unternehmen zu schaffen.

Während die zentrale Organisation eine einheitliche Vorgehensweise und Außenwirkung der Revision im Unternehmen besonders unterstützt und die Nähe zur Konzernleitung im

Vordergrund steht, kann eine dezentrale Organisation lokations-/unternehmensspezifischen Anforderungen sehr zielgerichtet entsprechen und die Verantwortung der dezentralen Unternehmensleitungen unterstützen.

Weitere Ausführungen zu Konzernrevision und dem Zusammenwirken mehrerer Revisi-
onseinheiten innerhalb eines Konzerns enthält Abschnitt 12.

1.3.3 Berichtslinien

Neben der in den MaRisk verankerten Berichtspflicht der Revision an die Geschäftsleitung bzw. an das Aufsichtsorgan sind grundsätzlich Ziele, Aufgabenstellung, organisatorische Zuordnung und Berichtslinien der Internen Revision in einer Geschäftsordnung der Internen Revision (Rahmenbedingungen, Audit Charter, o. ä.) zu regeln (vgl. Abschnitt 1.5). Hinsichtlich einer wirksamen Kommunikation liefert GIAS Standard 11.1 weiterführende Unterstützung.

Die „Berichtslinien“ stellen die „disziplinarische Zuordnung“ und die „fachliche Zuordnung“ dar. Eine Differenzierung kann hier insbesondere in Konzernen, bei denen in Tochtergesellschaften eine Revisionsabteilung eingerichtet ist, sinnvoll sein; hierbei können die disziplinarische Zuordnung zur lokalen Geschäftsleitung und die fachliche Zuordnung zur Konzernrevision erfolgen.

Die organisatorische Zuordnung der Internen Revision hängt insbesondere von den länderspezifischen regulatorischen Rahmenbedingungen sowie der Gesellschaftsform ab. Während in angelsächsisch geprägten Ländern im Wesentlichen das „monistische“ System der Bündelung von Geschäftsführungs- und Überwachungsaufgaben in einem Organ („one-tier board system“) vorzufinden ist, sind in Zentraleuropa die Geschäftsführung und die Überwachung in unterschiedlichen Organen getrennt angesiedelt („two-tier board system“).

Entsprechend der MaRisk ist die Verantwortung für die Interne Revision der Geschäftsleitung zugeordnet (siehe hierzu auch weitere externe Rahmenbedingungen gemäß Abschnitt 3). Empfohlen wird die Zuordnung zum Vorsitzenden der Geschäftsleitung, in begründeten Fällen sind jedoch Berichtslinien an andere Mitglieder der Geschäftsleitung möglich.

Gemäß § 25c Abs. 4a Nr. 3 lit. g KWG bzw. § 25c Abs. 4b Nr. 3 lit. g KWG haben die Geschäftsleiter bzw. die Geschäftsleiter des übergeordneten Unternehmens Sorge zu tragen, dass die Interne Revision bzw. die Konzernrevision in angemessenen Abständen, mindestens vierteljährlich, an die Geschäftsleitung und an das Aufsichts- oder Verwal-

tungsorgan berichtet. Insbesondere bei riskanten Entwicklungen kann der Leiter der Internen Revision, unabhängig von der Geschäftsleitung, direkt an das Aufsichtsorgan berichten (§ 25c Abs.4a lit. h KWG).

Bei einem in § 25d Abs. 7 KWG genannten Unternehmen soll das Verwaltungs- oder Aufsichtsorgan, abhängig von der Größe, der internen Organisation und der Art, des Umfangs, der Komplexität und dem Risikogehalt der Geschäfte des Unternehmens, aus seiner Mitte einen Prüfungsausschuss zu bestellen. Dieser unterstützt das Verwaltungs- oder Aufsichtsorgan gemäß § 25d Abs. 9 Nr. 2 KWG insbesondere bei der Überwachung der Wirksamkeit des Risikomanagementsystems, insbesondere des internen Kontrollsystems und der Internen Revision. Entsprechende Auskunftsrechte des Prüfungsausschusses bzw. Berichtslinien der Internen Revision sind zu regeln.

1.4 Organisatorische Bedingungen für die Interne Revision

1.4.1 Organisatorische Unabhängigkeit der Internen Revision

Die organisatorische Unabhängigkeit der Internen Revision ist wesentliches Merkmal jeglicher Revisionstätigkeit (GIAS Standard 7.1). Die Leitung der Internen Revision sollte der Ebene innerhalb der Organisation unterstehen, die sicherstellen kann, dass die Interne Revision ihre Aufgaben sachgerecht erfüllen kann. Um einen für die wirksame Ausführung der Revisionsaufgaben hinreichenden Grad der Unabhängigkeit zu erzielen, berichtet die Leitung der Internen Revision funktional an die Geschäftsleitung bzw. das Überwachungsorgan und hat direkten und unbeschränkten Zugang zu diesen. Die Leitung der Internen Revision bestätigt der Geschäftsleitung bzw. dem Überwachungsorgan mindestens jährlich die organisatorische Unabhängigkeit.

Im Fall des Verlustes der Unabhängigkeit ist die Funktionsfähigkeit der Revision ist nicht mehr gegeben.

Die Wahrung und Ausgestaltung der organisatorischen Unabhängigkeit der Internen Revision, speziell in Kredit- und Finanzdienstleistungsinstituten, begründet sich aus folgenden Gesetzen und aufsichtsrechtlichen Regelungen:

- Die Notwendigkeit einer unabhängigen Internen Revision, die nicht mit anderen Geschäftsbereichen oder Kontrollfunktionen des Instituts kombiniert werden darf, begründet sich in § 25a Abs. 1 S. 3 Nr. 3 KWG.
- Die organisatorische Unabhängigkeit der Internen Revision ist normenkonkretisierend durch die BaFin in den MaRisk AT 4.4.3 Ziffer 2 gefordert. Demgemäß ist die Interne Revision ein Instrument der Geschäftsleitung, ihr unmittelbar unterstellt und

berichtspflichtig. Konkretisiert wird in BT 2.2. Ziffer 1 die selbständige und unabhängige Erledigung der Aufgaben durch die Interne Revision.

- Erweitert wird die bankaufsichtliche Erwartung zur personellen Verantwortlichkeit für die Interne Revision durch die Öffnungsklausel, dass diese auch einem Mitglied der Geschäftsleitung, nach Möglichkeit dem Vorsitzenden, unterstellt sein kann. Hieraus ergibt sich eine mögliche Unterstellung der Revision nach folgender Abstufung: Gesamtvorstand, Vorstandsvorsitzender, nur bei objektiver Unmöglichkeit ein anderes Vorstandsmitglied.

Eine weitere Stärkung der Unabhängigkeit der Internen Revision ergibt sich aus § 25c Abs. 4a lit. i KWG, danach kann der Leiter der Internen Revision nicht ohne vorherige Zustimmung durch das Aufsichtsorgan von seiner Funktion entbunden werden. In eilbedürftigen Fällen kann der Vorsitzende des Aufsichtsorgans die Zustimmung vorläufig erteilen.

Die Prüfung der Angemessenheit des Risikomanagements und der Geschäftsorganisation umfasst nach § 11 Abs. 2 Ziffer 4 der Prüfungsberichtsverordnung auch die Beurteilung der Angemessenheit der Internen Revision. Dabei greift der Abschlussprüfer auf die berufsfachliche Stellungnahme des IDW PS 321 „Interne Revision und Abschlussprüfung“ zurück. Die Weisungsunabhängigkeit der Internen Revision ist dabei ein elementarer Beurteilungsfaktor.

1.4.2 Prozessunabhängigkeit der Internen Revision

Die Unabhängigkeit der Internen Revision von den Prozessen des Instituts ist neben der organisatorischen Unabhängigkeit eine weitere elementare Anforderung. Diese wurde mit der Änderung des § 25a Abs. 1 S. 3 Nr. 3 durch das Bankenrichtlinienumsetzungs- und Bürokratieentlastungsgesetz (BRUBEG) Anfang 2026 noch einmal besonders betont, danach gehört die Einrichtung „einer unabhängigen Internen Revision“ zu den Aufgaben der Geschäftsleitung, weiterhin wird klargestellt, dass die Interne Revision nicht mit anderen Geschäftsbereichen oder Kontrollfunktionen des Instituts kombiniert werden darf. Nach AT 4.4.3 Ziffer 3 der MaRisk hat die Interne Revision prozessunabhängig zu prüfen und zu beurteilen. Hiermit sollen die Neutralität und Objektivität der Internen Revision grundsätzlich gewährleistet werden.

Gemäß GIAS Standard 7.1 kann die Objektivität als beeinträchtigt angenommen werden, wenn die Leitung der Internen Revision die Verantwortung für die geprüfte Organisationseinheit trägt oder wenn bestimmte Beratungsleistungen durch die Interne Revision im geprüften Bereich erbracht wurden (vgl. Abschnitt 6). Bedrohungen der Unabhängigkeit sind auf Prüfer-, Prüfungs-, Funktions- und Organisationsebene zu steuern.

Die Bedeutung der prozessualen Unabhängigkeit findet auch in den besonderen Anforderungen der MaRisk an die Ausgestaltung der Internen Revision Berücksichtigung. So

wird beispielsweise der Revision in BT 2.1 Ziffer 2 aufgegeben, bei wesentlichen Projekten begleitend tätig zu sein. Der Wahrung der Unabhängigkeit und der Vermeidung von Interessenkonflikten wird allerdings ein höherer Stellenwert als der Projektmitwirkung beigemessen, denn diese sind als Kausalbedingungen in die Anforderung zur Projektbegleitung integriert (vertiefend zur Projektbegleitung Abschnitt 4).

1.4.3 Persönliche Unabhängigkeit und Objektivität der Revisionsmitarbeitenden

Die MaRisk adressieren grundsätzlich ihre Anforderungen an die organisatorische Ebene der Internen Revision. Zur Wahrung der sachbezogenen Unabhängigkeit dient MaRisk BT 2.2 Ziffer 3, wonach die in der Internen Revision beschäftigten Mitarbeitenden grundsätzlich nicht mit revisionsfremden Aufgaben betraut werden dürfen. Die Anforderung wird dadurch verstärkt, dass sie insbesondere keine Aufgaben wahrnehmen dürfen, die mit der Prüfungstätigkeit nicht im Einklang stehen. Hiervon betroffen sind auch Mitarbeiter anderer Organisationseinheiten des Instituts, die in die Interne Revision wechseln. Für diese sind grundsätzlich angemessene Übergangsfristen von mindestens einem Jahr vorzusehen, bevor sie in Prüfungsaktivitäten betreffend das vorherige Arbeitsgebiet eingebunden werden können („cooling off“). Hierdurch wird sichergestellt, dass sachliche Beeinträchtigungen die Unabhängigkeit und Objektivität nicht beeinträchtigen sollen. Gemäß GIAS Standard 2.2 kann die Objektivität als beeinträchtigt angenommen werden, wenn ein Interner Revisor eine Aktivität prüft, für die er im Verlauf des vorangegangenen Jahres operativ verantwortlich war. Unter Berücksichtigung des Proportionalitätsprinzips sind Erleichterungen aber möglich (BT 2.2 Tz. 3 MaRisk). Gründe für Beeinträchtigungen der individuellen Unabhängigkeit und der persönlichen Objektivität können aber auch aus der geschützten Privatsphäre (z. B. Partner, Freunde) der Mitarbeitenden resultieren. Sofern sich Mitarbeitende im Einzelfall hierzu nicht tiefergehend äußern möchten, sollte auch die Möglichkeit bestehen, dass sie die Beeinträchtigung ihrer Unabhängigkeit ohne Angabe von Gründen erklären können. Verantwortlich für seine Objektivität und seine individuelle Unabhängigkeit ist jeder Mitarbeitende selbst (GIAS Standard 2.1).

Von der Revisionsleitung sind organisatorische Regelungen zu schaffen, um dies angemessen in die Revisionsorganisation umsetzen. Dazu können gehören:

- Arbeitsvertragliche bzw. arbeitsanweisende Regelungen zur Wahrung der individuellen Unabhängigkeit und Verpflichtung zur Objektivität
- Turnusmäßige Befragung/Bestätigungen der Mitarbeitenden zu Beeinträchtigungen der individuellen Unabhängigkeit und Objektivität (ohne Verpflichtung zur Benennung von Gründen)
- Zusicherung der Vertraulichkeit freiwillig gegebener Informationen durch die Leitung der Internen Revision

- Anlassbezogene Verpflichtung der Mitarbeitenden bei besonders sensiblen Prüfungssachverhalten

Unabhängig von diesen Regularien muss der Mitarbeitende allerdings immer eine entsprechende Unabhängigkeit als Charaktereigenschaft mitbringen. Insofern kommt diesem Thema auch bei der Gewinnung neuer Mitarbeitender eine besondere Bedeutung zu.

1.4.4 Informationsrecht

Die MaRisk sehen in AT 4.4.3 Ziffer 4 ein vollständiges und uneingeschränktes Informationsrecht zur Wahrnehmung ihrer Aufgaben vor und verstärken diese Grundaussage durch die Anforderung diese Informationen der Revision unverzüglich, d. h. ohne schuldhaftes Zögern, zu geben, Unterlagen zur Verfügung zu stellen und Einblick in die Aktivitäten, Prozesse und IT-Systeme zu gewähren. Dieses Recht bezieht sich auch auf Weisungen und Beschlüsse der Geschäftsleitung, die für die Interne Revision von Bedeutung sein können.

In den von der Geschäftsleitung zu beschließenden Rahmenbedingungen (Charta, Geschäftsanweisung, Audit Policy) der Internen Revision sollte konkret geregelt werden, wie weit die Informationsrechte der Internen Revision gehen. Grundsätzlich sollten dabei keine Einschränkungen aufgenommen werden, die die Interne Revision in die Situation bringt, Begründungen für die Informationsbeschaffungen gegenüber den Fachbereichen liefern zu müssen. Allerdings ist in den Arbeitsanweisungen sicherzustellen, dass ein Bezug zur Aufgabenstellung stets gegeben ist und die Vertraulichkeit von Unternehmensgeheimnissen gewahrt bleiben muss.

Hat das Unternehmen eine Klassifizierung der Sensibilität von Unterlagen eingeführt, können hierauf Berechtigungen zur Informationsbeschaffung eingeführt werden.

Bestehen von Seiten der geprüften Organisationseinheiten Zweifel an der Notwendigkeit von angeforderten sensiblen Informationen, muss innerhalb der Internen Revision kompetenzgerecht über deren Nutzung im Unternehmensinteresse entschieden werden. Dieses Recht ist insbesondere bei Untersuchungen möglicher doloser Handlungen, bei denen eine verdeckte Prüfung erfolgt, von Bedeutung. Bei der Ausübung des Informationsrechts sind jedoch bestehende Betriebs-/Personalvereinbarungen und die Vorschriften des Datenschutzes zu beachten (vgl. Abschnitt 9).

Weiterhin wird die Interne Revision sich und den geprüften Einheiten regelmäßig die Frage beantworten müssen, was nach dem Need-to-know-Prinzip im Rahmen der Prüfung zur Erreichung der Prüfungsziele angemessen und verhältnismäßig ist (vgl. Abschnitt 1.4.5). Die zur Erreichung der Prüfungsziele notwendige Informationsverwertung

ist grundsätzlich zulässig. Dies sollte durch eine wirksame Ableitung von Prüfungszielen und -handlungen dokumentiert werden.

1.4.5 Vertraulichkeit und schutzwürdige Interessen

Die weit reichenden Befugnisse der Internen Revision führen zu einem besonderen Anspruch an die Vertraulichkeit im Umgang mit den gewonnenen sensiblen Informationen (GIAS Standard 5.2). Im Rahmen der Revisionsarbeit sind selbstverständlich gesetzlich geschützte Rechte von Personen zu beachten, insbesondere i. S. d. des BDSG und der DSGVO. Soweit möglich, sind „Sachverhalte“ von „Personen“ zu trennen und bei personenbezogenen Aussagen (z. B. Vorverurteilungen, persönliche Beziehungen, Interessenkonflikten) ist der Grundsatz der Objektivität stringent zu beachten. Insbesondere ist es erforderlich, besonders vertrauliche Informationen auch während und nach der Prüfung adäquat zu schützen, z. B. bei der Auswertung von personenbezogenen Daten von Mitarbeitenden oder Kunden. Daher ist der Zugriff auf die Prüfungsunterlagen zu regeln, geeignete Verfahren zum Datenschutz zu implementieren (z. B. Pseudonymisierung und Anonymisierung), ggf. der Datenschutzbeauftragte der Organisation einzubinden und – bei Berührung von Mitarbeiterinteressen – auch der Personal-/Betriebsrat in die Abstimmung über eine beabsichtigte Prüfung einzubeziehen.

Über diese schutzwürdigen Interessen hinaus ist die Vertraulichkeit von sensiblen personenbezogenen und unternehmensinternen Sachverhalten von der Leitung der Internen Revision organisatorisch sicherzustellen. Dies beginnt bei der Personalauswahl, der vertraglichen oder arbeitsanweislichen Mitarbeiterverpflichtung zum Ausschluss der Nutzung von Daten zum persönlichen Vorteil bzw. zum Nachteil des Arbeitgebers als auch für Regelungen über die Speicherung, Weiterleitung und Archivierung von Revisionsdaten.

Die Wahrung der Vertraulichkeit und der Verstoß gegen schutzwürdige personenbezogene Interessen müssen von der Leitung der Internen Revision angemessen überwacht und bei Verstößen sanktioniert werden.

1.5 Schriftlich fixierte Ordnung der Internen Revision

Unter der schriftlich fixierten Ordnung ist die Regelung hinsichtlich der Aufgabenstellung, Befugnisse und Verantwortung der Internen Revision zu verstehen. Wesentliche Anforderungen an die schriftlich fixierte Ordnung sind in den MaRisk sowie in den GIAS und weiteren Veröffentlichungen von IIA sowie DIIR enthalten.

Gemäß MaRisk (AT 4.3.1 Aufbau- und Ablauforganisation sowie AT 5 Organisationsrichtlinien) sind Prozesse sowie die damit verbundenen Aufgaben, Kompetenzen, Verantwort-

lichkeiten, Kontrollen sowie Kommunikationswege klar zu definieren und aufeinander abzustimmen. Es ist sicherzustellen, dass die Geschäftsaktivitäten auf der Grundlage von Organisationsrichtlinien betrieben werden, welche u. a. Regelungen zur Internen Revision beinhalten müssen. Die schriftlich fixierte Ordnung ist somit ein wesentlicher Bestandteil des Risikomanagements einer Unternehmung und auch für die Interne Revision angemessen zu gestalten.

Zu den berufsständischen Regelungen des IIA sind im Wesentlichen die GIAS Standards 6.1, 6.2 und 9.3 zu nennen. Auch wenn in Standard 9.3 für „kleine Revisionsabteilungen“ geringere formale Anforderungen an ein Revisionshandbuch gestellt werden, so ist doch die vollumfängliche Ausgestaltung einer schriftlich fixierten Ordnung als Best Practice zu betrachten.

Dem DIIR Standard Nr. 3 (Prüfung von Internen Revisionssystemen – Quality Assessment) in Verbindung mit dem Leitfaden zur Qualitätsbeurteilung (Glossar) können unter dem Stichwort „Regelung“ folgende wesentlichen Elemente der schriftlich fixierten Ordnung entnommen werden:

Die „Geschäftsordnung“ der Internen Revision ist ein offizielles schriftliches Dokument, das Aufgabenstellung, Befugnisse und Verantwortung der Internen Revision festlegt. Im Leitfaden zur Qualitätsbeurteilung, Nummer 28 stehen die Anforderungen an die Geschäftsordnung. Sie muss die folgenden Elemente enthalten:

- Zielsetzung der Internen Revision,
- Verpflichtung zur Einhaltung der GIAS,
- Mandat der Internen Revision und
- die organisatorische Positionierung sowie die Berichtslinien.

Im Vergleich zum Revisionshandbuch ist die „Geschäftsordnung“ zur Charakterisierung der Internen Revision im Unternehmen bestimmt (Außendarstellung), kann aber darüber hinaus auch ablauforganisatorische Regelungen mit Relevanz für die Fachbereiche beinhalten (z. B. zu Nachschauprüfungen oder zu Terminverlängerungen von vereinbarten Maßnahmen).

Weitere Anforderungen zur Geschäftsordnung können sich aus der BCBS-Veröffentlichung „The internal audit function in banks“ S. 7 und den EBA-Leitlinien zur Internen Governance (EBA/GL/2021/05 second revision) ergeben.

Das Revisionshandbuch dient der Zusammenfassung der für eine Interne Revisionsabteilung geltenden Festlegungen hinsichtlich der Aufgabenstellung, Struktur und ablauforganisatorischer Regelungen (Innendarstellung für Mitarbeitende der Internen Revision).

Der Leitfaden zur Qualitätsbeurteilung des DIIR stellt weitergehende Anforderungen an ein Revisionshandbuch unter Nummer 54:

- Die Revisionsleitung muss Methoden festlegen, um die Interne Revision systematisch und zielgerichtet anzuleiten, die Strategie der Internen Revision umzusetzen, den Revisionsplan zu entwickeln und die Standards einzuhalten.
- Die Revisionsleitung muss die Wirksamkeit der Methoden bewerten und sie bei Bedarf aktualisieren, um die Interne Revision zu verbessern und auf wesentliche Veränderungen, die die Funktion betreffen, zu reagieren.

Ein Revisionshandbuch sollte allen Mitarbeitenden der Internen Revision jederzeit und aktuell zur Verfügung stehen. Hierfür bietet sich die Einrichtung eines elektronischen Zugriffs an (z. B. Netzwerkdokument, Intranet). Die Zugriffsmöglichkeit durch andere interessierte Bereiche (z. B. Geschäftsleitung, sonstige Managementebenen) kann sinnvoll sein, sollte allerdings so restriktiv gewählt werden, dass vertrauliche Unterlagen (z. B. Checklisten für Sonderprüfungen, Prüfungsmethoden bei wirtschaftskriminellen Handlungen) weiterhin nur den Personen zur Verfügung stehen, die unmittelbar damit arbeiten sollen.

Ergänzend zur Geschäftsordnung der Internen Revision sind insbesondere Leitfäden bzw. Arbeitsprogramme für die konkrete Durchführung von Prüfungen von Bedeutung. Im Rahmen der konkreten Vorgaben in den Unternehmen sind auch Stellenbeschreibungen für Revisionsmitarbeitende zu erstellen.

1.6 Strategie der Internen Revision

1.6.1 Grundlagen zur Revisionsstrategie

Die Revisionsstrategie bildet den langfristigen Orientierungsrahmen für die Interne Revision und definiert deren Beitrag zur Zielerreichung der Gesamtorganisation. Sie ist Ausdruck eines strategischen Führungsverständnisses und dient der systematischen Weiterentwicklung der Revisionsfunktion im Einklang mit regulatorischen Anforderungen und den Erwartungen der Stakeholder (insbesondere Geschäftsleitung sowie ggf. Überwachungsorgan und weitere relevante Stakeholder in der Organisation).

Gemäß den aktuellen Anforderungen (GIAS Domain 4 – Prinzip 9) ist die Revisionsleitung angehalten strategisch zu planen, um die Interne Revision so zu positionieren, dass sie ihr Mandat erfüllen kann und langfristig erfolgreich ist.

Es sollte daher jede Interne Revision eine Revisionsstrategie entwickeln, dokumentieren und leben. Diese umfasst gemäß GIAS Standard 9.2 eine klar formulierte Vision – also

ein Zukunftsbild der Revisionsfunktion in z. B. drei bis fünf Jahren – sowie eine Mission, die den dauerhaften Auftrag und das Selbstverständnis der Revision beschreibt. Daraus leiten sich konkrete strategische Ziele und operative Maßnahmen ab.

Die diesbezüglichen Anforderungen waren in den vorherigen IPPF Standards nicht (explizit) formuliert und stellen somit eine Neuerung der GIAS dar. Die Formulierung von Auftrag und Zielen der Internen Revision sowie das Ergreifen von Maßnahmen zur Zielerreichung sind jedoch kein Novum. In Geschäftsordnungen bzw. Rahmenbedingungen der Internen Revision waren diesbezügliche Abschnitte in der Regel bereits enthalten.

Die Strategie ist kein statisches Dokument, sondern wird regelmäßig überprüft, ggf. angepasst und mit der Geschäftsleitung sowie ggf. dem Überwachungsorgan abgestimmt.

1.6.2 Inhalte einer Revisionsstrategie

Die Inhalte werden im GIAS Standard 9.2 konkretisiert. Je nach Größe und Komplexität der Internen Revisionsfunktion kann die Revisionsstrategie in Art und Umfang bzw. im Detaillierungsgrad variieren.

Die Vision der Internen Revision ist es, als vertrauenswürdiger, zukunftsorientierter Partner der Organisation zu agieren, der durch unabhängige Prüfungen, fundierte Analysen und konstruktive Empfehlungen zur nachhaltigen Wertschöpfung beiträgt.

Die in der Revisionsstrategie verankerten Ziele müssen mit den Zielen der Organisation abgestimmt sein und sicherstellen, dass Governance-, Risiko- und Kontrollsysteme wirksam unterstützt und bewertet werden. Die Ziele können lang- und kurzfristig gesetzt und ggf. mit einer Priorisierung, aufgeteilt nach Jahresscheiben, definiert werden.

In Instituten ist zu beachten, dass der Auftrag der Internen Revision in AT 4.4.3 Tz. 3 MaRisk als Mindestanforderung vorgegeben und bei der Formulierung der Revisionsstrategie entsprechend zu berücksichtigen ist. Die MaRisk betonen, dass die Interne Revision risikoorientiert, prozessunabhängig und systematisch arbeitet. Im Fokus steht die Angemessenheit und Wirksamkeit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse. Darüber hinaus gehende Zielsetzungen sind möglich.

Die Messung der Zielerreichung sollte über Key Performance Indicators (KPI; vgl. Kapitel 13 Leistungsmessung der Internen Revision) gesteuert und an die Stakeholder berichtet werden. Art, Umfang, Daittiefe und Turnus der Berichterstattung sowie abzuleitenden Maßnahmen bei erkannten Verbesserungspotentialen bzw. Abweichungen von den gesetzten Zielen sind durch die Leitung der Internen Revision, unter Einbezug der Stakeholder, zu definieren und dokumentieren.

Die Initiativen zur Zielerreichung der Revisionsstrategie sollten auch auf die Aspekte der Kompetenz(weiter)entwicklung, den Einsatz von (neuen) Technologien und die Verbesserung der Internen Revision insgesamt (Stichwort „Conformance“: Quality & Performance) einzahlen, z. B. durch Digitalisierung von Prüfprozessen, Stärkung analytischer Kompetenzen oder Förderung von Effizienz und Qualität.

Die Dokumentation der Revisionsstrategie kann in Form eines separaten Dokumentes, als Abschnitt in den Rahmenbedingungen der Internen Revision (Audit Charter) oder ggf. sogar als Teil(-Strategie) der Geschäfts- und Risikostrategie des Instituts erfolgen.

Die Revisionsstrategie in Instituten sollte durch die Geschäftsleitung genehmigt werden.

Eine Überprüfung der Revisionsstrategie insgesamt oder einzelner Ziele/ Initiativen/ KPI sollte regelmäßig, mind. jährlich oder anlassbezogen bei wesentlichen Änderungen erfolgen. Letztere könnten z. B. bei Anpassungen der betrieblichen, organisatorischen oder regulatorischen Bedingungen, bei einer Neufassung der berufsständischen Standards für die Interne Revision, bei geänderten Anforderungen/ Erwartungen der Stakeholder oder bei diesbezüglichen Ergebnissen/ Erkenntnissen des internen oder externen Quality Assessments vorliegen.

Durch die Revisionsstrategie besteht für die Interne Revision die Möglichkeit, ihre Ziele und Maßnahmen zur Umsetzung mit den Stakeholdern noch transparenter und fokussierter zu erörtern und zu berichten. So kann die Interne Revision ihren mehrwertstiftenden Beitrag für die Organisation noch besser aufzeigen.

2 Externe Rahmenbedingungen

2.1 Grundlagen

Der Rahmen für die Tätigkeit der Internen Revision wird maßgeblich auch durch externe Normen gesetzt. Diese beinhalten insbesondere gesellschaftsrechtliche, branchenspezifische als auch kapitalmarktorientierte Normen. Daneben bestehen berufsrechtliche Standards. Ergänzend ist die Erwartungshaltung diverser Stakeholder zu berücksichtigen (z. B. Kapitalmärkte oder Aufsicht bei Systemrelevanz).

Im Falle von Ermessensspielräumen oder Wahlrechten ist zu prüfen, ob diesbezügliche Entscheidungen in Abstimmung mit der Geschäftsleitung und dem Aufsichtsorgan, ggf. mit seinem Prüfungsausschuss, getroffen werden müssen. Soweit Prüfungsgegenstände des Abschlussprüfers betroffen sind (PrüfBV), ist auch dessen Einbindung zu empfehlen.

Grundsätzlich ist es sinnvoll, dass auch die Interne Revision eine Übersicht (wesentliche rechtliche Vorgaben) in Anlehnung an AT 4.4.2 Tz. 2 MaRisk führt, in der alle sie direkt betreffenden Regularien aufgeführt sind. Dabei können verschiedene Quellen als Grundlage verwendet werden, z. B.:

- Eigene aktive Recherche bei einschlägigen Regelungsgebern (z. B. EBA, Gesetzgeber, BaFin) oder weiterer im Internet vorhandene Datenbanken (z. B. KPMG Lex-Links)
- Informationen von einschlägigen Verbänden (Bankenverband, BVR, DK, VÖB, etc.), ggf. auch von berufsständischen Standardsetzern (z. B. IIA, DIIR und IDW)
- Auswertung der, im Rahmen der Aktivitäten rund um den AT 4.4.2 Tz. 2 MaRisk, gesammelten Unterlagen

Bei internationalen Aktivitäten können für die Revisionstätigkeit innerhalb eines Instituts bzw. innerhalb eines Konzerns unterschiedliche aufsichtsrechtliche Regelkreise gelten. In den Rahmenbedingungen der Internen Revision sollten die jeweils standortspezifisch geltenden Normen festgelegt werden. Die Interne Revision kann sich aber auch unternehmens- bzw. konzernweit auf die restriktivsten Normen selbstverpflichten.

Die nachfolgend genannten Regelungen stellen einen Ausschnitt der für eine Revision geltenden aufsichtlichen/gesetzlichen Regeln dar. Ziel ist eine Erwähnung wichtigsten Regelungskreise mit den einschlägigen Regelungen.

2.2 Gesellschaftsrecht

Gesellschaftsrechtlich stellen die § 91 Abs. 2 und Abs. 3 AktG, § 93 Abs. 1 S. 2 AktG sowie § 107 Abs. 3 und Abs. 4 AktG zentrale Normen dar.

Nach der Gesetzesbegründung zum Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) soll durch die Einfügung des § 91 Abs. 2 AktG auch die gesetzliche Verpflichtung zur Sicherstellung einer angemessenen Internen Revision verdeutlicht werden. Diese betrifft allerdings nur eine funktionale, nicht aber eine verpflichtende institutionelle Einrichtung.

Mit dem Finanzmarktintegritätsstärkungsgesetz (FISG) wurde explizit, die bereits aus dem KWG bekannte Verpflichtung zur Einrichtung eines Internen Kontroll- und Risikomanagementsystems für börsennotierte Aktiengesellschaften eingefügt (§ 91 Abs. 3 AktG). Für Kreditinstitute ergeben sich die Verpflichtungen aus § 91 Abs. 2 und Abs. 3 auch aus dem Aufsichtsrecht. Allerdings sind die beiden Regelkreise (Gesellschafts- vs. öffentliches Recht), z. B. wegen unterschiedlicher Anforderungen und ggf. Haftungsfolgen, getrennt zu beachten.

Die Tätigkeit der Internen Revision ist auch als Voraussetzung eines ordnungsgemäßen Informationsmanagements einzuordnen. Dies bekommt insbesondere Bedeutung im Rahmen der Nutzung der Business Judgement Rule (§ 93 Abs. 1 S. 2 AktG) durch den Vorstand. Diese besagt u. a., dass ein Vorstand dann nicht pflichtwidrig handelt, wenn er bei unternehmerischen Entscheidungen auf der Grundlage angemessener Information zum Wohle der Gesellschaft handelte und er dies auch vernünftigerweise annehmen durfte. Unzureichende Tätigkeiten der Internen Revision, z. B. aufgrund qualitativer und/oder quantitativer Unterkapazitäten, können zur Hinterfragung der „Angemessenheit der Informationsgrundlage“ führen.

§ 107 Abs. 3 S. 2 AktG regelt direkt die Überwachungsverpflichtung des Aufsichtsorgans. Falls kein Prüfungsausschuss gebildet ist, dann muss das Aufsichtsorgan insgesamt diese erfüllen. Die Überwachung betrifft den Rechnungslegungsprozess, die Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionsystems sowie der Abschlussprüfung, hier insbesondere der Auswahl und der Unabhängigkeit des Abschlussprüfers und der vom Abschlussprüfer zusätzlich erbrachten Leistungen.

Für Unternehmen von öffentlichem Interesse erfolgte durch das Finanzmarktintegritätsstärkungsgesetz folgende Erweiterung des Auskunftsrechts (§ 107 Abs. 4 AktG):

- Jedes Mitglied des Prüfungsausschusses kann über den Ausschussvorsitzenden unmittelbar bei den Leitungen derjenigen Zentralbereiche der Gesellschaft, die in der Gesellschaft für die Aufgaben zuständig sind, die den Prüfungsausschuss nach § 107 Abs. 3 S. 2 AktG betreffen, Auskünfte einholen. Der Ausschussvorsitzende

hat die eingeholte Auskunft allen Mitgliedern des Prüfungsausschusses mitzuteilen. Werden Auskünfte nach S. 4 eingeholt, ist der Vorstand hierüber unverzüglich zu unterrichten.

Die genannten Rechtsnormen gelten entweder direkt oder entfalten zumindest Ausstrahlungswirkungen auf andere Rechtsformen, z. B. die GmbH. Durch § 1 StaRUG (Krisenfrüherkennung und Krisenmanagement) wurden mittlerweile die Anforderungen aus § 91 Abs. 2 AktG und darüber hinaus gehende Anforderungen auf alle haftungsbeschränkte Unternehmensträger übertragen. Der IDW hat zur Konkretisierung der Anforderungen aus § 1 StaRUG den IDW-Standard S 16 veröffentlicht.

Das IDW hat im Zusammenhang mit der Prüfung des Internen Revisionssystems durch Wirtschaftsprüfer einen eigenen Prüfungsstandard verfasst (IDW PS 983). Dieser Prüfungsstandard wurde gemeinsam mit dem DIIR erarbeitet und seitens des DIIR parallel als Revisionsstandard Nr. 3 veröffentlicht. Der Standard beurteilt die Interne Revision als eine wesentliche Governance-Funktion und als dritte Linie im Three Lines-Modell (zur Erläuterung des Modells siehe Abschnitt 17.2).

Auf Basis der 2024 veröffentlichten GIAS wurde der Prüfungsstandard vom IDW gemeinsam mit dem DIIR überarbeitet und im Dezember 2025 in der neuen Fassung (IDW PS 983 n.F. (12.2025)) zeitgleich mit dem überarbeiteten Revisionsstandard Nr. 3 des DIIR veröffentlicht.

Das DIIR hat den DIIR-Leitfaden zur Qualitätsbeurteilung der Internen Revision, der als Ergänzung des DIIR Revisionsstandard Nr. 3 gilt, parallel aktualisiert und bereits mit Stand: 06.12.2024 veröffentlicht. Die Veröffentlichung des Leitfadens erfolgt formal als anwendbarer Entwurf, weil die Überarbeitung des IDW PS 983 durch das IDW zu diesem Zeitpunkt noch nicht abgeschlossen war.

2.3 Deutscher Corporate Governance Kodex (DCGK)

Der Deutsche Corporate Governance Kodex (DCGK) wirkt direkt über § 161 AktG (Erklärung zum Corporate Governance Kodex) auf börsennotierte Gesellschaften (AG und KGaA) und indirekt durch die Formulierung von Empfehlungen und Anregungen zur „Good Governance“ auf alle Unternehmen. Der IDW hat hierzu den IDW-Prüfungsstandard 2 „Auswirkungen des Deutschen Corporate Governance Kodex auf die Abschlussprüfung“ (IDW PS 345 n.F.) veröffentlicht. Die Interne Revision sollte die Auswirkungen beider Veröffentlichungen auf ihre Prüfungsobjekte, insbesondere bei Neufassungen des DCGK, beurteilen.

Für die Interne Revision von besonderer Bedeutung ist der Grundsatz 4 des DCGK 2022, der u.a. festlegt: „Die Angemessenheit und Wirksamkeit des internen Kontrollsystems und des Risikomanagementsystems setzt deren interne Überwachung voraus.“

2.4 Branchenspezifische Normen

2.4.1 Organisatorische Vorgaben zur Revisionsfunktion

Für Institute bilden insbesondere der § 25a Abs. 1 S. 3 KWG sowie dessen norminterpretierende Verwaltungsvorschrift, die MaRisk (AT 4.4.3 sowie BT 2), die zentralen Normen für die Ausgestaltung der Internen Revisionsfunktion.

Daneben finden sich Berichtspflichten der Internen Revision an Geschäftsleitung und Aufsichtsorgan in § 25c Abs. 4a Nr. 3 lit. g) KWG und der Konzernrevision in § 25c Abs. 4b S. 2 Nr. 3 lit. g) KWG sowie Regelungen zum Auskunftsrecht des Risikoausschussvorsitzenden in § 25d Abs. 8 S. 7 KWG zum Auskunftsrecht des Prüfungsausschussvorsitzenden in § 25d Abs. 9 S. 3 KWG und zum Auskunftsrecht des Vorsitzenden des Vergütungskontrollausschusses in § 25d Abs. 12 S. 6 KWG.

Institute, die besonders groß sind oder deren Geschäftsaktivitäten durch besondere Komplexität, Internationalität oder eine besondere Risikoexposition gekennzeichnet sind, haben die Inhalte einschlägiger Veröffentlichungen zum Risikomanagement des Baseler Ausschusses für Bankenaufsicht und des Financial Stability Board in eigenverantwortlicher Weise in ihre Überlegungen zur angemessenen Ausgestaltung des Risikomanagements einzubeziehen (AT 1 Tz. 3 MaRisk). Bezüglich der Internen Revision betrifft dies z. B. die Veröffentlichung „The internal audit function in banks (June 2012)“ des Basel Committee on Banking Supervision sowie Leitlinie der EBA zur Internen Governance (EBA/GL/2021/05).

2.4.2 Konkrete Prüfungs- oder Mitwirkungspflichten der Internen Revision

Insbesondere prüfobjektbezogene Vorgaben ergeben sich teilweise auch direkt aus dem Aufsichtsrecht (z. B. aus der Capital Requirements Regulation [CRR] oder Verordnungen des Gesetzgebers). Je nach Einordnung des Kreditinstituts können die Veröffentlichungen der European Banking Authority (EBA), insbesondere deren Leitlinien und Standards Relevanz für die Prüfungsplanung der Internen Revision entfalten. Exemplarisch sind dies Artikel 191 CRR (Interne Revision) oder § 3 Abs. 3 InstitutsVergV.

Weitere Tätigkeitsfelder können sich z. B. aufgrund von Verbandsempfehlungen oder durch Vorgaben der jeweiligen Sicherungseinrichtungen ergeben.

2.5 Überwachung durch die Security and Exchange Commission (SEC) und den Sarbanes-Oxley Act (SOX)

Für alle SEC-registrierten Unternehmen sowie für Unternehmen in deren Konzernkreis gelten die Regelungen des Sarbanes-Oxley-Acts (SOX). Dieser umfasst weitreichende Regelungen hinsichtlich Corporate Governance, Compliance und vor allem zum internen Kontrollsystem. Trotz der Einschränkung auf an US-Börsen gelistete Unternehmen können sich ggf. Ausstrahlungen auch auf andere Unternehmen mit internationaler Geschäftstätigkeit und deren Interne Revision im Sinne einer Best Practice ergeben. Die Regelungen des SOX werden insbesondere durch Ausführungsbestimmungen in Form von Standards des Public Company Accounting Oversight Board (PCAOB) ergänzt.

2.6 Handelsrechtliche Offenlegung im Lagebericht und Konzernlagebericht

Kapitalmarktorientierte Kapitalgesellschaften müssen i. S. d. § 264d HGB im Lagebericht die wesentlichen Merkmale des internen Kontroll- und des Risikomanagementsystems im Hinblick auf den Rechnungslegungsprozess beschreiben (§ 289 Abs. 4 HGB). Entsprechend ist im Konzernlagebericht einzugehen auf die wesentlichen Merkmale des internen Kontroll- und des Risikomanagementsystems im Hinblick auf den Konzernrechnungslegungsprozess, sofern eines der in den Konzernabschluss einbezogenen Tochterunternehmen oder das Mutterunternehmen kapitalmarktorientiert i. S. d. § 264d HGB ist (§ 315 Abs. 4 HGB). Textpassagen zur Internen Revision sollten mit derselben abgestimmt werden.

Durch den Deutschen Rechnungslegungsstandard Nr. 20 (DRS 20) „Konzernlagebericht“ erfolgt eine Konkretisierung:

- Risikobericht (unabhängig von der Kapitalmarktorientierung)
- Risikomanagementsystem (bei Kapitalmarktorientierung)

Sofern das Risikomanagementsystem auf einem allgemein anerkannten Rahmenkonzept basiert, muss dies angegeben werden (DRS 20.K139). Wesentliche Veränderungen des Risikomanagementsystems gegenüber dem Vorjahr sind darzustellen und zu erläutern (DRS 20.K139). Ebenso ist anzugeben, wenn eine Interne Revision das Risikomanagementsystem überprüft (DRS 20.K144).

- Internes Kontrollsystem und Risikomanagementsystem bezogen auf den Konzernrechnungslegungsprozess (bei Kapitalmarktorientierung)

Sofern das Mutterunternehmen oder eines der in den Konzernabschluss einbezogenen Tochterunternehmen kapitalmarktorientiert ist, sind die wesentlichen Merkmale des internen Kontrollsystems und des Risikomanagementsystems im Hinblick auf den Konzernrechnungslegungsprozess darzustellen und zu erläutern (DRS 20.K168). Sofern das IKS oder RMS im Hinblick auf den Konzernrechnungslegungsprozess auf einem allgemein anerkannten Rahmenkonzept beruht, ist dies anzugeben (DRS 20.K172). Die Ausführungen in Bezug auf das interne Kontrollsystem müssen u. a. auch das interne Revisionsystem umfassen, soweit es Maßnahmen in Bezug auf das Kontrollziel (Sicherstellung der Normenkonformität des Konzernabschlusses und des Konzernlageberichts) betrifft (DRS 20.K174). Hierbei können z. B. die Aufgaben im Zusammenhang mit der Rechnungslegung bzw. der Konzernrechnungslegung, die vom Bereich „Interne Revision“ wahrgenommen werden (DRS 20.K175 bzw. DRS 20.K176), dargestellt werden.

Die Berichterstattung im Lagebericht wird auch im A.5 zum Grundsatz 4 des DCGK 2022 behandelt.

2.7 COSO und COBIT

Zur Umsetzung sowie Beurteilung eines Risikomanagement- bzw. eines internen Kontrollsystems muss die Orientierung an einem systemischen Ansatz erfolgen. Für das interne Kontrollsystem kann dies das COSO-Internal Framework sein.

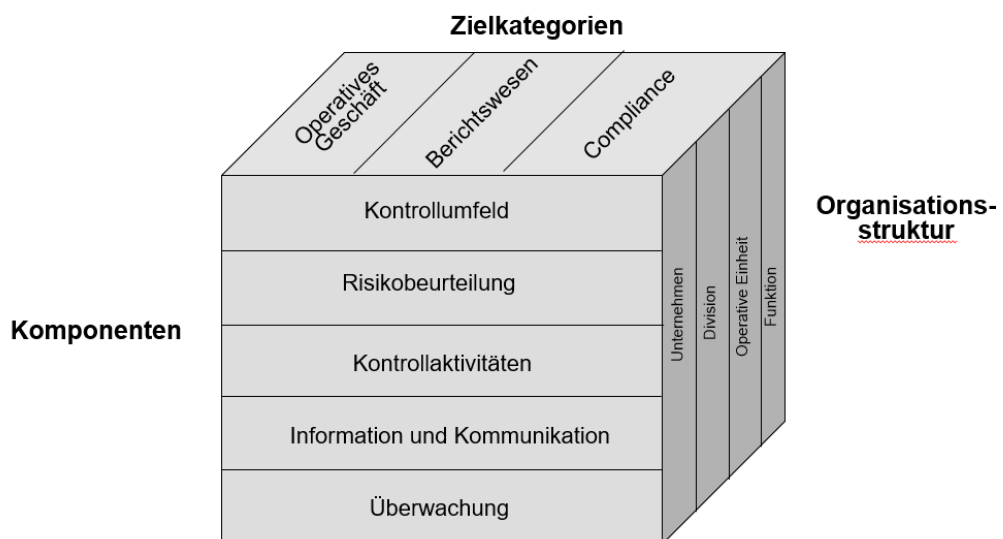


Abb. 1: COSO-Internal Control 2013

Das Berichtswesen umfasst dabei das interne Reporting und die Nachhaltigkeitsberichterstattung (z. B. CRSD i. V. m. ESRS); die Fokussierung auf die externe Finanzberichterstattung wurde aufgegeben. Zudem wurden 17 Prinzipien jeweils zugeordnet zu den fünf Komponenten zur Erleichterung der Umsetzung und der Überprüfung eingeführt. Ergänzend wurden als weitere Konkretisierung 77 Fokuspunkte eingeführt.

Bei Nichteinhaltung eines Prinzips verneint COSO grundsätzlich die Angemessenheit und die Wirksamkeit der dazugehörigen Komponente. Bezüglich einzelner Fokuspunkte kann es in Einzelfällen plausibel sein, einzelne nicht zu beachten. Die Entscheidungsgründe für die Nichteinhaltung von Prinzipien und Fokuspunkten sind zu dokumentieren.

Das COSO-Internal-Control-Modell wurde im Jahr 2004 zum COSO-Enterprise-Riskmanagement-Modell (COSO-ERM) erweitert. Dies betrifft insbesondere die Erweiterung der Ziele um die strategischen Aspekte sowie die Differenzierung der Komponente „Risikobeurteilung“ in die Komponenten „Zielfestsetzung“, „Ereignisidentifikation“, „Risikobeurteilung“ und „Risikosteuerung“.



Abb. 2: COSO-Enterprise Risk Management (2004)

Beide Modelle werden ausdrücklich vom IIA, DIIR, IDW und dem Sarbanes-Oxley Act empfohlen und bilden oftmals das theoretische Fundament für deren Veröffentlichungen. Das DIIR hat hierzu im Jahr 2006 eine Einführung unter dem Titel „Unternehmensüberwachung und Interne Revision – aktuelle Entwicklungen und Auswirkungen durch COSO ERM“ veröffentlicht. In den Rahmenbedingungen der Internen Revision ist die entsprechende Festlegung auf ein Modell des Risikomanagements bzw. des internen Kontrollsystems zu prüfen.

Im Juni 2017 wurde eine weiterentwickelte Fassung von COSO-ERM „Enterprise Risk Management – Integrating with Strategy and Performance“ veröffentlicht. Damit soll die Berücksichtigung von Risiken aus dem Strategieprozess sowie aus der Ergebnissteuerung stärker hervorgehoben werden. Die Anwendung von COSO-ERM 2004 ist jedoch weiterhin möglich.



Abb. 3: COSO: Implications from the strategy



Abb. 4: COSO: Enterprise Risk Management (Framework 2017)

Am 27.05.2025 hat COSO in Zusammenarbeit mit National Association of Corporate Directors (NACD) den Entwurf eines Corporate Governance Frameworks veröffentlicht. Hierin wurden 24 Prinzipien sowie dazugehörige Fokuspunkte veröffentlicht. Weiterhin wird u.a. der Zusammenhang Corporate Governance, Enterprise-wide Risk Management vs. Internal Control dargestellt.

Ein international anerkanntes Regelwerk zur IT-Governance stellt COBIT dar (aktuell Version 5.0/2019).

Für IT-Prüfungen liefern sowohl weitere Veröffentlichungen der ISACA als auch die IT-bezogenen Teile des Regelwerks der beruflichen Praxis (IPPF) des IIA Anregungen. Die bisherigen „Global Technology Audit-Guides (GTAG)“ und die „Guides to the Assessment

of IT Risk (GAIT)“ sind nun Inhalte im Bereich „Guidance“ des überarbeiteten IPPF. Weiterhin wurde der Topical Requirements „Cybersecurity“ im Februar 2025 veröffentlicht.

2.8 Berufsständische Regelungen (IPPF und DIIR-Veröffentlichungen)

Für Interne Revisoren stellen die Veröffentlichungen des DIIR, ggf. des ECIIA und das International Professional Practices Framework (IPPF) des IIA die zentralen berufsrechtlichen Normen dar. Diese wurden im Jahr 2024 umfassend überarbeitet veröffentlicht und gelten seit Anfang des Jahres 2025.



Abb. 5: Gegenüberstellung Struktur bisheriges IPPF und Struktur neues IPPF

Das neue IPPF hat drei zentrale Bereiche: die Global Internal Audit Standards (GIAS), die Topical Requirements sowie die Global Guidance, wobei die GIAS immer und die Topical Requirement, bei entsprechender Prüfungstätigkeit, verpflichtend sind.

Die **GIAS** regeln die weltweite berufliche Praxis der Internen Revision und dienen als Grundlage für die Bewertung und Verbesserung der Qualität der Internen Revision. Im Mittelpunkt der Standards stehen 15 Prinzipien, die eine wirksame Interne Revision ermöglichen. Jedes Prinzip wird durch Standards unterstützt, die Anforderungen, Überlegungen zur Umsetzung und Beispiele für den Nachweis der Einhaltung des Standards enthalten. Sie beinhalten die bisherigen fünf Pflichtelemente: Mission der Internen Revision, Definition der Interne Revision, Grundprinzipien, Ethikkodex und Standards, sowie das bisher nur empfohlene Element „Implementierungsleitlinien“ (vertiefend Bantleon/Eulerich, WPg 2023/1227 sowie Wissenschaftlicher Beirat des DIIR, WPg 2024/1163).

Von besondere Bedeutung für die Einbindung der Internen Revision in die Corporate Governance ist die GIAS Domain I „Zielsetzung der Internen Revision“ und die GIAS Domain III „Governance der Internen Revision“. In der GIAS Domain I wird u. a. die Erwartungshaltung an die Interne Revision und deren Wertbeitrag konkretisiert.

GIAS Domain III nennt konkrete Anforderungen an das Leitungs- und Überwachungsorgan und deren Verantwortlichkeiten. Letztlich werden angemessene Governance-Regelungen (= wesentlichen Bedingungen in den Standards der GIAS Domain III) genannt, welche für die Wirksamkeit der Internen Revision notwendig sind. Der Austausch mit dem Leitungs- und Überwachungsorgan über die Inhalte des Domain III ist daher eine zentrale Aufgabe der Leitung der Internen Revision. Besondere Bedeutung haben hierbei das Prinzip 6: „Autorisierung durch das Leitungs-Überwachungsorgan“ und Prinzip 8: „Aufsicht durch das leitungs- und Überwachungsorgan“. Die zentralen Aspekte des Prinzips 6 sind durch die Standards „Standard 6.1: Mandat der Internen Revision“, „Standard 6.2: Geschäftsordnung der Internen Revision“ und „Standard 6.3: Unterstützung durch Geschäftsleitung und Überwachungsorgan“ konkretisiert. Ein zentraler Aspekt des Prinzips 8 ist „Standard 8.1: Interaktion mit dem Leitungs- und Überwachungsorgan“.

Die **Topical Requirements** sollen die Konsistenz und Qualität von Leistungen der Internen Revision in Bezug auf bestimmte Prüfungsthemen verbessern und Interne Revisorinnen und Revisoren bei der Durchführung von Aufträgen in diesen Risikobereichen unterstützen. Interne Revisorinnen und Revisoren müssen die relevanten Anforderungen erfüllen, wenn der Umfang eines Auftrags eines der identifizierten Themen umfasst. Das erste Topical Requirement Dokument wurde am 05.02.2025 veröffentlicht und bezieht sich auf Cybersicherheit. Zum 15.09.2026 sind das Topical Requirement Dokument zum Thema Drittparteien-Risiko und zum 15.12.2026 das Topical Requirement Dokument zum Thema Verhalten in Organisationen anzuwenden. Für die Interne Revision in Instituten sollten die Anwendung weitgehend keine Neuerung darstellen, da bereits branchenspezifische Vorgaben wie DORA, EBA Leitlinien und die MaRisk viele Aspekte der Topical Requirements abdecken. Gleichwohl ist es sinnvoll, die einzelnen Anforderungen der Topical Requirements den Inhalten der relevanten Prüffelder zuzuordnen, um die vollständige Einhaltung sicherzustellen und bei Bedarf (externes Quality Assessment) nachweisen zu können.

Global Guidance unterstützt die Standards durch die Bereitstellung nicht verbindlicher Informationen, Ratschläge und Best Practices für die Leistungserbringung der Internen Revision. Global Guidance wird vom IIA formell überprüft und genehmigt.

Ergänzend sind die Standards des DIIR relevant.

Es kommen ggf. noch verbandsindividuelle (z. B. DSGVO, BVR) revisionsbezogene Normen dazu.

In den Rahmenbedingungen der Internen Revision (Charter) ist festzulegen, welcher Verpflichtungscharakter den jeweiligen Normen beigemessen wird.

3 Standardrevisionsprozess

Der Standardrevisionsprozess soll als Richtlinie und Referenzmedium dienen, um eine effektive und effiziente Revisionsarbeit leisten zu können. Als solches ist er Teil der schriftlich fixierten Ordnung (SFO) der Internen Revision.

Die Phasen des Standardrevisionsprozesses gelten grundsätzlich für alle Prüfungsarten und werden auf den folgenden Seiten im Detail beschrieben.

3.1 Prüfungsplanung

Die aufsichtsrechtlichen Anforderungen an die Prüfungsplanung sind in den MaRisk (BT 2.3, Tz. 1) formuliert. Danach muss die Prüfungsplanung umfassend, jährlich fortschreibend und risikoorientiert erfolgen. Grundsätzlich sind alle internen und ausgelagerten Aktivitäten und Prozesse innerhalb von drei Jahren zu prüfen, bei besonderen Risiken jährlich. Bei unter Risikogesichtspunkten nicht wesentlichen Aktivitäten und Prozessen kann vom dreijährigen Turnus abgewichen und ein Turnus von bis zu fünf Jahren geplant² werden. Ein Abweichen vom dreijährigen Turnus bedeutet nicht, dass weitgehend auf Prüfungshandlungen in diesen Bereichen verzichtet werden kann. Vielmehr sind auch diese unter Risikogesichtspunkten nicht wesentlichen Aktivitäten und Prozesse in die Prüfungsplanung zu integrieren und in angemessenen Abständen zu prüfen.

Der standardisierte, risikoorientierte Planungsprozess gliedert sich wie folgt:

- Rahmenplanung (strategisch, risikoorientiert)
 - Aktualisierung des Prüfungsuniversums (Prüfobjekte)
 - Risikobeurteilung der Prüfobjekte
- Mehrjahresplanung (langfristig, nach Risiko und Umfang)
- Jahresplanung (operativ, genehmigungspflichtig)
- Operative Planung (zur unterjährigen dispositiven Steuerung und wenn erforderlich, Änderungen der Jahresplanung)
- ggf. unterstützt durch ein Verfahren zur Ermittlung und Beurteilung wesentlicher, neuer und aufkommender Risiken (vgl. GIAS Standards 9.4).

² Vgl. BaFin, Protokoll zur virtuellen Sitzung des Fachgremiums MaRisk am 01.03.2023.

Die Prüfungsplanung, -methoden und -qualität sind regelmäßig vor Beginn der Aktivitäten und anlassbezogen auf Angemessenheit zu überprüfen und weiterzuentwickeln.

3.1.1 Rahmenplanung

3.1.1.1 Prüfungsuniversum

Das Prüfungsuniversum bildet die Gesamtheit aller Prüfobjekte ab, die der Unternehmensgruppe zugehören oder für die das Institut verantwortlich ist.

Die Prüfobjekte müssen alle Aktivitäten, Prozesse und Wertschöpfungsketten, die funktionalen und operativen Bereiche sowie Produkte und Systeme umfassen. Ein Prüfungsuniversum ist am nützlichsten, wenn es auf dem Verständnis der Ziele und strategischen Initiativen der Organisation beruht und mit der Struktur oder dem Risikorahmenwerk der Organisation abgestimmt ist (vgl. Überlegungen zur Umsetzung des GIAS Standard 9.4)

Alle wesentlichen Auslagerungen (MaRisk AT 9 Tz. 2), alle kritischen oder wichtigen IKT-Drittdienstleister (DORA) sowie Einlagerungen von Geschäftsaktivitäten, bei denen eine vertragliche Prüfungspflicht besteht, sind einzubeziehen. Nicht wesentliche Auslagerungen, nicht kritische oder wichtige IKT-Drittdienstleister (DORA) sowie sonstiger Fremdbezug kann Prüfungsobjekten zugeordnet und bei der Vorbereitung der konkreten Prüfung risikoadäquat zu berücksichtigen werden.

Es sind alle gesetzlichen und aufsichtsrechtlichen Anforderungen (z. B. die Prüfung von Ratingsystemen gem. der CRR, Prüfung der Geldwäscheprävention, lokale regulatorische Anforderungen ausländischer Niederlassungen) sowie ggf. besondere Anforderungen der Geschäftsleitung bei der Prüfungsplanung zu berücksichtigen.

Damit die Prüfungsabdeckung transparent ermittelt werden kann, verkörpert idealerweise ein Prüfobjekt eine einzelne Prüfung. Um Risiken und Schnittstellen in einer Prozesskette zu prüfen und zu bewerten, können mehrere Prüfobjekte zu einer Prüfung zusammengefasst werden. Die Granularität der Prüfobjekte sollte sich am inhärenten Risiko orientieren, dessen Gewicht aus Sicht der Geschäftsleitung und des Aufsichtsorgans eine gewisse Bedeutung haben sollte.

Die Überprüfung der Prüfobjekte hinsichtlich Vollständigkeit, Relevanz und Konsistenz muss jährlich so rechtzeitig erfolgen, dass für die Jahresplanung aktuelle Daten vorliegen. Eine strukturelle Veränderung der Prüfungsobjekte im Prüfungsuniversum ist nachvollziehbar zu dokumentieren und vom Kompetenzträger (zu definieren) zu genehmigen. Bei Bedarf - zum Beispiel im Falle von Änderungen in der Aufbau- und Ablauforganisa-

tion - sollte eine Anpassung des Prüfungsuniversums und eventuell auch eine Anpassung der Prüfungsplanung unterjährig erfolgen. Die Überprüfung ist zu dokumentieren und, im Fall von wesentlichen Änderungen in der Prüfungsplanung, der Geschäftsleitung zur Genehmigung vorzulegen. Hierzu sind die Wesentlichkeitskriterien schriftlich zu definieren (siehe 3.1.4 Operative Planung)

Eine nachvollziehbare Dokumentation und Genehmigung (Kompetenzträger sind zu definieren) ist notwendig für:

- Strukturelle Veränderungen der Prüfobjekte (Kapitel 3.1.1.1)
- Änderungen der Methodik der Risikobewertung (Kapitel 3.1.1.2)
- Anpassung der Gewichtungsfaktoren im Bewertungsverfahren (Kapitel 3.1.1.2)
- Festlegung des ersten Prüfungsjahres für neu angelegte Prüfobjekte inkl. Begründung (Kapitel 3.1.2)

3.1.1.2 Risikobeurteilung

Die systematische Analyse des Risikopotenzials aller Prüfobjekte hat nach einer einheitlichen Methodik zu erfolgen. Die Methodik ist regelmäßig und anlassbezogen auf Angemessenheit zu überprüfen und weiterzuentwickeln. Änderungen und Anpassungen in der Methodik der Risikobewertung wie auch der Anpassungen der Gewichtungsfaktoren im Bewertungsverfahren sind nachvollziehbar zu dokumentieren und durch den definierten Kompetenzträger zu genehmigen.

Die Risikoeinschätzungen sind regelmäßig und anlassbezogen kritisch zu hinterfragen bzw. zu überprüfen

Die inhärenten und residualen Risiken von Prüfobjekten werden anhand festgelegter Risikokategorien und Einflussfaktoren nach einem einheitlichen Ansatz bestimmt. Best Practice für die Ermittlung der inhärenten Risiken ist in diesem Fall die Nutzung eines Verfahrens, das die Risikotaxonomie und die Schwellenwerte des Risikomanagements des Instituts zu Grunde legt. Dies ermöglicht u. a. der Geschäftsleitung einen Vergleich der Risikoeinschätzungen unterschiedlicher Kontrollfunktionen im Institut. Zur Bestimmung der residualen Risiken ist das Kontrollumfeld zu bewerten und zu beurteilen inwieweit dieses das inhärente Risiko mitigiert. Bei der Beurteilung des Kontrollumfeldes sollten unter anderem Ergebnisse aus Vorjahresprüfungen und der Status der Abarbeitung der Feststellungen, Ergebnisse aus Prüfungen durch die externen Prüfer und die Aufsicht sowie Schadensvorfälle und Ergebnisse aus der Bewertung des Kontrollumfeldes durch Kontrollfunktionen in der 2nd Line einbezogen werden.

Die Risikobewertungsverfahren der Internen Revision haben eine Analyse des Risikopotenzials der Aktivitäten und Prozesse unter Berücksichtigung absehbarer Veränderungen (z. B. absehbare Marktentwicklungen und Veränderungen im regulatorischen Umfeld, neue Produkte/ Märkte/ Vertriebswege, geplante Ausweitung von Geschäftsaktivitäten, laufende und geplante Projekte) zu beinhalten.

Grundlage der Risikobewertung sind die institutsindividuell festgelegten wesentlichen Risikoarten gemäß MaRisk (u. a. Zinsänderungsrisiko, Markt- bzw. Liquiditätsrisiko, Adressenausfallrisiko, operationelles Risiko). Bei der Bewertung des operationellen Risikos ist auch die Manipulationsanfälligkeit der Prozesse angemessen zu berücksichtigen. Daneben können weitere Kriterien, wie z. B. die strategische oder betriebswirtschaftliche Bedeutung der Prüfobjekte und Risiken aus der Auslagerung von Aktivitäten und Prozessen bzw. Fremdbezug von IKT-Dienstleistungen herangezogen werden.

Darüber hinaus soll sie Risiken gebührend berücksichtigen, die möglicherweise mit mehr als einer Geschäftseinheit oder mehr als einem Prozess verbunden sind und eine komplexere Bewertung erfordern – beispielsweise Risiken im Zusammenhang mit Ethik, Fraud, IT, Beziehungen zu Dienstleistern und Nichteinhaltung regulatorischer Anforderungen (vgl. Überlegungen zur Umsetzung des GIAS Standard 9.4).

Bei der Bewertung sind ebenfalls z. B. die bereits gesammelten Erfahrungen/Kenntnisse durch Einbindung in „Neue Produkte Prozesse“ (NPP), wesentliche Projekte oder wesentliche Veränderungen der Aufbau- und Ablauforganisation zu berücksichtigen. Weitere Informationsquellen können sein:

- Laufende Gespräche mit den betroffenen Einheiten
- „Reguläre“ Prüfungstätigkeit/Follow-up Prozess
- Informationen aus Komitees und Meetings
- Ex ante-Aktivitäten
- Information/Konsultation aufsichtsrechtlicher Regelungen bzw. deren Überarbeitung (z. B. über Verbände).

Die Gesamtbewertung eines Prüfungsfeldes kann sich aus der Bewertung einzelner, für das Prüfungsfeld relevanter Risikotreiber ergeben. Zur Bewertung der Risikotreiber empfiehlt es sich, individuelle Bewertungskriterien (quantitativ und/oder qualitativ) zu definieren, die zu einer quantitativen (scorebasierten) oder qualitativen Bewertung führen. Wenn mehrere Risikofaktoren die Gesamtbewertung eines Prüfobjekts beeinflussen (z. B. Bewertung von Adressrisiko, Marktpreisrisiko usw.), ist die Verwendung eines Maximalprinzips im Gegensatz zu einem Durchschnittsprinzip eine gängige Praxis. Das bedeutet, dass der Risikofaktor mit der höchsten Bewertung die Gesamtbewertung maßgeblich bestimmt. Dadurch werden die Anforderungen der MaRisk zur Abdeckung von "Besonderen Risiken" erfüllt und hohe Risiken in der Gesamtbewertung nicht verwässert.

Alle in der Risikobeurteilung erhaltenen und verwendeten Informationen und die Gesamtbewertung eines Prüfungsfeldes sind angemessen zu dokumentieren. Die jeweils ermittelte „generische“ Risikokennziffer bestimmt die Prüfungsdringlichkeit für das jeweilige Prüfobjekt, aus der sich die Prüfungsfrequenz bzw. der Prüfungsturnus ableitet und die, bei Bedarf, als Grundlage für eine risikoorientierte Priorisierung von Prüfungen herangezogen werden kann.

Prüfungsobjekte die „besondere Risiken“ beinhalten, bedingen eine jährliche Prüfungsfrequenz. Sie sind dadurch gekennzeichnet, dass bei ihrem Eintreten die Gefahr einer deutlichen Verschlechterung der wirtschaftlichen Lage des Unternehmens besteht oder eine mögliche wirtschaftliche oder rechtliche Bestandsgefährdung vorliegt. Sie sind daher geeignet, Beurteilungen oder Entscheidungen von Stakeholdern zu verändern oder zu beeinflussen. Defizite im Risikomanagement, welche insbesondere durch unangemessene Risikostrategien, Regelungen zur Aufbau-/Ablauforganisation und Risikosteuerungs- und -controllingprozesse verursacht werden können, erhöhen die Eintrittswahrscheinlichkeit und das potenzielle Schadensausmaß von besonderen Risiken.

3.1.2 Mehrjahresplanung

Zur transparenten Darstellung der prüferischen Abdeckung der Aktivitäten und Prozesse des Unternehmens sowie zur Bewertung der Ressourcenausstattung (Glättung des Ressourcenbedarfs über mehrere Jahre) erfolgt auf Basis des jährlich ermittelten Prüfungsturnus eine Mehrjahresplanung, die sich mindestens über einen Zeitraum erstreckt, der dem längsten durch die Interne Revision zugelassenen und verwendeten Prüfungsturnus entspricht (damit i.d.R. drei bis fünf Jahre)³. Hierzu werden für alle Prüfungsobjekte des Prüfungsuniversums unter Berücksichtigung des Jahrs der letzten Prüfung, der objektbezogenen Faktoren (Datum der letzten Prüfung und entsprechendes Prüfungsergebnis) sowie des ermittelten oder aufsichtsrechtlich vorgegebenen Prüfungsturnus die Jahre der Fälligkeit einer Prüfung abgetragen. Abweichend von der Jahresplanung ist die Mehrjahresplanung nicht durch die Geschäftsleitung zu genehmigen.

Eine Mehrjahresplanung wird oftmals im Rahmen einer externen Prüfung oder durch die Aufsicht als Nachweis für eine adäquate Abdeckung aller Prüfungsfelder in einem bestimmten Rhythmus sowie für die adäquate Ausstattung der Internen Revision angefordert. Daher ist es ratsam eine Mehrjahresplanung zu erstellen und diese, zusammen mit der Jahresplanung, der Geschäftsleitung zur Kenntnis zu geben. Etwaige Ressourcenbeschränkungen der Internen Revision, die aus der Mehrjahresplanung ableitbar sind, sind deutlich gegenüber der Geschäftsleitung zu kommunizieren und ggf. durch externe Personalbeistellung zu kompensieren.

³ Vgl. BaFin, Protokoll zur virtuellen Sitzung des Fachgremiums MaRisk am 01.03.2023.

Grundsätzlich werden alle Prüfobjekte mindestens einmal innerhalb des definierten Prüfungsturnus (grundsätzlich ein bis drei Jahre, darüber hinaus bei unter Risikogesichtspunkten nicht wesentlichen Aktivitäten und Prozessen in Einzelfällen bis maximal fünf Jahre) für die Prüfung vorgesehen. Ein vollständiger Verzicht auf Prüfung eines Prüfobjektes ist nicht zulässig. Wie viele Prüfobjekte in einem Vier- oder Fünfjahreszyklus geprüft werden dürfen, so dass noch „grundsätzlich“ ein Dreijahreszyklus vorliegt, ist in dem MaRisk nicht konkretisiert. Die Bewertung der fehlenden Wesentlichkeit von Aktivitäten und Prozessen ist, wie für alle Prüfobjekte, über das Risikobewertungsverfahren oder die individuelle Dokumentation der Risikoeinschätzung nachvollziehbar zu begründen.

Prüfobjekte mit aufsichtsrechtlich vorgeschriebenem Intervall werden – unabhängig vom Ergebnis der Risikobeurteilung – im vorgeschriebenen Turnus zur Prüfung vorgesehen, wie z. B.:

- Nach der Capital Requirements Regulation (CRR) Artikel 191 muss bei Instituten, die den IRB-Ansatz nutzen, die Interne Revision oder eine andere vergleichbare unabhängige Revisionsstelle mindestens einmal jährlich die Ratingsysteme des Instituts prüfen. Dabei kann auf Basis eines jährlichen General Risk Assessment Konzepts festgelegt werden, mit welcher Intensität welche Teile der Modelle im jeweiligen Jahr geprüft werden. Unabhängig vom Ergebnis des Risk Assessments, sollte alle drei Jahre eine Prüfung stattfinden. Details sind im ECB Guide to Internal Models §§ 87 ff. zu finden, den auch die Deutsche Aufsicht in die Prüfungspraxis übernommen hat.
- Die CRR sieht eine jährliche Prüfung des allgemeinen Risikomanagements vor, sofern das Kreditinstitut interne Modelle zur Ermittlung des Gegenparteausfallrisikos (als Teil des Kreditrisikos) nutzt (Art. 293 Abs. 1h CRR). Dies gilt auch, wenn das Kreditinstitut interne Modelle zur Berechnung der Eigenmittelanforderungen für das Marktrisiko verwendet (von Art. 368 Abs. 1h und Abs. 2).
- Weitere jährliche Prüfungspflichten können sich aus regulatorischen Anforderungen (z. B. bei Nutzung des fortgeschrittenen Messansatzes für das operationelle Risiko lt. Art. 321 Abs. 1e CRR ergeben).
- Die Maßnahmen zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen sind nach den Auslegungs- und Anwendungshinweisen zum Geldwäschegesetz (AuA AT)“ der BaFin (11/2024 3.7) vollständig innerhalb eines Zeitraums von drei Jahren zu prüfen. Jährlich Prüfungspflichten gem. EU-Verordnung 2018/389 Art. 3 (technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation) zur Überprüfung der Sicherheitsmaßnahmen bei Zahlungsdienstleistern.
- Jährliche Überprüfung der Vergütungsgrundsätze gem. EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (hier Abschnitt 2.1 Ziff. 42 und 2.5 Ziff. 63).

In der Mehrjahresplanung sollten objektbezogene Planwerte, welche dem notwendigen zeitlichen Aufwand für eine Prüfung des Objektes entsprechen sollen, erfasst werden (Standardaufwand Prüfungsteam inkl. Steuerungs- und Unterstützungsfunktionen).

3.1.3 Jahresplanung

Die Jahresplanung zeigt alle Prüfungen auf, die im Folgejahr durchgeführt werden sollen. Dabei werden auf Basis der Prioritätenliste – in der die Prüfobjekte mit fälligem aufsichtsrechtlichem Pflichtprüfungsintervall besonders gekennzeichnet werden – und der bekannten Risikoindikatoren die Prüfobjekte ausgewählt, die im Folgejahr zur Prüfung anstehen.

Der Planungsprozess sollte einen Austausch mit dem Management (insbesondere Geschäftsleitung und nachfolgende Führungsebene) bezüglich risikoorientiert zu berücksichtigender Sachverhalte beinhalten. Zur Vermeidung von Redundanzen, soweit risikoorientiert möglich, bietet es sich an, sich auch mit dem Jahresabschlussprüfer und den Kontrollfunktionen der 2nd Line zu deren Prüfungsschwerpunkten auszutauschen.

Die Jahresplanung sollte vor Beginn des neuen Geschäftsjahres erstellt werden. Für die entsprechende Kapazitätsplanung sind dabei folgende Faktoren zu berücksichtigen:

- Berücksichtigung des der Internen Revision zur Verfügung stehenden Budgets (Personal- und Sachkostenbudget) sowie der Unternehmensplanung
- Berücksichtigung von Tagen für Trainings- und Weiterbildungsaktivitäten und interne administrative Aktivitäten sowie Krankheitstagen bei der Kalkulation des verfügbaren Personalkapazitäten
- Vorhalten von Kapazitäten für ex ante-Aktivitäten (Begleitung wesentlicher Projekte, Beratung der Facheinheiten) sowie für Follow-up-Tätigkeiten
- Vorhalten einer Reserve („Puffer“) für außerplanmäßig notwendig werdende Prüfungen und Sonderuntersuchungen. Die Größe eines derartigen Puffers ist nicht vorgeschrieben, sondern sollte sich an dem historischen Bedarf und an absehbaren Änderungen orientieren. In der Praxis wird vielfach ein Puffer in Höhe von 10% der Prüfungs-Kapazität als sinnvoll erachtet
- Aufnahme bereits bekannter und im Folgejahr fälliger Nachschauprüfungen
- Berücksichtigung von Prüfungsaktivitäten zu wesentlichen Auslagerungen bzw. kritischen oder wichtigen IKT-Drittdienstleistern sowie Einlagerungen von Geschäftsaktivitäten, bei denen eine vertragliche Prüfungspflicht besteht
- Berücksichtigung von Prüfungen als Konzernrevision und Prüfungsaktivitäten zur Unterstützung von angeschlossenen Unternehmen und/oder Tochtergesellschaften, wo dies organisatorisch oder vertraglich vorgesehen ist

Die Prüfungen für die Planungsperiode werden systematisch zusammengestellt, im Planungssystem angelegt und der Revisionsleitung spätestens zu Beginn des neuen Geschäftsjahres zur Genehmigung vorgelegt.

Für jede im Rahmen der Jahresplanung angelegte Prüfung sollten auf Grundlage der zu diesem Zeitpunkt vorliegenden/bekanntesten Informationen die Prüfungsdauer und die Prüfungsart sowie eine kurze Beschreibung des vorläufigen Prüfungsinhalts festgelegt werden.

Prüfobjekte, die, trotz ihrer Fälligkeit bzw. trotz der festgestellten Prüfungsnotwendigkeit, aus nachvollziehbaren Gründen nicht in die Jahresplanung aufgenommen werden, sind inklusive einer Begründung für die Nichtaufnahme aufzulisten.

Die jeweiligen Jahresplanungen/Genehmigungen (inkl. der jeweiligen Prioritätenliste und der fälligen, nicht in die Jahresplanung aufgenommenen Objekte) sind sechs Jahre aufzubewahren bzw. zu archivieren.

3.1.4 Operative Planung (unterjährige Disposition)

Auf Basis der genehmigten Jahresplanung wird die operative Planung unterjährig verfeinert und rollierend fortgeschrieben. Das Revisions-Management kann auf diese Weise risikoorientiert Prioritäten setzen oder auf die Verfügbarkeit von Teammitgliedern bzw. die erforderlichen Fähigkeiten reagieren.

Das geplante Start- und Enddatum der Prüfung muss die Zeiten für die Planung, Vorbereitung, Durchführung, Berichterstattung und Abschlussarbeiten umfassen.

Um eine erfolgreiche Zusammenarbeit und Kommunikation mit der geprüften Einheit zu ermöglichen, sollte der verantwortliche Prüfungsleiter frühzeitig benannt werden.

Wesentliche nachträgliche Anpassungen der genehmigten Jahresplanung, die sich im weiteren Verlauf durch Änderung von Prioritäten oder organisatorischen Rahmenbedingungen ergeben, sind unterjährig von der Geschäftsleitung zu genehmigen. Dies betrifft insbesondere geplante, aber nicht mehr durchführbare Prüfungen. Kriterien für die Wichtigkeit sollten sinnvollerweise festgelegt werden, damit Klarheit besteht, wann die Revision die Genehmigung einzuholen hat. Beispiele für Kriterien sind:

- Ein zu definierendes Verhältnis der Änderungen zum ursprünglichen Prüfungsplan (Anzahl Prüfungen oder Prüfungskapazitäten)
- Verschiebung von Prüfungen mit hohem Risikogewicht in das nächste Prüfungs-/Geschäftsjahr

- Verschiebung von regulatorischen Pflichtprüfungen in das nächste Prüfungs-/ Geschäftsjahr

Die Begründung für die Verschiebung/Absage geplanter oder für unterjährig nachgeplanter Prüfungen und deren Genehmigung sind zu dokumentieren.

3.2 Prüfungsvorbereitung

Mit der Phase der Prüfungsvorbereitung beginnt die Prüfung. Zunächst sind Hintergrundinformationen zu den Zielen, Strategien und Risiken der abgedeckten Prüfobjekte aus verfügbaren Quellen heranzuziehen, um eine fundierte Risikoeinschätzung vornehmen zu können. Dies können bspw. sein:

- Strategien wie z. B. Geschäfts- und Risikostrategie, IT-Strategie, Outsourcing Strategie, Personalstrategie
- Regulatorische Vorgaben (insbesondere Änderungen)
- Informationen zur Aufbau- und Ablauforganisation (inkl. Governance, Risikomanagement und Kontrollprozesse)
- Veränderungen an bestehenden Prozessen, Systemen und Produkten (z. B. NPP-Verfahren und Projekte)
- IT-Systeme
- Gespräche/Interviews
- Dauerakten/ Continuous Auditing
- Vorprüfungen
- Ergebnisse Drittprüfungen, z. B. des Wirtschaftsprüfers
- Informationen zu Auslagerungen
- Berichte für das Management, z. B. Risikoberichte
- Datenanalysen
- Beschwerden/Schadensfälle

Zudem sind vor jeder Prüfung grundsätzlich die Feststellungen aus vorangegangenen Prüfungen (interne und externe) sowie ggf. Risikoübernahmen zu identifizieren, um diese bei entsprechender Relevanz (z. B. Risikoorientierung) im Rahmen der anstehenden Prüfung erneut zu beurteilen.

3.2.1 Anforderungsliste

Sofern diese Unterlagen nicht direkt aus verfügbaren Systemen bzw. Dokumentationen zu beschaffen sind, ist eine Anforderungsliste zu erstellen. Diese Liste sollte rechtzeitig vor Beginn der Prüfungshandlungen an das Management der zu prüfenden Einheit/en (Ausnahme Sonderuntersuchungen) versandt werden (ggf. im Rahmen der Prüfungsankündigung, vgl. Abschnitt 3.2.6). Die Anforderungsliste ist während der Prüfungsdurchführung fortzuführen.

3.2.2 Risikoeinschätzung (Risk Assessment)

Aufbauend auf der im Rahmen der Jahresplanung erfolgten Risikoeinschätzung werden zu Beginn der Prüfung die zum Zeitpunkt der Jahresprüfungsplanung getroffenen Annahmen unter Berücksichtigung der aktuellen Risikoeinschätzung evaluiert. Im Rahmen dieser Risikoeinschätzung sind die gewonnenen aktuellen Informationen systematisch auf Risikosignale (inkl. Fraud-Risiken) zu untersuchen. Gesetzliche bzw. aufsichtsrechtliche Anforderungen und aktuelle Auslegungen von Regelungen sind dabei zu berücksichtigen. Bei der Erstellung der Risikoanalyse empfiehlt es sich, die einzelnen Prozesse oder Themenschwerpunkte des Prüfungsgebietes zu bewerten und daraus Schwerpunkte für die Prüfungshandlungen abzuleiten und diese nach Wesentlichkeit zu priorisieren. Das Ergebnis der Risikoanalyse ist dezidiert, z. B. in einem Prüfungshandbuch oder -memorandum (siehe Abschnitt 3.2.8), zu dokumentieren.

3.2.3 Prüfungsziele

Basierend auf den analysierten bzw. vermuteten Risiken sind die Prüfungsziele festzulegen. Die Prüfungsziele beschreiben die spezifischen Sollzustände, die erreicht werden sollen, einschließlich derer, die durch Gesetze und/oder Vorschriften vorgegeben sind. Die Revisionsleitung muss die Ziele, den Umfang der Prüfung (siehe Abschnitt 3.2.4) sowie das daraus abgeleitete Arbeitsprogramm sowie alle Änderungen während der Durchführung genehmigen.

Folgende grundsätzliche Prüfungsziele stehen dabei zur Auswahl:

Prüfungsziel	Erläuterung
Ordnungsmäßigkeit	<p>Einhaltung von unternehmensinternen und -externen Vorgaben</p> <p>Ziel der Prüfung der „Ordnungsmäßigkeit“ ist die Sicherstellung der Einhaltung unternehmensexterner Vorgaben (z. B. geltende gesetzliche und aufsichtsrechtliche Vorgaben sowie sonstige externe Regelungen und anerkannte Standards) sowie unternehmensinterner Anforderungen (z. B. Satzungen, Geschäftsanweisungen, interne Richtlinien, Kompetenzordnungen oder Geschäftsleitungsbeschlüsse) in formeller und materieller Hinsicht.</p> <p>Hierbei werden durch geeignete Prüfungshandlungen IST-Abweichungen zu dem durch die existierenden Vorgaben definierten SOLL-Zustand ermittelt⁴ und – in Verbindung mit der Formulierung geeigneter Empfehlungen – im Rahmen von Feststellungen adressiert, um zur Ordnungsmäßigkeit des Prüfobjektes beizutragen.</p>
Sicherheit	<p>Schutz von Menschen, Vermögen und Daten</p> <p>Ziel der Prüfung der „Sicherheit“ ist die Angemessenheit von Regelungen und Vorkehrungen zur Sicherung der Vermögenswerte und Daten sowie der Maßnahmen zur inneren und äußeren Sicherheit. Hierzu gehören u. a. der Schutz des eigenen und des für Dritte verwalteten Vermögens, die Verhinderung und Aufdeckung von Straftaten, die Vermeidung von physischen Gefährdungen der Infrastruktur (Gebäude, Betriebs- und Geschäftsausstattung, IT-Hardware), der Schutz der Daten und der Betriebsgeheimnisse, die Verfügbarkeit und Integrität der IT-Systeme sowie die Arbeitssicherheit.</p> <p>Hierbei wird das Interne Kontrollsystem auf Angemessenheit hinsichtlich des zu erreichenden Schutzniveaus, die Funktionsfähigkeit und Wirksamkeit der vorgesehenen Kontrollen und Schutzmaßnahmen beurteilt sowie bei Bedarf geeignete Maßnahmen zur Verbesserung des Internen Kontrollsystems adressiert.</p>

⁴ Vgl. Peemöller in Förstler/ Peemöller (Hrsg.), Wirtschaftsprüfung und Interne Revision, Heidelberg 2004.

Wirtschaftlichkeit	Effizienter Ressourceneinsatz sowie effiziente Prozess- und Kontrollgestaltung
	<p>Ziel der Prüfung der „Wirtschaftlichkeit“ ist die Verbesserung der Effizienz aller Betriebs- und Geschäftsabläufe. Hierbei wird untersucht, ob alle betrieblichen Sachverhalte und Abläufe dem ökonomischen Prinzip entsprechen⁵ und somit die Prozesse effizient gestaltet sind, die etablierten Kontrollen zum angenommenen Risiko in angemessenem Verhältnis stehen, das Verhältnis von Aufwand und Nutzen optimiert wurde und die zur Verfügung stehenden Mittel und Ressourcen effizient eingesetzt werden.</p> <p>Der als Maßstab anzulegende Soll-Zustand ist – mangels eindeutiger Vorgaben – auch hier vom Prüfer selbst zu erarbeiten. Abweichungen vom Soll-Zustand stellen nicht notwendigerweise Fehler, sondern in den meisten Fällen Optimierungspotential dar, welches die Interne Revision aufzeigen kann⁶.</p>
Zweckmäßigkeit	Ausrichtung von Prozessen und Kontrollen auf die (Unternehmens-)Ziele
	<p>Ziel der Prüfung der „Zweckmäßigkeit“ ist es, die Geschäftsprozesse (einschließlich Risikomanagement- und -controllingsystem, Berichtswesen, Informationssysteme, Finanz- und Rechnungswesen) sowie des Internen Kontrollsystems (IKS) hinsichtlich deren Eignung, die Unternehmensziele zu erreichen zu beurteilen. Vor diesem Hintergrund wird analysiert, ob die Prozesse an den Unternehmenszielen ausgerichtet sind und den Bedürfnissen der (internen/externen) Kunden entsprechen. Das diesbezüglich implementierte Kontrollsystem ist daraufhin zu überprüfen, ob die implementierten Kontrollen hinsichtlich ihrer Ausgestaltung (d.h. ihres „Designs“) geeignet sind, die mit ihnen verbundenen Kontrollziele (z. B. Vollständigkeit, Richtigkeit, Zeitnähe) zu erreichen.</p> <p>Bei der Zweckmäßigkeitprüfung hat der Revisor den Soll-Zustand (mangels eindeutig formulierter Vorgaben) aus den Unternehmenszielen heraus selbst abzuleiten⁷ und der Geschäftsleitung bei Abweichungen unterstützend Empfehlungen auszusprechen.</p>

⁵ Vgl. Peemöller in Förchler/ Peemöller (Hrsg.), Wirtschaftsprüfung und Interne Revision, Heidelberg 2004.

⁶ Vgl. ebd.

⁷ Vgl. Lück, Lexikon der Internen Revision, München 2001, Seite 384.

Zukunftssicherung**Sicherstellung adäquater Strategieprozesse und der Einhaltung strategischer Vorgaben**

Alle Ziele der Internen Revision dienen grundsätzlich der Zukunftssicherung der Unternehmung. Grundlage für die Zukunftssicherung einer Unternehmung ist eine nachhaltige Geschäftsstrategie der Geschäftsleitung. Ziel der Prüfung der „Zukunftssicherung“ ist zum einen die Einhaltung und Umsetzung der von der Geschäftsleitung vorgegebenen Unternehmensstrategie und zum anderen die konsistente Ausrichtung der Risikostrategie an der Geschäftsstrategie. Die umfasst – unter Berücksichtigung der Unternehmensstrategie – die Prüfung, ob geeignete Maßnahmen getroffen wurden, den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkennen zu können (§ 91 Abs. 2 AktG); ferner ist in diesem Rahmen zu prüfen, ob ein funktionsfähiges Risikomanagementsystem eingerichtet worden ist.⁸

Der Inhalt der Geschäftsstrategie selbst ist nicht Gegenstand von Prüfungshandlungen durch (Jahresabschlussprüfer oder) die Interne Revision, dieser liegt allein in der Verantwortung der Geschäftsleitung⁹ Stattdessen prüft die Interne Revision den Strategieprozess¹⁰ und leistet durch die Prüfung der Umsetzung der vor Geschäftsleitung beschlossenen Strategie sowie deren adäquater Berücksichtigung in der Risikostrategie und ggf. sonstigen Teilstrategien einen Beitrag zur Zukunftssicherung. Letzteres erfolgt u. a. durch Prüfung der vollständigen Identifikation und Erfassung aller Risiken, Beurteilung von Risikoanalyse und -bewertung, Prüfung der Realisierung und Zweckmäßigkeit der Maßnahmen zur Risikosteuerung und der Einhaltung der integrierten Kontrollen sowie der Prüfung der Kommunikation der Risiken.¹¹

Abb. 6: Prüfungsziele

Die MaRisk definieren den Prüfungsgegenstand der Internen Revision u. a. in AT 4.4.3 Tz. 3. Insbesondere ist dementsprechend „... die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen ...“ zu prüfen. Das interne Kontrollsystem umfasst nach § 25a Abs. 1, Nr. 3 KWG insbesondere „aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche, Prozesse zur Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken entsprechend den in Titel VII Kapitel 2

⁸ Lück, Lexikon der Internen Revision, München 2001, Seite 380.

⁹ BaFin, Rundschreiben 06/2024 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ (09.05.2024), AT 4.2 Tz. 1, Erläuterung.

¹⁰ BaFin, Rundschreiben 06/2024 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ (09.05.2024), AT 4.2 Tz. 5.

¹¹ DIIR e.V., DIIR Revisionsstandard Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision“.

Abschnitt 2 Unterabschnitt II der Richtlinie 2013/36/EU niedergelegten Kriterien sowie eine Risikocontrolling-Funktion und eine Compliance-Funktion.“

Ferner ist die Prüfungsstrategie so zu gestalten, dass die Prüfungshandlungen eine nachhaltige Aussage der festgestellten Prüfungsergebnisse im Kontext der Prüfungsziele ermöglichen.

3.2.4 Prüfungsumfang

Der Prüfungsumfang legt den inhaltlichen Schwerpunkt und die Grenzen der Prüfung fest. Dieser wird auf der Basis von vorläufig identifizierten Risiken und Schwachstellen festgelegt und muss ausreichend sein, um das Erreichen der Prüfungsziele zu ermöglichen. Dabei müssen auch relevante Systeme, Aufzeichnungen, Personalausstattung und Vermögensgegenstände einbezogen werden, einschließlich jener Aktivitäten, die sich unter der Kontrolle Dritter befinden (Drittbezüge).

Der Prüfungsumfang wird dem Management der geprüften Einheit zu Beginn der Prüfung vorgestellt. Zusätzliche im Prüfungsumfang aufzunehmende Hinweise oder Prüfungswünsche können ggf. berücksichtigt werden (vgl. Abschnitt 3.2.7).

Einschränkungen des Umfangs werden mit dem Management der geprüften Einheit besprochen, um eine Lösung zu finden. Einschränkungen des Umfangs sind Bedingungen, die die Revisoren daran hindern, ihre Arbeiten wie im Arbeitsprogramm vorgesehen durchzuführen, z. B. Ressourcenbeschränkungen oder Einschränkungen beim Zugang zu Personal, Einrichtungen, Daten und Informationen. Kann mit dem Management keine Einigung erzielt werden, wird die Revisionsleitung die Umfangsbeschränkung nach einem festgelegten Verfahren dokumentieren und ggf. an die Geschäftsleitung eskalieren.

Wesentliche Änderungen des Prüfungsumfangs während der Prüfung sind in den Arbeitspapieren und ggf. über eine Anpassung des Planungsdokuments (Prüfungshandbuch, oder -memorandum, vgl. Abschnitt 3.2.8) zu dokumentieren.

Die Prüfungsschwerpunkte bzw. die Prüfungstiefe spiegeln sich in den Fragen der Prüfungsleitfäden bzw. strukturierten Checklisten wider. Auch bei der Erstellung der Prüfungsleitfäden empfiehlt es sich (analog der Erstellung der Risikoanalyse), diese an den einzelnen Prozessen oder Themenschwerpunkten des Prüfungsgebietes auszurichten. Auf Basis von Expertenschätzungen werden die vorgesehenen Prüfungshandlungen (z. B. Prozessaufnahmen, Datenanalysen, Stichprobenprüfungen) definiert und die erforderlichen Ressourcen ermittelt (vgl. Abschnitt 3.2.8).

3.2.5 Organisation der Prüfung

Entsprechend der Zielsetzung der Prüfung sind fachlich versierte Revisoren in das Prüfungsteam aufzunehmen. Im Regelfall sind eine Prüfungsleitung und weitere klare Verantwortlichkeiten (Fachprüfungsarbeit, Überwachungsfunktion, Qualitätssicherer) zu benennen. Es sind Prüfungsbeginn und -ende sowie der geplante Aufwand in Prüferstunden oder -tagen festzulegen. Die Prüfungsleitung sollte in dieser Phase auch überprüfen, ob die in der Jahresplanung erfassten Planwerte (Aufwand Prüfungsteam inkl. Steuerungs- und Unterstützungsfunktionen) im Vergleich zum vorgesehenen Prüfungsumfang angemessen sind oder ggf. Anpassungen erforderlich sind. Es empfiehlt sich, in Abhängigkeit von der Komplexität der Prüfung, Meilensteine festzulegen, z. B. für Versand Prüfungsankündigung, Prüfungs-Kick-off, Ende Prüfungs-Fieldwork, Berichtsversand.

Sofern mit der Prüfung Reisetätigkeiten bzw. Prüfungsphasen z. B. in Niederlassungen des Instituts verbunden sind, sollten rechtzeitig (spätestens mit Ankündigung der Prüfung) die entsprechenden organisatorischen Vorkehrungen getroffen werden (z. B. die Sicherstellung der Infrastruktur für die Revisoren vor Ort).

3.2.6 Prüfungsankündigung

Vor Beginn einer Prüfung ist eine Prüfungsankündigung an das betroffene Management bzw. die betroffenen Organisationseinheiten zu versenden. Die Prüfungsankündigung informiert über das Prüfungsthema (ggf. auch den Prüfungsumfang und vorab zu übersendende Unterlagen, vgl. Abschnitt 3.2.1), über den Zeitraum der Prüfung vor Ort sowie die Namen der Mitglieder des Prüfungsteams und ggfs. der Prüfungsleitung. Die Prüfungsankündigung sollte in der Regel zwei Wochen vor Beginn der Prüfung erfolgen (Ausnahme: Sonderprüfungen, hier entfällt die Ankündigung). Bei kurzfristig angesetzten Prüfungen können die entsprechenden Informationen im Rahmen des Eröffnungsgesprächs erfolgen.

3.2.7 Eröffnungsgespräch (Kick-off-Meeting)

Es empfiehlt sich, vor Beginn einer Prüfung ein Eröffnungsgespräch durchzuführen. Teilnehmer des Eröffnungsgesprächs sollten nach Relevanz und in Abhängigkeit zu den Prüfungszielen die Leitung bzw. Verantwortlichen der geprüften Einheit/en, das Prüfungsteam sowie die Prüfungsleitung (ggf. auch Revisionsleitung) sein.

Das Eröffnungsgespräch ermöglicht, die Vorgehensweise der Internen Revision vorzustellen, die Ziele und den Umfang der Prüfung dem betroffenen Management darzulegen, sowie zusätzliche Informationen von der geprüften Einheit zu erhalten. Außerdem gibt es den Geprüften die Möglichkeit, ihre Einschätzung über den Zustand des internen

Kontrollsystems und des Risikomanagementsystems im Kontext mit dem Prüfungsgegenstand darzulegen. Die geprüften Einheiten sollen zudem ermutigt werden, die ihnen bekannten Schwächen während des Gesprächs offen anzusprechen. Hierzu zählen auch ggf. bestehende offene Feststellungen, die durch Einheiten der zweiten Linie (Kontrollfunktionen) getroffen wurden oder durch die geprüften Einheiten im Vorfeld selbst identifizierte Mängel und Weiterentwicklungsbedarfe und deren Abarbeitungsplanung und -stand. Das betroffene Management hat im spätestens Rahmen des Gesprächs noch die Möglichkeit, Prüfungswünsche (-themen) zu äußern. Es obliegt dann im Regelfall der Prüfungs- bzw. Revisionsleitung, darüber zu entscheiden, inwieweit diese Prüfungswünsche mit den Prüfungszielen vereinbar sind und berücksichtigt werden können.

Ziel des Eröffnungsgesprächs ist es insbesondere, ein gemeinsames Grundverständnis von Interner Revision und Geprüften zu schaffen und damit das gegenseitige Vertrauen zu stärken. Darüber hinaus werden organisatorische Fragestellungen geklärt (z. B. Ansprechpartner, An- und Abwesenheiten, Bereitstellung von Unterlagen).

3.2.8 Dokumentation

Unmittelbar im Anschluss an das Eröffnungsgespräch erfolgt die Fertigstellung und Genehmigung des Planungsdokuments (Prüfungsauftrag oder -memorandum), welches die Ergebnisse der zuvor beschriebenen Arbeitsschritte beinhaltet. Zur Dokumentation der Durchführung der Prüfung sollten Prüfungsleitfäden oder strukturierte Checklisten erstellt werden (ggf. auch unter Nutzung einer Risiko-Kontroll-Matrix) und es sind entsprechende (elektronische) Prüfungsverzeichnisse und -ordner anzulegen. Die MaRisk regeln die Anforderungen an die Dokumentation insbesondere in BT 2.4 Tz. 2: „Die Prüfungen sind durch Arbeitsunterlagen zu dokumentieren. Aus ihnen müssen die durchgeführten Arbeiten sowie die festgestellten Mängel und Schlussfolgerungen für sachkundige Dritte nachvollziehbar hervorgehen.“

3.3 Prüfung

3.3.1 Prüfungshandlungen

Den Mitgliedern des Prüfungsteams obliegt es, während der gesamten Prüfung ein konstruktives, offenes und von Fairness geprägtes Verhältnis zu den Führungskräften und Mitarbeitenden der geprüften Einheit aufzubauen. Hierdurch wird der Informationsaustausch zwischen der Internen Revision und den Geprüften gefördert und die Akzeptanz für die Prüfungshandlungen und -ergebnisse gesteigert.

Im Rahmen der Prüfungshandlungen wird der bei der Prüfungsvorbereitung festgelegte und genehmigte Prüfungsumfang anhand des vorgesehenen Arbeitsprogramms abgearbeitet.

Ziel der Prüfungshandlungen ist die Identifikation, Sammlung, Bewertung und Dokumentation von Informationen, auf deren Basis ein Prüfungsurteil im Hinblick auf die definierten Prüfungsziele gebildet und ggf. Prüfungsfeststellungen getroffen werden. Daneben kann durch die Betrachtung der Ursachen für getroffenen Prüfungsfeststellungen („root cause“) implizit die Risikokultur und das Führungsverhalten innerhalb der geprüften Einheit beurteilt werden.

Die im Rahmen der Prüfung gesammelten Informationen sollen relevant, zuverlässig und ausreichend sein:

- Relevante Informationen passen zu den Prüfungszielen, liegen innerhalb des Umfangs der Prüfung und tragen zur Entwicklung von Prüfungsergebnissen bei.
- Zuverlässige Informationen sind sachlich richtig und aktuell. Die Revisoren wenden professionelle Skepsis an, um zu bewerten ob Informationen zuverlässig sind.
- Ausreichende Informationen ermöglichen es Revisoren, Analysen durchzuführen und Bewertungen abzuschließen. Darüber hinaus wird es Dritten ermöglicht, anhand der Informationen zu den gleichen Schlussfolgerungen zu gelangen.

Die Prüfungshandlungen lassen sich grundsätzlich in Beurteilungen der Angemessenheit der Prozesse und Kontrollen (Test-of-Design) und deren Wirksamkeit (Test-of-Operating-Effectiveness) unterscheiden:

- Bei der Angemessenheit wird beurteilt, ob die beschriebenen Kontrollen und Prozesse so ausgestaltet und implementiert sind, dass sie geeignet sind, die Risiken gemäß den internen/externen Vorgaben zu mitigieren. Zur Prüfung der Angemessenheit bietet sich regelmäßig eine Aufnahme der Prozesse und Kontrollen anhand eines konkreten Geschäftsvorfalles an (Test-of-One).
- Bei der Wirksamkeitsprüfung wird anhand von Stichproben oder Datenanalysen (Freigabeprotokollen, Systemdateien, Belege etc.) untersucht, ob die Kontrollen oder Prozessschritte innerhalb des zu prüfenden Zeitraumes gemäß den Vorgaben (Organisationsrichtlinien) des Kreditinstituts ausgeführt wurden und die Durchführung anhand einer angemessenen Dokumentation nachvollziehbar ist. Die Prüfungshandlungen werden risikobasiert durchgeführt und es sollte festgelegt werden, in welchen Fällen neben der Angemessenheitsprüfung auch Wirksamkeitsprüfungen durchgeführt werden. Dies sollte abhängig von den zur Verfügung stehenden Ressourcen und einer spezifischen Risikoeinschätzung erfolgen. So empfiehlt es sich bei Schlüsselkontrollen für Prozesse mit einem hohen inhärenten Risiko auch stets die Kontrollwirksamkeit zu prüfen. Im Gegenzug kann z. B. auf eine Wirksamkeitsprüfung verzichtet werden, wenn bereits die Angemessenheitsprüfung ergibt, dass

die Kontrolle fehlt oder nicht angemessen ausgestaltet ist. In diesem Fall könnten sich die weiteren Prüfungshandlungen darauf fokussieren, die Wesentlichkeit des Kontrollversagens über Datenanalysen zu ermitteln. Ebenfalls können Wirksamkeitsbeurteilungen der 2nd Line herangezogen und bewertet werden, ohne dass die Interne Revision selbst noch zusätzliche Wirksamkeitsprüfungen durchführt. Die erstellten Nachweise für die im Rahmen der Prüfungshandlungen getroffene Prüfungsfeststellungen müssen

- eine sachlogische Beziehung zur Angelegenheit besitzen,
- einen nachvollziehbaren Schluss auf die Prüfungsfeststellung für einen sachverständigen Dritten erlauben und
- hinreichend gesichert sein.

Die Einhaltung dieser Anforderungen führt zu belastbaren Feststellungen, welche zu einer hohen Akzeptanz durch die Geprüften beitragen.

Der Prüfungsleiter überwacht laufend, ob der im Vorfeld festgelegte Prüfungsumfang sowie die Prüfungsschwerpunkte noch sachgerecht und angemessen ist. Ist dies nicht der Fall, sind entsprechende Anpassungen vorzunehmen, zu begründen und abhängig vom Sachverhalt kompetent zu genehmigen.

Zur Steuerung der Prüfung sind die bereits aufgewendeten Prüferzeiten durch den Prüfungsleiter zu überwachen. Dafür sollten alle Prüfer ihren Aufwand regelmäßig und im Allgemeinen vor Beendigung der Prüfung erfassen und dem Prüfungsleiter zugänglich machen. Die Angaben werden auch für künftige Planungen verwendet und bilden die Grundlage für eine ggf. erfolgreiche Kostenverrechnung.

Essenziell ist ein regelmäßiger Austausch des Prüfungsteams mit dem Prüfungsleiter, um die Ergebnisse der einzelnen Prüfungshandlungen, etwaige Feststellungen und weitere Prüfungshandlungen abzustimmen. Gleichzeitig werden getroffene Feststellungen und die hieraus abgeleiteten Maßnahmen mit den verantwortlichen Mitarbeitenden erörtert und in sinnvollen Abschnitten mit dem Prüfungsleiter sowie dem Management der geprüften Einheit besprochen. Unter Umständen empfiehlt sich die Vereinbarung eines Jour fixe des Prüfungsteams sowie zwischen Prüfungsleiter und Management der geprüften Einheit für den Prüfungszeitraum, um sich regelmäßig über den Status der Prüfungshandlungen und die getroffenen Feststellungen auszutauschen.

3.3.2 Dokumentation der Prüfungshandlungen

Alle Prüfungshandlungen sind so zu dokumentieren, dass sie für einen sachverständigen Dritten in angemessener Zeit verständlich sind. Die Arbeitspapiere sollen Ziel, Art und Umfang der durchgeführten Prüfungshandlungen, die daraus resultierenden Ergebnisse

und den Prüfer sowie den die Prüfungshandlungen Qualitätssichernden (z. B. Prüfungsleiter) ausweisen.

Aus den Prüfungshandlungen resultierende Feststellungen müssen belegt und transparent sein. Grundsätzlich gilt, dass der Weg von der Prüfungshandlung zum Revisionsbericht (und umgekehrt) nachvollziehbar sein muss. Zu diesem Zweck sind die Prüfungsunterlagen angemessen und nachvollziehbar zu referenzieren bzw. zu verlinken. Daneben sollte die sachliche Richtigkeit der Prüfungsergebnisse, die zu Prüfungsfeststellungen führen, mit dem Fachbereich abgestimmt und dokumentiert werden.

Änderungen des Prüfungsumfangs oder -schwerpunkts sind unter Angabe der Gründe zu dokumentieren und in Abhängigkeit vom Umfang der Änderungen kompetenzgerecht zu genehmigen.

Die Arbeitspapiere sind nach vorgegebenen Regelungen und Strukturen in einer einheitlichen und sachlogisch nachvollziehbaren Form abzulegen und sechs Jahre aufzubewahren.

3.3.3 Risikoeinstufung von Feststellungen und Revisionsergebnissen

Gemäß MaRisk, BT 2.4 Tz. 1 zur Berichtspflicht muss die Interne Revision zeitnah einen schriftlichen Bericht anfertigen. Hierbei sind wesentliche Mängel besonders herauszustellen und die Prüfungsergebnisse zu beurteilen. Diese Beurteilung sollte im Rahmen einer zusammenfassenden Beurteilung dem Bericht vorangestellt werden.

Neben der zusammenfassenden Bewertung der Prüfungsergebnisse ist eine gesonderte Beurteilung der einzelnen Prüfungsfeststellungen/Mängel vorzunehmen. Bei der Bewertung der Beurteilung der potenziellen Feststellungen sind die tatsächlichen bzw. potenziellen Auswirkungen des Mangels festzustellen und daraus die Wesentlichkeit des Mangels zu bewerten. Daneben sind die Ursachen (root cause) für die Feststellungen zu identifizieren.

Als Maßstab für die Einstufung der Prüfungsfeststellungen/Mängel empfiehlt es sich, auf das für das Gesamtinstitut resultierende Risiko abzustellen. Neben den in den MaRisk vorgegeben Mängelkategorien („besonders schwerwiegend“, „schwerwiegend“, „wesentlich“) könnten Prüfungsfeststellungen/Mängel hierbei z. B. auch als „bemerkenswert/mittel“ oder „gering(fügig)“ bewertet werden. Die konkreten Abstufungen von Prüfungsfeststellungen/Mängel könnten sich hierbei an folgendem Praxisbeispiel orientieren:

- **Besonders schwerwiegende Feststellung**
 - Unter Berücksichtigung der wesentlichen Risikoarten des Instituts (z. B. Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken, operationelle Risiken,

Konzentrationsrisiken, Reputationsrisiken, Platzierungsrisiken) besteht ein existenzielles Gefährdungspotenzial für den Geschäftsbetrieb des Instituts in der Gesamtbetrachtung.

- Es sind Maßnahmen zur sofortigen Schadensbegrenzung und der Abwendung möglicher der existenzbedrohenden Risiken zu ergreifen. Eine unverzügliche Berichterstattung durch die Geschäftsleitung an das Aufsichtsorgan ist erforderlich.

- **Schwerwiegende Feststellung**

- Unter Berücksichtigung der wesentlichen Risikoarten des Instituts (z. B. Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken, operationelle Risiken, Konzentrationsrisiken, Reputationsrisiken, Platzierungsrisiken) besteht ein erhebliches Gefährdungspotenzial für den Geschäftsbetrieb des Instituts in der Gesamtbetrachtung.
- Es sind Maßnahmen zur unverzüglichen Risikoreduktion bzw. Schadensbegrenzung erforderlich. Eine unverzügliche Berichterstattung an die Geschäftsleitung ist erforderlich.

- **Wesentliche Feststellung**

- Unter Berücksichtigung der wesentlichen Risikoarten des Instituts (z. B. Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken, operationelle Risiken, Konzentrationsrisiken, Reputationsrisiken, Platzierungsrisiken) besteht ein mittelbares Gefährdungspotenzial für den Geschäftsbetrieb des Instituts in der Gesamtbetrachtung
- Es sind Maßnahmen zur zeitnahen Risikoreduktion bzw. Schadensbegrenzung erforderlich. Eine Berichterstattung an die Geschäftsleitung sowie das Aufsichtsorgan ist im Rahmen der Quartals- und Jahresberichterstattung erforderlich

- **Bemerkenswerte Feststellung**

- Unter Berücksichtigung der wesentlichen Risikoarten des Instituts (z. B. Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken, operationelle Risiken, Konzentrationsrisiken, Reputationsrisiken, Platzierungsrisiken) besteht kein mittelbares Gefährdungspotenzial für den Geschäftsbetrieb des Instituts in der Gesamtbetrachtung
- Es existieren merkliche Auswirkungen auf die geprüfte Einheit. Für die Gesamtbank sind die Auswirkungen gering
- Eine über den Prüfungsbericht hinausgehende gesonderte Berichterstattung ist nicht erforderlich

- **Geringe Feststellung**

- Unter Berücksichtigung der wesentlichen Risikoarten des Instituts (z. B. Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken, operationelle Risiken, Konzentrationsrisiken, Reputationsrisiken, Platzierungsrisiken) besteht kein mittelbares Gefährdungspotenzial für den Geschäftsbetrieb des Instituts in der Gesamtbetrachtung
- Es existieren geringe Auswirkungen auf die geprüfte Einheit
- Eine über den Prüfungsbericht hinausgehende gesonderte Berichterstattung ist nicht erforderlich

Für die Ermittlung der Risikoeinstufungen der Einzelfeststellungen sollte dabei ein Verfahren gewählt werden, das zu einer in der Anwendung einer konsistenten Risikoeinschätzung der Internen Revision führt. Dabei ist zu prüfen, ob sich das Verfahren an den in der 2nd-Line (Risikomanagementfunktion, Compliance) verwendeten Verfahren orientieren kann. Eine Anlehnung an diese Risikobewertungsverfahren käme dann in Frage, wenn diese nach Prüfung der Internen Revision als angemessen beurteilt werden.

Die zusammenfassende Bewertung der Prüfungsergebnisse sollte dem Bericht vorangestellt werden. Sie muss nicht zwingend in Form von Score-Werten oder Noten erfolgen, könnte sich jedoch an folgendem Praxisbeispiel orientieren:

- **Gut (1)**

- Keine oder nur geringe Prüfungsfeststellungen
- Keine oder nur unwesentliche Verbesserungsmöglichkeiten hinsichtlich der Wirtschaftlichkeit innerhalb des Prüfungsgebietes sowie der Angemessenheit und Wirksamkeit des Internen Kontrollsystems

- **Zufriedenstellend (2)**

- Geringe Auswirkungen der Feststellungen auf das Prüfungsgebiet
- Moderate Verbesserungsmöglichkeiten hinsichtlich der Wirtschaftlichkeit innerhalb des Prüfungsgebietes sowie der Angemessenheit und Wirksamkeit des Internen Kontrollsystems

- **Noch zufriedenstellend (3)**

- Wesentliche Auswirkungen der Feststellungen auf das Prüfungsgebiet
- Keine wesentlichen Auswirkungen über das Prüfungsgebiet hinaus auf das Gesamtinstitut
- Deutliche Verbesserungsmöglichkeiten hinsichtlich der Wirtschaftlichkeit innerhalb des Prüfungsgebietes sowie der Angemessenheit und Wirksamkeit des Internen Kontrollsystems

- **Nicht zufriedenstellend (4)**
 - Wesentliche Auswirkungen der Feststellungen auf das Prüfungsgebiet
 - Wesentlichen Auswirkungen über das Prüfungsgebiet hinaus auf das Gesamtinstitut (z. B. durch Verstöße gegen Gesetze/aufsichtsrechtliche Vorgaben, dolose Handlungen)
 - Erhebliche, ggf. auch grundsätzliche Mängel hinsichtlich der Wirtschaftlichkeit sowie der Angemessenheit und Wirksamkeit des Internen Kontrollsystems innerhalb des Gesamtinstituts

- **Mangelhaft (5)**
 - Schwerwiegende oder besonders schwerwiegende Auswirkungen der Feststellungen auf das Prüfungsgebiet
 - Signifikante Auswirkungen über das Prüfungsgebiet hinaus auf das Gesamtinstitut (z. B. Reputationsschäden, Reduktion der Eigenmittel, deutlich negative Auswirkungen auf die GuV)
 - Massive Mängel hinsichtlich der Wirtschaftlichkeit innerhalb des Prüfungsgebietes sowie der Angemessenheit und Wirksamkeit des Internen Kontrollsystems des Gesamtinstituts

Zusätzliche Aspekte, welche bei der Vergabe des individuellen zusammengefassten Prüfungsergebnisses berücksichtigt werden können, sind:

- Angemessenheit, mit der sich das Management der geprüften Einheit der Überwachung des Geschäftsbetriebes widmet
- das Risikobewusstsein des Managements
- die Umsetzung vereinbarter Maßnahmen und die Bereinigung der Feststellungen aus vorangegangenen Prüfungen
- Ausmaß, Entwicklung und Management von Risiken
- Berücksichtigung von Feststellungen Dritter (Aufsicht, Wirtschaftsprüfer, Einheiten der zweiten Linie, Kontrollfunktionen) sowie von den geprüften Einheiten selbst identifizierte Feststellungen, die keinen Eingang in den Bericht gefunden haben

Erneute Feststellungen

Durch die hier beschriebenen Verfahrensweisen soll vermieden werden, dass ein noch offener Handlungsbedarf aus einer vorangegangenen Prüfung durch Erstellen einer neuen gleichartigen Feststellung (erneute Feststellung des gleichen Sachverhalts in einer neuen Prüfung) aus einer möglicherweise bereits erreichten Eskalationsstufe herausgenommen wird und dass somit durch die erneute Feststellung/ Handlungsempfehlung

der Nachverfolgungszyklus von neuem beginnt. Ziel ist es somit, dass die ursprünglich vereinbarten Erledigungstermine weiterhin Gültigkeit besitzen und nicht durch neue Termine ersetzt werden. Daneben weisen erneute Feststellungen darauf hin, dass in vorangegangenen Prüfungen getroffene Feststellungen nicht nachhaltig abgearbeitet wurden. Daher ist es wichtig, die Ursachen für den wiederholten Mangel aufzuzeigen, damit dieser Sachverhalt nachhaltig ausgeräumt wird.

- Szenario 1: Eine noch offene Feststellung liegt vor:
 - In den Prüfungshandlungen sollte beurteilt werden, ob der Abarbeitungsfortschritt adäquat ist. Nach Abschluss der Prüfungshandlungen wird im Prüfungsbericht auf die bestehende offene Feststellung verwiesen. Diese ist bei der Gesamtbewertung des Prüfungsergebnisses zu berücksichtigen.
 - Sofern sich aus den Prüfungshandlungen weitere Mängel ergeben, die durch die offene Feststellung nicht abgedeckt sind, kann eine neue inhaltlich aktualisierte Feststellung erfasst werden. Im Text der Feststellung/Handlungsempfehlung ist darauf hinzuweisen, dass es sich hierbei um eine bislang noch nicht erledigte Feststellung aus einer vorherigen Prüfung handelt (Angabe der alten Prüfungsnummer). Die Risikoeinstufung der neuen Feststellung kann, wenn sachlich begründet, abweichend von der alten Feststellung festgelegt werden. Die neue Feststellung ist mit dem ursprünglichen Erledigungstermin aus der alten Prüfung zu versehen.
 - Sofern sich im Prüfungsverlauf ergibt, dass die alte Feststellung/erledigt ist, wird diese unter Angabe der Gründe geschlossen.
- Szenario 2: Eine als erledigt gemeldete Feststellung ist noch offen:
 - Im Rahmen einer erneuten vertieften Prüfung zeigt sich, dass der Handlungsbedarf aus einer alten Feststellung, entgegen den früheren Angaben der geprüften Einheit und anschließender Beurteilung durch die Interne Revision (i. R. d. Plausibilitätsbeurteilung der Mängelbeseitigungsanzeige bei geringen bzw. bemerkenswerten Feststellungen), doch noch offen ist. In diesem Fall wird eine neue Feststellung/Handlungsempfehlung erfasst. Auf den Tatbestand wird in der Feststellung und je nach Materialität auch in der Zusammenfassung für das Management hingewiesen. Es wird dabei auch darüber berichtet, warum die Wiederholung der Feststellung erforderlich ist. Etwaige Managementfehler werden hierbei herausgearbeitet, um sicher zu stellen, dass die Sensibilität zur Abarbeitung von Feststellungen erhöht wird und eine nachhaltige Behebung des Mangels erfolgt.

3.3.4 Verfassen des Prüfungsberichtes

Über jede Prüfung wird unverzüglich ein schriftlicher Prüfungsbericht erstellt, der richtig, objektiv, prägnant, klar, konstruktiv und vollständig sein muss.

Der Prüfungsbericht zeigt den Auftrag und die Auftragsdurchführung (Prüfungsziel und -umfang, Prüfungsteam, Prüfungszeitraum, Prüfungsort, Prüfungsanlass und Art der Prüfung), das Prüfungsergebnis, Prüfungsfeststellungen nebst Bewertung und den hieraus resultierenden Handlungsbedarf nebst vereinbarten Erledigungsterminen und Verantwortlichkeiten auf. Dabei werden wesentliche Mängel sowie Gefahren und Risiken besonders herausgestellt. Alle Prüfungsberichte müssen nach einem verbindlichen Berichtskonzept erstellt werden, in welchem eine standardisierte Berichtsstruktur und formelle Merkmale vorgegeben werden. Für Sonderprüfungen und Nachschauprüfungen können separate Vorlagen verwendet werden.

Für die Prüfung wird eine zusammenfassende Bewertung der Prüfungsergebnisse (inkl. einer Aussage zur Ordnungsmäßigkeit der Prozesse) in die Zusammenfassung für das Management aufgenommen (vgl. Abschnitt 3.3.3). Das Gesamturteil eines Prüfungsberichtes umfasst das Urteil der Internen Revision bezüglich der Wirksamkeit der Governance-, Risikomanagement- und/oder Kontrollprozesse des Untersuchungsgegenstands, einschließlich einer Anerkennung, wenn die Prozesse wirksam sind.

Der Prüfungsbericht besteht aus einer prägnanten Zusammenfassung für das Management (Darstellung der Ergebnisse zu einzelnen Betrachtungsfeldern; wobei wesentliche Einzelergebnisse entsprechend herausgestellt werden) sowie unter Umständen einem umfassenden Hauptbericht und diversen Anlagen (u. a. Ausführungen zum Prüfungsauftrag und zur Prüfungsdurchführung, Prüfungsfeststellungen und Maßnahmen sowie risikoorientierte Erledigungstermine für die Umsetzung).

3.3.5 Qualitätssicherung und Abstimmung des Prüfungsergebnisses

Die einzelnen Berichtsteile werden im Verlauf der Prüfung mit den zuständigen Managementebenen der geprüften Einheit(en) besprochen und abgestimmt. Die Koordination erfolgt durch die Prüfungsleitung (vgl. Abschnitt 3.3.1).

Vor der abschließenden Behandlung des gesamten Prüfungsberichtes mit der/den geprüften Einheit(en) erfolgt eine Qualitätssicherung des Prüfungsberichtes durch den verantwortlichen Vorgesetzten des Prüfungsleiters.

Der qualitätsgesicherte Revisionsbericht wird mit der Leitung der geprüften Einheit in einer Schlussbesprechung abschließend behandelt.

Die Einladung der zuständigen Kompetenzträger zur Schlussbesprechung nach Abschluss der Prüfungshandlungen ist frühzeitig zu koordinieren.

An der Schlussbesprechung nehmen revisionsseitig i. d. R. der Prüfungsleiter, dessen Vorgesetzter sowie die Revisionsleitung (bei bedeutenden Prüfobjekten und -ergebnissen) teil. Ggf. sollten auch Mitglieder des Prüfungsteams an der Schlussbesprechung teilnehmen, falls deren Fachwissen für die Abstimmungen erforderlich ist. Der Berichtsentwurf sollte eine angemessene Zeitspanne vor der Schlussbesprechung bei der/den geprüften Einheit(en) vorliegen.

Durch die Schlussbesprechung wird sowohl der Internen Revision als auch der geprüften Einheit die Gelegenheit eingeräumt, abschließend zu Prüfungsfeststellungen Stellung zu beziehen. In der Schlussbesprechung werden angemessene Maßnahmen mit Durchführungsterminen und eindeutigen Verantwortlichkeiten verabschiedet sowie die Übereinstimmung oder Meinungsverschiedenheiten zu den Prüfungsergebnissen festgehalten. Wird von den Geprüften keine Schlussbesprechung gewünscht, so kann auf diese verzichtet werden. In diesem Fall erfolgt eine andere, nachvollziehbare und dokumentierte Form der Abstimmung des Prüfungsergebnisses z. B. per E-Mail.

Sofern über einzelne Feststellungen und die zur Erledigung dieser Feststellungen zu ergreifenden Maßnahmen keine Einigung erzielt werden kann, haben die geprüften Einheiten die Möglichkeit, hierzu separat Stellung zu nehmen (MaRisk BT 2.4 Tz. 3).

In der Praxis wird die entsprechende Stellungnahme („management response“) auf unterschiedliche Weise im Rahmen der Berichterstattung durch die Interne Revision dokumentiert. Entweder wird die entsprechende Stellungnahme direkt in den Bericht der Internen Revision aufgenommen oder, insbesondere bei Dissens zu Feststellungen oder Maßnahmen, separat durch den Fachbereich dokumentiert und dem Bericht der Internen Revision beigelegt.

Der revisionsseitig unterschriebene Bericht wird dann zusammen mit der Stellungnahme an sämtliche Berichtsempfänger verteilt.

Für die weitere Behandlung des Dissenses empfiehlt es sich, ein klares Verfahren festzulegen.

Die revisionsinterne Durchsicht/Prüfung des Revisionsberichtes sowie die Abstimmungen mit der/den geprüften Einheit(en) sind zu dokumentieren; dies schließt die Nachvollziehbarkeit von Änderungen am Prüfungsbericht ein.

Die Aktualität der Prüfungsinhalte und des Prüfungsergebnisses ist durch eine zeitnahe Berichterstattung zu gewährleisten.

3.4 Berichterstattung

Die Revision fasst das Prüfungsergebnis in einem Revisionsbericht zusammen. Die Berichtsverteilung hat zur Sicherstellung der Aktualität zeitnah zu erfolgen. Dabei ist folgendes zu beachten:

- Die Qualität der Berichte ist vor Versand kompetent zu sichern.
- Berichte sind innerhalb der Revision kompetenzgerecht freizugeben.
- Prüfungsberichte werden empfängerorientiert verteilt (bevorzugt elektronisch). Bei elektronischem Versand ist der Bericht in einem hinreichend manipulationssicheren Format (z. B. gesichertes PDF) zu verteilen.
- Versand des besprochenen Berichts erfolgt gemäß Berichtsverteiler – ggf. inklusive Stellungnahme – an sämtliche Adressaten unmittelbar nach abschließender Behandlung/Schlussbesprechung.

Der Prüfungsbericht wird grundsätzlich wie folgt verteilt:

- an die geprüften Einheiten
- an die für die geprüften Einheiten verantwortlichen Mitglieder der Geschäftsleitung
- an das für die Interne Revision verantwortliche Mitglied der Geschäftsleitung sowie dessen Stellvertreter
- an Einheiten mit berechtigtem Interesse (Kontrollfunktionen)
- an den Wirtschaftsprüfer der Bank (auf Nachfrage)
- an die zuständige Aufsichtsbehörde (auf Nachfrage)

Im Fall eines mangelhaften Prüfungsergebnisses bzw. ab Feststellungskategorie „wesentlich“:

- Verteilung des Berichtes an die gesamte Geschäftsleitung

Sofern die Prüfungshandlungen schwerwiegende Mängel ergeben, informiert die Interne Revision gem. MaRisk BT 2.4 Tz. 1

- die gesamte Geschäftsleitung unverzüglich - bereits vor Abschluss der Prüfungshandlungen.

Sofern die Prüfungshandlungen besonders schwerwiegende Mängel mit existenziellem Gefährdungspotenzial für den Geschäftsbetrieb des Instituts in der Gesamtbetrachtung ergeben, informiert die Interne Revision

- umgehend die gesamte Geschäftsleitung und

- in Absprache mit dem Vorsitzenden der Geschäftsleitung ggf. den Vorsitzenden des Aufsichtsorgans (vgl. Abschnitt. 3.6.3)

Bei Nachschauprüfungen:

- Verteilung an alle Empfänger des ursprünglichen Berichtes
- bei einer unzureichenden Umsetzung des aufgezeigten Handlungsbedarfs grundsätzlich Verteilung an die gesamte Geschäftsleitung

Schwerwiegende Feststellungen gegen ein Mitglied/Mitglieder der Geschäftsleitung

- müssen unverzüglich - bereits vor Abschluss der Prüfungshandlungen – der gesamten Geschäftsleitung berichtet werden
- Die Geschäftsleitung hat den Vorsitzenden des Aufsichtsorgans sowie die Aufsichtsinstitutionen (EZB, BaFin, Bundesbank) unverzüglich zu informieren. Kommt die Geschäftsleitung der Berichtspflicht nicht nach oder beschließt keine sachgerechten Maßnahmen, so hat der Revisionsleiter den Vorsitzenden des Aufsichtsorgans zu unterrichten.

Berichte über Sonderuntersuchungen

- werden nur an einen eingeschränkten Adressatenkreis verteilt. Den Adressatenkreis sowie die Versandart legt der Leiter der Internen Revision fest. Der informierte/involvierte Personenkreis ist zu dokumentieren.

Wird nach Berichtsverteilung festgestellt, dass der Bericht wesentliche Fehler/Auslassungen enthält, so hat der Leiter der Internen Revision allen Personen, die den ursprünglichen Bericht erhalten haben, die berichtigten Informationen zu übermitteln.

3.5 Prüfungsnacharbeit

3.5.1 Pflege der (elektronischen) Dauerakte, Informationsweitergabe, administrative Tätigkeiten

Um die Prüfungsergebnisse zu belegen, müssen Informationen und Nachweise dokumentiert werden. Die für die Prüfung relevanten Analysen, Bewertungen und unterstützenden Informationen sind so zu dokumentieren, dass ein sachverständiger Dritte die Arbeit wiederholen und dieselben Prüfungsergebnisse ableiten könnte.

Die während der Prüfung erzeugten Unterlagen werden abschließend noch einmal qualitätsgesichert und die Dokumentation zur Prüfung wird auf Richtigkeit, Relevanz und Vollständigkeit überprüft. Im Rahmen dessen werden auch die für die nächste Prüfung relevante Informationen (Unterlagen, Daten, etc.) in die (elektronische) Dauerakte bzw. alternativ in das Revisionsmanagementsystem überführt. Dies sollte zeitnah zur Prüfung erfolgen. Nicht mehr benötigte Unterlagen sollten in diesem Zuge aus der (elektronischen) Dauerakte entfernt werden, um die Aktualität zu gewährleisten.

Vorkommnisse oder Besonderheiten aus der aktuellen Prüfung sollten in der (elektronischen) Dauerakte hinterlegt werden, um auf diese prüfungsspezifischen Informationen während der Vorbereitung der nächsten Prüfung direkt zugreifen zu können. Für andere Einheiten der Internen Revision relevante Informationen sollten in angemessener Weise zeitnah an diese weitergeleitet werden.

Sich aus der Prüfung ergebende Vorschläge/Ideen für die Verbesserung von Prüfungsleitfäden/Arbeitsprogrammen sollten im Anschluss an die Prüfung besprochen werden. Dabei ist auch sicherzustellen, dass bei Abschluss der Prüfung eine Überprüfung/Aktualisierung der genutzten Prüfungsleitfäden/Arbeitsprogramme auf Basis der in der Prüfung gemachten Erfahrungen erfolgt, so dass diese für spätere Prüfungen genutzt werden können. Dies ist insbesondere beim erstmaligen Einsatz eines Prüfungsleitfadens/Arbeitsprogramms von Bedeutung.

Prüfungsleiter und Prüfer sollten sich in individuellen Gesprächen persönliches Feedback bzw. Feedback im Hinblick auf die Effektivität der Vorgehensweise geben. Auch ein Feedback des Prüfungsleiters an seinen Vorgesetzten über den Verlauf der Prüfung sollte erfolgen. Die Inhalte der Feedbackgespräche zum Prüfungsabschluss sollten ebenso dokumentiert werden, wie die daraus abgeleiteten Maßnahmen zur Verbesserung der Vorgehensweise für zukünftige Prüfungen. Auch die Einholung eines Feedbacks von den geprüften Einheiten nach Abschluss der Prüfung ist empfehlenswert.

Abschließend ist eine neue Risikobewertung der geprüften Prüfobjekte dokumentiert durchzuführen. Die die Dokumentation der Prüfung ist kompetenzgerecht zu überprüfen und zu genehmigen.

3.5.2 Archivierung und Löschung von Prüfungsunterlagen

Prüfungsunterlagen müssen zeitnah nach Berichtsverteilung zur Archivierung bereit sein. Die Prüfungsunterlagen werden im Einklang mit den gesetzlichen Bestimmungen im In- und Ausland sowie den Richtlinien und Verfahren der Internen Revision und der Organisation aufbewahrt und müssen in angemessener Zeit zugänglich bzw. reproduzierbar sein. Sowohl für papierhafte Unterlagen als auch für elektronische Dateien gelten folgende Aufbewahrungsfristen:

- Arbeitsunterlagen: sechs Jahre (gem. BT 2.4 Tz. 6 MaRisk); bei Sonderuntersuchungen, beispielsweise mit Bezug zu Gerichtsurteilen, staatsanwaltschaftlichen Untersuchungen, kann eine längere Aufbewahrungsfrist notwendig sein.
- Revisionsberichte und andere verwendete Berichtsformate für Standardprüfungen bzw. Projektbegleitungen sind sechs Jahre (gem. BT 2.4 Tz. 6 MaRisk) aufzubewahren. In der Praxis empfiehlt sich eine Aufbewahrung von zehn Jahren (in Anlehnung an § 257 Abs. 4 HGB); auch hier sollte bei Sonderuntersuchungen eine längere Aufbewahrungsfrist definiert werden.
- die lokalen, gesetzlichen Aufbewahrungsfristen sind auch bei international aufgestellten Revisionseinheiten zu beachten. Sofern diese kürzer als die oben angegebenen Perioden sind, sind die jeweils längeren Fristen zu beachten (die Aufbewahrungsfristen beginnen mit Ablauf des Kalenderjahres der Prüfung).

Der endgültige Originalbericht wird archiviert. Nach Abschluss der Prüfung verbleibt das Prüfungsverzeichnis auf den File-Servern und ist dort weiterhin verfügbar. Zusätzlich werden die elektronischen Daten regelmäßig in die Langzeitsicherung überführt. Bei elektronischen Arbeitsunterlagen ist darauf zu achten, dass nach Abschluss der Prüfung systemseitig eine nachträgliche Veränderung der Dateien ausgeschlossen bzw. auf wenige Personen beschränkt und systemseitig protokolliert wird.

Mit dem Ablauf der Archivierungsfristen ist die Pflicht zur Löschung der (personenbezogenen) Daten/ Prüfungsunterlagen im Sinne der EU-DSGVO verbunden. Beachtung DSGVO/ Löschung von Daten - Daten dürfen gemäß Art. 17 Abs. 3 DSGVO i. V. m. § 24 Abs. 1 Nr. 2 BDSG grundsätzlich nur so lange aufbewahrt werden, wie diese zur Geltendmachung, Ausübung oder Abwehr von (zivil-) rechtlichen Ansprüchen benötigt werden

Die Fristen zur Archivierung und Löschung/ Vernichtung von Daten und Prüfungsunterlagen ist zu definieren. Die Vernichtung/ Löschung von Daten/ Prüfungsunterlagen ist mittels Löschprotokoll zu dokumentieren.

3.5.3 Überwachung des Handlungsbedarfs („Follow-up“)

Die aktive Nachverfolgung der Mängelbeseitigung ist in den MaRisk BT 2.5 sowie GIAS Standard 15.2 kodifiziert. In der Follow-up Phase wird die fristgerechte Umsetzung der mit den geprüften Einheiten zur Beseitigung der Mängel vereinbarten Maßnahmen angemessen überwacht und unter Anwendung eines risikoorientierten Ansatzes überprüft. Im Sinne einer Ausrichtung der Revisionsaktivitäten an den strategischen Zielen des Instituts gilt an dieser Stelle, dass sowohl die jeweilige geprüfte Einheit als auch die Interne Revision das gemeinsame Ziel verfolgen, identifizierte Risiken nachhaltig zu mitigieren. Während die Verantwortung für die Umsetzung der vereinbarten risikomitigierenden

Maßnahmen den jeweiligen Linienverantwortlichen obliegt, liegt die Verantwortung für den unabhängig durchgeführten Follow-up Prozess und die hieraus resultierende Berichterstattung in der Internen Revision. Die Interne Revision ist dabei unter anderem zuständig für die Begleitung der geprüften Einheit bei der Mängelbeseitigung durch Überwachung, Nachschauprüfung, Management-Berichterstattung der umgesetzten Maßnahmen und ggf. Eskalation bei Fristüberschreitungen, sofern daraus ein inakzeptables Risikoniveau resultiert (GIAS Standard 11.5).

Basierend auf den im Revisionsbericht vereinbarten Maßnahmen und Umsetzungsterminen überwacht die Interne Revision die fristgerechte Umsetzung des Handlungsbedarfs zur Beseitigung der Mängel. Über die Erledigung vereinbarter Maßnahmen ist die Interne Revision von den für die Mängelbeseitigung verantwortlichen Stellen entsprechend zu informieren. Die formelle Kommunikation über den Erledigungsstand wird im Idealfall durch ein IT-basiertes Follow-up System unterstützt, worauf auch die geprüften Einheiten Zugriff haben, um darin die durchgeführten Maßnahmen und den aktuellen Umsetzungsstand fristgerecht zu erfassen und an die Interne Revision zu melden.

Die Interne Revision beurteilt die sachgerechte, nachhaltige und vollständige Umsetzung der Maßnahmen. Die Beurteilung erfolgt grundsätzlich anhand der erhaltenen Unterlagen bzw. Informationen. Hierbei wird zwischen einer Angemessenheit des Designs und der Wirksamkeit (Effectiveness) unterschieden, sofern dies in der Maßnahme vereinbart wurde.

Die Art und Weise der Überwachung durch die Interne Revision sollte nach Risikogehalt der zugrundeliegenden Feststellung in Umfang und Intensität abgestuft gehandhabt werden und kann sich an der Klassifizierung von Feststellungen gemäß Abschnitt 3.3.3 orientieren. Die Ausgestaltung bzw. Intensität der Überwachungsmaßnahmen für die Beurteilung der ergriffenen Maßnahmen zur Erledigung ist risikoorientiert festzulegen und kann dabei wie folgt gehandhabt werden:

- die Beurteilung erfolgt anhand der erhaltenen Unterlagen bzw. Informationen (Validierung/Plausibilitätsprüfung), ggf. erfolgt eine inhaltliche Prüfung (z. B. auf die Wirksamkeit einer implementierten Kontrolle) im Rahmen der nächsten planmäßigen Prüfung des Prüfungsobjekts
- die Beurteilung erfolgt anhand der erhaltenen Unterlagen bzw. Informationen (Validierung/Plausibilitätsprüfung), ggf. erfolgt eine Nachschauprüfung (vor Ort) einzelner Sachverhalte bzw. in Stichproben
- es erfolgt eine zeitnahe Nachschauprüfung (vor Ort) aller relevanten Sachverhalte; bezogen auf die Beurteilung der Wirksamkeit implementierter Maßnahmen (effectiveness) ist hierbei die Berücksichtigung einer angemessenen Zeitspanne von der Erstimplementierung bis zu einer ersten betrieblichen Übung zu empfehlen, nach deren Ablauf die Wirksamkeit angemessen auf deren Nachhaltigkeit hin beurteilt werden kann

Eine zeitnahe und effiziente Umsetzung der korrigierenden Maßnahmen ist unter anderem ein wesentliches Kennzeichen eines funktionierenden Internen Kontrollsystems, deshalb sollten Terminverlängerungen grundsätzlich vermieden werden. Vielmehr sind bereits bei der Terminierung der Maßnahmen adäquate Fristen zu vereinbaren. Im Ausnahmefall sind notwendige Terminverlängerungen von der für die Mängelbeseitigung verantwortlichen Stelle frühzeitig zu beantragen und zu dokumentieren, sowie mit der Internen Revision abzustimmen, dabei ist eine unter Risikoaspekten angemessene Nachfrist zu vereinbaren. Der ursprünglich vereinbarte Erledigungstermin bleibt zwar prinzipiell erhalten, die Interne Revision berücksichtigt die vereinbarte Nachfrist jedoch bei Eskalation und Berichterstattung. In Verbindung mit Anträgen auf Terminverschiebung muss es – je nach Ausgestaltung des Risikomanagementsystems – für die beantragenden Fachbereiche erforderlich werden, die Restrisiken einem kompetenzgerechten Genehmigungsprozess zuzuführen (vgl. Abschnitt 3.5.6).

Unabhängig von der Bewertung der Feststellungen und des aktuellen Umsetzungsstandes der Maßnahmen empfiehlt es sich, die zuständige Einheit in angemessener Zeit vor Fälligkeit an den baldigen Fristablauf zu erinnern, zum Beispiel via E-Mail (sofern nicht durch das IT-basierte Follow-up-System automatisch Erinnerungen versandt werden bzw. eine selbständige Überwachung durch die zuständige Einheit ermöglicht ist).

Die Dokumentation der Mängelbeseitigung erfolgt schriftlich durch die für die Mängelbeseitigung verantwortlichen Stelle (sofern nicht durch das Follow-up-System bereits sichergestellt). Die jeweilige Feststellung kann erst nach entsprechender Validierung durch die Interne Revision geschlossen werden, sofern eine solche Validierung (ggf. auch durch Nachschauprüfung) entsprechend der o. a. Intensitätsstufe der Überwachung bzw. Beurteilung durch die Interne Revision vorgesehen ist.

Die Interne Revision gibt der für die Mängelbeseitigung verantwortlichen Stelle Rückmeldung bezüglich der Beurteilung der ergriffenen Maßnahmen und deren Umsetzungsstand. Dies gilt insbesondere für Feststellungen mit höherem Risiko, als auch grundsätzlich für den Fall, dass die Interne Revision eine sach- und zeitgemäße Umsetzung von Maßnahmen als gefährdet ansieht. In diesen Fällen initiiert das verantwortliche Management geeignete Maßnahmen zur Sicherstellung einer angemessenen Umsetzung.

3.5.3.1 Feststellungen mit langfristigem Erledigungsdatum

Feststellungen mit langfristigem Erledigungsdatum sind im Regelfall dadurch gekennzeichnet, dass ihre Umsetzung in mehreren Abschnitten erfolgt, für die jeweils einzeln abzuarbeitende Meilensteine festgelegt werden.

Bei Feststellungen mit langfristigem Erledigungsdatum sollten die oben genannten Grundsätze auf jeden einzelnen Meilenstein sinngemäß angewendet werden. Die Dokumentation der Mängelbeseitigung, Eskalation bzw. die Berichterstattung erfolgt somit einzeln mit Bezug auf den jeweils nächsten Meilenstein. Mit Erledigung eines Meilensteins wird der Termin des jeweils nächsten Meilensteins für Überwachung, Eskalation und Berichterstattung berücksichtigt. Nur die Erledigung des jeweils letzten Meilensteins führt zur Erledigung der gesamten Feststellung.

Bei diesen langfristigen Maßnahmen kann die für die Mängelbeseitigung verantwortliche Stelle alternativ auch verpflichtet werden, der Internen Revision im Turnus von max. sechs Monaten über den aktuellen Stand der Umsetzung zu berichten. Die Interne Revision behält sich dabei vor, bei einem unbefriedigenden Zwischenergebnis auch vor Ablauf des vereinbarten Umsetzungszeitpunktes, die Erledigung der Maßnahme zu eskalieren.

Bei Erledigungsfristen von mehr als zwölf Monaten empfiehlt es sich, eine temporäre Risikoübernahme (Risk Acceptance) einzuholen (vgl. Abschnitt 3.5.6) und ggf. temporär mitigierende Maßnahmen zu ergreifen.

3.5.3.2 Follow-up von Feststellungen aus Prüfungen zu Einlagerungen („In sourcing“), und der Konzernrevision

Sofern Einlagerungssachverhalte von der Internen Revision geprüft worden sind, ist den Mandanten (Auslagerer) bzw. dessen Interner Revision je nach Vereinbarung im Auslagerungsvertrag über den Status der Nachverfolgung zu berichten.

Dies gilt analog auch für Feststellungen aus Prüfungen der Konzernrevision in Tochtergesellschaften (auch im Konzerninteresse).

3.5.3.3 Nachverfolgung von Feststellungen des Jahresabschlussprüfers

Die Interne Revision sollte auch die Feststellungen des Jahresabschlussprüfers aufnehmen und einem zu Revisionsfeststellungen analogen Follow-up-Prozess unterziehen.

Mit den verantwortlichen Einheiten sind – ggf. in Abstimmung mit dem Jahresabschlussprüfer - zu den abzuarbeitenden Feststellungen geeignete Umsetzungsmaßnahmen und -termine zu vereinbaren und auf Erledigung zu überwachen. Dabei kann die Risikoklassifizierung des Jahresabschlussprüfers übernommen werden.

3.5.3.4 Behandlung anderer externer Prüfungsberichte

Die Geschäftsleitung sollte auf Vorschlag der Internen Revision festlegen, ab welcher Einstufung Feststellungen aus anderen externen Prüfungen aufzunehmen und einem zu Revisionsfeststellungen analogen Follow-up-Prozess zu unterziehen sind. In der Praxis hat sich das Nachverfolgen und Berichten von Feststellungen aus regulatorischen Prüfungen der Aufsicht bewährt. Teilweise wird dies in Begleitschreiben zu den Prüfungsberichten von der EZB (JST) oder BaFin gefordert.

3.5.4 Nachschauprüfung

Bei insgesamt mangelhaften Revisionsergebnissen (vgl. Abschnitt 3.3.3) wird die routinemäßige Überwachung der Mängelbeseitigung ggf. durch eine Nachschauprüfung unterstützt. Der Zeitpunkt und der Umfang der Nachschauprüfung kann in Abhängigkeit von der Risikobewertung der zugrundeliegenden Feststellungen individuell festgelegt werden. Die Wirksamkeitsprüfung kann auch in die nächste Regelprüfung integriert werden. Sie sollte zeitnah nach Umsetzung der wesentlichen Maßnahmen erfolgen, die im Ergebnis der Prüfungshandlungen zur Risikomitigierung vereinbart wurden, wobei ein ausreichender Zeitraum für die Etablierung in den betrieblichen Abläufen abgewartet werden sollte.

Bei Prüfungen, in denen das Gesamtergebnis der geprüften Einheit zwar nicht mangelhaft ist, aber einzelne Abteilungen/Bereiche bzw. Prozessschritte mangelhafte Revisionsergebnisse aufgewiesen haben, ist in Erwägung zu ziehen, nur für diese Teilbereiche eine Nachschauprüfung anzusetzen.

Berichte über Nachschauprüfungen mit unzureichender Umsetzung des aufgezeigten Handlungsbedarfs sollten der gesamten Geschäftsleitung vorgelegt werden.

Für den Fall, dass zu den vereinbarten Fälligkeitsterminen keine Erledigung der Maßnahmen oder eine kompetenzgerechte Terminverschiebung erfolgt ist, wird ein dem zugrundeliegenden Risiko, dem tatsächlichen Erledigungsfortschritt und der Unternehmensstruktur Rechnung tragender Eskalationsprozess angewandt. Je nach Unternehmensgröße und Risiko der Feststellung, kann bis zur gesamten Geschäftsleitung eskaliert werden. Das Eskalationsverfahren gilt analog auch für nicht akzeptierte Erledigungsmeldungen oder Stellungnahmen.

Zu beachten ist, dass gemäß BT 2.5. Tz. 2 MaRisk Vorgaben für den Fall der nicht fristgerechten Erledigung von wesentlichen Mängeln bestehen. Werden diese nicht in einer angemessenen Zeit beseitigt, so hat der Leiter der Internen Revision darüber zunächst den fachlich zuständigen Geschäftsleiter schriftlich zu informieren. Erfolgt die Mängelbeseitigung nicht, so ist die Geschäftsleitung spätestens im Rahmen des nächsten Quar-

talsberichts schriftlich über die noch nicht beseitigten Mängel zu unterrichten. Über diesen Weg der Herstellung von innerbetrieblicher Transparenz wird ein weiterer Anreiz für eine zügige Mängelbeseitigung geschaffen.

3.5.5 Management-Berichterstattung zum Umsetzungscontrolling/Follow-up

Eine effektive Management-Berichterstattung basiert auf einem flächendeckenden und aktuellen Monitoring des Umsetzungsstands der Maßnahmen.

Die Revisionsleitung informiert die Geschäftsleitung regelmäßig zeitpunkt- und zeitraumbezogen über Anzahl und Erledigungsstand aller Maßnahmen, insbesondere über wesentliche, schwerwiegende und besonders schwerwiegende Mängel (Definition gem. MaRisk) sowie mit Fokus auf Feststellungen mit hohem Risiko.

Der Jahresbericht der Internen Revision muss ebenfalls Informationen zum Stand der Mängelbeseitigung enthalten (vgl. MaRisk BT 2.4 Tz. 4).

3.5.6 Risikoübernahmen

3.5.6.1 Begriffsbestimmung

Unter Risikoübernahme („risk acceptance“) versteht man grundsätzlich die bewusste Entscheidung durch die Geschäftsleitung oder autorisierte Entscheidungsträger bzw. -gremien, von der Internen Revision identifizierte Risiken nicht oder nicht vollständig zu mitigieren.

Der GIAS Standard 15.2 führt hierzu beispielsweise aus: „Wenn das Management bei der Umsetzung der vereinbarten Maßnahmen gemäß der festgelegten Erledigungstermine keinen Fortschritt erzielt hat, müssen Interne Revisorinnen und Revisoren eine Erläuterung vom Management einholen und dokumentieren und den Sachverhalt mit der Revisionsleitung besprechen“ Des Weiteren fordert der GIAS Standard 11.5: „Wenn die Revisionsleitung zum Schluss kommt, dass das Management ein Risikoniveau akzeptiert hat, das die Risikobereitschaft oder die Risikotoleranz der Organisation übersteigt, muss dies mit der Geschäftsleitung besprochen werden.“

In der Praxis werden drei Konstellationen unterschieden:

1. Der Fachbereich entscheidet nach Veröffentlichung des Prüfungsberichtes, die Revisionsfeststellungen nicht zu beseitigen, z. B. aus Kosten-/ Nutzen-Abwägungen oder strategischen Überlegungen.

2. Im Rahmen des Follow-up-Prozesses wird festgestellt, dass der Fachbereich die vereinbarten Maßnahmen nicht erledigen kann oder aus bestimmten Gründen nicht erledigen will, z. B. aufgrund von praktischen Umständen, die einer Erledigung in angemessenem Zeitrahmen entgegenstehen, wie z. B. Veränderung von Rahmenbedingungen bei IT-Projekten, Abwägung von Kosten und Nutzen usw.
3. Bei längeren Erledigungsdauern, z. B. ab einer Überschreitung von zwölf Monaten bis zur Beseitigung des der Feststellung zugrundeliegenden Risikos (initial oder bei einer Terminverlängerung), sollte eine temporäre Risikoübernahme erfolgen.

In allen drei Fällen sollte die Risk Acceptance durch den Fachbereich beantragt werden. Die Interne Revision beurteilt, ob die Vorlage des Fachbereiches sachgerecht ist und insbesondere die mit der Risikoübernahme verbundenen Risiken zutreffend darstellt. Sodann ist eine kompetenzgerechte Entscheidung zur Risikoübernahme zu treffen. Dabei ist eine, in Abhängigkeit der Mängelschwere(-kategorie), abgestufte Vorgehensweise denkbar (Kompetenzordnung). Z. B. könnte bei geringen Mängeln eine Risikoübernahme durch eine Leitungsebene unterhalb der Geschäftsleitung ausreichend sein. Ab der Stufe bemerkenswert sollte zumindest das ressortzuständige Geschäftsleitungsmitglied entscheiden. Bei wesentlichen Mängeln ist die Entscheidung von der gesamten Geschäftsleitung zu treffen. Wird das Risiko akzeptiert, kann die Feststellung mit entsprechendem Status aus dem Follow-up herausgenommen werden bzw., bei einer temporären Risikoübernahme, der entsprechende Erledigungstermin eingetragen werden.

Dieser Prozess muss mit der Geschäftsleitung abgestimmt werden und sollte im Sinne einer Förderung der Akzeptanz der Internen Revision in der Organisation auch als Bestandteil der schriftlich fixierten Ordnung kommuniziert werden.

Über Risikoübernahmen sollte im Rahmen der Quartalsberichterstattung berichtet werden. Des Weiteren sollte der Sachverhalt an die für das Management der operationellen Risiken zuständigen Organisationseinheit weitergeleitet werden und dort überwacht werden. Darüber hinaus sollten die Rahmenbedingungen der jeweiligen Risikoübernahmen im Rahmen von Folgeprüfungen erneut beurteilt werden.

3.6 Gremienberichterstattung

3.6.1 Überblick

Die Pflichten zur Berichterstattung an Geschäftsleitung und Aufsichtsorgan ergeben sich aus § 25c KWG sowie den MaRisk. Hierunter fallen die Quartalsberichterstattung, der Jahresbericht sowie ggf. die Ad-hoc-Berichte. Abb. 7 gibt einen Überblick zu den Berichtsarten und den Rechtsgrundlagen.

Berichtsart	Adressat	Rechtsgrundlage
Quartalsbericht/ Jahresbericht	Geschäftsleitung	§ 25c Abs. 4a Nummer 3 lit. g KWG bzw. § 25c Abs. 4b Nummer 3 lit. g KWG für Institutgruppen/ BT 2.4 Tz. 4 MaRisk
Quartalsbericht/ Jahresbericht	Aufsichtsorgan	§ 25c Abs. 4a Nummer 3 lit. g KWG bzw. § 25c Abs. 4b Nummer 3 lit. g KWG für Institutgruppen/ BT 2.4 Tz. 4 MaRisk
Ad-hoc Berichtspflicht	Geschäftsleitung	BT 2.4 Tz. 5 MaRisk
Ad-hoc Berichtspflicht	Aufsichtsorgan	BT 2.4 Tz. 5 MaRisk

Abb. 7: Berichtspflichten der Internen Revision und rechtliche Grundlagen

Darüber hinaus werden in den GIAS (Standards 8.1, 11.3 und 11.5) die Berichtspflichten der Internen Revision gegenüber der Geschäftsleitung und dem Überwachungsorgan geregelt.

3.6.2 Quartals-/ Jahresbericht

3.6.2.1 Quartalsberichterstattung

Die Anforderungen an die Quartalsberichterstattung und den Jahresbericht werden in § 25c Abs. 4a Nr. 3. lit. g) KWG und BT 2.4 Tz. 4 MaRisk spezifiziert. Die MaRisk bilden das deutsche dualistische System ab, in dem sie keine Differenzierung der Informationsinhalte für Geschäftsleitung und Aufsichtsorgan (alternativ Delegation an den Prüfungsausschuss) vornehmen. Dieses trägt auch dazu bei, das Vertrauensverhältnis zur Geschäftsleitung nicht zu belasten und Informationsasymmetrien vorzubeugen.

Empfehlenswert ist, noch einen Schritt weiterzugehen und aktiv mit der Geschäftsleitung Themen, die darüber hinaus Gegenstand der Berichterstattung sein sollen, abzustimmen und den Bericht adressatenorientiert auszugestalten. Hierdurch darf die Unabhängigkeit der Internen Revision jedoch nicht beeinträchtigt werden.

Die Quartalsberichterstattung hat zeitnah nach dem jeweiligen Stichtag zu erfolgen. In der Praxis erscheint eine Frist von 6 Wochen als angemessen.

Pflichtbestandteile der Berichterstattung

Die Pflichtbestandteile der Berichterstattung leiten sich aus den MaRisk (u. a. BT 2.4 Tz. 4 MaRisk) ab: unterjährige Abweichungen und Änderungen vom Jahresprüfungsplan bzw. Erfüllung des Jahresplans am Jahresende, wesentliche und schwerwiegende Feststellungen aus den Revisionsaktivitäten, diesbezüglich ergriffene Maßnahmen sowie deren Umsetzungsstand. Zu den Feststellungen zählen auch die im Rahmen eines Auslagerungsverhältnisses von einer anderweitig durchgeführten Prüfungstätigkeit getroffenen Feststellungen. Auf deren Aufnahme kann verzichtet werden, wenn diese Feststellungen bereits in anderen Berichten – beispielsweise in der Risikoberichterstattung – enthalten sind.

Bestandteile der Berichterstattung gem. MaRisk

Übersicht über die durchgeführten Prüfungen der Berichtsperiode, ggf. Nennung berichtenswerter Prüfungsergebnisse

Wesentliche unterjährige Abweichungen und Änderungen vom Jahresplan bzw. Erfüllung des Jahresplanes insgesamt am Jahresende

Festgestellte als wesentlich und höher eingestufte Mängel und beschlossene Maßnahmen. Schwerwiegende Mängel sind besonders hervorzuheben. *

Umsetzungsstand zu Feststellungen ab der Einstufung wesentlich **

* auch der anderweitig durchgeführten Internen Revision von Auslagerungsunternehmen, sofern nicht bereits in anderer Berichterstattung – z. B. Berichterstattung der Risikomanagementfunktion – enthalten

** Ergänzend hierzu sei auf MaRisk BT 2.5 Tz. 2 hingewiesen:

Hiernach gilt, dass bei wesentlichen Mängeln, die nicht in einer angemessenen Zeit beseitigt werden, der Leiter der Internen Revision zunächst den fachlich zuständigen Geschäftsleiter schriftlich zu informieren hat. Erfolgt die Mängelbeseitigung nicht, so ist die Geschäftsleitung spätestens im Rahmen des nächsten Gesamtberichts [Quartalsberichts] schriftlich über die noch nicht beseitigten Mängel zu unterrichten.

Abb. 8: Bestandteile der Berichterstattung an Geschäftsleitung und Aufsichtsorgan gemäß § 25c KWG in Verbindung mit BT 2.4 Tz 4 MaRisk

Weitere mögliche Berichtsinhalte

Auch wesentliche Informationen zur Internen Revision selbst (z. B. über Änderungen der Aufbau- und Ablauforganisation, neue regulatorische Anforderungen an die Interne Revision, Ressourcenausstattung, Beurteilung der Internen Revision durch Externe beispielsweise im Rahmen eines Quality Assessments oder über das Qualitätssicherungssystem der Internen Revision) sowie wesentliche unterjährige Aktivitäten der Internen Revision (z. B. auch Beratung, Begleitung von Projekten und aufsichtsrechtlichen Prüfungen) sind aus Best Practice Gesichtspunkten sinnvolle Informationen, damit Geschäftsleitung und

Aufsichtsorgan ihrer Leitungs- bzw. Überwachungsfunktion nachkommen können. Diese Informationen sollten daher in die Berichterstattung aufgenommen werden. Sofern unterjährig interne Qualitätssicherungsmaßnahmen vorgenommen wurden und kritische Erkenntnisse ergaben, sollte aus Transparenzgründen ebenfalls darüber berichtet werden.

Weitere empfohlene Bestandteile der vierteljährlichen Berichterstattung sind Informationen über wesentliche Prüfungen externer Prüfer wie beispielsweise Wirtschaftsprüfer, EZB, BaFin bzw. Deutsche Bundesbank sowie die dort getroffenen wesentlichen und schwerwiegenden Feststellungen und die ergriffenen Maßnahmen zu deren Beseitigung sowie regelmäßig der Erledigungsstand dieser Feststellungen.

Je nach Informationsbedürfnis der Berichtsempfänger sind auch weitere Themen denkbar. Als Best Practices bieten sich an:

Weitere mögliche Berichtsinhalte

Auftrag/Ziele der Internen Revision

Darstellung der Prüfungsschwerpunkte

Aussage zur Unabhängigkeit oder zu evtl. Beschränkungen des Prüfungsumfangs

Wesentliche Aktivitäten der Internen Revision (z. B. Beratung, Begleitung von Projekten und aufsichtsrechtlichen Prüfungen)

Wesentliche Informationen zur Internen Revision selbst (z. B. Änderungen in Aufbau- und/oder Ablauforganisation, neue regulatorische Anforderungen an die Interne Revision, Ressourcenausstattung, Beurteilung der Internen Revision durch Externe, Bericht über das Qualitätssicherungssystem der Internen Revision, Angaben zur Unabhängigkeit, Angaben zu ausgelagerten Prüfungen oder zu Beauftragungen Dritter)

Revisionsstatistiken (z. B. zu offenen/erledigten Feststellungen oder Erledigungsdauern)

Feststellungen externer Prüfer sowie ergriffene Maßnahmen

Umsetzungsstand zu berichteten Feststellungen externer Prüfer

Eine Beurteilung zur Wirksamkeit des Internen Kontrollsystems bzw. der Risikolage des Instituts auf Basis der durchgeführten Prüfungen oder des Continuous Monitoring

Beurteilung der „1st Line“

Beurteilung der „2nd Line“

Wesentliche Verluste und Schäden

Glossar

Abb. 9: Weitere mögliche Berichtsinhalte für die Quartalsberichterstattung

3.6.2.2 Jahresberichterstattung

Gemäß BT 2.4 Tz. 4 MaRisk hat die Interne Revision zeitnah einen Gesamtbericht über die von ihr im Laufe des Geschäftsjahres durchgeführten Prüfungen zu verfassen und der Geschäftsleitung und dem Aufsichtsorgan vorzulegen. Durch diesen Jahresbericht sollen die Geschäftsleitung und das Aufsichtsorgan bei der Wahrnehmung ihrer Aufgaben unterstützt werden. Dies erfordert eine sachgerechte und inhaltlich prägnante Darstellung risikorelevanter Ereignisse.

Eine Differenzierung der Jahresberichterstattung an Geschäftsleitung und Aufsichtsorgan erfolgt nicht.

Die Jahresberichterstattung sollte vor der ersten Sitzung des Aufsichtsorgans finalisiert und in der Geschäftsleitung befasst worden sein.

Der Quartalsbericht zum 31.12. und der Jahresbericht können nach BT 2.4. Tz. 4 MaRisk auch als jeweils gesonderte Abschnitte in einem Bericht zusammengefasst werden. Hierzu müssen folglich alle nach BT 2.4 Tz. 4 MaRisk vorgeschriebene Bestandteile enthalten sein.

Die Jahresberichterstattung an die Geschäftsleitung hat zeitnah zu erfolgen. In der Praxis erscheint hier eine Frist von sechs Wochen als angemessen. Die Berichterstattung an das Aufsichtsorgan sollte in der ersten Sitzung des Jahres erfolgen.

Pflichtbestandteile der Berichterstattung:

Der Gesamtbericht muss in Bezug auf das Berichtsjahr mindestens zu folgenden Themen informieren:

- festgestellte schwerwiegende und nicht behobene wesentliche Mängel
- ergriffene Maßnahmen hierzu
- den Status der Abarbeitung der Maßnahmen zu den schwerwiegenden Mängeln

Die Interne Revision kann im Jahresbericht Akzente setzen, indem sie einzelne Feststellungen hervorhebt und den Status von deren Abarbeitung darstellt oder bestimmte Aspekte ihrer Tätigkeit betont. Auch müssen die Feststellungen und deren Umsetzungsstand nicht einzeln dargestellt werden, sondern können – sofern sie inhaltlich gleichartig sind – zusammengefasst und somit die Situation als Ganzes dargestellt werden. Es muss jedoch sichergestellt sein, dass die gewählte Darstellungsweise alle von den MaRisk geforderten Berichtselemente beinhaltet. Folglich ist der Jahresbericht nicht eine reine Auflistung von einzelnen wesentlichen Feststellungen des Jahres, sondern für die Interne Revision auch ein Instrument, den Nutzen ihrer Tätigkeit darzulegen.

Weitere mögliche Berichtsinhalte

Je nach Informationsbedürfnis der Berichtsempfänger sind auch in der Jahresberichterstattung weitere Themen denkbar. Diesbezüglich verweisen wir auf unsere Ausführungen im Kapitel 3.6.2.1 Quartalsberichterstattung.

Vor dem Hintergrund der Anforderungen aus den GIASan eine Revisionsstrategie (GIAS Standard 9.2) und die Leistungsmessung (GIAS Standard 12.2) kann es auch eine Option sein, hierzu ein Kapitel in die Jahresberichterstattung aufzunehmen. Die in den Standards explizit geforderte Erörterung mit dem Aufsichtsorgan könnte dann über die Präsentation der Jahresberichterstattung im Aufsichtsorgan erfolgen.

Die in den GIAS (Standard 11.3) geforderte Analyse von Feststellungen und Gesamturteile über die Gesamtheit der Aufträge im Hinblick auf eine ganzheitliche Erkennung und Betrachtung von Mustern oder Trends (z. B. Grundursachen) wäre ebenfalls im Kontext der Jahresberichterstattung vorstellbar.

3.6.3 Ad-hoc-Berichtspflichten

Über besonders schwerwiegende Mängel hat die Interne Revision unverzüglich zu berichten (BT 2.4 Tz. 4 MaRisk).

Eine weitere ad hoc-Berichtspflicht folgt aus BT 2.4 Tz. 5 MaRisk. Sie kommt zum Tragen, wenn sich im Rahmen der Prüfungen schwerwiegende Feststellungen gegen Geschäftsleiter ergeben. In diesem Fall hat die Geschäftsleitung eine Berichtspflicht gegenüber dem Vorsitzenden des Aufsichtsorgans sowie den Aufsichtsinstitutionen (EZB, BaFin, Bundesbank). Sofern die Geschäftsleitung dieser Berichtspflicht nicht nachkommt oder die Geschäftsleitung diesbezüglich keine sachgerechten Maßnahmen ergreift, hat die Interne Revision ad hoc den Vorsitzenden des Aufsichtsorganes darüber zu unterrichten. Dies wird nur bei gesellschaftsrechtlich oder strafrechtlich relevanten Sachverhalten oder bei Vorgängen von besonderer aufsichtsrechtlicher Bedeutung der Fall sein.

Aus dem (GIAS Standard 11.5 ergibt sich eine weitere ad hoc-Kommunikationspflicht der Revisionsleitung. Sie kommt dann zum Tragen, wenn die Revisionsleitung auf Grund von Prüfungsergebnissen oder auf Grund der Abarbeitung der Feststellungen der Ansicht ist, dass das Management ein Risikoniveau akzeptiert hat, das die Risikobereitschaft oder die Risikotoleranz der Organisation übersteigt. Wenngleich dies nicht explizit gefordert ist, bietet es sich zur Objektivierung dieser Einschätzung an, vorab Kriterien zu definieren und zur Dokumentation die Kommunikation schriftlich vorzunehmen.

Zusammenfassende Übersicht

Mangel	nicht-wesentlich (geringfügig/bemerkenswert)	wesentlich	schwerwiegend	besonders schwerwiegend
Quartalsbericht	Über die durchgeführten Prüfungen ist zu berichten	Wesentlich oder höher eingestufte Mängel, die beschlossenen Maßnahmen sowie den Status dieser Maßnahmen (Gleichartige Einzelfeststellungen sowie der Stand der Maßnahmen können inhaltlich zusammengefasst werden. Der Bericht ist zeitnah der Geschäftsleitung und dem Aufsichtsorgan vorzulegen (Berichterstattung an Aufsichtsorgan kann auch über Geschäftsleitung erfolgen, wenn keine nennenswerte Verzögerung entsteht und Inhalt deckungsgleich ist.).		
Jahresbericht	Über die durchgeführten Prüfungen ist zu berichten	nicht behobene wesentliche noch Mängel	Alle schwerwiegenden Mängel, beschlossene Maßnahmen sowie der Status dieser Maßnahmen sind besonders hervorzuheben.	
Ad-hoc			Bei schwerwiegenden Feststellungen gegen Geschäftsleiter, ist der Geschäftsleitung unverzüglich Bericht zu erstatten Die Geschäftsleitung hat unverzüglich den Vorsitzenden des Aufsichtsorgans sowie die Aufsichtsinstitutionen (BaFin, Bundesbank) zu informieren. Kommt die Geschäftsleitung ihrer Berichtspflicht nicht nach oder beschließt sie keine sachgerechten Maßnahmen, so hat die Interne Revision den Vorsitzenden des Aufsichtsorgans zu unterrichten.	Die Interne Revision hat unverzüglich an die Geschäftsleitung und das Aufsichtsorgan zu berichten.

Abb. 10: Zusammenfassende Übersicht der Berichtspflichten

4 Begleitung wesentlicher Projekte

Gemäß BT 2.1 Tz. 2 MaRisk hat die Interne Revision unter Wahrung ihrer Unabhängigkeit und unter Vermeidung von Interessenkonflikten bei wesentlichen Projekten begleitend tätig zu sein.

Mögliche Beispiele für Themenstellungen sind größere IT-Migrationsprojekte, Projekte zur Umsetzung von bedeutenden aufsichtsrechtlichen/gesetzlichen Vorgaben, Auslagerungsprojekte, Projekte zur Abstellung von wesentlichen oder höher eingestuftten Feststellungen oder auch umfangreichere Bauprojekte.

Zur Identifizierung „wesentlicher Projekte“ ist Voraussetzung, dass die Interne Revision auf der Basis eines etablierten Prozesses von neuen und geplanten Projekten bzw. Vorhaben (außerhalb von Linienaktivitäten, z. B. Task Forces) Kenntnis erlangt. Dabei sollte die Interne Revision idealerweise auf den Prozessen des Projekt- bzw. Portfoliomanagements der Bank aufbauen. Auf Basis einheitlich festzulegender Kriterien sind die so identifizierten Projekte von der Internen Revision dahingehend zu beurteilen, ob sie für diese „wesentlich“ sind. Dabei können quantitative, qualitative Verfahren sowie Mischformen zur Anwendung kommen. Als mögliche Kriterien zur Bestimmung der Wesentlichkeit von Projekten kommen u. a. folgende Merkmale von Projekten in Betracht:

- Quantitative Merkmale
 - das Projektbudget (EUR oder Personentage)
 - das Neuinvestitionsvolumen eines Projekts (EUR)
 - die aus einem Projekt resultierenden laufenden Kosten (EUR) und/oder Aufwände (Personentage)
 - die Quote externer Ressourcen im Projekt (%)
- Qualitative Merkmale
 - die Auswirkungen der Projektumsetzung auf den Unternehmenserfolg/ die Unternehmensstrategie
 - die Auswirkungen der Projektumsetzung auf das Risikomanagement oder das Kontrollgefüge des Instituts
 - die regulatorische Relevanz der Projekthinhalte
 - die fachliche/organisatorische Komplexität der Projektumsetzung (als Indikation kann bspw. die Anzahl involvierter Fachbereiche dienen)
 - Auswirkungen auf Kunden.

Als „wesentlich“ eingestufte Projekte sind durch die Interne Revision (auch unterjährig) in die Kapazitätsplanung einzubeziehen. Zur Abdeckung der notwendigen Ressourcen kann ggf. auf die nach MaRisk gebildete Planreserve oder einen separat gebildeten Kapazitätspuffer zurückgegriffen werden, soweit Projekte im Zuge der Jahresplanung noch keine Berücksichtigung gefunden haben. Zumindest einmal jährlich sollte die Interne Revision die Projekteinstufung überprüfen.

Die Art der revisorischen Tätigkeiten kann durch die Interne Revision grundsätzlich risikoorientiert festgelegt werden - abhängig von Art und Umfang des zu betrachtenden Projekts, von dem seitens der Internen Revision verfolgten Ziel bzw. in Abhängigkeit von der Projektphase -:

- Informatorische Einbindung in ein Projekt bzw. Vorhaben (= informatorische Projektbegleitung) über die regelmäßige Bereitstellung von Projektdokumentationen/ Protokollen/ als nicht stimmberechtigtes Mitglied von Projektgremien
 - Ziel: Informationsgewinnung
- Beratende Einbindung in ein Projekt bzw. Vorhaben, z. B. im Rahmen regelmäßiger Jour Fixe mit Projektorganen bzw. durch schriftliche Stellungnahmen (siehe dazu auch Kapitel 3.8). Dabei ist über Verfahren sicher zu stellen, dass die prozessuale und personelle Unabhängigkeit der Revision nicht gefährdet wird (vgl. Abschnitt 1.4)
 - Ziel: Beratung des Projekts z. B. hinsichtlich Auswirkungen auf das Interne Kontrollsystem, Ausgestaltung des Projektmanagements
- Projektbezogene Prüfung eines Projekts bzw. Vorhabens. Die Prüfung eines Projektes kann auf die Beurteilung einzelner thematischer oder zeitlicher Abschnitte eines Projekts fokussieren oder das Projekt bzw. Vorhaben im Gesamtverlauf zum Gegenstand haben. Sie schließt mit einer Berichterstattung analog zu anderen Prüfungen der Internen Revision ab.
 - Ziel: Beurteilung des Prüfungsgegenstands, Ausgestaltung des Projektmanagements

Gegenstand projektbezogener Prüfungen können gemäß dem DIIR-Standard Nr. 4 „Prüfung von Projekten durch die Interne Revision“

- der Business Case des Projekts,
- das Projekt- und Portfoliomanagement oder/und
- die ordnungsgemäße Umsetzung der inhaltlichen fachlichen und/ oder technischen Anforderungen.

sein.

Die Prüfung des Business Case eines Projekts knüpft an das strategische oder finanzielle Zielbild an, für dessen Erreichung das Projekt initiiert wurde. Durch die Beurteilung der dem Business Case zugrunde gelegten Analysen, Gutachten, Berechnungen und Entscheidungen kann die Interne Revision im Wege einer Aussage über die Belastbarkeit getroffener Annahmen und relevanter Entscheidungsgründe einen Mehrwert schaffen.

Eine Prüfung des Projekt- und Portfoliomanagements umfasst insbesondere die Beurteilung der Einhaltung der durch das Institut definierten Projektmanagementstandards und Vorgehensmodelle (z. B. Wasserfallmodell, agile Methoden, hybride Formen). Hierunter fallen:

- die Projektorganisation, z. B. Einrichtung von Gremien, Aufgaben/ Rolle der Projektbeteiligten sowie eines Projektmanagement-Office
- die etablierten projektinternen Prozesse, z. B. Projektrisikomanagement, Budgetüberwachung, Entscheidungs-/ Qualitätssicherungsprozesse, Kommunikationswege und Berichterstattung, Eskalationswege sowie
- die zeitliche, personelle und inhaltliche Projektplanung, Inhalt- und Umfangmanagement, z. B. Meilensteinplanung, Product Backlog, Sprint-Planning, Identifizierung kritischer Pfade, Berücksichtigung von Change Requests.

Durch ihre Prüfungshandlungen trägt die Interne Revision dazu bei, die Ordnungsmäßigkeit des Projektvorgehens und damit die Einhaltung des für das Institut definierten Qualitätsniveaus sowie der zeitlichen Restriktionen zu unterstützen und dadurch die Wahrscheinlichkeit zu erhöhen, dass das Projektziel erreicht wird.

Die bei der Erreichung des Projektziels zu erfüllenden technischen/ fachlichen Anforderungen können Gegenstand einer inhaltlich orientierten Prüfung der Umsetzung bestehender Anforderungen sein. Hierbei werden die Projektergebnisse dahingehend beurteilt, ob sie die internen und externen Vorgaben erfüllen und das im Business Case definierte Zielniveau erreichen. Folgende Prüfthemen können Gegenstand der Prüfung sein:

- Abgleich des Anforderungskonzepts (ursprüngliche fachliche Anforderungen) mit dem Projektauftrag
- Abgleich der Zwischen- und Endergebnisse mit dem Anforderungskonzept
- Fach- und projektspezifischen Qualitätskriterien für Zwischen- und Endergebnisse, wobei die Qualitätskriterien sowohl selbst geprüft werden, im Hinblick darauf, ob sie geeignet sind die Qualität der Projektergebnisse zu messen, als auch Maßstab dahingehend sind, ob die Projektergebnisse die Qualitätskriterien erfüllen

Um zu gewährleisten, dass durch die Prüfung ein erkennbarer Mehrwert durch die Interne Revision geschaffen wird, sollten bei der Prüfungsplanung sowohl die inhaltliche

Ausgestaltung der Prüfung als auch deren Zeitpunkt in den Kontext der Projektphasen gestellt werden. So führen beispielsweise die Prüfung des Business Case des Projekts oder die Beurteilung der Projektorganisation mit zunehmendem inhaltlichem und zeitlichem Fortschritt des Projekts zu einem eher abnehmenden Zusatznutzen. Eine inhaltliche Prüfung fachlicher Konzeptionen trägt umso mehr zum Erfolg des Projektes bei, je näher sie an der eigentlichen Konzeption und zeitlich vor der technischen Umsetzung oder dem Testing liegt. Insbesondere in agil organisierten Projekten besteht aufgrund des inkrementellen Vorgehens die Herausforderung, den Impuls aus der projektbegleitenden Prüfung zum richtigen Zeitpunkt zu setzen.

Dabei gilt es den Prüfungsansatz dahingehend auszurichten, ob es sich um ein Projekt gem. Wasserfallprinzip, um ein agiles Projekt oder eine Mischform handelt. Bei der Prüfung von Projekten im Wasserfallprinzip konzentriert sich die Prüfung auf den klassischen Ablaufplan mit den Projektphasen Start, Planung, Durchführung, Überwachung und Abschluss. Bei der Prüfung von agilen Projekten ist das Kernelement, das im Projektverlauf zunächst „unfertige“ Produkte geliefert werden, die dann durch Kundenfeedback sukzessive bis zum Erreichen des Projektziels verbessert werden, womit dem Integrationsmanagement und dem Qualitätsmanagement eine hohe Bedeutung zukommt. Wesentliche Projektmanagementmethoden sind dabei Scrum, Kanban und Design Thinking. Bei hybriden Formen werden die Vorteile beider oben genannten Formen miteinander kombiniert.

Soweit das Institut über eine eigenständige 2nd-line-Funktion zum Projekt(portfolio)management verfügt, sind auch deren Aktivitäten in das Prüfungsuniversum der Internen Revision zu integrieren. Bei der Planung und Durchführung projektbezogener Prüfungen können die in Bezug auf die 2nd-line-Funktion gewonnen Prüfungsergebnisse verwendet werden. Die dezentral in den Prüfungen der Projekte gewonnen Erkenntnisse sollten im Gegenzug auch in der 2nd-line Prüfung Eingang finden.

Die revisorische Behandlung von Projekten stellt besondere Anforderungen an die Kenntnisse und Fähigkeiten der Beteiligten. Neben den erforderlichen fachspezifischen Kenntnissen zur Beurteilung des Projektgegenstands werden vertiefte Kenntnisse des Projektmanagements benötigt. In persönlicher Hinsicht bedingen die teilweise nebeneinander verwendeten Projektmanagementmethoden (z. B. Wasserfall vs. agil, hybride Formen) ein zunehmend hohes Maß an Flexibilität und Offenheit des Prüfenden, um die mit den Projektmanagementmethoden verbundenen Grundeinstellungen (stark planender, hierarchischer Ansatz vs. eher dezentraler, kollaborativer Ansatz) bei der revisorischen Analyse und der Beurteilung deren Ergebnisse angemessen zu berücksichtigen.

Für weitere Details hinsichtlich der Begleitung und Prüfung von Projekten sei auf den Prüfungsstandard Nr. 4 des DIIR verwiesen.

Quellen und Vertiefungen

DIIR-Prüfungsstandard Nr. 4: Standard zur Prüfung von Projekten (Version 3.0, September 2019).

DIIR-Schriftenreihe Nr. 45: Leitfaden zur Prüfung von Projekten – Erläuterungen und Empfehlungen zum DIIR Standard Nr. 4 (September 2010).

Institut der Wirtschaftsprüfer in Deutschland e.V.: IDW PS 850: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie.

5 Einbindung der Internen Revision in die Anpassungsprozesse gem. AT 8 MaRisk

Die Interne Revision ist in die in AT 8 MaRisk geregelten Anpassungsprozesse „im Rahmen ihrer Aufgaben“ einzubinden.

Dies betrifft:

- die Aufnahme von Geschäftsaktivitäten in neuen Produkten und auf neuen Märkten – „Neu-Produkt-Prozess“ (AT 8.1 MaRisk)
- „Änderungen betrieblicher Prozesse und Strukturen“ (AT 8.2 MaRisk)

Die Bezugnahme auf die Aufgaben der Internen Revision stellt insbesondere auf die Unabhängigkeit der Internen Revision ab. Die Rolle der Internen Revision ist dabei als beratende bzw. begleitende Funktion zu sehen. Die Einbindung der Interne Revision ist nachvollziehbar zu dokumentieren. Eine Stellungnahme ist in dem Prozess nicht zwingend erforderlich, kann aber je nach Ausgestaltung des Prozesses an geeigneter Stelle sinnvoll sein.

Gleichsam kann die Einbindung durch die Interne Revision dazu genutzt werden, um Erkenntnisse über kurz- sowie langfristige Veränderungen zu erlangen und hieraus Rückschlüsse für die (unterjährige) Prüfungsplanung und fachliche Schwerpunktsetzungen in Prüfungen sowie evtl. Veränderungen des Prüfungsuniversums abzuleiten. Dabei sind die Neu-Produkt-Prozesse und Anpassungsprozesse selbst als Prüfungsgegenstand in das Prüfungsuniversum der Internen Revision zu integrieren.

5.1 AT 8.1 Neu-Produkt-Prozess

Jedes Institut muss die von ihm betriebenen Geschäftsaktivitäten verstehen. Für die Aufnahme von Geschäftsaktivitäten in neuen Produkten oder auf neuen Märkten (einschließlich neuer Vertriebswege) ist vorab ein Konzept auszuarbeiten. Grundlage des Konzeptes muss das Ergebnis der Analyse des Risikogehalts dieser neuen Geschäftsaktivitäten und den betroffenen Prozessen und Kontrollen sowie deren Auswirkungen auf das Gesamtrisikoprofil sein. In dem Konzept sind u.a. die sich daraus ergebenden wesentlichen Konsequenzen für das Management unter Berücksichtigung der Risiken darzustellen.

Sowohl in die Erstellung des Konzeptes als auch in die Testphase sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion sowie die Interne Revision als unabhängige Instanz zu beteiligen. Die Anforderungen der MaRisk

sollten die Institute in einer entsprechenden Richtlinie konkretisieren, die als Arbeitsanweisung für den Neu-Produkt-Prozess dienen kann.

Da die Interne Revision als Instrument der Geschäftsleitung für die prozessunabhängige Überprüfung des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen zuständig ist, sollte sie nur insoweit eingebunden werden, wie ihre Unabhängigkeit sichergestellt bleibt (Vgl. AT 4.4.3 Tz. 3 MaRisk).

Aufgabe der Internen Revision in diesem Prozess ist vor allem auf die Einhaltung der regulatorischen und gesetzlichen Anforderungen sowie auf die Einhaltung der in der Richtlinie festgelegten Prozessschritte zu achten. Eine Einbindung der Internen Revision von Anfang bis Ende des gesamten Prozesses ist sinnvoll, um nicht nur eine vollständige Information während des Einführungsprozesses zu erhalten, sondern auch um diese Informationen für künftige Prüfungen nutzen zu können und so die jeweiligen „Rüstzeiten“ in den relevanten Prüfungen zu verringern.

5.2 AT 8.2 Änderungen betrieblicher Prozesse oder Strukturen

Jedes deutsche Kreditinstitut hat gemäß AT 8.2 MaRisk sicherzustellen, dass vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität (Internes Kontrollsystem - IKS) analysiert werden.

Relevante Änderungen können die folgenden Themen betreffen:

- Aufbauorganisation (Reorganisation von Bereichen und Abteilungen)
- Ablauforganisation (z. B. Änderungen von Prozessen in Art und Umfang, Reihenfolge von Prozessschritten, Änderung von Zuständigkeiten und Schnittstellen)
- Aufgabenzuschnitten inkl. der Berichtslinien und der Besetzung
- IT-Systeme/Anwendungen (z. B. Neueinführung von IT-Systemen, Release-Wechsel, Migrationen)

Zur Umsetzung empfiehlt es sich einen angemessenen Prozess, evtl. mit einer Evidenzzentrale, einzurichten. Dabei ist zu festzulegen, ob der Prozess lediglich Veränderungen unterhalb der Projektschwelle (klare Abgrenzung erforderlich) betrachtet oder ob auch Veränderungen, die in (wesentlichen) Projekten umgesetzt werden sollen, einbezogen werden.

Zur Bewertung der Veränderungen im Hinblick auf die Wesentlichkeit sind objektive Kriterien festzulegen. Die Einstufung der betreffenden Veränderungen nach diesen Kriterien sollte durch die Fachbereiche vorgenommen werden.

In die Auswirkungsanalyse sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzubeziehen. Im Rahmen ihrer Aufgaben sind gemäß AT 8.2 MaRisk zudem die Risikocontrolling-Funktion, die Compliance-Funktion sowie die Interne Revision zu beteiligen. Die entsprechende Information sollte bereits zu Beginn der Auswirkungsanalyse erfolgen.

Ziel der Einbindung der Internen Revision ist die Schaffung von Mehrwert in Bezug auf die durch das Unternehmen geplanten Veränderungen. Dieser Mehrwert kann u. a. durch Hinweise auf die notwendige Einbindung von bisher nicht am Veränderungsprozess beteiligten Einheiten, durch Anmerkungen zum Kontrollgefüge (z. B. bei geplanten „Workarounds“) oder durch eine Rückmeldung zur technischen/ fachlichen Umsetzung geschaffen werden. Die Einbindung der Internen Revision sollte durch diese auch genutzt werden, ggf. um frühzeitig auf Fehler oder auch Ineffizienzen hinzuweisen (beratende unabhängige Revision).

Daneben kann die Interne Revision die erhaltenen Informationen bei der regelmäßigen Überprüfung der Prüfungsplanung verwenden und bei Bedarf Anpassungen vornehmen.

5.3 AT 8.3 Übernahmen und Fusionen

Hier wird die Interne Revision im Gegensatz zu AT 8.1 MaRisk und AT 8.2 MaRisk nicht explizit erwähnt, so dass es den einzelnen Instituten obliegt, entsprechende Anforderungen hinsichtlich der Einbindung der Internen Revision zu definieren. Jedoch sollte die Kenntnisnahme über wesentlichen Änderungen der Konzernstruktur in jedem Fall sichergestellt werden.

6 Beratung

6.1 Veränderungen und Herausforderungen der Revisionstätigkeit

Das Risiko- und Chancenmanagement von Kreditinstituten unterliegt einem permanenten Wandel mit steigender Dynamik, stetig veränderten Unternehmensrisiken sowie wachsenden aufsichtsrechtlichen Anforderungen. Die daraus resultierende Komplexität stellt immer höhere Anforderungen an die Entscheidungsträger. Damit verbunden ist eine zunehmende Nachfrage nach Beratungsleistungen der Internen Revision. Der Internen Revision kommt dabei das Alleinstellungsmerkmal zu, eine unabhängige, konzeptionelle Gesamtsicht des Unternehmens in die Beratung einfließen lassen zu können, da sie von der operativen Arbeitsteilung und Aufgabenspezialisierung sowie von der Tagesgeschäft orientierten Entscheidungsfindung losgelöst ist. Die Rolle der Internen Revision entwickelt sich zu einem kompetenten Anbieter sowohl für Prüfungs- als auch für Beratungsleistungen. Studienergebnisse zeigen drei verschiedene Rollen für die Interne Revision auf, die bei den relevanten Stakeholdern mit einer Schaffung von Mehrwert assoziiert werden:

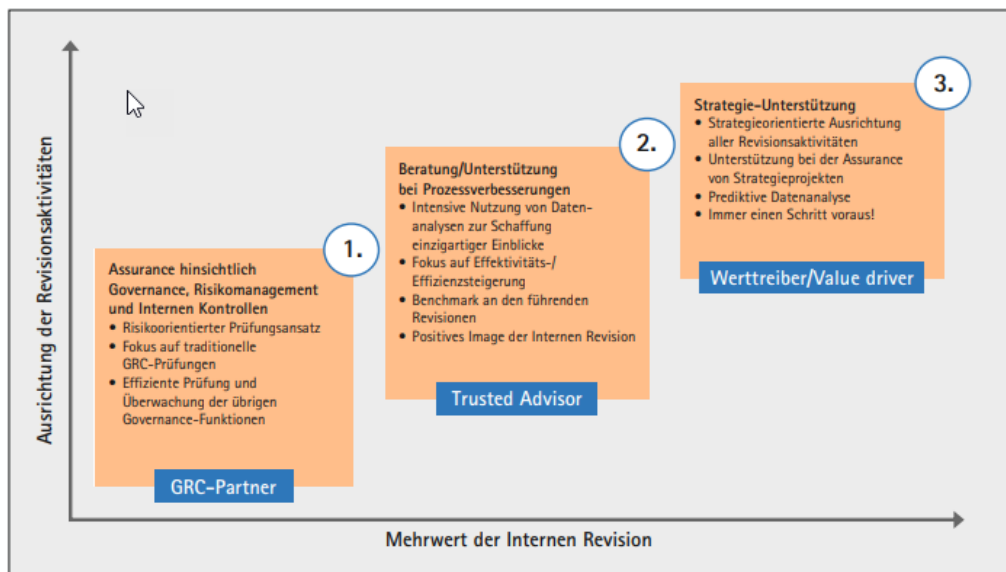


Abb. 11: Der Wert der Internen Revision¹²

Damit entwickeln sich auch die Revisionsaufgaben:

- Verlagerung der Zielsetzung der Revisionstätigkeit von einer „Ermittlung von Abweichungen und Schwachstellen“ hin zu einer „Verbesserung der Sachverhalte“
- Entwicklung von einer Ordnungsmäßigkeits- und Sicherheitsprüfung zu einer Wirtschaftlichkeits-, Zweckmäßigkeits- und insbesondere Risikoprüfung

¹² Eulerich/Lenz ZIR, 04/2020.

- Änderung der Blickrichtung der Internen Revision von einer Vergangenheits- zu einer Zukunftsorientierung

Die Interne Revision als eine Schlüsselfunktion („Key Player“) im (konzernweiten) Risikoüberwachungssystem muss sich im Sinne einer konsequenten, präventiven und flexiblen Risiko-, Prozess- und Wertorientierung diesen Herausforderungen stellen, um eine wachsende Effizienz, Effektivität und damit Akzeptanz zu erzielen.

Eine wirksame Revision muss aktuell, flexibel und dynamisch auf neue Risiken und Veränderungen reagieren, um durch präventive Maßnahmen Schwachstellen und Risiken frühzeitig angemessen zu begegnen. Dazu muss die Interne Revision sich neben ihren „klassischen“ Prüfungsleistungen „ex post“ stärker präventiv („ex ante“) und proaktiv beratend, begleitend und/oder prüfend in Strategiefindungs-, Entwicklungs- und Entscheidungsprozesse sowie bei Anpassungsprozessen gemäß AT 8 MaRisk einbringen. Durch die frühzeitige Identifikation von Risiken, Mängeln und Verbesserungspotenzialen werden

- Risiken durch angemessene Maßnahmen effektiv vermieden, reduziert, transferiert oder bewusst akzeptiert,
- Produkte, Prozesse oder Systeme in der Entwicklung verbessert,
- frühzeitig Mehrwerte für das Unternehmen geschaffen,
- das Revisions-Know-how durch kontinuierliche Lerneffekte aufgebaut,
- das Image der Internen Revision erhöht und
- der Erfolg für das Unternehmen gesteigert.

Die Interne Revision entwickelt sich damit zu einem strategischen und operativen Frühwarn-, Steuerungs- und Risikovermeidungsinstrument der Geschäftsleitung. Dabei darf sie jedoch ihre Revisionsgrundsätze, insbesondere Prozessunabhängigkeit und Objektivität, nicht verlassen.

6.2 Anforderungen

Die strategische Ausrichtung der Internen Revision in Richtung präventiver und risikoorientierter Beratungsleistungen ist in der Zielsetzung der Internen Revision des IIA bzw. DIIR (GIAS Domain I) der Internen Revision berücksichtigt:

- „Die Interne Revision stärkt die Fähigkeit der Organisation, Werte zu schaffen, zu schützen und zu erhalten, indem sie dem Leitungs- und Überwachungsorgan und dem Management unabhängige, risikobasierte und objektive Prüfungssicherheit, Beratung, Erkenntnisse und Voraussicht liefert.“

Die Interne Revision verbessert die Organisation in:

- der erfolgreichen Realisierung ihrer Ziele,
- den Governance-, Risikomanagement- und Kontrollprozessen,
- der Entscheidungsfindung und Aufsicht,
- der Reputation und Glaubwürdigkeit bei ihren Stakeholdern,
- der Fähigkeit, dem öffentlichen Interesse zu dienen.

Die entsprechenden aufsichtsrechtlichen Anforderungen im Rahmen von Projektbegleitungen, Anpassungsprozessen sowie beratenden Revisionsaktivitäten lauten:

- Die Interne Revision hat unter Wahrung ihrer Unabhängigkeit und unter Vermeidung von Interessenskonflikten bei wesentlichen Projekten begleitend tätig zu sein (BT 2.1 Tz. 2 MaRisk)
- Sowohl in die Erstellung des Konzeptes als auch in die Testphase sind die später in die Arbeitsabläufe eingebundenen Organisationseinheiten einzuschalten. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die Interne Revision zu beteiligen (AT 8.1 Tz. 5 MaRisk)
- Vor wesentlichen Veränderungen in der Aufbau- und Ablauforganisation sowie in den IT-Systemen hat das Institut die Auswirkungen der geplanten Veränderungen auf die Kontrollverfahren und die Kontrollintensität zu analysieren. Im Rahmen ihrer Aufgaben sind auch die Risikocontrolling-Funktion, die Compliance-Funktion und die Interne Revision zu beteiligen (AT 8.2 MaRisk)
- Soweit die Unabhängigkeit der Internen Revision gewährleistet ist, kann sie im Rahmen ihrer Aufgaben für die Geschäftsleitung oder andere Organisationseinheiten des Instituts beratend tätig sein (BT 2.2, Tz. 2 MaRisk)

Für die praktische Umsetzung dieser Revisionsanforderungen hat sich die Interne Revision daher u. a. mit folgenden Fragestellungen auseinanderzusetzen:

- Wie werden Beratung, Projektbegleitung sowie die Beteiligung der Internen Revision bei Anpassungsprozessen gemäß AT 8 MaRisk konkret ausgestaltet?
- Ist eine beratende Funktion der Internen Revision von der Geschäftsleitung gewollt?
- Wie werden diese Aufgaben definiert, geplant und organisiert?
- Welche Rahmenbedingungen und Grundsätze sind zu beachten (z. B. Wahrung der Unabhängigkeit, Vermeidung von Interessenskonflikten)?
- Verfügt die Interne Revision über ausreichende und geeignete Ressourcen, um Beratungsleistungen zu erbringen?

Entspricht das Verhältnis zwischen Prüfungs- und Beratungsaufträgen im Revisionsplan der Revisionsstrategie?

6.3 Abgrenzung der Begrifflichkeiten

Beratung ist in Art und Umfang mit dem Kunden (auch Auftraggeber oder Ratsuchender) vereinbart und leistet durch sachverständige Personen Verhaltens- und Handlungsempfehlungen, die als Entscheidungshilfen dienen, ohne Prüfungssicherheit zu geben oder Managementverantwortung zu übernehmen. Ziel ist es, optimale Lösungen zur Wertschöpfung und zur Verbesserung der Geschäftsprozesse vorzuschlagen, um die Effizienz und Effektivität der Abläufe zu steigern und die Wettbewerbsfähigkeit des Unternehmens zu sichern. Der Berater geht von einer gegebenen Situation („Ist“) aus und legt seinen Empfehlungen die Zielvorstellungen des Ratsuchenden („Soll“) zugrunde. Die Entscheidung über die Umsetzung der Empfehlungen und ggf. der Überwachung verbleibt ausschließlich beim Kunden.

Interne Revisorinnen und Revisoren können Beratungsleistungen initiieren oder auf Anforderung von Geschäftsleitung, Überwachungsorgan oder Management erbringen.

Beratung muss weder formell noch schriftlich erfolgen. Sie kann in unterschiedlichen Formen, z. B. über mündliche Beantwortung einer Frage, schriftlich definierte, formelle Einsätze mit schriftlicher Ergebnisdokumentation oder über die Teilnahme an ständigen oder zeitweiligen Management-Ausschüssen oder Projektteams erfolgen.

6.4 Regeln und Grundsätze

Um eine ordnungsgemäße, kompetente und effektive Erbringung von Beratungsleistungen durch die Interne Revision sicherzustellen, sind in der Revisionsordnung bzw. im Revisionshandbuch hinreichende formale Rahmenregelungen zu fixieren (Grundsätze, Abgrenzung, Aufgabenfelder, Prozessablauf, Kompetenzen etc.). Auch bei der Erbringung von Beratungsleistungen wird erwartet, dass die GIAS (eingehalten werden). Folgende Grundsätze sind in der Beratungspraxis insbesondere zu beachten:

- Standard 2.1 „Individuelle Objektivität“
- Standard 7.1 „Organisatorische Unabhängigkeit“
- Standard 11.3 „Kommunikation von Ergebnissen“

Dies auch, um die Erwartungshaltung des Auftragsgebers und die Möglichkeiten der Internen Revision in Einklang zu bringen und die Möglichkeiten sowie den Mehrwert der Beratungsleistung durch die Interne Revision für alle Beteiligten transparent zu machen. Es empfiehlt sich, Kriterien für die Einordnung einer Tätigkeit als Beratung zu definieren.

Bei komplexen Beratungsaufträgen, deren Ergebnis schriftlich dokumentiert werden soll, empfiehlt sich in Abhängigkeit vom Umfang und der Komplexität der Beratung die Beachtung der folgenden Punkte:

1. Annahme eines Beratungsauftrages sorgfältig und kritisch prüfen

- Prüfungsauftrag gem. Prüfungsplan geht vor Beratung (Beratungen ersetzen keine vorgesehenen Prüfungen)
- Keine revisionsfremden Aufgaben wahrnehmen
- Prozessunabhängigkeit, Objektivität und Vertraulichkeit wahren
- Interessenskonflikte meiden
- Beeinträchtigungen der Objektivität offenlegen
- Revisionsaufgaben unbeeinflusst wahrnehmen
- Revisionskompetenz (Wissen, Fähigkeiten und Qualifikation) anforderungsgerecht sicherstellen
- Vereinbarkeit des Beratungsauftrags mit der Revisionsplanung sicherstellen
- Übereinstimmung mit Instituts-/Revisionszielen prüfen (Verbesserung Geschäftsprozesse, IKS und Risikomanagement)
- Auswirkungen auf das Image der Internen Revision beachten

2. Beratungsauftrag soweit erforderlich schriftlich fixieren und mit Auftraggeber abstimmen

- Alle Fakten kennen (Ansprüche des Managements, Motive, Ziele, erforderlicher Leistungsumfang, Ressourcen, Termine, etc.)
- Ziele, Umfang, Rechte, Pflichten und Erwartungen gemeinsam festlegen
- Allgemeine Bedingungen, Absprachen, durchzuführende Arbeiten und Schlüsselfaktoren des offiziellen Beratungsauftrags schriftlich vereinbaren oder als Prüfungsplan dokumentieren
- Rolle der Internen Revision klarstellen.

3. Maßnahmen zur Minimierung möglicher Beeinträchtigungen treffen

- Keine unangemessene fachliche Verantwortung übernehmen

- In Komitees keine Entscheidungsverantwortung (non-voting member)
- Getrennte Ergebnisverantwortung vereinbaren (Verantwortung für Annahme/Umsetzung von Empfehlungen liegt beim Management)
- Auftraggeber auf die Rahmenbedingungen für die Interne Revision hinweisen
- Beratungsauftrag in der Revisionsplanung berücksichtigen

4. **Beratungsauftrag sorgfältig und systematisch durchführen**

- Klare Methodik festlegen/Abgrenzung zur Prüfung
- „Level“ der Beratungsleistung festlegen
- Soweit erforderlich Erstellung des Arbeitsprogramm in Zusammenarbeit mit den Stakeholdern, die die Beratungsleistung angefordert haben
- Notwendiges Informationsmaterial sammeln
- Geeignete Gesprächspartner identifizieren und Besprechungen festlegen
- Mögliche Risiken konstant beachten, analysieren und bewerten (bzgl. Beratungsziel, Geschäfts-/Risikostrategie(n), Revisionsgrundsätze)
- Wesentliche Kontrollschwächen erkennen und berücksichtigen
- Im Konfliktfall eindeutig Stellung beziehen
- Beeinträchtigungen bzw. Zweifel an der Angemessenheit des Beratungsauftrags unverzüglich melden und mit dem Kunden abstimmen
- Arbeitsunterlagen zur Beratungsabwicklung angemessen und nachvollziehbar dokumentieren
- Offenlegung der Arbeitsunterlagen/ -ergebnisse auf Nachfrage an interne und externe Stellen ermöglichen

5. **Angemessene Kommunikation und Berichterstattung sicherstellen (falls vom Auftraggeber gewünscht bzw. für die Geschäftsleitung erforderlich)**

- Entwicklung eines Gesamturteils (z. B. Fazit, Management Summary), das zu den Zielen und dem Umfang des Beratungsauftrags passt
- Kommunikation bzw. Berichterstattung über Risiken, Status und Ergebnis in Abhängigkeit von Art, Umfang, Komplexität und Risikogehalt

- Nachvollziehbare Dokumentation und Kommunikation gemäß Unternehmenspraxis, Kundenbedürfnis und inhaltlicher Bedeutung (mündlich, E-Mail, Vermerk, Bericht etc.)
- Risiken und Mängel zeitnah angemessen berichten

6. **Vereinbarte Umsetzung von Beratungsergebnissen begleiten/ überwachen**

- Im Rahmen von Beratungen gewonnene Erkenntnisse ggf. im Rahmen der risikoorientierten Prüfungsplanung in die Risikobeurteilung des betreffenden Prüfobjektes einfließen lassen
- Nur auf Wunsch des Auftraggebers: Die Umsetzung der Beratungsergebnisse in dem mit dem Auftraggeber vereinbarten Umfang überwachen

6.5 **Beratung in der Praxis**

Die Interne Revision verfügt über ein breites und ressortübergreifendes Fachwissen, kennt Prozesse, Produkte und Systeme des Instituts mit ihren Risiken und Kontrollinstrumenten und hat den Überblick über Zusammenhänge und Wechselwirkungen. In der Praxis wird sich der Schwerpunkt der Beratungsleistungen auf die Anforderungen zum Risikomanagement und der Internen Kontrollverfahren konzentrieren. Auch bestehen im Regelfall Erwartungen seitens der Auftraggeber an die Interne Revision, insbesondere aufsichtsrechtliche Anforderungen und Aspekte in die Beratungsleistung einzubeziehen (z. B. Erfahrungen aus § 44 KWG-Prüfungen).

Um das Know-how der Interne Revision den Gremien, dem Management und den Fachbereichen des Instituts zu erschließen, bieten sich in der Praxis u. a. folgende Themenbereiche für vorausschauende, begleitende Beratungsleistungen an:

- Umsetzung von (neuen) regulatorischen Anforderungen.
- Grundsatzfragen zur Angemessenheit und Wirksamkeit des Risikomanagements und der Internen Kontrollverfahren
- Umsetzung von Auslagerungsvorhaben (s. a. gesonderte Anforderung an die Revision gem. MaRisk AT 9 Tz. 2) oder Leistungsbezüge von IKT-Drittdienstleistern, die kritische oder wichtige Funktionen unterstützen
- Begleitung von Ausschüssen (Prüfungs-, Vergütungs-, Anlageausschuss)
- Koordination bzw. Begleitung von externen und aufsichtlichen Prüfungen
- Fusionen und Übernahmen (z. B. organisational due diligence)
- Analyse von Daten für die Geschäftsleitung (z. B. Continuous Risk Assessment)

- Umsetzung von IT-Veränderungen und Releasewechsel
- Begleitung Programmeinsatz- und Freigabeverfahren
- Inhouse-Seminare, -Vorträge und -Workshops
- forensische Dienstleistungen

Darüber hinaus kann eine Beratung auch im Rahmen der Begleitung von Anpassungsprozessen oder von wesentlichen Projekten erfolgen:

- Neu-Produkt-Prozess (NPP) zur Entwicklung, Einführung und Änderung von Produkten (inkl. neuer Märkte) (s. a. gesonderte Anforderung an die Revision gem. MaRisk AT 8.1)
- Änderungen betrieblicher Prozesse oder Strukturen, sofern wesentliche Veränderungen in der Aufbau- oder Ablauforganisation sowie in den IT-Systemen betroffen sind (s. a. gesonderte Anforderung an die Revision gem. MaRisk AT 8.2)
- Begleitung von Projekten (s. a. gesonderte Anforderung an die Revision gem. MaRisk BT 2.1. Tz. 2)

In der Revisionsplanung sind für derartige Beratungsleistungen entsprechende Revisionskapazitäten zu berücksichtigen, entweder in Form bereits konkretisierter und beauftragter Beratungsprojekte oder als „Platzhalter“ bei wiederkehrenden Beratungsaktivitäten.

Hinsichtlich seines Verhaltens als Berater sind für den Revisor unterschiedliche Vorgehensweisen bzw. Ergebnistypen denkbar:

- Keine Abgabe von Ratschlägen, sondern Unterstützung des Ratsuchenden bei der Lösungsfindung bzw. bei Einzelfragen/Meilensteinen
- Abgabe von Empfehlungen bzw. Aufzeigen alternativer Lösungsansätze im Sinne „Best Practice-Lösungen“
- Positionierung für die aus Sicht der Revision beste Lösung bei gleichzeitiger Betonung der Verantwortlichkeit der tatsächlichen Entscheider (Wahrung der Unabhängigkeit der Revision)

Entscheidend zur Wahrung der Unabhängigkeit ist es sicherzustellen, dass die Revision nicht an der Entscheidung beteiligt und auch nicht darüber der Anschein erweckt wird. Die Berichterstattung und Kommunikation bei Beratungen und der Begleitung wesentlicher Projekte ist abhängig von Art, Umfang, Komplexität und Risikogehalt des jeweiligen Einzelfalles. Eine Berichterstattung an die Geschäftsleitung ist grundsätzlich nicht erforderlich. Es empfiehlt sich jedoch, zum Projekt- bzw. Jahresende einen kurzen Ergebnis- bzw. Statusbericht für den Auftraggeber bzw. zur Dokumentation der eigenen Tätigkeit zu erstellen.

Sofern im Rahmen einer Beratung Risiken festgestellt werden, die eine risikoorientierte Prüfung durch die Interne Revision erforderlich machen, ist – ggf. in Abstimmung mit der Geschäftsleitung – über eine formelle Prüfung des zugrundeliegenden Sachverhaltes zu entscheiden.

6.6 Personelle Anforderungen

Entsprechend den MaRisk hat sich die quantitative und qualitative Personalausstattung i. d. R. an betriebsinternen Erfordernissen, der Komplexität der Geschäftsaktivitäten sowie der Risikosituation des Instituts zu orientieren). Der Leiter der Internen Revision muss einen Beratungsauftrag ablehnen oder kompetenten Rat und Unterstützung einholen, wenn Interne Revisoren nicht über das Wissen, die Fähigkeiten oder sonstige Qualifikationen verfügen, die zur teilweisen oder vollständigen Erfüllung des Auftrags erforderlich sind.

7 Continuous Auditing Continuous-Risk Assessment

7.1 Vorbemerkung

Die größer werdende Anzahl gesetzlicher und regulatorischer Anforderungen, die steigende Geschwindigkeit wirtschaftlicher Veränderungen mit ihren Einflüssen auf die Geschäftsmodelle, zunehmende Komplexitäten und Risikoschwankungen und nicht zuletzt die Digitalisierung und Automatisierung von Geschäftsprozessen verlangen verstärkt nach einer vorausschauend planenden und gleichzeitig zeitnah reagierenden Internen Revision. Daher ist es sinnvoll, dass sich die Interne Revision von einer statischen, zeitraumbasierten (ein bis fünf Jahre im Voraus erfolgenden) Risikobeurteilung und Prüfungsplanung hin zu einer direkt situativ-reaktiven Analyse von Risiken und Kontrollwirksamkeiten mit darauf aufbauender, risikoorientierten Prüfungsplanung entwickelt. Die risikoorientierte Ausrichtung von Prüfungstätigkeiten bildet die Grundlage für den effizienten Einsatz der Revisionsressourcen. Aufgrund der im Finanzwesen geforderten stringenten Messung und Steuerung von wesentlichen Risikotreibern liegen in vielen Banken regelmäßige und standardisierte Messungen von Steuerungs- und Leistungsdaten sowie ergänzende qualitative Informationen vor. Diese bilden eine gute Ausgangslage für den Aufbau und die Anwendung eines Continuous Auditing. Durch Continuous Auditing können - neben den klassischen ex-post orientierten Prüfungshandlungen - auch proaktiv Auffälligkeiten einer konkreten und mit aktuellen Entwicklungen verknüpften Überprüfung unterzogen werden. Die Ergebnisse dieser Überprüfung können sowohl Einfluss auf den Umfang/ Schwerpunkt und Zeitpunkt geplanter Prüfungen, als auch den Jahresprüfplan haben.

In den MaRisk ist die Einrichtung eines Continuous Auditing oder eines Continuous Monitoring nicht explizit gefordert. Entsprechende Maßnahmen können jedoch z. B. die risikoorientierte Prüfungsplanung oder die Schwerpunktsetzung in Prüfungen unterstützen.

Der DIIR-Arbeitskreis Continuous Auditing hat einen „Leitfaden für die Einführung eines Continuous-Auditing-Systems“ veröffentlicht. Der Leitfaden enthält praxisbezogene Lösungsansätze und Best-Practice-Erfahrungen.

7.2 Begriffsbestimmung und Abgrenzung

Zunächst ist eine Definition der inhaltlich stark verwandten Begriffe Continuous Monitoring und Continuous Auditing notwendig, um die praktischen Zusammenhänge klarer herauszuarbeiten.¹³

- Continuous Monitoring ist definiert als fortlaufende Methode, die sicherstellen soll, dass die Regeln, Prozesse und Geschäftsabläufe wirksam und funktionsfähig sind. Die Verantwortlichkeit liegt bei dem operativen Management.
- Continuous Auditing ist eine Methode, mit der fortlaufend eine ganzheitliche Bewertung der Risikosituation durch die Interne Revision gewährleistet wird und je nach Ausprägung abgestufte Prüfungshandlungen durchgeführt werden.

Die Unterscheidung liegt somit im Wesentlichen in den verantwortlichen Personen. Ein wirksames Continuous Monitoring ist aufgrund der inhaltlichen Verknüpfung der beiden Konzepte eine wesentliche Erleichterung, ein effektives und effizientes Continuous Auditing aufbauen zu können.

Die methodischen Bestandteile des Continuous Auditings lassen sich in Continuous Controls-Assessment und Continuous-Risk-Assessment unterscheiden. Das Continuous Controls-Assessment bewegt sich grundsätzlich näher am Continuous Monitoring und beschreibt die Bewertung der Wirksamkeit der wesentlichen Bestandteile des Internen Kontrollsystems. Das Continuous-Risk-Assessment ist auf einer höheren Ebene angeordnet und zielt darauf ab, Risiken zu identifizieren und unter Berücksichtigung von Schweregrad und Eintrittswahrscheinlichkeit die Auswirkungen und Implikationen für das Unternehmen und die Revisionsarbeit abzuleiten.

7.3 Ziele und Einsatzgebiete des Continuous Auditing

Abgeleitet aus der oben dargestellten Definition des Begriffes Continuous Auditing ergeben sich in der Praxis mehrere Ziele und Einsatzgebiete. Der Hauptfokus des Continuous Auditing liegt darin, die gemäß MaRisk vorgegebenen periodischen Prüfungshandlungen durch fortlaufende Überwachungshandlungen und Risikoeinschätzungen zwischen und integriert in den Standardprüfungen als weitere Prüfmethode zu ergänzen. Eine fortlaufende Überwachung und Bewertung der unternehmensweiten wesentlichen Kennzahlen und Indikatoren bietet der Internen Revision die Möglichkeit ihre Arbeit effektiver und effizienter zu gestalten:

¹³ Vgl. The Institute of Internal Auditors, Global Technology Audit Guide – Continuous Auditing: Implications for Assurance, Monitoring and Risk Assessment, S. 1.

- Regelmäßige Anpassung des Jahresprüfplans aufgrund valider Informationen über Änderungen in der Risikolandschaft des Unternehmens/Effektivere rollierende Prüfungsplanung
- Zielgerichtete Definition des Prüfungsumfangs in den Standardprüfungen aus dem Jahresprüfplan, da bereits unterjährig erhobene Daten in der Internen Revision vorliegen
- Identifikation von notwendigen Ad-hoc-/Sonderprüfung aufgrund von außergewöhnlichen Entwicklungen in Unternehmensteilbereichen
- Fortlaufende Kommunikation zwischen dem verantwortlichen Management der Geschäftsbereiche und der Internen Revision, die letztendlich zu einem besseren Verständnis der gegenseitigen Anforderungen und Aufgaben führt

7.4 Rahmenbedingungen

Für ein effektives Continuous Auditing ist eine einheitliche Risikodefinition und Risikokultur im Unternehmen ein wichtiger unterstützender Erfolgsfaktor. Eine einheitliche Orientierung aller Unternehmenstätigkeiten „top-down“ an den Unternehmenszielen erleichtert die praktische Durchführbarkeit des Continuous Auditing. Hierzu sei beispielhaft auf das international anerkannte Regelwerk zum unternehmensweiten Risikomanagement „COSO II – Enterprise Risk Management Framework“ verwiesen. Revisionsintern ist eine stringente Ausrichtung am Prüfungsuniversum (sprich Aufteilung/Abgrenzung der Objekte, Übernahme des inhärenten Risikos, etc.) notwendig, um ein Gleichlaufen der Aktivitäten zu gewährleisten (vgl. Abschnitt 2.7 (COSO) und 3.1.1.1 (Prüfungsuniversum) dieses Handbuches zu entnehmen.

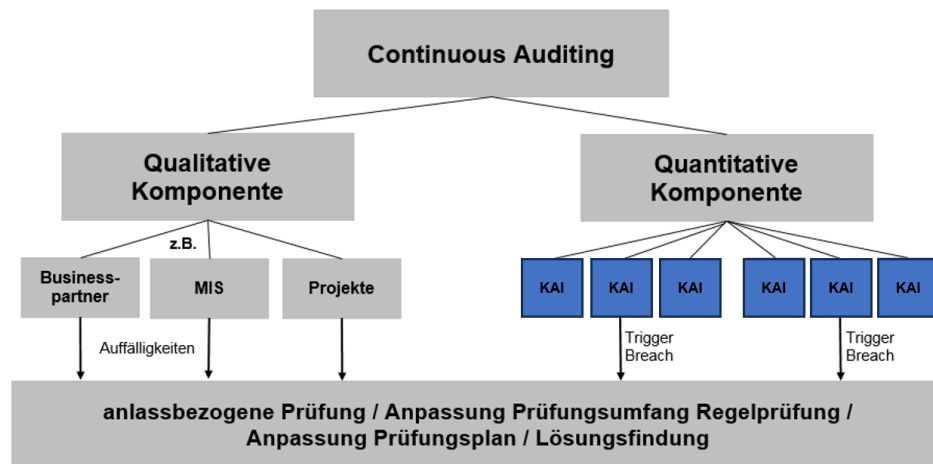
7.5 Bestandteile des Continuous Auditing

7.5.1 Grundsätzliches

Das Continuous Auditing ist in seiner Durchführung in zwei sich ergänzende Bestandteile zu unterteilen: Ein qualitatives Element, welches die Interne Revision befähigt, das Prozesswissen zu vertiefen und Informationen zu gewinnen, welche nicht Teil regelmäßiger Berichterstattung sind und ein quantitatives Element, in welchem wesentliche Steuerungsgrößen (Key-Audit-Indicators – KAI) aus verfügbaren und ggf. selbst verdichteten Datenquellen fortlaufend ausgewertet und überwacht werden.

Definition Key-Audit-Indicators

Key-Audit-Indicators sind quantitative Messgrößen, deren aktuelle Werte bzw. Ausprägungen und zeitliche Entwicklungen in einem erkennbaren Kausalitäts-Zusammenhang mit der Eintrittswahrscheinlichkeit der Prüfobjekt-Risiken und/oder mit der Chance zur Erreichung der Prüfobjekt-Performance-Ziele stehen.



Bestandteile des Continuous Auditing

Abb. 12: Bestandteile des Continuous Auditing

7.5.2 Qualitatives Element (Business Partnership)

Wichtige Grundlage zur Abdeckung der einzelnen Wertschöpfungsketten bzw. Unterstützungs- und Steuerungsprozesse ist das Relationship-Management. Hierunter ist insbesondere der Aufbau einer kontinuierlichen und offenen Beziehung zu dem Management der zu betreuenden Prüfobjekte zu verstehen, die sich durch zwei wesentliche Eckpfeiler charakterisieren lässt:

- Austausch über Probleme und aktuelle Entwicklungen mit dem Business Partner – z. B. Bereichszielsetzung, Personal- oder Strukturveränderung, IT-Umstellung, Profit & Loss-Entwicklung, Projekte in Planung oder Umsetzung – durch regelmäßige Treffen mit dem Management bzw. mit den im Vorfeld benannten Schlüsselpersonen

- Schnittstellenmanagement zwischen betreuender Fachabteilung und quantitativen Continuous Auditing-Aktivitäten

Über den Partnerschaftsgedanken sollen die verantwortlichen Revisoren kompetente Partner für das Business und die von ihnen betreuten Prozesse und Aktivitäten sein und sind insoweit gehalten, in regelmäßigen Treffen mit dem Management der Fachabteilungen sich nicht nur über Probleme und aktuelle Entwicklungen auszutauschen, sondern auch lösungsorientiert neue Erkenntnisse und externes Know-how i. S. eines Best-Practice-Ansatzes weiterzugeben.

Zusammenfassend sind folgende Aufgaben bei der Umsetzung des qualitativen Ansatzes im Rahmen des Continuous Auditing zu berücksichtigen:

- Interne Revision benötigt umfassendes Prozessverständnis
- Revisionsmitarbeiter als Kompetenzträger für die zu überprüfenden Geschäftsbereiche; dies schließt ein, die strategischen und operativen Ziele mit den daraus abgeleiteten Risiken und den wesentlichen Prozessen einschließlich der Kontrollen zu kennen
- Regelmäßig fachlicher Austausch mit verantwortlichem Management
- Revisionsvorbehalte müssen ausgeräumt werden, die Nähe zum Geschäftsbereich soll Mehrwert für die Bank und verständlicherweise dann auch für die Geschäftsbereiche bieten

7.5.3 Quantitatives Element

Ein weiterer wichtiger Faktor für die erfolgreiche Umsetzung des Continuous Auditing ist die Kenntnis der EDV-Systeme, mit denen die Daten zügig abgerufen, aufbereitet und in bewertbare Form gebracht werden. Bei der Identifikation der Datenquellen kann sowohl der System- als auch der Prozess-Owner behilflich sein. Weiterhin von Nutzen sind Beschreibungen wie Data-Dictionary und Prozess/Datenflusspläne. Die Identifikation der wesentlichen Datenquellen/ Source Systemen wird z. B. durch folgende Aktivitäten erleichtert:

- Durchsicht von Prozessbeschreibungen, Handbüchern, Arbeitsanweisungen, Datenflussdiagrammen, Beschreibung von Systemkontrollen
- Interviews mit Prozessverantwortlichen
- Durchsicht bestehender Management-Berichte (Managementinformationssystem - MIS)

Das Prozess- und EDV-Verständnis (welche Systeme gibt es) ist auf Ebene des qualitativen Ansatzes zu erarbeiten und über eine Kooperation mit den IT-Prüfern und Analysten der Internen Revision in den Aufbau des Continuous Auditing einfließen zu lassen.

Die umfassende Risikobewertung und -steuerung der Revisionsaktivitäten begründet sich nicht nur in einer Betrachtung der qualitativ zu prüfenden Komponenten, sondern auch in einer laufenden Analyse und Bewertung von quantitativen Performance-, Risiko- und Auditindikatoren. Wobei eine klare Abtrennung von qualitativen und quantitativen Indikatoren nicht immer möglich ist, es gibt hier auch Mischformen. Grundsätzlich ist in Erwägung zu ziehen, inwieweit diese wesentlichen Indikatoren in das Continuous Monitoring der Fachbereiche einfließen sollten.

Datenzugang

Der effektive Nutzen des Continuous Auditing hängt – um eine laufende Analyse und ein stringentes Follow-up zu gewährleisten – wesentlich von einem ungehinderten und vollständigen Zugang zu den benötigten Informationen ab. Die Methode des Datenzugangs wird durch die individuellen Ziele des Continuous Auditing vorbestimmt und hat Faktoren wie bspw. Datenvolumen, Netzverkehr, Systemleistungsfähigkeit in Betracht zu ziehen. Grundsätzlich ist davon auszugehen, dass das Continuous Auditing eine Kombination aus mehreren Datenzugangsvarianten bedingt, wie z. B.:

- Einbettung der Continuous-Auditing-Checks in die Business Systeme, um die Daten direkt am „Entstehungsort“ abzubilden
- Sicherstellung eines unabhängigen Zugangs zu den Systemdaten (ohne die Anwendersoftware zu gebrauchen) mit der Möglichkeit die Daten zu extrahieren und in die eigene Datenanalysesoftware zu überführen
- Erstellung von Kopien von Standardberichten (MIS) und Speicherung der Berichte in elektronischer Form für Folgeanalysen
- Sicherstellung eines physischen und logischen Zugangs zu den Bereichssystemen mit Read-only-Rechten

Die Kombination aus den verschiedenen Datenzugangsvarianten gibt der Internen Revision die Möglichkeit, zeitnah über das Continuous Auditing negative Entwicklungen und Trends zu identifizieren und in aggregierter sowie verständlicher Form hierüber zu berichten. Weiterhin hilft es den Revisionsmitarbeitenden schnell Auffälligkeiten (z. B. Abweichungen zu definierten Schwellenwerten, Sprünge) mit ähnlichen Parametern zu erkennen und daraufhin die markierten Auffälligkeiten nachzuverfolgen.

Sicherstellung der Datenqualität

Die Datenqualität ist von wesentlicher Bedeutung für den reibungslosen Ablauf des Continuous Auditing. Zur Sicherstellung der Datenqualität sind sowohl vom Datenanalysten als auch vom entsprechenden Kompetenzträger ausreichende Checks durchzuführen.

Von der Extraktion der Rohdaten über die weiteren Zwischenschritte (z. B. Datenaufbereitung) bis hin zur Datenanalyse und -interpretation kann die Qualitätssicherung folgende Merkmale und beispielhafte Fragestellungen umfassen:

Vollständigkeit

Um fundierte Aussagen aufgrund eines Datenbestandes treffen zu können, muss sichergestellt sein, dass alle verfügbaren und benötigten Datensätze und Attribute bis zur Erstellung des Endergebnisses durchgängig verwendet werden.

- Wurden die Quelldaten bereits gefiltert oder aggregiert?
- Können beim Zusammenführen von Daten alle Datensätze zugeordnet werden (Schlüsselqualität)?
- Ist die Vollständigkeit der Daten während des Datentransfers sichergestellt?

Gültigkeit

Zur ordnungsgemäßen Verarbeitung und Interpretation der Daten ist es notwendig, dass die Daten logisch der Datendefinition entsprechen.

- Wurden die Beschränkungen der Datentypen eingehalten?
- Sind die Felddarstellungen eindeutig?
- Können Fehler bei der Erstellung der Daten auftreten?

Richtigkeit

Ein kritischer Aspekt der Datenqualität betrifft die Richtigkeit der Daten. Dieser Punkt ist sehr differenziert zu sehen, da die Richtigkeit durch verschiedene Stellen, die mit den Daten arbeiten, sichergestellt werden muss. Hierzu ist eine enge Kooperation zwischen den Datenanalysten, der IT und dem Kompetenzträger notwendig, um sowohl bei der Erstellung als auch bei der Interpretation der Daten die Richtigkeit gewährleisten zu können.

- Ist die Richtigkeit der Quelldaten sichergestellt?
- Wird das Endergebnis korrekt interpretiert?

- Sind die Feldaussprägungen eindeutig?
- Sind Sonderausprägungen/ -fälle berücksichtigt?

Integrität

Die Datenintegrität beschreibt hauptsächlich den logischen Zusammenhang von Datensätzen und Feldern einzelner oder mehrerer Datenbestände untereinander. Neben Aspekten der Gültigkeit ist vor allem sicherzustellen, dass die Kombination der Datensätze immer eindeutig ist (Schlüsselsicherstellung).

- Ist ein Datensatz eindeutig identifizierbar?
- Sind verschiedenen Datenquellen untereinander kompatibel?
- Ist sichergestellt das Datenänderungen erkannt werden und transparent sind?

Aktualität

Insbesondere bei der Arbeit mit Daten verschiedener Quellen muss sichergestellt werden, dass die Datenbestände zeitlich miteinander kombinierbar sind. Ebenso ist oftmals die Aussagekraft der Daten davon abhängig, wie aktuell die entsprechenden Auszüge sind.

- Sind die Daten aktuell?
- Wie oft werden die Daten aktualisiert?
- Wann erfolgte die letzte Datenaktualisierung?
- Passen verschiedene Datenbestände zeitlich zueinander?

Wie groß der Arbeitsaufwand zur Sicherstellung der Datenqualität ist, hängt davon ab, wie schwerwiegend die Konsequenzen sein können, wenn das Continuous Auditing auf fehlerhaften Daten aufsetzt. Ebenso ist im Sinne einer Kosten-Nutzen-Betrachtung zu berücksichtigen, wie groß der Aufwand zur Sicherstellung aller Punkte durch die beteiligten Stellen ist und welcher Nutzen sich letztendlich ergibt. Prinzipiell kann eine umfassende Sicherstellung der Datenqualität nur durch die Kombination von Prozesskenntnis und technischem Verständnis erreicht werden.

Datennutzung

Nachdem die Schlüsselsysteme identifiziert wurden, der Datenzugang gewährleistet ist und die Datenintegrität verifiziert wurde, kann die konkrete Nutzung des Datenmaterials beginnen. Wichtig hierbei sind ein hohes Maß an Professionalität im Umgang mit IT und den zu prüfenden Objekten, Prozessen oder Funktionen. Insbesondere diejenigen Mitar-

beitenden der Internen Revision, die das Continuous Auditing über den qualitativen Ansatz umsetzen, benötigen zur Initiierung bzw. Ableitung konkreter Handlungen ein tiefergehendes Verständnis der zu überwachenden Aktivitäten einschließlich der zugrundeliegenden Systeme und Funktionalitäten.

Mit den erworbenen Kenntnissen aus Prüfungshandlungen und dem qualitativen Ansatz ist es nun die Aufgabe aussagekräftige Indikatoren zu entwickeln, welche regelmäßig ausgewertet werden, um hinreichende Aussagekraft bezüglich des betrachtenden Prüfgebietes zu liefern. Im Optimalfall liegen hierzu bereits die maßgeblichen Informationen in Form von MIS, Berichterstattungen etc. vor und müssen nur in geeigneter Form innerhalb der Internen Revision ausgewertet werden.

Bei der Selbstentwicklung und -erstellung von Indikatoren ist darauf hinzuweisen, dass hier auch eine Rückkopplung ins Continuous Monitoring, also eine Rückgabe ans Business geboten sein kann, um eine möglichst frühe Risikoevaluierung gewährleisten zu können.

Darüber hinaus sei erwähnt, dass bei der Nutzung des Datenmaterials die Grundsätze der Informationssicherheit zu berücksichtigen sind:

- Vertraulichkeit: Es ist sicherzustellen, dass die gespeicherten und bereitgestellten Informationen und Auswertungen sowie die Zugriffsmöglichkeiten auf diese nur einem begrenzten Personenkreis zur Verfügung gestellt werden
- Integrität: Es ist sicherzustellen, dass Änderungen nicht unautorisiert und unprotokolliert durchgeführt werden dürfen. Im Rahmen einer Datenbanklösung empfiehlt sich das „Einfrieren“ der Berichtsergebnisse nach einem festzulegenden Berichtszyklus, nach dem Änderungen ohne Administratorrechte nicht mehr möglich sind
- Verfügbarkeit: Es ist sicherzustellen, dass der Zugriff auf die Daten fortlaufend möglich ist

Sofern personenbezogene Daten verarbeitet werden sollen, sind insbesondere die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) zu beachten. Konkret regelt der Artikel 5 DSGVO die Grundsätze für die Verarbeitung personenbezogener Daten, z. B. die Prinzipien der „Zweckbindung“ und „Datenminimierung“. Sofern möglich, soll außerdem eine Anonymisierung bzw. Pseudonymisierung personenbezogener Daten stattfinden.

7.6 Management des Continuous Auditing

7.6.1 Dokumentation und Berichterstattung der Ergebnisse

Um eine nachhaltige Dokumentation sicherzustellen, empfiehlt es sich sowohl die qualitativen als auch die quantitativen Ergebnisse fortlaufend strukturiert (z. B. in einer Datenbank oder der jeweiligen Revisionssoftware) festzuhalten. Neben der Dokumentation sollte dies auch die Möglichkeit zur Visualisierung der Ergebnisse einschließlich kommentierender Bewertungen durch die verantwortlichen Personen bieten.

So können durch eine Reporting-Funktion, welche regelmäßig (z. B. quartalsweise) durchzuführen ist, die risikorelevanten Indikatoren zusammengestellt, bewertet und an den festgelegten Personenkreis (Revisionsmanagement, Senior Management, Geschäftsleitung, etc.) verteilt werden.

Darüber hinaus hat es sich als empfehlenswert herausgestellt, die Use Cases oder die Ergebnisse des Continuous Auditing innerhalb der Internen Revision regelmäßig durch die verantwortlichen Personen, z. B. im Rahmen eines Bereichsmeetings, vorzustellen. Dies bietet den Vorteil, dass relevantes Wissen in der Internen Revision flächendeckend verteilt wird und relevante Informationen effektiv und effizient für die Planung und Durchführung von Prüfungstätigkeiten genutzt werden können.

Ein Beispiel für die Dokumentation der regelmäßigen Auswertung qualitativer Informationen (Anlage 1) ist auf der Webseite des DIIR verfügbar. In der Tabelle können die Zuständigkeiten festgelegt und Hinweise sowie Erkenntnisse zur weiteren Nutzung im Continuous Auditing eingetragen werden.

7.6.2 Nutzung der gewonnenen Erkenntnisse

Die Ergebnisse des Continuous Auditing Ansatzes unterstützen die Interne Revision hinsichtlich der Erfüllung ihres Prüfauftrages nach MaRisk und ermöglichen neue Handlungs- und Prüfungsoptionen im Vergleich zu dem rein traditionellen Revisionsansatz. Folgende Beispiele seien hier erwähnt:

- Integration der Erkenntnisse in die regelmäßige, unterjährige Überarbeitung und Anpassung des Jahresprüfplans und Identifikation wesentlicher Plananpassungen
- Unterstützung in der Definition von Ziel und Umfang von Regelprüfungen durch die Möglichkeit detaillierterer Risikoinformation im Rahmen der Prüfungsvorbereitung
- Klares Erkennen der Notwendigkeit von Prüfungen/anlassbezogenen Prüfungen

- Adressieren von Erkenntnissen an die Fachbereiche auch außerhalb von Prüfungen im Rahmen des Business-Partner-Ansatzes

Dynamisierung der Prüfungsaktivitäten

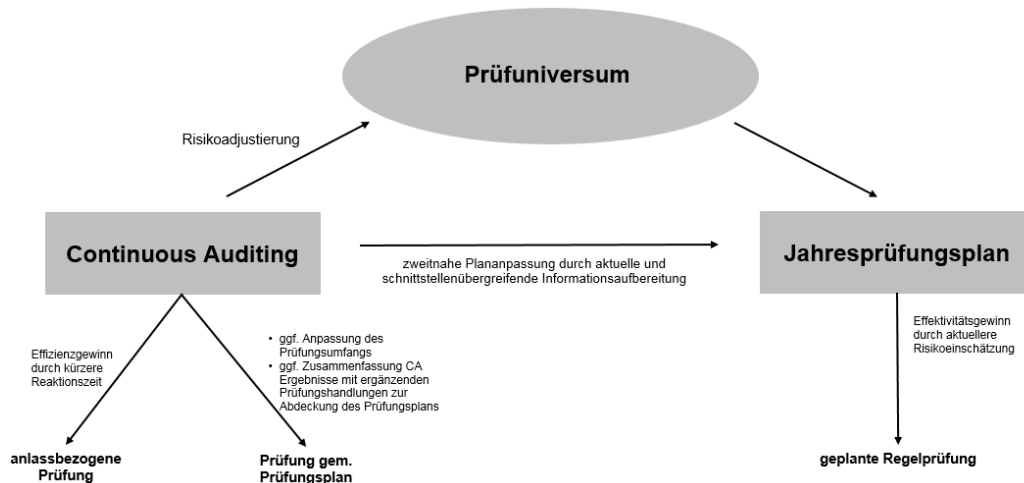


Abb. 13: Zusammenspiel von Prüfuniversum, Continuous Auditing und Jahresprüfplan

Das Konzept des Continuous Auditing lässt sich auch bei Banken mit hoher Geschäftsstellen-/Filialdichte auf diesen Vertriebskanal herunterbrechen. Durch eine zeitnahe Bewertung der einzelnen Geschäftsstellen anhand einheitlicher Bewertungsindikatoren ermöglicht ein Continuous Auditing hier die effektive Identifikation von zu prüfenden Einheiten und verkürzt dabei die insgesamt notwendige Vorbereitungszeit.¹⁴

7.6.3 Herausforderungen und Implikationen für das Continuous Auditing

Von zentraler Bedeutung für das erfolgreiche Umsetzen eines Continuous Auditing Ansatzes ist es, eine möglichst weitgehende Akzeptanz für die mit diesem Ansatz verbundenen Prüfungsaktivitäten bei dem verantwortlichen Management innerhalb des Unternehmens zu schaffen. Hohe Transparenz hinsichtlich des Umganges und der Verwendung der gewonnenen Informationen sind eine wesentliche Voraussetzung, um einen offenen Kommunikationsprozess zu schaffen, der als Grundvoraussetzung für einen effizienten und effektiven Continuous Auditing Prozess anzusehen ist.

¹⁴ Vgl. Roth, Thomas Christoph, Geschäftsstellenrating: Weiterentwicklung risikoorientierter Prüfungsansätze, RevisionsPraktiker 02-03/2013, Seite 33 ff.

Wie zuvor dargestellt, benötigt die Interne Revision in erheblichem Umfang Daten von den Fachbereichen. Die Datenbeschaffung ist i.d.R. mit hohem Aufwand und Ressourcenbedarf verbunden. Daneben sind Ziel, Zweck und Vorteile dieser Vorgehensweise im Rahmen des Business Partner Ansatzes zu vermitteln. Leicht könnte sonst bei den Fachbereichen der Eindruck entstehen, dass diese unter eine permanente Kontrolle durch die Interne Revision gestellt werden und ein erhöhter Arbeitsaufwand entsteht, obwohl dieser durch das Continuous Auditing tatsächlich durch Steigerung der Risikoorientierung reduziert werden soll.

Weiterhin besteht die Notwendigkeit eines offenen Umgangs mit der Vorgehensweise und den gewonnenen Erkenntnissen durch die Interne Revision. Bei den Fachbereichen darf nicht der Eindruck entstehen, dass erhaltene Informationen „gegen den Fachbereich verwendet“ werden. Insbesondere ist bei der Weiterverarbeitung der Informationen in Form von Berichten darauf zu achten, den Fachbereich nicht zu übergehen.

Auf folgende Punkte (nicht abschließend) ist im Rahmen einer offenen Kommunikation mit dem Fachbereich besonderer Wert zu legen:

- Klare Kommunikation der Zielsetzung (Steigerung der Risikoorientierung, verbesserte Kommunikation „auf Augenhöhe“)
- Darlegung der Vorteile für die Fachbereiche (u. a. geringerer Vor-Ort-Aufwand bei Revisionsprüfungen durch effizientere Prüfungsplanung und Informationsaustausch)
- Dem Fachbereich die Möglichkeit zu geben, Auffälligkeiten und Probleme auch außerhalb von offiziellen Prüfungen mit der Internen Revision zu erörtern und zu lösen
- Klare Darlegung, welche Informationen für welche Berichte der Internen Revision genutzt werden und Einbindung des Fachbereiches in den Verteilerkreis
- Regelmäßige Feedback-Runden, um Missverständnisse frühzeitig zu erkennen und auszuräumen.

8 Prüfung von Auslagerungen und IKT-Drittdienstleistungen

8.1 Vorbemerkungen

Nachfolgend wird die Umsetzung der nach MaRisk und der Verordnung (EU) 2022/2554 Digital Operational Resilience Act (DORA) bestehenden Pflicht zur Prüfung ausgelagerter Aktivitäten und Prozesse durch die Interne Revision beschrieben.

DORA regelt die Steuerung der Risiken aus IKT-Drittdienstleistungen. Dadurch entstanden für Auslagerungen „mit IKT-Bezug“ Überschneidungen zur bisherigen KWG/MaRisk-Regulatorik. Daher wurde von der EBA am 07.08.2025 ein Konsultationspapier zu den Guidelines on the sound management of third-party risk veröffentlicht. Die sich hieraus ergebenden Anpassungen werden in einer der kommenden MaRisk-Novellen berücksichtigt.

Generell sollte die Interne Revision dabei auf den etablierten Prozessen zum Management von Auslagerungsvorhaben und bestehenden Auslagerungsbeziehungen aufsetzen.

8.2 Handlungsrahmen nach MaRisk und DORA

Gemäß AT 4.4.3 Tz. 3 MaRisk hat die Interne Revision „risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse zu prüfen und zu beurteilen, unabhängig davon, ob diese ausgelagert sind oder nicht.“

Die Möglichkeit, bestimmte Aktivitäten und Prozesse unter Risikogesichtspunkten von der Prüfung auszunehmen („grundsätzlich aller Aktivitäten und Prozesse“), besteht hier zunächst auch für ausgelagerte Bereiche und IKT-Drittdienstleistungen.

Bei **wesentlichen Auslagerungen** bzw. im Fall von nicht wesentlichen Auslagerungen, sofern abzusehen ist, dass diese Auslagerungen in naher oder mittlerer Zukunft wesentlich werden könnten, sind gemäß AT 9 Tz. 7 h) MaRisk im Auslagerungsvertrag „angemessene Informations- und Prüfungsrechte der Internen Revision“ zu vereinbaren. Die Informations- und Prüfungsrechte umfassen auch die für den Zutritt, Zugang oder Zugriff erforderlichen Rechte.

Beim **Bezug kritischer oder wichtiger IKT-Drittdienstleistungen** sind gemäß Delegierter Verordnung (EU) 2024/1773 (DORA RTS 1773) Art 30 Abs. 3 lit i) uneingeschränkte Zugangs-, Inspektions- und Auditrechte einzuräumen.

Bei **nicht wesentlichen Auslagerungen** bzw. **nicht kritischen oder wichtigen IKT-Drittdienstleistungen** sollte die Prüfung der ausgelagerten Aktivitäten und Prozesse risikoorientiert im Rahmen der jeweiligen Prozessprüfung des betreffenden Prüfobjektes erfolgen. Darüber hinaus sollte der Prozess der Überwachung der nicht wesentlichen Auslagerungen Gegenstand einer risikoorientierten Prüfung der Prozesse des zentralen Auslagerungsmanagements sein.

Die Interne Revision kann gemäß BT 2.1 Tz. 3 MaRisk im Fall von Auslagerungen auf ein anderes Unternehmen auf **eigene Prüfungshandlungen verzichten**, „sofern die anderweitig durchgeführte Revisionstätigkeit den Anforderungen in AT 4.4.3 und BT 2 genügt“. In diesem Fall hat sich die Interne Revision des auslagernden Instituts „von der Einhaltung dieser Voraussetzungen regelmäßig zu überzeugen. Die für die Gesellschaft relevanten Prüfungsergebnisse sind an die Interne Revision der auslagernden Gesellschaft weiterzuleiten.“

Verfügt das andere Unternehmen über eine **eigene Interne Revision** oder **wird die Revisionsfunktion anderweitig übernommen**, so hat sich die Interne Revision von deren Ordnungsmäßigkeit zu überzeugen und entscheidet auf Basis der Ergebnisse über die Notwendigkeit zur Durchführung eigener (ergänzender) Prüfungshandlungen.

Eine **anderweitig durchgeführte Interne Revision** kann übernommen werden durch:

- die Interne Revision des Auslagerungsunternehmens
- die Interne Revision eines oder mehrerer der auslagernden Institute im Auftrag der auslagernden Institute
- einen vom Auslagerungsunternehmen beauftragten Dritten
- einen von den auslagernden Instituten beauftragten Dritten

Die zuvor genannten Möglichkeiten der anderweitig durchgeführten Revision ergeben sich lt. DORA RTS 1773 Art 6 Abs. 3 auch für die Prüfung von **IKT-Drittdienstleistern**.

Daneben kann die Interne Revision im Rahmen ihrer Revisionshandlungen auch auf Nachweise/Zertifikate auf Basis gängiger Standards (z. B. IDW PS 951 Typ 2, SOC 2 Typ 2, ISO 27001) zurückgreifen. Hierbei sind sowohl die Detailtiefe, Aktualität und Eignung der Nachweise/Zertifikate und der zugehörigen Prüfberichte als auch die Eignung des Zertifizierers oder Prüfers zu berücksichtigen (Erläuterung zu BT 2.1 Tz. 3 MaRisk).

Die Nachweise/Zertifikate sollten eine Beurteilung folgender Aspekte ermöglichen:

- Wurde die ausgelagerte Aktivität bzw. der Prozess im Rahmen der Zertifizierung vollständig erfasst?
 - Abgleich mit den Leistungen lt. Auslagerungsvertrag

- Erfüllung der relevanten aufsichtsrechtlichen Verpflichtungen
- Ermöglicht der Nachweis/das Zertifikat eine Beurteilung der Leistungserbringung?
 - Qualitative und quantitative Ressourcenausstattung
 - Angemessenheit und Wirksamkeit dienstleistungsbezogener Kontrollen
 - Erfüllung übergreifender Sicherungsmaßnahmen: Informationssicherheit, Datenschutz und Notfallmanagement
 - Angemessenheit und Vollständigkeit von Berichtswesen und Informationspflichten (auch ad-hoc, z. B. bei Informationssicherheitsvorfällen)

Geeignete Zertifizierer sind z. B. (Wirtschafts-) Prüfungsgesellschaften oder zertifizierte Sachverständige und Prüfer.

Das Ergebnis der Beurteilung ist nachvollziehbar zu dokumentieren. Bei **wesentlichen Auslagerungen** kann sich die Interne Revision dabei nicht ausschließlich auf Nachweise/ Zertifikate auf Basis gängiger Standards stützen. In diesem Fall sind z. B. ergänzend Prüfungen der Auslagerungssteuerung und -überwachung, analytische Prüfungshandlungen zur Qualität der erbrachten Leistung oder Interviews bzw. Vor-Ort-Prüfungen (bei Mehrmandanten-Dienstleistern auch im Rahmen von sogenannten „Joint Audits“ oder „Pooled Audits“) denkbar.

Entscheidend ist, dass durch den Verzicht auf eigene Prüfungshandlungen keine „weißen Flecken“ in der Prüfungsplanung entstehen.

Für die Prüfung von IKT-Drittdienstleistern gelten, sofern es sich um kritische oder wichtige IKT-Drittdienstleistungen handelt, gemäß DORA RTS 1773, Art 8 Abs. 3 weitergehende Anforderungen.

Die Interne Revision des auslagernden Instituts darf sich demnach auch bei kritischen oder wichtigen IKT-Drittdienstleistern nicht längerfristig nur auf Zertifizierungen Dritter verlassen. Diese Instrumente darf sich die Interne Revision des auslagernden Instituts nur heranziehen, wenn sie

- die mandantenrelevante Prüfungsplanung bzw. das Planungsmodell des IKT-Drittdienstleisters für die einschlägigen vertraglichen Vereinbarungen als zufriedenstellend erachtet,
- sicherstellt, dass der Umfang der Zertifizierungen oder Prüfungsberichte die von ihm ermittelten Systeme und wesentlichen Kontrollen abdeckt und die Einhaltung der einschlägigen rechtlichen Anforderungen gewährleistet,
- den Inhalt der Zertifizierungen oder Prüfungsberichte laufend gründlich bewertet und prüft, ob diese nachvollziehbar sind,

- sicherstellt, dass wesentliche Systeme und Kontrollen in künftigen Fassungen der Zertifizierung oder des Prüfungsberichts berücksichtigt werden,
- die zertifizierende oder prüfende Stelle bzw. Funktion in für geeignet hält;
- davon überzeugt ist, dass die Zertifizierungen und Prüfungen auf der Grundlage anerkannter, einschlägiger professioneller Standards durchgeführt werden und die Prüfung die Angemessenheit und Wirksamkeit wesentlichen Kontrollen umfasst,
- das vertragliche Recht hat, Änderungen des Umfangs der Zertifizierungen oder Prüfungen mit Blick zu verlangen,
- das vertragliche Recht hat, nach eigenem Ermessen Ergänzungsprüfungen bzw. Pooled Audits im Zusammenhang mit den vertraglichen Vereinbarungen durchzuführen und diese Rechte in der vereinbarten Häufigkeit wahrzunehmen.

Verfügt bei wesentlichen Auslagerungen das Auslagerungsunternehmen bzw. der kritische oder wichtige IKT-Drittdienstleister über **keine eigene Interne Revision bzw. anderweitig durchgeführte Interne Revision** und ist ein Rückgriff auf Nachweise/ Zertifikate auf Basis gängiger Standards nicht möglich, ist der ausgelagerte Prozess im Rahmen der risikoorientierten Prüfungsplanung zu berücksichtigen und entsprechende Prüfungshandlungen sind auf der Basis der vertraglich eingeräumten Prüfungs- und Informationsrechte durchzuführen.

Das nachfolgende Schaubild zeigt den seitens der Internen Revision durchzuführenden Entscheidungsprozess für **wesentliche** Auslagerungen bzw. kritische oder wichtige IKT-Drittdienstleister im Hinblick auf die Notwendigkeit eigener Prüfungshandlungen:

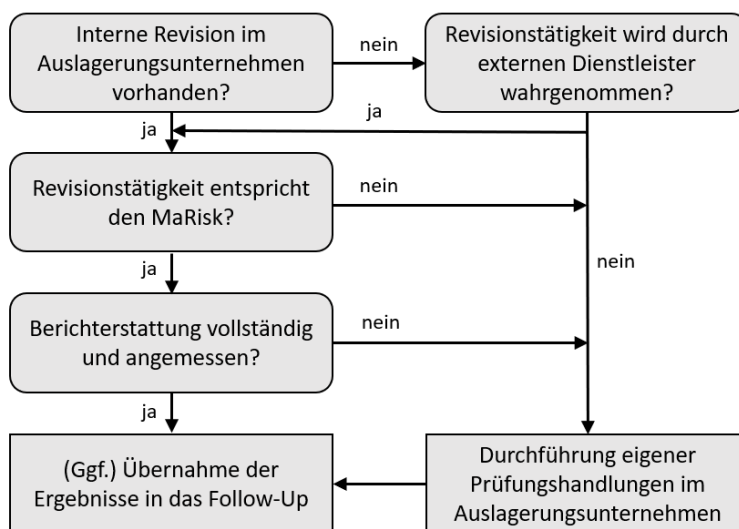


Abb. 14: Notwendigkeit eigener Prüfungshandlungen, Vgl. DIIR, Arbeitskreis „MaRisk“, ZIR 3/2008, Seite 128

8.3 Prüfung ausgelagerter Aktivitäten und Prozesse

Unternehmen, die wesentliche Dienstleistungen bzw. kritische oder wichtige IKT-Dienstleistungen für das Institut erbringen, sind grundsätzlich im Drei-Jahres-Turnus, ggf. auch Vor-Ort, zu prüfen. Die wesentlichen Auslagerungen bzw. kritisch oder wichtigen IKT-Drittdienstleistungen sind zu diesem Zweck in die Prüfungsplanung aufzunehmen und mindestens jährlich bzw. anlassbezogen auf Vollständigkeit zu prüfen. Dabei ist es unerheblich, ob die ausgelagerten Aktivitäten und Prozesse bei einer Prozessprüfung hinterlegt werden, oder das Auslagerungsunternehmen bzw. der IKT-Drittdienstleister als eigenes Prüfobjekt geführt wird.

Als nicht wesentlich qualifizierte Auslagerungen bzw. nicht kritische oder wichtige IKT-Drittdienstleistungen müssen aufgrund des geringeren Risikogehalts grundsätzlich nicht als separates Prüfobjekt in die Prüfungsplanung aufgenommen werden. Sie sind jedoch zu erheben und ggf. risikoorientiert in die relevanten prozessbezogenen Prüfungen des entsprechenden Prüfobjektes einzubeziehen. Dabei ist insbesondere auf die Wirksamkeit der operativen Auslagerungssteuerung und -überwachung abzustellen.

Bei der Identifizierung ausgelagerter Aktivitäten und Prozesse sowie der IKT-Drittdienstleistungen für die Revisionstätigkeit kann sich die Interne Revision auf die Prozesse des Auslagerungsmanagements und das zentral geführte Auslagerungsregister bzw. das Informationsregister stützen. Zumindest einmal jährlich im Rahmen der Prüfungsplanung ist ein Abgleich zwischen dem Auslagerungsregister bzw. dem Informationsregister und den Prüfobjekten der Internen Revision durchzuführen. Nach Aufstellung des Prüfungsplans und dessen Genehmigung durch die Geschäftsleitung sind die für das Planjahr vorgesehenen Prüfungen von **wesentlichen Auslagerungen** ebenso wie der Zeitpunkt der diesbezüglichen letzten Prüfung für eine Erfassung im Auslagerungsregister an den Auslagerungsbeauftragten zu melden (vgl. EBA GL on Outsourcing Tz. 55 lit. f. Das betreffende Feld ist im Format TT/MM/JJJJ zu melden. Da das genaue Prüfungsdatum i. d. R. nicht feststeht, wird in der Praxis häufig 31/12/JJJJ angegeben.

8.3.1 Neuauslagerung wesentlicher Aktivitäten und Prozesse bzw. IKT-Dienstleistungen

Die Interne Revision ist im Rahmen ihrer Aufgaben an der der Auslagerungsentscheidung bzw. im Fall eines neuen IKT-Drittdienstleistung an der vorgeschalteten Risikoanalyse bzw. Risikoermittlung zu beteiligen (AT 9, Tz. 2 MaRisk bzw. DORA Art. 6 Abs. 6). Hierbei steht zunächst die Information der Internen Revision und damit die Möglichkeit, auf eine Veränderung der Risikosituation zu reagieren, im Vordergrund.

Daneben ist bei neuen wesentlichen Auslagerungsverhältnissen sowie kritischen oder wichtigen IKT-Drittdienstleistungen im Rahmen des Auslagerungsprozesses sicherzustellen, dass der Internen Revision vertraglich angemessene Informations- und Prüfungsrechte zugesichert werden (AT 9 Tz. 7 h MaRisk bzw. DORA RTS 1773 Art 30 Abs. 3 lit. i)). Dies gilt auch im Fall von wesentlichen Weiterverlagerungen bzw. Unterbeauftragungen durch das Auslagerungsunternehmen/ den IKT-Drittdienstleister.

Die Handhabung der Informations- und Prüfungsrechte in Bezug auf das jeweilige Auslagerungsverhältnis ist im Rahmen des Auslagerungsprozesses und der Vertragsverhandlungen zu klären und ggf. weiter zu spezifizieren. Die Interne Revision ist auch insofern in den Auslagerungsprozess einzubeziehen.

8.3.2 Durchführung eigener Prüfungshandlungen beim Auslagerungsunternehmen und Berichterstattung

8.3.2.1 Eigene Prüfungshandlungen

Ausgelagerte Aktivitäten und Prozesse werden im Rahmen der relevanten Prüfobjekte (i.d.R. Prozesse) der risikoorientierten Prüfungsplanung adressiert. Für wesentliche Auslagerungen und für wesentliche Weiterverlagerungen sowie für kritische oder wichtige IKT-Drittdienstleistungen ist grundsätzlich vorzusehen, dass zumindest im Drei-Jahres-Turnus eine Prüfung (vor Ort/ Remoteprüfung) stattfindet. Sofern der Einbezug in eine Prozessprüfung nicht sinnvoll erscheint, kann für wesentliche Auslagerungen bzw. kritische oder wichtige IKT-Drittdienstleistungen auch ein eigenes Prüfobjekt angelegt werden.

Im Vorfeld der Prüfung ist eine grundsätzliche Abstimmung mit dem Auslagerungsbeauftragten und dem Auslagerungsunternehmen, insbesondere in logistischer Hinsicht (Zeitraum, Ansprechpartner, benötigte Zugangs- und Zugriffsrechte, vorab bereitzustellende Unterlagen/Daten sowie ggf. anfallende Kosten) herbeizuführen.

Sollte es bei Prüfungshandlungen im Auslagerungsunternehmen zu nachhaltigen Einschränkungen der Prüfungs- und Informationsrechte kommen, sind diese Einschränkungen unverzüglich zur weiteren Eskalation, z. B. an den Leiter der Internen Revision des Instituts, zu melden.

Prüfungsfeststellungen, die voraussichtlich eine Mängelbeseitigung durch das Auslagerungsunternehmen erfordern, sollten auf sachliche Richtigkeit mit den Ansprechpartnern des Auslagerungsunternehmens besprochen werden, um Fehleinschätzungen oder Missverständnissen vorzubeugen.

Der Prüfungsbericht richtet sich jedoch an den auslagernden Fachbereich im Institut (Auslagerungsbeauftragten) und wird mit diesem schlussbesprochen, da die Interne Revision nicht direkt in die Vertragsbeziehung mit dem Auslagerungsunternehmen eingreifen kann. Maßnahmen, die vom Auslagerungsunternehmen umzusetzen sind, sind daher im Rahmen der Auslagerungssteuerung vom Auslagerungsbeauftragten zu koordinieren.

8.3.2.2 Zusammenarbeit in gemeinschaftlichen Prüfungen bzw. Sammelprüfungen („Pooled Audits“)

Die MaRisk ermöglichen in BT 2.1 Tz. 3 unter Einbezug der Erläuterungen das Instrument der gemeinschaftlichen Prüfung durch die jeweilige Interne Revision der auslagernden Institute bei Mehrmandantendienstleistern. Auch die EBA Outsourcing Guideline (EBA/GL/2019/02¹⁵) und nicht zuletzt die EU-Verordnung über die digitale operationale Resilienz im Finanzsektor (kurz DORA, VO/EU/2022/2554¹⁶) erwähnen beispielhaft dieses Instrument.¹⁷

Darüber hinaus wurde das Instrument gemeinschaftlicher Prüfungen bzw. Pooled Audits vor dem Hintergrund der zunehmenden Anzahl von Auslagerungen an Cloud Service Provider (CSP) explizit durch Aufsichtsbehörden aufgegriffen. Sammelprüfungen werden insbesondere im Merkblatt der BaFin „Orientierungshilfe zu Auslagerungen an Cloud-Anbieter“¹⁸ und in den „Leitlinien zur Auslagerung an Cloud-Anbietern“¹⁹ der European Securities and Markets Authority (ESMA) erwähnt.

In der Folge haben sich mehrere institutsübergreifende Zusammenschlüsse (z. B. Collaborative Cloud Audit Group (CCAG), Switching Cloud Providers and Porting Data (SWIPO), European Cloud User Coalition (ECUC)) formiert, die gemeinschaftliche Prüfungshandlungen bei Cloud Service Providern organisieren und durchführen. Dies erfolgt vor allem mit dem Ziel einer starken Interessenvertretung der auslagernden Institute gegenüber den Cloud Service Providern, einer Wissensbündelung in den Prüfungen durch breiten Einbezug spezialisierter Prüffressourcen sowie zur Nutzung von Synergien und Effizienzen auf Seiten der prüfenden Institute und der Cloud Service Providern.

¹⁵ Vgl. European Banking Authority (EBA), Guidelines on outsourcing arrangements, dt. Titel: Leitlinien zu Auslagerungen, (EBA/GL/2019/02), vom 25. Februar 2019.

¹⁶ Vgl. Europäische Union (EU), Art. 28 Nr.6 (2) Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act), vom 14. Dezember 2022.

¹⁷ Kap. 7.3.2.2 basierte ursprünglich auf einem Exzerpt aus Rillinger/Luhmer, in ZIR 06.23, Titel: Zusammenarbeit in gemeinschaftlichen Prüfungen bzw. Sammelprüfungen („Pooled Audits“).

¹⁸ Vgl. Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, vom 08. November 2018.

¹⁹ Vgl. European Securities and Markets Authority (ESMA), Guidelines on outsourcing to cloud service providers, vom 10. Mai 2021.

Sofern die Interne Revision sich im Rahmen einer Sammelprüfung mit anderen Revisionen gemeinschaftlich an einer Prüfung beteiligt, stellt sich aber grundsätzlich die Frage, inwieweit es sich hierbei wiederum um eine Auslagerung i. S. d. § 25b KWG handeln könnte. Um eine Auslagerung kann es sich grundsätzlich immer dann handeln, wenn ein Prozess oder eine Tätigkeit an ein anderes Unternehmen übertragen wird. Wesensinhalt der Definition ist demnach, dass ein Prozess eine Tätigkeit, oder im Falle einer großen Vielzahl an gleichen Vorgängen eine gewisse Anzahl an Vorgängen, durch die Übertragung ohne eigenes Zutun des Instituts erfolgt. Dies bedeutet im Gegenzug, dass Prozesse und Tätigkeiten, bei denen die operative Durchführung in allen wesentlichen Elementen durch das Institut selber erfolgt, keine Auslagerung darstellen. Bezogen auf die Revisionstätigkeit und hier insbesondere auf das Element der Sammelprüfungen sind folgende Kernelemente des Revisionsprozesses zu betrachten:

- Jahres- und Mehrjahresprüfungsplanung
- Risikoanalyse des Prüfungsfelds bzw. -objekts
- Detailplanung der Prüfung und Festlegung des Prüfungsprogramms
- Beschaffung der notwendigen Informationen und Nachweise
- Identifizierung von Risiken und Feststellungen
- Berichterstattung
- Dokumentation
- Nachverfolgung von Feststellungen/Mängeln („Follow-up“)

Jedes Institut ist für die eigene **Jahres- und Mehrjahresprüfungsplanung** selbst verantwortlich, so dass jeder Teilnehmer eine eigene Prüfungsplanung nach den eigenen Methoden und auf Basis der individuellen Risikoeinschätzung vorzunehmen und institutsintern zu dokumentieren hat. Eine Sammelprüfung kann damit ein wirksames Mittel der individuellen Prüfungsabdeckung darstellen, kann aber die individuelle Prüfungsplanung nicht ersetzen.

Gleiches gilt für die **Analyse des Risikos des gemeinschaftlich geprüften Prüfungsfelds bzw. -objekts**. Neben sachlichen Gründen wie unterschiedlich bezogene Dienstleistungen können auch das unternehmensindividuelle Kontrollumfeld oder nicht zuletzt der Risikoappetit zu unterschiedlichen Risikoeinschätzungen führen. Dies allein steht aber einer gemeinschaftlichen Prüfung nicht entgegen.

Basierend auf den Risikoeinschätzungen der Teilnehmer ist dann eine gemeinsame **Detailplanung der Prüfung** zu erstellen. Ob dabei die Prüfung lediglich die gemeinsame Schnittmenge der Elemente beinhaltet oder als Vereinigungsmenge aller Themen und Kontrollen aller Teilnehmer gestaltet wird, ist jeweils festzulegen. In der Praxis wird es

aber nicht auszuschließen sein, dass aus Sicht einzelner Teilnehmer nicht alle notwendigen Themenfelder adressiert werden. In diesem Fall sind geeignete weitere Prüfungshandlungen zu planen. Diese können individuell durchgeführt werden oder es können andere Quellen wie externe Zertifikate zur Gewinnung von Prüfungssicherheit genutzt werden²⁰.

Ebenso erfolgt in dieser Phase die **Festlegung der gemeinschaftlich durchgeführten Prüfungshandlungen**. In der Praxis erweist es sich als hilfreich, sich unter den Teilnehmern auf einen gemeinsamen Kontrollstandard zu einigen. Da die Interne Revision eine gewisse Freiheit in der Methodenwahl hat, ist dies meist mit den internen Regularien der teilnehmenden Revisionen vereinbar.

Nächster Schritt ist die **Beschaffung der Unterlagen und Nachweise**. Dazu werden Unterlagen angefordert, Interviews geführt und geeignete andere Prüfungshandlungen wie Auswertungen vorgenommen. Letztendlich handelt es sich um eine Strukturierung der Informationen ggf. nach dem Schema einer vorher festgelegten Anforderung. Auch wenn dies mitunter ein aufwändiger Prozess sein mag, handelt es sich bei der Informationsbeschaffung um eine unterstützende Tätigkeit. Für eine Sammelprüfung bedeutet dies, dass ein Mitglied des gemeinsamen Revisionsteams die Gegenüberstellung der Anforderungen und der Informationen vornehmen und Abweichungen aufzeigen kann. Diese ist bspw. in Form einer Liste von Beobachtungen möglich.

Basierend auf den erhobenen Informationen findet dann eine Auswertung, Analyse und Risikobewertung der Erkenntnisse statt, die die **Identifizierung von Risiken und Feststellungen** zum Ziel hat. Diese Identifizierung ist der eigentliche Kern der Revisionstätigkeit. Dabei werden durch jeden Teilnehmer alle Unterlagen und Listen von Beobachtungen durchgesehen und unternehmensindividuell ausgewertet. Dabei erkannte Schwächen in der Prüfungsarbeit sollten im Prüfungsteam offengelegt und besprochen und idealerweise direkt abgestellt werden. Im Bedarfsfall hat jedes Institut weitere Prüfungshandlungen anzuregen oder selber durchzuführen, um den jeweiligen Prüfungsauftrag umzusetzen. Auf Basis dieser Erkenntnisse hat jeder Teilnehmer seine individuellen Feststellungen zu treffen und gemäß den eigenen Vorgaben in Risikokategorien einzustufen. Dabei kann auf die Liste der Beobachtungen zurückgegriffen werden, eine deckungsgleiche Einwertung der Teilnehmer ist aber nicht notwendig und in der Praxis unwahrscheinlich.

Aufgrund der individuellen Risikobewertung ist eine gemeinsame **Berichterstattung** wenig zielführend. Dem steht nicht entgegen, dem Mehrmandantendienstleister die Liste der Beobachtungen zur Verfügung zu stellen. Im Hinblick auf die spätere Mängelverfolgung ist dies auch sachgerecht und geboten. Für die jeweiligen Teilnehmer bleibt damit

²⁰ Vgl. EBA/GL/2019/02 Tz. 91 lit. b und Erläuterungen zu BT 2.1 Tz. 3 MaRisk.

die Aufgabe, aufbauend auf den gemeinsamen Unterlagen einen eigenständigen Revisionsbericht zu erstellen.

Die notwendige **Dokumentation** nach BT 2.4 Tz. 2 MaRisk obliegt jeder einzelnen teilnehmenden Internen Revision gemäß den individuellen internen Vorgaben. In der operativen Organisation ist daher sicherzustellen, dass allen Teilnehmern alle Unterlagen dauerhaft zur Verfügung stehen.

Hinsichtlich der **Mängelverfolgung** sind die gleichen Grundsätze anzuwenden wie bei der Prüfung als solches. Wichtig ist die Festlegung, dass alle risikorelevanten Entscheidungen jeweils durch die Interne Revision der einzelnen Institute getroffen werden. Durch dieses Vorgehen werden alle wesentlichen Prozessschritte weiterhin in den teilnehmenden Instituten der gemeinschaftlichen Prüfung vorgenommen, was dem Charakter einer Auslagerung entgegensteht. Bei den empfangenen Dienstleistungen handelt es sich demnach eher um Hilfsdienste in Form einer Informationsbeschaffung und -aufbereitung. Dieses aber erfüllt die Definition des sonstigen Fremdbezugs und nicht die einer Auslagerung bzw. eines Auslagerungsverhältnisses. Dies bedeutet jedoch auch, dass gewisse Qualitätssicherungsmaßnahmen zwingend eingehalten werden müssen. Diese umfassen unter anderem die Qualifikation der eingesetzten Mitarbeitenden, die Überwachung der Beistelleistungen sowie die sorgfältige und angemessene Dokumentation.

Soweit und solange die oben beschriebenen wesentlichen Elemente der Revisionsprozesse bei den teilnehmenden einzelnen Internen Revisionen verbleiben, handelt es sich bei „Pooled Audits“ bzw. Sammelprüfungen nach Auffassung des DIIR AK MaRisk nicht um Auslagerungen i. S. d. § 25b KWG bzw. der MaRisk und den Leitlinien zu Auslagerungen der EBA.

8.3.3 Handhabung der Internen Revision bei anderweitiger Durchführung der Revisionstätigkeit für Auslagerungen

8.3.3.1 Regelmäßige Beurteilung der anderweitig durchgeführten Revisionstätigkeit

Sofern das Auslagerungsunternehmen über eine Interne Revision verfügt und die Interne Revision des auslagernden Instituts beabsichtigt, auf eigene Prüfungshandlungen zu verzichten, ist einmal jährlich - i.d.R. mit Abschluss des Prüfungsjahres - die anderweitig durchgeführte Revisionstätigkeit auf Übereinstimmung mit AT 4.4 und BT 2 MaRisk zu beurteilen.

Diese Beurteilung ist auch gem. DORA RTS 1773 Art 8 Abs. 3 Voraussetzung für den Rückgriff auf Zertifizierungen Dritter oder Berichte über interne oder von Dritten durchgeführte Prüfungen, die vom IKT-Drittdienstleister zur Verfügung gestellt werden.

Zu beurteilen ist insbesondere:

- Die Übereinstimmung der Revisionstätigkeit mit AT 4.4.3 und BT 2 MaRisk
- die Angemessenheit und Relevanz der Berichterstattung in Bezug auf die ausgelagerten Aktivitäten und Prozesse und deren Risikogehalt
- die Notwendigkeit weiterer Maßnahmen, wie z. B. Ergänzungsprüfungen

Zur Beurteilung können eines oder mehrere der folgenden Dokumente herangezogen werden:

- ein von einer deutschen Wirtschaftsprüfungsgesellschaft erstellter Bericht über die Prüfung der Internen Revision nach MaRisk
- ein Auszug aus dem Bericht des Abschlussprüfers (bei einem inländischen Institut)
- ein nach einem (internationalen) Standard (ISAE 3402 Typ II, IDW PS 951 Typ B) erstellter Bericht über die Funktionsfähigkeit und Angemessenheit Interne Revision nach MaRisk
- ergänzend sind offenkundige Mängel aus der Analyse der Verfügung gestellten Berichte der anderweitig durchgeführten Internen Revision und aus Erkenntnissen der Auslagerungssteuerung (Vertragsverletzungen, Nicht-Einhaltung der Servicelevel, Schäden, ...) bei der Beurteilung zu berücksichtigen

Bei der Beurteilung der Angemessenheit der Prüfungsplanung sollte sich die Interne Revision vergewissern, ob die anderweitig durchgeführte Revision die ausgelagerten Aktivitäten und Prozesse und die damit verbundenen regulatorischen Anforderungen vollständig und in angemessenem Turnus in ihre Prüfungsplanung aufgenommen hat.

Bei komplexen Auslagerungen, kritisch oder wichtigen Drittdienstleistungen oder bestehenden Unklarheiten, sollte einmal jährlich eine Abstimmung von Prüfungsinhalten mit der Internen Revision des Auslagerungsunternehmens erfolgen, um „weiße Flecken“ zu vermeiden.

Exkurs:

Soweit das Auslagerungsunternehmen selbst nicht beaufsichtigt ist oder sich im Ausland befindet, sind die MaRisk i.d.R. unbekannt. Häufig wird jedoch von den entsprechenden Unternehmen ein Bericht nach internationalen Standards (z. B. ISAE 3402 Typ II, SOC 2 Typ 2) in Bezug auf die ausgelagerte Dienstleistung angeboten. Dieser wäre dann um die einschlägigen Anforderungen der MaRisk an die Interne Revision zu ergänzen.

Der AK MaRisk hat diese Anforderungen daher in Formate überführt, die von einem Wirtschaftsprüfer zur Beurteilung der Internen Revision im Rahmen einer Prüfung nach ISAE

3402 Typ II verwendet werden können (Anlagen 2 bis 4) und auf der Webseite des DIIR verfügbar sind.

8.3.3.2 Auswertung der Berichte der anderweitig durchgeführten Internen Revision

Die Interne Revision des Auslagerungsunternehmens hat die relevanten Prüfungsergebnisse an das auslagernde Institut weiterzuleiten (vgl. BT 2.1 Tz. 3 MaRisk). Die Relevanz ist dabei aus Sicht des auslagernden Instituts zu beurteilen. Als relevant sollten in diesem Zusammenhang nennenswerte Fehler oder Mängel in der vertraglich geschuldeten Leistung, die außerhalb ggf. vereinbarte Toleranzgrenzen liegen sowie Feststellungen zu Mängeln im Prozess oder im internen Kontrollsystem, die das Fehlerrisiko in Bezug auf die vertraglich geschuldeten Leistungen wesentlich erhöhen (vgl. AT 9 Tz. 7 lit. e) MaRisk) eingestuft werden.

Sofern Mängel oder einzelne Prüfungsfeststellungen mitgeteilt werden, sollten zu den einzelnen Prüfungsberichten im Anschluss auch regelmäßige Berichte über den Stand der Mängelverfolgung übersendet werden.

Grundsätzlich ist sowohl für die Berichterstattung zu den relevanten Prüfungsergebnissen als auch zum Stand der Mängelverfolgung eine jährliche Berichterstattung ausreichend. Je nach Umfang und Risikogehalt der ausgelagerten Aktivitäten und Prozesse, kann jedoch auch ein kürzerer Turnus (halbjährlich bzw. quartalsweise) angebracht sein. Wesentliche Feststellungen sollten dem auslagernden Institut unverzüglich mitgeteilt werden.

Die Berichte der anderweitig durchgeführten Revision sind direkt an die Interne Revision des Instituts zu adressieren. Diese überwacht, ob alle Berichte wie vorgesehen eingehen.

Nach Eingang sind die Berichte, die sich auf **wesentliche Auslagerungen bzw. kritische oder wichtige IKT-Drittdienstleistungen** beziehen, unverzüglich von der Internen Revision zu analysieren. Die mitgeteilten Prüfungsergebnisse oder Feststellungen sind dabei auf ihren Wirkungsgehalt mit Blick auf die ausgelagerten Dienstleistungen zu beurteilen. Gleichzeitig ist zu beurteilen, ob die Prüfungsergebnisse für die ausgelagerten Dienstleistungen einschlägig sind.

Dabei können auch Wertungshilfen von Verbänden bzw. von Gesellschaften, die ein zentrales Auslagerungsmanagement von Mehrmandantendienstleistern durchführen, herangezogen werden. In diesem Zusammenhang kann die Beurteilung der MaRisk-Konformität der anderweitig durchgeführten Internen Revision, die Auswertung der Berichte, die Ableitung von Maßnahmen und Ergänzungsprüfungen sowie die Durchführung des

Follow-up ganz oder teilweise ausgelagert werden. In diesem Fall muss seitens der Internen Revision des Instituts eine fachliche Überwachung der Ergebnisse dieser ausgelagerten „Internen Revision der Auslagerungen“ vorgenommen werden. Das Recht auf die Durchführung von Ergänzungsprüfungen bleibt dabei stets unberührt.

Sofern sich aus dieser Analyse wesentliche oder höher einzustufende Feststellungen ergeben, sind diese das eigene Follow-up und die daran anknüpfende Berichterstattung der Internen Revision zu übernehmen, um den Berichtspflichten gem. BT 2.4 und 2.5 MaRisk (Quartals- und Jahresberichterstattung sowie Eskalation) nachkommen zu können. Daneben ist über die Notwendigkeit weitergehender Revisionstätigkeiten, z. B. einer außerplanmäßigen Prüfung, zu befinden.

Es empfiehlt sich, seitens der Internen Revision zu jedem Bericht eine Notiz über die durchgeführten Analysen, die Ergebnisse sowie daraus ggf. abgeleitete Folgeaktivitäten zu erstellen. Der Bericht und die ergänzenden Analysen der Internen Revision sind zeitnah bzw. im Fall wesentlicher oder höher eingestufte Feststellungen unverzüglich an die zuständigen Stellen im Institut, insbesondere an den Auslagerungsbeauftragten und die verantwortlichen Fachbereiche, zu verteilen.

Über das Ergebnis ggf. durchgeführter, ergänzender Prüfungshandlungen hat die Interne Revision zu berichten.

Sofern nach dem Ergebnis der Analyse keine ergänzenden Prüfungshandlungen seitens der Internen Revision notwendig werden, kann die zeitnahe Weiterleitung der Berichte, der Analysen und der vorgesehenen Maßnahmen des Auslagerungsmanagements an die Geschäftsleitung auch durch das Auslagerungsmanagement bzw. den Auslagerungsbeauftragten erfolgen. Der Auslagerungsbeauftragte auf diese Weise seiner anlassbezogenen Berichtspflicht gemäß AT 9 Tz. 13 MaRisk nachkommen. Entsprechende Zuständigkeiten sind zu definieren.

Bei der Analyse der **Berichte über den Stand der Mängelverfolgung** bei wesentlichen Auslagerungen ist darauf zu achten, dass vollständig über die offenen Feststellungen berichtet wird und dass diese in angemessener Zeit erledigt werden. Über das Ergebnis des Follow-up hinsichtlich der offenen wesentlichen und aller höheren Mängel ist in den Quartals- und Jahresberichten der Internen Revision zu berichten.

Eine Aufnahme von bemerkenswerten oder geringen Mängeln in das eigene Follow-up und betreffende Berichterstattung der Internen Revision ist grundsätzlich nicht erforderlich, wenn bereits die anderweitig durchgeführte Interne Revision über ein wirksames Follow-up-Verfahren verfügt und die Mängel im Rahmen der Auslagerungssteuerung- und -überwachung berücksichtigt und nachverfolgt werden. In diesem Fall dient die Analyse der Berichte über den Stand der Mängelverfolgung durch die Interne Revision ledig-

lich der Überprüfung der Wirksamkeit des Follow-up-Verfahrens der anderweitig durchgeführten Internen Revision und kann ggf. in Stichproben durchgeführt werden (sofern z. B. die erteilte Bestätigung eines Wirtschaftsprüfers auch das Follow-up-Verfahren umfasst).

Bei **nicht wesentlichen Auslagerungen** stellen die von der Internen Revision des Auslagerungsunternehmens bereitgestellten Berichte hilfreiche Informationen für die Festlegung eines risikoorientierten Prüfungsturnus und -umfangs für die relevanten Prüfobjekte dar. Es ist keine aktive Anforderung und intensive Auswertung der Berichte notwendig.

8.3.3.3 Maßnahmen nach Auswertung der Berichte der anderweitig durchgeführten Internen Revision

Abhängig vom Ergebnis der Beurteilung der anderweitig durchgeführten Revisionstätigkeit sowie der Auswertung der vorgelegten Berichte sind folgende Maßnahmen möglich:

- a) Keine Aktivitäten erforderlich

Die Analyse ergab keine Feststellungen und es kann (weiterhin) auf eigene Prüfungshandlungen im Auslagerungsunternehmen verzichtet werden.

- b) Hinweis an den Auslagerungsbeauftragten

Kritische Sachverhalte, die eine Überwachung oder besondere Maßnahmen erfordern, werden an die für die Dienstleistersteuerung zuständige Stelle adressiert. Der entsprechende Schriftverkehr ist mit dem Bericht abzulegen und ggf. nachzuhalten.

Als „wesentlich“ und höher einzustufende Feststellungen der anderweitig durchgeführten Revisionsfunktion sind in das eigene Follow-up und die daran anknüpfende Berichterstattung zu übernehmen, um den Berichtspflichten gem. BT 2.4 und 2.5 MaRisk (Quartals- und Jahresberichterstattung sowie Eskalation) nachkommen zu können.

- c) Hinweis an die Interne Revision des Auslagerungsunternehmens

Sowohl zur Einholung von Hintergrundinformationen als auch zur Adressierung von methodischen, wie formalen Mängeln in der Tätigkeit oder der Berichterstattung kann es erforderlich sein, mit der Internen Revision bzw. der Geschäftsführung des Auslagerungsunternehmens in Kontakt zu treten. Die Kontaktaufnahme sollte über bzw. mit Kenntnisnahme des zuständigen Auslagerungsbeauftragten erfolgen.

Entsprechender Schriftverkehr ist abzulegen. Soweit erforderlich, ist eine Wiedervorlage einzurichten.

- d) Aufnahme eigener Prüfungen der ausgelagerten Leistungen bzw. Prozesse in die Prüfungsplanung

Insbesondere dann, wenn begründete Zweifel an der Funktionsfähigkeit und Wirksamkeit der Internen Revision des Dienstleisters bestehen, müssen eigene Prüfungshandlungen im Auslagerungsunternehmen in Betracht gezogen und entsprechend in die Prüfungsplanung aufgenommen werden. Das gilt auch, sofern die Prüfungsplanung der anderweitig durchgeführten Revision Lücken in Bezug auf die ausgelagerten Aktivitäten und Prozesse aufweist. Der Auslagerungsbeauftragte ist hierüber zu informieren.

- e) Durchführung einer außerplanmäßigen Prüfung

Bei besonderen Risiken kann die Durchführung einer unmittelbaren außerplanmäßigen Prüfung im Auslagerungsunternehmen erforderlich sein. In die hierfür notwendigen Vorbereitungen sollte der Auslagerungsbeauftragte einbezogen werden.

8.3.4 Exkurs: Auslagerung der Internen Revision

Eine vollständige oder teilweise Auslagerung der Internen Revision ist gem. AT 9 Tz. 10 MaRisk mit Einschränkungen möglich. Sie wird gem. AT 9 Tz. 2 MaRisk als Auslagerung von erheblicher Tragweite eingestuft, bei der im Rahmen der Risikoanalyse entsprechend intensiv zu prüfen ist, ob und wie der Einbezug der ausgelagerten Aktivitäten und Prozesse in das Risikomanagement (hier: die Funktion Interne Revision) sichergestellt werden kann. Im Rahmen der Vollauslagerung ist die Funktion des Revisionsbeauftragten zu etablieren, dessen Aufgaben in den MaRisk näher definiert werden (siehe unten). Bei einer Teilauslagerung sind vom Leiter der Internen Revision hinreichende Prozesse zur Überwachung der Tätigkeit des Dienstleisters zu definieren.

Auch die dauerhafte Übertragung von bestimmten Prüfungen an die Interne Revision des übergeordneten Unternehmens (Konzernrevision) kann zu einem Auslagerungsverhältnis führen (vgl. Protokoll der MaRisk-Fachgremiumssitzung vom 15.03.2018).

Sofern sich die Interne Revision lediglich externer Ressourcen oder Expertise bedient (Personalbeistellung), um eigene Prüfungen durchzuführen, ist nicht von einer Auslagerung der Internen Revision auszugehen. Dabei ist zu beachten, dass die Prüfungsdurchführung unter der Verantwortung und Steuerung der Internen Revision und nach deren Vorgaben erfolgt.

Die vollständige Auslagerung der Internen Revision ist gem. AT 9 Tz. 5 MaRisk nur in folgenden Fällen möglich:

- Bei Tochterinstituten innerhalb einer Institutsgruppe (an das Mutter- oder ein Schwesterunternehmen), sofern das auslagernde Institut sowohl hinsichtlich seiner

Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den nationalen Finanzsektor als auch hinsichtlich seiner Bedeutung innerhalb der Gruppe als nicht wesentlich einzustufen ist

- Bei Tochterinstituten innerhalb einer Gruppe, wenn das Mutterunternehmen kein Institut und im Inland ansässig und Auslagerungsunternehmen ist und das Tochterinstitut sowohl hinsichtlich Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den nationalen Finanzsektor als auch hinsichtlich der Bedeutung innerhalb der Gruppe als nicht wesentlich einzustufen ist
- Bei kleinen Instituten, sofern deren Einrichtung vor dem Hintergrund der Institutsgröße sowie der Art, des Umfangs, der Komplexität und des Risikogehalts der betriebenen Geschäftsaktivitäten nicht angemessen erscheint

In diesem Fall hat das Institut einen Revisionsbeauftragten zu benennen, der eine ordnungsgemäße Durchführung der Aufgaben unter Einhaltung von AT 4.4.3 und BT 2 MaRisk gewährleisten muss (AT 9 Tz. 10 MaRisk). Der Revisionsbeauftragte ist der Geschäftsleitung unmittelbar zu unterstellen.

Je nach Art, Umfang und Komplexität und Risikogehalt der Geschäftsaktivitäten des Instituts können die Aufgaben des Revisionsbeauftragten auch von einem Geschäftsleiter wahrgenommen werden.

Die Aufgaben des Revisionsbeauftragten sind in der zugehörigen Erläuterung näher spezifiziert:

- Erstellung des Prüfungsplans, gemeinsam mit dem beauftragten Dritten
- Verfassen des Gesamtberichts nach BT 2.4 Tz. 4, ggf. gemeinsam mit dem beauftragten Dritten
- Prüfung nach Maßgabe von BT 2.5, ob die festgestellten Mängel beseitigt wurden (Follow-up)

Die betreffenden Dokumente können vom beauftragten Dritten vorbereitet werden, sind jedoch stets vom Revisionsbeauftragten zu überprüfen und freizugeben.

Der Revisionsbeauftragte übernimmt somit, ggf. gemeinsam mit dem beauftragten Dritten, im Auslagerungsfall die Rolle des Leiters der Internen Revision. Die an diese Rolle anknüpfenden Vorgaben sind insofern zu beachten. Hierunter fallen z. B.:

- Adressat für die Einholung von Auskünften durch den Vorsitzenden des Aufsichtsorgans (AT 4.4.3 Tz. 2 MaRisk)
- Information des Aufsichtsorgans bei einem Wechsel (AT 4.4.3 Tz. 6 MaRisk)

- Unterrichtung des zuständigen Geschäftsleiters, wenn wesentliche Mängel nicht in angemessener Zeit beseitigt werden (BT 2.5 Tz. 2 MaRisk)
- Einschlägige Regelungen

9 Sonderprüfungen zur Aufklärung von Fraud

9.1 Einführung und Zielsetzung

Sofern ein Verdacht auf Fraud oder sonstige strafbare Handlungen innerhalb eines Instituts entstanden sein sollte, ist eine zeitnahe und lückenlose Aufklärung des Sachverhalts notwendig.

Nach der Definition des IIA umfasst Fraud jede illegale Handlung, die durch Täuschung, Verschleierung oder Vertrauensmissbrauch gekennzeichnet ist. Diese Handlungen sind dabei unabhängig von Gewaltandrohung oder von körperlicher Gewalt. Fraud wird begangen, um Geld, Eigentum oder Dienstleistungen zu erhalten, um Zahlungen oder den Verlust von Dienstleistungen zu vermeiden oder um einen persönlichen oder geschäftlichen Vorteil zu sichern. Der Fraud-Begriff umfasst auch die Korruption. Fraud kann zu Gunsten oder zu Lasten der Organisation stattfinden. Täter können Mitarbeiter oder Außenstehende sein.

Der deutsche Begriff der „dolosen Handlung“ kann mit der Definition von „Fraud“ gleichgesetzt werden.

Gemäß § 25h Abs. 1 KWG müssen Institute über ein angemessenes Risikomanagement sowie über interne Sicherungsmaßnahmen verfügen, die der Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstigen strafbaren Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können.

Während die Betrugsprävention und -aufklärung mit Kundenbezug in der Praxis regelmäßig Aufgabe der Zentralen Stelle nach § 25h Abs. 7 KWG ist, werden die Untersuchungen anlässlich möglicher doloser Handlungen bzw. die Aufklärung des Verdachts auf Manipulationen von Mitarbeitern häufig von der Internen Revision durchgeführt.

Selbstverständlich ist es auch möglich, dass alle Untersuchungen zur Aufdeckung von Fraud und sonstigen strafbaren Handlungen von der Zentralen Stelle wahrgenommen werden. Die Interne Revision wird in diesem Fall zeitnah über die Untersuchungsergebnisse unterrichtet und kann ggf. ergänzende Prüfungshandlungen vornehmen. Auch für den Fall, dass die Interne Revision die Sonderuntersuchung selbst durchführt, ist eine enge Kooperation mit der Zentralen Stelle zu empfehlen. Insbesondere, wenn andere Institute in den Ermittlungen eine Rolle spielen, sind die Kommunikationsmöglichkeiten der Zentralen Stelle mit diesen Instituten sehr viel weitgehender als die der Internen Revision.

Die MaRisk regeln in BT 2.3 Ziffer 4, dass sichergestellt sein muss, dass kurzfristig notwendige Sonderprüfungen, z. B. anlässlich deutlich gewordener Mängel oder bestimmter

Informationsbedürfnisse, jederzeit durchgeführt werden können. Diese Regelung umfasst auch die Aufklärung bzw. ergänzende Prüfung von Fraud-Sachverhalten.

Die einem Fraud-Sachverhalt zu Grunde liegenden Straftaten haben seit der Einführung des sogenannten All-crime-Ansatzes in der Geldwäschebekämpfung immer eine Relevanz zu dieser Thematik. Der bisherige Vortatenkatalog ist entfallen. Da der Geldwäschebeauftragte zur Abgabe einer Verdachtsmeldung gem. § 43 GwG unabhängig von den ggf. gesonderten Untersuchungen der Internen Revision verpflichtet ist, sollten Verdachtsmomente, die sich bereits im Verlauf einer Prüfung erhärten, unverzüglich an den Geldwäschebeauftragten gemeldet werden.

Sonderprüfungen von Fraud durch die Interne Revision unterscheiden sich von Regelprüfungen u. a. dadurch, dass personenbezogene Daten zur Sachverhaltsaufklärung fokussiert, genutzt und als Prüfungsergebnis personenbezogene Aussagen getroffen werden müssen.

Nach den Bestimmungen des Datenschutzrechts, insbesondere § 26 BDSG, dürfen personenbezogene Daten von Beschäftigten zur Aufdeckung von Straftaten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Hieraus leitet sich eine besondere Sorgfaltspflicht und Vertraulichkeit in der Prüfungsdurchführung ab. Denn die Reputation der in Rede stehenden Personen und die des Instituts sind gefährdet.

Die nachfolgenden Regelungen und Hinweise sollen den Revisionsmitarbeitern den sicheren Umgang mit Sonderprüfungen erleichtern und damit das Institut vor Haftungsrisiken und Reputationsschäden schützen.

Zielsetzung jeder Sonderprüfung ist auch die Aufklärung und Aufdeckung von Schwachstellen im Unternehmen. Daneben werden stets auch Verbesserungen im Risikomanagement oder des Internen Kontrollsystems als Prüfungsergebnis angestrebt, wobei die Sorgfaltspflicht der Unternehmensleitung zur angemessenen eigenen Überwachung aller präventiven Maßnahmen davon unberührt bleibt.

An die Qualität der Prüfungsergebnisse bestehen hohe Anforderungen, da insbesondere in Gerichtsverfahren die Art der Ermittlung oder der Nachweis der belastenden Sachverhalte oft entscheidend sind. Wurden die Sachverhalte gegen bestehendes Recht oder in unangemessener Weise erlangt, besteht die Gefahr einer Nichtberücksichtigung im Verfahren. Hieraus können erhebliche Nachteile hinsichtlich der arbeits- und zivilrechtlichen

Durchsetzbarkeit resultieren. Es ist insofern – je nach Erfahrung der mit der Prüfung betrauten Mitarbeiter der Internen Revision – oder der Komplexität der Sachlage zu überlegen, ob ein externer Spezialist und die Rechtsabteilung bzw. ein externer Rechtsanwalt einzubeziehen sind.

9.2 Ablauf der Sonderprüfung

9.2.1 Einleitungsvermerk

Hinweise auf Fraud können sich aus verschiedenen Anlässen ergeben:

- Datenanalysen der Internen Revision, z. B. im Rahmen eines Continuous-Auditing-Ansatzes oder des Process-Minings zeigen auffällige Datenmuster (Red Flags).
- Die Interne Revision wird im Rahmen der allgemeinen Informationsverpflichtung aller Mitarbeiter des Instituts gegenüber der Internen Revision über mögliche Unregelmäßigkeiten informiert.
- Hinweise auf dolose Handlungen können sich auch aus einem Hinweisgebersystem gem. § 25a Abs. 1 KWG bzw. § 53 GwG ergeben und zu Sonderuntersuchungen der Zentralen Stelle bzw. der Internen Revision führen.

Zu Beginn einer Sonderprüfung bedarf es eines aussagefähigen Einleitungsvermerks. Der Einleitungsvermerk und die damit festgelegten konkreten ersten Maßnahmen und Datenauswertungen sind mit einem Prüfungsauftrag gleichzusetzen. Aufgrund der möglichen Auswirkung und Komplexität einer Sonderprüfung sollte der Einleitungsvermerk kompetenzgerecht innerhalb der Internen Revision genehmigt werden.

Es muss jederzeit zum Nachweis der Verhältnismäßigkeit gegenüber dem hausinternen Datenschutzbeauftragten und gegenüber Dritten (oder z. B. in Gerichtsprozessen oder gegenüber den Datenschutzbehörden) belegt werden können, dass der Einleitungsvermerk vor weiteren Datenauswertungen im Rahmen der Sonderprüfung erstellt wurde. Bei einer Erstellung und Ablage als Datei ist auszuschließen, dass das Speicherungsdatum des Dokumentes nachträglich verändert werden kann oder sich unbemerkt (z. B. bei Öffnung der Datei) verändert.

Der Einleitungsvermerk sollte mit dem Datenschutzbeauftragten abgestimmt werden.

Gemäß § 87 Abs. 1 Nr. 6 des Betriebsverfassungsgesetzes steht dem Betriebsrat (Personalrat gemäß dem Personalvertretungsrecht der Länder analog) ein Mitbestimmungsrecht hinsichtlich der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen

zu. Nach aktueller Rechtsauffassung gilt dieses Mitbestimmungsrecht auch für Datenauswertungen, die der Leistungs- und Verhaltenskontrolle dienen. Alle Datenauswertungen zur Aufklärung von Fraud-Fällen dienen selbstverständlich der Verhaltenskontrolle der beschuldigten Mitarbeiter. Insofern besteht im Einzelfall oder im Rahmen einer Betriebs- oder Dienstvereinbarung hinsichtlich des generellen Verfahrens ein Mitbestimmungsrecht des Betriebs- bzw. Personalrats. Die Mitbestimmung umfasst aber nicht das „ob“, d. h. die Tatsache, dass das Institut zur Aufklärung von Fraud verpflichtet ist, kann nicht durch die Mitbestimmung unterlaufen werden. Betriebs- oder Dienstvereinbarungen, welche die Einleitung von Sonderprüfungen an die Zustimmung des Betriebs- bzw. Personalrats knüpfen, sollten daher vermieden werden. Gleichwohl unterliegt das „wie“ der Mitbestimmung. Vereinbarungen können den Verfahrensablauf einer Sonderprüfung (z. B. die vorrangige Pseudonymisierung der Daten), Informationspflichten oder die Teilnahme weiterer Personen an Datenerhebungen (Kontrollrechte) regeln. Sofern derartige Regelungen im Institut bestehen, sind diese für die Tätigkeit der Internen Revision bindend.

Wird eine Betriebs- bzw. Dienstvereinbarung als Ablauf von Prozessschritten gestaltet, so wird ein Standardablauf mit einer höheren Rechtssicherheit für die durchführenden Personen geschaffen. Dies erhöht auch die Wahrscheinlichkeit der gerichtlichen Verwertbarkeit.

Bei der späteren Fallbearbeitung sind situativ nach Abwägung der BDSG-Erfordernisse Entscheidungen über weitere Datenauswertungen erforderlich. Bei Zweifeln sollte der Datenschutzbeauftragte auch in diese Entscheidungsfindung einbezogen werden.

9.2.2 Dokumentationserfordernis 1: Zu dokumentierende tatsächliche Anhaltspunkte auf eine Straftat

Die Zulässigkeitskriterien des § 26 Abs. 1 Satz 2 BDSG greifen, wenn Tatsachen vorliegen, die zwar nicht den Straftatbestand erfüllen, wohl aber Indizien dafür bilden. Im Einleitungsvermerk ist nachvollziehbar herauszuarbeiten, dass der Verdacht auf einen konkreten Straftatbestand besteht.

Verstöße gegen das Ordnungswidrigkeitsrecht, das Privatrecht und bankinterne Vorschriften können als Auswertungsgrund nur dann angeführt werden, wenn diesbezüglich eine Einwilligung gem. § 26 Abs. 2 BDSG des Beschäftigten vorliegt. Diese Einwilligung kann auch in Form einer Betriebsvereinbarung vorliegen.

Es müssen Tatsachen (Zahlen, Daten, Fakten) aufgeführt werden, die konkret sind. Anschuldigungen ohne konkrete Indizien auf einen Straftatbestand können eine Auswertung nicht rechtfertigen. Bei der Verarbeitung von anonymen Hinweisen, z. B. aus dem Hinweisgebersystem, bestehen erhöhte Anforderungen an die Konkretisierung der Indizien,

da eine Überprüfung aufgrund der Angaben und der fehlenden Rückfragemöglichkeit beim Hinweisgeber erschwert wird.

9.2.3 Dokumentationserfordernis 2: Straftat im Beschäftigungsverhältnis

Die mögliche Straftat eines Mitarbeiters muss im Beschäftigungsverhältnis begangen worden sein. Der Bezug der Begehung im Beschäftigungsverhältnis muss argumentativ hergestellt werden, wenn dieser sich nicht zweifelsfrei aus den Umständen der Tatvorwürfe erläutert.

Besteht beispielsweise der Vorwurf von Veruntreuungen von Geldern im Rahmen bestehender, genehmigter Kontovollmachten des Mitarbeiters, so ist der Bezug der Begehung der Straftat im Beschäftigungsverhältnis nicht ohne weiteres herzustellen. Eine Betriebsvereinbarung mit entsprechenden Regelungsinhalten könnte einen Bezug eventuell herstellen.

9.2.4 Dokumentationserfordernis 3: Notwendigkeit der Datenerhebung

Es ist der Nachweis argumentativ zu führen, dass die Erhebung, Verarbeitung oder Nutzung von Daten zur Aufdeckung der Straftat erforderlich ist.

Auch wenn zur Sachverhaltsbelegung final eine Datenauswertung legitimiert werden könnte, verbleibt die Argumentationshürde, weshalb die Datenauswertung bereits zum Zeitpunkt der Verdachtsbewertung unerlässlich war.

Es muss die von Arbeitsrechtlern häufig vorgetragene Standardargumentation argumentativ ausgeräumt werden, dass eine Befragung der Verdachtsperson zum Verdachtsfall ohne vorherige Datenauswertung ausgereicht hätte und somit die Datengewinnung unrechtmäßig war.

9.2.5 Dokumentationserfordernis 4: Schutzwürdige Interessen des Beschäftigten und Verhältnismäßigkeit

Im Verlauf der Datenauswertungen muss jederzeit die Abwägung der schutzwürdigen Interessen gegen die Notwendigkeit der Prüfungshandlungen vorgenommen und die Verhältnismäßigkeit gewahrt werden.

Die Datenauswertungen müssen stets als zwangsläufig begründbar und nicht durch andere Mittel ersetzbar sein.

9.2.6 Dokumentationserfordernis 5: Einsatz von Künstlicher Intelligenz bei der Durchführung von Sonderuntersuchungen

Künstliche Intelligenz (KI) kann auf verschiedene Weise bei der Prüfung von dolosen Handlungen eingesetzt werden. Beispiele für mögliche Ansätze:

- a. **Datenanalyse:**
 - KI-Algorithmen können große Datenmengen analysieren, um Muster und Anomalien zu identifizieren, die auf dolose Handlungen hinweisen könnten. Dies umfasst Transaktionsdaten, Buchhaltungsunterlagen und andere relevante Informationen.
- b. **Verhaltensanalyse:**
 - Durch maschinelles Lernen können Modelle entwickelt werden, die das normale Verhalten von Mitarbeitern oder Kunden analysieren. Abweichungen von diesem Verhalten können auf potenziell betrügerische Aktivitäten hinweisen.
- c. **Automatisierte Überwachung:**
 - KI kann in Echtzeit Transaktionen überwachen und Warnungen ausgeben, wenn verdächtige Aktivitäten erkannt werden. Dies ermöglicht eine schnellere Reaktion auf potenzielle dolose Handlungen.
- d. **Textanalyse:**
 - Natural Language Processing (NLP) kann verwendet werden, um Dokumente, E-Mails oder andere Textdaten zu analysieren, um Hinweise auf betrügerische Absichten oder Handlungen zu finden.
- e. **Risikobewertung:**
 - KI-gestützte Systeme können Risikoanalysen durchführen, um die Wahrscheinlichkeit doloser Handlungen in bestimmten Bereichen oder bei bestimmten Kunden zu bewerten.
- f. **Vorhersagemodelle:**
 - Durch die Anwendung von prädiktiven Analysen können Banken und Unternehmen potenzielle Risiken frühzeitig identifizieren und Maßnahmen ergreifen, um dolose Handlungen zu verhindern.
- g. **Kollaboration mit Experten:**

- KI kann als Unterstützung für Prüfer und Ermittler dienen, indem sie relevante Informationen bereitstellt und Entscheidungsprozesse optimiert.

Der Einsatz von KI in der Prüfung doloser Handlungen kann die Effizienz und Genauigkeit erhöhen, indem er menschliche Prüfer unterstützt und ihnen hilft, verdächtige Aktivitäten schneller zu identifizieren. Es ist jedoch wichtig, dass KI-gestützte Systeme regelmäßig überwacht und angepasst werden, um sicherzustellen, dass sie effektiv bleiben. Selbstverständlich sind die in den vorigen Abschnitten genannten Dokumentationserfordernisse auch beim Einsatz von KI umfassend zu beachten. Eine ausführliche Dokumentation der Vorgehensweise und eine Abstimmung im Vorfeld mit den relevanten Ansprechpartnern in Geschäftsleitung, Rechtsabteilung und Betriebsrat ist unbedingt zu empfehlen.

9.3 Verfahren zur Wahrung der schutzwürdigen Interessen des/der Betroffenen und der Verhältnismäßigkeit

9.3.1 Prüfungstagebuch

Der Verlauf einer Sonderuntersuchung ist im Voraus nicht in einem dem BDSG entsprechenden Detaillierungsgrad strukturierbar, so dass im Einleitungsvermerk meist nur die Anfangsphase der Sonderuntersuchung abgebildet werden kann. In der Folge sind weitere Dokumentationen zur Zulässigkeit der jeweiligen Auswertungen zu führen.

Um den situativen und dynamischen Verlauf einer Sonderuntersuchung belegen zu können, bietet es sich an ein Prüfungstagebuch zu führen, welches die Vorgehensweise und den jeweiligen Erkenntnisstand chronologisch dokumentiert.

Die Verhältnismäßigkeit und die Wahrung der schutzwürdigen Interessen in Bezug auf bereits durchgeführte und geplante weitere Schritte können dann im zeitlichen Bezug – unter Einbeziehung der Arbeitsunterlagen und der Prüfungsnachweise – hergestellt werden.

Dies ist darüber hinaus sinnvoll, da die Verhältnismäßigkeit und die Wahrung der schutzwürdigen Interessen meist mit erheblicher Zeitverzögerung im Rahmen der juristischen Bearbeitung vom Prüfungsdurchführenden zu vertreten und belegen ist.

Die Durchführung einer Sonderprüfung zur Aufdeckung von Fraud sollte mit hoher zeitlicher Priorität durchgeführt werden. Anhand des Prüfungstagebuchs kann der Nachweis einer stringenten Prüfungsdurchführung der Internen Revision jederzeit erbracht werden.

9.3.2 Auswertungen mit erstmaligem Ausschluss personenbezogener Daten

Insbesondere zur Validierung des Anfangsverdachts ist es häufig nicht notwendig, Daten und ergänzend mit angeforderten personenbezogenen Daten gemeinsam auszuwerten. Wird als angebliche Tatsache ein außergewöhnlicher Betrag, Verwendungszweck oder ähnliches überprüft, so müssen hierzu nicht die weiteren personenbezogenen Daten (z. B. Erfasser, Begünstigter, Kontoinhaber) im ersten Schritt mit ausgewertet werden.

In die weitere Validierung gemeinsam mit den personenbezogenen Daten werden dann nur die Datensätze mit den vorher erfüllten Kriterien einbezogen.

9.3.3 Anonymisierung personenbezogener Daten

Müssen personenbezogene Daten in die Auswertungen einbezogen werden, so ist eine Anonymisierung zu prüfen. Dies bedeutet, dass die Einzelangaben nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand zugeordnet werden können.

Bei der Auswertung strukturierter Datenbestände ist es oft unvermeidbar, dass nicht notwendige sensible Datenfelder (z. B. Geburtsdatum, Behinderungsgrade) mitgeliefert werden. Diese sollten vor der Auswertung anonymisiert werden, da diese für den Auswertungszweck oft nicht relevant sind. Zufallserkenntnisse über nicht beteiligte Personen oder unzulässige Auswertungszwecke (z. B. mögliche Anschriftenabgleiche zur proaktiven Feststellung von Beziehungen) erschweren die Legitimation des Auswertungserfordernisses.

9.3.4 Pseudonymisierung personenbezogener Daten

Die Pseudonymisierung ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung der Betroffenen auszuschließen oder wesentlich zu erschweren.

Sofern nicht bereits bei der Datenselektion eine ausreichende Dateneingrenzung, z. B. auf die Transaktionen des verdächtigen IT-Benutzers, möglich ist, sollten die zu analysierenden Datenbestände immer pseudonymisiert werden, damit gewährleistet ist, dass nicht relevante Auswertungserkenntnisse nicht in Bezug zu unbeteiligten Personen gebracht werden können.

9.3.5 Auswertung von E-Mail und sonstiger elektronischer Kommunikation

Grundsätzlich ist zu unterscheiden, ob die Sonderuntersuchung mit oder ohne Wissen des/der Betroffenen erfolgt. Während der Umgang mit E-Mail-Verkehr über das dienstliche E-Mail-Account im Rahmen einer Sonderuntersuchung – wie in den folgenden Absätzen beschrieben – vergleichsweise klar geregelt ist, sollte die Übertragbarkeit der im Weiteren aufgeführten Maßnahmen auf sonstige elektronische Kommunikation (Chats usw.) eng mit dem Datenschutzbeauftragten bzw. der Rechtsabteilung abgestimmt werden.

In jedem Fall sollte auch die Auswertung von E-Mail wegen ungewisser Rechtsrisiken mit dem Datenschutzbeauftragten bzw. der Rechtsabteilung abgestimmt werden.

Eine Einwilligung des Betroffenen zur Auswertung seiner E-Mails kann eine Alternative darstellen. Dabei ist darauf zu achten, dass die Freiwilligkeit der Entscheidung nicht in Zweifel gezogen werden kann.

E-Mail-Datenbestände sind der Gruppe der unstrukturierten Datenbestände zuzuordnen. Bei diesen Datenbeständen sind die Formate und Inhalte nicht standardisiert, so dass diese nicht im Voraus, wie beispielsweise in einer Datenbank, beurteilt werden können. Es muss also damit gerechnet werden, dass schutzwürdige Sachverhalte des Betroffenen im Datenbestand nur schwer erkennbar sind (z. B. E-Mails eines Mitarbeiters als Betriebsrat und zur Betriebsratstätigkeit, E-Mails zu privaten Vermögenstransaktionen mit Abteilungen des Hauses).

Ist der private E-Mail-Verkehr über das dienstliche E-Mail-Account unzulässig, dann kann die Auswertung von E-Mails zulässig sein. Allerdings ist dann die Verhältnismäßigkeit besonders zu bedenken.

Ist privater E-Mail-Verkehr über das dienstliche E-Mail-Account vom Arbeitgeber zugelassen oder offen toleriert, so ist eine Auswertung nur unter sehr erschwerten Bedingungen zulässig. Die Bank unterliegt dann dem Telemediengesetz bzw. dem Telekommunikationsgesetz. Mangels einer einheitlichen Rechtsauffassung muss der E-Mail-Verkehr grundsätzlich dem Telefonverkehr gleichgestellt werden.

Die Auswertung von E-Mail-Beständen ist meist ein aufwändiger Prozess und kann durch spezielle Software (Löschung von Dubletten, Suche mit Suchbegriffen, Filterfunktionen) erheblich effektiver durchgeführt werden.

9.3.6 Auswertung ohne Anlass im Einzelfall von Mitarbeiterkonten

Die Verarbeitung von Daten erfolgt auf der Grundlage und für den Zweck der vertraglichen Beziehung. Hieraus ergibt sich die grundsätzliche Beschränkung, dass Daten der Kontoführung für diese Vertragsbeziehung und Daten des Arbeitsverhältnisses für jene Vertragsbeziehung genutzt werden dürfen. Ist der Angestellte eines Kreditinstituts gleichzeitig auch Kunde, so ist es in der Regel nicht gestattet, die Daten über die Bewegungen seines Kontos für im Rahmen des Arbeitsverhältnisses zu treffende Personalbeurteilungen heranzuziehen. Die generelle Kontrolle von Mitarbeiterkonten zur Prävention gegen Straftaten ist nicht zu akzeptieren. Zur Aufklärung konkreter Straftaten kann eine Auswertung von Kontodaten unter vorheriger Einschaltung des Betriebs- bzw. Personals (ggf. über eine Betriebs- bzw. Dienstvereinbarung) sowie des Datenschutzbeauftragten erfolgen.

9.4 Prüfungsnachweise und Qualitätssicherung

9.4.1 Prüfungsnachweise

Prüfungsnachweise, Prüfungsdokumentation und Berichtsdarstellung sollen so beschaffen sein, dass sie auch juristisch belastbar sind.

In den Arbeitsunterlagen ist auf die Art der jeweiligen Prüfungsnachweise präzise einzugehen. Dabei ist die Wertigkeit der Prüfungsnachweise zu berücksichtigen und darzustellen (Originaldokument, Fotokopie, Dokument der optischen Archivierung, Ergebnis einer Befragung). Im Zweifel ist eine Prüfungsaussage auf der Grundlage nicht valider Prüfungsnachweise in den Arbeitsunterlagen und im Prüfungsbericht aussagefähig zu relativieren.

Im Grundsatz sollte ein einzelner Prüfungsnachweis als nicht ausreichend angesehen werden.

Muss mit der Beschlagnahme von Arbeitsunterlagen durch die Ermittlungsbehörden gerechnet werden, sollte die Vollständigkeit der Arbeitsunterlagen durch eine fortlaufende Nummerierung (Seite 1 bis X) gesichert und ein Inhaltsverzeichnis vorgegeben werden. Der Umfang der Unterlagen sollte in einem Vermerk festgehalten werden. Dies erleichtert den Nachweis der Vollständigkeit der vorgelegten Unterlagen und lässt später verschwundene Prüfungsnachweise erkennen. Darüber hinaus können die Arbeitsunterlagen auf die Prüfungsnachweise leichter referenziert werden.

Elektronische Arbeitsunterlagen können durch schwer veränderbare Dokumentformate (z. B. pdf-Dokumente) generiert werden, allerdings bestehen Risiken hinsichtlich der

ungewollten Veränderungen von Erstellungsdaten und möglicher nachträglich vorgenommener Veränderungen.

Prüfungsnachweise aus elektronischen Speichermedien (Festplatten, Smartphone, USB-Stick, Speicherung auf Server oder in einer Cloud) bergen bei unsachgemäßer Beweissicherung erhebliche Rechtsrisiken. Hier ist eine IT-forensische Unterstützung notwendig, um die gerichtsfeste Verwertbarkeit zu sichern.

Bei elektronischen Speichermedien (z. B. Mail-Server) ist vor der Auswertung zusätzlich aufzuklären, ob ausländische Rechtsvorschriften bei der Auswertung zusätzlich zu berücksichtigen sind.

9.4.2 Befragungen zur Gewinnung von Prüfungsnachweisen

Befragungen von Verdachtspersonen und anderen Mitarbeitern bedürfen einer erhöhten Sorgfalt. Befragungen von Verdachtspersonen sollten grundsätzlich durch mindestens zwei Revisionsmitarbeiter geführt werden.

Umfeld und Ablauf der Befragung sind so auszugestalten, dass dem nachträglichen Vorwurf einer möglichen Nötigung begegnet werden kann. Zum Beispiel sollten Getränke, Gesprächspausen oder der jederzeitige Abbruch des Gesprächs angeboten werden. Auch sollten keine direkten oder indirekten Drohungen ausgesprochen werden.

Wünscht der Mitarbeiter die Hinzuziehung von Betriebs- oder Personalrat oder eines Anwaltes, sollte die Interne Revision diesen Vorschlägen folgen.

Zu Befragungen ist ein Verlaufsprotokoll zu führen (kein Ergebnis- oder Kurzprotokoll), welches dem Befragten zur Stellungnahme oder Anerkennung zugeleitet werden kann.

In der Praxis hat sich auch die Anforderung einer Stellungnahme (unter angemessener Fristsetzung) bewährt, da diese Ausführungen später mit den Aussagen im Gespräch abgeglichen und Widersprüche identifiziert werden können.

9.4.3 Berichterstattung

Bei der Berichterstattung sind höchste Anforderungen an die Richtigkeit der Darstellungen und die Objektivität zu stellen.

Wichtige Meilensteine der Untersuchung (Einträge des Prüfungstagebuchs) sollten in die Berichterstattung aufgenommen werden, um eine stringente Prüfungsdurchführung zu belegen.

Sämtliche Prüfungsaussagen sind auf logische Schlüssigkeit zu untersuchen.

Spätestens mit dem Versand eines Berichtsentwurfs oder einer mündlichen oder schriftlichen Information der Geschäftsleitung oder der Vorgesetzten eines beschuldigten Mitarbeiters beginnen arbeitsrechtliche Fristen.

Sofern der Sachverhalt komplex und die Untersuchung zeitaufwändig ist, bietet es sich an, über bereits abgeschlossene Prüfungshandlungen und entsprechende Prüfungsfeststellungen vorab Teilberichte zu verfassen.

9.4.4 Qualitätssicherung

Im Regelfall ist eine vollständige Qualitätssicherung von Arbeitsunterlagen und Prüfungsbericht durch die Revisionsleitung oder einen qualifizierten Mitarbeiter unverzichtbar.

Quellenverzeichnis

IIA, Positionspapier „Fraud und Interne Revision“, Stand Januar 2019

DIIR, Positionspapier „Datenauswertungen und personenbezogene Datenanalyse: Beispiele für den praktischen Umgang im Revisionsumfeld“

10 Interne Revision im Rahmen von agilen Strukturen (inkl. agile Prüfungsmethodik)

Kreditinstitute sehen sich immer kürzeren Innovationszyklen, zunehmendem Wettbewerbsdruck durch FinTechs und einem steigenden Kosten- und Ertragsdruck ausgesetzt. Ein weiterer nicht zu vernachlässigender Faktor ist der Kundenwunsch nach bequemen und innovativen Produkten und mobilen Lösungen, die sich der jeweiligen Lebenssituation anpassen. Wettbewerbsentscheidend ist vor allen Dingen die Schnelligkeit in der Bereitstellung skalierbarer und marktfähiger Produkte und Lösungen sowie die Fähigkeit auf sich verändernde Kundenbedürfnisse schnell zu reagieren.

Vor diesem Hintergrund gewinnt die Agilität auch in Kreditinstituten an Bedeutung. Es gibt zahlreiche Literatur zu agilem Mindset, Werten Prinzipien, Frameworks und Methoden, so dass wir dies hier aussparen. Es soll an dieser Stelle nur ein wichtiger Erfolgsfaktor für die Implementierung in der Revision aus der Praxis hervorgehoben werden. Die Implementierung in Organisationen startet mit der Anwendung der sichtbaren Praktiken und Erlernen der Prinzipien. Agile Werte und Mindset müssen sich über Jahre in den Mitarbeitern noch bilden bzw. festigen. Dafür sind regelmäßig durchgeführte **Retrospektiven**, bei denen die Zusammenarbeit verbessert wird, der entscheidende Kern für eine lernende Organisation, der leider allzu oft als Erstes eingespart wird. Ohne diese regelmäßige Reflexion fallen Organisationen meist in alte Verhaltensmuster zurück und bleiben „doing agile“ aber erreichen nicht den Zustand „being agile“²¹.

Die wesentlichen Führungsaufgaben in agilen Strukturen und Projekten²² haben sich geändert gegenüber traditionellen Strukturen und Wasserfallprojekten. Insbesondere sollen Führungskräfte nun:

- Rahmenbedingungen schaffen
- Ressourcen sicherstellen
- Prioritäten klären
- Hindernisse beseitigen
- Eigenverantwortung fördern
- Feedback und Reviews durchführen
- Transparenz und Kommunikation sicherstellen

²¹ Literaturempfehlung: Agile Transformation - Der Praxisguide zum Change abseits des Happy Path; Schmiedinger/Rasche/Thonfeld/Tuchen; ISBN 978-3-446-47778-0.

²² Literaturempfehlung: Selbstorganisation braucht Führung: Die einfachen Geheimnisse agilen Managements; Glogner/Rösner; ISBN 3446438289.

Die Tätigkeit der Internen Revision ist hiervon auf mehreren Ebenen betroffen:

- Prüfung von nach agilen Methoden aufgebauten Organisationsformen
- Prüfung des Projektmanagements und Projektbegleitung von mittels agiler Methoden gemanagten Projekten (vgl. DIIR-Standard Nr. 4 „Prüfung von Projekten durch die Interne Revision“)
- Nutzung von agilen Methoden in der Prüfungsdurchführung der Internen Revision
- Einsatz agiler Vorgehensweisen und Projektmethoden bei der Durchführung revisionsinterner Prozesse, zum Beispiel der Erstellung des Prüfungsplans (Rahmenplanung, Mehrjahresplanung, Jahresplanung) oder zur Verbesserung der Revisionsprozesse

10.1 Prüfung von agilen Organisationsstrukturen durch die Interne Revision

Die grundlegende Herausforderung für eine Interne Revision in einem agil aufgestellten Unternehmen, ist die Erlangung eines detaillierten Verständnisses über die unternehmensspezifische Ausprägung von Agilität. Dieses umfasst neben der Kenntnis von im Unternehmen verwendeten Tools, Methoden und agilen Organisationsstrukturen (Tribes, Squads, Circles) auch ein Verständnis der darunter liegenden Prinzipien und Werte, um die Wirksamkeit beurteilen zu können. Idealerweise arbeitet eine Revision in einem solchen Unternehmen selbst agil.

Eine weitere Herausforderung für die Interne Revision ist die Prüfung von Themengebieten und Organisationsstrukturen, die nach agilen Methoden aufgestellt sind. Dies ist vor allem darin begründet, dass Geschäftsmodelle, Produkte und Prozesse üblicherweise sehr schnell weiterentwickelt werden und damit die einmal aufgestellte Prüfungsplanung schnell überholt sein könnte. Auch zwischenzeitliche Prüfungsergebnisse/ Feststellungen der Internen Revision können bereits zum Ende einer Prüfung nicht mehr aktuell sein.

Die Interne Revision in einem nach agilen Strukturen und Prozessen aufgestellten Unternehmen bewegt sich daher in einem Spannungsfeld zwischen den ihr einerseits auferlegten regulatorischen Anforderungen an den Prüfungszyklus und die Prüfung spezifischer Bereiche im Unternehmen (z. B. regulatorische Modelle) und einem sich dynamisch entwickelnden Geschäftsumfeld auf der anderen Seite.

In diesem Umfeld rückt eine starre Ein-Jahres Planung in den Hintergrund und andere Instrumente der Interne Revision, wie Continuous Auditing und Business Monitoring treten stärker in den Vordergrund, die einer unterjährigen Anpassung des Prüfplans dienen. Das Ergebnis ist eine Revision, die dynamisch und zeitnah auf Veränderungen reagieren kann (vgl. auch GIAS Standard 9.4). im Rahmen der aktuell durch die Aufsicht gesetzten

Möglichkeiten, sowohl in den zu prüfenden Gebieten selbst als auch in Bezug auf die für ein Prüfungsgebiet definierten Prüfungsschwerpunkte. In diesem Kontext erhöhen sich auch die Anforderungen an die kommunikativen Fähigkeiten von Mitarbeitern der Internen Revision und in Bezug auf das Management der internen Stakeholder.

Die Planungszyklen der Internen Revision sollten sich idealerweise an den Planungszyklus der Geschäftsbereiche anpassen. Ist dieser Planungszyklus quartalsweise ausgelegt, so kann auch die Interne Revision eine grobe Planung für das Jahr durch eine detaillierte Planung auf die Quartale anpassen, um Änderungen in der Priorisierung Rechnung zu tragen.

Unabhängig davon, ob sich eine Interne Revision diesen Strukturen durch einen klassischen oder agilen Prüfungsansatz nähert, gewinnt auch die Prüfung der Wertschöpfungskette an Bedeutung. Die grundlegenden Ziele von Prüfungen der Internen Revision wie Ordnungsmäßigkeit, Sicherheit, Wirtschaftlichkeit und Zweckmäßigkeit von Prozessen und Kontrollen bleiben davon unberührt.

Agile Organisationsstrukturen in Form cross-functional Teams, sind für die Entwicklung und Produktivsetzung ihres Produktes über die Grenzen von Strukturen hinweg verantwortlich („Purpose End-to-End“). Die Interne Revision muss in der Lage sein, die betreffenden Process-Owner in der Planungsphase einer Prüfung und später bei der Zuordnung von Maßnahmen zur Beseitigung von Mängeln zu identifizieren.

Wichtig in einem agilen Umfeld ist die Zeitnähe der Veröffentlichung von Prüfungsberichten und in diesem Sinne der Zuschnitt der Größe von Prüfungsgebieten oder eine zu den Time-Boxes der Geprüften passende agile Prüfungsdurchführung. Ändert man die Prüfgebiete, so werden diese in der Regel granularer und eher an Risiken als an Strukturen ausgerichtet. Auffälligkeiten oder Risiken, die im Rahmen der Prüfung identifiziert werden, sollten den geprüften Einheiten zeitnah kommuniziert werden. Zudem sollte eine regelmäßige Berichterstattung über die Ergebnisse der Prüfung während der Durchführung stattfinden, mit dem Ziel, den geprüften Bereichen eine zeitnahe Abarbeitung identifizierter Schwachstellen zu ermöglichen. Dies lässt sich z. B. durch die Nutzung von agilen Methoden in der Prüfung erreichen, wie z. B. für den Fachbereich offenen Review-Meetings des Revisionsteams.

10.2 Nutzung agiler Prüfungsmethoden durch die Interne Revision

In einem agilen Umfeld ist die Anwendung agiler Arbeits-/Projektmethoden im Rahmen von Prüfungen vorteilhaft. Wesentliche Vorteile bei der Nutzung von agilen Arbeits-/Projektmethoden in der Prüfungsdurchführung sind insbesondere

- eine höhere Qualität der Prüfungsergebnisse durch eine zielgenauere Risikoorientierung der Prüfungshandlungen (Fokus auf die höchsten Risiken von Inkrement zu Inkrement)
- Inkrementeller Fortschritt der Prüfung durch Limitierung des Work-in-Progress: Es wird nicht alles gleichzeitig begonnen und gleichzeitig am Ende des Prüfungszeitraum fertig, sondern am Ende jedes Inkrements ist ein Teil der Prüfungsergebnisse fertig und eine Teilaussage möglich
- eine schnellere Lieferung und Kommunikation von Prüfungsergebnissen durch Abschneiden von Prüfungshandlungen, die die Bewertung nicht mehr verändern werden (Start-Finishing, Definition of Done)
- dadurch ggf. eine kürzere Prüfungsdauer
- ein intensiverer Austausch/Kommunikation mit den geprüften Einheiten (Kunden-nähe) durch mehrere Reviews innerhalb des Prüfungszeitraums
- eine höhere Zufriedenheit der Teammitglieder durch erhöhte Eigenverantwortung und Handlungsspielräume aus der Selbstorganisation

Hierzu erfolgt die Übertragung von in anderen Branchen bewährten Methoden auf die Durchführung von Revisionsprüfungen. Die wesentlichen Unterschiede lassen sich wie folgt darstellen²³:

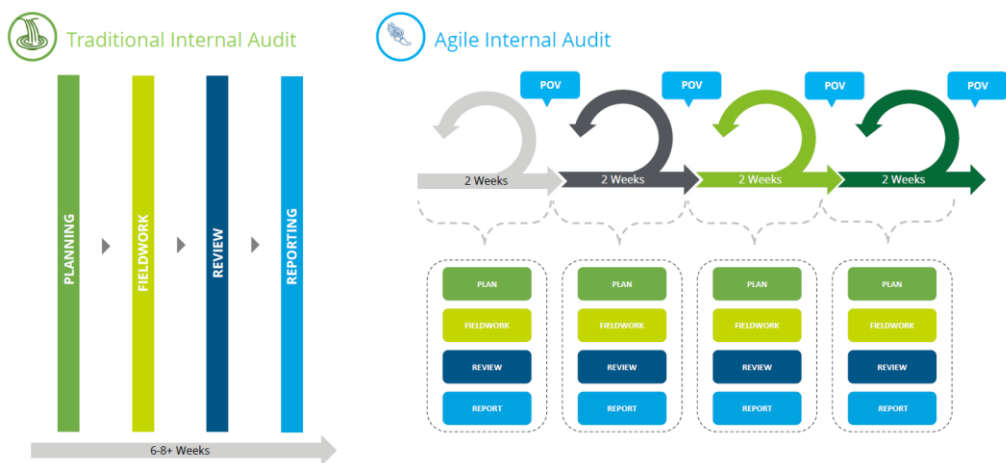


Abb. 15: Traditional vs. Agile Internal Audit²⁴

In der „klassischen“ Prüfungsdurchführung werden alle Themengebiete des Prüfungsumfangs parallel in den Phasen der Prüfung bearbeitet, z. B. gleichzeitige Durchführung von

²³ Quelle: Deloitte.

²⁴ vgl. ebd.

Prozessaufnahmen in verschiedenen Themenbereichen. Hierdurch können erst nach der Sichtung aller Arbeitspapiere die identifizierten Mängel kommuniziert werden. Bei einem agilen Prüfungsansatz werden einzelne Themenblöcke in sogenannten Sprints sequenziell geprüft, so dass die Ergebnisse für den Themenbereich nach Abschluss des Sprints vorliegen und mit der geprüften Einheit abgestimmt werden können. Diesen wird somit frühzeitig die Abstellung der Mängel ermöglicht.

Das Aufbrechen der Prüfung in einzelne Sprints erfordert eine enge Zusammenarbeit und Kommunikation sowohl im Prüfungsteam als auch mit den geprüften Einheiten (z. B. bzgl. kurzfristiger Lieferung der notwendigen Unterlagen und Abstimmung der Ergebnisse). Daneben wird eine hohe Transparenz über die vorgesehenen Prüfungsziele und -umfang benötigt, so werden zum Beispiel offene Punkte aus vorangegangenen Sprints über einen Prüfungsbacklog fortgeschrieben. Häufig wird ein sogenanntes „Audit Canvas“ zur Visualisierung von wesentlichen Informationen für die einzelne Prüfung verwendet. Hierbei werden die Informationen im Sinne von WARUM – WER – WAS aufgezeigt und regelmäßig aktualisiert. Beispielhaft:

WARUM: Informationen/kritische Punkte zum geprüften (Geschäfts-)Bereich, Bedeutung der Prüfung (Warum ist diese Prüfung wichtig?), Was ist der Mehrwert der Prüfung für die geprüfte Einheit?

WER: Hauptansprechpartner/Beteiligte, Prüfungsteam, Bedeutung für/von anderen Funktionen (neben dem direkt geprüften Geschäftsbereich)

WAS: Prüfungsziele und -umfang, Offene Aufgaben/Themen („Audit Backlog“), Zeitpläne der Prüfungen.

Regelmäßige, üblicherweise tägliche, Besprechungen im Prüfungsteam sind essenziell für den Austausch über die Prüfungsziele, den Arbeitsfortschritt, die Ergebnisse und eventuelle Hindernisse.

Gleichzeitig können für die Prüfungen auch Meilensteine („Tollgates“) definiert werden, bei denen bei ausreichender Substanz zur Bewertung des Prüfungsergebnisses eine Prüfung nach Abdeckung der Schlüsselrisiken beendet und das Ergebnis unmittelbar veröffentlicht werden kann. Dieses ermöglicht sowohl einen effizienten Einsatz von Ressourcen in der Internen Revision als auch eine zeitnahe Veröffentlichung von Prüfungsergebnissen.

Die Anwendung der Standards muss auf die inkrementelle Arbeitsweise modifiziert werden. So ist z. B. die Freigabe des Prüfprogrammes vor Beginn der Prüfungsdurchführung vorgesehen. Ganz klassisch in einer Wasserfall Prüfung erstellt das Prüfungsteam am Ende der Prüfungsvorbereitungsphase ein Prüfungshandbuch und lässt sich dieses ge-

nehmigen und prüft es danach ab. In einer agilen Welt mit Reviews nach jedem Inkrement und Planning nur für das jeweils nächste Inkrement ist die Freigabe jedes Inkrements zu dokumentieren. Also in einer 2-monatigen Prüfung mit wöchentlichen Sprints wären das 8 oder 9 Arbeitsstände des Prüfungshandbuchs, welches sich von Sprint zu Sprint weiterentwickelt hat und jeweils ein Teil vor jedem Sprint freigegeben wurde für die Prüfungsdurchführung.

Ebenso sind Sachverhaltsabstimmung und Berichtsabstimmung neu zu denken. Durch den inkrementellen Fortschritt kann die Sachverhaltsabstimmung, die Bewertung von Feststellungen oder die Abstimmung von Berichtspassagen kontinuierlich erfolgen anstelle eines großen abschließenden Termins oder Dokuments.

In der agilen Prüfung werden häufig auch neue Rollen vergeben. Die Aufgaben der Prüfungsleitung werden nach dem Scrum Framework auf den Product Owner (auch Audit Owner), den Scrum Master (auch Audit Master) und das Prüfungsteam auch Audit Team verteilt.

Der Audit Owner stellt die Abstimmung des Prüfungsteams mit den Verantwortlichen des Geschäftsbereiches sicher und definiert die Richtung für das Team, insbesondere in Bezug auf Prüfungszeile und -ergebnisse. Er ist für die Priorisierung des Prüfungsbacklog (risikobasiert) und die Klärung von eskalierten Fortschrittshindernissen verantwortlich und nimmt das Prüfungsprodukt (d.h. den Bericht) ab.

Der Audit Master ermöglicht den agilen Prozess und trainiert das Prüfungsteam. Er ist die Ressource für die Eskalation und Beseitigung von Hindernissen in der Prüfungsdurchführung und schützt das Team vor äußeren Einflüssen, die den Prüfungsfortschritt verhindern. Er organisiert den regelmäßigen Austausch im Team durch die regelmäßigen Meetings und stellt sicher, dass das Team vorankommt, überwacht den Fortschritt und die Kommunikation mit dem Audit Owner. Der Audit Master limitiert Work in Progress und versucht die Effizienz des Teams zu optimieren (Velocity).

Das Audit Team als selbst organisierte Gruppe trägt zur Priorisierung des Audit Backlog und der Definition der gewünschten Arbeitsergebnisse und Stichproben bei. Das Team führt die Prüfungshandlungen durch und bewertet die Ergebnisse, inklusive Entwurf der Prüfungsfeststellungen und Kommunikation der Ergebnisse. Gemeinsam mit dem Audit Master löst es mögliche Hindernisse und Blockaden für den Prüfungsfortschritt. Das Team nimmt aktiv an den täglichen Scrum Meetings teil und überprüft die Arbeitsergebnisse.

Audit Owner und Audit Master verhandeln im Kern einen dauerhaften Zielkonflikt zwischen Qualität/Menge und den noch verfügbaren Ressourcen. Sie sollten daher beide ähnlich starke Persönlichkeiten auf Augenhöhe sein sowie ein hohes Maß an Konfliktfähigkeit und Kommunikationsfähigkeit besitzen.

Es bietet sich an, gerade bei der Einführung von agilen Projektmethoden in der Prüfungsdurchführung, das Team durch einen Agile Coach zu unterstützen. Dieser unterstützt den Audit Master, Audit Owner und das Audit Team beim Erlernen der agilen Methoden, coacht das Team in Bezug auf den Scrum Prozess und die agile Haltung (Mindset) und hilft bei der Definition von Sprints und gewünschten Arbeitsergebnissen. Er hilft Audit Owner und Audit Master ihre jeweiligen Rollen zu finden und die Arbeitspakete zu priorisieren und den Audit Backlog zu managen.

10.3 Abschließende Bewertung

Bezüglich der Umsetzung agiler Arbeitsmethoden und agiler Prüfungsansätze zeigt sich derzeit noch ein heterogenes Bild in der Internen Revision. Einige Revisionen haben ihre Arbeitsweise bereits komplett umgestellt. Andere nutzen hilfreiche Praktiken oder Tools ohne die Prozesse oder Rollen verändert zu haben.

Dennoch lässt sich Folgendes bereits heute festhalten: Fokusthemen in Bezug auf die Arbeitsweise der Internen Revision wie Continuous Auditing, Dynamische Planung, Einsatz von Künstlicher Intelligenz (KI), Durchführungen von Projektprüfungen sowie auch die Rolle der Internen Revision als Change Agent und Advisor im Unternehmen gewinnen vor dem Hintergrund immer schneller werdender Innovationszyklen der Banken und damit auch einem veränderten Anspruch des Managements an die Interne Revision weiter an Bedeutung. Damit verbunden sind auch höhere Anforderungen an Flexibilität und geistige Beweglichkeit von Mitarbeitenden der Internen Revision sowie eine noch fokussiertere Ausrichtung der Prüfungstätigkeiten an den Risiken der Bank und dem Risiko-Appetit der Geschäftsleitung. Dies gilt unabhängig von agilen Arbeitsweisen und der damit verbundenen Methodik.

Quelle und Vertiefung:

DIIR-Prüfungsstandard Nr. 4: Standard zur Prüfung von Projekten (Version 3.0, September 2019).

11 Digitalisierung der Prüfungsprozesse

Gemäß BT 2.3, Tz. 3 MaRisk sind die Prüfungsplanung, -methoden und -qualität regelmäßig und anlassbezogen auf Angemessenheit zu überprüfen und weiterzuentwickeln.

Hierbei gewinnt die Digitalisierung für die Interne Revision zunehmende Bedeutung. Vereinfacht dargestellt meint Digitalisierung dabei den Ersatz manueller Prozessschritte durch Softwarelösungen. Zum einen erzeugen Anforderungen von außen (z. B. Digitalisierung allgemeiner Prozesse und Effizienzziele in den Instituten, Vorgaben von Behörden, Erwartung des Wirtschaftsprüfers) Handlungsdruck zur Digitalisierung innerhalb der Internen Revision; auch weil die Aufsicht verstärkt auf digitale Prüfungsmethoden setzt, ist die Interne Revision gefordert mitzuhalten. Zum anderen erhöhen die Möglichkeiten der Digitalisierung die Qualität der Prüfungsergebnisse (z. B. durch hochwertige und schnelle Analysen großer Datenmengen). Gleichzeitig sind mit einem steigenden Digitalisierungsgrad auch Risiken verbunden, wie beispielsweise der Missbrauch verfügbarer Daten durch Mitarbeitende und die Anfälligkeit für Cyberangriffe. Diese Faktoren muss die Interne Revision einerseits in ihrer Prüfungsplanung berücksichtigen und andererseits auch in Bezug auf die IT-Governance für die bei ihr gespeicherten Daten. Bei der Digitalisierung in der Internen Revision ist zu unterscheiden zwischen:

- Digitalisierung der Revisionsprozesse
- Digitalisierung von Prüfungsmethoden

11.1 Digitalisierung der Revisionsprozesse

Bei der Digitalisierung der Revisionsprozesse sind die eigenen Prozesse der Internen Revision, d. h. insbesondere der Planungs-, Prüfungs-, Follow-up- und Berichtsprozess im Hinblick auf mögliche Digitalisierungspotenziale zu betrachten und weiterzuentwickeln. Zielsetzung ist es, mit der zunehmenden Digitalisierung der eigenen Prozesse eine Steigerung der Effizienz und eine Reduzierung der Anfälligkeit für Fehler zu bewirken.

Phasen der Digitalisierung

Die Digitalisierung der Prozesse lässt sich in drei aufeinander aufbauende Phasen unterteilen:

- Umstellung auf das „paperless office“.
Die früher papiergebundene Revisionsdokumentation wurde in den Internen Revisionen bereits überwiegend ersetzt durch elektronische Medien (z. B. elektronische Prüfungsakte).

- Umstellung auf „Workflow-Tools“ und „Collaborative-Tools“, d. h. eine systemunterstützte, workflowbasierte Abwicklung der Revisionsprozesse (wie Planungs-, Prüfungs-, Follow-up Prozess) sowie eine toolunterstützte Kollaboration und Kommunikation.

In der Revisionspraxis wird der Workflow durch sogenannte Revisionsmanagementsysteme unterstützt. Je nach Größe und Spezialisierung der Kreditinstitute kommen dabei entweder Standardsoftwarelösungen oder eigenentwickelte Softwarelösungen zum Einsatz.

Der Einsatz von „Collaborative-Tools“ (z. B. Microsoft Teams) ermöglicht einen weitgehend reibungsfreien Wechsel zwischen Vor-Ort-Prüfungen und Remote-Prüfungen (einschließlich Mobilarbeit von Prüfern und Geprüften). Relevante Rahmenbedingungen sind zu beachten (z. B. Informationssicherheit, Datenschutz).

- Vollständige, digitale Integration bedeutet die Integration aller Revisionsprozesse, von der risikoorientierten Prüfungsplanung, Prüfungssteuerung, Prüfungsdokumentation, Datenaustausch, Kommunikation der Prüfungsergebnisse bis zum Follow-up, in ein oder mehrere miteinander verbundene IT Systeme.

Zudem können durch eine digitale Integration unternehmensweiter Daten die Effektivität und die Effizienz der Internen Revision weiter gesteigert werden.

Für diese Phase besteht noch der größte Handlungsbedarf für die Interne Revision.

Einsatz von IT-Systemen bzw. von Revisionsmanagementsoftware

Zunächst ist über die Zielsetzung einzelner Digitalisierungsschritte bzw. eine Digitalisierungsstrategie im Kontext der dargestellten Phasen und auf der Basis des erfassten Istzustandes zu entscheiden. Die Kenntnis über die im Unternehmen vorhandenen bzw. unterstützten IT-Strukturen (z. B. IT-Systemlandschaft, Informationsarchitektur, IT-Prozesse und -Ressourcen) ist dabei ein wichtiger Faktor.

Zu den erforderlichen Entscheidungen gehört auch die Frage zu „make or buy“. Die Erstellung individueller Software („make“), welche auf eigene Bedürfnisse zugeschnitten ist, ist aufwändig, teuer und mit hohen Risiken behaftet. Sie kann dennoch teilweise sinnvoll oder notwendig sein, insbesondere zur Umsetzung im Rahmen der dritten der oben dargestellten Phasen. Verfügbare Standardsoftware („buy“) kann insbesondere für kleinere Institute die sinnvollere Lösung sein. Herausforderungen bestehen hier bei der Integration in eine existierende Systemlandschaft, durch Abhängigkeiten von einem Hersteller, und bei Releasewechseln. Bei Einsatz einer Standardsoftware wird zumindest kleineren Häusern empfohlen, weitgehend von einem „Customizing“ abzusehen, um Aufwand und

Risiken bei Releasewechseln zu begrenzen. Demgegenüber sind bei Anpassungsbedarfen die von dem Systemanbieter ermöglichten Konfigurationsmöglichkeiten des Tools zu präferieren.

11.2 Digitalisierung der Prüfungsmethoden

Bei der Digitalisierung der Prüfungsmethoden stehen der Prüfungsprozess und hier die zur Anwendung kommenden Methoden und Werkzeuge im Fokus. Ziel ist es, durch den Einsatz digitaler Prüfungsmethoden den Prüfungsprozess effizienter zu gestalten und die Qualität der Prüfungsaussagen zu steigern.

Bereits im Einsatz sind insbesondere Datenanalysen, entweder mit spezifisch dafür entwickelten Anwendungen wie z. B. IDEA oder ACL oder mit Microsoft Excel und Power BI. Insbesondere bei wiederholten Auswertungen müssen ggf. die Anforderungen von DORA (bei kleinen Instituten bis 31.12.2026 noch die BAIT) zur Individuellen Datenverarbeitung beachtet werden.

Weiterhin stehen fortgeschrittene Analysemethoden und Automatisierungsmöglichkeiten wie Process Mining Tools und Robotic Process Automations (RPAs) zur Verfügung und werden auch vereinzelt genutzt. Zusammen mit der zunehmenden Verfügbarkeit von Anwendungen mit künstlicher Intelligenz (z. B. Textanalysesoftware) sind dies die kurz- bis mittelfristigen Entwicklungen bei den modernen digitalen Prüfungsmethoden und -werkzeugen.

Zunehmend werden Chatbots wie ChatGPT, Microsoft Copilot, Gemini, Perplexity oder Claude eingesetzt. Die Nutzungsmöglichkeiten für die Interne Revision sind davon abhängig, ob der Chatbot in einer proprietären Umgebung betrieben wird und Eingaben sowie ggf. hochgeladene Dokumenten in einer geschützten Umgebung verbleiben oder ob allgemein im Internet verfügbare Chatbots genutzt werden. Letztere sollen nur als Ersatz für die Internet-Recherche und nicht mit unternehmensspezifischen Daten genutzt werden. Idealerweise steht der Internen Revision ein eigener Chatbot zur Verfügung, in dem eine Prompting Library, wiederkehrend genutzte Dokumente als Wissensbasis (z. B. die schriftlich fixierte Ordnung, Gesetze und Verordnungen) und spezifische Einstellungen für Prüfungszwecke dauerhaft hinterlegt werden können.

11.2.1 Datenanalysen

11.2.1.1 Ziele und Voraussetzungen

Datenanalysen als Prüfungsmethode ermöglichen es:

- Prüfungsaussagen zu treffen, die auf den Gesamtdatenbestand abstellen,
- Auffälligkeiten zu identifizieren, die einen risikoorientierten Einstieg in eine Stichprobenprüfung ermöglichen,
- Prozesse hinsichtlich eines sachgerechten Prozessablaufs mit Hilfe historisierter/protokollierter Prozessdaten zu prüfen und
- Gesamtrisikoaussagen zum geprüften Bestand/Portfolio (z. B. ein Kreditportfolio) zu treffen.

Organisatorische Voraussetzung für die Etablierung/Durchführung von Datenanalysen ist z. B. eine geeignete Ausbildung der Mitarbeiter, Zugriffe auf Datenbestände, ausreichende Anzahl von Softwarelizenzen sowie entsprechende zeitliche Möglichkeiten.

11.2.1.2 Konzeptioneller Angang

Für die Implementierung von Datenanalysen als Prüfungsmethode empfiehlt sich zunächst die Festlegung eines grundlegenden Rahmens.

Als wesentliche Eckpunkte empfehlen sich:

- die Festlegung der Zuständigkeiten (Fachprüfer, Datenanalyst),
- die Festlegung der grundlegenden Prozessschritte einer Datenanalyse (inkl. Qualitätssicherung),
- die Auswahl des Datenanalysetools (hier bestehen Abhängigkeiten zur IT-Strategie des Kreditinstituts sowie dem Know-how der Datenanalysten),
- die Aufnahme der verfügbaren Datenquellen,
- die Ergebnisse der Abstimmung mit dem Datenschutzbeauftragten (Datenschutzaspekte, Umgang mit personenbezogenen Daten),
- die grundsätzliche Klassifizierung im Hinblick auf IDV-Relevanz.

11.2.1.3 Umsetzungsplanung und Umsetzung

Für die Umsetzungsplanung bietet es sich an, im Jahresplanungsprozess bereits die Prüfungen zu identifizieren, bei denen das Instrument der Datenanalysen zum Einsatz kommen soll und diese dann mit entsprechenden Kapazitäten und Datenanalyse Know-how zu planen.

Die Umsetzung von Datenanalysen erfolgt im Zusammenspiel zwischen Fachprüfer und Datenanalyst (ggf. auch in Personalunion):

- Voraussetzung für Datenanalysen sind jeweils konkrete fachliche Fragestellungen und Analyseansätze, die seitens der Fachprüfer vorzugeben sind. Auf dieser Grundlage ist durch die Fachprüfer zu definieren, aus welchen Systemen welche Daten benötigt werden.
- Hierauf aufsetzend erfolgt die Aufbereitung und Bereitstellung der Daten durch den Datenanalysten und ein anschließendes Testing durch den Fachprüfer.
- Auf Basis der bereitgestellten Daten erfolgen die Prüfungshandlungen durch den Fachprüfer. Dabei sind die Eigenschaften des analysierten Datenbestandes im Blick zu behalten.

Es bietet sich an, Prüfungen in Kategorien mit vergleichbaren datenanalytischen Ansätzen zusammenzufassen (z. B. Kreditprozess Kundengruppe A, B, C). Eine solche Kategorisierung erlaubt es, übergreifende generische Abfragen für die Kategorie zu definieren, die dann jeweils um spezifische Ansätze für das konkrete Segment ergänzt werden.

11.2.2 Weitere Digitalisierungsansätze

Die IT als Enabler erlaubt Prüfungshandlungen, die bislang nicht oder nur eingeschränkt möglich waren. Einige IT-Bereiche, welche für die Interne Revision neue Möglichkeiten eröffnen, sind hier beispielhaft genannt:

- Dash Boards tragen Informationen aus verschiedenen Bereichen zusammen und stellen wichtige Kennzahlen übersichtlich und leicht verständlich dar. Prüfer können schneller einen Überblick über einen Bereich erhalten und Prüfungshandlungen ableiten.
- „Big Data“ ermöglicht, Daten in großen Mengen zu analysieren, die für bisherigen Methoden zu umfangreich oder komplex waren. Prüfer können in massiven Datenvolumen Probleme und Fragestellungen angehen, welche sie bislang nicht lösen konnten.
- Beim „Process Mining“ geht es um die Visualisierung des tatsächlichen Ablaufs von (weitgehend elektronischen) Geschäftsprozessen und somit um die Wirksamkeit des Internen Kontrollsystems bzw. der Vorgaben. Es stellt damit eine Ergänzung zur theoretischen Prozessanalyse mittels Flow-Charting, die den gewünschten Prozess beschreibt und zur Beurteilung der Angemessenheit dient, dar.
- Strukturiert vorliegende Daten, z. B. in Datenbanken, erlaubten bisher bereits, IT-Tools und Methoden zu entwickeln, welche für wiederholende Prüfungshandlungen mehrfach eingesetzt werden können. Dank Digitalisierung weitet sich die Menge an strukturierten Daten aus, jedoch auch die Zugänglichkeit von unstrukturierten Daten (z. B. E-Mails). Somit können IT-Tools auf eine noch größere Datenbasis zugreifen und erlauben damit noch mehr Analysen.

11.2.3 Künstliche Intelligenz

KI ermöglicht es Prüfern, durch einfach zu erstellende Eingaben Datenbankabfragen oder Software-Anweisungen erzeugen lassen, was bisher speziellen Experten wie Software-Entwicklern vorbehalten war.

Mit der 7. MaRisk-Novelle wurden erstmalig konkrete aufsichtsrechtliche Vorgaben an die Verwendung von KI adressiert. Das Kapitel AT 4.3.5 (zur Verwendung von Modellen) bezieht sich explizit auch auf Modelle mit Charakteristika von KI.

Aus den MaRisk (AT 4.3.5) ergeben sich Anforderungen

- an eine hinreichende Erklärbarkeit der Ergebnisse
- an geeignete Verfahren zur Sicherstellung der Qualität der zugrundeliegenden Daten und Erkennung und Bereinigung von Qualitätsschwächen
- an Regelungen zur Verwendung der Modellergebnisse und Vorgaben zum Vorgehen bei Überschreibungen der Ergebnisse
- an regelmäßige Modellvalidierung (Genauigkeit, Stabilität, Konsistenz der Verfahren, Grenzen und Beschränkungen, zugrundeliegende Annahmen und darin einfließende Daten)

Hier empfiehlt sich revisionsseitig eine Begleitung der Umsetzungsphase. Zunächst sollte auf bankweite Vorgaben an die Nutzung von KI hingewirkt werden (eine bankweite Definition, bankweitere Anforderungen an den Einsatz). Außerdem empfiehlt es sich, im Institut eine Evidenz über die bereits laufenden KI-Initiativen zu schaffen. Hierauf aufsetzend sind dann institutsinterne Regelungen zur Umsetzung der Anforderungen aus MaRisk AT 4.3.5 zu implementieren.

KI als Prüfungsthema für die Revision

Der Einsatz von KI wird **als Prüfungsthema** für die Revision zunehmend an Bedeutung gewinnen. Hier empfiehlt es sich, im Rahmen einer übergeordneten Prüfung die Rahmenbedingungen (Strategie, übergeordnete Vorgaben der Bank) zu betrachten und in allen Fachprüfungen ein Grund-set an Fragen mitzunehmen.

KI-Agenten werden zunehmend in der Automatisierung von Geschäftsprozessen eingesetzt als Weiterentwicklung von Robotic Process Automation. Hierbei treffen die Agenten Entscheidungen mithilfe von KI Modellen anstatt fester Regeln. Daher kann bei der Prüfung der Angemessenheit nicht mehr bei den Regeln angesetzt werden und Prüfprogramme sind dahingehend zu überdenken.

KI als Werkzeug im Prüfungsprozess

Inzwischen hat sich der Einsatz von KI Chatbots in der Internen Revision etabliert. Soweit der Internen Revision hierfür eine geschützte Umgebung zur Verfügung steht und die relevanten Daten in digitalisierter Form vorliegen, kann KI in allen Phasen der Prüfung – Prüfungsvorbereitung, Prüfungsdurchführung und Berichterstattung sowie bei der Qualitätssicherung – sowohl die Effizienz als auch die Effektivität verbessern.

Einfach ist der Ersatz von Recherche zum Prüfungsgegenstand und zur einschlägigen Regulierung sowie den damit verbundenen Risiken im Rahmen der Prüfungsvorbereitung durch geeignete Prompts. So können z. B. die Analyse und die Zusammenfassung von Dokumenten deutlich schneller und mit qualitativ guten Ergebnissen durchgeführt werden. Gleiches gilt für eine Auflistung und Beschreibung der Risiken. Ein weiterer Anwendungsfall ist die Analyse und Aufbereitung von Ergebnissen aus Vorprüfungen und Vormerkungen.

Im Rahmen der Prüfungsdurchführung sind einfache Anwendungsfälle z. B. der Abgleich aufsichtsrechtlicher Anforderungen mit internen Regelungen oder mit Verträgen. Analysen und Aufbereitung von Datenbeständen sind ebenfalls möglich. Zukünftig werden KI-Agenten Prüfungshandlungen, wie z. B. das Testing von wesentlichen Kontrollen (Wirksamkeitsprüfung) übernehmen können; bei gut definierten Kontrollen (Kontrollziel, Input, erwartetes Ergebnis) und idealerweise digitaler Kontrolldokumentation können so große Datenmengen in kurzer Zeit analysiert werden. Bei der Überprüfung der Objektsicherheit kann KI bereits heute Drohnenbilder auswerten und erkennen, ob erhöhte Gefahren bestehen. Gespräche mit Geprüften können real-time vollständig transkribiert werden, so dass die nachträgliche Protokollierung gespart wird. Viele weitere Anwendungsgebiete sind mit der zunehmenden Integration von KI in alle Lebens- und Arbeitsbereiche in der näheren Zukunft noch vorstellbar.

Im Rahmen der Berichterstattung kann ein KI Chatbot z. B. Prüfungsfeststellungen aus den Arbeitspapieren generieren sowie bei der Formulierung weiterer Berichtsteile unterstützen.

KI kann bei der Qualitätssicherung und im Quality Assessment als Arbeitsmittel eingesetzt werden, um anstatt einer Stichprobe sämtliche Berichte, Arbeitspapiere und Unterlagen „zu lesen“ oder den Quality Assessor von eher einfachen Überprüfungen zu entlasten, so dass insgesamt eine höhere Breite und/oder Tiefe erreicht werden kann.

Für die Ausbildung von Mitarbeitenden können Schulungsunterlagen mittels KI in Videos mit Avatar, Sprechstimme und einem Quiz in verschiedene Sprachen umgewandelt werden, so dass die Inhalte leichter und besser angenommen werden.

Aktuell sollten die Ergebnisse der KI, noch durch den Prüfer plausibilisiert werden, so dass in letzter Instanz der Mensch die Verantwortung für die Ergebnisse übernimmt. Vor diesem Hintergrund ist KI im Prüfungsprozess nicht als ein Modell im Sinne der MaRisk einzustufen.

Der digital affine Revisor

Einhergehend mit der Digitalisierung verändern sich die Anforderungen an den Revisor.

Zunehmend gefragt sind eine IT-Affinität, die Fähigkeit Daten zu analysieren und Kenntnis der hierfür benötigten Software und Methodik (weitere Einzelheiten hierzu vgl. Abschnitt 11).

Auch wenn nicht jeder Revisor über eine detaillierte Datenanalyse-/Digitalisierungskompetenz verfügen muss, so sind für das Zusammenspiel von Datenanalyst und Fachprüfer Grundkenntnisse und ein digitales Grundverständnis auf Seiten des Fachprüfers in zunehmendem Maß erforderlich. Umgekehrt müssen auch Analysten und IT-Prüfer über ein fundiertes Verständnis der fachlichen Anforderungen und Prozesse verfügen.

Dies wird unterstützt durch ein angemessenes Weiterbildungsprogramm für den Erhalt und die Förderung digitaler Kompetenz.

11.3 Durchführung von Remote-Prüfungen

Heutzutage ermöglichen digitale Prozesse und Arbeitsmethoden, dass ein Großteil der Prüfungsaktivitäten als so genannte Remote-Prüfungen durchgeführt werden. Im Folgenden werden praxisorientierte Überlegungen, wie Revisionseinheiten Remote-Prüfungen zusammen mit ihren Risikopartnern (geprüfte Bereiche) sowie weiteren Stakeholdern mehrwertbringend einsetzen können dargestellt.

11.3.1 Kurzdefinition von Remote-Prüfungen

In einer Remote-Prüfung wird die Prüfungskommunikation hauptsächlich mittels elektronischer Kommunikationsmittel vorgenommen.

In der bisherigen Praxis wird als Remote-Prüfung die Durchführung von Revisionsprüfungen von einem abweichenden Arbeitsort als dem Standort des geprüften Bereichs verstanden (z. B. andere Niederlassung oder Home-Office). Die örtliche Trennung von geprüftem Bereich und Revision bedingt den Einsatz digitaler Werkzeuge und Kommunikationsmittel (z. B. Besprechung über Videokonferenzen und Zusammenarbeit mittels Kollaborationssoftware).

Der remote Anteil einer Prüfung ist nicht festgeschrieben, sondern kann je nach Prüfungstyp (Operational Audit, Management Audit, Sonderprüfung usw.), Größe, Branche und Internationalisierung des Unternehmens, Digitalisierungsgrad des Geschäftsmodells sowie der Revisionseinheit²⁵ variieren.

Die mit der Nutzung von Remote-Prüfungstechniken einhergehenden Vorteile bestehen in einer schnelleren und flexibleren Kommunikation mit der geprüften Stelle und durch den Wegfall von Reisezeiten in der Reduktion des Ressourcenaufwands. Durch Screen-Sharing können Antworten der geprüften Stelle anhand geeigneter Nachweise bereits im Gespräch verifiziert werden. Gleichzeitig vereinfacht Remote-Audit die Arbeit in dezentral organisierten Prüfungsteams und ermöglicht die Arbeit aus dem Home-Office. Durch Remote-Prüfungen ergeben sich, bei sorgfältiger Planung und Durchführung, grundsätzlich keine wesentlichen, negativen Abweichungen in Bezug auf die Prüfungssicherheit gegenüber der Vor-Ort Prüfungen. Jedoch können Videokonferenzen die Einschätzung der Reaktionen der geprüften Stelle sowie den informellen Austausch mit dem geprüften Fachbereich erschweren.

11.3.2 Umsetzung von Remote-Prüfungen

In den letzten Jahren hat sich bei vielen Revisionseinheiten ein hybrider Prüfungsansatz bestehend aus Remote- und Vorort-Prüfungshandlungen fest etabliert. Grundsätzlich können alle Prüfungen mit wenigen Ausnahmen (z. B. räumliche Begehungen, physische Aufnahme, „Fraud-Interviews“) mittels remote-Prüfungstechniken durchgeführt werden. Ein gänzlicher Verzicht auf Vorortprüfungshandlungen ist für manche Prüfungshandlungen jedoch nicht möglich.

Bei der risikoorientierten Festlegung der Prüfungsschwerpunkte ist zu bewerten, ob das Prüfungsziel und eine ausreichende Risikoabdeckung durch die Remote Prüfung erreicht werden können. Insoweit sind auch Prüfungshandlungen in Betracht zu ziehen, die vor Ort ausgeführt werden sollten. Beispielsweise eignen sich Prüfungen von Auslandsniederlassungen dann nicht uneingeschränkt für Remote-Prüfungen, wenn die Einhaltung lokaler oder internationaler Standards erstmalig geprüft werden. Ähnliches gilt bei Sonderprüfungen, bei denen die Aufklärung einer dolosen Handlung die Überführung des Täters oder zumindest die Sachverhaltsaufklärung mit arbeits- bzw. strafrechtlicher Würdigung zum Inhalt hat²⁶.

²⁵ Siehe S. 3, Prüfen in Covid-19 Zeiten, Ein Erfahrungsbericht aus der Prüfungspraxis der DAX 30 Unternehmen, Ralf Herold, Oktober 2020.

²⁶ Vgl. Seite 4, Remote-Auditing Chancen und Herausforderungen in der Durchführung von Remote-Audits, DIIR Fachbeitrag Nr. 3 vom 18.09.2020).

Unter Berücksichtigung des Umstands, dass die räumliche Trennung die Beschaffung von relevanten Informationen erschweren kann, ist bei der Prüfungsvorbereitung intensiv auszuarbeiten, welche Dokumente bzw. Unterlagen und welche Datenauswertungen benötigt werden und diese uneingeschränkt der Internen Revision bereitgestellt werden können.

11.3.3 Praxishinweise

Die Corona-Pandemie hat gezeigt, wie schnell und dynamisch sich Bewährtes verändert hat. Mit Bezug zur Arbeitswelt bedeutet es, dass sich vor allem durch digitale Prozesse und Homeoffice Lösungen eine weitere Verschmelzung von Arbeit und Freizeit (New Work) ergeben wird. Insoweit bietet die neue Arbeitswelt die Chance, verantwortungsbewusst und nutzenstiftend, Remote-Prüfungen, insbesondere auch in einem agilen Kontext, zu etablieren.

Hierbei kann Folgendes empfohlen werden:

- Regelmäßige virtuelle Treffen im Prüfungsteam („Stand-Ups“ oder „Dailys“) um eine laufende Synchronisierung der verfügbaren Informationen sicherzustellen!
- Aktiv moderierte Meetings in denen sich die Teilnehmer gegenseitig aussprechen lassen. Durch die fehlende soziale Nähe kommt es in der Kommunikation leichter zu Missverständnissen und evtl. Verstimmungen. Daher sollte festgelegt werden, dass die Teilnehmer wertschätzend und respektvoll miteinander kommunizieren.
- Nutzung von Tools zur Kollaboration und Aufgaben- und Zeitplanung. Sie erlauben allen Teilnehmern, auf Informationen zugreifen und sie ändern zu können (z. B. Jira). Für die Dokumentation, z. B. von Interviews oder zur Verteilung von Informationen, helfen Tools wie Confluence, welche sehr leicht bedienbar sind.
- Strukturierte Aufgabensteuerung innerhalb des Prüfteams, z. B. mit Kanban-Boards, um Aufgaben zu verteilen und zu verfolgen.
- Durchführung von regelmäßigen Status Meetings. Aufgrund des fehlenden Austauschs „im Vorbeigehen beim Kollegen“, sollten Abstimmungen stärker getriggert und gesteuert werden.
- Auch den „privaten“ Austausch in Gesprächen zulassen und ggf. fördern. Durch den fehlenden persönlichen Kontakt sollte alles, was soziale Beziehung zwischen Menschen erzeugt und damit die Zusammenarbeit fördert, einen Raum in „offiziellen“ Gesprächen finden.
- Je nach Möglichkeit und Bedarf können Vor-Ort und Remote Audits variieren, wobei sich nicht alle Prüfgebiete oder Prüfungsanlässe uneingeschränkt für Remote-Prüfungen eignen.

11.3.4 Fazit

„Remote Audit“ und die damit einhergehende Nutzung moderner Kommunikationsmittel und Prüfungstools sind nicht mehr wegzudenken und haben sich fest in der Praxis der Internen Revision etabliert. Umfang und Detaillierungsgrad der Remote-Prüfungshandlungen sind spezifisch für das jeweilige Prüfungsobjekt festzulegen und liegen damit in der Verantwortung der jeweiligen Revisionseinheiten. Mit der fortschreitenden Digitalisierung der Geschäftsprozesse wird auch Remote-Audit einem stetigen Wandel unterliegen. Sicher ist jedoch, dass die zunehmende Verzahnung von Business- und Revisionsprozessen die Leistungsfähigkeit und Effizienz der Revisionseinheiten weiter erhöhen wird.

Quelle:

ISACA-Leitfaden zu Datenanalysen (Ausgabe 2019).

12 Qualitätssicherung und -verbesserung in der Internen Revision

12.1 Grundlagen des Qualitätsmanagements

Als Folge steigender Anforderungen im Bereich der Corporate Governance und seitens der Bankenaufsicht kommt der Sicherung und Verbesserung der Qualität der Internen Revision ein hoher Stellenwert zu. Um dauerhaft die Wirksamkeit der Internen Revision zu gewährleisten, ist eine fortlaufende Bewertung und Verbesserung ihrer Prozesse und Methoden notwendig.

Die GIAS beinhalten die folgenden detaillierte Vorgaben zur Qualitätssicherung und Qualitätsverbesserung für die Interne Revision:

- GIAS Standard 8.3 „Qualität“: Danach ist es Pflicht der Revisionsleitung, ein „Programm zur Qualitätssicherung und -verbesserung, das alle Aspekte der Internen Revision abdeckt, zu entwickeln, umzusetzen und aufrechtzuerhalten“. Das Programm umfasst externe und interne Beurteilungen und mind. jährlich muss hierzu eine Berichterstattung/ Kommunikation der Ergebnisse erfolgen.
- Im GIAS Standard 8.4 „Externe Qualitätsbeurteilung“ ist die Anforderung formuliert, eine externe Qualitätsbeurteilung der Internen Revision als Element des Qualitätsmanagements einzubeziehen. Dies muss mind. alle fünf Jahre erfolgen und kann auch in Form einer internen Selbstbeurteilung mit externer Validierung erfolgen.
- Die GIAS Domain IV „Leitung der Internen Revision“ enthält im Prinzip 12 die „Verbesserung der Qualität“ mit den GIAS Standards 12.1 „Interne Qualitätsbeurteilung“, 12.2 „Leistungsmessung“ (vgl. vertiefend Kapitel 13) und 12.3 „Überwachung und Verbesserung der Leistung bei der Durchführung von Aufträgen“.

Die Etablierung eines Qualitätssicherungsprogramms hilft nicht nur die Effizienz und Effektivität der eigenen Prozesse kontinuierlich zu verbessern, sondern ermöglicht es der Internen Revision auch das erreichte Qualitätsniveau nach außen zu kommunizieren. Somit kann die Gestaltung eines erfolgreichen Qualitätssicherungsprogramms und die darauf aufbauende Berichterstattung ein geeignetes Selbstmarketingtool für die Interne Revision darstellen.

Im Qualitätsmanagement sind auch die strategischen Ziele aus der Revisionsstrategie (vgl. hierzu Kapitel 1.6 „Revisionsstrategie“ und Kapitel 13 „Leistungsmessung“) zu berücksichtigen und mittels Key Performance Indicators messbar zu implementieren, messen und berichten.

12.2 Elemente des Qualitätsmanagements

Nachfolgende Übersicht fasst die Elemente eines Qualitätsmanagements zusammen:

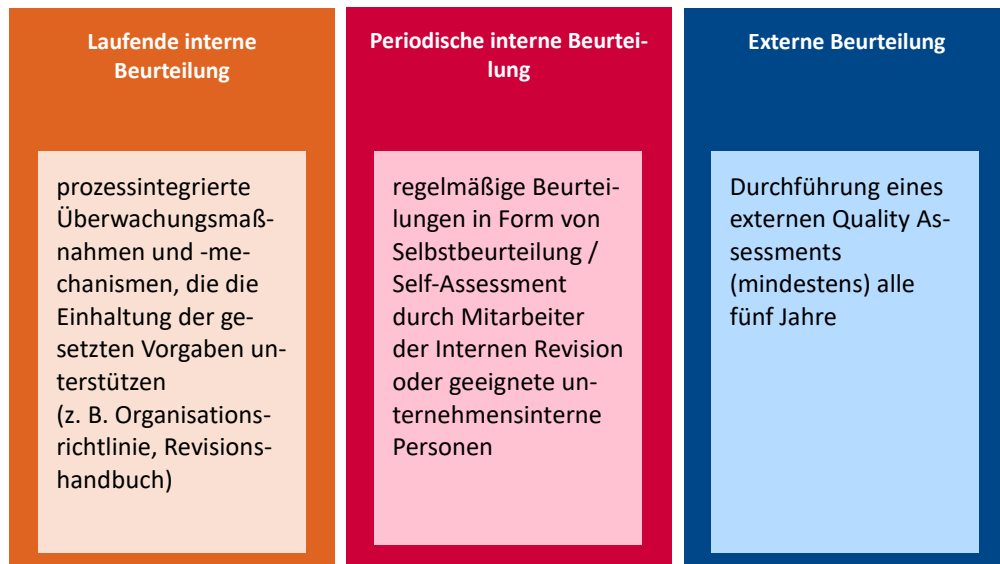


Abb. 16: Elemente des Qualitätsmanagements

12.3 Interne Qualitätsüberwachung

Der GIAS Standard 12.1 formuliert zur internen Qualitätsbeurteilung, dass „die Revisionsleitung eine interne Beurteilung der Einhaltung der GIAS und des Fortschritts in Bezug auf die Leistungsziele entwickeln und durchführen muss (...).“ Die Ergebnisse hierzu sind zu berichten/ kommunizieren.

12.3.1 Laufende interne Beurteilung (→ prozessintegrierte Maßnahmen)

Kernelemente zur Zielerreichung, Qualitätssicherung und -verbesserung der Revisionsfunktion sind interne Richtlinien und Verfahren sowie die laufende Steuerung und Überwachung aller Revisionsaktivitäten.

Hierbei sind insbesondere die GIAS Standards 8.3 und 12.3 zu berücksichtigen. Diese sehen eine laufende interne Beurteilung der Beachtung der Qualität der Tätigkeit der Internen Revision und der Auftragsausführung vor.

Nachfolgend sind wichtige Aspekte, die dabei berücksichtigt werden sollten, exemplarisch dargelegt:

- Einhaltung der berufsständischen Standards (GIAS)

Die laufende Qualitätssicherung sollte eine Überprüfung der Beachtung/ Einhaltung der berufsständischen Standards (GIAS) beinhalten. Abweichungen bzw. Nicht-Beachtung/ -Einhaltung ist transparent offenzulegen und ggf. zu berichten.

- Planung

Durch geeignete Verfahren ist die Risikoorientierung und Vollständigkeit der Prüfungsplanung zu gewährleisten. Insbesondere ist sicher zu stellen, dass alle Aktivitäten und Prozesse erfasst sind und grundsätzlich der Prüfungsturnus von drei Jahren eingehalten wird. Zu regeln ist dabei, wer die Prüfungsplanung vorbereitet und durchführt und durch wen die wesentlichen Ergebnisse kontrolliert werden. Die Kontrolle sollte dabei sowohl die Vollständigkeit und Korrektheit der Dokumentation wie auch eine fachlich/ inhaltliche Kontrolle beinhalten und nach Möglichkeit funktionsgetrennt/ neutral erfolgen. Durch die Revisionsleitung sollte eine stichprobenhafte Überprüfung der Ergebnisse durchgeführt werden.

- Prüfungsvorbereitung

Das Prüfungsprogramm sollte durch die Prüfungsleitung oder durch erfahrene Prüfer erstellt und die fachlich/ inhaltliche Qualität (bspw. thematische Vollständigkeit, Risikoorientierung) durch die zuständige Führungskraft überprüft werden. Während der Prüfung vorgenommene wesentliche fachlich/inhaltliche Änderungen des Prüfungsprogramms sind ebenfalls zu genehmigen.

- Durchführung

Durch die Prüfungsleitung und ggf. in einem geregelten Turnus durch Führungskräfte ist sicherzustellen, dass das genehmigte Arbeitsprogramm planmäßig durchgeführt wird, es sei denn, Änderungen sind gerechtfertigt und genehmigt. Insbesondere die ausreichende Tiefe der Prüfungshandlungen und Abdeckung des Prüfungsgebietes sind hierbei zu berücksichtigen. Hierzu sollte nach Abschluss der Prüfungshandlungen verifiziert werden, dass etwaige Änderungen mit der zuständigen Führungskraft abgestimmt wurden.

- Dokumentation/Berichterstattung

Es ist festzulegen, dass Arbeitspapiere die Feststellungen, Schlussfolgerungen und Empfehlungen ausreichend untermauern. Die Berichterstattung muss fehlerfrei, objektiv, klar, knapp, konstruktiv und zeitnah erstellt sein. Hierzu sollte z. B. die Prüfungsleitung schon während der Prüfung die Arbeitspapiere kontrollieren und etwaige Mängel an den jeweiligen Prüfer adressieren. Festzulegen ist, welche Führungskräfte zu welchem Zeitpunkt die Berichtskritik durchführen. Nach Abschluss der Prüfung sollte eine angemessene/ stichprobenhafte Kontrolle durch die zuständige

Führungskraft erfolgen. Für die Bewertung der Effizienz der Prüfung können vorher definierte Meilensteine (z. B. Ende der Vorbereitung, Ende der Prüfungshandlungen, Versand des Berichtes, Abschlusskonferenz) auf ihre Einhaltung überprüft werden. In Stichproben sollten Kontrollen auch durch die Revisionsleitung oder eine von ihr benannte/ beauftragte qualifizierte Person durchgeführt werden.

- Follow-up

Das Verfahren zur Überwachung der Erledigung von festgestellten Mängeln (Follow-up) sollte in einer für das Gesamtinstitut veröffentlichten Organisationsrichtlinie oder Arbeitsanweisung geregelt sein, so dass die geprüften Einheiten über ihre Mitwirkungspflichten informiert sind. Revisionsintern ist – ggf. in Abhängigkeit vom Risikogehalt der getroffenen Feststellungen – zu regeln, wer Überwachungstätigkeiten durchführt, in welcher Tiefe die Rückmeldungen der Fachbereiche plausibilisiert oder geprüft werden und wer die Ergebnisse der Überwachung kontrolliert (Qualitätssicherung).

- Qualifikation

Es ist sicherzustellen, dass die Personalausstattung quantitativ und qualitativ zur Aufgabenerfüllung angemessen ist und dass die Mitarbeitenden fortlaufend weiterentwickelt werden. Die Überprüfung der Kapazitätsausstattung (quantitativ) und der Mitarbeitendenqualifikation (fachlich/ inhaltlich, qualitativ) ist mit in das Qualitätsmanagement der Revision einzubeziehen.

- Budgeteinhaltung

Die Einhaltung des zur Verfügung stehenden Budgets sollte in einem geordneten Verfahren überwacht und gesteuert werden. Hierbei sollten eindeutige Verantwortlichkeiten hinsichtlich der Überwachung und der Berichterstattung festgelegt werden. Zu folgenden Budgets sollten Überwachungsmaßnahmen eingerichtet werden, die neben einer Stichtagsbetrachtung auch auf die Einhaltung von Jahreszielen abzielen sollten:

- Einhaltung Prüfungsplanung:

Die in der Planung gebildeten Zeitbudgets insbesondere für Prüfungen, Beratungen, Projektbegleitungen, Follow-up Bearbeitung und Zeitreserven für Sonderprüfungen sollten laufend (mindestens vierteljährlich) überwacht werden. Ab festgelegten Schwellenwerten sollten Informations- oder Genehmigungspflichten geregelt werden. Im Ergebnis muss das Verfahren geeignet sein, frühzeitig Risiken der Einhaltung der Prüfungsplanung aufzudecken.

- Personalkostenbudget:

Je nach Erfordernis sollte ein regelmäßiges Controlling die Einhaltung des Budgets gewährleisten.

- Sachkostenbudget:
Die Auslastung des Sachkostenbudgets sollte regelmäßig ausgewertet werden und eine Hochrechnung erfolgen.
- Budget für Technologie:
Mit Hilfe eines Budgets für technologische Ressourcen kann die Digitalisierung der Revision weiterentwickelt werden (z. B. Anpassung des Revisionsmanagementsystems, Digitalisierung der Prüfungsmethoden, z. B. Datenanalysen).

Unterstützend zur laufenden internen Überwachung ist nach Prüfungsabschluss auch ein Feedback der geprüften/beratenen Stelle, z. B. in Form eines Fragebogens, einzuholen, in dem einzelne Aspekte zur Wahrnehmung der Revisionsvertreter, Prüfungsplanung, -durchführung, -berichterstattung und zum Nutzen/Mehrwert der Prüfung bewertet werden können. Alternativ kann Feedback auch zu einem späteren Zeitpunkt gebündelt eingeholt werden.

Beispiele für Feedbackbogen (Anlage 6) und für Kundenbefragung zu Revisionsprüfungen (Anlage 7) sind auf der Webseite des DIIR verfügbar.

Bei der Auswertung des Feedbacks der geprüften/beratenen Stelle ist jedoch zu beachten, dass die Prüfungsergebnisse das Feedback beeinflussen können.

Es können auch (turnusmäßige) „Stakeholder Surveys“ durchgeführt werden. Als „Stakeholder“ kommen hier Aufsichtsorgan/Prüfungsausschuss, Geschäftsleitung und ausgewählte Vertreter der 1. und ggf. 2. Führungsebene unterhalb der Geschäftsleitung sowie ggf. auch in Prüfungen involvierte Mitarbeiter in Frage. Hierbei können über einen strukturierten Fragebogen die Fragenkreise

- Wahrnehmung der Revisionsvertreter
- Betätigungsfeld der Internen Revision
- Revisionsprozess und Berichterstattung
- Steuerung der Internen Revision
- Kommunikation mit bzw. Verhältnis zu den Stakeholdern

hinsichtlich ihrer Bedeutung bzw. des Erfüllungsgrades behandelt werden.

Beispiele für Stakeholder Survey Aufsichtsgremium (Anlage 8) und für Stakeholder Survey Geschäftsleitung (Anlage 9) sind auf der Webseite des DIIR verfügbar.

Die Gesamtverantwortung für die laufende Überwachung liegt bei der Revisionsleitung wobei die Durchführung der Qualitätsüberwachung auf geeignete Mitarbeitende (z. B.

Grundsatzfunktion, Führungskräfte, Prüfungsleiter) übertragen werden kann. Für die Dokumentation der erfolgten laufenden Überwachung empfiehlt es sich, für Prüfungsaufträge eine Prüfungs-/Qualitätscheckliste zu nutzen. Diese sollte z. B. Verantwortlichkeiten, Planungsaspekte und -vorgaben, zeitliche Meilensteine und Qualitätssicherungspunkte enthalten sowie nach Prüfungsabschluss von der Prüfungsleitung und einer weiteren von der Revisionsleitung benannten Person unterschrieben und den Prüfungsunterlagen beigelegt werden.

Ein Beispiel für eine Checkliste zur Prüfungsqualität ist auf der Webseite des DIIR verfügbar (Anlage 10).

12.3.2 Periodische interne, prozessunabhängige Beurteilung und Leistungsmessung

Ergänzend zur laufenden internen Überwachung schreiben die Berufsstandards (GIAS Standard 12.1) regelmäßige Beurteilungen in Form von Selbstbeurteilung durch Mitarbeitende der Internen Revision mit geeigneter Qualifikation (z. B. Anerkannter Prüfer IRS) vor, die die Übereinstimmung der Internen Revision mit

- ihrer Definition
- den Ethikanforderungen (GIAS Domain II)
- und den GIAS insgesamt

bewerten sollen. Als Ergebnis der Beurteilung soll ein abschließendes Urteil bzgl. der Qualität der Aufgabenerfüllung der Internen Revision stehen, in dem Verbesserungspotentiale identifiziert und dokumentiert werden. Der Leiter der Internen Revision muss sicherstellen, dass erforderliche korrigierende Maßnahmen ergriffen werden. Es empfiehlt sich diese interne Qualitätssicherungsmaßnahme neutral (in der Internen Revision) anzusiedeln. Eine Selbstüberprüfung sollte auf jeden Fall vermieden werden.

Soweit die Anforderungen nicht jährlich vollständig überprüft werden, empfiehlt es sich ein umfassendes, ggf. auf einem mehrjährig rollierenden risikoorientierten Plan angelegtes Qualitätsmanagementprogramm zu implementieren. Diese sollte die einzelnen Qualitätsmanagement-Maßnahmen und alle Prozesse/ Tätigkeiten der Internen Revision abdecken. Neben turnusmäßig anfallenden Tätigkeiten (z. B. Überprüfung Revisionshandbuch und Rahmenbedingungen, stichprobenhafte Überprüfung der Einhaltung ausgewählter Vorgaben) sollten hier auch aktuelle Themen Berücksichtigung finden.

Die Ergebnisse interner Beurteilungen sollten durch die Revisionsleitung gem. GIAS Standard 8.3 mindestens jährlich an relevante interne Stellen (z. B. Geschäftsleitung,

Aufsichtsorgan, Audit Committee) kommuniziert und berichtet werden (z. B. separate Berichterstattung über die Beurteilung, alternativ Berichterstattung im Jahresbericht der Internen Revision).

Des Weiteren sollten mögliche Verbesserungspotentiale für die Weiterentwicklung der Internen Revision, die aus der internen Qualitätssicherung erkannt werden, aufgegriffen werden.

Periodische interne Beurteilungen dienen auch als Vorbereitung und Unterstützung für die mindestens alle fünf Jahre durchzuführenden externen Beurteilungen. Somit ist es empfehlenswert sich hier eng an der inhaltlichen Gestaltung externer Reviews, z. B. durch Abgleich mit den GIAS-Anforderungen und zu orientieren.

Ein weiteres bedeutendes Element ist die Leistungsmessung (GIAS Standard 12.2) unter dem Aspekt der Qualitätsverbesserung.

Die Revisionsleitung hat abgeleitet aus der Revisionsstrategie Ziele zu entwickeln und zu messen sowie die Erreichung der Ziele zu beurteilen, die darauf abzielen die Qualität/ Leistung der Internen Revision kontinuierlich zu verbessern (Stichwort „Conformance“ – Quality & Performance). Die Ergebnisse dieser Zielerreichung/ -messung ist zu berichten/ kommunizieren.

Weitergehende Ausführungen zu Kriterien/ Key Performance Indicators für die Interne Revision sind im Kapitel 15 – Leistungsmessung (KPI) in diesem RV-HB detailliert dargestellt.

Es sollte sichergestellt werden, dass bei der Entwicklung/ Definition und Messung der KPI in der Internen Revision die Revisionsstrategie, die strategischen/ operativen Ziele und die Aspekte des Qualitätsmanagements angemessen berücksichtigt werden, so dass diese auf die Erfüllung des Mandates der Internen Revision einzahlen.

12.4 Externe Beurteilung

12.4.1 Externe Beurteilung

Eine wesentliche Maßnahme zur Sicherung der Qualität interner Revisionsleistungen stellt die Durchführung einer externen Beurteilung (Assessment) dar. Gemäß GIAS Standard 8.4 müssen externe Beurteilungen von einem qualifizierten, unabhängigen Prüfer oder Prüfungsteam mindestens alle fünf Jahre durchgeführt werden. Das DIIR bietet Fortbildungsveranstaltungen zum anerkannten Prüfer für Interne Revisionsysteme^{DIIR}

an. Bei der Auswahl des unabhängigen Beurteilers muss die Revisionsleitung sicherstellen, dass mindestens eine Person eine aktive Zertifizierung als Certified Internal Auditor® besitzt.

Ergänzt werden die GIAS durch den vom DIIR veröffentlichten Revisionsstandard Nr. 3 Prüfung von Internen Revisionssystemen (Quality Assessments) In Zusammenarbeit mit dem IDW (Institut der Wirtschaftsprüfer in Deutschland e.V.) entstanden mit IDW PS 983 und DIIR Revisionsstandard Nr. 3 inhaltlich weitestgehend gleichlautende Standards zur Prüfung von Internen Revisionssystemen. Dieser Leitfaden enthält Empfehlungen zur Beurteilung der Einhaltung der Global Internal Audit Standards. Dies umfasst die Erreichung der Prinzipien und der Zielsetzung einer wirksamen Internen Revision.

Der DIIR Revisionsstandard Nr. 3 enthält ein Modell für die Beurteilung der Einhaltung der Standards, der Erreichung der Prinzipien sowie der Beurteilung der Wirksamkeit insgesamt. Er umfasst den Kriterienkatalog (aus den GIAS), als empfohlenes Hilfsmittel für die Beurteilung und geht abschließend auf die Berichterstattung über die Qualitätsbeurteilung ein. Die quantitative Bewertung ist dabei optional.

Die Details zur Vorgehensweise/ Methodik, Berichterstattung und Bewertung sind ausführlich im DIIR Revisionsstandard Nr. 3 geregelt und definiert.

12.4.2 Selbstbeurteilung mit unabhängiger Überprüfung

Zur regelmäßigen Standortbestimmung empfiehlt sich in Ergänzung zur Externen Beurteilung (ggf. z. B. auch zwischen den externen Beurteilungsterminen) eine Selbstbeurteilung durch den Bereich Revision. Diese bietet sich auch in Vorbereitung eines Externen Quality Assessments an. Ferner kann eine interne Selbstbeurteilung mit unabhängiger Überprüfung auch das Element der externen Beurteilung erfüllen.

Es besteht auch die Möglichkeit, eine Selbstbeurteilung mit unabhängiger externer Bestätigung anstelle einer Externen Beurteilung durchzuführen (GIAS Standard 8.4). Dies kann insbesondere bei kleineren Revisionsabteilungen angebracht sein. Hierbei wird im Rahmen des zuvor dargestellten internen Qualitätssicherungsprogramms ein umfassender und vollständig dokumentierter Selbstbewertungsprozess durchgeführt, der auch den externen Beurteilungsprozess nachbilden muss. Insoweit empfiehlt es sich das interne Qualitätsprogramm eng an den externen Qualitätsvorgaben anzulehnen.

Hier ist im Nachgang eine unabhängige Überprüfung vor Ort durch einen qualifizierten Prüfer durchzuführen, allerdings sollte durch die Erarbeitung der Selbstbeurteilung der Zeit- und Ressourceneinsatz im Vergleich zu einem umfänglichen externen Assessment verringert sein.

Empfohlen wird, dass eine Arbeitsgruppe im Auftrag der Revisionsleitung den Selbstbeurteilungsprozess durchführen und vollständig dokumentieren soll. In größeren Revisi-
onseinheiten besteht auch die Möglichkeit, bestimmte Mitarbeitende dauerhaft mit Aufga-
ben des Qualitätsmanagements zu betrauen, die dann auch für die Durchführung von
Quality Self Assessments und (internen) Quality Audits eingesetzt werden können. Ein
Berichtsentwurf, gleich dem für eine externe Beurteilung, sollte erstellt werden. Ein fach-
kundiger, unabhängiger Prüfer sollte eine Validierung der Selbstbeurteilung vornehmen,
um die Ergebnisse zu bestätigen und eine Stellungnahme über das angegebene Niveau
der Übereinstimmung mit den Standards für die berufliche Praxis der Internen Revision
abzugeben. Als Abschluss der unabhängigen Bestätigung soll er dem Bericht eine zu-
stimmende Stellungnahme hinzufügen.

Wenn der unabhängige Prüfer der Beurteilung bezüglich des Einhaltens der GIAS nicht
zustimmt, soll er dem Bericht eine widersprechende Stellungnahme hinzufügen, welche
die Meinungsverschiedenheiten und – soweit als sinnvoll erachtet – die wesentlichen
Feststellungen, Schlussfolgerungen und Empfehlungen in dem Bericht konkretisiert.

Obwohl eine vollständig externe Prüfung den größten Nutzen für die Interne Revision
bietet und im Qualitätsprogramm der Internen Revision vorgesehen sein sollte, bietet die
Selbstbeurteilung mit externer Überprüfung eine alternative Methode zum vollständigen
Erfüllen der Anforderungen der GIAS Standard 8.4. Trotzdem und soweit möglich, sowie
um den größtmöglichen Nutzen für Qualitätssicherung und Ablaufverbesserung zu erzie-
len, sollte eine Interne Revision die Selbstbeurteilung mit unabhängiger Überprüfung als
Zwischenlösung betrachten und eine vollständig externe Prüfung in den Folgeperioden
anstreben.

Die Vorgaben zur Berichterstattung sind auch bei der Selbstbeurteilung mit externer Vali-
dierung entsprechend der Standards zu berücksichtigen.

Quellenverzeichnis:

DIIR-Revisionsstandard Nr. 3/ DIIR-Leitfaden zur Qualitätsbeurteilung der Internen Revision

DIIR-Insights: Die neuen Global Internal Audit Standards für die Interne Revision, 2024

13 Leistungsmessung der Internen Revision

Aufgabe der Internen Revision ist, die strategischen Ziele und den Erfolg der Organisation zu unterstützen sowie ggf. weitere Erwartungen der Geschäftsleitung und anderer wichtiger Stakeholder zu erfüllen. Die Revisionsleitung muss eine entsprechende Strategie entwickeln und daraus die strategischen Ziele für die Interne Revision ableiten (vgl. GIAS Standard 9.2). Dabei ist für die Interne Revision in Instituten der Auftrag gemäß AT 4.4.3 Tz. MaRisk, risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse zu prüfen und zu beurteilen, unabhängig davon, ob diese ausgelagert sind oder nicht, zu berücksichtigen.

Eine weitere Anforderung an die interne Steuerung der Internen Revision ergibt sich auch aus GIAS Standard 12.2. Die Leitung der Revision muss Ziele – abgeleitet aus der Revisionsstrategie und unter Einbindung der Stakeholder (z. B. Geschäftsleitung) und deren Erwartungshaltung – definieren, mit denen er die Leistung der Revision bewerten, steuern und messen kann. Die Ziele sollen darauf einzahlen, die Leistung der Revision kontinuierlich zu verbessern und die diesbezüglichen Fortschritte zu messen. Zur Beurteilung der Leistung der Revision sollte auch ein Feedback von den Stakeholdern eingeholt werden. Sofern Probleme auftreten oder die gesteckten Ziele nicht erreicht werden, sind geeignete Maßnahmen abzuleiten und zu überwachen.

Daneben können sich weitere operative Ziele im Zusammenhang mit den Maßnahmen zur Qualitätssicherung, -verbesserung und -messung ergeben, die in die Leistungsmessung einbezogen werden können (vergl. hierzu auch die Ausführungen im Kapitel 12 Qualitätssicherung/ -verbesserung).

In die Leistungsziele fließen somit die institutsspezifisch relevanten Aspekte aus den Prinzipien der GIAS, der Audit Charter bzw. den Rahmenbedingungen der Internen Revision, der Revisionsstrategie und dem Qualitätsmanagement ein. Das übergeordnete Ziel sollte sein, mit einer angemessenen und wirksamen Leistungsmessung die erfolgreiche Erfüllung des Mandates der Revision sicherzustellen und damit einen klaren und messbaren Mehrwert für das Institut zu erbringen.

Wichtig ist, dass die Leitung der Internen Revision darauf achtet, sowohl die Effektivität als auch die Effizienz ihrer Prüfungs- und Beratungsleistungen sicherzustellen und zu steuern, um einen größtmöglichen Mehrwert zu erzielen. Der Fokus nicht nur auf eine effiziente bzw. „kostenoptimale“ Prozessdurchführung, sondern auch auf die Qualität der Prüfungs- und Beratungsleistung gelegt werden. Die qualitativen Aspekte spiegeln sich insbesondere in einer risikoorientierten Vorgehensweise, der umfassenden, objektiven Beurteilung von Sachverhalten und einer hohen Qualifikation der Prüfer wider.

Für die erfolgreiche Durchführung einer regelmäßigen Leistungsmessung der Internen Revision gilt es, eine Vielzahl von Informationen in geeigneter Form zu verdichten und die Relevanz für die Überwachung und Steuerung mit Blick auf die Zielerreichung zu bestimmen. In der Regel erfolgt die Umsetzung anhand von festzulegender Steuerungs- bzw. Kenngrößen, die auch als sog. Key Performance Indicator (KPI) bezeichnet werden.

13.1 Definition und Ziele von KPIs

Unter KPIs werden im Allgemeinen Kenngrößen zur Leistungsmessung verstanden, die häufig quantitativ, aber durchaus auch qualitativ ausgeprägt sein können. Zum Teil lassen sich qualitative Kenngrößen in einem gewissen Rahmen quantifizieren bzw. auf eine Ordinalskala übertragen und somit rechnerisch auswertbar machen. Eine über das allgemeine Verständnis hinausgehende Definition von KPIs existiert nicht. Auch für Institute ist der Begriff KPI nicht spezifisch definiert.

KPIs können die Erreichung strategischer wie auch operativer Ziele messen. In der Praxis hat sich in Bezug auf die Leistungsmessung in der Internen Revision gezeigt, dass die verwendeten Kenngrößen primär auf die operative Steuerung ausgerichtet sind. Dabei ist jedoch auch zu berücksichtigen, dass eine eindeutige Abgrenzung zwischen strategischen und operativen Kenngrößen in der Praxis schwierig ist, da auch die Zielsetzungen ineinander übergehen.

Im Hinblick auf die Verfolgung strategischer und operativer Ziele kann die Ermittlung und Berichterstattung von KPIs u. a. auch, unmittelbar oder mittelbar als ein Beurteilungskriterium bei der Festlegung der Vergütung bzw. der jährlichen variablen Vergütung für den Leiter der Revision und ggf. für die Führungskräfte und Mitarbeiter in der Internen Revision einfließen.

13.2 Prozess zur Festlegung von KPIs

13.2.1 Ableitung und Definition von KPIs

Die Erwartungen der Stakeholder sollten sich in einer GIAS-konformen Revisionsstrategie wiederfinden. Insofern ist eine gesonderte Erhebung dieser Erwartungen nicht erforderlich. Die strategischen KPIs können aus der Revisionsstrategie abgeleitet werden und die Umsetzung der in der Revisionsstrategie definierten Ziele messbar machen. Dazu sollten in der Revisionsstrategie Kriterien enthalten sein, die die Aspekte der Effektivität und Effizienz („Performance“) sowie Qualität („Conformance“) und damit auch die Erwartung der Stakeholder berücksichtigen. Darüber hinaus können weitere – operative – KPIs zur Weiterentwicklung/ Steuerung der Revision definiert werden.

Sofern keine Revisionsstrategie vorliegt, können zur Definition von KPIs Faktoren, die die Effektivität einer Internen Revision im Hinblick auf ihre Aufgabenstellung ausmachen zu identifizieren. Die Aufgabenstellung der Internen Revision kann aus gesetzlichen bzw. aufsichtsrechtlichen Vorgaben, den GIAS, den strategischen Zielen des Unternehmens abgeleitet werden. Daraus sind konkrete Zielsetzungen abzuleiten und messbare Zielwerte zu definieren.

In einem zweiten Schritt sollten die in- und externen Interessensgruppen (Stakeholder) der Internen Revision identifiziert, deren Erwartungshaltung eruiert und in die Entwicklung der KPI einbezogen werden. Stakeholder sind insbesondere die Organe bzw. Funktionen, die einen Nutzen aus den Ergebnissen der Internen Revision ziehen und/oder die Ressourcenausstattung direkt oder indirekt festlegen oder zumindest beeinflussen können.

Auf dieser Basis können dann Messgrößen für die Effektivität und Effizienz sowie Qualität der Internen Revision entwickelt werden, die auf unterschiedliche Stakeholder ausgerichtet sind und verschiedenen Perspektiven in Bezug auf die Leistungsmessung zugeordnet werden.

Im letzten Schritt gilt es dann, angemessene Überwachungs- und Berichtsprozesse zu etablieren und die Ergebnisse für die Steuerung und Ausrichtung der Internen Revision zu verwenden bzw. Maßnahmen zur Zielerreichung einzuleiten.

Die KPIs sollten regelmäßig, zumindest jährlich bzw. bei Änderungen der Revisionsstrategie, zu überprüft und ggf. aktualisiert werden.

13.2.2 Einbindung in Konzernstrukturen und Konzernvorgaben

Im Rahmen von Konzernstrukturen sind einzelne KPIs häufig bereits von der Obergesellschaft vorgegeben oder die Interne Revision in der Tochtergesellschaft ist in eine konzernweite KPI-Struktur eingebunden. Jedoch bedeutet die Existenz von Konzernstrukturen nicht, dass damit zwangsläufig konzernweit einheitliche KPIs vorzugeben bzw. zu berichten sind. Ggf. können neben Konzern-KPIs weitere spezifische KPIs in den Tochterunternehmen festgelegt werden.

13.2.3 Ableitungen anhand der Dimensionen einer Balanced Scorecard

Die Ableitung von KPIs aus der Revisionsstrategie bzw. der Audit Charter hat gezeigt, dass sich die Leistungsmessung über ein breites Spektrum erstrecken kann und nicht nur auf die originären Revisionsprozesse begrenzt ist. Um dieser erweiterten Perspektive Rechnung zu tragen, wird in der Praxis z. B. auf den Ansatz der „Balanced Scorecard“

zurückgegriffen. Hierbei erfolgt die Leistungsmessung im klassischen Modell anhand von vier Perspektiven, die grundsätzlich auch für die Steuerung der Internen Revision herangezogen werden können:

- Interne Prozesse in der Internen Revision
- Personal- und Sachaufwand der Internen Revision (Finanzen)
- Kunden bzw. Stakeholder der Internen Revision
- Mitarbeitende (inkl. Qualifikation)

Der Schwerpunkt, der in der Praxis verwendeten KPIs liegt bei den Revisionsprozessen, so ist z. B. die Einhaltung der Prüfungsplanung ein häufig verwendeter KPI. Weitere prozessbezogene KPIs sind beispielsweise Anzahl von Datenanalysen im Rahmen von Prüfungen, der Umfang des Continuous Monitorings oder der Umfang des Wissensmanagements. Finanzkennzahlen spielen in der Revisionspraxis eher eine untergeordnete Rolle.

13.2.4 Operationalisierung und Festlegungen bei KPIs

Prinzipiell ist die Messung rein quantitativer KPIs leichter als bei qualitativ ausgerichteten KPIs. Die Übersetzung qualitativer KPIs in quantitative Kenngrößen bzw. in eine Ordinalskala (z. B. Schulnoten) stellt einen praktikablen Weg dar, Auswertungen zu ermöglichen. Die Übersetzung erfordert jedoch deutlich klare und eindeutige Regelungen bzw. Festlegungen, um eine konsistente Bewertung über Organisationseinheiten und Zeitperioden hinweg sicherzustellen.

Aber auch für rein quantitative KPIs ist es in der Regel hilfreich, eine klare Definition zu Inhalt und Berechnung der Kennzahlen zu festzulegen und zu dokumentieren.

13.2.5 Managementaufgabe

KPIs werden grundsätzlich vom Leiter der Internen Revision, unter Einbindung bzw. in Abstimmung der Geschäftsleitung und ggf. unter Information des Überwachungsorgans, festgelegt. Hierbei wird auch die Berichterstattung zur Leistungsmessung definiert.

Bei der Entwicklung der Kennzahlen bietet es sich an, eine Grundsatzabteilung wie auch die erste Führungsebene der Internen Revision einzubinden, um die interne Akzeptanz und damit die Steuerungswirkung zu erhöhen.

Darüber hinaus ist sicherzustellen, dass der Betriebs- bzw. Personalrat bezüglich der vorgesehenen KPIs sowie den zugrundeliegenden Datenhaushalten bzw. Auswertungen

in den Revisionssystemen eingebunden wird, wenn einzelne Kenngrößen die Leistungsbeurteilung von Mitarbeitenden ermöglichen können. Des Weiteren sind Aspekte der EU-DSGVO ggf. zu berücksichtigen.

Neben der Festlegung von KPIs sind vom Leiter der Internen Revision auch die organisatorischen Voraussetzungen für die Erhebung und Berichterstattung zu schaffen. In der Praxis werden diese Aufgaben von einer zentralen Stelle innerhalb der Internen Revision wahrgenommen. Für die Ermittlung von Kennzahlen werden üblicherweise Daten aus der eingesetzten Revisionssoftware ausgewertet, so dass für die Erhebung bzw. Ermittlung der Kennzahlen nicht zwangsläufig weitere Systeme eingerichtet werden müssen.

13.3 Auswertung und Berichterstattung von KPIs

Die Ermittlung und Auswertung von KPIs mündet grundsätzlich in eine regelmäßige Berichterstattung, die als Adressaten neben der Leitung der Revision auch die relevanten Stakeholder (z. B. Geschäftsleitung, ggf. Aufsichtsorgan, ggf. Konzernrevision) beinhalten sollte. Eine Zweistufigkeit ist denkbar. So können z. B. aus der Strategie abgeleitete KPIs an die Stakeholder und eher operative, aus dem Qualitätsmanagement abgeleitete KPIs lediglich an die Revisionsleitung berichtet werden.

In der Berichterstattung sollten auch Maßnahmen festgehalten werden, sofern Ziele verfehlt wurden.

Die Berichterstattung von KPIs zielt damit auch auf die nachvollziehbare Einhaltung aufsichtsrechtlicher Vorgaben oder der Internationalen Grundlagen für die berufliche Praxis (IPPF/ GIAS) ab. Darüber hinaus ist es auch ein Medium, gegenüber den Stakeholdern die Leistungsfähigkeit der Internen Revision darzustellen. Gleichzeitig wird mit der Berichterstattung die insbesondere im GIAS Standard 12.2 geforderte kontinuierliche Leistungsmessung und -beurteilung der Internen Revision transparent dargestellt.

13.3.1 Datenquellen und Aufwand für Aufbereitung

Die Ermittlung und Auswertung von KPIs erfolgt in der Regel durch eine zentrale Stelle innerhalb der Internen Revision. Die KPIs werden in den überwiegenden Fällen aus der Software zur Prüfungsadministration ermittelt. Dies liegt auch darin begründet, dass eine Vielzahl der verwendeten KPIs sich auf den Revisionsprozess beziehen.

Weitere Datenlieferungen erfolgen durch (ergänzende) zentrale, anlassbezogene Abfragen. Für die Auswertungen von KPIs werden zum Teil separate, zentral geführte Datenbanken eingesetzt. Die Auswertung der Daten kann je nach Art des KPIs monatlich, quartalsweise bzw. halbjährlich oder jährlich erfolgen.

In der Praxis wird der Zusatzaufwand für die Datenerfassung und die Ermittlung der KPIs in den überwiegenden Fällen als vertretbar mit grundsätzlich mittlerem Aufwand eingestuft. Je nach Umfang der Auswertungen und Verfügbarkeit der Daten kann dies bei einzelnen Instituten aber auch zu abweichenden Einstufungen führen. Insgesamt muss vor dem Hintergrund eines effizienten internen Controlling-Prozesses der Nutzen einer Steuerungsmöglichkeit den damit verbundenen Zusatzaufwand rechtfertigen.

Bei den Datenquellen und deren Aufbereitung ist auch auf die Schutzbedürftigkeit von Daten, die zur Leistungsmessung von Mitarbeitern herangezogen werden können, zu achten und die Datenhaltung bzw. -auswertung ggf. mit dem Betriebs- bzw. Personalrat abzustimmen.

13.3.2 Grenzen von KPIs

Die Kenngrößen zeichnen sich durch die Aggregation von vielen Informationen zu einer Größe aus. Darüber hinaus liegt es bei der Vielzahl von möglichen KPIs nahe, sich auf wesentliche KPIs zu begrenzen und diese für die Steuerung einzusetzen. Vor diesem Hintergrund muss jedoch immer auf die begrenzte Aussagekraft einzelner Kennzahlen hingewiesen werden. Es ist wichtig, im Rahmen der Auswertung von Kennzahlen auch Zusammenhänge zu verdeutlichen und auf Wechselwirkungen einzugehen. Die Bewertung und Steuerung nach einzelnen Kenngrößen birgt die Gefahr von Fehlinterpretationen und Fehlimpulsen.

Am Beispiel der Anzahl der durchgeführten Prüfungen bzw. der Erfüllung des Prüfungsplans lässt sich beispielhaft nachvollziehen, dass selbst ein hoher Erfüllungsgrad dieser KPIs nichts über die Qualität der Prüfung selbst und der Bedeutung des Prüfungsgebietes bzw. der Relevanz des Prüfungsgebietes aussagt. Eine Steuerung ausschließlich nach diesem KPI könnte dazu führen, dass kritische Aspekte im Rahmen der Prüfung nicht hinreichend betrachtet werden, um den engen Zeitplan einzuhalten. Die Ansprüche an die Qualität der Prüfung und somit die Erfüllung der GIAS könnten beeinträchtigt werden.

13.4 Steuerungsmaßnahmen

Die Auswertung und Berichterstattung von KPIs ist kein Selbstzweck, sondern stellt die Grundlage für ggf. zu ergreifende Steuerungsmaßnahmen in der Internen Revision dar. Hinsichtlich der Steuerungsfunktion durch KPIs sind unterschiedliche Ebenen zu betrachten.

Durch klare Kommunikation der betrachteten Kenngrößen können sich Mitarbeitende daran ausrichten, ihr eigenes Handeln im Sinne der Zielwerte zu steuern und dadurch maßgeblich zur Erreichung der Ziele und der Erfüllung des Mandats sowie der Revisionsstrategie der Internen Revision als Ganzes beitragen.

Auf der Ebene der Führungskräfte bedeutet dies, dass neben der Analyse der Entwicklung einzelner Kennzahlen auch die erforderlichen Schlüsse daraus gezogen und bei Bedarf Aktivitäten initiiert werden müssen. Die Wirksamkeit und Akzeptanz der KPIs hängt entscheidend davon ab, dass die Ergebnisse für Steuerungszwecke sinnvoll genutzt werden. Insbesondere bei negativen Abweichungen von Zielwerten sind die Ursachen hierfür zu ermitteln und geeignete Gegensteuerungsmaßnahmen abzuleiten.

Auf Ebene der Stakeholder ist zu hinterfragen, ob die Ressourcen bzw. die Qualifikation der in der Internen Revision beschäftigten Personen ausreichen, wenn bestimmte KPIs dauerhaft verfehlt werden. Sofern die Leitung der Internen Revision in diesem Fall nicht selbst geeignete Maßnahmen vorschlägt, sind von Seiten der Stakeholder – bei einem Institut von der Geschäftsleitung bzw. dem Vorstand – Maßnahmen zu ergreifen.

13.5 Erwartungshaltung und Akzeptanz

Die Identifikation und Definition von KPIs bzw. vorgelagert die Entwicklung einer Revisionsstrategie gem. GIAS, bietet der Leitung der Internen Revision die Möglichkeit die Erwartungshaltung der Stakeholder zu adressieren bzw. den Nutzen und Mehrwert der Internen Revision sichtbar zu machen. In Abhängigkeit von der Geschäfts- und Risikostrategie des Instituts, dem Reifegrad der Organisation und den Mindset der verantwortlichen Personen können sich unterschiedliche Schwerpunkte ergeben. Wichtig ist, dass sich auf Basis der KPIs bzw. der Berichterstattung ein fruchtbarer Dialog zwischen der Revisionsleitung und den Stakeholdern ergibt.

Auf Seiten der Führungskräfte in der Internen Revision besteht i. d. R. eine positive Erwartungshaltung in Bezug auf KPIs, die zur Steuerung der Revisionseinheit genutzt werden können, entsprechend hoch ist auch die Akzeptanz für deren Einsatz.

Hingegen ist auf Ebene der Mitarbeitenden die Akzeptanz von Kenngrößen typischerweise weniger stark ausgeprägt und löst zum Teil auch Widerspruch bzw. Widerstand aus. Dabei sind die Bedenken hinsichtlich einer möglichen individuellen Leistungsmessung zu berücksichtigen. Daher sollte insbesondere gegenüber den Mitarbeitenden die Ermittlung und Auswertung von KPIs sowie die abgeleiteten Aktivitäten und Maßnahmen transparent gemacht werden, um möglichen Vorbehalten entgegenwirken zu können.

13.6 Kenngrößen für die Leistungsmessung der Internen Revision

Der Einsatz bzw. Umfang von KPIs ist abhängig von der individuellen Strategie und Zielsetzung und der kulturellen Prägung der jeweiligen Internen Revision bzw. des Instituts. Allgemeingültige bzw. als Mindeststandard zu verstehende Kenngrößen können daraus bisher nicht abgeleitet werden.

Neben den einzelnen Kenngrößen sind auch deren Zielgrößen grundsätzlich von der jeweiligen Internen Revision individuell festzulegen. Auch hierbei kann kein allgemeingültiger Zielwert abgeleitet werden. Im Hinblick auf die Grenzen von KPIs (vgl. Abschnitt 1.4.2) sind Zielwerte als Einzelgrößen zu relativieren. Wichtig ist die Referenzierung und Berücksichtigung der Ziele und Vorgaben aus der Revisionsstrategie und ggf. weiterer Anforderungen, z. B. seitens der Stakeholder.

13.6.1 KPIs zum Revisionsprozess

Die KPIs zum Revisionsprozess stellen die größte Anzahl bzw. Vielfalt von Kennzahlen dar und haben auch bezüglich ihrer praktischen Nutzung grundsätzlich einen hohen Anwendungsgrad. Der Schwerpunkt liegt insbesondere auf quantitativen Kenngrößen zur Prozessdurchführung und somit auf der effizienten Ausgestaltung der Internen Revision. Im Folgenden eine Auswahl möglicher KPIs zum Revisionsprozess:

KPIs zum Revisionsprozess	Erläuterung
Prüfungsdauer/Zeitdauer bis zur Erreichung von Meilensteinen im Prüfungsprozess	Zeitdauer der Prüfung (seit Kick-Off) Zeitdauer bis Berichterstattung
Abarbeitung des Jahresprüfungsplans	Grad der Planerfüllung in Anzahl Prüfungen bzw. gewichtet nach geplanten Prüfertagen; gemessen am Ende des Jahres oder z. B. quartalsweise
Prüfungsaufwand	Personelle (Prüfertage) und/oder finanzielle Ressourcen
Budgettreue (Prüfungstage)	Ist-Aufwand/Plan-Aufwand Messung für Gesamtaufwand oder für die einzelnen Teilprozesse der Prüfungsdurchführung
Zeitdauer/Termtreue im Follow-up	Durchschnittliche Dauer bis zur Erledigung von Maßnahmen
Überfällige bzw. wiederholt getroffene Feststellungen	Anteil an der Gesamtanzahl von Feststellungen
Zielrichtung (z. B. IKS, Compliance oder Effizienz) und Schweregrad von Feststellungen	Anzahl von Feststellungen nach Risiko-klasse/Schweregrad bzw. nach Zielrichtung
Externe Feststellungen an die Interne Revision	Anzahl der Feststellungen, ggf. nach Schweregrad
Qualität und Zufriedenheit	Ergebnis eines externen Quality Assessments in Bezug auf Revisionsprozess; Ergebnis des Kundenfeedbacks
Prüfungs- und Beratungsaufträge	Anzahl/Umfang (in PT) der Prüfungs- und Beratungsleistungen

Abb. 17: KPIs zum Revisionsprozess

13.6.2 KPIs zur Mitarbeitenden-Perspektive

Bei den KPIs aus der Mitarbeitenden-Perspektive handelt es sich häufig um quantitativ übersetzte Kenngrößen, die in der Regel auf qualitative Aspekte im Hinblick auf die Kenntnisse und Fertigkeiten (inkl. Einsetzbarkeit in anderen Einheiten) abzielen. Im Folgenden eine Auswahl möglicher KPIs zur Mitarbeitenden-Perspektive:

KPIs zu Mitarbeitenden-Perspektive	Erläuterung
Weiterbildungstage	Anzahl der Weiterbildungstage/Mitarbeitender
Mitarbeitendenanzahl Interne Revision/ Gesamtunternehmen	Personelle Ausstattung der Internen Revision
Abrechenbare Prüfungsleistung (Prüfertage)	Einsatz der Mitarbeitenden in Prüfungen und prüfungsnahen Leistungen (Effizienz des Personaleinsatzes)
Fluktuation	Wechselquote
Entwicklung in anspruchsvolle Management- und Spezialistenfunktionen (revisionsintern/-extern)	Auswertung der Fluktuation
Berufserfahrung (in Jahren)	Durchschnittliche Revisionserfahrung bzw. Erfahrung in relevanten Prüfungsgebieten
Anteil Mitarbeitende mit Berufsexamina	(z. B. CIA, CISA, Interner Revisor ^{DIR} , Teilnahme an Fachseminaren)
Mitarbeitendenzufriedenheit und -engagement	Ergebnisse aus Umfragen
Fristgerecht durchgeführte Beurteilungsgespräche	Nutzung von Potenzialbeurteilungs- und -entwicklungsmöglichkeiten

Abb. 18: KPIs zur Mitarbeitendenperspektive

13.6.3 KPIs zur Finanz-Perspektive

Die Auslastung der Personal- und Sachkostenbudgets der Internen Revision stellt grundsätzlich den klassischen KPI in der Finanzperspektive dar und wird am häufigsten ausgewertet. Zusätzlich können KPIs auf Unternehmensebene, die die Erreichung des Prüfungsziels „Wirtschaftlichkeit“ im Rahmen von Prüfungen adressieren, aufgenommen werden.

KPIs zu Finanzperspektive	Erläuterung
Budgetauslastung (Personal-/Sachkosten, Projektbudget)	Plan/Ist-Vergleich der Aufwände
Einzelbudgets: Reisekostenbudget, Trainingsbudget, Co-Sourcing Budget	Finanzielle Ressourcenausstattung zur Erfüllung der Aufgaben
Allokation auf Prüfungen, prüfungsnah und sonstige Tätigkeiten	Verwendung der Ressourcen
Identifizierte Wirtschaftlichkeitspotenziale	durch Prüfungen/Beratungen generierte finanzielle Optimierungen

Abb. 19: KPIs zur Finanzperspektive

13.6.4 KPIs zur Stakeholder-Perspektive

Die KPIs zielen primär auf qualitative Aspekte der Revisionsfunktion ab. Der Anwendungsgrad ist relativ hoch und spiegelt die hohe Bedeutung dieser Perspektive wider: Die Ableitung von KPIs aus strategischen Zielen der Kreditinstitute führt dabei regelmäßig zu einer hohen Akzeptanz der Internen Revision.

KPIs zur Stakeholder-Perspektive (Geprüfte und Auftraggeber)	Erläuterung
Externe Feststellungen mit Bezug zur Internen Revision	Effektivität der Internen Revision, Umsetzung des Revisionsauftrages
Ergebnis externes Quality Assessment	Einhaltung von Standards und Prozessen
Ergebnis Interner Quality Review	Einhaltung interner Standards und Prozessvorgaben (z. B. rechtzeitige Ankündigung der Prüfung) sowie des Leitbildes (z. B. wertschätzende Kommunikation)
Akzeptanz der geprüften Einheit/Abschlussbewertung	Beurteilung/Note aus dem Feedback
Anzahl der Beratungsaufträge vs. Prüfungsaufträge	Grad der (freiwilligen) Einbindung
Anzahl wesentlicher Impulse oder Feststellungen	Ableitung von Impulsen zur Erfüllung strategischer Ziele

Abb. 20: KPIs zur Stakeholder-Perspektive

13.6.5 KPIs zur Verwendung in Zielvereinbarungen mit der Leitung der Internen Revision

Grundsätzlich eignen sich die vorgenannten KPIs auch zur Zielvereinbarung mit der Leitung und Führungskräften der Internen Revision und können bei der Bemessung der variablen Vergütung einfließen. Meist werden in diesem Zusammenhang ergänzend Ziele aufgenommen, die mit dem gesamten Managementteam des Instituts vereinbart werden, wie z. B. Betriebsergebnis/Gewinn, Cost-Income-Ratio, ESG/ Nachhaltigkeitsziele und Diversity-Ziele.

KPIs zur Verwendung in Zielvereinbarungen mit der Revisionsleitung	Erläuterung
Mehrwert der Internen Revision	Beiträge/Impulse der Internen Revision zur Weiterentwicklung des Instituts oder der Geschäftsprozesse bzw. zur erforderlichen Umsetzung von (aufsichts-)rechtlichen Anforderungen. Messbar durch Abstufung der Anzahl von Beiträgen/Impulsen der Internen Revision, die jedoch einer abgestimmten Definition bedürfen. Ggf. wird vom (zuständigen) Mitglied der Geschäftsleitung festgelegt, welche von der Revisionsleitung vorgelegten Beträge/Impulse gezählt werden.
Steuerung	Kann die Erreichung von Zielen zur geplanten Weiterentwicklung der Internen Revisionsfunktion, zur Digitalisierung der Revisionsprozesse, zur Reduktion des CO2-Ausstoßes, zur Erfüllung von Diversity-Quoten oder von sonstigen für die Geschäftsleitung wichtigen Aufgaben enthalten. Ggf. werden zu den vorgenannten Themen auch spezifische Ziele vereinbart.
Einhaltung des Jahresprüfungsplanes	Idealerweise wird ein Stichtag (z. B. 31.12) festgelegt und es werden Prozentgrößen zur Abstufung verwendet. Dabei sollte festgelegt werden, wie mit genehmigten Planänderungen bzw. risikoorientiert vorgenommenen Anpassungen umzugehen ist.
Revisionsqualität	Anzahl und Schweregrad der Feststellungen nach Prüfung der Internen Revisionsfunktion durch den Abschlussprüfer oder einen Sonderprüfer. Ergebnisse/Zielerreichung in einem Quality Review der Intern Revision. Ergebnisse/Zielerreichung in einer Stakeholder-Befragung. Fristgerechte/zeitnahe Schließung von Gaps bzw. Feststellungen aus vorgenannten Prüfungen.
Effizienz/Produktivität	Anteil der Tage für Prüfungen, und prüfungsnahen Leistungen (z. B. Projektbegleitung, Beratung, Unterstützung bei externen Prüfungen) an den insgesamt verfügbaren Arbeitstagen. Oder Revisoren pro 100 Mitarbeitende des Instituts.
Qualität der Mitarbeitenden	Anteil der Mitarbeitenden mit Zertifizierungen (CIA, CISA ö. ä). Anteil der Mitarbeitenden mit praktischer Erfahrung in relevanten Prüfgebieten. Fort-/Weiterbildungstage bzw. CPE pro Mitarbeitenden.

Budgeteinhaltung	<p>Einhaltung des Personal- und Sachkostenbudgets der Internen Revision.</p> <p>Ggf. auch Senkung von (externen) Prüfungskosten durch Identifikation und Hebung von Synergien.</p>
Kultur	<p>Ergebnisse von Befragungen, die die Unternehmenskultur zum Gegenstand haben bzw. Umsetzungsstand von Maßnahmen hieraus.</p> <p>Ansonsten eher subjektiv: Beiträge zum offenen Austausch bzw. zur Speak-Up-Culture, zur Integration von neuen Mitarbeitenden. Zusammenarbeit mit den Funktionen der 2nd Line.</p>
Umsetzung von Maßnahmen	<p>Durchschnittliche Dauer zur Erledigung von Prüfungsfeststellungen, ggf. abgestuft nach Schweregrad.</p> <p>Oder Anteil der umgesetzten Maßnahmen, z. B. nach 12 / 24 / 36 Monaten.</p> <p>Die Interne Revision hat hier nur einen mittelbaren Einfluss. Sie kann jedoch durch adäquat formulierte und terminierte Maßnahmen, einen intensiven Dialog mit den Fachbereichen, konstruktive Beiträge zur Lösungsfindung sowie wirksame Überwachung und rechtzeitige Eskalation zu einer schnelleren Erledigung beitragen.</p>
Außenwirkung/Netzwerk	<p>Anzahl der internen/externen Vorträge.</p> <p>Veröffentlichung von Fachartikeln.</p> <p>Teilnahme an Benchmarking.</p> <p>Mitwirkung in Arbeitskreisen.</p>
Fristeinhaltung	<p>Einhaltung von Fristen, die gegenüber den geprüften Bereichen (z. B. in der schriftlich fixierten Ordnung der Revision) zugesagt sind. Z. B. Ankündigungsfristen, Prüfungsdauer, Dauer bis zum Versand des Berichtsentwurfs nach Abschluss der Prüfungshandlungen.</p>
Führung	<p>Basis für die Messung kann standardisiert erhobenes Feedback der Mitarbeitenden sein.</p> <p>In größeren Revisionseinheiten kann ggf. auch die Fluktuationsrate herangezogen werden.</p>
Projektbegleitung	<p>Vollständige oder anteilmäßig abgestufte, beratende Begleitung der wesentlichen Projekte/Anpassungsprozesse des Instituts.</p>

Abb. 21: Ziele für die Revisionsleitung

14 Gewinnung und Weiterentwicklung von Mitarbeitenden und Fit & Proper-Anforderungen

14.1 Hintergrund

Moderne Interne Revisionen sehen sich seit geraumer Zeit, getrieben durch Weiterentwicklung der Geschäftsmodelle und Produkte sowie durch technologischen Fortschritt, einem komplexer werdenden Umfeld – intern wie extern – ausgesetzt. Mit der zunehmenden Komplexität und einem damit korrespondierend umfangreicher und inhaltlich komplexer werdendem Aufsichtsrecht auf nationaler und europäischer Ebene, steigen auch die Anforderungen an Mitarbeitende der Internen Revision in Instituten.

In die MaRisk wurden mit Abschnitt AT 7.1 explizit Anforderungen an das Personal der Institute und somit auch an die Mitarbeitenden der Internen Revision aufgenommen. In den EBA Leitlinien zur internen Governance (EBA/GL/2021/05) finden sich entsprechende Anforderungen in Abschnitt 19.4. Zuvor wurden, mit der Überarbeitung der BCBS-Leitlinie „The internal audit function in banks“ vom Juni 2012, mit den Prinzipien zu Kompetenz und Wissen sowie Integrität, besondere Anforderungen an Mitarbeitende der Internen Revision definiert.

Generell sollte ein Revisor neben der persönlichen Eignung (Integrität, Objektivität, Verschwiegenheit) über revisionspezifische Methodenkompetenz (Beurteilung von Risiken und Anwendung von Prüfungstechniken), Technologiekompetenz (z. B. Einsatz von Datenanalysen), allgemeine betriebswirtschaftliche Kenntnisse, Branchenkenntnisse sowie Sozialkompetenz verfügen. Daneben sind spezifische Fachkompetenzen bezogen auf das Prüfobjekt (z. B. Informationstechnologie, Risikomanagement, Rechnungslegung, Projektmanagement) im Einzelfall erforderlich. Aktuell gefragte Kompetenzen und Bereiche für die Weiterbildung können der jeweiligen Enquete-Studie des DIIR entnommen werden.

Entsprechend den MaRisk und dem dort verankerten Prinzip der doppelten Proportionalität, müssen die institutsinternen Prozesse zur Identifizierung, Beurteilung und Steuerung der Risiken proportional, d. h. angemessen zur Größe der Institute sowie zu Art, Umfang und Risikogehalt der Geschäfte sein. Analog sind die betriebsinternen Erfordernisse, die Geschäftsaktivitäten und die Risikosituation auch Grundlage für die Bemessung quantitativen und qualitativen Personalausstattung nach AT 7.1, Tz. 1 MaRisk. Die Interne Revision hat fachlich versierte Mitarbeitende vorzuhalten, die entsprechende Prüfungs- und Beratungsleistungen durchführen können. Auch wenn im Einzelfall Experten hinzugezogen (Co-Sourcing) bzw. einzelne Revisionstätigkeiten ausgelagert werden, muss der Leiter der Internen Revision sicherstellen, dass die Aktivitäten und Prozesse des Instituts hinreichend beurteilt werden können.

Neben der Rekrutierung von geeigneten Mitarbeitenden ist dabei auch die Fortbildung der Mitarbeitenden in den vorhandenen Qualifikationen sowie die Weiterbildung in Bezug auf neue Qualifikationen – zuletzt z. B. in Bezug auf das Management von ESG-Risiken – im Blick zu behalten, um mit der Entwicklung des Instituts, der Branchen- und Marktentwicklung sowie den sich ändernden Anforderungen der Aufsicht mithalten zu können.

14.2 Anforderungsprofil für Mitarbeitende der Internen Revision

14.2.1 GIAS Standards 3.1 und 10.2

Die GIAS Standards 3.1 und 10.2 geben einen grundlegenden Rahmen für die Qualifikation von Mitarbeitern der Internen Revision. Es wird klargestellt, dass die Interne Revision insgesamt das erforderliche Wissen, die Fähigkeiten und die sonstigen Qualifikationen besitzen oder erwerben muss, um ihre Aufgaben erfolgreich erfüllen zu können. Insofern ist auch ein Rückgriff auf externe Ressourcen möglich. Jede Interne Revisorin und jeder Interne Revisor ist dafür verantwortlich, die zur Erfüllung der beruflichen Verantwortung erforderlichen Kompetenzen kontinuierlich weiterzuentwickeln und anzuwenden. Die Fachkompetenz umfasst auch die Berücksichtigung von aktuellen Aktivitäten, Trends und neuen Themen (Überlegungen zur Umsetzung zu GIAS Standard 3.1). Als besondere Kompetenzen werden das Wissen um Risiken für dolose Handlungen und über grundlegende Risiken und Kontrollen von Informationstechnologien sowie der verfügbaren technologiegestützten Prüfungstechniken gefordert.

14.2.2 Mögliches Anforderungsprofil

Das IIA hat ein Internal Audit Competency Framework (aktuelle Fassung von 2025) veröffentlicht, das die notwendigen Kompetenzen in der Internen Revision beschreibt. Das Competency Framework besteht aus:

- Vier übergeordnete Kategorien:
 - Kompetenzen in der Internen Revision.
 - Berufliche Kompetenzen.
 - Kompetenzen in den Bereichen Governance und Risikomanagement.
 - Kompetenzen im operativen Bereich
- Kenntnisse- und Fähigkeiten (Unterkategorien) innerhalb der übergeordneten Kategorien.

- Die Unterkategorien sollten so bearbeitet werden, dass wichtige Themen hervorgehoben werden und mit der Struktur, den Prozessen und den Prioritäten der Organisation übereinstimmen.
- Leistungsniveaus und Merkmale für die Beurteilung der Kompetenz, die zunehmend komplexere Nachweise der Beherrschung von Unterkategorien der Kenntnisse und Fähigkeiten beschreiben.

Das IIA Framework enthält zu jeder der Kategorien entsprechende Unterkategorien, zu denen die Revision über Kenntnisse und Fähigkeiten verfügen muss. Dazu gehören:

- Kompetenzen in der Internen Revision: Kenntnisse über Revisionsstandards und -methoden.
- Berufliche Kompetenzen: Von Kenntnissen in organisatorischer Führung, professioneller Kommunikation bis hin zu Datenanalyse zielen diese Kompetenzen auf die Planung und Durchführung von Aufträgen der Internen Revision in Übereinstimmung mit den Standards ab.
- Kompetenzen in den Bereichen Governance und Risikomanagement: Eine Grundvoraussetzung für die Identifizierung von Risiken, die für die Branche und das Umfeld, in dem eine Organisation tätig ist, spezifisch sind, ist ein Verständnis über strategische Planung, Compliance bis hin zu organisatorischer Resilienz und Nachhaltigkeit.
- Kompetenzen im operativen Bereich: Eine Grundvoraussetzung für die Identifizierung ist ein Verständnis der operativen Prozesse und der Geschäftspraktiken, wie Rechnungswesen, Vertrieb, IT oder andere wichtige Funktion und Prozesse des Unternehmens.

Das IIA Framework unterscheidet zwischen den vier Kompetenzstufen „Grundlegendes Niveau“, „Mittleres Niveau“, „Fortgeschrittenes Niveau“ und „Expertenniveau“

Basierend auf dem obengenannten Rahmenwerk sowie vor dem Hintergrund der spezifischen Anforderungen an Institute sind folgende Kompetenzen und Fachkenntnisse für einen Revisor in Instituten relevant:

- Persönlichkeit
 - Integrität (beachtet Gesetze und Vorgaben des Instituts und lehnt illegale Aktivitäten ab)
 - Objektivität (handelt unabhängig von persönlichen Interessen oder Anweisungen bezüglich der Berichterstattung und der Wertung der Prüfungsergebnisse)
 - Sorgfalt (arbeitet korrekt und verantwortungsbewusst)

- Verschwiegenheit (geht umsichtig und interessewährend mit den im Verlauf der Tätigkeit erhaltenen Informationen um)
- Analytisches Denken (kann komplexe Geschäftsvorgänge analysieren und verstehen und daraus Schlussfolgerungen ziehen)
- Strategisches Denken (denkt zukunftsorientiert und ist in der Lage auf Chancen und Risiken hinzuweisen)
- Vernetztes Denken (kann unternehmerische Zusammenhänge und Wechselwirkungen verstehen)
- Flexibilität (ist in der Lage, in einem sich immer schneller wandelnden Umfeld zu agieren und sich auf neue Situationen einzustellen)
- Sozialkompetenz
 - Kommunikationsfähigkeit (kann Ergebnisse und Empfehlungen klar und verständlich kommunizieren und auf hohem Niveau Feedback geben)
 - Kontaktfähigkeit (kann Netzwerke pflegen und fachlichen Austausch organisieren)
 - Zusammenarbeit und Teamfähigkeit (ist in der Lage, zusammen mit anderen Fachleuten zu arbeiten und gemeinschaftlich Ergebnisse zu erzielen)
 - Konfliktfähigkeit und Resilienz (kann mit, ggf. auch andauerndem, Widerstand und unfairen Angriffen umgehen)
- Allgemeine Betriebswirtschaftliche Kenntnisse
 - Management und Betriebsorganisation
 - Governance
 - Prozess- und Kontrolldesign
 - Aufdeckung und Prävention von Wirtschaftskriminalität
 - Rechnungslegung (Grundkenntnisse)
 - Kostenrechnung (Grundkenntnisse)
 - ESG/Nachhaltigkeit
- Revisionsspezifische Methodenkompetenz (z. B. belegt durch das CIA-Examen)
 - Prüfungsplanung und (Projekt)-management
 - Identifikation von Risiken
 - Prüfungsmethoden
- Technologiekompetenz

- Allgemeine Technologiekompetenz (kennt sich mit den neuesten technologischen Entwicklungen aus und versteht, wie diese die Geschäftsprozesse beeinflussen können)
- Grundkenntnisse im Informationsrisikomanagement (kann Schutzbedarfe, Berechtigungskonzepte und anwendungsspezifische Kontrollen aus fachlicher Sicht beurteilen)
- Prüfungsbezogene Technologiekompetenz (kann moderne Tools zur Daten- und Prozessanalyse anwenden)
- Branchenkenntnisse
 - Geschäftsmodelle und damit verbundene Risiken
 - Regulierung der Branche
- Spezifische Kenntnisse (beispielhaft)
 - Risikomanagement (Quantitativ ausgerichtete Expertise zur Beurteilung von den in den Geschäfts- und Risikosteuerungsprozessen eingesetzten Modellen und deren Validierung)
 - Informationstechnologie (technische Expertise zur Beurteilung von Entwicklung und Betrieb von Informationstechnologie)
 - Rechnungslegung (z. B. Expertise in der Prüfung von IFRS Standards)
- Sonstige Kenntnisse
 - Fähigkeit zur Anwendung agiler Methoden und Vorgehensweisen

14.2.3 Exkurs: Generalist versus Spezialist

Vor dem Hintergrund der Forderung nach einem angemessenen Qualifikationsniveau der Mitarbeitenden (AT 7.1, Tz. 2 MaRisk) stellt sich die Frage, ob die Interne Revision eher auf Generalisten oder Spezialisten setzen soll. Hierbei kann sich der Leiter der Internen Revision an der Größe, den Geschäftsaktivitäten und dem Risikoprofil des Instituts orientieren. So wird z. B. die Interne Revision in einem Institut mit einem großen Handelsbereich, der sich durch Nutzung einer breiten Palette von komplexen Finanzinnovationen auszeichnet, eher Spezialisten mit finanzmathematischen Kenntnissen vorhalten (müssen), während eine kleine Regionalbank mit einem Standardgeschäftsmodell eher Generalisten einstellen wird. Hier kommt der Grundsatz der Proportionalität zur Anwendung, nachdem sich das Qualifikationsniveau der Mitarbeitenden in der Internen Revision proportional an Größe, Geschäftsvolumen und Risikostruktur des Instituts orientiert.

Der Leiter der Internen Revision muss insgesamt dafür Sorge tragen, dass die Interne Revision in der Lage ist, die Aktivitäten und Prozesse des Instituts angemessen zu prüfen. Soweit für einzelne Prüfungen Spezial-Know-how zwar erforderlich ist, aufgrund der Größe der Internen Revision jedoch nicht wirtschaftlich vorgehalten werden kann, besteht die Möglichkeit, externe Expertise einzukaufen. Je nach Ausgestaltung der Beauftragung kann es sich dabei um eine Auslagerung oder Personalbestellung handeln.

14.2.4 Anforderungen an die Revisionsleitung

14.2.4.1 Fit and Proper Anforderungen der EBA

Basierend auf den EBA-Leitlinien zur Beurteilung der Eignung der Mitglieder des Leitungsorgans und der Inhaber von Schlüsselfunktionen (EBA/GL/2021/06) bei EZB-beaufsichtigten Instituten (SI) müssen neben den Mitgliedern des Leitungsorgans auch alle Inhaber von Schlüsselfunktionen, die unterhalb der gesamtverantwortlichen Leitungsebene einen signifikanten Einfluss auf die Ausrichtung des Instituts haben, hinsichtlich ihrer Eignung, ihrer fachlichen Qualifikation und ihrer persönlichen Zuverlässigkeit bewertet werden. Mit dem BRUBEG wurden die betreffenden Anforderungen Anfang 2026 in das KWG überführt. Bei großen Instituten ist die Bestellung und Abberufung des Leiters der Internen Revision der Aufsicht anzuzeigen.

Inhaber von Schlüsselfunktionen sind u. a. die Leitungen der Funktionen „Risikocontrolling“, „Compliance“ und „Interne Revision“. Eine Eignungsbewertung soll vor Bestellung erfolgen und einer laufenden bzw. jährlichen Kontrolle unterzogen werden. Die Bewertung orientiert sich an dem von der EZB herausgegebenen „Leitfaden zur Beurteilung der fachlichen Qualifikation und persönlichen Zuverlässigkeit“ (Dezember 2021) und dem Fragebogen „Fit and Proper Questionnaire“ (Dezember 2021).

Die Fragenbereiche gliedern sich in die Themen:

- Erfahrung (praktische, theoretische und funktionsspezifische)
- Leumund
- Interessenkonflikte (persönlich, beruflich, finanziell und politisch) und Unvoreingenommenheit
- Zeitaufwand
- kollektive Eignung.

14.2.4.2 Anforderungen der MaRisk

Bei den weniger bedeutenden Instituten (LSI), die der direkten Aufsicht durch die BaFin und die Bundesbank unterstehen, gelten die Fit and Proper Anforderungen für die Schlüsselpositionen nicht direkt. Grundlage für die erforderliche Eignung ist hier AT 7.1 Tz. 2 MaRisk, nach dem die mit der Leitung der Risikocontrolling-Funktion und der Leitung der Internen Revision betrauten Personen sowie der Compliance-Beauftragte besonderen qualitativen Anforderungen entsprechend ihrem Aufgabengebiet zu genügen haben.

Daher empfiehlt es sich auch bei den LSIs, bei der Neubesetzung der Revisionsleitung, in Abhängigkeit von Art, Größe und Komplexität des Instituts, Kriterien für die Stellenausschreibung sowie die Eignungsbewertung (Anforderungsprofil) festzulegen. Diese können auch als Grundlage für die regelmäßige Leistungsbeurteilung verwendet werden.

Fachkenntnisse im Prüfungswesen, z. B. die Anwendung von Prüfungsgrundsätzen, -verfahren und -techniken sind hierbei von besonderer Bedeutung. Diese können z. B. nachgewiesen werden durch:

- Berufserfahrung in einer Internen Revision oder bei einem Wirtschaftsprüfer bzw. einer Wirtschaftsprüfungsgesellschaft von mindestens drei Jahren auf mindestens Prüfungsleiterenebene (in Abhängigkeit von Größe und Komplexität des Instituts kann eine weitergehende Berufserfahrung im Prüfungswesen sowohl in Jahren als auch in führenden Funktionen erforderlich sein) oder
- die Ablegung des Berufsexamens CIA (ggf. auch CPA, Verbandsprüfer oder Wirtschaftsprüfer oder revisionsspezifische Qualifikationsprogramme der Bankenverbände)

Eine Beauftragung mit der Leitung der Internen Revision – bevor die notwendige Fachkenntnis erlangt wurde – ist möglich, wenn:

- eine Verpflichtung zur zeitnahen Erlangung der erforderlichen Fachkenntnisse (z. B. durch Berufsexamina) erfolgt,
- der stellvertretende Leiter bzw. die stellvertretende Leiterin der Internen Revision über die erforderlichen Fachkenntnisse verfügt und
- das Aufsichtsorgan hierüber im Rahmen der Informationspflicht gem. AT 4.4.3 Tz. 6 MaRisk informiert wird.

Darüber hinaus sind erforderlich:

- Verständnis der Geschäftstätigkeit des Instituts und der damit verbundenen Risiken
- Kenntnis des wirtschaftlichen und (aufsichts-)rechtlichen Umfelds des Instituts

- Führungserfahrung
- Durchsetzungsfähigkeit
- Zuverlässigkeit

Das Beispiel eines Anforderungsprofils für den Leiter der Internen Revision und die ggf. erforderlichen Nachweise (Anlage 5) sind auf der Webseite des DIIR verfügbar.

14.2.4.3 Fortbildungsverpflichtung

Der Leiter der Internen Revision ist verpflichtet, sich fachlich fortzubilden (GIAS 3.1 Kompetenz sowie 3.2 Kontinuierliche Berufliche Weiterbildung²⁷). Die Fortbildung soll die Fachkenntnisse, die Fähigkeit zu ihrer Anwendung sowie das Verständnis der Berufspflichten auf einem ausreichend hohen Stand halten. Auch wenn die GIAS keine konkreten Vorgaben zum zeitlichen Umfang der Fortbildung mehr beinhalten, hat sich in der Praxis folgender Ansatz bewährt: Die Fortbildung soll in Anlehnung an die Richtlinie des IIA zur jährlichen Erneuerung der Zertifizierung CIA einen Umfang von 40 Stunden jährlich nicht unterschreiten. Die Fortbildungsmaßnahmen können als Teilnehmer oder als Dozent sowie durch Selbststudium erbracht werden. Mindestens 20 Stunden jährlich können durch Teilnahme an oder Dozententätigkeit bei Fachveranstaltungen (Vorträge, Seminare, Diskussionsgruppen oder ähnliche Veranstaltungen) erbracht werden. Zu den weiteren Fortbildungsmaßnahmen gehören:

- die Absolvierung von IT-gestützten Fachkursen (E-Learning, Web Based Training), wenn die Dauer der Teilnahme nachgewiesen werden kann
- die schriftstellerische Facharbeit
- die Tätigkeit in externen Fachgremien

Die Erfüllung der Fortbildungsverpflichtung ist zu dokumentieren. Eine nicht erbrachte Fortbildungsverpflichtung kann im Folgejahr nachgeholt werden.

Die Überwachung der Einhaltung der Fortbildungsverpflichtung des Leiters der Internen Revision obliegt grundsätzlich dem zuständigen Mitglied der Geschäftsleitung. Entsprechende Prozesse sind, z. B. im Personalbereich, einzurichten.

²⁷ Indirekt auch über AT 7.1 Tz. 2 MaRisk.

14.3 Gewinnung von Mitarbeitenden für die Interne Revision

14.3.1 Märkte und Instrumente

Nachdem vor dem Hintergrund der MaRisk und berufsständischen Regeln ein Anforderungsprofil konkretisiert und ggf. in eine Personalstrategie der Internen Revision übergeleitet wurde, beginnt die gezielte Mitarbeiterauswahl und -gewinnung. Der Personalgewinnungsprozess an sich ist von enormer Bedeutung und bedarf sorgfältiger Planung und Durchführung, da dieser im Kern entscheidet, ob „die richtige Person am richtigen Ort“ tätig wird. Unzweifelhaft eine der Voraussetzungen für erfolgreiche Personalbeschaffung und langfristige Bindung von qualifizierten Mitarbeitenden. Die Anstrengungen zur Personalgewinnung sind auf den in zwei nachfolgende Gruppen zu unterteilenden Personalmarkt zu konzentrieren:

- Interner Markt
- Externer Markt.

Unter **internem Markt** sind alle Mitarbeitenden des Unternehmens oder Unternehmensgruppe zu verstehen, dem die Interne Revision als Einheit angehört bzw. mit dem sie verbunden ist. Hier bieten sich mit den Instrumenten

- Beschäftigung von Werksstudenten,
- Trainee-Programm,
- Personalentwicklungsprogramme (Entwicklung zur Seniorfachkraft oder Führungskraft),
- Innerbetrieblichen Vorstellungsrunden (z. B. Präsentation der Internen Revision in diversen Arbeitsgruppen oder Netzwerkveranstaltungen) und
- Intranetpräsenz

viele Möglichkeiten, Personal für die Interne Revision zu gewinnen. Ein Vorteil ist der vorhandene „Fit“ der Mitarbeitenden, d. h. die Identifikation mit dem Arbeitgeber und seinen Werten und Vorstellungen. Daneben können unternehmenserfahrene Kräfte gewonnen werden, welche die Facheinheiten des Instituts kennen und entsprechendes Detailwissen mitbringen. Dabei sind jedoch anfängliche Einschränkungen bei einem Wechsel in die Revisionsfunktion zur Vermeidung einer möglichen Selbstprüfung (Cooling-off-Phase) einzuplanen.

Der **externe Markt** umfasst diejenigen Personen, die noch keinen direkten Bezug zu dem Unternehmen haben und als solches von „außen“ angeworben werden bzw. sich von außen bewerben. Mögliche Instrumente sind:

- Stellenausschreibungen (insbesondere über Stellenbörsen im Internet)
- Präsenz des Instituts im Internet (z. B. Homepage, Facebook, Instagram, LinkedIn, XING)
- Direkte Ansprache von geeigneten Kandidaten über soziale Netzwerke (z. B. LinkedIn, XING)
- Empfehlungsmarketing (Nutzung des persönlichen Netzwerks von Mitarbeitenden des Instituts)
- Beauftragung von Personalberatungen
- Hochschulmarketing
- Betreuung von Examensarbeiten.

Für den richtigen und zielorientierten Einsatz der Instrumente auf dem externen Markt ist zum Teil ein erhöhter finanzieller Aufwand notwendig. Potenzielle Mitarbeitende werden stets, ob intern oder extern, als erstes Bewertungs- und Evaluierungsschritte durchlaufen (z. B. Vorstellungsgespräch, Assessment Center, Arbeitsprobe). Vor der eigentlichen Prüfung der Eignung für revisionsspezifische Aktivitäten wird dabei auch die grundsätzliche Überlegung angestellt, ob der Kandidat in das Unternehmen bzw. das Team passt. Dabei sind als Rahmenbedingung u. a. die einschlägigen Vorschriften des allgemeinen Gleichbehandlungsgesetzes (AGG) zu beachten.

Den Revisionsverantwortlichen muss es bei der Personalgewinnung – in Zusammenarbeit mit der Personalabteilung – gelingen, mit Hilfe des Personalmarketings attraktive Merkmale der Position, des Unternehmens und der Branche herauszuarbeiten und passende Kandidaten zu identifizieren. Doch was sind mögliche Erfolgsfaktoren eines guten Personalmarketings?

14.3.2 Personalmarketing

Neben der Auswahl der richtigen Personalbeschaffungsinstrumente ist es wichtig, die Interne Revision als „interessanten“ und „modernen“ Unternehmensbereich zu „vermarkten“. Je nach Auftrag und personeller Ausstattung der Internen Revision können folgende Instrumente zur Anwendung kommen:

- Professionelle revisorische Arbeit im Rahmen von Prüfung, Beratung und der Begleitung von Projekten
- Vorträge über die Funktion der Internen Revision innerhalb des Unternehmens und bei externen Veranstaltungen oder (Fach-)Kongressen sowie an Universitäten und Hochschulen, aktive Pflege von Netzwerken

- Veröffentlichen von Artikeln im Intranet, in internen Newslettern bzw. Fachartikeln in Fachzeitschriften
- Präsenz in einschlägigen fachbezogenen Internetseiten bzw. sozialen Netzwerken
- Teilnahme an Unternehmens- oder Jobmessen

Die Attraktivität der Internen Revision wird dabei von Bewerbern u. a. anhand nachfolgender Aspekte bemessen:

- Interessante, herausfordernde und abwechslungsreiche Aufgabenstellungen
- Erkennbar wertstiftende Arbeit im Unternehmen
- Managementnahe Tätigkeit (konstruktiver Dialog und Zusammenarbeit mit Stakeholdern)
- Möglichkeit, das Institut als Ganzes oder zumindest in größeren Bereichen kennen zu lernen
- Möglichkeiten, eigene Ideen umzusetzen
- Attraktive Aus- und Weiterbildungskonzepte, mittel- und langfristige Perspektiven
- Angemessene Vergütung
- Offene Unternehmenskultur mit flachen Hierarchien
- Positive Bewertungen im Internet (z. B. einschlägige Netzwerkplattformen, Bewertungsportale, soziale Medien)

Besonders wichtig ist es, den Mitarbeitenden ein Umfeld zu schaffen, das von flachen Hierarchien, Offenheit für Innovationen, großer Entscheidungsfreiheit und Eigenverantwortung geprägt ist. Gerade hierzu bietet eine moderne Revisionsabteilung gute Voraussetzungen. Schließlich wird – wie im Anforderungsprofil oben festgehalten – insbesondere auch die Übernahme von Eigenverantwortung erwartet. Jeder Prüfungsauftrag erfordert den Mut und die unternehmerische Weitsicht, Entscheidungen zu treffen und diese gegenüber den unterschiedlichsten Interessengruppen (Management, externe Prüfer, ggf. Aufsicht) zu vertreten. Hinzu kommt die Möglichkeit, über externe Weiterbildungsangebote (z. B. Qualifizierung zum Certified Internal Auditor) den eigenen Erfahrungsschatz zu erweitern bzw. sein Profil zu schärfen.

Mit der Gewinnung geeigneter Mitarbeitender ist das Fundament zur Aufrechterhaltung einer funktionsfähigen Internen Revision gelegt. Die Komplexität des regulatorischen Umfelds als auch der zunehmende Wettbewerb um „gute Köpfe“ („War for Talents“) erfordern jedoch geeignete Fort- und Weiterbildungskonzepte, um den Erfolg der Internen Revision nachhaltig zu sichern.

14.4 Weiterentwicklung

14.4.1 Personalentwicklung

Die Funktionsfähigkeit der Internen Revision erfordert neben der angemessenen quantitativen Ausstattung auch eine regelmäßige Weiterentwicklung der Kompetenzen. Revisorinnen und Revisoren müssen ihre Kompetenzen erhalten und kontinuierlich weiterentwickeln, um die Wirksamkeit und Qualität der Revisionsleistungen zu verbessern (GIAS 3.2 Kontinuierliche Berufliche Weiterbildung).

AT 7.1 Tz. 2 MaRisk gibt insoweit vor, dass die Mitarbeitenden sowie deren Vertreter abhängig von ihren Aufgaben, Kompetenzen und Verantwortlichkeiten über die erforderlichen Kenntnisse und Erfahrungen verfügen müssen. Durch geeignete Maßnahmen ist zu gewährleisten, dass das Qualifikationsniveau der Mitarbeitenden angemessen ist. Vor dem Hintergrund eines sich schnell verändernden Umfelds und detaillierteren gesetzlichen bzw. regulatorischen Vorgaben empfiehlt es sich, für Interne Revisionen eine mittel- bis langfristige Personalentwicklungsstrategie zu verfolgen. Diese sollte sich an der unternehmensspezifischen Strategie und an den daraus für die Interne Revision abgeleiteten Prüfobjekten orientieren.

Die Personalentwicklungsstrategie kann dabei von folgenden Überlegungen flankiert werden:

- Welche Anforderungen bestehen heute bzw. zukünftig und werden diese über die vorhandene Personalstruktur bereits abgedeckt?
→ Bedarfsanalyse
- Welche Qualifikationsziele oder -methoden und -inhalte sollen vermittelt werden?
→ Planung der jeweiligen Entwicklungsschritte
- Wie kann das Erlernte im Rahmen der täglichen Arbeit gesichert werden?
→ Transfersicherung nach Durchführung
- Wie sieht das Kosten-Nutzenverhältnis der Qualifizierungsmaßnahme aus?
→ nachgelagerte Erfolgskontrolle

Wichtig zur richtigen Durchführung der Weiterbildung ist eine adäquate Auswahl der Trainingsinstrumente. Diese können auf der einen Seite unterteilt werden in Weiterbildungsmaßnahmen zur Entwicklung

- persönlicher Kompetenzen,
- revisionsmethodischer Kompetenzen und
- besonderer fachlicher Kenntnisse für das Prüfungsgebiet.

Auf der anderen Seite in Maßnahmen, die „on-the-job“ oder „off-the-job“ durchgeführt werden.

14.4.2 Entwicklung persönlicher Kompetenzen

Wie unter dem Anforderungsprofil dargestellt, müssen Revisoren starke kommunikative Fähigkeiten mit ausgewogener Persönlichkeitsstruktur mitbringen. Über (unternehmens-)interne oder externe Seminare können Aspekte wie Zeitmanagement, Verhandlungstechniken, Umgang mit Konflikten oder Führung von Mitarbeitenden entwickelt werden. Darüber hinaus bieten sich je nach Organisationskultur oder interner Personalstrategie auch Coaching bzw. Mentoringprogramme an.

Erfahrene Mitarbeitende mit guter Unternehmenskenntnis begleiten dabei vor allem neue Kollegen in der Durchführung ihrer Arbeit und stehen als Ansprechpartner und Ratgeber zur Verfügung (beispielhaft für eine „on-the-job“ Maßnahme). Mehrwert entsteht dabei, wenn Revisionsmitarbeitende von Kollegen aus anderen Bereichen begleitet werden, die je nach Unternehmensgusto aus revisionsnahen (operativen Kontrollbereichen oder Compliance) oder stark operativ geprägten Einheiten wie Vertrieb oder Marketing kommen. Allerdings sind hierbei die Vermeidung von Zielkonflikten und die denkbare Beeinträchtigung der Unabhängigkeit der Revisionsmitarbeitenden streng zu beachten.

14.4.3 Entwicklung von revisionsmethodischen Kompetenzen und besonderem Fachwissen

Im Hinblick auf mögliche Instrumente zur Entwicklung und Vertiefung revisionsmethodischer Kompetenzen und dem Aufbau von Fachwissen für das Prüfungsgebiet stehen z. B. zur Auswahl:

- Qualifizierung zum Certified Internal Auditor (CIA) oder anderen berufsständischen Zertifikaten
- Studium von Fachliteratur
- Mitwirken in Arbeitskreisen oder -gruppen
- externe/interne Seminare
- Projektbegleitungen (ggf. mit Unterstützung durch einen Mentor)
- Hospitationen im Fachbereich (unter gleichzeitiger Wahrung von Unabhängigkeit und Vermeidung von Interessenskonflikten)
- Qualifizierung zum Datenanalysten durch entsprechende Zertifizierung (z. B. Data Scientist/ VöB, Bankverlag) oder Know-how Aufbau durch externe Unterstützung, dies

vor dem Hintergrund der zunehmenden Bedeutung von Datenanalysen als Prüfungsmethode

- Hospitation oder temporärer Einsatz in einer Grundsatzfunktion der Internen Revision

Die Konzeption der Entwicklung der Mitarbeitenden sowie die Durchführung von Weiterentwicklungsmaßnahmen in der Internen Revision sind hinreichend zu dokumentieren, um die Verpflichtungen aus den MaRisk hinsichtlich eines angemessenen Qualifikationsniveaus der Mitarbeitenden sicherzustellen. Vergleichbare Verpflichtungen ergeben sich aus dem GIAS Standard 3.2 sowie internationalen Guidelines des Basler Ausschusses. Insbesondere die vom IIA zertifizierten Revisoren haben zudem innerhalb eines festgelegten Zeitraums Weiterbildungsstunden nachzuweisen. Die Weiterbildungsmaßnahmen sind quantitativ in der jährlichen Prüfungs- und Ressourcenplanung angemessen zu berücksichtigen.

15 Konzernrevision

15.1 Rechtliche Grundlagen

Kreditinstitute müssen gemäß § 25a Abs. 1 KWG über eine ordnungsgemäße Geschäftsorganisation verfügen. Eine ordnungsgemäße Geschäftsorganisation muss insbesondere ein angemessenes und wirksames Risikomanagement umfassen. Das Risikomanagement beinhaltet die Festlegung von Strategien, Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit sowie die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem und einer Internen Revision.

Dies gilt nach § 25a Abs. 3 KWG u. a. auch für Institutsgruppen und Finanzholding-Gruppen, die somit eine Konzernrevision einrichten müssen. Diese ist Teil des Konzernrisikomanagements und unterstützt den Konzernvorstand bei der Überwachung des Konzerns. Sie wird i.d.R. von der Internen Revision der Konzernmuttergesellschaft wahrgenommen.

In AT 4.5 Nr. 6 der MaRisk werden die Anforderungen an die Interne Revisionsfunktion auf Gruppenebene näher beschrieben. Danach hat die Konzernrevision im Rahmen des Risikomanagements auf Gruppenebene ergänzend zur Internen Revision der gruppenangehörigen Unternehmen tätig zu werden. Dabei kann die Konzernrevision auch die Prüfungsergebnisse der Internen Revisionen der gruppenangehörigen Unternehmen berücksichtigen. Um die Vergleichbarkeit der Prüfungsergebnisse zu gewährleisten, fordert der AT 4.5 MaRisk für die Revisionen der gruppenangehörigen Unternehmen und der Konzernrevision die Sicherstellung einheitlicher Revisionsgrundsätze und Prüfungsstandards. Des Weiteren sind die Prüfungsplanung sowie die Verfahren zur Überwachung der fristgerechten Beseitigung von Mängeln aufeinander abzustimmen.

Die rechtlichen Anforderungen an die Ausgestaltung der Konzernrevision sind damit weniger umfangreich und detailliert ausgestaltet als die Anforderungen an die Interne Revision auf Ebene der Einzelinstitute. Dies erfordert und ermöglicht gleichermaßen eine individuelle und auf die Bedürfnisse des jeweiligen Konzerns ausgerichtete organisatorische und prozessuale Ausgestaltung der Zusammenarbeit der Internen Revisionen im Konzern. Dabei können und sind folgende Punkte zu berücksichtigen:

- Konzernstruktur
- Größe und Bedeutung der Unternehmen innerhalb der Konzernstruktur
- Umfang der konzernweit zu berücksichtigenden regulatorischen bzw. konzernintern definierten Anforderungen
- Regulierungsstatus der Konzerngesellschaften
- Homogenität bzw. Heterogenität des Leistungsspektrums der Konzerngesellschaften

- Auslagerungsgrad zwischen den Konzernunternehmen

Die konkrete Ausgestaltung der Konzernrevisionsfunktion ist in einer Richtlinie (Geschäftsordnung, Rahmenbedingungen) zu regeln. Diese sollte für die Gruppe zumindest die Stellung und Rechte der Konzernrevision, eine Abgrenzung des Prüfungsuniversums, die Berichtswege (incl. Einbindung der Vorstände in den Tochtergesellschaften), den Austausch innerhalb der Konzernrevision, die Informationspflichten der Revisionsleitung in den Tochtergesellschaften, die Planungs- und Prüfungsprozesse auf Gruppenebene, die Handhabung von Sonderprüfungen sowie Standards – wie Berichtsformate und Einstufung von Feststellungen – beinhalten. Die Richtlinie sollte von den Revisionsleitungen im Konzern jährlich überprüft, aktualisiert und von den jeweiligen Vorständen in Mutter- und Tochtergesellschaften in Kraft gesetzt werden.

Die Grundherausforderung bei der Ausgestaltung der Konzernrevisionsfunktion besteht in der Ausbalancierung der effektiven und effizienten prüferischen Durchdringung des Konzerns durch die Konzernrevision auf der einen Seite und der Berücksichtigung der rechtlichen Selbständigkeit der beteiligten Unternehmen mit eigener Governance und eigenen gesetzlichen bzw. regulatorischen Anforderungen auf der anderen Seite. Bei der Ausgestaltung der Konzernrevisionsfunktion ist dabei insbesondere zu beachten, dass Konflikte mit dem Gesellschaftsrecht auftreten können. So ist z. B. der Vorstand eines als Aktiengesellschaft geführten Tochterunternehmens gem. § 76 Abs. 1 AktG (Leitungsrecht, Autonomie des Vorstands in der Führung der Gesellschaft) allein für die Leitung des Unternehmens verantwortlich. Im konkreten Modell bedeutet dies, dass die Steuerung und Überwachung auf Gruppenebene nicht zu nachteiligen Maßnahmen für das Tochterunternehmen führen darf.

15.2 Kernfunktion der Konzernrevision

Die Konzernrevision wird funktional im Rahmen des Risikomanagements auf Gruppenebene tätig und unterstützt den Konzernvorstand in seiner Überwachungsfunktion. Im Rahmen dessen prüft sie Prozesse, welche gruppenweit verbindlich definiert wurden, sowie auch Aktivitäten/Themen aus den Tochtergesellschaften, die für die Gruppe aus Risiko- oder Ertragsicht etc. relevant sind. Während die Konzernrevision auf den Prüfungsergebnissen der Internen Revisionen in Tochterunternehmen aufbauen kann, ist ihr Fokus auf die Anforderungen des übergeordneten Unternehmens der Gruppe gerichtet.

Der Grad der Integration zwischen Interner Revision der Tochtergesellschaft und der Konzernrevision kann unterschiedlich ausgestaltet sein. In einer wenig integrierten Zusammenarbeit prüft die Konzernrevision lediglich das auf Gruppenebene implementierte Risikomanagementsystem (Mindestanforderung) sowie ggf. auf Gruppenebene imple-

mentierte Aktivitäten und Prozesse; die dezentralen Revisionseinheiten in den Tochtergesellschaften sind selbständig. Diese Form wird in einem stärker dezentralisiert geführten Konzern präferiert.

Die stärkste Form der Integration liegt vor, wenn die Interne Revision der Konzernmutter alle Prüfungen innerhalb des Konzerns selbst verantwortet. Dies kann entweder durch eine Vollausslagerung der Revisionsfunktion der Tochtergesellschaften an die Konzernmutter oder durch faktische Integration der Internen Revision der Tochtergesellschaften in die Interne Revision der Konzernmutter erfolgen.

Voraussetzung für das Funktionieren dieses vollständig integrierten Modells ist ein stark integrierter Konzern, der vom Konzernvorstand mit Bündelung der Stabsfunktionen in der Muttergesellschaft zentral gesteuert wird. Dies ist insbesondere bei homogenen Geschäftsmodellen oder bei arbeitsteiligen Organisationsmodellen (Bündelung von Aktivitäten durch konzerninterne Auslagerungen, wie z. B. IT in Tochterunternehmen, Risikomanagementmethoden in der Konzernmutter) der Fall. Ferner können eine starke regulatorische Durchdringung des Konzerns und eine hohe Dichte an Konzernvorgaben dafür sprechen, die Aktivitäten von Konzernrevision und Revision des Einzelinstituts stärker miteinander zu verknüpfen, um Synergien in der Prüfungsdurchführung zu heben. Die ebenfalls zu einer Integration der Prüfungsaktivitäten führende Vollausslagerung der Internen Revision ist gem. MaRisk für regulierte Institute nur dann möglich ist, wenn das auslagernde Institut sowohl hinsichtlich seiner Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den nationalen Finanzsektor als auch hinsichtlich seiner Bedeutung innerhalb der Gruppe als nicht wesentlich einzustufen ist (AT 9 Tz 5 MaRisk). Gerade in diesen Fällen kann das bei der Konzernrevision i.d.R. breiter vorhandene Spezial-Know-how genutzt werden, um eine effektive Abdeckung des Tochterunternehmens aus Einzelinstituts- wie aus Konzernsicht sicherzustellen und gleichzeitig Kostenvorteile gegenüber einer konzernexternen Auslagerung erzielt werden.

Exkurs: regulatorische Anforderungen an die Vollausslagerung der Internen Revision:

Eine (Voll)Auslagerung der Revisionsfunktion bei Banken hat im Einklang mit den Regelungen des AT 9 „Outsourcing“ der MaRisk zu erfolgen. Sie ist dadurch gekennzeichnet, dass die Interne Revision der Konzernmutter auf Basis eines Auslagerungsvertrages mit der Revisionsfunktion der Tochter beauftragt wird, welche andernfalls von der Tochter selbst erbracht würde. Es ist regelmäßig davon auszugehen, dass die Vollausslagerung der Internen Revision eines beaufsichtigten Unternehmens durch die Aufsichtsbehörden als wesentlich angesehen wird. In diesem Fall ist sicher zu stellen, dass die durch AT 9 der MaRisk vorgegebenen Regelungen eingehalten werden, z. B. hinsichtlich der Einhaltung der Mindestanforderungen an die Ausgestaltung des Auslagerungsvertrags gem. AT 9 Tz. 7 oder mit Blick auf die Steuerung und Überwachung der mit der Auslagerung

verbundenen Risiken anhand vorzuhaltender Kriterien (KPI, KRI) bzw. vertraglich vereinbarter Informationen gem. AT 9 Tz. 9. Daneben ist zu beachten, dass die Auslagerung der Internen Revision der Tochtergesellschaft nur zulässig ist, wenn das Tochterinstitut hinsichtlich seiner Größe, Komplexität und dem Risikogehalt der Geschäftsaktivitäten für den Finanzsektor als auch hinsichtlich seiner Bedeutung in der Gruppe als nicht wesentlich einzustufen ist (AT 9 Tz. 5 MaRisk). Sofern die Interne Revision vollständig ausgelagert wird, ist zudem innerhalb der Tochtergesellschaft ein Revisionsbeauftragter zu benennen, der eine ordnungsgemäße Interne Revision gewährleisten muss. Die Anforderungen in AT 4.4.3 und BT 2 MaRisk auf Ebene des Tochterunternehmens sind auch im Falle einer Auslagerung der Revisionsfunktion zu beachten.

Auch bei einer stark integrierten Zusammenarbeit der Internen Revision des Konzerns bleibt die Interne Revision des Tochterunternehmens grundsätzlich mit eigener Governance bestehen, ist jedoch faktisch in die Konzernrevision eingegliedert, indem die Leitung der Konzernrevision über konzerninterne Regelungen Weisungsbefugnisse erhält und damit die personelle und fachliche Verantwortung für die Interne Revision der Tochtergesellschaft übernimmt oder andere Zusammenarbeitsformen etabliert werden, die eine enge Verzahnung der Prüfungsplanung, -durchführung und -berichterstattung auf Basis einheitlicher Revisionsmethoden und -standards sicherstellen. Diese Variante ist dann sinnvoll, wenn in einem zentralistisch aufgestellten Konzern, aufgrund spezifischer Gegebenheiten (z. B. Tochterunternehmen im Ausland, Tochterunternehmen mit wesentlicher Bedeutung für den Konzern) eine Auslagerung der Internen Revisionsfunktion auf die Muttergesellschaft nicht sinnvoll bzw. möglich ist. Die Stellung der Internen Revision in der Tochtergesellschaft ist bei dieser Konstellation im Rahmen der konzernweiten Aufbauorganisation im Innenverhältnis mit einer Abteilung der Konzernrevision vergleichbar. Daneben ist zusätzlich das jeweils für das Tochterunternehmen geltende Recht zu beachten. Formal benötigt die Leitung der Konzernrevision für wesentliche Entscheidungen (insbesondere Personalthemen) die Genehmigung der Geschäftsleitung des Tochterunternehmens.

Unabdingbare Voraussetzung für die Umsetzung des vollständig integrierten Modells ist die Verankerung der hierfür notwendigen Rechte und Pflichten der Internen Revision der Konzernmutter in konzernweit gültigen Richtlinien (Rahmenbedingungen) bzw. bei Auslagerung zusätzlich in einem Auslagerungsvertrag. Die Richtlinien sind sowohl durch den Konzernvorstand als auch durch die Vorstände der Tochterunternehmen in Kraft zu setzen.

15.2.1 Prüfungsplanung

Die Konzernrevision hat analog zur Internen Revision der Tochtergesellschaft einen umfassenden und jährlich fortzuschreibenden Prüfungsplan aus Konzernsicht zu erstellen.

Dieser kann in den Prüfungsplan der Muttergesellschaft integriert oder separat dokumentiert werden. Hier gelten hinsichtlich Risikoorientierung, Prüfungsturnus oder Mehrjahresplan im Wesentlichen die bereits in Kap. 4.1 „Prüfungsplanung“ dieses Revisionshandbuchs genannten Prinzipien.

Der Ausprägungsgrad der organisatorischen Integration bzw. der Integration der Zusammenarbeit mit der Internen Revision der Tochtergesellschaft beeinflusst auch die Ausprägung des Prüfungsuniversums. Hierzu sind mehrere Varianten möglich:

- ein konsistentes bzw. einheitliches Prüfungsuniversum für den gesamten Konzern, inklusive der Prüfungsgebiete in den Tochtergesellschaften (in diesem Fall ist es erforderlich, die Teil-Prüfungsuniversen der Tochtergesellschaften durch entsprechende Kennzeichnung der Prüfungsobjekte identifizierbar zu machen)
- separate Prüfungsuniversen für die Tochtergesellschaften.

Um eine Abstimmung der Prüfungsplanung nach AT 4.5 Tz. 6 MaRisk durchführen zu können, ist zumindest eine Überleitbarkeit der Prüfungsuniversum erforderlich. Hierzu bedarf es einheitlicher Standards, denkbar sind z. B. die Orientierung der Gliederung anhand konzernweit einheitlichen Prozesslandkarten oder entlang der Definition von Risikoarten. Etwaige Abweichungen von diesen konzernweit einheitlichen Standards für die Prüfungsplanung, die z. B. aus unterschiedlichen Branchenspezifika resultieren, sind entsprechend zu begründen. Im Sinne von Synergien und Vergleichbarkeit von Prüfungsergebnissen im Konzern sollte auch betrachtet werden, inwiefern man Prüfungsobjekte in ihrem Inhalt und ihrer Abgrenzung aus Konzernsicht mit denen der einzelnen Tochtergesellschaften koppeln kann und z. B. gemeinsam oder nach einheitlichen und abgestimmten Prüfungsprogrammen prüfen kann.

Mit Blick auf die bestehenden Anforderungen an die Vereinheitlichung der wesentlichen Revisionsstandards und -prozesse werden, ein vergleichbares Geschäftsmodell vorausgesetzt, sollten auch die zur Prüfungsplanung verwendeten Risikobewertungsverfahren in ihrer Grundausrprägung harmonisiert werden. Unternehmensspezifische Besonderheiten (z. B. Geschäftsarten, Größe des Unternehmens) können dabei individuell über die verwendeten Risikofaktoren oder Bewertungskriterien berücksichtigt werden. Die Risikobewertung der Prüfobjekte sowie die Ableitung der (Mehr)Jahresprüfungspläne erfolgt zunächst eigenständig durch die Konzernrevision (auf Basis Konzern-Prüfungsuniversums inkl. Betrachtung der Tochterunternehmen) sowie die Internen Revisionen der Tochterunternehmen (auf Ebene des Einzelinstituts).

Der Mehrjahresprüfungsplan der Konzernrevision auf Gruppenebene enthält zwei Arten von Prüfungen: zum einen Prüfungen von Aktivitäten und Prozessen, welche aus regulatorischen Erfordernissen konzernweit reglementiert sein müssen. Dies sind insbesondere die Themen Konzernrisikomanagement inkl. IT-Risiko- und -sicherheitsmanagement, Konzernrechnungswesen, Konzernmeldewesen, Konzerngeldwäscheprävention sowie

Daten Qualität und Data Governance. Zum anderen beinhaltet der Mehrjahresprüfungsplan Aktivitäten und Prozesse, welche der Konzernvorstand aus strategischen und geschäftspolitischen Gründen gruppenweit verbindlich definiert hat. Hier ist eine Vielzahl von Themen – wie z. B. Konzernliquiditätsmanagement, Konzernsteuern (Organschaft), Beschaffungen oder Compliance möglich.

Die Prüfungsplanung von Konzernrevision und die Prüfungsplanung der Tochterunternehmen sind aufeinander abzustimmen (AT 4.5 Tz. 6 MaRisk). Hierbei ist durch die Konzernrevision im Sinne einer Qualitätssicherung zu gewährleisten, dass die konzernbezogenen Themen nach eigener Risikoeinschätzung angemessen abgedeckt werden. Alle gruppenweit eingerichteten Prozesse sollten unter der Verantwortung der Konzernrevision geprüft werden (als Konzernprüfungen bzw. zentrale Prüfungen). Neben der Durchführung eigener Prüfungshandlungen kann sich die Konzernrevision bei Gleichwertigkeit der Prüfungsdurchführung durch die Tochterrevision auch deren Ergebnisse zu eigen machen oder gemeinsame Prüfungsaktivitäten mit den Tochterrevisionen vereinbaren. Je nach konkreter Ausgestaltung der Prüfungsdurchführung stellt die Revisionsleitung der jeweiligen Tochtergesellschaften sicher, dass diese Prüfungen ebenfalls in den Planungen ihrer Gesellschaft berücksichtigt werden.

Im Rahmen des Planungsprozesses hat sich die Leitung der Konzernrevision auch einen Überblick über Themen und Risiken in den Prüfungsplänen der Tochterunternehmen zu verschaffen, die nicht zu vernetzten Prüfungsaktivitäten führen, aus Konzernsicht für die Risikofrüherkennung und -steuerung aber relevant sind. Hierzu zählen z. B. Prüfungen des Risikomanagements oder der Rechnungslegungsprozesse auf Ebene des Tochterunternehmens. Die entsprechenden Prüfungen (konzernrelevante oder dezentrale Prüfungen) sind in den Prüfungsplänen zu kennzeichnen, so dass die Weitergabe der Prüfungsergebnisse an die Konzernrevision überwacht werden kann.

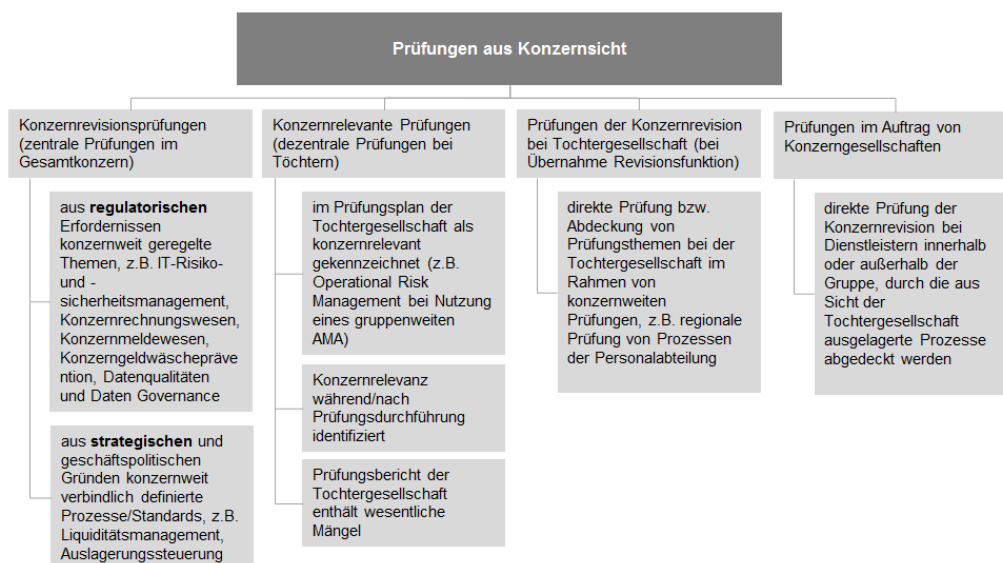


Abb. 22: Übersicht über die Prüfungsarten aus Konzernsicht

Bei einer vollständigen Integration der Internen Revision der Tochtergesellschaften in die Konzernrevision werden im Rahmen des Planungsprozesses die Prüfungspläne zentral erstellt. Da auch auf Ebene der Einzelunternehmen die Revisionsfunktion ausgeübt werden muss, muss der Prüfungsplan auf Konzernebene auch Einzelpläne für die jeweiligen Tochterunternehmen beinhalten. Sofern es sich bei den Tochterunternehmen um beaufsichtigte Unternehmen handelt, muss der Prüfungsplan mit dem jeweiligen Revisionsbeauftragten separat erstellt und von der Geschäftsleitung der jeweiligen Tochtergesellschaft beschlossen werden.

15.2.2 Überwachung der Qualität der Internen Revision bei Verwendung von Prüfungsergebnissen

Da die Konzernrevision „ergänzend zur Internen Revision der Tochtergesellschaft“ tätig werden muss, werden in der Prüfungsplanung der Konzernrevision i.d.R. risikoorientierte Prüfungshandlungen auch in den Tochterunternehmen vorgesehen. In den Prüfungstheemen, in denen keine eigenen Prüfungsaktivitäten der Konzernrevision in den Tochtergesellschaften durchgeführt werden, besteht die Möglichkeit, die Prüfungsergebnisse der Internen Revisionen der nachgeordneten Unternehmen zu verwenden.

Sowohl mit Blick auf die Initiierung gemeinsamer Prüfungsaktivitäten als auch hinsichtlich der möglichen Nutzung der Prüfungsergebnisse der Tochterrevisionen durch die Konzernrevision kommt der angemessenen und auf den Einzelfall abgestimmten Vereinheitlichung der Revisionsmethoden und -prozesse eine bedeutende Rolle zu. Die Sicherstellung einheitlicher Revisionsgrundsätze und Prüfungsstandards setzt jedoch voraus, dass die Interne Revision der Tochtergesellschaft den MaRisk bzw. einem anderen vergleichbaren Standard, z. B. DIIR/ IIA, entspricht. Gleichzeitig sollen im Konzern einheitliche Standards bezüglich des Revisionsprozesses, insbesondere der Risikobewertung von Prüfobjekten sowie der Bewertung von Revisionsergebnissen und Feststellungen definiert werden, z. B. durch Nutzung einer einheitlichen Feststellungsmatrix. Folglich hat sich die Konzernrevision regelmäßig davon zu überzeugen, ob die Voraussetzungen der Vereinheitlichung erfüllt sind und ob die Funktionsfähigkeit der Internen Revision des Tochterunternehmens gegeben ist. Um sicherzustellen, dass die Interne Revision der Tochtergesellschaft den MaRisk entspricht, bietet sich die Einsichtnahme in den vom Wirtschaftsprüfer verfassten Jahresabschlussbericht an. Der Abschlussprüfer hat hier gem. § 11 Abs. 2 Nr. 4 PrüfBV die Angemessenheit und Wirksamkeit der Internen Revision zu beurteilen. Somit hat der Abschlussprüfer Ausführungen zur Organisation der Internen Revision zu machen und zu bestätigen, ob die Ausgestaltung der Internen Revision sowie deren Einbindung in das interne Überwachungssystem in qualitativer und quantitativer Hinsicht zu den besonderen Anforderungen der Geschäftsstruktur in angemessenem Verhältnis stehen. Diese Ausführungen kann sich die Konzernrevision für die

Beurteilung der Qualität der Internen Revisionen in den Tochtergesellschaften zu Nutzen machen. Bei ausländischen Tochtergesellschaften besteht die Problematik, dass in vielen Ländern eine Berichterstattung des Abschlussprüfers über die Interne Revision nicht vorgesehen ist bzw. keine den MaRisk vergleichbare Regelung existiert. In diesen Fällen müssen – soweit nach jeweiligem Landesrecht möglich – die Anforderungen der MaRisk in eine konzernweit gültige Regelung aufgenommen werden, von deren Einhaltung sich die Konzernrevision dann selbst überzeugen muss.

Eine andere, komplementär zu nutzende Möglichkeit, sich der angemessenen Qualität der Internen Revision zu vergewissern, ist die Durchführung eines Quality Assessments. Gemäß Quality Assessment-Leitfaden des DIIR stellt ein positiv beschiedenes Quality Assessment einen Nachweis dar, dass die Interne Revision nach international einheitlichen Standards arbeitet und somit verlässliche Prüfungs- und Beratungsleistungen erbringt. Ferner bietet die im Rahmen des Quality Assessments vorgeschriebene Mindestberichterstattung zur Internen Revision die Möglichkeit, sich über die Qualität der Internen Revision der Tochtergesellschaft ein eigenes Bild zu machen. Mindestberichts-inhalte sind neben einer zusammenfassenden Schlussbemerkung zur Angemessenheit und Wirksamkeit der Internen Revision demnach beispielsweise die Beschreibung der Struktur und organisatorischen Einordnung der Internen Revision, die Darstellung der Prüfungsstrategie, des Prüfungsprogrammes und der Risikoanalyse.

Ein Quality Assessment kann entweder durch unabhängige Dritte oder in Form eines Self Assessments mit unabhängiger Validierung durchgeführt werden (vgl. hierzu die Ausführungen in Kap. 10 Qualitätssicherung und -verbesserung in der Internen Revision dieses Handbuchs). Das Quality Assessment kann auch durch die Konzernrevision selbst oder von einem Team aus den Internen Revisionen der Gruppe umgesetzt werden. Einschränkung ist jedoch zu vermerken, dass in diesem Fall, wegen der fehlenden Unabhängigkeit der Auditoren der diesbezügliche Standard des DIIR nicht erfüllt wird und somit keine Drittverwendungsfähigkeit für das Quality Assessment besteht.

Ergänzend kann die Konzernrevision/ die Interne Revision der Tochtergesellschaft die Ergebnisse der Prüfungen der Internen Revision der Tochtergesellschaft/ der Konzernrevision bzw. der Internen Revision von Schwestergesellschaften berücksichtigen und diese zur Abdeckung ihres Prüfungsuniversums heranziehen, wenn sie die Prüfungskonzeption (Breite und Tiefe der Prüfung), die Prüfungsdurchführung (Prüfungsdokumentation) und den Revisionsbericht (ggf. Auszug) auf Ebene der relevanten Einzelprüfungen angemessen qualitätssichert, um die durchgeführten Prüfungshandlungen bewerten sowie die Prüfungsergebnisse auf Relevanz und Risiko für die eigene Gesellschaft analysieren zu können. Eine solche Qualitätssicherung ist in den Fällen, in denen Konzernrevision und Interne Revision des Tochterunternehmens unter Federführung der Konzernrevision gemeinschaftlich prüfen, systemimmanent.

15.2.3 Prüfungstätigkeit und Berichterstattung

Prüfungen konzernrelevanter Themen können eigenständig durch die Konzernrevision, in gemeinschaftlichen Prüfungsaktivitäten von Konzernrevision und Interner Revision des Tochterunternehmens (Joint Audits) oder eigenständig von der Internen Revision des Tochterunternehmens geprüft werden.

Werden Konzernprüfungen zentral („top-down“) durch die Konzernrevision selbst oder gemeinsam mit der/ den Internen Revision(en) der Tochtergesellschaften durchgeführt, ist eine Einbeziehung der Internen Revisionen der Tochtergesellschaften insbesondere dann ratsam, wenn durch das Know-how und die Produkt-, Prozess- und Systemkenntnisse derselben eine effektivere und effizientere Prüfungsdurchführung im Tochterunternehmen möglich ist und die notwendigen Kapazitäten für die Prüfungsdurchführung vorhanden sind und/ oder ein hoher Auslagerungsgrad zwischen Mutter- und Tochterunternehmen besteht. Die Prüfungshandlungen der Internen Revision der Tochtergesellschaft sollten bei gemeinschaftlichen oder thematisch koordinierten Prüfungen, auf deren Ergebnisse sich die Konzernrevision stützt, inhaltlich von der Konzernrevision vorbereitet (Prüfungsleitfaden) und die Ergebnisse der Prüfungshandlungen anschließend plausibilisiert werden. Im Rahmen der Berichterstattung sind die Prüfungsergebnisse aus den Tochtergesellschaften in diesen Fällen zu einem aussagefähigen Gesamtbericht für den Vorstand der Muttergesellschaft zu aggregieren. Die Einzelfeststellungen des konsolidierten Gesamtberichtes sind durch die Konzernrevision nachzuverfolgen, wobei sie sich unter Nutzung entsprechender Qualitätssicherungsmaßnahmen analog zur Prüfungsdurchführung auch auf die Follow-up-Aktivitäten der Tochtergesellschaften stützen kann. Die von Tochterrevision und Konzernrevision verwendeten Verfahren zur Überwachung der fristgerechten Beseitigung von Mängeln sind dabei nach AT 4.5 der MaRisk aufeinander abzustimmen.

Prüfungen und Risiken, die dezentral von den Internen Revisionen der Tochtergesellschaften geplant bzw. bewertet werden, aber auch aus Konzernsicht für die Risikofrüherkennung und -steuerung relevant sind (dezentrale Prüfungen), werden im Gegensatz zu zentralen Prüfungen eigenverantwortlich durch die Internen Revisionen der Tochtergesellschaften lokal durchgeführt. Nach Abschluss dieser Prüfungen werden der Konzernrevision die Prüfungsergebnisse „bottom-up“ zur Verfügung gestellt.

Bei der vorgenannten Überlassung von Prüfungsergebnissen ist zu beachten, dass die Konzernrelevanz von Revisionsthemen nicht notwendigerweise auf den ersten Blick erkennbar ist. So gibt es Themen oder Prüfungsergebnisse, bei denen sich die Konzernrelevanz erst im Laufe der Prüfungen oder bei der Berichterstattung herauskristallisiert. Dies ist beispielsweise der Fall, wenn die Risiken bzw. Auswirkungen der Feststellung zwar die Tochtergesellschaft unmittelbar betreffen aber mittelbar auch Reputation der Muttergesellschaft oder Buchwert der Tochtergesellschaft bzw. Beteiligungsergebnis in der Bilanz der Muttergesellschaft nennenswert beeinflussen können. In diesem Fall sind der Konzernrevision ebenfalls die Ergebnisse zuzuleiten. Risikoorientiert abgestuft ist

dann zu entscheiden, ob die Ergebnisse der Internen Revisionen der Tochtergesellschaften in die Nachverfolgung der Konzernrevision aufgenommen werden, wobei i.d.R. eine eigene Risikobewertung der Konzernrevision zugrunde gelegt wird. Gleiches gilt für risikorelevante Ergebnisse aus Prüfungsberichtern Dritter zu den Tochtergesellschaften (Wirtschaftsprüfung, Aufsicht).

Die Regelungen zur Berichterstattung sollten in geeigneter Form möglichst einheitlich in der Gruppe definiert werden.

15.2.4 Informationsweitergabe und Austausch

Neben der gemeinsamen Planung von Prüfungen und der Überlassung von Prüfungsergebnissen ist zur Ausübung einer wirksamen Konzernrevisionsfunktion notwendig, dass die Revisionsleitungen im Konzern vertrauensvoll und auf Basis eines gemeinsamen Revisionsverständnisses zusammenarbeiten. Um den Austausch konzernweit sicherzustellen, bietet sich z. B. ein regelmäßiges Treffen der Revisionsleitungen im Konzern an, im Rahmen dessen man sich über konzernweit relevante Fachthemen sowie die Prüfungsmethodik und die Prüfungsplanung austauscht oder Schnittstellenprobleme der Revisionen untereinander bespricht. Daneben können Arbeitskreise für ausgewählte Aspekte, wie beispielsweise gruppenweit regulierte Themen oder Spezifizierung der Revisionsmethodik, eingerichtet werden.

Insgesamt ergibt sich daher folgender Informationsfluss zwischen der Internen Revision der Tochtergesellschaft und der Konzernrevision:

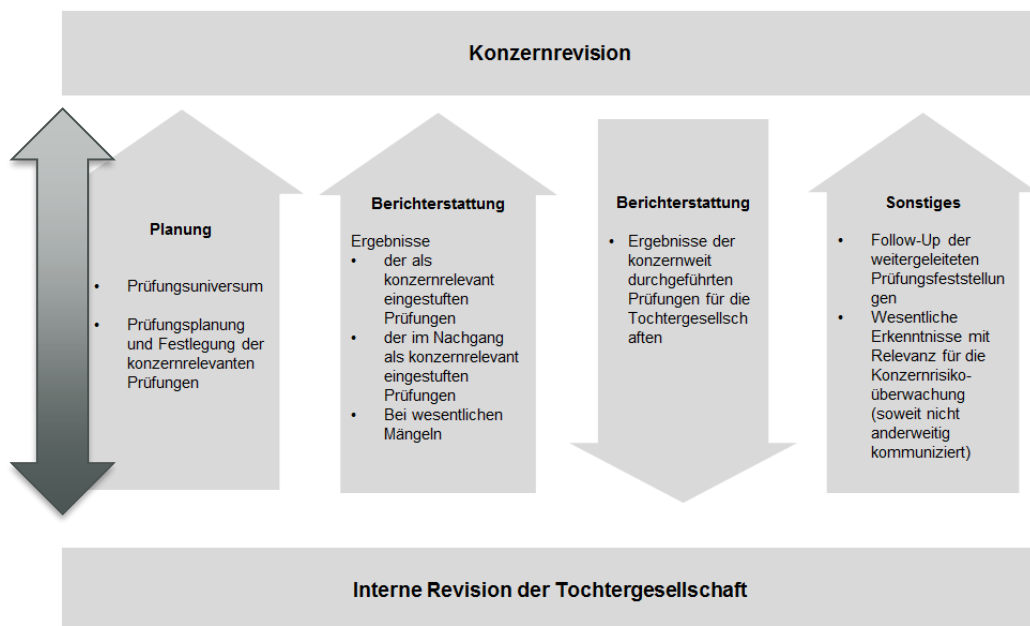


Abb. 23: Informationsflüsse zwischen den Internen Revisionen der Tochtergesellschaften und der Konzernrevision

Die Konzernrevision sollte einheitliche Standards zur Informationsweitergabe zwischen Konzernrevision und den Internen Revisionen der Tochtergesellschaften vorgeben.

15.2.5 Berichterstattung an den Konzernvorstand

Die Konzernrevision hat den Vorstand und das Aufsichtsorgan des Mutterunternehmens über ihre Tätigkeit auf Gruppenebene zu informieren. Neben den Prüfungsberichten über die Konzernprüfungen, ist auch über die nach vergleichbaren Bewertungsmaßstäben der Konzernrevision wesentlichen Prüfungsfeststellungen und -ergebnisse aus den unterjährig durch die Revisionsleiter der Tochtergesellschaften gemeldeten Prüfungsergebnissen zu berichten. Dies hat in angemessenen Abständen, mindestens aber vierteljährlich, zu erfolgen und schließt das Aufsichtsorgan des übergeordneten Unternehmens als Berichtsempfänger mit ein (AT 4.5 MaRisk). In analoger Anwendung des BT 2.4 Tz. 4 MaRisk sind hierbei u. a. die wesentlichen oder höher eingestufteten Mängel, die beschlossenen Maßnahmen einschließlich des jeweiligen Abarbeitungsstandes zu berichten.

Bei besonders schwerwiegenden Feststellungen ist auch der Konzernvorstand sofort zu informieren. Die Entscheidung hierüber liegt im Ermessen der Konzernrevisionsleitung und hat durch diese – nach vorheriger Abstimmung mit der Revisionsleitung der betroffenen Tochtergesellschaft – zu erfolgen.

Der Vorstand des Mutterunternehmens im Konzern kann die Konzernrevision in Einzelfällen beauftragen, Prüfungen in einzelnen Gesellschaften durchzuführen, um konzernrelevante Risiken zu beurteilen. Da dies zu Konflikten mit dem Vorstand im Tochterunternehmen führen kann, sollten die Vorgehensweise und die Einbindung des Vorstandes des Tochterunternehmens in den Richtlinien (Rahmenbedingungen) für die Konzernrevision geregelt sein.

Es ist zu beachten, dass die Interne Revision der Konzernmutter im Rahmen der Konzernfunktion mehrere „Rollen“ einnimmt, welche insbesondere bei der Berichterstattung und der Informationsweitergabe zu berücksichtigen sind. Die Anzahl dieser Rollen variiert in Abhängigkeit der konkreten Ausgestaltung des Konzerns sowie der Konzernbeziehungen:

- Mit der Prüfung von konzernübergreifenden Prozessen auf Ebene der Gruppe fungiert sie gem. § 25a Abs. 3 KWG i. V. m. AT 4.5 Tz. 6 MaRisk als „Konzernrevision“
- in der Konzernmutter führt sie gem. § 25a Abs. 1 S. 3 Nr. 3 KWG i. V. m. AT 4.4.3 und BT 2 MaRisk prozess- bzw. organisationsbezogene Prüfungen als „Interne Revision der Konzernmutter“ durch und fungiert

- im Tochterunternehmen im Falle der Auslagerung auf Basis eines Auslagerungsvertrages gem. AT 9 MaRisk, als Erbringer von Revisionsdienstleistungen gem. § 25a Abs. 1 S. 3 Nr. 3 KWG i. V. m. AT 4.4.3 und BT 2 MaRisk als „Interne Revision des Tochterunternehmens“

In diesem Zusammenhang sind die Anforderungen an die Prüfung von Auslagerungen und IKT-Bezügen zu berücksichtigen (siehe auch Kapitel 7 Prüfung von Auslagerungen und IKT-Bezügen).

In der Prüfungsplanung, der Prüfungsdurchführung und der Berichterstattung müssen die verschiedenen Rollen hinsichtlich der Governance und des Adressatenkreises berücksichtigt werden. Als Konzernrevision (a) erfolgt die Berichterstattung an den Vorstand der Konzernmutter. Als Interne Revision der Konzernmutter (b) erfolgt die Berichterstattung ebenfalls an den Vorstand der Konzernmutter. Als Erbringer von Revisionsdienstleistungen auf Basis eines Auslagerungsvertrages (c) erfolgt die Berichterstattung primär an die Geschäftsleitung der auslagernden Unternehmen, wobei ggf. die Prüfungsberichte zusätzlich an den ressortzuständigen Vorstand im Konzern oder bei entsprechender RisikoEinstufung an den Gesamtvorstand des Konzerns weitergeleitet werden.

Sonderfall: Interne Revision eines gruppeninternen Mehrmandantendienstleisters

Sofern Tochtergesellschaften mit eigener (jedoch an die Interne Revision der Konzernmutter ausgelagerter) Revisionsfunktion, Dienstleistungen für andere beaufsichtigte Gesellschaften dieses Konzerns erbringen, sind die Prüfungen dieser Dienstleistungen sowie die Berichterstattung entsprechend zuzuschneiden. So ist darauf zu achten, dass Prüfungsumfang und Prüfungsmethodik ein Urteil für alle leistungsempfangenden Gesellschaften ermöglichen und dass, neben der Berichterstattung an die Geschäftsleitung des leistungserbringenden Unternehmens, die relevanten Prüfungsergebnisse auch an die leistungsempfangenden Gesellschaften weitergeleitet werden (vgl. AT 9 Tz. 7 i. V. m. BT 2.1 Tz. 3. MaRisk). Dies kann in Form eines (z. B. vierteljährlichen) Mandantenberichtes an die Geschäftsleitungen der leistungsempfangenden Gesellschaften umgesetzt werden.

Sonderfall: Externe Revision eines Mehrmandantendienstleisters

Sofern Gesellschaften nicht reguliert sind bzw. keinen entsprechenden rechtlichen Vorgaben unterliegen, benötigen sie per se keine eigene Interne Revision. Sobald diese Gesellschaften jedoch Leistungen für beaufsichtigte Gesellschaften erbringen, kann es zur Erfüllung der Anforderungen des AT 9 Tz. 7 i. V. m. BT 2.1 Tz. 3 MaRisk sinnvoll sein, die Konzernrevision mittels eines Dienstleistungsvertrages mit der Wahrnehmung der Internen Revisionsfunktion zu beauftragen. Auch in diesem Fall wird die Konzernrevision primär an die Geschäftsleitung des nicht beaufsichtigten Unternehmens berichten

und die relevanten Prüfungsergebnisse in Form eines Mandantenberichtes an die leistungsempfangenden Gesellschaften weiterleiten. Gleiches gilt, sollte die Konzernrevision Prozesse eines gruppenexternen Mehrmandantendienstleisters prüfen.

Die folgende Tabelle fasst noch einmal die unterschiedlichen Rollen und Berichtswege zusammen:

Rolle der Internen Revision der Muttergesellschaft	Aufsichtsrechtliche bzw. vertragliche Basis	Berichterstattung
Konzernrevision	§ 25a Abs. 3 KWG i. V. m. AT 4.5 Tz. 6 MaRisk	An die Geschäftsleitung der Konzernmutter
Interne Revision der Konzernmutter	§ 25a Abs. 1 KWG i. V. m. AT 4.4.3 und BT 2 MaRisk	An die Geschäftsleitung der Konzernmutter
Interne Revision der Tochtergesellschaft	§ 25a Abs. 1 S. 3 Nr. 3 KWG i. V. m. AT 4.4.3 und BT 2 MaRisk sowie Auslagerungsvertrag gem. AT 9 MaRisk	Primär an die Geschäftsleitung der die Revisionstätigkeit auslagernden Unternehmen
Interne Revision eines beaufsichtigten Mehrmandantendienstleisters (gruppenintern)	§ 25a Abs. 1 S. 3 Nr. 3 KWG i. V. m. AT 4.4.3 und BT 2 MaRisk und Auslagerungsvertrag gem. AT 9 MaRisk sowie Handhabung gem. AT 9 Tz. 7 i. V. m. BT 2.1 Tz. 3 MaRisk	Primär an die Geschäftsleitung der leistungserbringenden Gesellschaft und Mandantenbericht an die Geschäftsleitungen der leistungsempfangenden Gesellschaften
Externe Revision eines Mehrmandantendienstleisters (gruppenintern/-extern)	Dienstleistungsvertrag und Handhabung gem. AT 9 Tz. 7 i. V. m. BT 2.1 Tz. 3 MaRisk	Primär an die Geschäftsleitung der leistungserbringenden Gesellschaft und Mandantenbericht an die Geschäftsleitungen der leistungsempfangenden Gesellschaften

Abb. 24: Mögliche Rollen der Internen Revision der Muttergesellschaft und deren Auswirkung auf die Berichterstattung

Quellenverzeichnis:

Luz, G./Neus, W./Schaber, M./Scharpf, P./Schneider, P./Weber, M.: Kreditwesengesetz (KWG), Kommentar zum KWG inklusive SolvV, LiqV, GroMiKV und MaRisk, 2. Aufl., Stuttgart 2011.

Torwegge, C.: § 1 Gesellschaftsrechtliche Vorgaben, in: Kirchner, A./Torwegge, C./Rüth, H. H. (Hrsg.): Beteiligung und Holding, Wiesbaden 2009, S. 13 - 66, Tz. 10, 17.

16 Internes Kontrollsystem

16.1 Einleitung/ Grundlage der Thematik

16.1.1 Problemstellung

Für die Interne Revision gilt es, ihre Rolle bezüglich des Internen Kontrollsystems zu definieren und hierbei die Erwartungshaltung der diversen Stakeholder an das Interne Kontrollsystem und die Interne Revision zu berücksichtigen. Für die Interne Revision bei Kreditinstituten sind dabei neben den dominierenden bankaufsichtsrechtlichen Regelungen, auch u. a. Regelungen des Gesellschaftsrechts (inklusive Rechnungslegung) zu beachten. Teilweise treten diese in Konkurrenz bzw. ergänzen sich.

Im Zusammenhang mit der Corporate Governance werden verschiedene Subsysteme, wie Risikomanagementsystem, Internes Kontrollsystem und internes Revisionssystem, z. B. § 107 Abs. 3 S. 2 AktG, genannt. Neben der Begrifflichkeit stellt sich in der Praxis die Herausforderung der konkreten Ausgestaltung derselben unter Nutzung des Proportionalitätsgrundsatzes. Hier besitzen die Institute gewisse Freiheitsgrade, so dass man in der Praxis eine große Heterogenität vorfindet.

Im Gegensatz zu einer „losen Ansammlung von Kontrollen“ ist das Interne Kontrollsystem durch einen systematischen Ansatz geprägt. Dieser kann im Reifegrad stark variieren, z. B. Einführung eines umfangreichen Rahmenwerks wie COSO Internal Control 2013.

Der Schwerpunkt der folgenden Ausführungen liegt auf den wesentlichen Aspekten und dem sich daraus ableitenden Prüfungsansatz eines Internen Kontrollsystems in einem Institut, welches durch die systematische Identifikation sogenannter Schlüsselkontrollen, einer strukturierten Risikobewertung und einem standardisierten Berichtswesen geprägt ist. Dieses Maß an Standardisierung erfordert einen angepassten Prüfungsansatz der Internen Revision. Die Ausführungen können als Hilfestellung für Revisionsfunktionen in Instituten dienen, falls diese das Interne Kontrollsystem optimieren möchten. Es ist nicht als genereller Prüfungsansatz für jegliche Art von Kontrolle, wie sie in vielen Prozessen vorkommen und auch bereits in verschiedenen Abschnitten dieses Handbuchs angesprochen wurden, zu verstehen.

16.1.2 Wesentliche relevante Normen

Aufsichtsrechtlich ergibt sich die Verpflichtung zur Einrichtung eines internen Kontrollsystems aus § 25a Abs.1 S. 3 Nr. 3 KWG. Zunächst umfasst eine ordnungsgemäße Geschäftsorganisation insbesondere ein angemessenes und wirksames Risikomanagement. Das Risikomanagement umfasst insbesondere die Einrichtung interner Kontrollverfahren mit einem Internen Kontrollsystem und einer Internen Revision. Im Gegensatz zur allgemeinen Definition wurde damit im aufsichtsrechtlichen Bereich folgende andere Begrifflichkeit gewählt: „Interne Kontrollverfahren“ als Überbegriff für die beiden Teilkomponenten „Internes Kontrollsystem“ und „Interne Revision“ (§ 25a Abs. 1 Nr. 3 KWG; AT 1 Nr. 1 MaRisk). Die Interne Revision beurteilt nach dem Wortlaut des KWG damit das „Interne Kontrollsystem“ ist aber kein Teil von diesem.

Nach § 25a Abs.1 S. 3 Nr. 3 KWG umfasst das Interne Kontrollsystem insbesondere:

- aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche,
- Prozesse zur Identifizierung, Beurteilung, Steuerung sowie Überwachung und Kommunikation der Risiken entsprechend den in Titel VII Kapitel 2 Abschnitt 2 Unterabschnitt II der Richtlinie 2013/36/EU niedergelegten Kriterien und
- eine Risikocontrolling- und eine Compliance-Funktion.

Die Ausgestaltung des Risikomanagements und damit auch des internen Kontrollsystems hängt von Art, Umfang, Komplexität und Risikogehalt der Geschäftstätigkeit ab. Die Angemessenheit und Wirksamkeit des IKS ist regelmäßig zu überprüfen.

Die MaRisk nehmen die Struktur und Vorgaben des § 25a KWG hinsichtlich des Internen Kontrollsystems auf und konkretisieren diese insbesondere in AT 4.3 (Internes Kontrollsystem). Allerdings sind viele MaRisk-Regelungen konkrete (geschäftsspezifische) Umsetzungen (z. B. AT 5 Organisationsrichtlinien bzw. BT 1 Besondere Anforderungen an das Interne Kontrollsystem).

Weitere aufsichtsrechtliche Erwartungen ergeben sich ggf. aus den EBA/GL/2021/ 05 2. Juli 2021 „Leitlinien zur internen Governance“. Allerdings spricht die Leitlinie vom „Internen Kontrollrahmen“. U. a. sollen die Institute gemäß Rn. 141 „eine Kultur entwickeln und pflegen, die eine positive Haltung gegenüber der Risikokontrolle und Compliance innerhalb des Instituts sowie einen stabilen und umfassenden internen Kontrollrahmen bestärkt.“ Nach Rn. 145 soll der interne Kontrollrahmen eines Instituts Folgendes sicherstellen:

- wirksame und effiziente Betriebsabläufe
- umsichtige Führung der Geschäfte
- angemessene Ermittlung, Messung und Minderung von Risiken

- die Zuverlässigkeit der finanziellen und nichtfinanziellen Berichterstattung, sowohl intern als auch extern
- solide Verwaltungs- und Rechnungslegungsverfahren
- Einhaltung von Gesetzen, Rechtsvorschriften, aufsichtlichen Anforderungen sowie der internen Richtlinien, Verfahren, Regelungen und Entscheidungen des Instituts

Diese Anforderungen zeigen deutliche Bezüge zu COSO Internal Control 2013 (hier: Ziele).

Neben den aufsichtsrechtlichen Normen beschäftigen sich verstärkt gesellschaftsrechtliche Normen mit dem Internen Kontrollsystem, exemplarisch für Aktiengesellschaften § 91 Abs. 2 und 3 AktG i. V. m. § 93 Abs. 2 S. 1 AktG (BJR) auch unter Berücksichtigung der Ausstrahlungswirkung dieser Regel auf andere Unternehmensformen. Dabei sind auch die Ausführungen des Deutschen Corporate Governance Kodex zu beachten. Ergänzend regelt § 289 Abs. 4 HGB i. V. m. DRS 20 die Lageberichterstattung über das Interne Kontrollsystem.

Weitere Erwartungen an ein Internes Kontrollsystem ergeben sich aus den berufsständischen Normen der Internen Revisoren (IPPF n. F. i. V. m. den DIIR Revisionsstandards n. F.) als auch den berufsrechtlichen Regelungen für Wirtschaftsprüfer (z. B. IDW PS 261 n. F., IDW PS 980, IDW PS 982).

16.1.3 Erwartungshaltung hinsichtlich des Internen Kontrollsystems an die Geschäftsleitung (Organisationsverantwortung)

Gemäß EBA Leitlinien zur internen Governance (EBA/GL/2021/05) Rn. 22 gilt:

Die Zuständigkeiten des Leitungsorgans sollten die Festlegung, Genehmigung und die Überwachung der Umsetzung der folgenden Aspekte umfassen:

...

c. ein angemessener und wirksamer Rahmen für die interne Governance und die interne Kontrolle nach der Definition in Titel V

...

Nach AT 2 Tz. 2 MaRisk ist jeder Geschäftsleiter – ungeachtet der Gesamtverantwortung der Geschäftsleitung für die ordnungsgemäße Geschäftsorganisation und insbesondere für ein angemessenes und wirksames Risikomanagement – für die Einrichtung angemessener Kontroll- und Überwachungsprozesse in seinem jeweiligen Zuständigkeitsbereich verantwortlich. Für die Geschäftsleitung ergibt sich damit eine Festlegungs-, Einrichtungs-, Pflege- und Aktualisierungsverantwortung.

Gemäß der EBA/GL/2021/05 muss das konsolidierende Institut die Einhaltung der Governance-Richtlinien und des in Titel V genannten internen Kontrollrahmens auf Gruppenebene durch alle Institute und sonstigen Einrichtungen im aufsichtlichen Konsolidierungskreis, einschließlich seiner Tochtergesellschaften, die selbst nicht der Richtlinie 2013/36/EU unterliegen, sicherstellen.

16.1.4 Erwartungshaltung hinsichtlich des Internen Kontrollsystems an die Interne Revision (Überwachungsverantwortung)

Die Rolle der Internen Revision bezüglich des Internen Kontrollsystems ergibt sich aus der Erwartungshaltung der Stakeholder, u. a. der Aufsicht, an die Interne Revision. Aufsichtsrechtlich ergibt sich aus den MaRisk:

AT 4.4.3 Tz. 3: Die Interne Revision hat risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements im Allgemeinen und des internen Kontrollsystems im Besonderen sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse zu prüfen und zu beurteilen, unabhängig davon, ob diese ausgelagert sind oder nicht.

Die Interne Revision beurteilt damit nicht nur die einzelnen Komponenten (z. B. Kontrollen oder Kontrollmechanismen), sondern unter Berücksichtigung der Risikoorientierung auch das Interne Kontrollsystem als Ganzes.

Gemäß Rn. 218 der EBA Leitlinie sollte die Interne Revision bewerten, ob der interne Kontrollrahmen des Instituts sowohl wirksam als auch effektiv ist. Insbesondere sollte die Interne Revision Folgendes beurteilen:

- die Angemessenheit des Rahmenwerks für die interne Governance des Instituts
- den Umstand, ob bestehende Richtlinien und Verfahren nach wie vor angemessen sind und den gesetzlichen und aufsichtlichen Anforderungen sowie dem Risikoappetit und der Risikostrategie des Instituts entsprechen

- die Übereinstimmung der Verfahren mit den anwendbaren Gesetzen und Rechtsvorschriften sowie mit den Entscheidungen des Leitungsorgans
- den Umstand, ob die Verfahren korrekt und wirksam umgesetzt werden (z. B. Compliance der Durchführung von Transaktionen, der Umfang des tatsächlich eingegangenen Risikos, usw.)
- die Eignung, Qualität und Wirksamkeit der durchgeführten Kontrollen sowie die erfolgte Berichterstattung seitens der operativen Geschäftsbereiche, der Risikomanagementfunktion und Compliance-Funktion

Bezüglich der Internen Revision wird in Rn. 221 der EBA Leitlinien zur internen Governance formuliert: „Die Interne Revision sollte nationale und internationale Normen des Berufsstandes einhalten. Ein Beispiel für die hier angeführten Normen des Berufsstandes sind die vom Institute of Internal Auditors (IIA) verfassten Standards.“ Hieraus ergibt sich zumindest eine Erwartungshaltung, dass die berufsrechtlichen Regelungen des IIA hinsichtlich Anforderungen bezüglich der Überwachung des Internen Kontrollsystems analysiert werden.

Während der Begriff Internes Kontrollsystem, wie oben eingeführt, keine direkte Verwendung in den Standards findet, zieht sich die Berücksichtigung von Governance-, Risikomanagement- und Kontrollprozessen durch nahezu alle Domains der GIAS (exemplarisch hervorzuheben sind u.a.

- Domain I: GIAS Standard 1.2 „Ethische Erwartungen der Organisation“, GIAS Standard 4.2 „Berufliche Sorgfalt“,
- Domain III: GIAS Standard 8.1 „Interaktion mit dem Leitungs- und Überwachungsorgan“,
- Domain IV: GIAS Standard 9.1 „Verstehen von Governance-, Risikomanagement und Kontrollprozessen“, Standard 9.4 „Revisionsplan“,
- Domain V: GIAS Standard 13.2 „Risikobeurteilung zu einem Auftrag“, GIAS Standard 14.5 „Gesamturteil zu einem Auftrag“)

und zeigt damit auf, dass eine systematische Betrachtung dieser Prozesse durch die Interne Revision an Bedeutung gewinnt.

Hier und an anderen Stellen wird erkennbar, dass sich aus den GIAS die Erwartung ergibt, dass sich die Interne Revision mit den Instrumenten „Rahmenwerke“, „Reifegrad-Modelle“, „Risk-Control-Matrix“ und „Schlüsselkontrollen“ hinsichtlich Zweckmäßigkeit auseinandersetzt und die Geschäftsleitung beim Verständnis der Wirksamkeit der Governance-, Risikomanagement- und Kontrollprozesse der Organisation unterstützt. Dies bedeutet aber keine Umsetzungsverpflichtung für die Etablierung eines Internen Kontrollsystems durch die Interne Revision.

Die Interne Revision führt sowohl Angemessenheits- (Test-of-Design) als auch Wirksamkeitsbeurteilungen (Test-of-Operating-Effectiveness) durch. Die Bewertung der Angemessenheit des Kontrolldesigns wird häufig im Rahmen der Auftragsplanung durchgeführt, da dies Internen Revisorinnen und Revisoren hilft, Schlüsselkontrollen klar zu identifizieren, die weiter auf ihre Wirksamkeit getestet werden sollen. Der Nachweis kann durch Dokumentation in den Arbeitspapieren erfolgen.

Anstatt der Beurteilungen einzelner Sachverhalte kann eine Gesamtbetrachtung des internen Kontrollsystems erforderlich sein bzw. eingefordert werden (vertiefend Standard 11.3).

16.1.5 Rolle der IKS-Koordinationsstelle als „Second Line“ bzw. als Standardsetzer

Beim Aufsatz eines systematischen Internen Kontrollsystemansatzes sind die Verantwortlichkeiten für die Vorgaben und die möglichen Aufgaben einer IKS-Koordinationsstelle bzw. der Stelle des Standardsetzers für die Governance des IKS im Institut festzulegen. Die Verantwortung des Standardsetzers umfasst die Definition und kontinuierliche Weiterentwicklung des Ansatzes zur strukturierten und risikoorientierten Erhebung der Funktionsfähigkeit des IKS (auf Basis von IKS-Schlüsselkontrollen), die Initiierung und Steuerung des jährlichen IKS-Prozesses sowie die Berichterstattung zum IKS. Einheiten, die üblicherweise als Standardsetzer fungieren, sind unter anderem die Organisationsabteilung und das Risikomanagement (z. B. wegen Operational Risk).

Zur Sicherstellung einer homogenen Anwendung sind in der IKS-Governance auch entsprechende Umsetzungsrichtlinien und der Ablauf des IKS-Prozesses, exemplarisch in Form eines Regelkreises (z. B. Risikoidentifikation und -bewertung (vor Kontrollen), Kontrollinventur, Kontrollbewertung, Kontrolloptimierung, unabhängiges Testing und Berichterstattung) zu definieren.

Zu berücksichtigen ist auch die Verzahnung mit anderen Elementen des Risiko- und/oder des Compliance-Management-Systems, was entsprechend zu dokumentieren und im Unternehmen zu kommunizieren ist. Dabei kommt der Verortung des Internen Kontrollsystemansatzes im Kontext des Three Lines-Modells, insbesondere bezüglich der Verantwortlichkeiten zur Etablierung von Kontrollen, zum Testen von Kontrollen und die Auswirkung des Rollenverständnisses (u. a. der Internen Revision) eine wichtige Bedeutung zu.

16.2 Rolle der Internen Revision

Das Thema Kontrollen sollte durch die Interne Revision aus zwei unterschiedlichen Perspektiven betrachtet werden: die Identifikation und das Steuern von Schlüsselkontrollen im Revisionsprozess und das Prüfen bzw. das Testen von Kontrollen.

16.2.1 IKS in der Internen Revision

Die Revision sollte diejenigen Kontrollen bzw. Schlüsselkontrollen („Quality Gates“) im Rahmen ihres Standardrevisionsprozesses identifizieren, die essentiell sind, angemessene, fristgerecht erstellte Ergebnisse bzw. Ergebnisdokumente zu generieren. In Frage kommen hier bspw. die Prozesse zur Erstellung des Prüfungsberichts, Quartals-/Jahresberichts oder des Jahresprüfungsplans. Oftmals sind bereits entsprechende Kontrollen eingerichtet (z. B. die Freigabe von (Zwischen-)Ergebnissen bei der Erstellung), so dass diese für eine Integration in ein bankweites, konsistentes IKS nur entsprechend systematisch aufbereitet werden müssen, ggf. ergänzt um das Testing dieser Kontrollen. Hierfür ist es von Vorteil, wenn die Kontrollen technisch im Revisionsmanagementsystem durchgeführt werden. Wird z. B. die Freigabe des Revisionsberichtes vor Versand an die Geschäftsleitung als Schlüsselkontrolle etabliert, so vereinfacht es das Testing, wenn die Durchführung der Kontrolle, d. h. in diesem Beispiel die Freigabe des Berichts, im System stattfindet. So kann im Rahmen des Testings verifiziert werden, ob tatsächlich alle Berichte wie vorgesehen durch den Kompetenzträger freigegeben wurden. Entsprechend ist für die Kontrollen auch der Kontrolleigner-, der Kontrolltester, das Kontrollziel, die zu mitigierenden Risiken, die Testingfrequenz etc. festzulegen.

Neben der intrinsischen Motivation, sich mittels strukturierter Kontrollen der Qualität des Wertschöpfungsprozesses in der Revision zu versichern, können, da der Internen Revision auch eine Art Vorbildfunktion zuzurechnen ist, andere Fachbereiche eher dazu zu bewegt werden, sich dem Thema (Schlüssel-)Kontrollen zu öffnen.

16.2.2 Kontrollen im Prüfungsuniversum

Die Interne Revision ist – nicht zuletzt auch durch regulatorische Vorschriften – dazu angehalten, sich mit Kontrollen im Rahmen der Prüfungen auseinanderzusetzen. Dies beinhaltet sowohl die „normalen“ Kontrollen als auch die Schlüsselkontrollen, die wesentliche Risiken mitigieren und primärer Gegenstand dieses Textes sind. Eine prüferische Auseinandersetzung wird durch ein strukturiertes IKS deutlich erleichtert, da durch eine systematisch erhobene Liste von Schlüsselkontrollen eine Zuordnung zu den einzelnen Prüfobjekten im Revisionsmanagementsystem ermöglicht wird. Dies gestattet eine fundiertere Risikobewertung der Prüfobjekte in Hinblick auf das Kontrollumfeld. Im Rahmen der Konzeption des Bewertungsverfahrens ist festzulegen, unter welchen Bedingungen

die Kontrollen das Risiko in welchem Maße reduzieren. Dazu sollten die Ergebnisse aus den eigenen Prüfungen, aber z. B. auch die der Kontrolltester, herangezogen werden.

Neben der Betrachtung der Schlüsselkontrollen auf Prüfobjektebene ist es zweckmäßig, auch ein Prüfobjekt zur Prüfung der IKS-Governance, d. h. die Prozesse rund um die IKS-Koordinationsstelle, anzulegen.

Die Informationen welche Schlüsselkontrollen mit welchen Prüfobjekten verknüpft sind, sollte auch bei der Jahresplanung und beim Scoping der individuellen Prüfungen als wichtige Informationen herangezogen werden. In diesem Kontext muss die Revision ein Konzept entwickeln, wie das Prüfen von Kontrollen bzw. Schlüsselkontrollen sich in den verschiedenen Aspekten des Revisionsprozesses niederschlägt (d. h. Prüfungsvorbereitung, -durchführung, etc.).

16.2.3 Prüfungsansätze zur IKS-Koordinationsstelle bzw. Funktion des Standardsetzers durch die Interne Revision

Prüfungsansätze der Internen Revision zur Funktion des Standardsetzers können, orientiert an den Vorgaben zu den Aspekten eines Regelkreises, folgende sein:

Risikoidentifikation und -bewertung (vor Kontrollen):

Basis des IKS-Regelkreises ist die Risikoeinschätzung, welche die Identifizierung, Erfassung und Bewertung der prozessinhärenten operationellen Risiken in den jeweiligen Anwendungen des Kreditinstitutes sowie die regelmäßige Überprüfung der Vollständigkeit und Aktualität der Risiken gemäß den Vorgaben des Risikomanagements (Operational Risk Controlling) durch den IKS-Verantwortlichen umfasst.

Mögliche Fragestellungen:

- Werden Kontrollen nach Kontrollzielen (z. B. Finanzberichterstattung, Operations, Compliance) strukturiert, z. B. anhand eines methodischen Rahmenwerks wie COSO Internal Control 2013?
- Erfolgt eine Qualitätssicherung durch den Standardsetzer bei dezentraler Risikoidentifikation und -bewertung (z. B. QS von Operational Risk Controlling)?
- Wird die Vollständigkeit der Kontrollen durch den Standardsetzer beurteilt?

Kontrollinventur:

Das Ziel der Kontrollinventur ist es, den identifizierten und bewerteten Risiken entsprechenden Schlüsselkontrollen zuzuordnen, welche das jeweilige Risiko mitigieren sollen

und diese angemessen in Organisationsrichtlinien, Kontrollsteckbriefen sowie in der Risikokontrollmatrix zu beschreiben.

Mögliche Fragestellungen:

- Werden Kontrollen, Kontrollbeschreibungen und Nachweise für die Kontrolldurchführung systemisch erfasst?
- Erfolgt ein vollständiges Mapping der identifizierten wesentlichen Risiken auf die relevanten Prozesse und Schlüsselkontrollen.

Kontrollbewertung:

a) Kontrollangemessenheit:

Diese ist gegeben, wenn die Schlüsselkontrolle geeignet ist, ein Risiko gemäß den intern/externen Vorgaben entsprechend zu mitigieren. Die Bewertung der Angemessenheit von Schlüsselkontrollen erfolgt z. B. auf Basis einer Ampel, welche Bestandteil der Berichterstattung an die Geschäftsleitung und das Aufsichtsorgan (Prüfungsausschuss) ist.

b) Kontrollwirksamkeit:

Diese zeichnet sich dadurch aus, dass die Schlüsselkontrolle gemäß den Vorgaben (Organisationsrichtlinien) des Kreditinstituts ausgeführt wurde und die Durchführung anhand einer angemessenen Dokumentation nachvollziehbar ist und dadurch der Eintritt des Risikos tatsächlich vermieden oder begrenzt werden konnte. Dies kann z. B. anhand von Stichproben im Rahmen des Testings beurteilt werden (Freigabeprotokollen, Systemdateien, Belege etc.), welche durch die IKS-Verantwortlichen zu dokumentieren und archivieren sind.

Mögliche Fragestellungen:

- Wird die Funktionsfähigkeit und Erreichung des Kontrollziels durch den Standardsetzer oder andere Funktionen bewertet?
- Wurde eine standardisierte Bewertungssystematik für die IKS-Schlüsselkontrolldurchführung festgelegt?

Kontrolloptimierung:

Das Ziel der Kontrolloptimierung ist es, identifizierte Kontrollschwächen und -lücken, aber auch Dopplungen, durch entsprechende Maßnahmen zu beheben. Es ist Aufgabe des IKS-Verantwortlichen in den Fachbereichen, entsprechende Maßnahmen zu entwickeln und deren Implementierung nachzuhalten.

Unabhängiges Testing:

Für die Überwachung des IKS empfiehlt sich eine Kombination aus einem dezentralen Self-Assessment und einem dezentralen Control Testing.

Mögliche Implementierung der Schritte eines dezentralen Self-Assessments und eines dezentralen Control Testings:

- Schritt 1: Die Schlüsselkontrolle wird durch den Kontrollverantwortlichen durchgeführt und dokumentiert.
- Schritt 2: Die Angemessenheit (Test of Design) und die Funktionsfähigkeit (Test of Operating Effectiveness) der Schlüsselkontrolle wird regelmäßig (z. B. quartalsweise, risikoorientiert) durch den IKS-Verantwortlichen geprüft und dokumentiert (Self-Assessment). Die Ergebnisse werden an die IKS-Koordinationsstelle berichtet.
- Schritt 3: Es erfolgt in Stichproben ein Control Testing durch die IKS-Koordinationsstelle, welche die Angemessenheit und die Wirksamkeit der Schlüsselkontrolle anhand der Dokumentation des Kontrollverantwortlichen/IKS-Verantwortlichen prüft.
- Schritt 4: Seitens der Internen Revision werden die Schlüsselkontrollen aufbauend auf dem Test of Design (ToD: Angemessenheit) und dem Test of Operation Effectiveness (ToE: Funktionsfähigkeit) geprüft. Im Rahmen dessen wird die Verknüpfung zwischen operationellen Risiken, Schlüsselkontrollen, Organisationsrichtlinien und Kontrollsteckbriefen berücksichtigt. Diesbezüglich werden zum einen die identifizierten Mängel den Kategorien „ToD: Kontrolldesign“, „ToD: Kontrollbeschreibung“, „ToE: Kontrolldurchführung“ und „ToE: Kontrolldokumentation“ zugeordnet. Zum anderen wird die Bewertung des Schweregrads des Mangels einer Schlüsselkontrolle durch die Interne Revision anhand der Bewertungsstufen „gering“, „mittel“ und „hoch“ eingestuft. Die Ergebnisse der geprüften Schlüsselkontrollen werden im Rahmen jeweiligen Prüfungsberichts dargestellt und für die Quartalsberichte und den Jahresbericht der Internen Revision konsolidiert ausgewertet. Sofern keine Mängel bei einer geprüften Schlüsselkontrolle festgestellt wurden, wird diese ebenso im entsprechenden Prüfungsbericht kommuniziert.

Berichterstattung:

Das Ziel der Berichterstattung ist es, insbesondere die die Geschäftsleitung sowie den Prüfungsausschuss in die Lage zu versetzen, die Angemessenheit und Wirksamkeit des IKS beurteilen zu können (vgl. auch § 25a KWG).

16.2.4 Prüfung von Kontrollen

Das Prüfen von Kontrollen ist eine der Kernaufgaben der Internen Revision. Um eine möglichst einheitliche Vorgehensweise in unterschiedlichen Prüferteams sicherzustellen, sollte im Revisionsprozess dargelegt werden, wie der revisorische Umgang mit (Schlüssel-)Kontrollen in Prüfungen dargestellt wird.

In der Praxis finden sich die unterschiedlichsten Ausprägungen bei der Behandlung von Schlüsselkontrollen in Prüfungen. Diese reichen von der „einfachen“ Integration der Prüfung der Kontrollen in den normalen Prüfungen bis hin zur vollständigen, zusätzlichen Übernahme des Kontrolltestings und Erstellung von entsprechenden Berichten an die Kontrollorgane (Aufsichtsorgan etc.). Neben der Frage, welche Aufgaben die Revision im IKS-Regelkreis wahrnimmt, muss die Festlegung des Vorgehens daran ausgerichtet sein, wie sich die erhobenen Informationen im Berichtswesen der Revision niederschlagen, aber auch wie welche Informationen an andere potenziell betroffene Bereiche der Bank (z. B. 2nd Line für IKS; OpRisk-Management) weitergeleitet werden.

Bei der Betrachtung der verschiedenen Phasen der Prüfungsdurchführung, gibt es die unterschiedlichsten Berührungspunkte:

- Beauftragung des Prüfens von (Schlüssel-)Kontrollen im Prüfungsauftrag/Audit Planning Memorandum.
Hier ist zu beachten, dass „normale“ Kontrollen auch ohne ausdrücklichen Hinweis der revisorischen Betrachtung unterliegen.
- Verwendung von Risiko-Kontroll-Matrizen, beispielsweise im Rahmen der Prüfungsvorbereitung/Scoping und/oder im Fieldwork.
Dabei werden den Kontrollen einzelner Prozessschritten den entsprechenden Risiken gegenübergestellt, unabhängig ob es sich um „normale“ Kontrollen oder Schlüsselkontrollen handelt. Dies stellt eine systematische Behandlung des Kontrollumfelds im jeweils betrachteten Prüfobjekt sicher.
- Darstellung der Ergebnisse der Prüfung von (Schlüssel-)Kontrollen im Revisionsbericht und im Jahres-/Quartalsbericht, Darstellung der Angemessenheit und Wirksamkeit von Kontrollen im Bericht.
Erstellen von besonders aufbereiteten Berichten für Prüfungen, in denen nur getestet wurde („Blocktesting“), kann die Entwicklung eines eigenen Berichtsvorlage und von den „normalen Prüfungen“ abweichender Standards praktikabel sein.
- Bewertung „durchgefallener“ (Schlüssel-)Kontrollen: standardisierte Textmodule für Feststellungen und Maßnahmen (Design/Effectiveness)

Die Prüfung der IKS-Kontrollen sollte insbesondere folgende Elemente enthalten:

Angemessenheitsprüfung (Design)

Sind die Kontrollen in Hinblick auf die erfolgreiche Erstellung des Produktes/der Dienstleistung (Kontrollgegenstand) unter Berücksichtigung eines definierten Sicherheitsniveaus angemessen aufgesetzt? Wird durch das Design/Setup der Kontrolle das Kontrollziel erreicht (z. B. Prüfungsziele im Rahmen der Finanzberichterstattung: Completeness – Vollständigkeit, Existence – Existenz, Accuracy – Genauigkeit, Valuation – Bewertung, Obligation – rechtlicher Besitz, Presentation – Ausweis)? Ist die Kontrolle angemessen dokumentiert und enthält die Dokumentation alle wesentlichen Informationen?

Wirksamkeitsprüfung (Effectiveness)

Werden Kontrollen auf Basis des Designs und des Kontrollziels angemessen, in einer geeigneten Häufigkeit durchgeführt und sind sie wirksam? Werden aufgrund der Ergebnisse der Kontrolldurchführung ggf. erforderliche Maßnahmen abgeleitet?

Die Interne Revision kann auch Hinweise zu fehlenden, aber auch überflüssigen Kontrollen aus ihren Prüfungshandlungen gewinnen.

Die Beurteilung der Angemessenheit, Wirksamkeit und Vollständigkeit der IKS-Kontrollen insgesamt bzw. des IKS als Ganzes, sollte allerdings bei Verantwortlichen im Unternehmen liegen (z. B. IKS-Koordinationsstelle), um die Unabhängigkeit und Objektivität der Internen Revision diesbezüglich nicht zu gefährden.

16.2.5 Testing durch die Interne Revision

Sofern sich das Institut dafür entscheidet, dass die Interne Revision – neben der Prüfung von Kontrollen – das Testing aller Schlüsselkontrollen übernimmt, sollten einige Dinge beachtet werden.

Pro und Contra: Die Testdurchführung durch die Interne Revision ist mit Vor- und Nachteilen verbunden. Die hohe Überlappung mit eigenen Prüfungsthemen, die bereits vorhandenen Unternehmenskenntnisse und die möglichen Synergieeffekte sprechen für die Interne Revision als Einheit für die Testdurchführung. Darüber hinaus sind der IKS-Prozess und die Aufgabenwahrnehmung des Standardsetzers Aktivitäten des Unternehmens, die gemäß MaRisk BT 2.3 Tz. 1 durch die Interne Revision zu prüfen sind. Andererseits ist zu berücksichtigen, dass die Testdurchführung bei einem systematischen IKS-Ansatz und entsprechender technischer Unterstützung grundsätzlich unter dem Anforderungsprofil eines Internen Revisors liegt und je nach Reifegrad des IKS-Systems gewisse Risiken hinsichtlich der Unabhängigkeit und Objektivität für die Interne Revision birgt.

Auch die Testdurchführung durch die Interne Revision muss angemessen geplant werden, wobei z. B. ein potenziell vorhandener Regelprozess des Standardsetzers berücksichtigt werden muss.

Erfolgt die unabhängige Testdurchführung durch die Interne Revision, bietet sich eine Integration in die reguläre Revisionsprüfungsplanung an. Die Struktur des Prüfungsuniversums der Internen Revision und der methodische Ansatz des IKS (meist prozessbasiert) sollten hierbei homogen sein, um bestmögliche Synergien zu erzielen.

Darüber hinaus sind die Prüfungs- und Testfrequenz abzugleichen. Sollte das IKS eine in Teilen höhere Testfrequenz erfordern, ist diese in der Prüfungsplanung zu berücksichtigen. Dies kann z. B. durch Zusammenfassung der zu testenden Kontrollen mit abweichender Testfrequenz in separaten Prüfungen, sogenannten Blocktestings, erreicht werden.

In den Fällen, in denen sowohl ein homogener Ansatz und eine gleichartige Test- bzw. Prüfungsfrequenz vorliegen, können die Testingaktivitäten im Rahmen der regulären Revisionsprüfungen erfolgen. Im Sinne einer risikoorientierten Prüfung sollten Schlüsselkontrollen regelmäßig im Prüfungsumfang von Revisionsprüfungen berücksichtigt sein.

16.2.6 IKS im Berichtswesen der Internen Revision

Für den zentralen Prüfungsgegenstand „Internes Kontrollsystem“ ist auch das Berichtswesen der Internen Revision festzulegen. Die Festlegung erfolgt durch den Leiter der Internen Revision in Abstimmung mit und unter Berücksichtigung der Erwartungshaltung der Stakeholder. Die Berichterstattung kann in unterschiedliche Ebenen geregelt sein:

- a) Berichterstattung über den Teilaspekt „Internes Kontrollsystem“ in einzelnen Prüfobjekten (z. B. Kreditverwendungskontrolle) als Teil des Prüfungsauftrags (= Prüfobjektebene)
- b) Berichterstattung über das Interne Kontrollsystem als Hauptprüfobjekt eines Prüfungsauftrags (= Systemebene)
- c) Gesamtbetrachtung des Internen Kontrollsystems durch die Interne Revision (= Unternehmensebene)

Wenn eine Beurteilung des prüfungsobjektbezogenen IKS erfolgt, ergeben sich neben der Beurteilung des konkreten prüfungsobjektbezogenen IKS und der Berichterstattung auch eine Vielzahl an Mosaiksteinen für die Berichterstattungen der Ebenen b) und c).

So können „Schlüsselkontrollen“ seitens der Internen Revision auf Prüfobjektebene nachfolgenden Dimensionen dargestellt werden:

- Test of Design (ToD: Angemessenheit) und
- Test of Operation Effectiveness (ToE: Funktionsfähigkeit)

Bei der Prüfung der Schlüsselkontrollen wird die Verknüpfung zwischen operationellen Risiken, Schlüsselkontrollen, Organisationsrichtlinien und Kontrollsteckbriefen berücksichtigt. In diesem Kontext kann die Bewertung des Schweregrads des Mangels in einer Schlüsselkontrolle durch die Interne Revision beispielsweise anhand der Bewertungsstufen „gering“, „mittel“ und „hoch“ eingestuft werden. Diesbezüglich werden die identifizierten Mängel den Kategorien

- „ToD: Kontrolldesign“
- „ToD: Kontrollbeschreibung“
- „ToE: Kontrolldurchführung“
- „ToE: Kontrolldokumentation“

zugeordnet.

Durch die Prüfungsplanung wird angestrebt, dass die Interne Revision über die Angemessenheit und Wirksamkeit einzelner Schlüsselkontrollen berichtet und eine übergreifende Beurteilung der Schlüsselkontrollen grundsätzlich möglich ist.

Die Ergebnisse der geprüften prüfungsobjektbezogenen Schlüsselkontrollen werden im Rahmen jeweiligen Prüfungsberichts dargestellt. Sofern keine Mängel bei einer geprüften Schlüsselkontrolle festgestellt wurden, kann dies ebenso kommuniziert werden.

Zusätzlich erfolgt auch die konsolidierte Berichterstattung in den Quartalsberichten und dem Jahresbericht der Internen Revision, die beispielsweise auch einen „Key Control Finding Ratio“ (Anteil der Anzahl geprüfter Schlüsselkontrollen im jeweiligen Quartal mit IKS-Mängeln (niedrig; mittel; hoch) an der Gesamtanzahl geprüfter Schlüsselkontrollen im jeweiligen Quartal) enthält (Ebene c).

Bei einer auf Ebene b) fokussierten Prüfung des Prüfobjekts „IKS/Schlüsselkontrollen“ im Rahmen einer Systemprüfung (z. B. hinsichtlich Definition, Bestimmung, Verantwortlichkeit etc.) erfolgt eine entsprechende Berichterstattung. Diese fließt dann in die Berichterstattung über die Gesamtbeurteilung des Internen Kontrollsystem ein.

Bei dieser Systemprüfung (Ebene b) stellen die prüfungsobjektspezifischen Prüfungsergebnisse (Ebene a) Einzelfallprüfungen dar, d. h. eine positive Beurteilung Systemebene b) ist bei einer Vielzahl von negativen Beurteilungen auf Prüfobjektebene (Ebene a) nicht plausibel. Dies ist bei der Berichterstattung zu beachten.

Von den bisher behandelten „normalen“ Berichterstattungsformaten ist die Ad Hoc-Berichterstattung zu unterscheiden, insofern ist auch hinsichtlich des Internen Kontrollsystems die Schwelle für eine Ad Hoc-Berichterstattung festzulegen.

17 Schnittstelle mit Aufsichtsbehörden, externen Prüfern und der Zweiten Linie

17.1 Einleitung/ Grundlage der Thematik

Für eine effektive Internen Revision ist die Interaktion mit der Geschäftsleitung, den Fachbereichen der 1st und 2nd Line und dem Prüfungsausschuss des Aufsichtsorgans sowie mit externen Prüfern und Aufsichtsbehörden. Diese Interaktion dient der Information über aktuelle Entwicklungen sowie der frühzeitigen Erkennung von existierenden und zukünftigen Risiken und damit der risikoorientierten Ausrichtung ihrer Aktivitäten an den Bedürfnissen des Institutes.

Mit Inkrafttreten der GIAS sind die Anforderungen an den Aufbau von Beziehungen und Kommunikation mit Stakeholdern im GIAS Standard 11.1 definiert. Demgemäß muss die Revisionsleitung einen Ansatz für die Interne Revision entwickeln, um Beziehungen und Vertrauen zu den wichtigsten Stakeholdern aufzubauen, einschließlich Überwachungsorgan, Geschäftsleitung, dem operativen Management, den Aufsichtsinstitutionen sowie interner und externer Assurance Provider und anderer Berater. Dieses kann beispielsweise über eine Relationshipmatrix und ein dazugehöriges Konzept gesteuert werden, in der den Mitarbeitern der Internen Revision Stakeholdern zugeordnet werden mit dem Ziel des regelmäßigen Austauschs.

In diesem Kontext ist der GIAS Standard 9.5 anzuführen. Dieser Standard definiert die Muss-Anforderung an die Revisionsleitung sich mit internen und externen Assurance Providern abzustimmen und zu erwägen sich auf deren Arbeit zu verlassen. Zu den besonderen Schnittstellen der Internen Revision zählen die Einheiten der zweiten Linie (Kontrollfunktionen), die externen Prüfer bzw. Jahresabschlussprüfer und die Aufsichtsinstitutionen. Mit diesen gilt einen regelmäßigen Austausch über die jeweiligen Prüfungstätigkeiten und Schwerpunkte herzustellen.

In diesem Zusammenhang fällt auch der Begriff der „Combined Assurance“. Die Zielsetzung ist, eine – so weit möglich – abgestimmte Vorgehensweise zu implementieren und sicherzustellen, so dass sich insbesondere an der Schnittstelle zwischen Interner Revision und den Einheiten der zweiten Linie eine für das Institut mehrwertstiftende und effiziente Zusammenarbeit ergibt. Als Kommunikations-, Koordinations- und Überwachungsinstrument wird im Standard eine Prüfungsübersicht (= Assurance Map) vorgeschlagen, in der die Ergebnisse strukturiert zusammengeführt werden.²⁸ An dieser Stelle sei darauf

²⁸ Praxisleitfaden Koordination und Vertrauen – Entwicklung einer Prüfungsübersicht, DIIR, 2020 (Version1).

hingewiesen, dass diesem Ansatz für Internen Revisionen im Bankenumfeld Grenzen gesetzt sind. Die Unabhängigkeit der Internen Revision hat gerade von den Aufsichtsinstanzen unverändert einen hohen Fokus, und wurde mit den Änderungen durch das BRU-BEG in § 25a Abs 1 S.3 Nr. 3 KWG noch einmal besonders betont.

Die Interaktion der Internen Revision mit Einheiten der zweiten Linie, die externen Prüfer bzw. Jahresabschlussprüfer und die Aufsichtsinstanzen inkludiert die Aufnahme von Feststellungen aus externen Prüfungen (z. B. Aufsichtsbehörden, Jahresabschlussprüfer, etc.) in den Überwachungsprozess zur Mängelbeseitigung (Follow-up) der Internen Revision.

Der Bedarf an Zusammenarbeit und Kommunikation zwischen der 1st und 2nd Line und der Internen Revision (immer unter Berücksichtigung der Unabhängigkeit der Funktion), zur Vermeidung unnötiger Doppelarbeiten, Überschneidungen oder Lücken ergibt sich bereits aus dem Three-Lines-Model, welches die Weiterentwicklung des Three Lines of Defence Modells darstellt. Daher wird vor einer näheren Beleuchtung der Zusammenarbeit mit internen und externen Assurance Providers im nächsten Kapitel zunächst kurz auf dieses Modell eingegangen.

17.2 Grundlagen des Drei-Linien Modells

Das Drei-Linien-Modell (Three Lines Model, TLM) hat sich zum aktuellen Grundmodell aufsichtsrechtlichen Denkens entwickelt.

Das IIA Drei- Linien-Modell

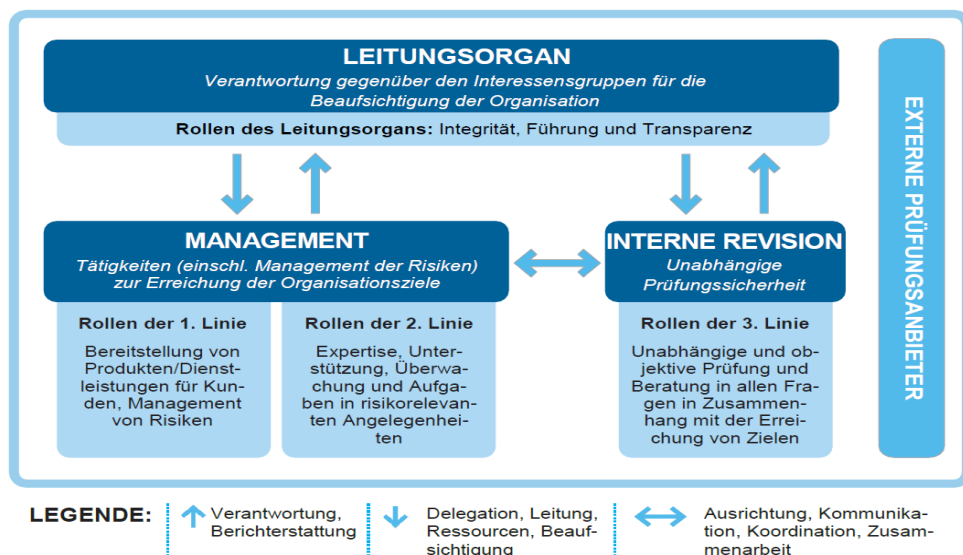


Abb. 25: Das IIA - Drei Linien-Modell

Im Sinne des Modells wird als erste Linie die (Selbst-) Kontrolle (z. B. durch Funktionstrennung, Vier-Augen-Prinzip) der operativ tätigen Geschäftsbereiche angesehen. Diese einzurichten und zu pflegen ist die Verantwortung des jeweiligen Risikoträgers (Risk Owners).

Die zweite Linie besteht aus der prozessabhängigen Überwachung und Kontrolle durch z. B. die Risikocontrolling-Funktion, die Compliance-Funktionen, etc. Die Einheiten der Zweiten Linie sollten im engen Austausch mit der Ersten Linie stehen und sicherstellen, dass die Risiken im Institut angemessen identifiziert und gesteuert werden und die implementierten Kontrollen bzw. Überwachungsprozesse wirksam umgesetzt werden. Hierzu führen sie eigene Kontroll-/ Überwachungshandlungen aus.

Die prozessunabhängige Interne Revision nimmt als dritte Linie eine besondere Stellung im Modell ein. Sie hat die Aufgabe, die Angemessenheit und Wirksamkeit des Risikomanagements allgemein und des internen Kontrollsystems im Besonderen (sowohl der Ersten als auch der Zweiten Linie) zu überprüfen und zu beurteilen. Die Übernahme von Aufgaben der ersten und zweiten Linie durch die Interne Revision ist aufgrund ihrer Stellung ausgeschlossen, da diese ansonsten die notwendige (Prozess-)Unabhängigkeit verlieren würde. Die Interne Revision stellt somit auch einen unverzichtbaren Bestandteil einer „guten“ Corporate-Governance und auch Risikokultur eines Institutes dar.

Bei der letzten Überarbeitung des TLM wurde klargestellt, dass mit den Linien keine vollständig voneinander abgegrenzten Silos gemeint sind und auch keine starre Abfolge von der ersten über die zweite zur dritten Linie, sondern vielmehr Kommunikation, Koordination und Zusammenarbeit erforderlich ist. Es geht weniger um Linienzugehörigkeit, sondern vielmehr um „Rollen und Beziehungen, die zugewiesen, kombiniert oder getrennt werden können, und um Wechselbeziehungen“.²⁹

17.3 Schnittstelle zu der Zweiten Linie (inkl. weiteren Einheiten des Risikomanagements)

Die Funktionen der 2nd Line sind aufgrund ihrer Natur als prozessabhängige Überwachung und Kontrolle ein wichtiger Stakeholder für die Interne Revision sowohl mit Blick auf Informationen zur Wirksamkeit des Kontrollsystems als auch die Berücksichtigung der Ergebnisse bei der prüferischen Abdeckung durch die Interne Revision. In diesem Zusammenhang sind insbesondere die unter „Besondere Funktionen“ im AT 4.4 genannten Funktionen Risikocontrolling und Compliance zu nennen sowie darüber hinaus beispielsweise der Informationssicherheitsbeauftragte und der Datenschutz.

²⁹ So IIA/DIIR, Global Perspectives and Insights: Das Drei-Linien-Modell – ein wichtiges Instrument für den Erfolg jeder Organisation, S. 6.

Neben den oben genannten Funktionen können weitere Funktionen ebenfalls prozessunabhängige Überwachungs- und Kontrollhandlungen in den Instituten vornehmen oder auch Standards für das Institut setzen. Diese können der 1st und 2nd Line oder in manchen Instituten der „1,5 Line“ als Teil der 1st Line zugeordnet sein. In letzterer sind oftmals Funktionen beheimatet, die die 1st Line beispielsweise bei der Umsetzung der durch die 2nd Line definierten Kontrollstandards unterstützen sowie das Business Process & IKS Management und Key Control Testing durchführen. Diese Funktionen umfassen unter anderem folgende:

- Marktfolge.
- Finanzen und Controlling (ICOFR).
- Beschwerdemanagement.
- Vergütungsbeauftragter.
- Liquiditätsmanagementfunktion.
- Qualified Intermediary (QI) Responsible Officer.
- Strategischer Einkauf, Lieferantenmanagement.
- Zentrales Auslagerungsmanagement inkl. Auslagerungsbeauftragter.
- (Zentraler) Data Quality Manager.
- IT-Compliance.
- Neutrale Stelle (§ 81 Abs. 5 WpHG).
- Tax Compliance.
- Business Process & IKS Management.
- Organisationseinheit oder Governance Office.

Um einen konstruktiven und mehrwertstiftenden Austausch zwischen der Internen Revision und den Einheiten der zweiten Linie sicherzustellen, sollte ein regelmäßiger Austausch vereinbart werden. Dieser sollte unterjährig fortlaufend und anlassbezogen sowie im Rahmen des Prüfungsplanungsprozesses der Internen Revision erfolgen.

Dieser Austausch kann auf Basis eines Informationsprotokolls zwischen der Internen Revision und den Einheiten der zweiten Linie definiert werden aus dem hervorgeht: wer, wen, über was, wie häufig informiert. Eine weitere Option ist die Definition der Berichtspflichten der Bereiche gegenüber der Internen Revision in der Geschäftsordnung der Internen Revision. Die Interne Revision sollte die durch die Einheiten der zweiten Linie erstellten Berichte vollumfänglich und unverzüglich erhalten. Im Idealfall ist die Interne Revision als nicht stimmberechtigter Gast in den Gremien der Bank vertreten, erhält die Protokolle und Unterlagen aus Sitzungen der Geschäftsleitung und ist auf dem Verteiler

von Standardreports des Institutes sowie von Ad-hoc Meldungen zum Beispiel bei Datenschutz- und Informationssicherheitsvorfällen. Im Gegenzug sollte die Interne Revision über ihren Berichtsverteiler festlegen, welche Einheiten der zweiten Linie die Revisionsberichterstattung erhalten.

Empfehlenswert ist es festzulegen, dass die Interne Revision, sofern ihr zumindest ein begründeter Anfangsverdacht hinsichtlich einer potenziellen Gefährdung oder Benachteiligung von Instituts-/ Kunden-/ Anlegerinteressen oder vergleichbarer Fälle vorliegen, die in die Themenzuständigkeit einer Einheit der zweiten und auch der ersten Linie fallen, mit dieser in einen angemessenen Austausch eintritt. Umgekehrt sollten eindeutige Sachverhalte/ Fakten definiert werden, die zu einer ad-hoc-Informationspflicht der Einheiten der zweiten Linie an die Interne Revision führen.

Wie oben angeführt, fordert GIAS Standard 9.5 die Revisionsleitung dazu auf sich mit internen und externen Assurance Providern abzustimmen und zu erwägen, sich auf deren Arbeit zu verlassen. In diesem Rahmen sollten die Interne Revision und die Einheiten der zweiten Linie, insbesondere die Compliance- und Risikocontrolling-Funktionen, Informationen über die Jahresplanungen zu Kontrollhandlungen und Prüfungen sowie auch die Prüfungs-/ Kontrollergebnisse austauschen. Eine wichtige Quelle für Informationen ist die zentrale IKS-Stelle und die Ergebnisse des hier angesiedelten IKS Regelkreises.

Die genannten Funktionen verbleiben vollumfänglich Gegenstand der Prüfungstätigkeit der Internen Revision, gleichwohl ist es im Interesse des Instituts und auch der Aufsicht, dass die Prüfungshandlungen aufeinander abgestimmt werden. Dies bedeutet Lücken in der Abdeckung zu vermeiden, aber auch Prüfungen desselben Prüfungsobjekts durch beide Einheiten möglichst nicht im selben Prüfungszyklus vorzunehmen. Die Interne Revision kann die Kontrollergebnisse der Einheiten der zweiten Linie im Rahmen der Risikoorientierung der Prüfungsplanung/ -tätigkeit berücksichtigen.

17.4 Schnittstelle der Internen Revision zum Externen Prüfer

Die Schnittstellen zu externen Prüfern (Jahresabschlussprüfer und Aufsicht) sind im Gesamtinstitut zu definieren und festzulegen. Dabei sollten zumindest folgende Aspekte berücksichtigt und geregelt sein:

- Kommunikationswege und Ansprechpartner in dem Institut und auf Seiten der externen Prüfer.
- Informationsweitergabe (Was durch wen? Dokumentation der Unterlagen, Interviewdokumentation, Austausch telefonisch zulässig oder nur schriftlich, Fristen für Rückmeldungen, etc.).
- Wesentlichkeits-/Eskalationsstufen und eine Eskalationsschwelle, ab welcher die Geschäftsleitung eingeschaltet werden muss/ sollte.

- Abstimmungsprocedere von Feststellungen/ des Berichtes.
- Koordination/ Durchführung notwendiger Berichterstattung & Beantwortung von Anfragen.

Dies betrifft insbesondere die internen Ansprechpartner und die Zuständigkeiten für die Vorbereitung und Begleitung der Jahresabschlussprüfung. Für den Prozess der Jahresabschlussprüfung empfiehlt es sich einen kleinen und eng abgestimmten „Zirkel“ von Ansprechpartnern (je nach Themengebiet der Prüfung durch einen externen Prüfer auch auf Seiten der betroffenen Fachbereiche) festzulegen. Die Prüfungsvorbereitung und die Prüfungskoordination auf Seiten des Instituts kann dabei von der Internen Revision übernommen werden.

In Bezug auf die Schnittstelle zwischen der Internen Revision und externen Prüfern sollte eine eindeutige Zuständigkeit für den Informationsaustausch festgelegt werden. Die Interne Revision sollte einer der Ansprechpartner für die Jahresabschlussprüfer sein und diesen durch einen konstruktiven Austausch bei der Ausführung seines Prüfungsauftrags unterstützen. Die Interne Revision stellt dem Jahresabschlussprüfer ihre gesamte Berichterstattung sowie alle weiteren von ihm zu Prüfungszwecken angeforderten Revisionsunterlagen an geeigneter und vereinbarter Stelle zur Verfügung.

Darüber hinaus sollte standardisiert ein regelmäßiger Austausch zwischen der Internen Revision und dem Jahresabschlussprüfer stattfinden. Gegenstand der Gespräche können u. a. der Umsetzungsstand der Feststellungen aus der jeweils vorangegangenen Jahresabschlussprüfung, die aktuelle Risikosituation des Instituts sowie die Prüfungsaktivitäten und -ergebnisse der Internen Revision und des Abschlussprüfers sein.

Der Jahresabschlussprüfer kann in eigenem Ermessen auf Prüfungsergebnisse der Internen Revision zurückgreifen. Hierfür sind jedoch seitens der Internen Revision bestimmte formale Anforderungen einzuhalten. Den erwarteten Synergien ist daher der Aufwand entgegenzusetzen, der mit der Erfüllung dieser Anforderungen einhergeht. Für den Abschlussprüfer ist insbesondere IDW PS 321 (Interne Revision und Abschlussprüfung) relevant.

17.5 Interaktion der Internen Revision mit Aufsichtsinstitutionen

Es finden bei EZB-beaufsichtigten Instituten regelmäßig (institutsindividuell von monatlich bis jährlich) Gespräche über Revisionsthemen zwischen dem Joint Supervisory Team (JST) der EZB und dem Leiter der Internen Revision statt. Bei internationalen Häusern mit Auslandsniederlassungen ggf. auch mit ausländischen Aufsichtsbehörden wie z. B. der FED in den USA. Bei nicht-EZB-beaufsichtigten Instituten können regelmäßige Meetings mit den nationalen Aufsichtsbehörden, wie BaFin und/ oder Bundesbank, stattfinden.

Hier kann ein Informationsaustausch u. a. zu folgenden Themen stattfinden:

- Prüfungsaktivitäten der Internen Revision
- Personalausstattung der Internen Revision
- Diskussion über Risiken im Institut, die von beiden Parteien festgestellt wurden
- Verständnis der von dem Kreditinstitut eingesetzten Risikominderungstechniken
- Geplante/ implementierte wesentliche methodische Veränderungen im Revisionsprozess und
- Überwachung der Reaktion auf festgestellte Schwächen/ Feststellungen
- ggf. Konzernrevisionsthemen.

Sofern Prüfungsberichte der Internen Revision von einer Aufsichtsbehörde angefordert werden, so sollten diese durch die Leitung der Internen Revision bzw. einer von ihr beauftragten Stelle zur Verfügung gestellt werden. Bei global tätigen Instituten muss hierbei geprüft werden, ob die Berichte Inhalte enthalten, die nicht in den Zuständigkeitsbereich der Aufsicht fallen (Confidential Supervisory Information). Diese sind ggf. unkenntlich zu machen.

Es erfolgt ferner eine Information der Geschäftsleitung durch den Leiter der Internen Revision über Aufsichtstermine und Inhalt der Gespräche sowie (ggf.) ausgehändigte Prüfungsberichte. Dies kann z. B. in die regelmäßige Berichterstattung an die Geschäftsleitung integriert werden.

18 Nachhaltigkeit in der Revisionsfunktion

18.1 Einleitung und Herausforderung:

Neben dem technologischen Wandel in Form einer fortschreitenden Vernetzung und Digitalisierung wird der Klimawandel einen zunehmend wichtigeren Einfluss auf das Risikomanagement und damit auf die Zukunft von Instituten haben.

Der Klimawandel geht nicht nur mit Umweltrisiken in Form von Naturgefahren (physischen Risiken) und Transitionsrisiken, sondern auch mit veränderten Anforderungen von Gesellschaft, Kunden, Politik und Aufsicht an Unternehmen einher.

Die Frage, was Nachhaltigkeit generell und in der Revisionsfunktion ist, wird im öffentlichen Diskurs relativ weit gefasst und aktuell noch unscharf beantwortet.

Dieser Abschnitt beschreibt Ansätze zur Integration von Nachhaltigkeitsaspekten in die Ablauforganisation der Internen Revision. Hinsichtlich der Prüfung von Nachhaltigkeit im Rahmen der zu bearbeitenden Prüfobjekte wird auf den ESG-Prüfungsleitfaden des DIIR (siehe Quellenverzeichnis) verwiesen.

18.2 Bedeutung und Abgrenzung des Nachhaltigkeitsbegriffs im Revisionskontext

Nachhaltigkeit wird im Revisionskontext vielfältig verwendet. So findet dieser Begriff mit seinen gesellschaftlich anerkannten Bedeutungen auch Eingang und Verwendung in der revisorischen Fachsprache, z. B. als „nachhaltiges Prüfen“, „nachhaltige Dokumentation“, „nachhaltige Maßnahmen“, „nachhaltiger Erfolg“ der Revisionsfunktion.

Es empfiehlt sich eine klare Unterscheidung zwischen Nachhaltigkeit in der Revision (z. B. ressourcenschonendes Arbeiten) und nachhaltigkeitsbezogene Prüf- und Beratungsthemen, die in der Organisation wirken, sozusagen durch die Revision (z. B. Prüfungen von ESG-Risiken).

Die deutsche Bankenaufsicht definiert Nachhaltigkeit im Sinne des UN Sustainable Development Verständnisses synonym mit ESG-Risiken (Environmental, Social, Governance – ESG) und macht spätestens mit der 7. MaRisk-Novelle (29.06.2023) diese Risikofaktoren bzw. Risikotreiber zum Prüfungsobjekt bzw. -gegenstand für die Interne Revision. Mit dem Leitfaden zu Klima- und Umweltrisiken (November 2020) und den Leitlinien zum Management der Umwelt-, Sozial- und Governance-Risiken bzw. ESG-Risiken (Januar 2025) hat auch die EZB ihre Erwartungen konkretisiert.

Eine nachhaltige Revisionsfunktion verfolgt das Ziel, durch nachhaltige Prüfungsmethoden und -prozesse die Effizienz und Zukunftsfähigkeit der Organisation zu schützen und zu erhalten. In einer Phase der Etablierung von Good-Practices-Ansätzen lässt sich Nachhaltigkeit zusammenfassend wie folgt definieren: Nachhaltigkeit in der Revisionsfunktion bedeutet: eine effiziente Aufgabenerfüllung unter Berücksichtigung einer kurz-, mittel- und langfristigen Ressourcen- und Kapazitätsplanung, ausgerichtet an den Zielen und Strategien der Organisation.

18.3 Themenbereiche für die Beurteilung und Verbesserung der Nachhaltigkeit

Die Nachhaltigkeit der Internen Revisionsfunktion lässt sich anhand von vier Bereichen beurteilen:

18.3.1 Strategie, SfO und Prozesse

- Die bestehenden Rahmenbedingungen für die Tätigkeit der Internen Revision sollten hinsichtlich der Möglichkeiten, Nachhaltigkeitsaspekte zu integrieren, kritisch hinterfragt werden, um Chancen zu nutzen (bspw. im Hinblick auf Prozesse, Ressourcen und Kapazitäten) und sich ggf. neu zu positionieren (bspw. in der Strategie der Internen Revision oder der Prozesslandkarte).³⁰
- Eine wichtige Bezugsgröße ist das Interesse der Geschäftsleitung an der Beteiligung der Internen Revision bei strategischen Risiken, Zielen und Projekten. Die GIAS empfehlen der Revisionsleitung in Domain III, Prinzip 8.1 eine regelmäßige Kommunikation und Interaktion mit der Geschäftsleitung auch zu nichtfinanziellen Governance- und Risikomanagementthemen, wie Nachhaltigkeit.
- In Abhängigkeit von der Größe und Organisationsstruktur des Revisionsbereichs empfiehlt es sich, die Verantwortlichkeiten in Bezug auf Nachhaltigkeit in der Ablauforganisation bzw. Organisationsrichtlinien (z. B. Audit Charta) transparent und angemessen zu verankern.

18.3.2 Methoden und Werkzeuge (Tools)

Digitale Methoden und Werkzeuge wie elektronische Arbeitspapiere, Remote-Tools und Co-Working-Plattformen fördern ressourcenschonendes Arbeiten und können zur Nachhaltigkeit in der Revision einen wichtigen Beitrag leisten.

³⁰ In Anlehnung an IIA GLOBAL PERSPECTIVES AND INSIGHTS, Agilität und Innovation, 2018, dt. Übersetzung DIIR

Prozessautomatisierung kann ebenfalls zur Effizienzsteigerung beitragen. Die Nachhaltigkeitswirkung sollte allerdings regelmäßig bewertet werden.

Die Möglichkeit, Nachhaltigkeits-KPIs für die Interne Revision zu definieren (z. B. Anteil der Remote-Prüfungen zur Reduktion von Dienstreisen) sollte in Betracht gezogen werden.

18.3.3 Ressourcen und Know-how

Einen weiteren Ansatzpunkt bieten angemessene Informationen und Planungen des zukünftigen Personalbedarfs unter Berücksichtigung von Wirtschaftlichkeit (Stichwort: make or buy) und Nachhaltigkeit (kurze vs. lange Perspektive).

Entscheidend ist in diesem Zusammenhang, der frühzeitige Aufbau von ausreichenden und geeigneten personellen und sonstigen Ressourcen zur Bewältigung der neuen Herausforderungen im Umgang mit Nachhaltigkeitsrisiken.

Auch beim Thema Nachhaltigkeit ist eine starke Analysekompetenz in der Internen Revision erforderlich. Hier sollte der Fragestellung nachgegangen werden, bei welchen traditionellen Revisionsaktivitäten und in welchem Umfang können diese extern vergeben (Stichwort: Outsourcing) bzw. vollständig automatisiert werden.

In die Schulungsprogramme der Internen Revision sollten auch Bausteine zu Nachhaltigkeit und ESG-Risiken für Mitarbeiter und Führungskräfte aufgenommen werden.

Revisionsprojekte (z. B. im Bereich Digitalisierung) bieten eine geeignete Plattform, um Talente in IT- oder Betriebsfunktionen für die Arbeit in der Internen Revision zu gewinnen, um damit auch sekundär das Nachhaltigkeitspotential durch die Digitalisierung der Internen Revision zu heben.

18.3.4 Effektivität und Effizienz

Unter nachhaltigem bzw. effizientem Prüfen wird branchenüblich ressourcenschonendes Prüfen verstanden. Die Instrumente und Methoden, die der Internen Revision hierfür zur Verfügung stehen, sollten hinsichtlich des Ressourcenbedarfs und des Zwecks (Erzielung von Prüfnachweisen) bewertet und den Prüfenden bekannt gemacht werden.

Einen weiteren Beitrag kann auch eine enge Zusammenarbeit (auf Basis von geeigneten Schnittstellenvereinbarungen) und ein gemeinsames Verständnis der institutseigenen Risk-Taxonomie mit der zweiten Linie leisten.

Auch die Zusammenarbeit mit der ersten Linie spielt eine wichtige Rolle, um die Strategien und Geschäftsrisiken zur Erreichung ihrer Ziele ausreichend zu identifizieren.

Dasselbe gilt für die Abstimmung der Prüf- bzw. Kontrollpläne mit den anderen Linien unter Wahrung der eigenen Verantwortlichkeiten und zur Vermeidung von Doppelarbeiten im Interesse des Instituts.

18.4 Praktische Umsetzung und Integration in die Management- bzw. Steuerungsprozesse

Für die praktische Umsetzung von Nachhaltigkeit im Revisionskontext müssen konkrete Maßnahmen bei (Revisions-) Produkten, Prozessen sowie bei Räumlichkeiten und der Art der Tätigkeitserbringung entwickelt und umgesetzt werden. Dies kann bspw. in Form einer Analyse, der Identifizierung und Definition von Handlungsbedarfen und einer sich daran anschließenden Abarbeitung des vorher identifizierten Handlungsbedarfs erfolgen. Wünschenswert mit Blick auf die Effizienz ist, ein unternehmensweites und zielgerichtetes Vorgehen innerhalb der Organisation und zusammen mit der Internen Revision.

Beispielhaft könnten Klimaziele bei der Planung von Dienstreisen (u. a. Wahl der Transportmittel unter Berücksichtigung des CO₂ Verbrauchs oder der Ersatz bzw. die Kürzung von Vor-Ort Phasen durch Remote-Interviews) berücksichtigt werden. Soziale Nachhaltigkeitsziele sollten beim Personalmanagement angemessen berücksichtigt werden. Governance Aspekte sollten bei Strategie, Zielsetzung und der Definition von Verantwortlichkeiten nachhaltig ausgestaltet werden.

Quellenverzeichnis:

The Institute of Internal Auditors (IIA): GLOBAL PERSPECTIVES AND INSIGHTS, Agilität und Innovation, 2018, dt. Übersetzung DIIR, Link: https://www.diir.de/fileadmin/fachwissen/downloads/GPAI_Agilit%C3%A4t_und_Innovation.pdf

DIIR e.V.: ESG-Prüfungsleitfaden, Beurteilung des Managements von ESG-Risiken in Kredit- und Finanzdienstleistungsinstituten, Version 2.0, 07.05.2025, Link: <https://www.diir.de/content/uploads/2025/05/2025-DIIR-ESG-Leitfaden-Kreditinstitute-v2.pdf>

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Merkblatt zum Umgang mit Nachhaltigkeitsrisiken, 13.01.2020, Link: https://www.bafin.de/SharedDocs/Downloads/DE/Merkblatt/dl_mb_Nachhaltigkeitsrisiken.pdf?__blob=publicationFile&v=9

Europäische Zentralbank (EZB): Leitfaden zu Klima- und Umweltrisiken, November 2020, Link: <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011final-guideonclimate-relatedandenvironmentalrisks~58213f6564.de.pdf>

Europäische Zentralbank (EZB): Leitlinien zum Management der Umwelt-, Sozial- und Governance-Risiken (ESG-Risiken), 08.01.2025, Link: https://www.eba.europa.eu/sites/default/files/2025-04/fb22982a-d69d-42cc-9d62-1023497ad58a/Guidelines%20on%20the%20management%20of%20ESG%20risks%20%28EBA%20GL%202025%2001%29_DE_COR.pdf

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Sustainable-Finance-Strategie der BaFin, 05.07.2023, Link: https://www.bafin.de/DE/DieBaFin/Sustainable_Finance_Strategie/SF_Strategie_node.html

IV. Autoren

Das Revisionshandbuch wurde von den Mitgliedern des Arbeitskreises MaRisk verfasst. Der Arbeitskreis übernimmt die Weiterentwicklung und die Anpassung der Abschnitte auf aktuelle Entwicklungen. Dabei fließen die praktischen Erfahrungen und Prozesse aus den Instituten der Arbeitskreismitglieder mit ein.

Zum Redaktionsschluss setzt sich der Arbeitskreis MaRisk aus folgenden Mitgliedern zusammen:

Name	Unternehmen
Prof. Ulrich Bantleon	Hochschule Offenburg
Peter Duscha	Deutsche Leasing Finance GmbH
Anja Engel	ING-DiBa AG
Jens-Peter Falke	Kreditanstalt für Wiederaufbau
Konrad Fischer	TARGOBANK AG
Bernd Hombach	DZ BANK AG
Ulrich Hurmer	BMW Group
Dr. André Klengel	Helaba
Horst Ulrich Kremer	Stadtsparkasse Düsseldorf
Oliver Martens	Hamburg Commercial Bank AG
Thomas Maurer	Münchner Bank eG
Jan Meyer im Hagen	S Auslagerungsmanagement GmbH
Thomas Millitzer	DekaBank
Rudolf Moschitz	Aareal Bank AG
Sabine Nakath	Deutsche Apotheker- und Ärztebank eG
Insa Redenius	Oldenburgische Landesbank AG
Carsten Rilinger (Gast)	Landesbank Baden-Württemberg
Jürgen Rohrmann	Union Investment
Ines Schröder	Bayerische Landesbank
Michael Seifert	Bausparkasse Schwäbisch-Hall AG
Marion Stadter	UniCredit
Sandra Strelow	dwpbank

Monika Wiffel	NRW.BANK
Steve Wilkens	Commerzbank AG

Wir bedanken uns bei Jan Meyer im Hagen für die Koordination und Redaktion der Überarbeitung.

An früheren Fassungen haben mitgewirkt:

Jochen Bender
Hubert Breuer
Christopher Ecks
Gert Eßer
Gabriele Fischer
Jürgen Jung
Michael Helfer
Patricia Kordesch
Lutz Kranzbühler
Thomas Ramke
Anna Reich
Günter Ruck
Jan T. Saul
Holger Scharmann
Thorsten Schmidt
Steffen Schöffler
Arne Schreiber
Sabine Schrödl
Manuela Straube
Oliver Terhorst
Holger Wagner