Online-Revisionshandbuch

für die Interne Revision
in Kreditinstituten

vom DIIR Arbeitskreis MaRisk

Stand Dezember 2021

DIIR Deutsches Institut für Interne Revision e.V.

I. Vorwort

Der Arbeitskreis MaRisk hat ein Online-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 Internationalen Standards für die berufliche Praxis der Internen Revision des DIIR (IPPF) basieren. Diese wurden mit dem Ziel verglichen und bearbeitet, alle Themen der Revisionsorganisation in möglichst breit anwendbarer Form darzustellen. Das Handbuch soll dabei auch Anregungen für die Neufassung oder Weiterentwicklung der in Kreditinstituten vorhandenen Revisionshandbücher geben.

In der letzten Zeit werden im Rahmen von Prüfungen nach § 44 Abs. 1 KWG zum Teil Feststellungen getroffen, die über die in diesem Handbuch niedergelegte Praxis hinausgehen und sich auch so nicht unmittelbar aus den MaRisk ableiten lassen. Soweit die individuelle Risikosituation des Instituts nicht weitergehende Maßnahmen erfordert (Proportionalität) hält der Arbeitskreis MaRisk die hier beschriebenen Vorgehensweisen für hinreichend im Sinne der MaRisk.

Der Anspruch, eine jederzeitige Aktualität mit Blick auf veränderte oder weiterentwickelte Rahmenbedingungen zu gewährleisten, wird jedoch nicht erhoben. Das gesamte Online-Revisionshandbuch wurde zuletzt im Dezember 2021, unter Berücksichtigung der MaRisk-Novelle 2021 und des Finanzmarktintegritätsstärkungsgesetzes (FISG), aktualisiert.

Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Anmerkungen oder Anregungen für Ergänzungen und Weiterentwicklungen können gerne an die Arbeitskreisleitung Jürgen Rohrmann und Bernd Hombach gesandt werden.

II. Inhaltsverzeichnis

I. Vorwort 2

II. Inhaltsverzeichnis 3

III. Abbildungsverzeichnis 4

1 Ziele, Aufgaben und Strukturen der Internen Revision 6

2 Grundprinzipien der Revision 19

3 Externe Rahmenbedingungen 32

4 Standardrevisionsprozess 42

5 Continuous Auditing / Continuous-Risk Assessment 79

6 Prüfung von Auslagerungen 90

7 Begleitung wesentlicher Projekte / Anpassungsprozesse 101

8 Interne Revision im Rahmen von agilen Strukturen (inkl. agile Prüfungsmethodik) 106

9 Digitalisierung der Prüfungsprozesse (inkl. Durchführung von Remoteprüfungen) 113

10 Gewinnung (Recruitment) und Weiterentwicklung von Revisionsmitarbeitern inkl. Beachtung der Fit & Proper-Anforderungen für die Revisionsleitung 122

11 Qualitätssicherung und -verbesserung in der Internen Revision 134

12 Konzernrevision 143

13 Sonderprüfungen zur Aufklärung von Fraud 155

14 Leistungsmessung in der Internen Revision anhand von KPIs 166

15 Schnittstelle mit Aufsichtsbehörden, externen Prüfern und der Zweiten Verteidigungslinie 178

IV. Autoren 186

III. Abbildungsverzeichnis

Abb. 1: Der Wert der Internen Revision 24

Abb. 2: COSO-Internal Control 2013 38

Abb. 3: COSO-Enterprise Risk Management (2004) 39

Abb. 4: COSO: Implications from the strategy 40

Abb. 5: COSO: Enterprise Risk Management (Framework 2017) 40

Abb. 6: Berufsrechtliche Normen der Internen Revision (IPPF) 41

Abb. 7: Prüfungsziele 53

Abb. 8: Berichtspflichten der Internen Revision und rechtliche Grundlagen 73

Abb. 9: Bestandteile der Berichterstattung an Geschäftsleitung und Aufsichtsorgan gemäß § 25c KWG in Verbindung mit BT 2.4 Tz 4 MaRisk 75

Abb. 10: Weitere mögliche Berichtsinhalte für die Quartalsberichterstattung 76

Abb. 11: Bestandteile des Continuous Auditings 81

Abb. 12: Zusammenspiel von Prüfuniversum, CA und Jahresprüfplan 88

Abb. 13: Notwendigkeit eigener Prüfungshandlungen 92

Abb. 14: Traditional vs. Agile Internal Audit 109

Abb. 15: Übersicht über die Prüfungsarten aus Konzernsicht 147

Abb. 16: Informationsflüsse zwischen den Internen Revisionen der Tochtergesellschaften und der Konzernrevision 151

Abb. 17: Mögliche Rollen der Internen Revision der Muttergesellschaft und deren Auswirkung auf die Berichterstattung 153

Abb. 18: KPIs zum Revisionsprozess 174

Abb. 19: KPIs zur Mitarbeiterperspektive 175

Abb. 20: KPIs zur Finanzperspektive 176

Abb. 21: KPIs zur Stakeholder-Perspektive 177

Abb. 22: Modell der Drei Verteidigungslinien 179

Abb. 23: Das IIA - Drei Linien-Modell 182

1 Ziele, Aufgaben und Strukturen der Internen Revision

1.1 Ziele und Aufgabenstellung 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 ergeben sich grundsätzlich aus dem Selbstverständnis der Internen Revision und der Erwartungshaltung der Stakeholder. Diese werden sich regelmäßig an der Definition des IIA/DIIR orientieren.

Definition Interne Revision des IIA/DIIR

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

Ziel der Internen Revision ist damit primär die Schaffung von Mehrwerten für die gesamte Organisation. Dies darf allerdings nicht zu einem undifferenzierten Mehrwertversprechen führen (= Erwartungslücke), sondern ist zu konkretisieren und mit der Geschäftsleitung und dem Aufsichtsorgan abzustimmen.

Das International Professional Practice Framework (IPPF) enthält hierzu die folgende Mission für die Interne Revision: “Den Wert einer Organisation durch risikoorientierte und objektive Prüfung, Beratung und Einblicke zu erhöhen und zu schützen.”

Die Aufnahme einer Mission in die Geschäftsordnung der Internen Revision ist zu prüfen.

Die Mission wird im IPPF durch folgende Prinzipien ergänzt:

Die Interne Revision

- zeigt Integrität,
- zeigt Sachkunde und berufsübliche Sorgfalt,
- ist objektiv und frei von ungebührlichem Einfluss (unabhängig),
- richtet sich an Strategien, Zielen und Risiken der Organisation aus,
- ist geeignet positioniert und mit angemessenen Mitteln ausgestattet,
- zeigt Qualität und kontinuierliche Verbesserung,

- kommuniziert wirksam,
- erbringt risikoorientierte Prüfungsleistungen,
- ist aufschlussreich, proaktiv und zukunftsorientiert,
- fördert organisatorische Verbesserungen.

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.

Wenn Interne Revisoren die IPPF Standards gemeinsam mit Standards anderer Regelungsinstanzen (hier: MaRisk) nutzen, können sie gegenüber Dritten zusätzlich auf die Anwendung dieser Standards hinweisen, soweit dies sachgerecht ist. Sollten Unterschiede zwischen den IPPF Standards und den anderen Standards (hier: MaRisk) bestehen, sind diese zu ermitteln. In diesem Fall hat sich die Interne Revision sich an die jeweils restriktiveren Standards halten.

Die Ziele und die Aufgaben der Internen Revision werden in ihrer Geschäftsordnung (Charter oder Rahmenbedingungen der Internen Revision) operationalisiert und konkretisiert und bestimmen den von der Geschäftsleitung gesetzten Rahmen für das Tätigkeitsfeld der Internen Revision. Es empfiehlt sich, hierbei auch das Aufsichtsorgan zu einzubeziehen.

Die Interne Revision wird sich hinsichtlich ihres Tätigkeitsspektrums als auch hinsichtlich ihrer Qualitätsanforderungen an den Erwartungshaltungen ihrer Stakeholder ausrichten.

- Berufsständig ist dies im Rahmen der Überarbeitung des IPPF Standards 2010 durch die Einfügung von „2010.A2 – Der Leiter der Internen Revision muss feststellen und berücksichtigen, welche Erwartungen bezüglich der Beurteilungen und Schlussfolgerungen der Internen Revision bei leitenden Führungskräften, der Geschäftsleitung bzw. dem Überwachungsorgan und anderen Interessengruppen bestehen.“ umgesetzt worden.

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

- Insgesamt ist gemäß IPPF Standard 1000.A1 die Art der zu erbringenden Prüfungsleistungen in der Geschäftsordnung der Internen Revision festzulegen. Wenn Prüfungsleistungen für Dritte erbracht werden, müssen diese ebenfalls in der Geschäftsordnung der Internen Revision definiert werden Dies gilt gemäß IPPF Standard 1000.C1 ebenso für Beratungsleistungen.

Im Rahmen der Kapazitätsplanung sind ausreichend Ressourcen für Sonderprüfungen einzuplanen.

- BT 2.3 Tz.4 MaRisk
  Es muss sichergestellt sein, dass kurzfristig notwendige Sonderprüfungen, z. B. anlässlich deutlich gewordener Mängel oder bestimmter Informationsbedürfnisse, jederzeit durchgeführt werden können.

In der Praxis haben sich hier Ansätze von 10 bis 15 Prozent der Mitarbeiterkapazität als geeignet erwiesen. Der gewählte Ansatz ist regelmäßig zu überprüfen.

Die Folgen einer etwaigen Ressourcenbeschränkung hat der Leiter der Internen Revision an die Geschäftsleitung und das Aufsichtsorgan zu kommunizieren.

- IPPF Standard 2020: Berichterstattung und Genehmigung
  Der Leiter der Internen Revision muss der Geschäftsleitung bzw. dem Überwachungsorgan die Planung der Internen Revision, den Bedarf an Personal und Sachmitteln sowie zwischenzeitliche wesentliche Änderungen zur Kenntnisnahme und Genehmigung berichten. Außerdem muss der Leiter der Internen Revision die Folgen etwaiger Ressourcenbeschränkungen erläutern.

Die periodenbezogene Konkretisierung ihrer Aufgabenstellung erfährt die Interne Revision durch die Genehmigung ihres Prüfungsplans durch die Geschäftsleitung (BT 2.3 Tz. 5 MaRisk). Ergänzend sollte das Aufsichtsorgan über den genehmigten Prüfungsplan in Kenntnis gesetzt werden (IPPF Standard 2020). Aufgrund der Besonderheiten der deutschen Unternehmensverfassung, in der das Aufsichtsorgan im Kern eine Überwachungsfunktion wahrnimmt, kann der betreffende IPPF Standard, der eigentlich zusätzlich zur Kenntnisnahme eine Genehmigung vorsieht, nicht vollständig angewendet werden.

- BT 2.3 Tz. 1 MaRisk
  Die Tätigkeit der Internen Revision muss 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 vom dreijährigen Turnus abgewichen werden. 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 den Vorstand 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 IPPF das Risikomanagement und das interne Kontrollsystem.

- AT 4.4.3 Tz. 3 MaRisk
  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.

Daneben sind auch die IT-Prozesse von besonderer Bedeutung.

- IPPF Standard 2110.A2
  Die Interne Revision muss beurteilen, ob die IT-Führung und -Überwachung der Organisation die Strategien und Ziele der Organisation fördert.

Aus den Erläuterungen der IPPF Standards 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 zu erkennen. Hieraus leiten sich auch die klassischen Tätigkeitsfelder einer Internen Revision Financial Auditing, Compliance Auditing und Operational Auditing ab. Fraud-bezogene Prüfungshandlungen sind hierbei als Spezialfall des Compliance Auditing bzw. des Operational Auditing einzuordnen.

- IPPF Standard 2120.A2
  Die Interne Revision muss die Möglichkeit des Auftretens doloser Handlungen und die Vorgehensweise der Organisation bei der Steuerung des Risikos doloser Handlungen beurteilen.

- IPPF Standard 2210.A2
  Interne Revisoren müssen bei der Festlegung der Prüfungsziele die Wahrscheinlichkeit, dass wesentliche Fehler, dolose Handlungen, Regelverstöße sowie sonstige

Risikopotenziale vorliegen und Vorschriften nicht eingehalten werden, berücksichtigen.

Aus der Anforderung der Unabhängigkeit folgt, dass die in der Internen Revision beschäftigten Mitarbeiter grundsätzlich nicht mit revisionsfremden Aufgaben betraut werden dürfen. Sie dürfen insbesondere keine Aufgaben wahrnehmen, die mit der Prüfungstätigkeit nicht im Einklang stehen (BT 2.2. Tz. 2 MaRisk).

Sollte die Interne Revision ausnahmsweise operative Tätigkeiten und/oder operative Verantwortungen übernehmen, dann müssen auch diese Tätigkeiten unabhängig überprüft werden. Beim Wechsel von Mitarbeitern anderer Organisationseinheiten zur Internen Revision sind angemessene Übergangsfristen von in der Regel mindestens einem Jahr vorzusehen, innerhalb derer diese Mitarbeiter keine Tätigkeiten prüfen dürfen, die gegen das Verbot der Selbstprüfung und -überprüfung verstoßen (BT 2.2. Tz. 3 MaRisk, „Cooling-Off“, vgl. auch IPPF Standard 1130.A1). Unter Berücksichtigung des Proportionalitätsprinzips sind Erleichterungen aber möglich (BT 2.2 Tz. 3 MaRisk).

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 sinnvoll sein.

Konkretisierungen zu einzelnen Prüfobjekten ergeben sich aus dem IPPF (z. B. Implementierungsleitlinie 2120 zur Beurteilung des Risikomanagements, Implementierungsleitlinie 2130 zur Beurteilung von Kontrollen) als auch den DIIR Revisionsstandards (z. B. Nr. 2 „Prüfung des Risikomanagements durch die Interne Revision“, Nr. 4 „Prüfung von Projekten“ und Nr. 5 „Prüfung des Anti-Fraud-Management-Systems“). Seit Dezember 2017 veröffentlicht das IIA auch finanzinstitutsbezogene Praxisleitfäden, zuletzt „Foundations of Internal Auditing in Financial Services Firms“ (August 2019). Diese berufsständischen Veröffentlichungen sollten auf ihren Nutzen für die Revisionstätigkeit im jeweiligen Institut beurteilt werden.

Bei Kreditinstituten ergeben sich Prüfobjekte auch direkt aus dem Aufsichtsrecht; z. B. aus der CRR.

Artikel 191 CRR: Die Interne Revision oder eine andere vergleichbare unabhängige Revisionsstelle prüft mindestens einmal jährlich die Ratingsysteme des Instituts und deren Funktionsweise, einschließlich der Tätigkeit der Kreditabteilung sowie der PD-, LGD-, EL- und Umrechnungsfaktor-Schätzungen. Überprüft wird die Einhaltung aller geltenden Anforderungen.“

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.

Die sich aus dem Aufsichtsrecht ergebenden Pflichtprüfungen sind gesondert zu erfassen.

Weitere Tätigkeitsfelder können sich aufgrund von Verbandsempfehlungen oder durch Vorgaben der jeweiligen Sicherungseinrichtungen ergeben. Teilweise können sich auch aus Versicherungsbedingungen, insbesondere bei Vertrauensschadensversicherungen, Prüfobjekte für die Interne Revision 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 (siehe IIA/DIIR-Definition) als auch den MaRisk die Überwachung der fristgerechten Beseitigung von Mängeln (Follow-Up).

- BT 2.5 Tz. 1 MaRisk:
  Die Interne Revision hat die fristgerechte Beseitigung der bei der Prüfung festgestellten Mängel in geeigneter Form zu überwachen. Gegebenenfalls ist hierzu eine Nachschauprüfung anzusetzen.

Sofern keine Nachschauprüfung angesetzt wird, sollte die Behebung von Mängeln zeitnah individuell validiert werden. Je nach Schweregrad der Feststellungen, kann die Intensität der Validierung angepasst werden, z. B. Plausibilisierung für geringere Mängel, substanzielle Prüfungshandlungen für schwerwiegende Mängel (vgl. Abschnitt 4.6).

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

- IPPF Standard 1000.C1
  Die Art der zu erbringenden Beratungsleistungen muss in der Geschäftsordnung der Internen Revision festgelegt werden.

Aufsichtsrechtlich besteht folgende Regelung:

- BT 2.2 Tz. 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.

Für Kreditinstitute ergeben sich aus den MaRisk weitere Aufgabenstellungen. Im Falle wesentlicher Projekte ist eine Projektbegleitung notwendig.

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

Dies muss nicht zwingend in Form einer Prüfungstätigkeit und nicht zwingend kontinuierlich erfolgen. Das konkrete Vorgehen wird sich an Wesentlichkeitsüberlegungen ausrichten.

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
  Der Inhalt der Geschäftsstrategie liegt allein in der Verantwortung der Geschäftsleitung und ist nicht Gegenstand von Prüfungshandlungen durch Jahresabschlussprüfer oder die Interne Revision. Bei der Überprüfung der Risikostrategie ist die Geschäftsstrategie heranzuziehen, um die Konsistenz zwischen beiden Strategien nachvollziehen zu können. Gegenstand der Prüfung ist außerdem der Strategieprozess nach AT 4.2 Tz. 5.
- AT 8.1 Tz. 5 MaRisk: Neu-Produkt-Prozess
  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 8.2 Tz. 1 MaRisk: Änderungen betrieblicher Prozesse oder Strukturen
  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. In diese Analysen 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 9 Tz. 2 MaRisk: Auslagerung
  Das Institut muss anhand einer Risikoanalyse bewerten, welche Risiken mit einer Auslagerung verbunden sind. Ausgehend von dieser Risikoanalyse ist eigenverantwortlich festzulegen, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). … Im Rahmen ihrer Aufgaben ist auch die Interne Revision zu beteiligen.

Als weitere Aufgabenstellung ergibt sich aus den MaRisk eine eigenständige Qualitätsmanagementaufgabe für die Interne Revision bezogen auf die Revisionsprozesse.

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

- IPPF Standard 1300: Programm zur Qualitätssicherung und -verbesserung
  Der Leiter der Internen Revision muss ein Programm zur Qualitätssicherung und -verbesserung das alle Aufgabengebiete der Internen Revision umfasst, entwickeln und pflegen.

Hinsichtlich der Anforderungen an die Qualitätssicherung und -verbesserung sollte auf die konkreten Anforderungen der IPPF Standards abgestellt werden. Die ergänzende Implementierungsleitlinie 2000 „Leitung der Internen Revision“ empfiehlt u. a. die Entwicklung einer Metrik für die Bewertung von Effizienz und Wirksamkeit der Internen Revision, der Einholung von Feedbacks nach Durchführung der Prüfungen sowie einen Vergleich mit anderen Internen Revisionen der Branche (Benchmarking). Turnusmäßig sollte eine Selbstbeurteilung auf Basis des DIIR-QA-Leitfadens erfolgen.

Nach IPPF Standard 1310 (Anforderungen an das Qualitätssicherungs- und -verbesserungsprogramm) hat das Programm zum Qualitätsmanagement sowohl interne als auch externe Beurteilungen zu umfassen. Der Leiter der Internen Revision muss die Ergebnisse des Qualitätssicherungs- und Verbesserungsprogramms an die Geschäftsleitung und das Überwachungsorgan berichten. Hinsichtlich des mindestens alle fünf Jahre durchzuführenden externen Quality Assessments gemäß IPPF Standard 1312 ist zu entscheiden, ob eine vollständige externe Beurteilung oder eine Selbstbeurteilung mit unabhängiger Bestätigung durchgeführt wird. Der Leiter 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 der 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 Mitarbeiter 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:

- AT 4.4.3 Tz. 2 MaRisk
  … Unbeschadet dessen ist sicherzustellen, dass der Vorsitzende des Aufsichtsorgans unter Einbeziehung der Geschäftsleitung direkt bei dem Leiter der Internen Revision Auskünfte einholen kann.

- § 25d Abs. 9 S. 3 KWG
  Der Vorsitzende des Prüfungsausschusses oder, falls ein Prüfungsausschuss nicht eingerichtet wurde, der Vorsitzende des Verwaltungs- oder Aufsichtsorgans, kann unmittelbar beim Leiter der Internen Revision und beim Leiter des Risikocontrollings Auskünfte einholen. Die Geschäftsleitung muss hierüber unterrichtet werden.

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

Veränderungen in der Position des Leiters der Internen Revision sind vom Aufsichtsorgan in seiner Überwachung besonders zu berücksichtigen.

- AT 4.4.3 Tz. 6 MaRisk
  Wechselt die Leitung der Internen Revision, ist das Aufsichtsorgan rechtzeitig vorab unter Angabe der Gründe für den Wechsel zu informieren.

Hintergrund ist, dass das Aufsichtsorgan die Möglichkeit haben soll, mit dem Leiter 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.

1.2 Struktur und Berichtslinien

1.2.1 Struktur der Revision

Die Gestaltung der Aufbauorganisation der Internen Revision ist eine der wesentlichen Aufgaben in Verantwortung des Leiters 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.

1.2.2 Zentrale/dezentrale Organisation

Bei einem Unternehmen, 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 die 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 Revisionseinheiten innerhalb eines Konzerns enthält der Abschnitt 8.

1.2.3 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, Charter, o. ä.) zu regeln (vgl. Abschnitt 1). Hinsichtlich der verschiedenen Berichtspflichten und -inhalte aus dem IPPF liefert die Implementierungsleitlinie 2060 „Berichterstattung an leitende Führungskräfte und Geschäftsleitung bzw. Überwachungsorgan“ 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 landesspezifischen 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 Verwaltungsorgan berichtet.

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.

1.3 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 IPPF Standards und praktischen Ratschlägen 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, Verantwortlichkeiten, 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 der IPPF Standard 1000 (Aufgabenstellung, Befugnisse und Verantwortung) mit den Anforderungen an eine Geschäftsordnung der Internen Revision (siehe auch Implementierungsleitlinie 1000 und die ergänzende Leitlinie „Muster-Geschäftsordnung der Internen Revision (März 2017)“) sowie der IPPF Standard 2040 (Richtlinien und Verfahren) mit der dazugehörigen Implementierungsleitlinie 2040 zu nennen. Auch wenn mit der Implementierungsleitlinie 2040 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 (Qualitätsmanagement in der Internen Revision) in Verbindung mit dem Leitfaden zum Quality Assessment (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. Die Geschäftsordnung muss

- die Stellung der Internen Revision innerhalb des Unternehmens festlegen,
- den Zugang zu den Aufzeichnungen, zur Belegschaft und zu den Vermögensgegenständen sichern, die für die Erfüllung von Prüfungs- und Beratungsaufträgen relevant sind und
- den Umfang der Tätigkeiten der Internen Revision festlegen.

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 Mitarbeiter der Internen Revision).

Der QA-Leitfaden des DIIR stellt weitergehende Anforderungen an ein Revisionshandbuch:

8. Die Interne Revision verfügt über ein Revisionshandbuch mit folgenden wesentlichen Inhalten: Regelungen und/oder Methoden zur Prüfungsplanung, -vorbereitung, -durchführung, -nachbereitung, Berichterstattung, Dokumentation, Zugriff auf und Archivierung von Prüfungsergebnissen.

9. Das Revisionshandbuch ist den Mitarbeitern bekannt und wird regelmäßig auf Aktualität und Angemessenheit überprüft. Die Einhaltung wird laufend überwacht.

Ein Revisionshandbuch sollte allen Mitarbeitern 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.

Das Online-Revisionshandbuch des DIIR ist ein konkretes Beispiel für die Darstellung der Internen Revision im Rahmen der schriftlich fixierten Ordnung einer Organisation. 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 Revisionsmitarbeiter zu erstellen.

2 Grundprinzipien der Revision

2.1 Organisatorische Unabhängigkeit der Internen Revision

Die organisatorische Unabhängigkeit der Internen Revision ist wesentliches Merkmal jeglicher Revisionstätigkeit (vgl. IPPF Standard 1100 „Unabhängigkeit und Objektivität“). Der Leiter 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 der Leiter der Internen Revision funktional an die Geschäftsleitung bzw. das Überwachungsorgan und hat direkten und unbeschränkten Zugang zu diesen. Der Leiter der Internen Revision bestätigt der Geschäftsleitung bzw. dem Überwachungsorgan mindestens jährlich die organisatorische Unabhängigkeit.

Im Fall des Verlustes der Unabhängigkeit kann das Arbeitsergebnis nicht der Revisionstätigkeit zugeordnet werden, d. h. 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 Internen Revision an sich 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 qualitativer Abstufung: Gesamtvorstand, Vorstandsvorsitzender, nur bei objektiver Unmöglichkeit ein anderes Vorstandsmitglied.

Die Prüfung der Angemessenheit des Risikomanagements und der Geschäftsorganisation umfasst nach § 11 Absatz 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.

Ein Quality Assessment, welches basierend auf dem Leitfaden zur Durchführung eines Quality Assessment des DIIR – Deutsches Institut für Interne Revision e.V. durchgeführt wird, bewertet den Verlust der Unabhängigkeit als zu erfüllenden Mindeststandard im Sinne eines „K.O.-Kriteriums“, d. h. Versagung eines positiven Gesamtergebnisses.

Weitere Hilfestellung sind bei konkreten Anwendungsproblemen ersichtlich in: „Internationale Standards für die berufliche Praxis der Internen Revision 2017“ (Stand 11. März 2019, Version 7) des DIIR/IIA zu finden.

2.2 Prozessunabhängigkeit der Internen Revision

Die Unabhängigkeit der Internen Revision von den Prozessen des Instituts ist neben der organisatorischen Unabhängigkeit eine weitere elementare Anforderung. 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 IPPF Standard 1100 „Unabhängigkeit und Objektivität“ kann die Objektivität als beeinträchtigt angenommen werden, wenn der Leiter der Internen Revision die Verantwortung für die geprüfte Organisationseinheit trägt oder wenn bestimmte Beratungsleistungen durch die Interne Revision im geprüften Bereich erbracht wurden (vgl. Kap. 2.6). Bedrohungen der Unabhängigkeit sind auf Prüfer-, Prüfungs-, Funktions- und Organisationsebene zu steuern (vgl. IPPF Standard 1100).

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.

2.3 Persönliche Unabhängigkeit und Objektivität der Revisionsmitarbeiter

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 Mitarbeiter 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. Gem. IPPF Standard 1130.A1 „Beeinträchtigung von Unabhängigkeit oder Objektivität“ 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.

Gründe für Beeinträchtigungen der individuellen Unabhängigkeit und der persönlichen Objektivität können aber auch aus der geschützten Privatsphäre (z. B. Partner, Freunde) der Mitarbeiter resultieren. Da Fragen an Mitarbeiter hierzu nicht statthaft sind, sollte auch die Möglichkeit bestehen, dass der Prüfer die Beeinträchtigung seiner Unabhängigkeit ohne Angabe von Gründen erklären kann. Verantwortlich für seine Objektivität und die individuelle Unabhängigkeit ist jeder Mitarbeiter selbst (vgl. Ethikkodex/IPPF Standard 1120).

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 Mitarbeiter zu Beeinträchtigungen der individuellen Unabhängigkeit und Objektivität (ohne Verpflichtung zur Benennung von Gründen)
- Zusicherung der Vertraulichkeit freiwillig gegebener Informationen durch den Revisionsleiter
- Anlassbezogene Verpflichtung der Mitarbeiter bei besonders sensiblen Prüfungssachverhalten

Unabhängig von diesen Regularien muss der Mitarbeiter allerdings immer eine entsprechende Unabhängigkeit als Charaktereigenschaft mitbringen. Insofern kommt diesem Thema auch bei der Rekrutierung von Mitarbeitern eine besondere Bedeutung zu.

2.4 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 Zweifel an der Notwendigkeit von angeforderten sensiblen Informationen durch die verantwortlichen Bereiche, muss der Revisionsleiter verantwortlich über deren Nutzung im Unternehmensinteresse entscheiden. 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 13).

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. Kap. 2.5). Die zur Erreichung der Prüfungsziele notwendige Informationsverwertung ist grundsätzlich zulässig. Dies sollte durch eine wirksame Ableitung von Prüfungszielen und -handlungen dokumentiert werden.

2.5 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. 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 Mitarbeitern 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 vom Revisionsleiter 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 vom Revisionsleiter angemessen überwacht und bei Verstößen sanktioniert werden.

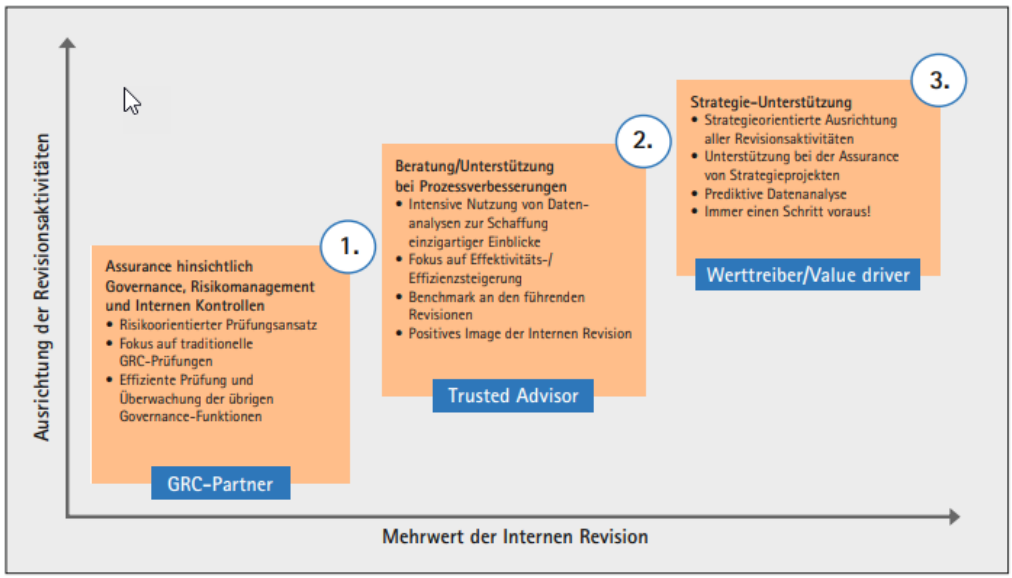
2.6 Beratung und Projektbegleitung

2.6.1 Veränderungen und Herausforderungen der Revisionstätigkeit

Das Risiko- und Chancenmanagement von Unternehmen und insbesondere 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 der Organisation. Damit einhergehend ist eine zunehmende Nachfrage nach Beratungsleistungen der Internen Revision verbunden. Der Internen Revision kommt dabei das Alleinstellungsmerkmal zu, eine 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 Interne 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. 1: Der Wert der Internen Revision[1]



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

Die Interne Revision als ein „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, insbesondere bei Anpassungsprozessen gemäß AT 8 MaRisk einbringen. Durch die frühzeitige Identifikation von Risiken, Mängeln und Verbesserungspotenzialen werden

[1] Eulerich / Lenz ZIR, 04/2000

- 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 und
- das Revisions-Know-how durch kontinuierliche Lerneffekte aufgebaut.

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.

2.6.2 Anforderungen

Die strategische Ausrichtung der Internen Revision in Richtung präventiver und risikoorientierter Beratungsleistungen ist in der Definition des IIA bzw. DIIR berücksichtigt:

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

Die 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; vgl. Abschnitt 8).
- 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 in der Praxis konkret ausgestaltet?
- Ist eine beratende Funktion der Internen Revision von der Geschäftsleitung gewollt?
- Wie werden diese Aufgaben definiert, geplant und organisiert?
- Welchen Rahmenbedingungen und Grundsätze sind zu beachten (z. B. Wahrung der Unabhängigkeit, Vermeidung von Interessenskonflikten)?

2.6.3 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. Ziel ist es, optimale Lösungen zur Wertschöpfung und zur Verbesserung der Geschäftsprozesse vorzuschlagen. 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 verbleibt ausschließlich beim Kunden. Es erfolgt kein Follow-up durch die Interne Revision.

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.

2.6.4 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.). Als Grundlage können die IPPF Standards des IIA (C/Consulting) herangezogen werden. Folgende Grundsätze sind in der Beratungspraxis insbesondere zu beachten – 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.

Bei komplexen Beratungsaufträgen, deren Ergebnis schriftlich dokumentiert werden soll, empfiehlt sich die Beachtung der folgenden Punkte:

1. **Annahme eines Beratungsauftrages sorgfältig und kritisch prüfen**

   - Prüfungsauftrag geht vor Beratung (keine Umgehung)
   - Keine revisionsfremden Aufgaben wahrnehmen
   - Prozessunabhängigkeit, Objektivität und Vertraulichkeit wahren
   - Interessenskonflikte meiden
   - Revisionsaufgaben unbeeinflusst wahrnehmen
   - Revisionskompetenz (Wissen, Fähigkeiten und Qualifikation) anforderungsgerecht sicherstellen
   - Vereinbarkeit des Beratungsauftrags mit der Revisionsplanung bewerten
   - Übereinstimmung mit Instituts-/Revisionszielen prüfen (Verbesserung Geschäftsprozesse, IKS und Risikomanagement)

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 vereinbaren
   - Allgemeine Bedingungen, Absprachen, durchzuführende Arbeiten und Schlüsselfaktoren des offiziellen Beratungsauftrags schriftlich vereinbaren oder als Prüfungsplan dokumentieren

3. **Maßnahmen zur Minimierung möglicher Beeinträchtigungen treffen**

   - Keine unangemessene Führungsverantwortung übernehmen
   - In Komitees keine Entscheidungsverantwortung (non-voting member)
   - Unabhängige Leitung/Aufsicht benennen
   - Getrennte Ergebnisverantwortung vereinbaren (Verantwortung für Annahme/ Umsetzung von Empfehlungen liegt beim Management)
   - Bestätigung des Auftraggebers über Kenntnis der Rahmenbedingungen für die Interne Revision einholen
   - Beratungsauftrag in der Revisionsplanung berücksichtigen
   - Personelle Trennung in der Revision sicherstellen

4. **Beratungsauftrag sorgfältig und systematisch durchführen**

   - Klare Methodik festlegen/Abgrenzung zur projektbegleitenden Prüfung
   - „Level“ der Beratungsleistung festlegen
   - 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 an interne und externe Stellen sicherstellen

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

   - 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.)
   - Vermutete bzw. erwartete Risiken und Mängel immer schriftlich berichten
   - Für das Institut bedeutende Risiken, Schwachstellen und Ergebnisse zeitnah an die Geschäftsleitung kommunizieren

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.

2.6.5 Beratung in der Praxis

Die Interne Revision verfügt über ein breites und überparteiliches Fachwissen, kennt Prozesse, Produkte und Systeme des Instituts mit ihren Risiken und Kontrollinstrumenten und hat den besten 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:

- Strategieentwicklungen (Findungsprozesse)
- Jährliche Überprüfung der Geschäfts- und Risikostrategie(n) auf Schwachstellen, Angemessenheit, Konsistenz, Nachhaltigkeit
- Grundsatzfragen zur Angemessenheit und Wirksamkeit des Risikomanagements und der Internen Kontrollverfahren
- 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)
- Risikoanalyse von Betriebsauslagerungen/Outsourcing-Prozesse (s. a. gesonderte Anforderung an die Revision gem. MaRisk AT 9 Tz. 2)
- Begleitung wesentlicher Projekte (s. a. gesonderte Anforderung an die Revision gem. MaRisk BT 2.1. Tz. 2)
- 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.

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).

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.

2.6.6 Besonderheiten der Projektbegleitung

Im Sinne der MaRisk soll die Interne Revision bei wesentlichen Projekten mit ihrer profunden, übergreifenden Fachkompetenz risikoorientiert und präventiv Risiken und Schwachstellen betrachten, um frühzeitig durch Hinweise, Anregungen und Empfehlungen zur Angemessenheit und Wirksamkeit des Risikomanagements und des Internen Kontrollsystems beizutragen. Gleichzeitig benötigt die Interne Revision Informationen über Änderungen in den Geschäftsprozessen, um ihre Prüfungsplanung entsprechend ausrichten zu können. Daher handelt es sich bei der Begleitung wesentlicher Projekte um eine „Muss-Vorschrift“ für die Interne Revision (MaRisk BT 2.1 Tz. 2; vgl. Abschnitt 8)

Besonderheiten der Projektbegleitung für die Interne Revision sind u. a.:

- Bestimmung der Wesentlichkeit von Projekten in Form einer standardisierten, nachvollziehbaren Risikoanalyse (z. B. Projektscoring) zur Identifikation und Bewertung der kritischen Risikotreiber
- Grundsätzliche Teilnahme an wichtigen Projektsitzungen und in Projektlenkungsgremien
- Frühzeitige Information der Projektverantwortlichen bei sich abzeichnenden Projekt-, Abwicklungs- und Realisierungsrisiken
- Erstellung einer angemessenen Projektdokumentation (z. B. Risikoeinschätzung, Projektauftrag, Sitzungsprotokolle, Statusberichte, eigene Aufzeichnungen, Vermerke und Berichte).

2.6.7 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 (vgl. Abschnitt 10). Gemäß IPPF Standard 1210 muss der Leiter der Internen Revision 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.

Quellenverzeichnis:

Bünis, M./Gossens, T.: Das 1x1 der Internen Revision – Bausteine eines erfolgreichen Revisionsprozesses, Deutsches Institut für Interne Revision e.V. (DIIR), DIIR-Forum, Band 10, 3. Auflage, 2020, Erich Schmid Verlag.

DIIR-Arbeitskreis „MaRisk“: Die Begleitung wesentlicher Projekte in Kreditinstituten, Zeitschrift Interne Revision (ZIR) 5/2010, S. 237 ff.

Eulerich, M./Lenz, R.: Der Wert der Internen Revision, Zeitschrift Interne Revision (ZIR) 4/2020, S. 178 ff.

Helfer, M.: Beratungskompetenz der Revisoren systematisch fördern, Betriebswirtschaftliche Blätter 01/2011, S. 19 ff.

Herold, R.: Der Revisor 2025, Zeitschrift Interne Revision (ZIR) 4/2021, S. 164 ff.

Lück, W.: Aktuelle und zukünftige Schwerpunkte erfolgreicher Revisionsarbeit, Deutsches Institut für Interne Revision e.V. (DIIR), DIIR-Forum, Band 6, 2006, Erich Schmid Verlag.

Ullrich, Walter: Die Near-Time-Revision ist der nächste Schritt in die Zukunft, Betriebswirtschaftliche Blätter 01/2011, S. 6 ff.

Wendt, T./ Eichler, H.: Interne Revision für Aufsichtsräte, 2018, Erich Schmid Verlag.

3 Externe Rahmenbedingungen

3.1 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. Hierzu kommen noch berufsständische Normen.

Im Falle von Ermessensspielräumen, z. B. Einschätzung der Wahrnehmung des eigenen Instituts aus Sicht der Kapitalmärkte (z. B. Systemrelevanz), oder Wahlrechten ist zu prüfen, ob diese in Abstimmung mit der Geschäftsleitung und dem Aufsichtsorgan, ggf. mit seinem Prüfungsausschuss, getroffen werden müssen. Soweit dies Prüfungsgegenstände des Abschlussprüfers betrifft oder diese beeinflusst, ist auch dessen Einbindung zu empfehlen.

Grundsätzlich ist es sinnvoll, dass auch die Interne Revision eine Übersicht gem. AT 4.4.2 Tz. 2 MaRisk führt (wesentliche rechtliche Vorgaben), 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.), Interessenvertretungen (z. B. DIIR),
- Auswertung der, im Rahmen der Aktivitäten rund um den AT 4.4.2 Tz. 2 MaRisk, gesammelten Unterlagen.

Dabei muss sich die Interne Revision über die relevanten Jurisdiktionen und deren jeweilige Regelungsgeber Gedanken machen und ihre Suchkanäle danach auswählen. Mittlerweile gibt es Anbieter, die mit Hilfe „künstlicher Intelligenz“ und entsprechendem Zugriff auf regulatorische/rechtliche Vorschriften Möglichkeiten bieten, die Suche nach neuen/geänderten Regularien und deren Auswertung zu vereinfachen. Zwar können auch diese keine Vollständigkeit garantieren, allerdings ist – bei effizientem Einsatz der Instrumente – eine schnellere und für die ausgewählten Quellen umfassende Identifikation relevanter Fundstellen möglich.

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

3.2 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.

- § 91 Abs. 2 AktG:
  Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.

Mit dem Finanzmarktintegritätsstärkungsgesetz (FISG) wurde § 91 Abs. 3 AktG neu eingefügt, der nun explizit, die bereits aus dem KWG bekannte Verpflichtung zur Einrichtung eines Internen Kontroll- und Risikomanagementsystems für börsennotierte Aktiengesellschaften beinhaltet, was auch die Einrichtung einer Internen Revision umfasst.

- § 91 Abs. 3 AktG:
  Der Vorstand einer börsennotierten Gesellschaft hat darüber hinaus ein im Hinblick auf den Umfang der Geschäftstätigkeit und die Risikolage des Unternehmens angemessenes und wirksames internes Kontrollsystem und Risikomanagementsystem einzurichten.

Die Prüfungstätigkeit der Internen Revision ist auch als Voraussetzung eines ordnungsgemäßen Informationsmanagements einzuordnen. Dies bekommt insbesondere Bedeutung im Rahmen der Nutzung der Business Judgement Rule 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.

- § 93 Abs. 1 S. 2 AktG:
  Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied bei einer unter-

nehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln.

§ 107 Abs. 3 S. 2 AktG regelt direkt die Überwachungsverpflichtung des Aufsichtsorgans.

- § 107 Abs. 3 S. 2 AktG:
  Er kann insbesondere einen Prüfungsausschuss bestellen, der sich mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems sowie der Abschlussprüfung, hier insbesondere der Auswahl und der Unabhängigkeit des Abschlussprüfers und der vom Abschlussprüfer zusätzlich erbrachten Leistungen, befasst.

Falls kein Prüfungsausschuss gebildet ist, dann muss das Aufsichtsorgan insgesamt diese Überwachungsaufgaben erfüllen. Wenn dies formell den Verantwortungsbereich des Aufsichtsorgans auch nicht ausweitet, erfolgt doch eine explizite Kodifizierung dieser Überwachungsaufgaben. Eine entsprechend intensivere Beschäftigung des Aufsichtsorgans mit diesen Themen ist zu erwarten.

Für Unternehmen von öffentlichem Interesse erfolgte durch das Finanzmarktintegritätsstärkungsgesetz folgende Erweiterung:

- § 107 Abs. 4 AktG:
  Der Aufsichtsrat einer Gesellschaft, die Unternehmen von öffentlichem Interesse nach § 316a S. 2 des Handelsgesetzbuchs ist, hat einen Prüfungsausschuss im Sinne des Absatzes 3 S. 2 einzurichten. Besteht der Aufsichtsrat nur aus drei Mitgliedern, ist dieser auch der Prüfungsausschuss. Der Prüfungsausschuss muss die Voraussetzungen des § 100 Absatz 5 erfüllen. Jedes Mitglied des Prüfungsausschusses kann über den Ausschussvorsitzenden unmittelbar bei den Leitern derjenigen Zentralbereiche der Gesellschaft, die in der Gesellschaft für die Aufgaben zuständig sind, die den Prüfungsausschuss nach Abs. 3 S. 2 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.

Das IDW hat im Zusammenhang mit der Prüfung des Internen Revisionssystems durch Wirtschaftsprüfer einen eigenen Prüfungsstandard veröffentlicht (IDW PS 983). Dieser Prüfungsstandard wurde gemeinsam mit dem DIIR erarbeitet. Der Standard beurteilt die Interne Revision als eine wesentliche Governance-Funktion und als dritte Verteidigungslinie im Three-Lines-of-Defense-Modell.

3.3 Branchenspezifische Normen

3.3.1 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 Risikoexponierung 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).

3.3.2 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): Die Interne Revision oder eine andere vergleichbare unabhängige Revisionsstelle prüft mindestens einmal jährlich die Ratingsysteme des Instituts und deren Funktionsweise, einschließlich der Tätigkeit der Kreditabteilung sowie der PD-, LGD-, EL und Umrechnungsfaktor-Schätzungen. Überprüft wird die Einhaltung aller geltenden Anforderungen.

- Institutsvergütungsverordnung (InstitutsVergV): Die Kontrolleinheiten (hierzu zählt gemäß § 2 Abs. 11 InstitutsVergV auch die Interne Revision) sind bei der Ausgestaltung und der Überwachung der Vergütungssysteme sowie in bedeutenden Instituten gemäß § 25n des Kreditwesengesetzes auch in Bezug auf den Prozess der Ermittlung der Risikoträger und Risikoträgerinnen gemäß § 25a Absatz 5b des Kreditwesengesetzes sowie der Gruppen-Risikoträger und Gruppen-Risikoträgerinnen gemäß § 27 Abs. 2 S. 1 angemessen zu beteiligen. (§ 3 Abs. 3 InstitutsVergV).

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

3.4 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-Act (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 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.

3.5 Handelsrechtliche Offenlegung im Lagebericht und Konzernlagebericht

Im Lagebericht bzw. Konzernlagebericht sind die voraussichtliche Entwicklung mit ihren wesentlichen Chancen und Risiken zu beurteilen und zu erläutern (§ 289 Abs. 1 S. 4 HGB bzw. § 315 Abs. 1 S. 4 HGB). Im Lagebericht bzw. Konzernlagebericht ist auch einzugehen auf die Risikomanagementziele und -methoden der Gesellschaft bzw. des Konzerns einschließlich ihrer bzw. seiner Methoden zur Absicherung aller wichtigen Arten von Transaktionen, die im Rahmen der Bilanzierung von Sicherungsgeschäften erfasst werden. Dies gilt in Bezug auf die Verwendung von Finanzinstrumenten durch die Gesellschaft bzw. den Konzern und sofern dies für die Beurteilung der Lage oder der voraussichtlichen Entwicklung von Belang ist (§ 289 Abs. 2 S. 1 Nr. 1 lit. a) bzw. § 315 Abs. 2 S. 1 Nr. 1 lit. a) HGB).

Kapitalmarktorientierte Kapitalgesellschaften i. S. d. § 264d HGB müssen zudem 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).

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

- *Risikobericht*

Unabhängig von der Kapitalmarktorientierung umfasst die Risikoberichterstattung Angaben zum Risikomanagementsystem (DRS 20.135).

- *Risikomanagementsystem*

Im Falle der Kapitalmarktorientierung des Mutterunternehmens sind die Merkmale des konzernweiten Risikomanagementsystems darzustellen (DRS 20.K137). Hierbei ist auf die Ziele und die Strategie sowie auf die Strukturen und Prozesse des Risikomanagements einzugehen (DRS 20.K137). 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). Im Rahmen der Ziele und der Strategie des Risikomanagements ist darzustellen, ob und ggf. welche Risiken grundsätzlich nicht erfasst bzw. vermieden werden (DRS 20.K140). Bei der Darstellung des Risikomanagements ist der Risikokonsolidierungskreis anzugeben, sofern dieser von dem Konsolidierungskreis des Konzernabschlusses abweicht (DRS 20.K142). Im Rahmen der Darstellung der Risikomanagementprozesse ist die Identifikation, Bewertung, Steuerung und Kontrolle der Risiken sowie die interne Überwachung dieser Abläufe zu erläutern (DRS 20.K144). Ebenso ist anzugeben, wenn eine Interne Revision das Risikomanagementsystem überprüft (DRS 20.K144).

- *Internes Kontrollsystem und Risikomanagementsystem bezogen auf den Konzernrechnungslegungsprozess*

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). Die Berichtspflicht erstreckt sich auf die Teile des IKS und des RMS, die den Konzernabschluss und Konzernlagebericht wesentlich beeinflussen. Hierbei ist auf die Strukturen und Prozesse einzugehen (DRS 20.K170). 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 Revisionssystem 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.

3.6 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.

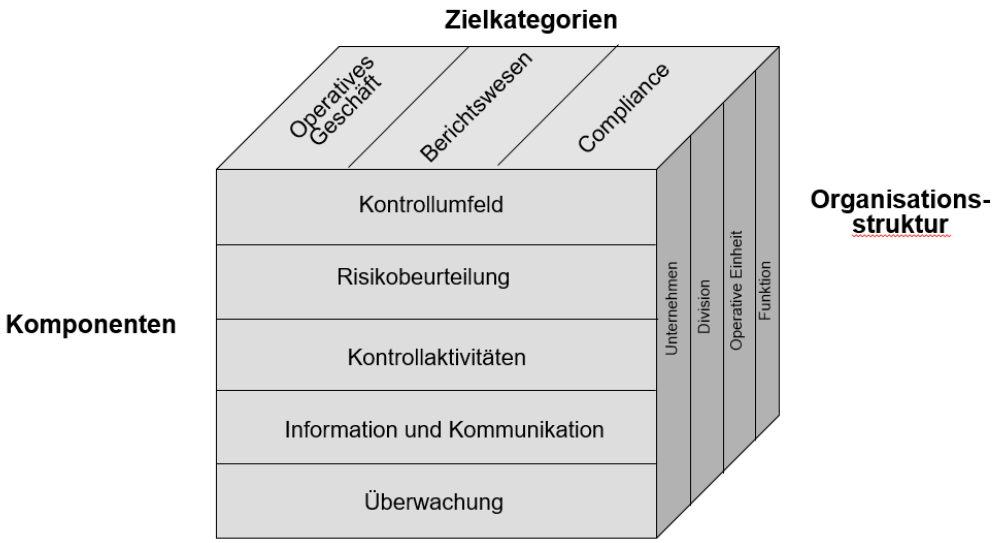


Abb. 2: COSO-Internal Control 2013

Durch die überarbeitete Version 2013 erfolgte eine Erweiterung des „Reporting“ um internes Reporting und nicht-finanzielles Reporting (z. B. Corporate Social Responsibility oder Nachhaltigkeitsaspekte); 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. 3: COSO-Enterprise Risk Management (2004)

Beide Modelle werden ausdrücklich vom IIA, DIIR, IDW und dem Sarbanes-Oxley Act empfohlen. 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. 4: COSO: Implications from the strategy

Abb. 5: COSO: Enterprise Risk Management (Framework 2017)

Ein international anerkanntes Regelwerk zur IT-Governance stellt COBIT dar (aktuell Version 5.0/2019; bis Version 4.1 noch als Control Objectives for Information and related Technology).

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

3.7 Berufsständische Regelungen (IPPF und DIIR-Veröffentlichungen)

Für Interne Revisoren stellen die Veröffentlichungen des DIIR und die Veröffentlichungen des International Professional Practices Framework (IPPF) die zentralen berufsständischen Normen dar.

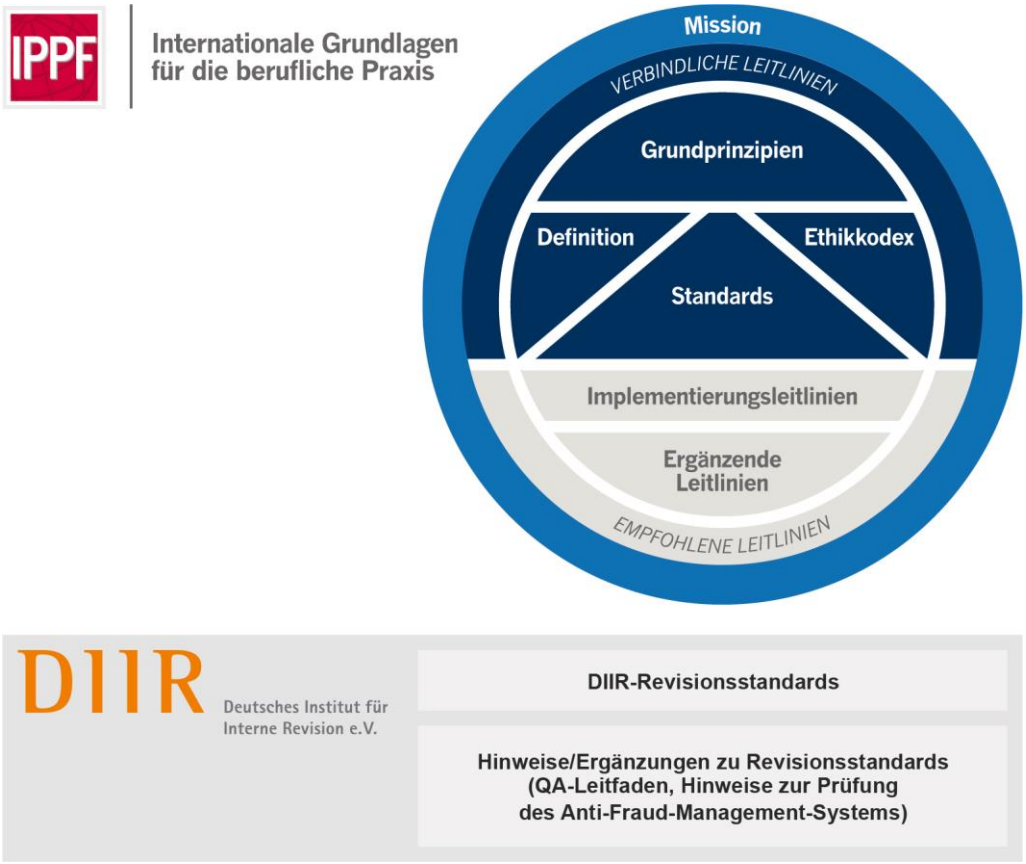


Abb. 6: Berufsrechtliche Normen der Internen Revision (IPPF)

Es kommen ggf. noch verbandsindividuelle revisionsbezogene Normen dazu. In den Rahmenbedingungen der Internen Revision (Charter) ist festzulegen, welcher Verpflichtungscharakter den jeweiligen Normen beigemessen wird.

4 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 Standardrevisionsprozess gelten grundsätzlich für alle Prüfungsarten und werden auf den folgenden Seiten im Detail beschrieben.

4.1 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 werden. Ein Abweichen vom dreijährigen Turnus bedeutet jedoch 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 der Prüfobjekte (Prüflandkarte, Prüfungsuniversum)
  - Risikobeurteilung der Prüfobjekte
- Mehrjahresplanung (langfristig, nach Risiko und Umfang)
- Jahresplanung (operativ, genehmigungspflichtig)
- Operative Planung (zur unterjährigen dispositiven Steuerung)

4.1.1 Rahmenplanung

4.1.1.1 Prüfungsuniversum

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

- Die Prüfobjekte müssen alle wesentlichen Prozesse und Wertschöpfungsketten, funktionalen und operativen Bereiche sowie Produkte und Systeme umfassen.
- Alle wesentlichen Auslagerungstatbestände sowie Einlagerungen von Geschäftsaktivitäten, bei denen eine vertragliche Prüfungspflicht besteht, sind einzubeziehen. Nicht wesentliche Auslagerungen und sonstiger Fremdbezug sind bei der Vorbereitung der Prüfung risikoadäquat zu berücksichtigen.
- Es sind alle gesetzlichen und aufsichtsrechtlichen Anforderungen sowie ggf. besondere Anforderungen der Geschäftsleitung zu berücksichtigen.
- Spezifische aufsichtliche Anforderungen wie z. B. die Prüfung von Ratingsystemen gem. der CRR sind ebenfalls angemessen zu berücksichtigen.
- Damit die Prüfungsabdeckung transparent ermittelt werden kann verkörpert idealerweise ein Prüfobjekt eine einzelne Prüfung. Die Granularität der Prüfobjekte sollte so gewählt werden, dass eine trennscharfe Beurteilung der Risiken möglich ist (risikoorientierte Planung).
- Die Überprüfung der Prüfobjekte hinsichtlich Vollständigkeit, Relevanz und Konsistenz muss jährlich so rechtzeitig erfolgen, dass für die Jahresplanung aktuelle Daten vorliegen.
- Die Überprüfung ist zu dokumentieren.
- Eine nachvollziehbare Dokumentation und Genehmigung (Kompetenzträger sind zu definieren) ist notwendig für:
  - Strukturelle Veränderungen der Prüfobjekte
  - Ermittlung des ersten Prüfungsjahres für neu angelegte Prüfobjekte inkl. Begründung
  - Anpassung der Gewichtungsfaktoren im Bewertungsverfahren.
  - Änderungen der Methodik der Risikobewertung.

4.1.1.2 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.
- 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.

- Die Risikobewertungsverfahren der Internen Revision haben eine Analyse des Risikopotenzials der Aktivitäten und Prozesse unter Berücksichtigung absehbarer Veränderungen (z. B. absehbare Marktentwicklungen, neue Produkte/ Märkte/ Vertriebswege, geplante Ausweitung von Geschäftsaktivitäten, Projekte) zu beinhalten.
- Bei der Risikobewertung sind verschiedene Risikoquellen zu berücksichtigen. Neben den typischen bankgeschäftlichen Risikoarten gemäß MaRisk (Zinsänderungsrisiko, Markt- bzw. Liquiditätsrisiko, Adressenausfallrisiko) und der betriebswirtschaftlichen Bedeutung der Prüfobjekte sind insbesondere die operationellen Risiken zu bewerten (die Unangemessenheit oder das Versagen von internen Verfahren, Menschen, Systemen sowie externe Ereignisse).
- Bei der Bewertung des operationellen Risikos ist auch die Manipulationsanfälligkeit der Prozesse durch Mitarbeiter angemessen zu berücksichtigen.
- Bei dieser anfänglichen Risikobeurteilung sind z. B. das inhärente und das residuale Risiko bereits existierender vergleichbarer Prüfobjekte und 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-Arbeit
    - Information/Konsultation aufsichtsrechtlicher Regelungen bzw. deren Überarbeitung (z. B. über Verbände)
- „Besondere Risiken“ bedingen eine jährliche Prüfungsfrequenz. Sie sind wie folgt definiert:
    - Besondere Risiken 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 zu Aufbau-/Ablauforganisation und Risikosteuerungs-/-controllingprozesse verursacht werden können, erhöhen die Eintrittswahrscheinlichkeit und das potenzielle Schadensausmaß von besonderen Risiken.

Daneben können auch für das Institut wesentliche Projekte mit besonderen Risiken behaftet sein.

- Das Interne Kontrollsystem (Aufbau- und Ablauforganisation sowie Risikosteuerungs- und -controllingprozesse) ist gemäß MaRisk zentraler Prüfungsgegenstand der Internen Revision und sollte daher integraler Bestandteil möglichst jeder Prüfung sein.
- Alle in der Risikobeurteilung erhaltenen und verwendeten Informationen sind angemessen zu dokumentieren.
- Die ggf. jeweils ermittelte „generische“ Risikokennziffer bestimmt die Prüfungsdringlichkeit für das jeweilige Prüfobjekt, aus der sich die Prüfungsfrequenz bzw. der Prüfungsturnus (z. B. alle drei Jahre) ableitet und die, bei Bedarf, als Grundlage für eine risikoorientierte Priorisierung von Prüfungen herangezogen werden kann.

4.1.2 Mehrjahresplanung

- Alle Prüfobjekte werden zur Ermittlung eines Rahmen- bzw. Mehrjahresplanes vollständig abgebildet.
- 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. Die entsprechende Risikobeurteilung sollte, z. B. über ein Scoringverfahren, nachvollziehbar begründet sein.
- Wie viele Prüfobjekte in einem Vier- oder Fünfjahreszyklus geprüft werden dürfen, so dass noch „grundsätzlich“ ein Dreijahreszyklus vorliegt, ist in dem MaRisk nicht konkretisiert. In der Praxis führt ein granulareres Prüfungsuniversum in der Regel zu längeren Prüfungsturnus, da die Gesamtrisiken des Instituts in kleinere Einheiten heruntergebrochen werden.
- 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) muss bei Instituten, die den IRB-Ansatz nutzen, die Interne Revision oder eine andere vergleichbare unabhängige Revisionsstelle mindestens einmal jährlich die Ratingsysteme des Instituts und deren Funktionsweise, einschließlich der Tätigkeit der Kreditabteilung sowie der PD-, LGD-, EL- und die Umrechnungsfaktor-Schätzungen prüfen. Die Prüfung umfasst die Einhaltung aller geltenden Anforderungen und ist hinsichtlich des Ratingsystems bzw. der Komponenten von Ratingsystemen unabhängig von der Größe des zugrundeliegenden Portfolios bzw. des sich

aus dem zugrundeliegenden Portfolio resultierenden Risikos durchzuführen (Art. 191 CRR).

- Daneben sieht die CRR eine jährliche Prüfung des allgemeinen Risikomanagements vor, sofern das Kreditinstitut interne Modelle zur Ermittlung des Gegenparteiausfallrisikos (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 der Deutschen Kreditwirtschaft vollständig innerhalb eines Zeitraums von drei Jahren zu prüfen. Es wird erwartet, dass jedes Jahr in risikoangemessenem Umfang Teilbereiche geprüft werden, sofern innerhalb eines Drei-Jahres-Rhythmus sämtliche Bereiche einer Prüfung unterzogen werden.

- Ergebnis der Mehrjahresplanung ist eine Prioritätenliste, welche die Prüfungsfrequenz für alle Prüfobjekte in der Regel verteilt über drei bis fünf Folgejahre ausweist. Hierbei ist es nicht erforderlich formelle Prüfungspläne für drei Jahre aufzustellen. Es genügt vielmehr, den Prüfungsplan für das nächste Jahr aufzustellen. Die Informationen über die Folgejahre dienen im Wesentlichen einer Überprüfung des Kapazitätsbedarfs im Mehrjahresvergleich (Gleichverteilung, Ableitung von Ressourcenbedarfen).
- Bei einer im Einzelfall zulässigen Ausweitung des Planungszeitraums auf vier oder fünf Jahre muss die Darstellung der Mehrjahresplanung über einen entsprechend längeren Zeitraum erfolgen. Die Ausweitung sollte im Einzelfall begründet werden.
- Die Prüfungsdringlichkeit ergibt sich dabei aus einer Kombination des dem Prüfungsgebiet zugewiesenen Risk- Assessments (in der Regel Berücksichtigung von inhärenten Risiken und Residualrisiken nach der Beurteilung des IKS) sowie objektbezogenen Faktoren (Datum der letzten Prüfung und entsprechendes Prüfungsergebnis) bzw. aus den aufsichtsrechtlich vorgeschriebenen Prüfungsintervallen.
- Die Risikoeinschätzungen sind regelmäßig und anlassbezogen kritisch zu hinterfragen bzw. überprüfen und führen ggf. rollierend zu einer Anpassung der Prüfungsplanung.
- In der Mehrjahresplanung sollten objektbezogene Planwerte, welche dem notwendigen zeitlichen Aufwand für eine Prüfung des Objektes entsprechen sollen, erfasst werden (Aufwand Prüfungsteam inkl. Steuerungs- und Unterstützungsfunktionen).
- Damit entsprechend der Risikobewertung grundsätzlich alle Prozesse und Aktivitäten im vorgegebenen Prüfungsturnus angemessen bewältigt werden können, ist

eine angemessene Personal- und Kapazitätsausstattung sicherzustellen. Etwaige Ressourcenbeschränkungen sind deutlich gegenüber der Geschäftsleitung zu kommunizieren.

- Nach der jährlichen Überprüfung der Prüfobjekte und Risikobewertung sind die wesentlichen Veränderungen zusammen mit der Prioritätenliste der Leitung der Internen Revision zwecks jährlicher Genehmigung vorzustellen.

4.1.3 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.
- Daneben ist festzulegen, welche Prüfobjekte aufgrund ihrer jeweiligen IRBA-Relevanz (wesentliche Änderungen oder Nicht-/Schlechtfunktionieren von Ratingsystemen bzw. deren Komponenten) neben der risikoorientierten Planung zusätzlich in die Jahresplanung aufzunehmen sind.
- Der Planungsprozess sollte einen Austausch mit dem Management (Geschäftsleitung und nachfolgende Führungsebene) bezüglich risikoorientiert zu berücksichtigen der Sachverhalte beinhalten. Zur Vermeidung von Redundanzen (soweit risikoorientiert möglich) bietet sich auch ein Austausch mit dem Jahresabschlussprüfer zu dessen Prüfungsschwerpunkten an.
- Die Jahresplanung sollte vor Beginn des neuen Geschäftsjahres erstellt werden. Für die entsprechende Kapazitätsplanung sind dabei folgende Faktoren zu berücksichtigen:
  - Ausrichtung an dem der Internen Revision zur Verfügung stehenden Budget (Personal- und Sachkostenbudget) sowie an der Unternehmensplanung.
  - Vorhalten von Kapazitäten für ex ante-Aktivitäten (Prüfung bzw. Begleitung wesentlicher Projekte, Beratung der Facheinheiten) sowie für Follow Up-Tätigkeiten.
  - Vorhalten einer Reserve („Puffer“) für außerplanmäßig notwendig werdende Prüfungen bzw. Sonderuntersuchungen. Die Größe eines derartigen Puffers ist nicht vorgeschrieben, sondern sollte sich an dem historischen Bedarf und an absehbaren Änderungen orientieren – als Orientierungswert wird vielfach ein Puffer in Höhe von 10% - 15% der Kapazität als sinnvoll erachtet.
  - Aufnahme bereits bekannter und im Folgejahr fälliger Nachschauprüfungen
  - Auslagerungen sowie Einlagerungen von Geschäftsaktivitäten, bei denen eine vertragliche Prüfungspflicht besteht.

- Prüfungen als Konzernrevision und Prüfungsaktivitäten zur Unterstützung von angeschlossenen Unternehmen und/oder Tochtergesellschaften, wo dies organisatorisch vorgesehen ist.

- Die Prüfungen für die Planungsperiode werden systematisch zusammengestellt, im Planungssystem angelegt und der Revisionsleitung vorgelegt.
- Für jede im Rahmen der Jahresplanung angelegte Prüfung sollten auf Grundlage der zu diesem Zeitpunkt vorliegenden/bekannten Informationen die Prüfungsdauer und die Prüfungsart sowie das vorläufige Prüfungsziel und der vorläufige Prüfungsumfang 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 und der kompetenzgerechten Genehmigung der Nichtaufnahme aufzulisten. Die Liste ist der Revisionsleitung und der Geschäftsleitung mit der Planung zur Kenntnis zu bringen.
- Die Jahresplanung sollte der Geschäftsleitung spätestens zu Beginn des neuen Geschäftsjahres zur Genehmigung vorgelegt werden.
- Die jeweiligen Jahresplanungen/Genehmigungen (inkl. der jeweiligen Prioritätenliste und der fälligen, nicht in die Jahresplanung aufgenommenen Objekte) sind sechs Jahre aufzubewahren bzw. zu archivieren.

4.1.4 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 zu benannt werden.
- Innerhalb des laufenden Jahres sind die IRBA-relevanten Objekte, die nicht in die Jahresplanung für das aktuelle Jahr aufgenommen wurden, quartalsweise auf das Vorliegen von Informationen (siehe auch „Prüfobjekte mit aufsichtsrechtlich vorgeschriebenem Intervall“) zu wesentlichen Änderungen oder dem Nicht-/Schlechtfunktionieren von Ratingsystemen/Komponenten von Ratingsystemen zu untersuchen. Die Ergebnisse der Überprüfung und ggf. daraus resultierende Vorschläge zu Änderungen an der Jahresplanung sind zu dokumentieren und der Revisionsleitung zur Genehmigung vorzulegen.

- Wesentliche nachträgliche Anpassungen der genehmigten Jahresplanung, die sich im weiteren Verlauf durch Änderung von Prioritäten, personellen oder organisatorischen Rahmenbedingungen ergeben, sind unterjährig von der Geschäftsleitung zu genehmigen. Dies betrifft insbesondere geplante, aber nicht mehr durchführbare Prüfungen. Kriterien für die Wesentlichkeit 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) oder
  - Verschiebung von Prüfungen mit hohem Risikogewicht oder
  - Verschiebung von regulatorischen Pflichtprüfungen.
- Die Begründung für die Verschiebung/Absage geplanter Prüfungen und deren Genehmigung sind zu dokumentieren.

4.2 Prüfungsvorbereitung

Mit der Phase der Prüfungsvorbereitung beginnt die Prüfung. Zunächst sind Hintergrundinformationen zu den Prüfobjekten aus allen verfügbaren Quellen (z. B. Geschäftsstrategien, regulatorische Vorgaben, organisatorische Regelungen, IT-Systeme, Gespräche/Interviews, Dauerakten, Vorprüfungen, Informationen zu Auslagerungen, Reports, Datenanalysen, etc.) heranzuziehen, um eine fundierte Risikoeinschätzung vornehmen zu können.

Zudem sind vor jeder Prüfung grundsätzlich alle offenen Feststellungen aus vorangegangen Prüfungen (interne und externe) zu identifizieren, um diese bei entsprechender Relevanz (Risikoorientierung) im Rahmen der anstehenden Prüfung erneut zu beurteilen. Die Aufstellung der zu Prüfungsbeginn noch offenen Feststellungen ist in der Prüfungsdokumentation zu hinterlegen.

4.2.1 Anforderungsliste

Sofern diese Unterlagen nicht direkt aus verfügbaren Systemen bzw. Dokumentationen zu beschaffen sind, ist eine Anforderungsliste zu erstellen. Diese Liste sollte spätestens zwei Wochen vor Beginn der Prüfungshandlungen an das Management der zu prüfenden Einheit/en (Ausnahme Sonderuntersuchungen) versandt werden (ggf. im Rahmen der Prüfungsankündigung, vgl. Abschnitt 4.2.6). Die Anforderungsliste ist während der Prüfungsdurchführung fortzuführen.

4.2.2 Risikoeinschätzung (Risk Assessment)

Aufbauend auf der im Rahmen der Jahresplanung erfolgten Risikoeinschätzung der inhärenten Risiken und der Kontrollrisiken werden zu Beginn der Prüfung die zum Zeitpunkt der Jahresprüfungsplanung getroffenen Annahmen unter Berücksichtigung der Analyse 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. Das Ergebnis der Risikoanalyse ist dezidiert, z. B. in einem Prüfungshandbuch oder -memorandum (siehe Abschnitt 4.2.8), zu dokumentieren.

4.2.3 Prüfungsziele

Basierend auf den analysierten bzw. vermuteten Risiken sind die Prüfungsziele festzulegen. Folgende grundsätzliche Prüfungsziele stehen dabei zur Auswahl (in Anlehnung an DIIR Revisionsstandard Nr. 1 Tz. 1):

Prüfungsziel	Erläuterung
Ordnungsmäßigkeit	**Einhaltung von unternehmensinternen und -externen Vorgaben**
	Ziel der Prüfung der „Ordnungsmäßigkeit“ ist die Sicherstellung der Einhaltung unternehmensexterner (z. B. geltende gesetzliche und aufsichtsrechtliche Vorgaben sowie sonstige externe Regelungen und anerkannte Standards) sowie unternehmensinterner Vorgaben (z. B. Satzungen, Geschäftsanweisungen, interne Richtlinien, Kompetenzordnungen oder Geschäftsleitungsbeschlüsse) in formeller und materieller Hinsicht. Hierbei werden durch geeignete Prüfungshandlungen IST-Abweichungen zu dem durch die existierenden Vorgaben definierten SOLL-Zustand ermittelt[2] und – in Verbindung mit der Formulierung geeigneter Empfehlungen – im Rahmen von Feststellungen adressiert, um zur Ordnungsmäßigkeit des Prüfobjektes beizutragen.
Sicherheit	**Schutz von Menschen, Vermögen und Daten**
	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. 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.

[2] Vgl. Peemöller in Förschle/Peemöller (Hrsg.), Wirtschaftsprüfung und Interne Revision, Heidelberg 2004.

Wirtschaftlichkeit	**Effizienter Ressourceneinsatz sowie effiziente Prozess- und Kontrollgestaltung**
	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 entsprechen[3] 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. 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 kann[4].
Zweckmäßigkeit	**Ausrichtung von Prozessen und Kontrollen auf die (Unternehmens-)Ziele**
	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. Bei der Zweckmäßigkeitsprüfung hat der Revisor den Soll-Zustand (mangels eindeutig formulierter Vorgaben) aus den Unternehmenszielen heraus selbst abzuleiten[5] und dem Vorstand bei Abweichungen unterstützend Empfehlungen auszusprechen.

[3] Vgl. Peemöller in Förschle/Peemöller (Hrsg.), Wirtschaftsprüfung und Interne Revision, Heidelberg 2004.

[4] Vgl. ebd.

[5] 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 vom Vorstand 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.[6] Der Inhalt der Geschäftsstrategie selbst ist nicht Gegenstand von Prüfungshandlungen durch (Jahresabschlussprüfer oder) die Interne Revision, dieser liegt allein in der Verantwortung der Geschäftsleitung[7] Stattdessen prüft die Interne Revision den Strategieprozess[8] und leistet durch die Prüfung der Umsetzung der vom Vorstand 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.[9]

Abb. 7: 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

[6] Lück, Lexikon der Internen Revision, München 2001, Seite 380.

[7] BaFin, Rundschreiben 10/2021 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ (18.08.2021), AT 4.2 Tz. 1, Erläuterung.

[8] BaFin, Rundschreiben 10/2021 (BA) „Mindestanforderungen an das Risikomanagement – MaRisk“ (18.08.2021), AT 4.2 Tz. 4.

[9] 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 zu den Prüfungszielen ermöglichen.

4.2.4 Prüfungsumfang

Der Prüfungsumfang wird auf der Basis der bereits bekannten bzw. vermuteten Risiken und Schwachstellen festgelegt. Dabei müssen auch relevante Systeme, Aufzeichnungen, Personalausstattung und Vermögensgegenstände einbezogen werden, einschließlich jener Aktivitäten, die sich unter der Kontrolle Dritter befinden (Auslagerungen).

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 4.2.7).

Wesentliche Änderungen des Prüfungsumfangs während der Prüfung sind in den Arbeitspapieren und ggf. über eine Anpassung des Planungsdokuments (Prüfungshandbuch, oder -memorandum, vgl. Abschnitt 4.2.8) zu dokumentieren.

Die Prüfungsschwerpunkte bzw. die Prüfungstiefe spiegeln sich in den Fragen der Prüfungsleitfäden bzw. strukturierten Checklisten wider. Bei Stichprobenprüfungen sind zumindest die Grundgesamtheit, das Verfahren für die Stichprobenauswahl nebst Begründung und die Stichprobe nachvollziehbar zu dokumentieren.

4.2.5 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) zu benennen. Es sind Prüfungsbeginn und -ende sowie der geplante Aufwand in Prüferstunden oder -tagen festzulegen. Es empfiehlt sich, in Abhängigkeit von der Komplexität der Prüfung, Meilensteine festzulegen.

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).

4.2.6 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 4.2.1), über den Zeitraum der Prüfung vor Ort sowie die Namen der Mitglieder des Prüfungsteams und ggfs. der Prüfungsleitung. Die Prüfungsankündigung sollte spätestens zwei Wochen vor Beginn der Prüfung erfolgen (Ausnahme: Sonderprüfungen, hier entfällt die Ankündigung). Bei kurzfristig angesetzten Prüfungen können die entsprechenden Informationen im Rahmen des „Prüfungs-Kick-off“ erfolgen.

4.2.7 Prüfungs-Kick-off

Es empfiehlt sich, vor Beginn einer Prüfung ein „Kick-off Meeting“ durchzuführen. Teilnehmer des Kick-off Meetings 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.

Dieses Eröffnungsgespräch ermöglicht, 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. Das betroffene Management hat im Rahmen des Gesprächs auch 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 Kick-off-Meetings ist es insbesondere, ein gemeinsames Grundverständnis von Interner Revision und Geprüften zu schaffen und damit ein Vertrauensverhältnis zu fördern. Darüber hinaus werden organisatorische Fragestellungen geklärt (z. B. Ansprechpartner, An- und Abwesenheiten, Bereitstellung von Unterlagen).

4.2.8 Dokumentation

Unmittelbar nach Abschluss des „Kick-Off-Meetings“ erfolgt die Fertigstellung und Genehmigung des Prüfungshandbuchs, welches die Ergebnisse der zuvor beschriebenen Arbeitsschritte beinhaltet. Zur Dokumentation von Planung und Durchführung der Prüfung 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.“

4.3 Prüfung

4.3.1 Prüfungshandlungen

Den Mitgliedern des Prüfungsteams obliegt es, während der gesamten Prüfung ein konstruktives, offenes und von Fairness geprägtes Verhältnis zu den Führungskräften und Mitarbeitern 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 im Wesentlichen auf Basis eines Arbeitsprogramms untersucht. Das Arbeitsprogramm beinhaltet die möglichen Prüfungsansätze und -handlungen.

Ziel der Prüfungshandlungen ist die Identifikationen, Sammlung, Bewertung und Dokumentation von Informationen auf deren Basis ein Prüfungsurteil gebildet und ggf. Prüfungsfeststellungen getroffen werden.

Die so 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 eine hohe Akzeptanz durch die Geprüften haben.

Wesentliche Aspekte der Revisionsarbeit sind die sich aus dem Prüfungsobjekt ergebenden fachlichen Themenstellungen der Prüfung. Darüber hinaus werden auch Aspekte wie Ordnungsmäßigkeit, Sicherheit, Risikohaftigkeit, Wirtschaftlichkeit, Rentabilität, Zweckmäßigkeit, Unternehmenszielsetzungen sowie Wirksamkeit der Maßnahmen zur Verhinderung und Aufdeckung doloser Handlungen beurteilt. Daneben wird implizit das Führungsverhalten innerhalb der geprüften Einheit beurteilt. Der Prüfungsleiter überwacht laufend, ob der im Vorfeld festgelegte Prüfungsumfang sowie die Prüfungsschwerpunkte noch sachgerecht und angemessen sind. Ist dies nicht der Fall, sind entsprechende Anpassungen vorzunehmen, zu begründen und in Abhängigkeit des Sachverhaltes 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 für künftige Planungen verwendet und bilden die Grundlage für eine ggf. erfolgende Kostenverrechnung.

Getroffene Feststellungen und die hieraus abgeleiteten Maßnahmen werden mit den verantwortlichen Mitarbeitern 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.

Die Einladung der zuständigen Kompetenzträger zur Schlussbesprechung nach Abschluss der Prüfungshandlungen ist frühzeitig zu koordinieren. Zur Vorbereitung auf die Schlussbesprechung ist der geprüften Einheit bereits ein Entwurf des Schlussberichtes zur Verfügung zu stellen. 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.

4.3.2 Dokumentation der Prüfungshandlungen

Alle Prüfungshandlungen sind so zu dokumentieren, dass sie für einen sachverständigen Dritten ohne vorherigen Bezug zur Prüfung in angemessener Zeit verständlich sind. Die Arbeitspapiere sollen Ziel, Art und Umfang der durchgeführten Prüfungshandlungen, die daraus resultierenden Ergebnisse, den Zeitraum der Durchführung 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.

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

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

4.3.3 Risikoeinstufung von Feststellungen und Revisionsergebnissen

- Gemäß MaRisk, BT 2.4 Berichtspflicht, Tz. 1 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. Eine zusammenfassende Bewertung der Prüfungsergebnisse 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, sowie
- Ausmaß, Entwicklung und Management von Risiken.

Neben der dargestellten zusammenfassenden Bewertung der Prüfungsergebnisse ist eine gesonderte Beurteilung der einzelnen Prüfungsfeststellungen/Mängel vorzunehmen. Als Maßstab für die Einstufung der Prüfungsfeststellungen/Mängel empfiehlt sich hierbei, differenzierend zur zusammenfassenden Bewertung der Prüfungsergebnisse, dass für das Gesamtinstitut resultierende Risiko hervorzuheben. Neben den in den MaRisk vorgegeben Mängelkategorien („besonders schwerwiegend“, „schwerwiegend“, „wesentlich“) könnten Prüfungsfeststellungen/Mängel hierbei auch als „bemerkenswert“ oder „geringfügig“ bewertet werden. Die konkreten Abstufungen von Prüfungsfeststellungen/Mängel könnten sich hierbei an folgendem Praxisbeispiel orientieren:

- **Besonders schwerwiegende Feststellung**
  - Unter Berücksichtigung der 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.
  - Eine unverzügliche Berichterstattung durch die Geschäftsleitung an das Aufsichtsorgan ist erforderlich.
- **Schwerwiegende Feststellung**
  - Unter Berücksichtigung der 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.

- Eine unverzügliche Berichterstattung an die Geschäftsleitung ist erforderlich.

- **Wesentliche Feststellung**
  - Unter Berücksichtigung der 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.
  - Eine Berichterstattung an die Geschäftsleitung sowie das Aufsichtsorgan ist im Rahmen der Jahresberichterstattung erforderlich.
- **Bemerkenswerte Feststellung**
  - Unter Berücksichtigung der 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 deutliche 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 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.

4.3.4 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 sollte eine zusammenfassende Bewertung der Prüfungsergebnisse (inkl. einer Aussage zur Ordnungsmäßigkeit der Prozesse) in die Zusammenfassung für das Management aufgenommen werden (vgl. Abschnitt 4.3.3).

Der abschließende 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).

Bei Meinungsverschiedenheiten ist die Möglichkeit zur Berücksichtigung einer Stellungnahme des geprüften Bereiches im Bericht vorgesehen oder es wird zumindest auf die Meinungsverschiedenheit hingewiesen.

Der Prüfungsbericht sollte allen Personen zugänglich gemacht werden, die einen Handlungsbedarf oder ein berechtigtes Interesse (Kontrollfunktionen) an den Ergebnissen haben. Der Bericht wird inklusive des Verteilers vor der Verteilung vom Leiter der Internen Revision oder von einer anderen autorisierten Person genehmigt.

4.3.4.1 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 in einer neuen Prüfung) aus einer möglicherweise bereits erreichten Eskalationsstufe herausgenommen wird und das 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.

- Szenario 1: Eine noch offene Feststellung liegt vor:
  - Nach Abschluss der Prüfungshandlungen wird eine inhaltlich aktualisierte Feststellung erfasst. 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:
  - Falls sich im Rahmen einer erneuten vertieften Prüfung zeigt, 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, 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.

4.3.5 Prüfung, Diskussion 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 4.3.1).

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 bzw. per Telefon oder E-Mail (falls seitens der geprüften Einheit auf eine Schlussbesprechung verzichtet wird) abschließend behandelt.

An der Schlussbesprechung nehmen revisionsseitig i.d.R. der Prüfungsleiter, dessen Vorgesetzter sowie der Revisionsleiter (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.

Sofern über einzelne Berichtsaussagen 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 diese Stellungnahme („management response“) auf unterschiedliche Weise im Rahmen der Berichterstattung durch die Interne Revision dokumentiert. Teilweise werden die entsprechenden Stellungnahmen direkt in den Bericht der Internen Revision aufgenommen oder insbesondere bei Dissens zu den Maßnahmen separat dokumentiert und dem Bericht der Internen Revision beigefügt.

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 (vgl. Abschnitt 4.6.5) 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.

4.4 Berichterstattung

- Die Qualität der Berichte ist vor Versand kompetent zu sichern.
- Berichte sind zu genehmigen.
- 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 Vorstandsmitglieder,
- an das für die Interne Revision verantwortliche Vorstandsmitglied sowie dessen Stellvertreter,
- an Einheiten mit berechtigtem Interesse (Kontrollfunktionen)
- an den Wirtschaftsprüfer der Bank (auf Nachfrage).

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

- Verteilung des Berichtes an den Gesamtvorstand.

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

- den Gesamtvorstand umgehend.

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

- umgehend den Gesamtvorstand und
- in Absprache mit dem Vorstandsvorsitzenden ggf. den Vorsitzenden des Aufsichtsorgans (vgl. Abschnitt. 4.7.3).

Bei Nachschauprüfungen:

- Verteilung an alle Empfänger des ursprünglichen Berichtes,
- bei einer unzureichenden Umsetzung des aufgezeigten Handlungsbedarfs grundsätzlich Verteilung an den Gesamtvorstand.

Schwerwiegende Feststellungen gegen ein Mitglied/Mitglieder des Vorstands

- müssen unverzüglich schriftlich dem Gesamtvorstand berichtet werden.
- Der Vorstand hat den Vorsitzenden des Aufsichtsorgans sowie die Aufsichtsinstitutionen (EZB, BaFin, Bundesbank) unverzüglich zu informieren. Kommt der Vorstand der Berichtspflicht nicht nach oder beschließt keine sachgerechten Maßnahmen, so hat der Revisions-Leiter 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.

Wenn 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.

4.5 Prüfungsnacharbeit

4.5.1 Pflege der Dauerakte/Informationsweitergabe/administrative Tätigkeiten

Die während der Prüfung erzeugten Unterlagen werden abschließend noch einmal gesichtet; dabei werden die für die nächste Prüfung relevanten Dokumente für die Dauerakte kopiert (alternativ im Revisionsmanagementsystem hinterlegt). Die Dauerakte ist in zeitlichem Zusammenhang mit der Prüfung zu aktualisieren.

Vorkommnisse oder Besonderheiten aus der aktuellen Prüfung sollten in der Dauerakte abgelegt 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 weitergeleitet werden.

Sich aus der Prüfung ergebende Vorschläge/Ideen für die Verbesserung von Prüfungsleitfäden sollten im Anschluss an die Prüfung besprochen werden. Dabei ist sicherzustellen, dass bei Abschluss der Prüfung eine Überprüfung/Aktualisierung der genutzten Prüfungsleitfäden 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 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.

Abschließend ist eine neue Risikobewertung der geprüften Prüfobjekte durchzuführen.

4.5.2 Archivierung von Prüfungsunterlagen

Prüfungsunterlagen (papierhaft/elektronisch) müssen zeitnah nach Berichtsverteilung zur Archivierung bereit sein.

Die Revisionsunterlagen werden im Einklang mit den gesetzlichen Bestimmungen im In- und Ausland 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 30 Jahre (wenn die Prüfung externe Ansprüche zum Gegenstand hatte, die nach § 197 BGB erst nach 30 Jahren verjähren),
  Arbeitsunterlagen: Sechs Jahre (gem. BT 2.4 Tz. 6 MaRisk); bei

Sonderuntersuchungen 30 Jahre (wenn die Prüfung externe Ansprüche zum Gegenstand hatte, die nach § 197 BGB erst nach 30 Jahren verjähren),

- Originale von Revisionsberichten für Standardprüfungen 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); bei Sonderuntersuchungen: 30 Jahre (wenn die Prüfung externe Ansprüche zum Gegenstand hatte, die nach § 197 BGB erst nach 30 Jahren verjähren),
- die lokalen, gesetzlichen Aufbewahrungsfristen sind 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 unterschriebene Originalbericht bzw. der im Revisionssystem erzeugte endgültige elektronische Bericht wird archiviert.

Nach Abschluss der Prüfung verbleibt das Prüfungsverzeichnis auf den File-Servern und ist dort weiterhin verfügbar. Zusätzlich werden die elektr. Daten regelmäßig in die Langzeitsicherung überführt (wenn nötig, können diese auch auf CD-ROM gebrannt werden). Bei elektronsichen Arbeitsunterlagen ist darauf zu achten, dass nach Abschluss der Prüfung systemseitig eine nachträgliche Veränderungen der Dateien ausgeschlossen bzw. auf wenige Personen beschränkt und systemseitig protokolliert wird.

4.6 Follow-up

In der Follow-up Phase wird die fristgerechte Umsetzung der mit den geprüften Einheiten zur Beseitigung der Mängel vereinbarten Maßnahmen überwacht. Im Sinne einer Ausrichtung der Revisionsaktivitäten an den Unternehmenszielen gilt an dieser Stelle, dass sowohl die jeweilige geprüfte Einheit als auch die Interne Revision gemeinsame Ziele verfolgen, wobei die Verantwortung für die Umsetzung risikomitigierender Maßnahmen den jeweiligen Linienverantwortlichen obliegt. Schließlich ist es im Interesse aller, bestehende Kontrollschwächen und Prozessmängel zeitnah und effektiv zu beheben.

Die Verantwortung für den Follow-up Prozess und der hieraus resultierenden Berichterstattung obliegt hingegen der Internen Revision. Sie ist dabei unter anderem zuständig für die Begleitung und Unterstützung der geprüften Einheit bei der Mängelbeseitigung durch Überwachung, Nachschauprüfung, Eskalation und Management-Berichterstattung der umgesetzten Maßnahmen. Der Follow-up-Prozess umfasst die nachfolgenden Arbeitsschritte. Zielsetzung sollte im Follow-up-Prozess immer sein, die Angemessenheit und Wirksamkeit der beabsichtigten Risikomitigation zu beurteilen. Eine formale Umsetzung zunächst vereinbarter Maßnahmen kann dann nicht ausreichend für die Erledigung von Maßnahmen sein, wenn das Ziel der Reduktion von Risiken nicht erfolgreich erreicht wurde.

4.6.1 Überwachung des Handlungsbedarfs

- Basierend auf den im Revisionsbericht vereinbarten Maßnahmen und Umsetzungsterminen überwacht die Interne Revision die fristgerechte Umsetzung des Handlungsbedarfs zur Beseitigung der Mängel und ist von den hierfür verantwortlichen Stellen entsprechend zu informieren. Dies 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.
- 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 Firstablauf 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 Interne Revision überwacht und beurteilt die sachgerechte 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 unterschieden, sofern dies in der Maßnahme vereinbart wurde. Von der Umsetzung aller Maßnahmen, unabhängig von der Risikoklasse, hat sich die Interne Revision spätestens im Rahmen der nächsten planmäßigen Prüfung des entsprechenden Prüfungsgebiets zu überzeugen (materielle/inhaltliche Prüfung).
- Die Art und Weise der Überwachung durch die Interne Revision sollte nach Risikogehalt der zugrundeliegenden Feststellung in Umfang und Intensität unterschiedlich gehandhabt werden und kann sich an der Klassifizierung von Feststellungen gemäß Abschnitt 4.3 orientieren. Die Ausgestaltung bzw. Intensität der Überwachungsmaßnahmen für die Beurteilung der ergriffenen Maßnahmen zur Erledigung kann dabei wie folgt abgestuft sein und ist risikoorientiert festzulegen:
  - Die Umsetzung der Maßnahmen wird bis hin zur vollständigen Behebung des Mangels von der Internen Revision in risikoorientiert unterschiedlicher Ausprägung überwacht:
    - es erfolgt eine zeitnahe Nachschauprüfung (vor Ort) aller relevanten Sachverhalte.
    - die Beurteilung erfolgt anhand der erhaltenen Unterlagen bzw. Informationen (Validierung/Plausibilitätsprüfung), ggf. erfolgt eine Nachschauprüfung (vor Ort) einzelner Sachverhalte bzw. in Stichproben.
    - 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.

- Eine zeitnahe und effiziente Umsetzung der korrigierenden Maßnahmen ist unter anderem ein wesentliches Kennzeichen eines funktionierenden Internen Kontrollsystems, deshalb werden Terminverlängerungen grundsätzlich nicht eingeräumt. Daher sind bei der Terminierung der Maßnahmen von vornherein adäquate Fristen zu vereinbaren. Im Ausnahmefall sind notwendige Terminverlängerungen von der 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 Risikomanagement Systems – für die beantragenden Fachbereiche erforderlich werden, die Restrisiken einem kompetenzgerechten Genehmigungsprozess zuzuführen (vgl. Abschnitt 4.6.5).
- Die Interne Revision gibt der geprüften Einheit Rückmeldung bezüglich der Beurteilung der berichteten 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 für eine größere Anzahl von Maßnahmen als gefährdet ansieht. In diesen Fällen initiiert das verantwortliche Management geeignete Maßnahmen zur Sicherstellung einer angemessenen Umsetzung.
- Die Dokumentation der Mängelbeseitigung erfolgt schriftlich durch die geprüfte Einheit (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.

4.6.1.1 Feststellungen mit langfristigem Erledigungsdatum

Feststellungen mit langfristigem Erledigungsdatum (Definition „langfristiges Erledigungsdatum“ ist abhängig von der Risikoklasse der Feststellung) sind im Regelfall dadurch gekennzeichnet, dass ihre Umsetzung in mehreren Abschnitten erfolgt, für die jeweils einzeln abzuarbeitende Meilensteine festgelegt werden (vgl. Abschnitt 4.4.2).

- Für Feststellungen mit langfristigem Erledigungsdatum gelten die bereits genannten Grundsätze und sind auf jeden einzelnen vorher festgelegten Meilenstein sinngemäß anzuwenden. Die Dokumentation der Mängelbeseitigung, Eskalation bzw. die Berichterstattung erfolgen 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 verantwortliche Einheit 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 4.6.5) und ggf. temporär mitigierende Maßnahmen zu ergreifen.

4.6.1.2 Follow-up von Feststellungen aus Prüfungen zu Insourcing, Outsourcing und im Konzerninteresse

- Sofern Einlagerungssachverhalte von der Internen Revision geprüft worden sind, ist jedem Mandanten (Auslagerer) bzw. dessen Interner Revision über den Status der Nachverfolgung zu berichten. Dies gilt analog auch für Feststellungen aus Prüfungen der Konzernrevision in Tochtergesellschaften (auch im Konzerninteresse).
- Sofern Auslagerungssachverhalte von der Internen Revision des Einlagerers geprüft worden sind, hat die Interne Revision des Auslagerers Informationen zur Nachverfolgung einzuholen.

4.6.1.3 Nachverfolgung von Feststellungen des Wirtschaftsprüfers

- Die Interne Revision sollte auch die Feststellungen externer Prüfer aufnehmen und einem zu Revisionsfeststellungen analogen Follow-Up-Prozess unterziehen.
- Mit den verantwortlichen Einheiten sind in Abstimmung mit dem externen Prüfer die zu erledigenden Feststellungen und deren Risikoklassifizierung nach dem Bewertungsschema für eigene Feststellungen der Internen Revision und entsprechende Umsetzungsmaßnahmen und -termine zu vereinbaren und auf Erledigung zu überwachen.

4.6.1.4 Behandlung anderer externer Prüfungsberichte

- Die Organe sollten auf Vorschlag der Internen Revision festlegen, welche 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 und Jahresabschlussprüfungen bewährt.

4.6.2 Nachschauprüfung

- Bei insgesamt mangelhaften Revisionsergebnissen (vgl. Abschnitt 4.3.3) wird die routinemäßige Überwachung der Mängelbeseitigung durch eine Nachschauprüfung unterstützt. Der Zeitpunkt und der Umfang der Nachschauprüfung kann in Abhängigkeit von der Risikobewertung der zugrundeliegenden Feststellungen individuell festgelegt werden, sie sollte jedoch grundsätzlich innerhalb eines halben Jahres nach Abschluss der ursprünglichen Prüfung beginnen.
- 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, für diese Teilbereiche eine Nachschauprüfung anzusetzen.
- Berichte über Nachschauprüfungen mit unzureichender Umsetzung des aufgezeigten Handlungsbedarfs sollten nicht nur dem verantwortlichen Management, sondern zusätzlich der gesamten Geschäftsleitung vorgelegt werden. Die Leitung der Internen Revision wird die Berichte mit dem jeweils zuständigen Mitglied der Geschäftsleitung behandeln und individuelle Maßnahmen veranlassen.

4.6.3 Eskalation

Für den Fall, dass zu den vereinbarten Fälligkeitsterminen keine Erledigung der Maßnahmen oder 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 zum Gesamtvorstand eskaliert werden. Das Eskalationsverfahren gilt analog auch für nicht akzeptable 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 Gesamtberichts 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.

4.6.4 Management-Berichterstattung zum Umsetzungscontrolling/Follow-up

- Ein 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).

4.6.5 Risikoübernahmen

4.6.5.1 Begriffsbestimmung

Unter Risikoübernahme (risk acceptance) versteht man grundsätzlich die Übernahme von Verantwortung für eingegangene Risiken durch die Geschäftsleitung oder autorisierte Entscheidungsträger bzw. -gremien.

Der IPPF Standard 2500.A1 führt hierzu beispielsweise aus: „Der Leiter der Internen Revision muss ein Follow-up-Verfahren einrichten, mit dem überwacht und sichergestellt wird, dass vereinbarte Maßnahmen wirksam umgesetzt werden oder die leitenden Führungskräfte das Risiko auf sich genommen haben, keine Maßnahmen durchzuführen.“ Des Weiteren fordert der IPPF Standard 2600: „Kommt der Leiter der Internen Revision zu dem Schluss, dass das Management ein für die Organisation nicht tragbares Risiko akzeptiert, so muss der Leiter der Internen Revision diese Sachlage mit den leitenden Führungskräften besprechen. Falls der Leiter der Internen Revision der Auffassung ist, dass die Angelegenheit nicht zufriedenstellend gelöst wurde, muss er die Angelegenheit der Geschäftsleitung bzw. dem Überwachungsorgan vortragen.“

In der Praxis werden drei Konstellationen unterschieden:

1. Der Fachbereich entscheidet unmittelbar mit 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 ist die Risk Acceptance durch den Fachbereich zu beantragen. 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 Risken zuständigen Organisationseinheit weitergeleitet werden und dort überwacht werden. Darüber hinaus sollten die Rahmenbedingungen der jeweiligen Risikoübernahmen im Rahmen von Folgeprüfungen erneut beurteilt werden.

4.7 Gremienberichterstattung

4.7.1 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. 8 gibt einen Überblick zu den Berichtsarten und den Rechtsgrundlagen.

Berichtsart	Adressat	Rechtsgrundlage
Quartalsbericht/ Jahresbericht	Geschäftsleitung	§ 25c Absatz 4a Nummer 3 lit. g KWG bzw. § 25c Absatz 4b Nummer 3 lit g KWG für Institutsgruppen / BT 2.4 Tz. 4 MaRisk
Quartalsbericht/ Jahresbericht	Aufsichtsorgan	§ 25c Absatz 4a Nummer 3 lit g KWG bzw. § 25c Absatz 4b Nummer 3 lit g KWG für Institutsgruppen / 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. 8: Berichtspflichten der Internen Revision und rechtliche Grundlagen

4.7.2 Quartals-/Jahresbericht

4.7.2.1 Quartalsberichterstattung

Mit dem im Rahmen des „Trennbankengesetzes“ eingeführten Absatz 4a des § 25c KWG wurde die quartalsweise Berichterstattung an die Geschäftsleitung verpflichtend und durch eine quartalsweise Berichterstattung der Internen Revision direkt an das Aufsichtsorgan ergänzt. In der Gesetzesbegründung wird aufgeführt, dass damit der zeitliche Abstand dieser Berichterstattung konkretisiert, der Bedeutung der Internen Revision Rechnung getragen und dass mit der Berichtslinie an das Aufsichtsorgan bewusst über die in den MaRisk niedergelegten Regelungen hinausgegangen wird.

Der Gesetzgeber hat Aufbau und Inhalt dieser Berichterstattung nicht spezifiziert. Die Anforderungen an die Quartalsberichterstattung und den Jahresbericht werden in 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 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 Gegenstand der Berichterstattung sein sollen, abzustimmen und den Bericht adressatenorientiert auszugestalten.

Die Pflichtbestandteile der Berichterstattung leiten sich aus den MaRisk (u. a. BT 2.4 Tz. 4 MaRisk) ab: unterjährige Abweichungen 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 Revisionstätigkeit getroffenen Feststellungen. Auf deren Aufnahme kann jedoch verzichtet werden, wenn diese Feststellungen bereits in anderen Berichten – beispielsweise in der Risikoberichterstattung – enthalten sind.

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 oder Deutsche Bundesbank sowie die dort getroffenen wesentlichen Ergebnisse und Feststellungen und die ergriffenen Maßnahmen zu deren Beseitigung. Ob dies Inhalt der Berichterstattung wird, sollte davon abhängen, inwieweit die Geschäftsleitung bereits auf anderem Wege über die Prüfungsergebnisse informiert wurde. Sofern dies bereits erfolgt ist, ist eine Aufnahme in den Vierteljahresbericht nicht nötig. Allerdings bietet es sich in diesem Falle an, den aktuellen Umsetzungsstand (Follow-up) zu diesen Feststellungen in die Vierteljahresberichterstattung aufzunehmen.

Folgende Übersicht gibt einen Überblick über die Berichtsinhalte der Quartalsberichterstattung an Geschäftsleitung und Aufsichtsorgan:

Bestandteile der Berichterstattung
Übersicht über die durchgeführten Prüfungen der Berichtsperiode, ggf. Nennung berichtenswerter Prüfungsergebnisse
Wesentliche unterjährige Abweichungen 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. im Risikobericht – enthalten

Abb. 9: Bestandteile der Berichterstattung an Geschäftsleitung und Aufsichtsorgan gemäß § 25c KWG in Verbindung mit BT 2.4 Tz 4 MaRisk

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
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 of defense“*
Beurteilung der „2nd line of defense“*
Wesentliche Verluste und Schäden
Glossar

* Vgl. hierzu das „Three lines of defense Modell“, z. B. anhand des IIA Position Paper: „The Three Lines of Defense in effective Risk Management and Control“ (Januar 2013)

Abb. 10: Weitere mögliche Berichtsinhalte für die Quartalsberichterstattung

Eine andere Option der Berichterstattung an das Aufsichtsorgan ist die Weiterleitung des Vierteljahresberichtes für die Geschäftsleitung an das Aufsichtsorgan durch die Geschäftsleitung selbst, soweit die weitergeleiteten Informationen deckungsgleich und keine nennenswerten Verzögerungen bei der Weiterleitung entstehen.

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

- festgestellte schwerwiegende und nicht behobene wesentliche Mängel,
- ergriffene Maßnahmen hierzu und
- 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. In jüngster Zeit wurden von externen Prüfern und der Aufsicht vermehrt „thematische Analysen“ der offenen Feststellungen in der Berichterstattung gefordert, die über die rein quantitative Darstellung hinausgehen. Das können – nach Entscheidung des jeweiligen Instituts – qualitative Schlussfolgerungen, die auf Konzentrationen, Trends oder ähnliche Phänomene hinweisen, sein.

Eine Differenzierung der Jahresberichterstattung an Geschäftsleitung und Aufsichtsorgan erfolgt nicht.

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. Der Quartalsbericht sollte in diesem Fall um einen Ausblick auf den Jahresplan für das Folgejahr (unabhängig vom formalen Genehmigungsprozess) ergänzt werden.

4.7.3 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 IPPF Standard 2600 ergibt sich eine weitere Ad-hoc-Kommunikationspflicht des Revisionsleiters. Sie kommt dann zum Tragen, wenn der Revisionsleiter auf Grund von Prüfungsergebnissen oder auf Grund der Abarbeitung der Feststellungen der Ansicht ist, dass das Unternehmen zu hohe Risiken eingeht. 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.

5 Continuous Auditing / Continuous-Risk Assessment

5.1 Vorbemerkung

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.

Einzelheiten zur Einführung, Umsetzung und den Auswirkungen eines Continuous Auditing werden nachfolgend skizziert.

5.2 Begriffsbestimmung und Abgrenzung

Zunächst ist eine Definition der inhaltlich stark verwandten Begriffe Continuous Monitoring (CM) und Continuous Auditing (CA) notwendig, um die praktischen Zusammenhänge klarer herauszuarbeiten.[10]

- 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.

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

Die methodischen Bestandteile des Continuous Auditings lassen sich in Continuous Controls-Assessment (CCA) und Continuous-Risk-Assessment (CRA) unterscheiden. Das CCA bewegt sich grundsätzlich näher am Continuous Monitoring und beschreibt die Bewertung der Wirksamkeit der wesentlichen Bestandteile des Internen Kontrollsystems. Das CRA 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.

5.3 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 CA 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:

- 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.

5.4 Rahmenbedingungen

Für ein effektives CA 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 sowohl von CM als auch von CA. Hierzu sei beispielhaft auf das international anerkannte Regelwert 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. Näheres hierzu ist den Abschnitt 3.6 (COSO) und 4.1.1.1 (Prüfungsuniversum) dieses Handbuches zu entnehmen.

5.5 Bestandteile des Continuous Auditing

5.5.1 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-Risiko-Indikatoren – KRI und Key-Performance-Indikatoren – KPI) aus verfügbaren und ggf. selbst verdichteten Datenquellen fortlaufend ausgewertet und überwacht werden.

Bestandteile des CA

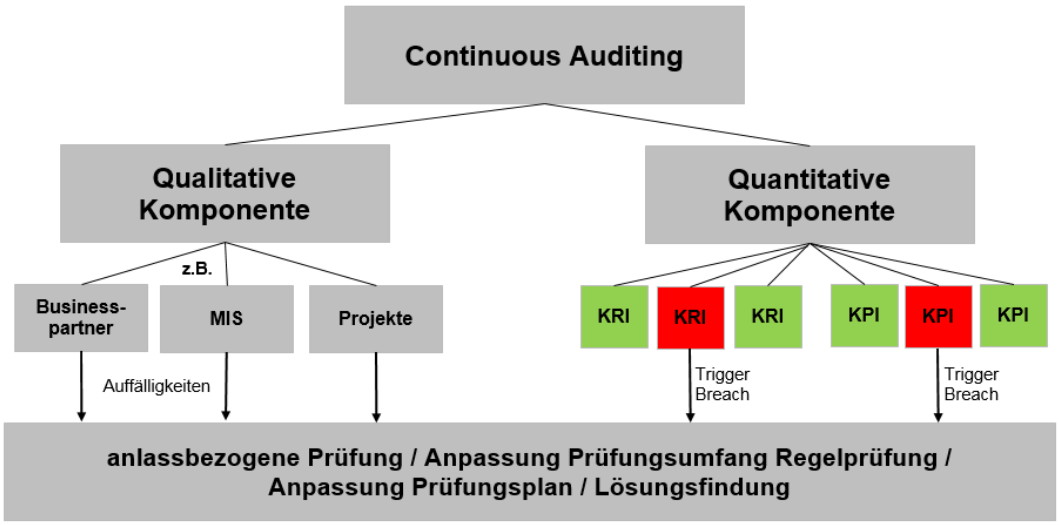


Abb. 11: Bestandteile des Continuous Auditings

5.5.2 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 CA-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:

- IR benötigt umfassendes Prozessverständnis
- IR-Mitarbeiter 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

5.5.3 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. Es ist zu hinterfragen, welche IT-Systeme den Geschäfts-, Kontroll- oder Steuerungsprozessen der Prüfobjekte dienen. 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- und Risikoindikatoren. 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 Risikoindikatoren in das CM 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 Revisionsmitarbeitern schnell Transaktionen mit ähnlichen Parametern zu erkennen und daraufhin die markierten Transaktionen nachzuverfolgen.

Sicherstellung der Datenqualität

Die Datenqualität ist von wesentlicher Bedeutung für den reibungslosen Ablauf des Continuous Auditing. Zur Sicherstellung der Datenqualität sind sowohl vom Analysten 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 Feldausprägungen 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 Analysten, 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 Feldausprägungen eindeutig?
- Sind Sonderausprägungen /-fälle berücksichtigt?
- Ist während der Verarbeitung die Unveränderbarkeit der Rohdaten sichergestellt?

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?
- Sind die Daten veränderbar?
- Ist während der Verarbeitung die Unveränderbarkeit der Rohdaten sichergestellt?

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 der zu prüfenden Objekte, Prozesse oder Funktionen. Insbesondere diejenigen Mitarbeiter 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 Transaktionen einschließlich der zugrundeliegenden Systeme und Funktionalitäten.

Mit den erworbenen Kenntnissen aus Prüfungshandlungen und dem qualitativen Ansatz ist es nun die Aufgabe aussagekräftige Performance- und Risikoindikatoren 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.

5.6 Management des Continuous Auditing

5.6.1 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 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 im Mitgliederbereich des DIIR-Net verfügbar. In der Tabelle können die Zuständigkeiten festgelegt und Hinweise sowie Erkenntnisse zur weiteren Nutzung im Continuous Auditing eingetragen werden.

5.6.2 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

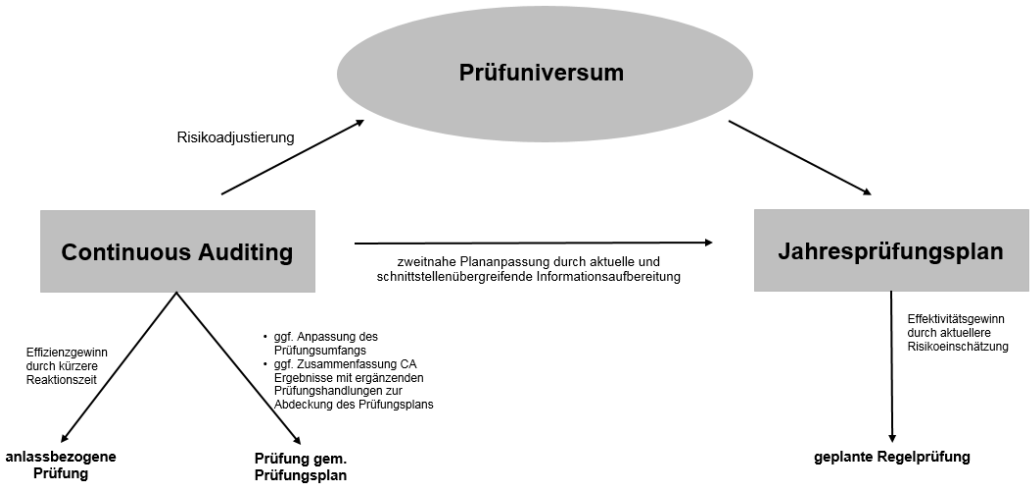


Abb. 12: Zusammenspiel von Prüfuniversum, CA und Jahresprüfplan

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 CA hier die effektive Identifikation von zu prüfenden Einheiten und verkürzt dabei die insgesamt notwendige Vorbereitungszeit.[11]

5.6.3 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.

Wie zuvor dargestellt, benötigt die Interne Revision einen erhöhten Umfang an Information und Daten von den Fachbereichen. Die zentrale Aufgabe besteht hierbei darin Ziel, Zweck und Vorteile dieser Vorgehensweise im Rahmen des Business Partner Ansatzes zu vermitteln. Leicht könnte sonst bei den Fachbereichen der Eindruck entstehen, dass

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

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 unverzüglich „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.

6 Prüfung von Auslagerungen

6.1 Vorbemerkungen

Nachfolgend wird die Umsetzung der nach MaRisk bestehenden Pflicht zur Prüfung ausgelagerter Aktivitäten und Prozesse durch die Interne Revision beschrieben. Generell sollte die Interne Revision dabei auf den etablierten Prozessen zum Management von Auslagerungsvorhaben und bestehenden Auslagerungsbeziehungen aufsetzen.

6.2 Handlungsrahmen nach MaRisk

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.

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.

Bei **nicht wesentlichen Auslagerungen** 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 der Revisionsfunktion 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.

Daneben kann die Interne Revision im Rahmen ihrer Revisionshandlungen auch auf Nachweise/Zertifikate auf Basis gängiger Standards (z. B. IDW PS 951 Typ 2) 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 gewährleisten:

- 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.

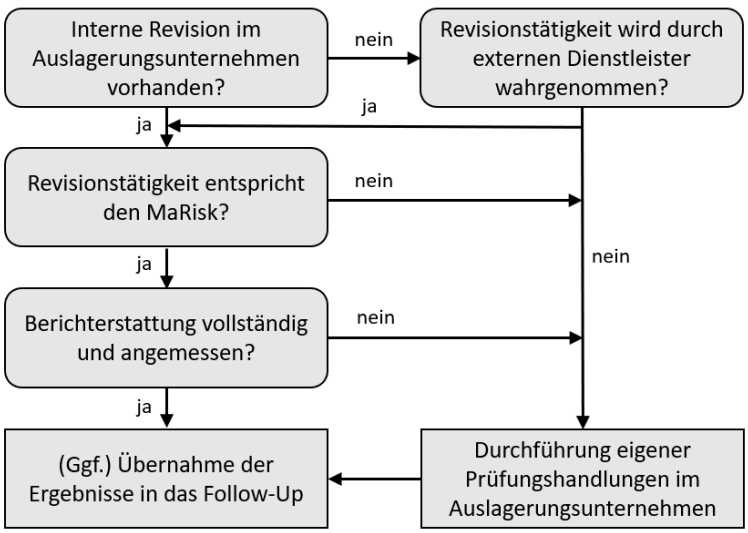
Das Ergebnis der Beurteilung ist nachvollziehbar zu dokumentieren. Bei **wesentlichen Auslagerungen** kann sich die Interne Revision dabei nicht ausschließlich auf Nachweise/Zertifikate auf Basis gängiger Standards stützen. In diesem Fall sind z. B.

ergänzend Prüfungen der Auslagerungssteuerung und -überwachung, analytische Prüfungshandlungen zur Qualität der erbrachten Leistung oder ggf. Vor-Ort-Prüfungen denkbar.

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

Verfügt bei wesentlichen Auslagerungen das Auslagerungsunternehmen 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.

Der seitens der Internen Revision durchzuführende Entscheidungsprozess für **wesentliche** Auslagerungen im Hinblick auf die Notwendigkeit eigener Prüfungshandlungen kann nachfolgendem Schaubild entnommen werden:



[12])

Abb. 13: Notwendigkeit eigener Prüfungshandlungen

6.3 Prüfung ausgelagerter Aktivitäten und Prozesse

Unternehmen, die wesentliche Dienstleistungen für das Institut erbringen, sind grundsätzlich im Drei-Jahres-Turnus, ggf. auch Vor-Ort, zu prüfen. Die wesentlichen Auslagerungen sind zu diesem Zweck in die Prüfungsplanung aufzunehmen und mindestens jährlich bzw. anlassbezogen auf Vollständigkeit zu prüfen. Dabei ist es unerheblich, ob

[12] Vgl. DIIR Arbeitskreis „MaRisk“, ZIR 3/2008, Seite 128.

die ausgelagerten Aktivitäten und Prozesse bei einer Prozessprüfung hinterlegt werden, oder das Auslagerungsunternehmen als eigenes Prüfobjekt geführt wird.

Als nicht wesentlich qualifizierte Auslagerungen müssen aufgrund des geringeren Risikogehalts grundsätzlich nicht als separates Prüfobjekt in die Prüfungsplanung aufgenommen werden. Sie sind jedoch spätestens bei der Aufstellung des Prüfungsplans 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 für die Revisionstätigkeit kann sich die Interne Revision auf die Prozesse des Auslagerungsmanagements und das zentral geführte Auslagerungsregister stützen. Zumindest einmal jährlich im Rahmen der Prüfungsplanung ist ein Abgleich zwischen dem Auslagerungsregister und den Prüfobjekten der Internen Revision durchzuführen. Nach Aufstellung des Prüfungsplans und dessen Genehmigung durch die Geschäftsleitung sind die für das Planjahr vorgesehen 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). Dabei ist die Nennung des jeweiligen Prüfungsjahres regelmäßig ausreichend. Aus dem Protokoll zur MaRisk-Fachgremiumssitzung vom 04.03.2021 geht hervor, dass die entsprechende Information nicht erfasst werden muss, wenn der Termin der Prüfung, z. B. aus dem Prüfungsplan heraus, nicht bekannt ist.

6.3.1 Neuauslagerung wesentlicher Aktivitäten und Prozesse

Die Interne Revision ist im Rahmen ihrer Aufgaben an der der Auslagerung vorgeschalteten Risikoanalyse zu beteiligen (AT 9, Tz. 2 MaRisk). 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 im Rahmen des Auslagerungsprozesses sicherzustellen, dass der Internen Revision vertraglich angemessene Informations- und Prüfungsrechte zugesichert werden (AT 9 Tz. 7 h) MaRisk). Dies gilt auch im Fall von wesentlichen Weiterverlagerungen durch das Auslagerungsunternehmen.

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.

6.3.2 Durchführung eigener Prüfungshandlungen beim Auslagerungsunternehmen und Berichterstattung

6.3.2.1 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 ist grundsätzlich vorzusehen, dass zumindest im Drei-Jahres-Turnus eine Prüfung, ggf. vor Ort, stattfindet. Sofern der Einbezug in eine Prozessprüfung nicht sinnvoll erscheint, kann für wesentliche Auslagerungen 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 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.

6.3.2.2 Sonderfall „Pooled Audits“

Insbesondere im Zusammenhang mit wesentlichen Auslagerungen an Cloud Service Provider (Microsoft, Amazon, Google, …) besteht die Möglichkeit, eigene Prüfungshandlungen durch gemeinschaftliche Prüfungshandlungen der ausgelagerten Aktivitäten und Prozesse mit anderen Instituten (Pooled Audits) durchzuführen. Die beteiligten Institute steuern festgelegte Prüfungskontingente bei und stimmen die Prüfungsinhalte und -durchführung untereinander ab. Im Gegenzug können die jeweiligen Prüfungsergebnisse von den beteiligten Instituten gemeinschaftlich verwendet werden.

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

6.3.3.1 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.

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 auslagerten 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 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) in Bezug auf die auslagerte 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 im Mitgliederbereich des DIIR-Net verfügbar sind.

6.3.3.2 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** 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.

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 eingestufter 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 in Maßnahmen des Auslagerungsmanagements an den Vorstand 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 die Quartals- und Jahresberichterstattung 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 lediglich 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.

6.3.3.3 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.

6.3.4 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 Beauftragten 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).

Der Revisionsbeauftragte übernimmt somit 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 der InstitutsVergV für Kontrolleinheiten.

7 Begleitung wesentlicher Projekte / Anpassungsprozesse

7.1 Projektbegleitende Prüfungen durch die Interne Revision

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.

Zur Identifizierung „wesentlicher Projekte“ ist Voraussetzung, dass die Interne Revision auf der Basis eines etablierten Prozesses von neuen und geplanten Projekten bzw. Vorhaben Kenntnis erlangt. 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 des Instituts,
  - die regulatorische Relevanz der Projektinhalte,
  - die fachliche/organisatorische Komplexität der Projektumsetzung,
  - 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 hinterfragen.

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

- Informatorische Einbindung in ein Projekt bzw. Vorhaben 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 oder durch schriftliche Entäußerung von Ergebnissen aus revisorischen Analysen des Projektes (vgl. Abschnitt 2.6, insbesondere hinsichtlich der zu wahrenden Unabhängigkeit)
    - Ziel: Beratung des Projekts z. B. hinsichtlich Auswirkungen auf das Interne Kontrollsystem, Ausgestaltung des Projektmanagements
- (Projektbegleitende) 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 Organisation des Projekts (z. B. Einrichtung von Gremien, Aufgaben / Rolle der Projektbeteiligten sowie eines Projektmanagement-Office), die etablierten projektinternen Prozesse (z. B. laufende Risikoinventur und damit verbundenes Projektrisikomangement, Budgetüberwachung, Entscheidungs- / Qualitätssicherungsprozesse, Kommunikationswege und Berichterstattung, Eskalationswege) sowie die zeitliche und inhaltliche Projektplanung (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.

Die bei der Erreichung des Projektziels zu erfüllenden technischen / fachlichen Anforderungen können Gegenstand einer inhaltlich orientierten projektbegleitenden 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.

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.

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.

7.2 Einbindung der Internen Revision in Anpassungsprozesse (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 / auf neuen Märkten (Neu-Produkt-Prozess AT 8.1 MaRisk) sowie
- Änderungen betrieblicher Prozesse und Strukturen (AT 8.2 MaRisk).

Die Bezugnahme auf die Aufgaben der Internen Revision stellt dabei insbesondere auf die Unabhängigkeit der Internen Revision ab. Durch die unternehmensinternen Regelungen sollte sichergestellt sein, dass die Interne Revision keinen direkten Einfluss auf die Entscheidungsfindung, bspw. über ein Stimm- oder Vetorecht, zur Umsetzung der Anpassungen besitzt. Die Rolle der Internen Revision ist daher i.d.R. als beratende Funktion einzustufen.

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 eine Rückmeldung zur technischen / fachlichen Umsetzung geschaffen werden. 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. Erweiterungen/Veränderungen des Prüfungsuniversum abzuleiten.

Da Art und Umfang der in einem Geschäftsjahr initiierten Anpassungsprozesse im Rahmen der Jahresplanung nur schwer abzuschätzen sind, sollte auf Basis von Erkenntnissen aus Vorjahren bzw. aktuellen Ereignissen Kapazitätspuffer für die Begleitung durch die Interne Revision hinterlegt werden. Weiterhin sind die Anpassungsprozesse nach AT 8 MaRisk als Prüfungsgegenstand in das Prüfungsuniversum der Internen Revision zu integrieren.

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.

8 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 gewinnen agile Methoden auch in Kreditinstituten an Bedeutung. Während keine einheitliche Definition für „agiles Projektmanagement“ existiert, umfasst dieses in den Unternehmen häufig eine Kombination aus agilen Vorgehensmodellen, Rollen und Werten, wobei letztere sich im sogenannten „Agilen Manifest“ widerspiegeln. Mit agilen Methoden erfolgt die Steuerung von Projekten und Prozessen dynamisch und flexibel, um auf erforderliche Änderungen, z. B. am gewünschten Endprodukt, schnell reagieren zu können. Während bei nach „klassischen Methoden“ (z. B. Wasserfall) durchgeführten Projekten die Projektziele stabil, Termine und Kosten jedoch eher flexibel sind, sind bei agilen Projekten eher die Ziele flexibel. Der Kunde erhält beim agilen Projektmanagement von Beginn an Ergebnisse („Minimum Viable Product“, „MVP“) und erhält die Möglichkeit, durch den stetigen Austausch mit dem Projektteam, das MVP weiterzuentwickeln.

Agilität zeigt sich oft in der Nutzung von Tools wie z. B. Kanban Boards, in der Durchführung von Daily standups und Implementierung von agilen Organisationsformen (z. B. Tribes mit Chapters und Squads). Dieses sind greifbare Erkennungsmerkmale von Agilität, jedoch steht und fällt Agilität mit der entsprechenden Haltung (Mindset) und einem entsprechenden Führungsverständnis.

Generell erlaubt eine agile Arbeitsorganisation den Mitarbeitern eine hohe Eigenverantwortung und damit Autonomie im Rahmen des jeweiligen Ziels (z. B. Squad Ziel), auf das die Tätigkeiten der Mitarbeiter ausgerichtet sind. Innerhalb der Einheit (z. B. Squad) herrscht Transparenz über die Tätigkeiten des Einzelnen. Damit einhergehend verändern sich Führungsstrukturen hin zu flacheren Hierarchien und die Führungskräfte wirken eher unterstützend als direktiv. Sie setzen Ziele und Aufgaben und im gesetzten Rahmen entscheidet das Team eigenverantwortlich über Priorisierung und Lösungswege. Die Führungskräfte unterstützen lediglich bei auftretenden Problemen und Konflikten.

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

8.1 Prüfung von agilen Organisationsstrukturen durch die Interne Revision

Die grundlegende Herausforderung für eine Interne Revision in einem agil aufgestellten Unternehmen, ist, unabhängig von der Anwendung agiler Prüfungsmethoden, die Erlangung eines detaillierten Verständnisses über Agilität. Dieses umfasst neben der Kenntnis von Tools, Methoden und agilen Organisationsstrukturen (Tribes, Squads, Circles) auch ein Verständnis des Agilen Manifests und der damit verbundenen Haltung (Mindset). Idealerweise sollten der Internen Revision hierfür Agile Coaches zur Seite gestellt werden, die sowohl Wissen vermitteln als auch im Detailverständnis helfen.

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 bald überholt sein kann. 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. Das Ergebnis ist eine weitgehend dynamische Planung, 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 (vgl. Abschnitt 9.2), 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, wie z. B. Squads in einem Tribe, 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 Prozess-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. Diese werden daher 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.

In der Zusammenfassung ergeben sich folgende Anforderungen an die Interne Revision in einem nach dem agilen Manifest aufgestellten Unternehmen:

- Flexibilität in der Planung (rollierende Planung in kürzeren Zyklen)
- Fokus auf eher kleinteilige Prüfungsgebiete
- Stetiger Austausch mit den geprüften Bereichen
- Transparenz in der Zusammenarbeit
- Schnellere Kommunikation der Ergebnisse
- Zunehmende Bedeutung von Continuous Auditing, Data Analytics und Business Monitoring.

8.2 Nutzung agiler Prüfungsmethoden durch die Interne Revision

In einem agilen Umfeld ist die Anwendung agilem 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
- eine zielgenauere Risikoorientierung der Prüfungshandlungen (Fokus auf die höchsten Risiken)
- eine erhöhte höhere Zufriedenheit der Teammitglieder durch erhöhte Eigenverantwortung und Handlungsspielräume
- eine schnellere Lieferung und Kommunikation von Prüfungsergebnissen
- eine kürzere Prüfungsdauer
- ein intensiverer Austausch/Kommunikation mit den geprüften Einheiten (Kundennähe).

Hierzu erfolgt die Übertragung von in anderen Branchen bewährten Methoden auf die Durchführung von Revisionsprüfungen. Die wesentlichen Unterschiede lassen sich wie folgt darstellen[13]:

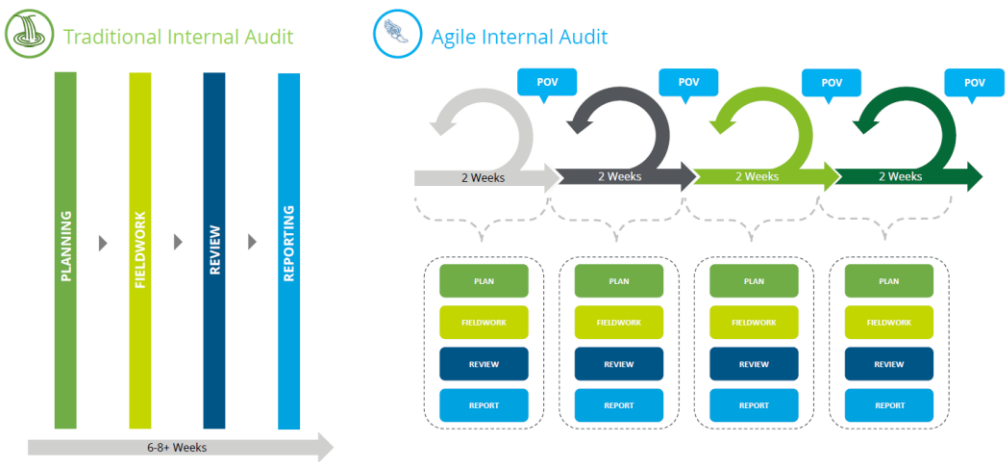


Abb. 14: Traditional vs. Agile Internal Audit[14]

In der „klassischen“ Prüfungsdurchführung werden alle Themengebiete des Prüfungsumfangs parallel in den Phasen der Prüfung bearbeitet, z. B. gleichzeitige Durchführung von Prozessaufnahmen in verschiedenen Themenbereichen. Hierdurch können erst nach der

[13] Quelle: Deloitte

[14] vgl. ebd.

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 (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.

In der agilen Prüfung werden neue Rollen vergeben. Die Aufgaben der Prüfungsleitung (einer klassischen Prüfung) werden auf den Product Owner, den Scrum Master und das Prüfungsteam (auch Scrum Team) verteilt.

Jeder agilen Prüfung wird ein Product Owner und ein Scrum Master zugeordnet, die gemeinsam die Führung des Prüfungsteams im Rahmen der Prüfung übernehmen. Beide sind u. a. für die Vorbereitung, die Organisation und Durchführung sowie die Steuerung

des Prüfungsteams der jeweiligen Prüfung und das Erstellen des Prüfungsberichtes verantwortlich (zur vollständigen Erfüllung des jeweiligen Prüfungsziels).

Der Audit Product 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 Scrum 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 Product Owner.

Das Audit Scrum 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 Scrum Master löst es mögliche Hindernisse und Blockaden für den Prüfungsfortschritt. Das Team nimmt aktiv an den täglichen Scrum Meetings teil und überprüft die Arbeitsergebnisse.

Gleichzeitig bietet es sich an, gerade bei der Einführung von agilen Projektmethoden in der Prüfungsdurchführung, das Team durch einen Agile Coach zu unterstützen. Dieser unterstützt den Scrum Master, Product Owner und das 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 Product Owner und Scrum Master, die Arbeitspakete zu priorisieren und den Audit backlog zu managen.

Grundsätzlich lässt sich sagen, dass die Nutzung von agilen Methoden in der Prüfungsdurchführung eine andere Denk- und Herangehensweise erfordert und die Einführung dieser Methoden durch „Agile Coaches“ und spezifische Schulungsmaßnahmen der Mitarbeiter der Internen Revision unterstützt werden sollte. Gleichzeitig empfiehlt sich die Nutzung von entsprechenden Tools, die ein gemeinsames Arbeiten und schnelleren Austausch von Informationen im Prüfungsteam unterstützen, z. B. OneNote und die Durchführung von Standups im Team.

Bei der Einführung von agilen Prüfungsmethoden empfiehlt es sich darüber hinaus, vor Beginn der Prüfung im Rahmen des „Kick-off-Meeting“ (vgl. Abschnitt 4.2.7) die Vorgehensweise der Internen Revision und die Organisation der Prüfung zu präsentieren.

Hierbei sollten auch die Anforderungen an die gemeinsame Zusammenarbeit (z. B. Lieferfristen für Unterlagen) vereinbart werden.

Wenngleich nicht jede Prüfung für den Einsatz von agilen Methoden prädestiniert ist, zeigen die bisherigen Erfahrungen, dass diese Prüfungsmethoden wertstiftend sind und sich einzelne Tools (z. B. die täglichen Meetings) auch auf andere Bereiche der Revisionsarbeit überragen lassen.

8.3 Abschließende Bewertung

Bezüglich der Umsetzung agiler Arbeitsmethoden und agiler Prüfungsansätze zeigt sich derzeit noch ein heterogenes Bild in der Internen Revision. Ob sich agile Herangehensweisen als Standards für Prüfungen herausbilden, ist derzeit noch nicht abzusehen. Daher ist dieser Abschnitt im Sinne eines Schlaglichtes auf den aktuellen Status zu verstehen.

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 Mitarbeitern der Internen Revision sowie eine noch fokussiertere Ausrichtung der Prüfungstätigkeiten an den Risiken der Bank und dem Risiko-Appetit der Geschäftsleitung. Dies gilt auch 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).

9 Digitalisierung der Prüfungsprozesse (inkl. Durchführung von Remoteprüfungen)

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

Im Rahmen dieser Überprüfung und Weiterentwicklung gewinnt das Thema Digitalisierung der Internen Revision eine zunehmende Bedeutung. Digitalisierung meint dabei den Ersatz manueller Prozessschritte durch Softwarelösungen.

Bei der Digitalisierung der internen Revision ist zu unterscheiden zwischen:

- der Digitalisierung der Revisionsprozesse sowie
- der Digitalisierung von Prüfungsmethoden.

9.1 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 Digitalisierungsansätze 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“,
  d. h. die Umstellung der früher papiergebundenen Revisionsdokumentation auf elektronische Medien (z. B. auf eine elektronische Prüfungsakte).
  => Diese Umstellungsphase „paperless office“ haben die Internen Revisionen überwiegend durchlaufen.
- 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. Wir empfehlen, bei Einsatz einer Standardsoftware - soweit möglich -

von einem Customizing abzusehen, um Releasewechsel ohne größeren Aufwand vornehmen zu können.

Der Einsatz von „Collaborative-Tools“ (z. B. Microsoft Teams), um auch online zusammenarbeiten zu können, ermöglicht einen weitgehend reibungsfreien Wechsel zwischen Remote- und Vor-Ort-Prüfungen und verkürzt Rüstzeiten bzw. verringert Transaktionskosten. Dabei sind die relevanten Rahmenbedingungen zu beachten (z. B. Informationssicherheit, Datenschutz).

=> „Workflow-Tools“ (in unterschiedlichen Ausprägungsgraden) und „Collaborative-Tools“ finden in den meisten Internen Revisionen der Kreditinstitute Anwendung.

- Ausblick: Vollständige, digitale Integration:
  Die Erfahrungen im Rahmen der Corona-Pandemie haben gezeigt, dass digitale Integration immer mehr an Bedeutung gewinnt. Vor diesem Hintergrund ist es wichtig, Revisionssysteme in Richtung Kollaborationsfähigkeit und Prüfungsmethodik weiterzuentwickeln.

  Zudem kann durch eine digitale Integration unternehmensweiter Daten die Effektivität und die Effizienz der Internen Revision weiter gesteigert werden.
  => Hier besteht noch Handlungsbedarf. Insofern haben wir diese Phase als Ausblick dargestellt.

9.2 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. auf die Anforderungen der BAIT zur Individuelle Datenverarbeitung beachtet werden.

Weiterhin stehen 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.

9.2.1 Datenanalysen

9.2.1.1 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 Voraussetzungen für die Etablierung/Durchführung von Datenanalysen sind z. B. entsprechend ausgebildete Mitarbeiter, Zugriffe auf Datenbestände, ausreichende Anzahl von Softwarelizenzen sowie entsprechende zeitliche Möglichkeiten.

9.2.1.2 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.

9.2.1.3 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.

9.2.2 Weitere Digitalisierungsansätze

Zur Effizienzsteigerung sollten die Datenanalysen auch durch „Prozess Scheduler“ oder Robotik Prozess Automation (RPA) unterstützt werden.

Weiterhin sollten man über den Einsatz von künstlicher Intelligenz für die Datenanalysen nachdenken, um Muster zu erkennen, an die die Fachprüfer oder der Datenanalyst nicht gedacht haben oder, die vollkommen neue Prüfungsideen hervorbringen.

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. Die Visualisierung kann auf verschiedenen Ebenen erfolgen und z. B. 80%, 90% oder 95%, im besten Fall 100% der Prozessdurchläufe (Transaktionen) umfassen. Dabei gehen die derzeitigen Tools grundsätzlich so vor, dass die Transaktionen anhand der Anzahl von Abweichungen zum Standardprozess sortiert werden. Der Standardprozess wird dabei statistisch als die Transaktion definiert,

die am häufigsten vorkommt. Damit sammeln sich die Transaktionen mit den meisten Abweichungen in den letzten 5 bis 10% aller Transaktionen. Die Visualisierung wird erfahrungsgemäß immer differenzierter und komplexer, je mehr Transaktionen man einbezieht. Process Mining verwendet Event-Logs der Prozesse. Anhand dieser „Zeitstempel“ und einer eindeutigen ID können der Zusammenhang und die Reihenfolge von Prozessschritten erfasst werden. Bei Prozessen, die in mehreren Systemen abgebildet sind, müssen die Transaktionen also anhand von übergreifenden IDs eindeutig identifizierbar sein. Dies ist bei einer heterogenen IT-Landschaft, die in den meisten Banken üblich ist, nicht immer gegeben. Sie stellt jedoch die Mindestvorrausetzung für das Process Mining dar, um die Prozessschritte in die in der Realität aufeinanderfolgenden Reihenfolge abbilden zu können. Selbstverständlich können in einem Data Warehouse solche IDs vergeben werden, es bietet sich also als Grundlage für Process Mining an, solange auch die Event-Logs der Quellsysteme dort gespeichert werden.

9.3 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 10).

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 hilfreich.

9.4 Durchführung von Remote-Prüfungen

Digitale Prozesse und Arbeitsmethoden führten vor dem Hintergrund der pandemischen Lage zu einer deutlichen Ausweitung von Remote-Prüfungen[15]. Im Folgenden werden praxisorientierte Überlegungen, wie Revisionseinheiten Remote-Prüfungen zusammen mit ihren Risikopartnern (geprüfte Bereiche) sowie weiteren Stakeholdern mehrwertbringend einsetzen können dargestellt. Dazu wird ein Ausblick gegeben, welche Chancen sowie Risiken Remote-Prüfungen bieten und wie sich die Remote-Prüfung als zukunftsfähige Prüfungsart bzw. -methodik weiterentwickeln kann.

[15] Im Arbeitskreis MaRisk haben sich 20 Revisionseinheiten namhafter Unternehmen mit dem Status-Quo von Remote-Prüfungen in der Praxis beschäftigt. Grundlage war eine Expertenbefragung mittels 17 offener Fragen in Anlehnung an den Fachbeitrag von Prof. Dr. Eulerich (Remote-Auditing Chancen und Herausforderungen in der Durchführung von Remote-Audits, DIIR Fachbeitrag Nr. 3 vom 18.09.2020).

9.4.1 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 entweder aus dem Home-Office oder einem anderen abweichenden Arbeitsort als dem Standort des geprüften Bereichs verstanden. 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 Revisionseinheit[16] variieren.

9.4.2 Umsetzung von Remote-Prüfungen

Grundsätzlich können alle Prüfungen mit wenigen Ausnahmen (z. B. räumliche Begehungen, physische Aufnahme, „Fraud-Interviews“) mittels remote-Prüfungstechniken durchgeführt werden. Herausforderungen ergeben sich in der praktischen Umsetzung für die beteiligten Bereiche insbesondere durch die Besonderheiten bei der Kommunikation und der Vorbereitung sowie Abwicklung der Prüfung.

Bei der risikoorientierten Festlegung des Prüfungsschwerpunkts ist zu bewerten, wie sich eine ggf. geringere Prüfungssicherheit durch die Remote Prüfung mit dem identifizierten Risiko verträgt. Insoweit sind auch Prüfungshandlungen in Betracht zu ziehen, die vor Ort ausgeführt werden sollten. Beispielsweise eigenen 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 hat[17].

Unter Berücksichtigung des Umstands, dass die räumliche Trennung die Beschaffung von relevanten Informationen erschweren kann, ist bei der Prüfungsvorbereitung intensiv

[16] Siehe S. 3, Prüfen in Covid-19 Zeiten, Ein Erfahrungsbericht aus der Prüfungspraxis der DAX 30 Unternehmen, Ralf Herold, Oktober 2020.

[17] Vgl. Seite 4, Remote-Auditing Chancen und Herausforderungen in der Durchführung von Remote-Audits, DIIR Fachbeitrag Nr. 3 vom 18.09.2020).

auszuarbeiten, welche Dokumente bzw. Unterlagen und welche Datenauswertungen benötigt werden.

Durch die Nutzung digitaler Medien findet die Prüfung über Videokonferenzen und Chats statt. Dabei sollten zusätzlich kollaborative Tools (wie z. B. MS Teams) zur unterlagengestützten, veranschaulichenden Gesprächsführung und zur online-Einsichtnahme in Anwendungen und Dokumente genutzt werden. Zu Beginn einer Telefon- oder Videokonferenz sollte mit ein paar persönlichen Worten die Gesprächsatmosphäre entspannt werden, um so den fehlenden persönlichen Kontakt zu kompensieren. Es sollte dabei ein besonderes Augenmerk auf eine gute Vorbereitung der Termine liegen und bestenfalls vorab geklärt werden, welche Regeln und Zuständigkeiten für die Durchführung der digitalen Besprechung gelten. In der Praxis hat sich als wichtig herausgestellt, die Kamera dauerhaft einzuschalten und sich vorab zu vereinbaren, ob und wie die Chatfunktion genutzt werden soll.

Der Prüfungsplan sollte in einer Interaktion zwischen Prüfer und Geprüften durchgearbeitet werden, die Prüfungsfragen können dabei entweder vorab bereitgestellt oder über eine Agenda entsprechend vorgestellt und eingeleitet werden. Für den direkten und verbindlichen Austausch mit der geprüften Stelle hat sich die Nutzung von sogenannten digitalen Audit Logs bewährt. Es handelt sich um ein Tagebuch, in dem die Beobachtungen der Prüfer aktuell und zeitnah gespeichert und mit dem Management des geprüften Bereichs geteilt werden. Das Audit Log dient später als abgestimmtes Dokument für die Status-Meetings sowie als Grundlagendokument der Feststellungen.

9.4.3 Vorteile und Chancen

Die Nutzung von Remote-Techniken kann bei einer guten Planung und Strukturierung sowie einer disziplinierten Durchführung der Sitzungen zur Effizienzsteigerung beitragen. Durch die erhöhte Flexibilität in der Terminierung können Geschwindigkeit und Frequenz des Austauschs mit den geprüften Einheiten gesteigert werden. Die Reaktion auf Erkenntnisse aus Prüfungsgesprächen wird beschleunigt, da Unterlagen „live" gemeinsam eingesehen werden können und zur Veranschaulichung der konkreten Situation benötigte Nachweise oder Dokumente schneller verfügbar gemacht werden können.

Darüber hinaus wird die Digitalisierung der Revision gefördert und die Entwicklung zum „paperless office“ vorangebracht. Die weitere Flexibilisierung des mobilen Arbeitens bringt ohnehin die Notwendigkeit der digitalen Dokumentation von Prüfungstätigkeiten und den Austausch von digitalisierten Inhalten mit sich. Ortsunabhängig können z. B. standortübergreifende Teams einfach zusammenarbeiten.

Weniger Reisezeit bzw. „Rüstzeiten“ sorgen ferner für einen reduzierten Ressourcenaufwand. In der Summe ermöglichen Remote-Prüfungen auch eine flexiblere Einsatzplanung der Prüfer, gerade wenn man Aktivitäten prüft, die an verschiedenen Orten

stattfinden. Dazu kommen positive Effekte auf die Mitarbeiterzufriedenheit und Motivation, da die Arbeitszeiten flexibler werden und die Mitarbeitenden ihrerseits Zeit und Geld für den Weg zur Dienststätte vermeiden.

9.4.4 Nachteile und Risiken

Durch Remote-Prüfungen ergeben sich, bei sorgfältiger Planung und Durchführung, grundsätzlich keine wesentlichen, negativen Abweichungen in Bezug auf die Prüfungssicherheit gegenüber der Vor-Ort Prüfung. Physische Gegebenheiten und menschliche Zwischentöne bzw. Reaktionen des Gegenübers können jedoch ggf. nur eingeschränkt beurteilt werden. Auch das informelle Gespräch oder der „Beifang" durch zufälligen Austausch und spontane Interaktion entfallen. Der Beziehungsaufbau wird eher oberflächlicher Art sein, was gerade im Umgang mit neuen, noch unbekannten Prüfungsobjekten und Gesprächspartnern hinderlich sein kann.

Schwierige Sachverhalte oder negative Prüfungsergebnisse lassen sich i.d.R. besser in einem persönlichen Gespräch diskutieren. Neben der Sachebene kommt bei der Vermittlung negativer Botschaften auch der Beziehungsebene und der Gestik bzw. Mimik eine gewisse Bedeutung zu. Dies kann in Teilen durch die Wahl des richtigen Kommunikationsmittels ausgeglichen werden. Die Nutzung der Kamerafunktion, die Möglichkeit des Screen-Sharings sowie eine vorher abgestimmte Strategie, wie kritische Punkte „verpackt" werden sollen, sind wichtige Bausteine und bedingen ggf. mehr Vorbereitung als bei einer konventionellen Besprechung vor Ort.

Als Alternative zur physischen Inaugenscheinnahme oder zur Beobachtung von manuellen Bearbeitungsschritten vor Ort können digitale Werkzeuge eingesetzt werden. So kann z. B. die Einsichtnahme in kritische Räume oder Infrastrukturen wie Rechenzentren, mit Hilfe von Kameras oder durch Auswertung von Bild- oder Videomaterial erfolgen.

9.4.5 Praktische Tipps

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:

- Implementieren Sie in ihrem Prüfungsteam regelmäßige virtuelle Treffen („Stand-ups" oder „Dailys") um eine laufende Synchronisierung der verfügbaren Informationen sicherzustellen!

- Schaffen Sie klare Regelungen zur digitalen Ablage von Prüfungsunterlagen, damit alle Prüfer jederzeit einen vollumfänglichen Überblick über den aktuellen Status haben, z. B. der Prüfungsfragenkataloge!
- Klären Sie technische Rahmenbedingungen (Telefon- oder Videokonferenz, Videokonferenztool) und den groben Ablauf der Termine bereits bei der Terminvereinbarung.
- Die Mischung macht es! Je nach Möglichkeit und Bedarf können Sie Vor-Ort und Remote Audits variieren, wobei sich nicht alle Prüfgebiete oder Prüfungsanlässe uneingeschränkt für Remote-Prüfungen eignen.

Quelle:

ISACA-Leitfaden zu Datenanalysen (Ausgabe 2019).

10 Gewinnung (Recruitment) und Weiterentwicklung von Revisionsmitarbeitern inkl. Beachtung der Fit & Proper-Anforderungen für die Revisionsleitung

10.1 Hintergrund

Moderne Interne Revisionen sehen sich seit geraumer Zeit einem komplexer werdenden Umfeld – intern wie extern – gegenüber. In die MaRisk wurden explizit die Anforderungen an das Personal und somit auch an die Mitarbeiter der internen Revision aufgenommen. Ebenso wurde 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 Mitarbeiter der Internen Revision definiert.

Mit der steigenden Komplexität der Geschäftsprozesse bei Banken und einem stetig umfangreicher und inhaltlich komplexer werdendem Aufsichtsrecht in Verbindung mit der Europäisierung der Bankenaufsicht steigen auch die fachlichen, methodischen und persönlichen Anforderungen an Mitarbeiter der Internen Revision bei Kreditinstituten.

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. So sind auch Grundlage der quantitativen und qualitativen Personalausstattung nach AT 7.1, Tz. 1 MaRisk die

- betriebsinternen Erfordernisse,
- Geschäftsaktivitäten und
- Risikosituation.

Die Interne Revision hat dementsprechend fachlich versierte Mitarbeiter 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 Prüfungstätigkeit hinreichend beurteilt werden kann und ein Wissenstransfer in die Bank erfolgt.

10.2 Anforderungsprofil

10.2.1 Fachliche und persönliche Anforderungen

Aufgrund der oben erwähnten MaRisk-Vorgaben hat sich der Revisor mit weit mehr als z. B. den IPPF Standards für die berufliche Praxis der Internen Revision (IIA sowie DIIR) zu beschäftigen. Gleichwohl stellen die IPPF Standards, konkret der IPPF Standard 1200 „Fachkompetenz und berufliche Sorgfaltspflicht“ zusammen mit den weiterführenden Praktischen Ratschlägen (PA 1200-1 und 1210-1), einen guten Rahmen zur Bestimmung grundlegender Kriterien eines qualifizierten Revisionsmitarbeiters dar.

Entsprechend dem Praktischen Ratschlag 1210-1 ist es für die Durchführung von Revisionsprüfungen vor allem erforderlich, die Anwendung von Prüfungsgrundsätzen, -verfahren und -techniken zu beherrschen. Die Beherrschung von Rechnungslegungsgrundsätzen und -verfahren wird darüber hinaus bei Revisoren vorausgesetzt, die häufig mit Bilanzierungsunterlagen und Jahresabschlüssen zu tun haben. Weiterhin erforderlich sind allgemeine betriebswirtschaftliche Kenntnisse, im Besonderen der ordnungsgemäßen Führung von Geschäften, um eine qualifizierte Beurteilung bei Soll-Ist-Vergleichen vornehmen zu können. Die Beherrschung von Revisionsmethodik (Prüfungsverfahren und -methoden) sind dabei elementar notwendig, um entsprechenden Handlungsbedarf zu recherchieren und ableiten zu können.

Jeder Revisor hat insbesondere ein Grundverständnis für Bereiche wie Unternehmensführung, Rechnungswesen, Handels- und Steuerrecht, Finanzierung, quantitative Methoden, Informationstechnologie, Risikomanagement und dolose Handlungen einzubringen. Grundverständnis bedeutet dabei die Fähigkeit, Risiken zu erkennen und das weitere Vorgehen festzulegen.

Hinsichtlich persönlicher Qualifikationen sind gute Menschenkenntnis, Kommunikations- und soziale Kompetenz und hier insbesondere die Konfliktfähigkeit für Revisoren unabdingbar. Sie sollten sich in zwischenmenschliche Beziehungen hineindenken können und angemessene Kontakte zu den geprüften Facheinheiten und deren handelnden Personen aufrechterhalten. Konfliktgespräche so zu führen, dass konstruktive Beziehungen Bestand haben und ein fortgesetzter sachlich-kooperativer Austausch über jegliche Themen möglich ist, sind weitere Fertigkeiten, die der Revisor mitbringen sollte.

10.2.2 Exkurs: Generalist versus Spezialist

Vor dem Hintergrund AT 7.1 MaRisk (bezüglich der qualitativen Personalausstattung) stellt sich die Frage, ob die Interne Revision eher auf Generalisten oder Spezialisten setzen soll. Dabei fungiert die Geschäfts- und Risikostrategie der Bank auch als Leitplanke für die Intensität und Tiefe der Mitarbeiterkompetenz. So wird z. B. die Interne Revision,

die sich in ihrem Institut aufgrund der Strategieorientierung im Handelsbereich durch die Nutzung einer ganzen Palette von Finanzinnovationen speziellen Herausforderungen an die Personalausstattung ausgesetzt sieht, vermehrt Spezialisten vorhalten (müssen). Hier zeigt sich der Grundsatz der Proportionalität, in dem auch das Anforderungsprofil und in der Umsetzung dessen, die Personalausstattung der Internen Revision proportional zur Größe, zum Geschäftsvolumen und zur Risikostruktur und Art und Umfang der Geschäfte sein muss.

Gemäß den IPPF Standards muss jeder Revisor – unabhängig von Status und Aufgabengebiet – die in den IPPF Standards formulierte Mindestkompetenz (generelle Anforderung) erfüllen. Hinzu kommt, dass der Revisor auch Spezialist für die Prozess- und Ordnungsmäßigkeitsanforderungen seines Prüfungsbereichs sein muss. Insoweit bleibt es – wie auch vom IIA gefordert – bei der Vorgabe, dass die Interne Revision insgesamt das Wissen, die Fähigkeiten und sonstige Qualifikationen besitzen oder sich beschaffen muss, die erforderlich sind, um der Verantwortung der Abteilung gerecht zu werden. Jede Revisionsleitung hat dementsprechend für die von der Geschäftsleitung auferlegten Aufgaben und Pflichten eigenständig und individuell eine angemessene Personalausstattung in quantitativer und qualitativer Hinsicht sicherzustellen. Dies gilt insbesondere auch, wenn Expertenwissen oder einzelne Prüfungstätigkeiten extern beschafft werden.

10.2.3 Mögliches Anforderungsprofil

Im Jahr 2020 hat das IIA das Internal Audit Competency Framework veröffentlicht, das die notwendigen Kompetenzen in der Internen Revision beschreibt. Das IIA Framework unterscheidet zwischen den drei Kompetenzstufen „Allgemeines Bewusstsein“, „Angewandtes Wissen“ und „Expertenwissen“ und beschreibt hierzu im Detail die Ausprägungen der einzelnen Anforderungen.

In einer anderen Systematik hat das DIIR das „Qualifikationsmodell für Revisoren“ 2012 entwickelt, das die Qualifikation wie auch die Anforderung an den Revisor in vier übergeordnete Kompetenzfelder unterteilt und diese im Modell entsprechend weiter auffächert:

- Fachwissen zu einzelnen „betrieblichen Funktionen“ (z. B. Risikomanagement)
- Branchen-Kenntnisse
- Methoden: Know-how zu Prüfungsmethoden der Internen Revision
- Persönlichkeit: Soziale Kompetenzen des Revisors

Die Anforderungen wie auch existierende Kompetenzen werden für die einzelnen Felder mit Grundlagenwissen, vertieften Kenntnisse sowie Expertenwissen bewertet. Es gilt, das Anforderungsprofil für die jeweilige Funktion bzw. das Aufgabengebiet in der Internen Revision zu definieren und die bestmögliche Abdeckung hierzu zu erreichen.

Vor dem Hintergrund der steigenden Anforderungen an die Interne Revision sind auch nachfolgende Kompetenzen und Fachkenntnisse zu berücksichtigen:

- Strategisches Denken (z. B. Ausrichtung/Planung der Prüfungshandlungen)
- Vernetztes Denken/Integrale Anwendung von Know-how-Gebieten (z. B. Steuerung von Prüfungsteams bei prozessübergreifenden Prüfungen)
- Fähigkeit Netzwerke zu pflegen und fachlichen Austausch zu organisieren (auch unter Einsatz des Internets)
- Flexibilität in einem, sich immer schneller wandelnden Umfeld (bspw. wegen Institutsinterner Umstrukturierungen)
- Quantitativ ausgerichtete Expertise zur Beurteilung von den in den Geschäfts- und Risikosteuerungsprozessen eingesetzten Modellen und deren Validierung
- Fähigkeit zur Anwendung agiler Methoden und Vorgehensweisen
- methodische und datenanalytische Kenntnisse zur Durchführung von Datenauswertungen
- Kenntnisse zur IT-Sicherheit (z. B. Schutzbedarf, Benutzerrechte etc.)
- sowie die Fähigkeit Fach- und Methodenkenntnisse mit zielgerichtetem Technologieeinsatz zu kombinieren.

10.2.4 Anforderungen an die Revisionsleitung

10.2.4.1 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/2017/12) bei EZB-beaufsichtigten Instituten (SI), die seit dem 30.06.2018 gelten, 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.

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“ (2018) und dem Fragebogen „Fit and Proper Questionnaire“ (2016).

Die Fragenbereiche gliedern sich in die Themen:

- Erfahrung (praktische, theoretische und funktionsspezifische),
- Leumund,
- Interessenkonflikte (persönlich, beruflich, finanziell und politisch) und Unvoreingenommenheit,
- Zeitaufwand und
- kollektive Eignung.

10.2.4.2 Anforderungen der MaRisk

Bei den weniger bedeutenden Institute (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 Prüfungsleiterebene (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 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) ist im Mitgliederbereich des DIIR-Net verfügbar.

10.2.4.3 Fortbildungsverpflichtung

Der Leiter der Internen Revision ist verpflichtet, sich fachlich fortzubilden (IPPF Standard 1230 Regelmäßige fachliche Weiterbildung[18]). Die Fortbildung soll die Fachkenntnisse, die Fähigkeit zu ihrer Anwendung sowie das Verständnis der Berufspflichten auf einem ausreichend hohen Stand halten. Die Fortbildung soll 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 sowie
- die Tätigkeit in externen Fachgremien.

Die Erfüllung der Fortbildungsverpflichtung ist zu dokumentieren. Eine nicht erbrachte Fortbildungsverpflichtung kann im Folgejahr nachgeholt werden.

[18] Indirekt auch über AT 7.1 Tz. 2 MaRisk.

Die Überwachung der Einhaltung der Fortbildungsverpflichtung des Leiters der Internen Revision obliegt grundsätzlich dem zuständigen Vorstandsmitglied. Entsprechende Prozesse sind, z. B. im Personalbereich, einzurichten.

10.3 Gewinnung (Recruitment) von Revisionsmitarbeitern

10.3.1 Märkte und Instrumente

Nachdem vor dem Hintergrund der MaRisk und berufsständischen Regeln ein Anforderungsprofil konkretisiert und in eine Personalstrategie der Internen Revision übergeleitet wurde, beginnt die gezielte Mitarbeiterauswahl und -gewinnung. Der Recruitment-Prozess 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 Mitarbeitern. Die Recruitment-Anstrengungen sind auf den in zwei nachfolgende Gruppen zu unterteilenden Personalmarkt zu konzentrieren:

- Interner Markt und
- Externer Markt.

Unter internem Markt sind alle Mitarbeiter 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

- Trainee-Programm,
- Personalentwicklungsprogramme (Entwicklung zur Seniorfachkraft oder Führungskraft),
- Innerbetrieblichen Vorstellungsrunden (z. B. Präsentation der Internen Revision bei diversen Arbeitsgruppen oder Netzwerkveranstaltungen) oder
- Intranetpräsenz

viele Möglichkeiten, Personal für die Interne Revision zu gewinnen. Größter Vorteil ist das vorhandene „Branding“ der Mitarbeiter/innen, d. h. die Identifikation mit dem Arbeitgeber und seinen Werten und Vorstellungen. So können unternehmenserfahrene Kräfte gewonnen werden, welche die Facheinheiten des Instituts sehr gut kennen und entsprechendes Detailwissen mitbringen. Dabei sind jedoch anfängliche Einschränkungen bei einem Wechsel in die Revisionsfunktion zur Vermeidung einer möglichen Selbstprüfung (Cooling-Off-Period) 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:

- Hochschulmarketing,
- Stellenausschreibungen (insbesondere auch online),
- Beauftragung von Personalberatungen,
- Betreuung von Examensarbeiten bzw.
- Empfehlungsmarketing/Präsenz im Internet (z. B. soziale Medien).

Für den richtigen und zielorientierten Einsatz der Instrumente auf dem externen Markt ist ein erhöhter finanzieller Aufwand notwendig. Potenzielle Mitarbeiter/innen 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 als Rahmenbedingung zu beachten sind u. a. die einschlägigen Vorschriften des allgemeinen Gleichbehandlungsgesetzes (AGG).

Den Revisionsverantwortlichen – in Zusammenarbeit mit der Personalabteilung – muss es beim Recruitment 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?

10.3.2 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:

- Vorträge über die Funktion der Internen Revision innerhalb des Unternehmens und bei externen Veranstaltungen oder (Fach-)Kongressen, aktive Pflege von Netzwerken
- Veröffentlichen von Artikeln in Mitarbeiterzeitung bzw. Fachartikeln in Fachzeitschriften
- Präsenz in einschlägigen fachbezogenen Internetseiten
- Teilnahme an Unternehmens- oder Jobmessen

- Professionelle revisorische Arbeit im Rahmen von Prüfung, Beratung und der Begleitung von Projekten

Die Attraktivität der Internen Revision wird dabei von Bewerbern u. a. anhand nachfolgender Aspekte bemessen:

- Interessante, herausfordernde und abwechslungsreiche Aufgabenstellungen
- 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 Mitarbeitern/innen ein Umfeld zu schaffen, das von flachen Hierarchien, 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 Mitarbeiter ist das Fundament zur Aufrechterhaltung einer funktionsfähigen Internen Revision gelegt. Die Komplexität des regulatorischen Umfelds als auch der zunehmende Wettbewerb um „gute Köpfe“ erfordern jedoch geeignete Weiterbildungskonzepte, um den Erfolg der Internen Revision nachhaltig zu sichern.

10.4 Weiterentwicklung

10.4.1 Personalentwicklung

Die Funktionsfähigkeit der Internen Revision bedingt neben der angemessenen quantitativen Ausstattung auch eine regelmäßige Weiterentwicklung der Kompetenzen. AT 7.1 Tz. 2 MaRisk gibt insoweit vor, dass „Mitarbeiter 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 Mitarbeiter angemessen ist.“ Vor dem Hintergrund

eines sich schnell verändernden Umfelds und intensiveren 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 Aktivitäten orientieren.

Die Personalentwicklungsstrategie kann dabei von folgenden Überlegungen flankiert werden:

- Welche Anforderungen bestehen heute bzw. zukünftig und werden diese über die Ist-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 oder
- revisionsmethodischer Kompetenzen oder
- besonderer fachlicher Kenntnisse für das Prüfungsgebiet,

auf der anderen Seite in Maßnahmen, die „on-the-job“ oder „off-the-job“ durchgeführt werden.

10.4.2 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, Konfliktmanagement oder Mitarbeiterführung entwickelt werden. Darüber hinaus bieten sich je nach Organisationskultur oder interner Personalstrategie auch Coaching bzw. Mentoringprogramme an.

Erfahrene Mitarbeiter/innen 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 Revisionsmitarbeiter 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. Streng zu beachten hierbei sind allerdings die Vermeidung von Zielkonflikten und denkbaren Beeinträchtigungen der Unabhängigkeit der Revisionsmitarbeiter.

10.4.3 Entwicklung von revisionsmethodischen Kompetenzen und besonderem Fachwissen

Im Hinblick auf mögliche Instrumente zur Entwicklung und Vertiefung revisionsmethodischer Kompetenzen und 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 oder
- externe/interne Seminare,
- Projektbegleitungen,
- sonstige beratende Tätigkeiten für die Fachbereiche,
- Hospitationen im Fachbereich (unter gleichzeitiger Wahrung von Unabhängigkeit und Vermeidung von Interessenskonflikten),
- Qualifizierung zum Datenanalyst 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.

Die Konzeption der Mitarbeiterentwicklung sowie die Durchführung von Weiterentwicklungsmaßnahmen in der Internen Revision sind hinreichend zu dokumentieren, um die Verpflichtungen aus den MaRisk hinsichtlich eines angemessenen Qualifikationsniveaus der Mitarbeiter/innen sicherzustellen. Vergleichbare Verpflichtungen ergeben sich aus den berufsständischen Standards (IPPF Standard 1200) 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.

Quellenverzeichnis:

Amling, Th./Bantleon, U.: Handbuch der Internen Revision, 2007, Erich-Schmidt Verlag, S. 179.

Arntz, A. et al., „Qualifikationsmodell für Revisoren“, ZIR 5/2012, S. 249-250.

DSGV, DSGV Interpretationsleitfaden zu den MaRisk (Version 6 aus 04/2018), S. 99 ff.

DIIR - Deutsches Institut für Interne Revision e.V., DIIR-Broschüre: „Konzept zur Gewinnung und Qualifizierung von Mitarbeitern für die Interne Revision, 2002, S. 5 f.

DIIR - Deutsches Institut für Interne Revision e.V.: Qualifikationsmodell für Revisoren, Version 1, Oktober 2012.

IIA, Internal Audit Competency Framework (Übersetzung durch DIIR), 2020, https://na.theiia.org/translations/PublicDocuments/Internal-Audit-Competency-Framework-German.pdf.

Helfer, M./Ruck, G.: Sicherstellung der MaRisk-konformen Qualifikation der Mitarbeiter der Internen Revision in Kreditinstituten, ZIR 06/2007, S. 264 f.

Schmelter, H.: Interner Revisor – Generalist oder Spezialist, ZIR 5/2009, S. 225.

11 Qualitätssicherung und -verbesserung in der Internen Revision

11.1 Grundlagen des Qualitätsmanagements

Als Folge steigender Anforderungen im Bereich der Corporate Governance und seitens der Bankenaufsicht kommt der Sicherung der Qualität der Internen Revision ein hoher Stellenwert zu. Um dauerhaft die Wirksamkeit der Internen Revision zu gewährleisten, ist eine ständige Bewertung und Verbesserung ihrer Arbeit notwendig.

Die IPPF Standards des The Institute of Internal Auditors (IIA) beinhalten Vorgaben zur Qualitätssicherung und Qualitätsverbesserung, die auch die regelmäßige externe Beurteilung der Revisionsarbeit (vgl. IPPF Standards 1300 -1322) beinhalten. Danach ist es Pflicht der Revisionsleitung, ein „Programm zur Qualitätssicherung und -verbesserung, das alle Aufgabengebiete der Internen Revision umfasst (zu) entwickeln und (zu) pflegen“. Unterstützt werden die Regelungen 1300 ff. der IPPF Standards durch den DIIR Revisionsstandard Nr. 3 Prüfung von Internen Revisionssystemen (Quality Assessments) und den Kriterienkatalog zur Prüfung des Internen Revisionssystems (Anlage 1 des DIIR Revisionsstandard Nr. 3).

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. Dies insbesondere dann, wenn die von der Geschäftsleitung verabschiedete Revisionscharta die Einhaltung der IPPF Standards ausdrücklich vorsieht.

11.2 Interne Qualitätsüberwachung

11.2.1 Laufende interne Beurteilung

Kernelemente zur Zielerreichung, Qualitätssicherung und -verbesserung der Revisionsfunktion sind interne Richtlinien und Verfahren (IPPF Standard 2040) sowie die laufende Steuerung und Überwachung aller Revisionsaktivitäten (u. a. IPPF Standard 2340). Es sollten durch den Revisionsleiter prozessintegrierte Überwachungsmaßnahmen und -mechanismen geschaffen werden, die die Einhaltung der gesetzten Vorgaben (z. B. Organisationsrichtlinie, Revisionshandbuch) gewährleisten.

Nachfolgend sind wichtige Aspekte, die dabei berücksichtigt werden sollten, exemplarisch dargelegt:

- Planung

  Durch geeignete Verfahren ist die Risikoorientierung und Vollständigkeit der Planung 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 Ziffernkontrolle beinhalten und nach Möglichkeit funktionsgetrennt erfolgen. Durch die Revisionsleitung sollte eine Plausibilisierung der Ergebnisse durchgeführt werden.

- Prüfungsvorbereitung

  Das Prüfungsprogramm sollte durch die Prüfungsleitung oder erfahrenen Prüfern erstellt und die inhaltliche Qualität (bspw. thematische Vollständigkeit, Risikoorientierung) durch die zuständige Führungskraft überprüft werden.

- 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 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 durchgeführt werden.

- Follow-up

  Das Verfahren zur Überwachung der Erledigung von festgestellten Mängeln (Follow-up) sollte in einer Organisationsrichtlinie oder Arbeitsanweisung veröffentlicht sein, so dass die geprüften Einheiten zur Unterstützung der Internen Revision verpflichtet werden. Intern 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).

- Ergebnis

  Es ist sicherzustellen, dass der Auftrag der Internen Revision, zur Funktionsfähigkeit und Wirtschaftlichkeit der Führungs-, Überwachungs-, Risikomanagement- und -kontrollprozesse beizutragen, erreicht wird. Hierzu kann eine regelmäßige Analyse von Art, Schwere und Inhalt der getroffenen Feststellungen/Empfehlungen der Internen Revision sowie deren Erledigungsstand bzw. -dauer über einen längeren Zeitraum dienen. Aus der Analyse können ggf. auch Belege für die Wirksamkeit der Internen Revision gewonnen werden.

- Qualifikation

  Es ist sicherzustellen, dass die Personalausstattung quantitativ und vor allem qualitativ zur Aufgabenerfüllung angemessen ist und die Mitarbeiter fortlaufend weiterentwickelt werden (vgl. Abschnitt 10).

- 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 für Prüfungen, Beratungen, Projektbegleitungen, Zeitreserven für Sonderprüfungen sollten laufend (mindestens vierteljährlich) überwacht und Abweichungen schriftlich begründet 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 p.a. erfolgen.

- Projektbudget:
  Mit Hilfe eines Projektbudget kann die Revision weiterentwickelt werden (z. B. Anpassung des Revisionsmanagementsystems, Weiterentwicklung des Revisionsprozesses).

Unterstützend zur laufenden internen Überwachung kann nach Prüfungsabschluss auch ein Feedback der geprüften/beratenen Stelle in Form eines Fragebogens eingeholt werden, in dem einzelne Aspekte zur Wahrnehmung der Revisionsvertreter, Prüfungsplanung, -durchführung, -berichterstattung und zum Nutzen/Mehrwert der Prüfung bewertet werden können.

Beispiele für Feedbackbogen (Anlage 6) und für Kundenbefragung zu Revisionsprüfungen (Anlage 7) sind im Mitgliederbereich des DIIR-Net verfügbar.

Bei der Auswertung des Feedbacks der geprüften/beratenen Stelle ist jedoch zu beachten, dass eine verlässliche Messung der Prüfungsqualität durch dieses Instrument schwierig ist, da die Prüfungsergebnisse das Feedback beeinflussen können.

Alternativ können auch (jährliche) „Stakeholder Surveys“ durchgeführt werden. Als „Stakeholder“ kommen hier Aufsichtsorgan/Prüfungsausschuss, Geschäftsleitung und ausgewählte Vertreter der 1. und ggf. 2. Führungsebene unterhalb der Geschäftsleitung in Frage. Hierbei können über einen strukturierten Fragebogen die Fragenkreise

- Wahrnehmung der Revisionsvertreter,
- Betätigungsfeld der Internen Revision,
- Revisionsprozess und Berichterstattung,
- Steuerung der Internen Revision sowie
- 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 im Mitgliederbereich des DIIR-Net verfügbar.

Die Gesamtverantwortung für die laufende Überwachung liegt bei der Revisionsleitung wobei die Durchführung der Qualitätsüberwachung auf geeignete Mitarbeiter übertragen werden (Führungskräfte, Senior Revisoren). 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 beigefügt werden.

Ein Beispiel für eine Checkliste zur Prüfungsqualität ist im Mitgliederbereich des DIIR-Net verfügbar (Anlage 10).

11.2.2 Periodische interne Beurteilung

Ergänzend zur laufenden internen Überwachung schreiben die Berufsstandards (IPPF Standard 1311 Interne Beurteilungen) regelmäßige Beurteilungen in Form von Selbstbeurteilung durch Mitarbeiter der Internen Revision oder geeignete unternehmensinterne Personen (z. B. CIAs oder geeignete Fachleute aus anderen Bereichen der Organisation) vor, die die Übereinstimmung der Internen Revision mit

- ihrer Definition
- dem Ethikkodex des IIA
- und den IPPF Standards des IIA

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 und deren Umsetzung überwacht wird.

Die Ergebnisse interner Beurteilungen sollten durch die Revisionsleitung an relevante interne Stellen (z. B. Geschäftsleitung, Aufsichtsorgan, Audit Committee) kommuniziert werden.

Periodische interne Beurteilungen dienen weiterhin 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 Nutzung des QA Leitfadens des DIIR zu orientieren.

11.3 Externe Beurteilung

11.3.1 Externe Beurteilung

Eine wesentliche Maßnahme zur Sicherung der Qualität interner Revisionsleistungen stellt die Durchführung einer externen Beurteilung (Assessment) dar. Gemäß IPPF Standard 1312 müssen externe Beurteilungen von einem qualifizierten, unabhängigen Prüfer oder Prüfungsteam mindestens alle fünf Jahre durchgeführt werden. Das DIIR bietet Fortbildungsveranstaltungen zum Prüfer für Interne Revisionssysteme[DIIR] an.

Ergänzt werden die IPPF Standards durch den vom DIIR veröffentlichten Revisionsstandard Nr. 3 Prüfung von Internen Revisionssystemen (Quality Assessments), aktuelle Fassung veröffentlicht im April 2017, der das Vorhandensein eines Internen Revisionssystems (IRS) fordert. 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. Das IRS ist als „die Gesamtheit der Regelungen, die darauf ausgerichtet sind, die Einrichtung einer Internen Revisionsfunktion sowie die unabhängige und objektive Erbringung von Prüfungs- und Beratungsleistungen durch die Interne Revision in Übereinstimmung mit den angewandten IRS-Grundsätzen zu gewährleisten, dokumentiert in einer formellen IRS-Beschreibung“ definiert.

Der DIIR Revisionsstandard Nr. 3 enthält in Anlage 1 einen Kriterienkatalog zur Prüfung des IRS bestehend aus 82 Fragen, die mit den Blöcken Grundlagen (Organisation der Internen Revision, Einordnung im Unternehmen, Budget und Planung), Durchführung von Prüfungen (Vorbereitung, Durchführung, Nachbereitung) und Mitarbeiter (Auswahl, Entwicklung und Fortbildung) die vom IIA identifizierten Schlüsselkriterien aufgreifen. In Beantwortung des Kriterienkatalogs muss der unabhängige Prüfer jede Frage auf einer Skala von 3-0 bewerten, wobei 3 für voll erfüllt, 2 für leichtes Verbesserungspotenzial, 1 für deutliches Verbesserungspotenzial und 0 für unzureichend steht. Anschließend addiert der Prüfer die Punkte und verdichtet sie zu einem Gesamturteil. Die Bewertung ergibt sich aus der prozentualen Zielerreichung für das Betrachtungsfeld: Voll erfüllt (> = 90%), Leichte Verbesserungspotenziale (75% - < 90%), Deutliche Verbesserungspotenziale (50% - < 75%), Unzureichend (< 50%). Hierbei sind sechs Mindeststandards zu berücksichtigen, deren Nichteinhaltung (Bewertung „0“) grundsätzlich zur Bewertung „unzureichend“ führt. Auf Basis der prozentualen Zielerreichung je Betrachtungsfeld erfolgt zunächst die Beurteilung nach quantitativen und qualitativen Faktoren, ob Beanstandungen auf Ebene der Betrachtungsfelder wesentlich sind: Bei der Beurteilung ist zu berücksichtigen ob und wenn ja, wie viele (quantitativ) und welche (qualitativ) Einzelkriterien zu einer Beanstandung (0, 1 oder 2) geführt haben. Die rechnerisch ermittelten Prozentsätze können dabei Indikatoren für oder gegen das Vorliegen wesentlicher Beanstandungen darstellen. Es ist grundsätzlich davon auszugehen, dass eine wesentliche Beanstandung bezogen auf ein Betrachtungsfeld vorliegt, wenn der überwiegende Teil der Einzelkriterien eines Betrachtungsfelds eine Beanstandung (0, 1 oder 2) aufweist und/oder eine größere Anzahl der Einzelkriterien als unzureichend (0) eingestuft worden ist. Diese Situation wird durch einen Score < 75 % indiziert. Die Vermutung kann aufgrund einer Würdigung qualitativer Faktoren widerlegt werden. Auch bei einem Score > 75 % können grundsätzlich wesentliche Beanstandungen vorliegen.

Ist eine wesentliche Beanstandung auf ein Betrachtungsfeld und damit einen abgrenzbaren Teilbereich des IRS beschränkt, führt dies grundsätzlich zu einer Einschränkung des Prüfungsurteils. Sollten mehrere Betrachtungsfelder eine wesentliche Beanstandung aufweisen ist nach prüferischem Ermessen zu beurteilen, ob die Beanstandungen mangels

Abgrenzbarkeit auf einzelne Teilbereiche des IRS zu einer Versagung des Prüfungsurteils (negative Gesamtaussage) führen.

Anschließend ist zu beurteilen, ob Beanstandungen – über die einzelnen Betrachtungsfelder hinweg – auf Ebene des IRS zusammengefasst wesentlich sind. Dabei gelten die oben gemachten Ausführungen analog. Eine wesentliche Beanstandung auf Ebene des IRS als Ganzem führt mangels Abgrenzbarkeit grundsätzlich zu einer Versagung des Prüfungsurteils (negative Gesamtaussage).

Abschließend wird – wie weiter unten dargestellt – ein Bericht, der ein zusammengefasstes Prüfungsurteil zum IRS beinhaltet erstellt. Sollte ein Verbesserungsbedarf bei einzelnen Kriterien des Kriterienkatalogs festgestellt worden sein, ohne dass jedoch ein wesentlicher Mangel vorliegt, so sollte hierüber zumindest in Form einer Zusammenfassung ebenfalls im Prüfungsbericht berichtet werden.

11.3.2 Selbstbeurteilung mit unabhängiger Überprüfung

In Anbetracht der durch ein externes Assessment verursachten Kosten und Ressourcenbindung sind Revisionsleitungen oftmals nicht willens oder in der Lage, entsprechende Budgets für eine externe Qualitätsüberprüfung bereit zu stellen.

Als Reaktion auf Bedenken, dass externe Beurteilungen durch unabhängige Prüfer zu aufwändig für kleinere Revisionsabteilungen sein könnten, hat das IIA daher einen alternativen Ablauf vorgesehen (Erläuterung zu IPPF Standard 1312 Externe Beurteilungen). Hierbei handelt es sich um eine sog. „Selbstbeurteilung mit einer unabhängigen (externen) Bestätigung“. Im Rahmen des zuvor dargestellten internen Qualitätssicherungsprogramms wird 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. Beispielsweise können Bereiche wie Benchmarking, Untersuchung und Beratung hinsichtlich des Einsatzes von Best Practices sowie Interviews mit leitenden und operativen Führungskräften (deren Ansichten und Anliegen der Revisionsleitung und den Revisionsmitarbeitern bereits bekannt sind) eingeschränkt berücksichtigt oder fallengelassen werden. Ansonsten gelten die gleichen Anforderungen und Kriterien wie im IPPF Standard 1312.

Empfohlen wird, dass eine Arbeitsgruppe unter Leitung der Revisionsleitung den Selbstbeurteilungsprozess durchführen und vollständig dokumentieren soll. In größeren Revi-

sionseinheiten besteht auch die Möglichkeit, bestimmte Mitarbeiter dauerhaft mit Aufgaben 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 fachkundiger, unabhängiger Prüfer sollte eine Validierung der Selbstbeurteilung vornehmen, um die Ergebnisse zu bestätigen und eine Stellungnahme über das angegebene Niveau der Übereinstimmung mit den IPPF Standards für die berufliche Praxis der Internen Revision abzugeben. Als Abschluss der unabhängigen Bestätigung soll er dem Bericht eine zustimmende Stellungnahme hinzufügen.

Wenn der unabhängige Prüfer der Beurteilung bezüglich des Einhaltens der IPPF Standards und des Ethikkodex 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 Abteilung bietet und im Qualitätsprogramm der Abteilung vorgesehen sein sollte, bietet die Selbstbeurteilung mit externer Überprüfung eine alternative Methode zum vollständigen Erfüllen der Anforderungen des IPPF Standards 1312. Trotzdem und soweit möglich, sowie um den größtmöglichen Nutzen für Qualitätssicherung und Ablaufverbesserung zu erzielen, sollte eine Revisionsabteilung die Selbstbeurteilung mit unabhängiger Überprüfung als Zwischenlösung betrachten und eine vollständig externe Prüfung in den Folgeperioden anstreben.

11.3.3 Berichterstattung über externe Beurteilungen

Die vorläufigen Ergebnisse der Untersuchung sollten mit der Revisionsleitung während und bei Abschluss des Beurteilungsverfahrens diskutiert werden. Die endgültigen Ergebnisse sind neben der Revisionsleitung in geeigneter Form an die Geschäftsleitung und das Überwachungsorgan zu berichten. Die Berichterstattung sollte gemäß DIIR Revisionsstandard Nr. 3 und Implementierungsleitlinien zum IPPF Standard 1312 vor allem folgendes enthalten:

- Feststellungen zum IRS und gegebenenfalls Empfehlungen
- Gegebenenfalls Darstellung geplanter Maßnahmen des Unternehmens zur Behebung der festgestellten Mängel mit Verantwortlichkeiten und Umsetzungstermin
- Zusammengefasstes Prüfungsurteil, ob die im geprüften Zeitraum implementierten Regelungen des IRS in der IRS-Beschreibung in Übereinstimmung mit den angewandten IRS-Grundsätzen in allen wesentlichen Belangen angemessen dargestellt sind, ob die dargestellten Regelungen in Übereinstimmung mit den angewandten IRS-Grundsätzen in allen wesentlichen Belangen während des geprüften Zeitraums geeignet waren, mit hinreichender Sicherheit die Einrichtung einer Internen Revisionsfunktion sowie die unabhängige und objektive Erbringung von Prüfungs- und

Beratungsleistungen durch die Interne Revision zu gewährleisten und ob die dargestellten Regelungen in allen wesentlichen Belangen während des geprüften Zeitraums wirksam waren.

11.4 Ergänzende Elemente eines Qualitätsmanagementsystems

In Ergänzung zu den vorhergehend dargelegten Maßnahmen und Aktivitäten können auch „Key Performance Indicators“ (vgl. Abschnitt 14) definiert werden, mit denen regelmäßig bestimmte Kriterien und/oder Ziele hinsichtlich ihrer Erfüllung bzw. Erreichung gemessen werden. Diese werden regelmäßig in engem Zusammenhang mit definierten Qualitätsmerkmalen stehen (z. B. zeitgerechte und klare/transparente Berichterstattung) bzw. sich auf quantitative (z. B. Budgeteinhaltung) oder sich auf sonstige qualitative Faktoren (Mitarbeiterqualifizierung, Ergebnisse von Prüfungsfeedbacks/Stakeholder Surveys, Ergebnisse Quality Self Assessments/externer Beurteilungen) beziehen.

Darüber hinaus ist auch die Einbettung von Kriterien bzw. Zielen aus einem Qualitätsmanagementsystem in eine Balanced Scorecard möglich.

Quellenverzeichnis:

Albinus, S./Heydemann, N.: Quality Assessment – Grundlagen und Erfahrungen der Stadtwerke München, ZIR 6/2007, S. 252 ff.

IIA: Practice Guide: Quality Assurance and Improvement Program (QAIP), 2012.

Magnus, M.: Client Auditor Feedback – ein Instrument mit unerwünschten Nebenwirkungen?, ZIR 1/2008, S. 31 ff.

Seelis, M.: „Client Auditor Feedback – ein Instrument mit unerwünschten Nebenwirkungen?“, ZIR 3/2008, S. 138.

Westhausen, H.-U.: Externe Quality Assessments in der Internen Revision, ZIR 8/2010, S. 3 ff.

12 Konzernrevision

12.1 Rechtliche Grundlagen

Kreditinstitute müssen gemäß § 25a Absatz 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 (vgl. Darstellung des 3-Lines-of-Defense Modells in Abschnitt 14).

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. Während die Konzernrevision auf den Prüfungsergebnissen der Internen Revision in Tochterunternehmen aufbauen kann, ist ihr Fokus auf die Anforderungen des übergeordneten Unternehmens der Gruppe gerichtet. Bei der Ausgestaltung der Konzernrevisionsfunktion ist 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. Daher besteht bei der konkreten Ausgestaltung des Steuerungs- und Überwachungsverfahrens ein Ermessenspielraum. Dieser ist notwendig, da die verschiedenen Gruppen mit Blick auf Entscheidungs- und Informationswege zumeist unterschiedlich straff organisiert sind und zudem hinsichtlich ihrer Geschäftsmodelle und den dadurch bedingten unterschiedlichen regulatorischen Anforderungen oft sehr heterogen sind. Daher hängt die konkrete Ausgestaltung der Konzernrevisionsfunktion insbesondere von Art, Umfang, Komplexität und Risikogehalt der von der Gruppe betriebenen Geschäftsaktivitäten, dem Integrationsgrad der Unternehmen sowie von den gesellschaftsrechtlichen Möglichkeiten ab.

Die 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 Revisionsleiter 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 Revisionsleitern im Konzern jährlich überprüft, aktualisiert und von den jeweiligen Vorständen in Mutter- und Tochtergesellschaften in Kraft gesetzt werden.

12.2 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 Ertragssicht etc. relevant sind.

Der Grad der Integration zwischen Interner Revision der Tochtergesellschaft und der Konzernrevision wird beeinflusst vom Grad der Integration der Tochter in die Gruppenstruktur (z. B. Waiver, Gewinnabführungsvertrag, (Teil-)Beherrschungsvertrag, Risikomanagement). In der leichtesten Ausprägung prüft die Konzernrevision lediglich das auf Gruppenebene implementierte Risikomanagementsystem (Mindestanforderung) sowie ggf. auf Gruppenebene implementierte Aktivitäten und Prozesse; die dezentralen Revisionseinheiten in den Tochtergesellschaften sind jedoch 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 inklusive des gesamten Prüfungsuniversums innerhalb des Konzerns selbst verantwortet. Dies kann entweder durch eine Vollauslagerung 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, wie z. B. IT in Tochterunternehmen) der Fall, bei denen die Tochtergesellschaften vorwiegend aus formellen Gründen bestehen. In diesem Fall sollte auch die Interne Revision zentral geführt werden und ihre Prüfungstätigkeit an der Konzernorganisation ausrichten. Gleichzeitig gilt zu berücksichtigen, dass eine Vollauslagerung der Internen

Revision für gem. MaRisk regulierte Institute nur möglich ist, 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 (AT 9 Tz 5 MaRisk).

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 Vollauslagerung 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.

Bei der Integration der Internen Revision des Tochterunternehmens in die Konzernrevision bleibt die Interne Revision des Tochterunternehmens grundsätzlich 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. Dieses Variante ist dann sinnvoll, wenn in einem zentralistisch aufgestellten Konzern, aufgrund spezifischer Gegebenheiten (z. B. Tochterunternehmen im Ausland) eine Auslagerung der Internen Revisionsfunktion auf die Muttergesellschaft nicht sinnvoll 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.

12.2.1 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 Revisionshandbuches genannten Prinzipen.

Dieser Mehrjahresprüfungsplan 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.

Alle gruppenweit eingerichteten Prozesse sollten unter der Verantwortung der Konzernrevision geprüft werden (als Konzernprüfungen bzw. zentrale Prüfungen). Die Konzernrevision kann sich hierbei jedoch auch den Internen Revisionen der Tochtergesellschaften bedienen (vgl. Abschnitt 4.3).

Die Planung erfolgt durch die Konzernrevision in Abstimmung mit den Revisionsleitern der Tochtergesellschaften (AT 4.5 Tz. 6 MaRisk). Je nach konkreter Ausgestaltung der Prüfungsdurchführung stellen die Revisionsleiter der 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 aus Konzernsicht für die Risikofrüherkennung und -steuerung 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. 15: Übersicht über die Prüfungsarten aus Konzernsicht

Bei einer vollständigen Integration der Internen Revision der Tochtergesellschaften in die Konzernrevision ist im Rahmen des Planungsprozesses der Prüfungsplan zentral zu erstellen. Da auch auf Ebene der Einzelunternehmen die Revisionsfunktion ausgeübt werden muss, muss der Prüfungsplan 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.

Das Prüfungsuniversum des Konzerns besteht somit aus Prozessen und Aktivitäten aller relevanten Gesellschaften des Konzerns. Da die Prüfungstätigkeit im Konzern in diesem Fall allein von der Internen Revision der Konzernmutter verantwortet und durchgeführt wird, kommen hierbei einheitliche und harmonisierte Standards zur Anwendung. Diese betreffen sowohl die prüferische Vorgehensweise als auch die Berichterstattung und die Risikoeinstufung von Prüfungsfeststellungen.

Der Ausprägungsgrad der Integration der Internen Revision der Tochtergesellschaft beeinflusst auch die Ausprägung des Prüfungsuniversums. Hierzu sind zwei Varianten möglich:

- ein konsistentes Prüfungsuniversum für den gesamten Konzern, inklusive der Prüfungsgebiete in den Tochtergesellschaften bzw.
- 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 Prüfungsthemen aus Konzernsicht mit denen der einzelnen Tochtergesellschaften verbinden und z. B. gemeinsam oder nach einheitlichen und abgestimmten Prüfungsprogrammen prüfen kann.

12.2.2 Überwachung der Qualität der Internen Revision bei Verwendung von Prüfungsergebnissen

Wie einleitend beschrieben, hat die Konzernrevision im Rahmen des Risikomanagements der Gruppe gemäß AT 4.5 Tz. 6 MaRisk ergänzend zur Internen Revision des gruppenangehörigen Unternehmens tätig zu werden. Hierbei kann die Konzernrevision auch die Prüfungsergebnisse der Internen Revisionen der nachgeordneten Unternehmen verwenden. 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 einheitlich Standards bezüglich des Revisionsprozesses, insbesondere 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 diese Voraussetzungen erfüllt sind. 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. Mit dieser Regelung soll nach der Begründung zur PrüfBV sichergestellt werden, dass die Aufsicht jährlich Grundinformationen über das Risikomanagement der Gesellschaft erhält. 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 Nutze 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. Mindestberichtsinhalte 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 Handbuches). Das Quality Assessment kann auch durch die Konzernrevision selbst oder von einem Team aus den Internen Revisionen der Gruppe umgesetzt werden. Einschränkend 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.

Im gleichen Zusammenhang kann sich die Interne Revision der Tochtergesellschaft auf die Ergebnisse der Prüfungen der Konzernrevision bzw. der Internen Revision von Schwestergesellschaften verlassen und diese zur Abdeckung ihres Prüfungsuniversums verwenden. Dies setzt voraus, dass sie den Revisionsbericht (ggf. Auszug), um die durchgeführten Prüfungshandlungen bewerten sowie die Prüfungsergebnisse auf Relevanz und Risiko für die eigene Gesellschaft analysieren zu können.

12.2.3 Prüfungstätigkeit und Berichterstattung

Konzernprüfungen können zentral („top-down“) durch die Konzernrevision selbst oder mit Unterstützung der Internen Revisionen der Tochtergesellschaften durchgeführt werden. Eine Einbeziehung der Internen Revisionen der Tochtergesellschaften ist 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. Die Prüfungshandlungen der Internen Revision der Tochtergesellschaft sollten inhaltlich von der Konzernrevision vorbereitet (Prüfungsleitfaden) und die Ergebnisse anschließend plausibilisiert werden. Im Rahmen der Berichterstattung sind die Prüfungsergebnisse aus den Tochtergesellschaften zu einem aussagefähigen Gesamtbericht für den Vorstand der Muttergesellschaft zu aggregieren. Die Verantwortlichkeit für das Follow-up der Einzelfeststellungen auf Ebene der Tochtergesellschaften verbleibt aus Praktikabilitätsgründen bei der Internen Revision der jeweiligen Tochtergesellschaft mit entsprechender Meldung an die Konzernrevision, wohingegen die

Einzelfeststellungen des konsolidierten Gesamtberichtes durch die Konzernrevision nachzuverfolgen sind. Die von Tochterrevision und Konzernrevision verwendeten Verfahren zur Überwachung der fristgerechten Beseitigung von Mängeln sind dabei nach AT 4.5 der MaRisk aufeinander abzustimmen.

Themen 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.

Die Regelungen zur Berichterstattung sollten in geeigneter Form möglichst einheitlich in der Gruppe definiert werden.

12.2.4 Informationsweitergabe und Austausch

Neben der gemeinsamen Planung von Prüfungen und der Überlassung von Prüfungsergebnissen ist zur Ausübung einer wirksamen Konzernrevisionsfunktion notwendig, dass die Revisionsleiter im Konzern vertrauensvoll und auf Basis eines gemeinsamen Revisionsverständnisses zusammenarbeiten. Um den Austausch konzernweit sicherzustellen, bietet sich z. B. ein regelmäßiges Treffen der Revisionsleiter 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:

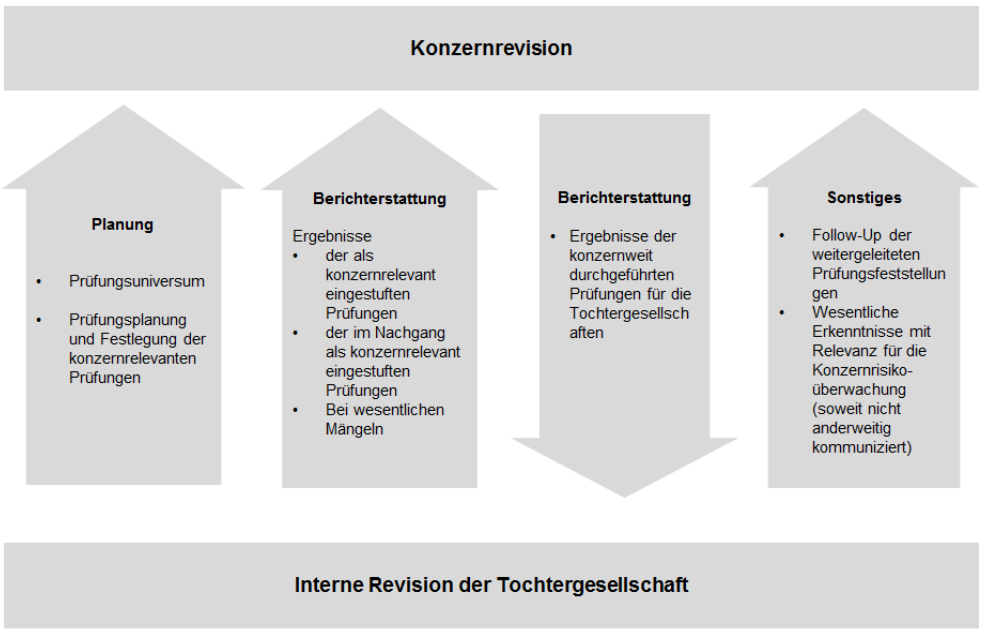


Abb. 16: Informationsflüsse zwischen den Internen Revisionen der Tochtergesellschaften und der Konzernrevision

Die Konzernrevision sollte einheitliche Standards zur Informationsweitergabe zwischen Konzernrevision und den Internen Revisionen der Tochtergesellschaften vorgeben.

12.2.5 Berichterstattung an den Konzernvorstand

Die Konzernrevision als Instrument des Konzernvorstandes, hat diesen über die Prüfungsergebnisse im Konzern zu informieren. Neben den Prüfungsberichten über die Konzernprüfungen, ist auch über die nach vergleichbaren Bewertungsmaßstäben der Konzernrevision wesentlichen Prüfungsfeststellungen und -ergebnissen 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 eingestuften 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 Konzernvorstand 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 der Prüfungsplanung, der Prüfungstätigkeit und der Berichterstattung müssen die verschiedenen Rollen hinsichtlich des Umfangs und 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 Konzernvorstand 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. 17: Mögliche Rollen der Internen Revision der Muttergesellschaft und deren Auswirkung auf die Berichterstattung

Quellenverzeichnis:

Deutscher Sparkassen- und Giroverband: Mindestanforderungen an das Risikomanagement, Interpretationsleitfaden, Version 6.1, Juli 2019.

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.

13 Sonderprüfungen zur Aufklärung von Fraud

13.1 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 und/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 dienen, die zu einer Gefährdung des Vermögens des Instituts führen können.

Das Institut sollte festlegen, welche Funktion/en (z. B. Zentrale Stelle, Compliance, Sicherheitsdienst, Interne Revision) Fraud-Untersuchungen durchführt/durchführen.

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 zunächst 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.

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 stellen nach dem One-crime-Ansatz der Aufsicht grundsätzlich eine Vortat zur Geldwäsche dar. 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.

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 der arbeitsrechtlichen Durchsetzbarkeit resultieren. In diesem Zusammenhang ist insbesondere zu berücksichtigen, dass eine Prüfung bzw. die resultierende Berichterstattung arbeitsrechtliche Fristen auslösen kann. Es ist – je nach Erfahrung der 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. Für Externe können entsprechende Rahmenverträge hilfreich sein, um zeitnah auf Externe zugreifen zu können. Führt die Interne Revision Untersuchungen selbst durch, ist sicherzustellen, dass dafür erforderliche Fähigkeiten bzw. Qualifizierungen ihrer Mitarbeiter vorhanden sind.

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

13.2 Ablauf der Sonderprüfung

13.2.1 Einleitungsvermerk

Hinweise auf Fraud können sich aus verschiedenen Anlässen ergeben:

- Auffällige Mangelkonstellationen werden von der Internen Revision im Rahmen von turnusgemäßen, risikoorientierten Prozessprüfungen festgestellt.
- 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. In diesem Zusammenhang sollte auch entschieden werden, ob sofort alle eventuell relevanten Daten vorsorglich gesichert werden, auch wenn zunächst noch keine Auswertung dieser Daten erfolgt. 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. Je nach Institut kann das Erfordernis bestehen, weitere Entscheidungsträger ebenfalls einzubinden.

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.

13.2.2 Dokumentationserfordernis 1: Zu dokumentierende tatsächliche Anhaltspunkte auf eine Straftat

Die Zulässigkeitskriterien des § 26 Abs. 1 S. 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.

13.2.3 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.

13.2.4 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.

13.2.5 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.

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

13.3.1 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.

13.3.2 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.

13.3.3 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.

13.3.4 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.

13.3.5 Auswertung von Daten inkl. elektronischer Kommunikation

Grundsätzlich ist zu unterscheiden, ob die Sonderuntersuchung mit oder ohne Wissen des/der Betroffenen erfolgt. In jedem Fall sollte die Auswertung von auf elektronischen Medien des Instituts (z. B. PC, persönliche Netzlaufwerke, ggf. Cloud-Lösungen) verfügbaren Daten, d. h. elektronische Kommunikation (z. B. E-Mails, Chat-Protokolle) und Dokumente, wegen ungewisser Rechtsrisiken mit dem Datenschutzbeauftragten bzw. der Rechtsabteilung abgestimmt werden. Zudem sollte vor Sicherung und Auswertung dieser Daten das Vorgehen im Hinblick auf die Beweissicherung geklärt werden.

Nachfolgend wird die Auswertung von E-Mails beispielhaft näher betrachtet. Das dargestellte Vorgehen sollte, soweit zutreffend, analog für andere Datenauswertungen angewendet 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.

13.3.6 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. Personalrats (ggf. über eine Betriebs- bzw. Dienstvereinbarung) sowie des Datenschutzbeauftragten erfolgen.

13.4 Prüfungsnachweise und Qualitätssicherung

13.4.1 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.

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.

13.4.2 Befragungen zur Gewinnung von Prüfungsnachweisen

Befragungen von Verdachtspersonen und anderen Mitarbeitern bedürfen einer erhöhten Sorgfalt. Befragungen von Verdachtspersonen sollten grundsätzlich durch mindestens zwei Personen geführt werden. Es ist zu prüfen, inwieweit Mitarbeiter vor der Befragung zu belehren sind, dass sie entweder aufgrund arbeitsrechtlicher Pflichten zu kooperieren

haben und alle Antworten richtig und vollständig zu geben sind (z. B. als Zeuge) bzw. dass sie das Recht haben zu schweigen (z. B. als Beschuldigte).

Falls Daten außerhalb der EU transferiert werden (z. B. bei Konzernen) ist der Mitarbeiter ggf. darüber zu belehren.

Es ist zu prüfen, ob der Mitarbeiter dahingehend zu belehren ist, dass das Gespräch aufgezeichnet wird bzw. schriftliche Notizen erstellt werden.

Es ist zu prüfen, ob über Verschwiegenheitspflichten zu belehren ist (z. B. Zeugen).

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.

13.4.3 Berichterstattung

Bei der Berichterstattung sind höchste Anforderungen an die Richtigkeit der Darstellungen und die Objektivität zu stellen. Es ist zu prüfen, ob weitere Informationspflichten, z. B. an die Aufsicht aufgrund von BT 2.4 MaRisk, bestehen.

Wichtige Meilensteine der Untersuchung (Einträge des Prüfungstagebuchs) sollten in die Berichterstattung aufgenommen werden, um eine stringente Prüfungsdurchführung zu belegen. Es sollte der Zustand des Compliance Management Systems und Internen Kontrollsystems vor der Prüfung beschrieben werden. Weiterhin sollten Aktualisierungen (z. B. Einführung zusätzlicher Kontrollen oder sonstige Mitigationsmaßnahmen) während der Prüfung in den Bericht aufgenommen werden. Sind mehrere Stellen des Instituts an der Prüfung beteiligt, sollte ihre jeweilige Rolle in der Prüfung beschrieben werden.

Sämtliche Prüfungsaussagen sind auf logische Schlüssigkeit zu untersuchen.

Empfänger und Zeitpunkt der Berichterstattung sind sorgfältig zu wählen. 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.

13.4.4 Qualitätssicherung

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

13.5 Ableitung von Erkenntnissen aus einer Sonderprüfung

Erkenntnisse aus einer Fraud-Untersuchung im Hinblick etwaige Mängel im Risikomanagement und Internen Kontrollsystem sind durch die Interne Revision aufzuzeigen. Die frühzeitige Dokumentation von Maßnahmen und deren zeitnahe Umsetzung kann geeignet sein, bei möglichem Organisationsversagen behördliche Sanktionen gegen das Institut zu verringern oder zu verhindern.

Die Umsetzung von Maßnahmen ist im Rahmen des Follow-up Prozesses der Internen Revision zu überwachen.

Erkenntnisse aus einer Sonderprüfung sollten nach Möglichkeit in die risikoorientierte Prüfungsplanung der Internen Revision einfließen.

Das Einfordern von Schadensersatz bzw. die Sanktionierung von Mitarbeitern ist durch die zuständigen Fachstellen bzw. Vorgesetzten zu initiieren, Das Institut sollte zudem prüfen, inwieweit Fraud-Schäden versichert sind.

Quellenverzeichnis:

DIIR, Positionspapier „Datenauswertungen und personenbezogene Datenanalyse: Beispiele für den praktischen Umgang im Revisionsumfeld“, Stand 2013.

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

14 Leistungsmessung in der Internen Revision anhand von KPIs

Die Aufgabe der Internen Revision sieht vor, die Organisation bei der Erreichung ihrer Ziele zu unterstützen, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese zu verbessern hilft. Letztendlich ist es das Ziel, durch Prüfungs- und Beratungsleistungen einen Mehrwert für das Unternehmen zu generieren.

Dabei ist es wichtig, dass auch die Interne Revision selbst darauf achtet, wie sie die Effektivität und Effizienz ihrer Prüfungs- und Beratungsleistungen im Hinblick auf ihre Aufgabenstellung sicherstellt und steuert, um somit einen größtmöglichen Mehrwert zu erzielen. Dabei ist der Fokus nicht nur auf eine effiziente bzw. „kostenoptimale“ Prozessdurchführung ausgerichtet, sondern muss insbesondere auch die Qualität der Prüfungs- und Beratungsleistung einbeziehen. Die qualitativen Aspekte spiegeln sich insbesondere in der umfassenden, objektiven Beurteilung von Sachverhalten und einer hohen Qualifikation der Prüfer wider.

Grundlage für die Anforderung einer internen Steuerung der Internen Revision ergeben sich auch aus den Internationalen Grundlagen für die berufliche Praxis (IPPF) (vgl. PA1300 – Programm zur Qualitätssicherung und -verbesserung). Der Leiter der Internen Revision muss demnach ein Programm zur Qualitätssicherung und -verbesserung das alle Aufgabengebiete der Internen Revision umfasst, entwickeln und pflegen und hat die Erfüllung der Aufgaben der Internen Revision laufend zu überwachen.

Aus den vorgenannten Aspekten ergibt sich der Bedarf, eine regelmäßige Leistungsmessung der Internen Revision durchzuführen. Dabei gilt es, eine Vielzahl von Informationen in geeigneter Form zu verdichten und die Relevanz für die Überwachung und Steuerung zu bestimmen. In der Praxis erfolgt die Umsetzung anhand von festzulegender Steuerungs- bzw. Kenngrößen, die auch als sog. Key Performance Indicator (KPI) bezeichnet werden.

14.1 Definition und Ziele von KPIs

Unter Key Performance Indicator (KPI) werden im Allgemeinen wesentliche 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. Dies ist auch im Rahmen der Ableitung von KPIs zu berücksichtigen.

Im Hinblick auf die Verfolgung strategischer und operativer Ziele dient die Ermittlung und Berichterstattung von KPIs u. a. auch dazu, unmittelbar oder mittelbar als ein Beurteilungskriterium bei der Festlegung der Vergütung bzw. der jährlichen Sonder-/Tantiemezahlung für den Leiter der Revision und ggf. für die Führungskräfte in der Internen Revision einzufließen.

14.2 Prozess zur Festlegung von KPIs

14.2.1 Idealtypischer Prozess in Anlehnung an die Implementierungsleitlinien des IPPF

Idealtypisch werden KPIs im Rahmen eines Prozesses abgeleitet. Hierbei sind zunächst die Faktoren, die die Effektivität einer Internen Revision im Hinblick auf ihre Aufgabenstellung ausmachen, zu bestimmen. Die Aufgabenstellung ergibt sich aus gesetzlichen bzw. aufsichtsrechtlichen Vorgaben, den berufsständischen Standards, den strategischen Zielen des Unternehmens sowie aus der strategischen Ausrichtung der Internen Revision bzw. ihrer Zielsetzung gemäß ihrer Audit Charter. Hieraus sind die konkreten Aufgaben und Zielsetzungen im Sinne eines Mindestumfangs und eines künftig angestrebten Zielwertes zu definieren.

In einem zweiten Schritt sind die in- und externen Interessensgruppen (Stakeholder) der Internen Revision sowie deren direkter bzw. mittelbarer Anspruch auf Verwendung der Ergebnisse der Internen Revision zu identifizieren. Dies schließt auch mit ein, wer entsprechenden Nutzen aus den Ergebnissen zieht und wer die Ressourcenausstattung direkt oder indirekt festlegt oder zumindest beeinflussen kann.

Auf dieser Basis können dann Messgrößen für die Effektivität und Effizienz der Internen Revision entwickelt werden, die auf unterschiedliche Stakeholder ausgerichtet werden 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 aus den definierten Kenngrößen für die Steuerung und Ausrichtung der Internen Revision zu verwenden.

14.2.2 Einbindung in Konzernstrukturen und Konzernvorgaben

Im Rahmen von Konzernstrukturen können darüber hinaus einzelne KPIs bereits von der Obergesellschaft vorgegeben bzw. kann die Interne Revision in eine konzernweite KPI-Struktur eingebunden werden. In der Praxis werden überwiegend von der übergeordneten Konzernrevision vorgegebene KPIs in den nachgeordneten Revisionseinheiten verwendet. 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 festgelegt werden.

14.2.3 Ableitung aus strategischen Zielen

Bei vielen Instituten werden im Rahmen der Revisionsstrategie oder der Audit Charter „strategische“ (Entwicklungs-) Ziele definiert. Sie ergeben sich unter anderem aus der Anforderung zur Qualitätssicherung und -verbesserung sowie zur Sicherstellung der Erfüllung der Aufgabenstellung (vgl. IPPF – PA1300 Programm zur Qualitätssicherung und -verbesserung)). Diese Ziele werden meist in konkrete Kenngrößen bzw. KPIs übersetzt, deren Entwicklungen für die laufende Steuerung der Zielerreichung ausgewertet werden. Zum Teil werden in der Strategie darüber hinaus auch konkrete Zielwerte festgelegt, anhand derer die jeweilige Zielerreichung eindeutig gemessen werden kann.

Diese aus den „strategischen“ Zielen abgeleiteten KPIs sind häufig deckungsgleich mit KPIs, die im laufenden Steuerungsprozess „operativ“ in der Internen Revision eingesetzt werden. Hierbei ist zu berücksichtigen, dass eine eindeutige Abgrenzung zwischen „strategischen“ und „operativen“ Zielen häufig in der Praxis schwer möglich ist bzw. diese Ziele ineinander übergehen.

Letztlich ist zu beachten, dass mit den KPIs Aspekte zur Effektivität als auch zur Effizienz der Internen Revision betrachtet werden können. Beide haben grundsätzlich strategische Implikationen, wobei sich die Effektivität intensiver mit dem grundsätzlichen Auftrag und den Anforderungen der Stakeholder auseinandersetzt, während sich die Effektivität auf die internen Prozesse der Internen Revision fokussiert.

14.2.4 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 häufig 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
- Mitarbeiter (inkl. Qualifikation)

Eine Umfrage im DIIR Arbeitskreis MaRisk zu genutzten KPIs aus diesen vier Perspektiven zeigte erwartungsgemäß auf, dass der Schwerpunkt, der in der Praxis angewandten bzw. ausgewerteten KPIs bei den Revisionsprozessen liegt und Finanzkennzahlen im Gegensatz dazu eine untergeordnete Rolle spielen. Hinsichtlich der Revisionsprozesse lassen sich die KPIs dagegen weiter in Kennzahlen zu Effektivität und Effizienz bzw. Plantreue aufteilen.

Bezüglich der Gliederung von KPIs für die Interne Revision sind auch weitere bzw. andere Aufgliederungen der Dimensionen wie beispielsweise zur IT-Unterstützung (Anzahl von Datenanalysen, Umfang des Continuous Monitorings, Umfang der IT-Unterstützung bei Prüfungsplanung und -durchführung) oder zum Wissensmanagement möglich.

14.2.5 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, ein einheitliches Verständnis zu Inhalt und Ermittlung der Kennzahlen zu schaffen und zu dokumentieren.

14.2.6 Managementaufgabe

In der Praxis werden KPIs grundsätzlich vom Leiter der Internen Revision festgelegt. Bei der Entwicklung der Kennzahlen bietet es sich an, eine Grundsatzabteilung wie auch die erste Führungsebene der Internen Revision in die Entwicklung von KPIs mit einzubinden, um damit auch intern die Akzeptanz und Steuerungswirkung zu erhöhen.

Ebenso ist es üblich, die entwickelten KPIs mit dem zuständigen Geschäftsleiter, ggf. auch mit der gesamten Geschäftsleitung, abzustimmen. In diesem Zusammenhang ist auch zu klären, in welchem Umfang KPIs zur Leistungsfähigkeit der Internen Revision

und entsprechende Erläuterungen gegenüber der Geschäftsleitung berichtet werden sollen.

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 Mitarbeitern ermöglichen können.

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.

14.3 Auswertung und Berichterstattung von KPIs

Die Ermittlung und Auswertung von KPIs mündet grundsätzlich in eine regelmäßige Berichterstattung, die an den Leiter und ggf. die Führungskräfte der Internen Revision gerichtet ist.

Eine Berichterstattung der KPIs an die Geschäftsleitung (und ggf. sogar an das Aufsichtsorgan) ist nicht weit verbreitet, wird aber bei einzelnen Instituten durchaus angewandt. Dabei kann der Umfang der intern ermittelten KPIs von dem Umfang der an die Geschäftsleitung berichteten KPIs abweichen und sich die Berichterstattung nur auf einzelne als wesentlich eingestufte KPIs begrenzen.

Die Berichterstattung von KPIs kann dazu dienen, die Einhaltung aufsichtsrechtlicher Vorgaben oder der Internationalen Grundlagen für die berufliche Praxis (IPPF), wie zum Beispiel der zeitnahen Berichterstattung oder der angemessenen Qualifikation der Mitarbeiter, zu dokumentieren.

Darüber hinaus ist es auch ein Medium, der Geschäftsleitung und ggf. dem Aufsichtsorgan (insbesondere dem Prüfungsausschuss) die Leistungsfähigkeit der Internen Revision darzustellen. Gleichzeitig wird eine kontinuierliche Leistungsmessung und -beurteilung der Internen Revision ermöglicht, wie dies auch bei anderen Einheiten des Unternehmens der Fall ist.

14.3.1 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 Datenzulieferungen erfolgen durch (ergänzende) zentrale, anlassbezogene Abfragen. Für die Auswertungen von KPIs werden zum Teil separate, zentral geführte Datenbanken eingesetzt. Die Auswertung der Daten erfolgt in der Regel auf monatlicher Basis, zum Teil aber auch quartalsweise.

In der Praxis wird der Zusatzaufwand für die Datenerfassung/Ermittlung für KPI 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.

14.3.2 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 dieses KPIs nichts über die Qualität der Prüfung selbst und der Bedeutung des Prüfungsgebiets 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 Berufsstandards könnten beeinträchtigt werden.

14.4 Steuerungsmaßnahmen

Die Auswertung und Berichterstattung von KPIs ist kein Selbstzweck, sondern stellt die erforderliche 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 Mitarbeiter daran ausrichten, ihr eigenes Handeln im Sinne der Zielwerte steuern und dadurch maßgeblich zur Erreichung der Ziele auf der Ebene 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 KPI 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.

14.5 Erwartungshaltung und Akzeptanz

Von Seiten der Stakeholder kann eine Erwartungshaltung hinsichtlich der Steuerung der Internen Revision anhand von KPIs und eine Berichterstattung an die Stakeholder bestehen. Aus der Praxis lässt sich kein eindeutiges Meinungsbild hierzu ableiten – eine mögliche Erwartungshaltung seitens der Stakeholder ist institutsindividuell und auch im Hinblick auf die unterschiedlichen Stakeholder-Gruppen abzuklären.

Es besteht eine hohe Erwartungshaltung seitens der Führungskräfte in der Internen Revision hinsichtlich der Steuerung nach Kenngrößen, entsprechend hoch ist auch der Akzeptanzgrad für deren Einsatz. Hingegen ist auf Ebene der Mitarbeiter die Akzeptanz von Kenngrößen typischerweise weniger stark ausgeprägt und löst zum Teil auch Widerspruch aus. Dabei sind die Bedenken hinsichtlich einer möglichen individuellen Leistungsmessung zu berücksichtigen. Daher sollte insbesondere gegenüber den Mitarbeitern die Ermittlung und Auswertung von KPIs sowie die abgeleiteten Aktivitäten und Maßnahmen transparent gemacht werden, um möglichen Vorbehalten entgegentreten zu können.

14.6 Kenngrößen für die Leistungsmessung der Internen Revision

Der DIIR Arbeitskreis MaRisk hat auf Basis der klassischen Perspektiven einer Balanced Scorecard die in der Praxis bei den Instituten der Mitglieder eingesetzten KPIs abgefragt. Neben der Häufigkeit bereits vordefinierter KPIs konnte über die Zumeldung weiterer in der Praxis eingesetzter KPIs ein großes Spektrum an relevanten Kenngrößen zur

Leistungsmessung der Internen Revision ermittelt werden. Die nachfolgenden Übersichten geben die Ergebnisse dieser Umfrage wieder.

Der Einsatz bzw. Umfang von KPIs ist abhängig von der individuellen Zielsetzung und der kulturellen Prägung der jeweiligen Internen Revision. Allgemeingültige bzw. als Mindeststandard zu verstehende Kenngrößen können daraus nicht abgeleitet werden.

Neben den einzelnen Kenngrößen sind auch deren Zielgrößen grundsätzlich von der jeweiligen Interne Revision individuell festzulegen. Auch hierbei kann kein allgemeingültiger Zielwert abgeleitet werden. Im Hinblick auf die Grenzen von KPIs (vgl. Abschnitt 1.3.2) sind Zielwerte als Einzelgrößen zu relativieren.

14.6.1 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 Jahresarbeitsplan	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/Termintreue 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 Schwergrad von Feststellungen	Anzahl von Feststellungen nach Risikoklasse/Schweregrad bzw. nach Zielrichtung
Externe Feststellungen an die Interne Revision	Anzahl der Feststellungen
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. 18: KPIs zum Revisionsprozess

14.6.2 KPIs zur Mitarbeiter-Perspektive

Bei den KPIs aus der Mitarbeiter-Perspektive handelt es sich häufig um quantitativ übersetzte Kenngrößen, die in der Regel auf qualitative Aspekte im Hinblick auf die Qualifikation (inkl. Einsetzbarkeit in anderen Einheiten) abzielen. Im Folgenden eine Auswahl möglicher KPIs zur Mitarbeiter-Perspektive:

KPIs zu Mitarbeiter-Perspektive	Erläuterung
Weiterbildungstage	Anzahl der Weiterbildungstage/Mitarbeiter
Mitarbeiteranzahl Interne Revision/ Gesamtunternehmen	Personelle Ausstattung der Internen Revision
Abrechenbare Prüfungsleistung (Prüfertage)	Einsatz der Mitarbeiter 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 Mitarbeiter mit Berufsexamina	(z. B. CIA, CISA, Interner Revisor^{DIIR}, Teilnahme an Fachseminaren)
Mitarbeiterzufriedenheit und -engagement	Ergebnisse aus Umfragen
Fristgerecht durchgeführte Beurteilungsgespräche	Nutzung von Potenzialbeurteilungs- und -entwicklungsmöglichkeiten

Abb. 19: KPIs zur Mitarbeiterperspektive

14.6.3 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, prüfungsnahe und sonstige Tätigkeiten	Verwendung der Ressourcen
Identifizierte Wirtschaftlichkeitspotenziale	durch Prüfungen/Beratungen generierte finanzielle Optimierungen

Abb. 20: KPIs zur Finanzperspektive

14.6.4 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 Revisionsauftrags
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. 21: KPIs zur Stakeholder-Perspektive

Quellenverzeichnis:

DIIR AK Revision in der Logistik: Key Performance Indicators (KPI) in der Internen Revision am Beispiel in der Logistik, ZIR 01/2012, S. 32.

Minder, S. W.: „What Do You Measure?“, Internal Auditor/The Institute of Internal Auditors, 01.04.2014, https://iaonline.theiia.org/what-do-you-measure.

The Institute of Internal Auditors (IIA): IPPF – Practice Guide „Measuring Internal Audit Effectiveness and Efficiency“, December 2010.

15 Schnittstelle mit Aufsichtsbehörden, externen Prüfern und der Zweiten Verteidigungslinie

15.1 Einleitung / Grundlage der Thematik

Eine Interne Revision sollte im gesamten Institut vernetzt sein und einen intensiven Austausch mit den Fachbereichen pflegen, um über aktuelle Entwicklungen informiert zu sein und auftretende Risiken möglichst frühzeitig erkennen zu können.

Zu den besonderen Schnittstellen der Internen Revision zählen die Einheiten der zweiten Verteidigungslinie (Kontrollfunktionen), die externen Prüfer bzw. Jahresabschlussprüfer und die Aufsichtsinstitutionen. Mit diesen gilt es eindeutige Aufgabenzuordnungen, Schnittstellen und Zuständigkeiten verbindlich festzulegen.

15.2 Schnittstelle zu der Zweiten Verteidigungslinie (inkl. weiteren Einheiten des Risikomanagements)

15.2.1 Grundlagen des Modells der Drei Verteidigungslinien

Das Modell der „Drei Verteidigungslinien“ (Three-Lines-of-Defense-Model) hat insbesondere seit seiner Erwähnung in den BCBS-Guidelines „The internal audit function in banks“ und im COSO „Internal Control – Integrated Framework“ stark an Bedeutung gewonnen und ist das aktuelle Grundmodell aufsichtsrechtlichen Denkens, daher wird dieses nachfolgend dargestellt. Eine Beschreibung des im Juli 2020 vom IIA veröffentlichten Papiers „The IIA’s Three Lines Model – An update of the Three Lines of Defense“ und dessen Einordnung erfolgt im Abschnitt 11.2.3.

Das Modell der Drei Verteidigungslinien (Three-Lines-of-Defense-Model) lässt sich graphisch wie folgt darstellen, wobei die Funktionen der zweiten Verteidigungslinie beispielhaft genannt sind (vgl. Abschnitt 15.2.2):[19]

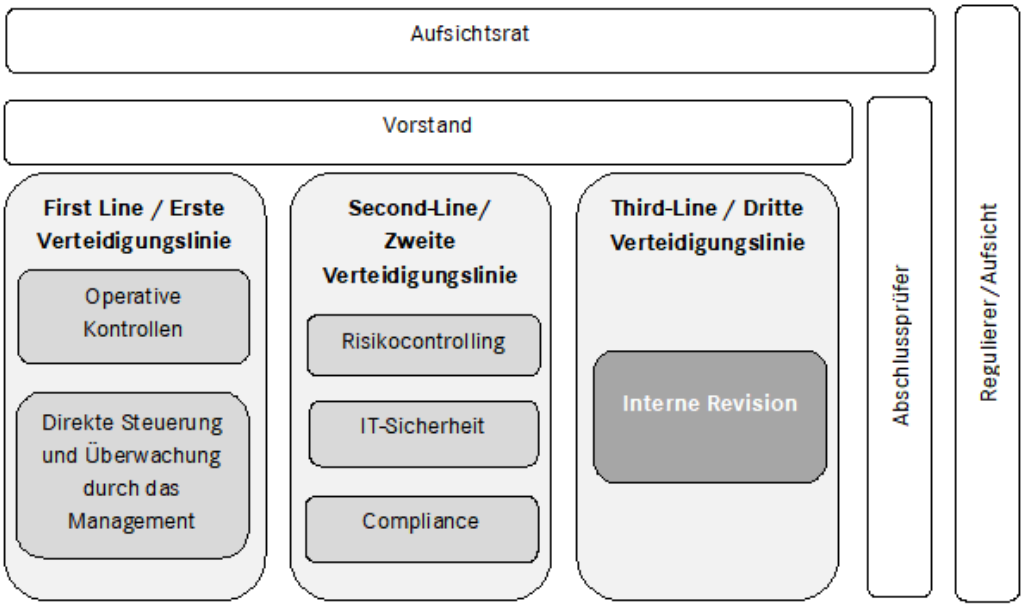


Abb. 22: Modell der Drei Verteidigungslinien

Im Sinne des Modells wird als erste Verteidigungslinie 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 Verteidigungslinie besteht aus der prozessabhängigen Überwachung und Kontrolle durch z. B. die Risikocontrolling-Funktion, die Compliance-Funktionen, etc. Die Einheiten der Zweiten Verteidigungslinie sollten im engen Austausch mit der Ersten Verteidigungslinie stehen und sicherstellen, dass die Risiken im Institut angemessen identifiziert und gesteuert werden und die implementierten Kontrollen bzw. Überwachungsprozesse wirksam umgesetzt werden. Hierzu führen die Verteidigungslinien eigene Kontroll-/ Überwachungshandlungen aus.

Die prozessunabhängige Interne Revision nimmt als dritte Verteidigungslinie 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 Verteidigungslinie) zu überprüfen und zu beurteilen. Die Übernahme von Aufgaben der ersten und zweiten Verteidigungslinie durch die

[19] In Anlehnung an das Positionspapier des IIA zum Three Lines of Defense Model.

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.

15.2.2 Operative Schnittstelle der Internen Revision und der Zweiten Verteidigungslinie

Die Interne Revision sollte einen intensiven und konstruktiven Austausch mit den Bereichen der Zeiten Verteidigungslinie pflegen, die teils auch als Beauftragtenwesen bezeichnet werden.

Zur Zweiten Verteidigungslinie können (in alphabetischer Reihenfolge) u. a. die folgenden Funktionen zählen. Je nach Institut können die Bezeichnungen variieren.

In den MaRisk werden unter „Besondere Funktionen“ in AT 4.4 folgende Funktionen der Zweiten Verteidigungslinie aufgeführt:

- Risikocontrollingfunktion
- Compliance-Funktion, ggf. mit
  - WpHG-Compliance-Funktion/ -Beauftragter
  - Geldwäschebeauftragter / Zentrale Stelle
  - Informationssicherheitsbeauftragter
  - Datenschutzbeauftragter

Darüber hinaus können die weiteren folgenden Funktionen ebenfalls prozessunabhängige Überwachungs- und Kontrollhandlungen in den Instituten vornehmen und können damit auch (institutsindividuell) der zweiten Verteidigungslinie bzw. dem Beauftragtenwesen zugeordnet werden:

- Marktfolge
- Beschwerdemanagement
- Vergütungsbeauftragter
- Liquiditätsmanagementfunktion
- QI Responsible Officer
- Zentrales Auslagerungsmanagement inkl. Auslagerungsbeauftragter
- (Zentraler) Data Quality Manager
- IT-Compliance

- Neutrale Stelle (§ 81 Abs. 5 WpHG)

Um einen konstruktiven und „mehrwertstiftenden“ Austausch zwischen der Internen Revision und den Einheiten der zweiten Verteidigungslinie sicherzustellen, sollte ein regelmäßiger und – je nach Bedeutung ggf. abgestufter – Austausch vereinbart werden. Dieser sollte unterjährig / fortlaufend und anlassbezogen sowie im Rahmen des Prüfungsplanungsprozesses der Internen Revision erfolgen.

Es sollten hierzu ferner eindeutige Informationswege und Anlässe zwischen der Internen Revision und den Einheiten der zweiten Verteidigungslinie definiert werden (Stichwort: Ab wann informiert wer wen über was?).

Empfehlenswert ist es festzulegen, dass, sofern der Internen Revision zumindest ein begründeter Anfangsverdacht hinsichtlich einer potenziellen Gefährdung oder Benachteiligung von Instituts- / Kunden- / Anlegerinteressen oder vergleichbarer Fälle, die in die Themenzuständigkeit einer Einheit der zweiten Verteidigungslinie fallen, durch die Internen Revision eine ad-hoc Information an die entsprechende Stelle zu erfolgen hat. Umgekehrt sollten eindeutige Sachverhalte / Fakten definiert werden, die zu einer ad-hoc-Informationspflicht der Einheiten der zweiten Verteidigungslinie an die Interne Revision führen.

Darüber hinaus sollte festgelegt werden, welche Einheiten der zweiten Verteidigungslinie Zugriff auf die Revisionsberichterstattung erhalten. Hier kommen insbesondere die Compliance- und Risikocontrolling-Funktionen in Betracht. Die Interne Revision wiederum sollte die durch die Einheiten der zweiten Verteidigungslinie erstellten Berichte vollumfänglich und unverzüglich erhalten.

Zur Optimierung von Schnittstellen sollten die Interne Revision und die Einheiten der zweiten Verteidigungslinie, und hier insbesondere die Compliance- und Risikocontrolling-Funktionen, Informationen über die Jahresplanungen zu Kontrollhandlungen und Prüfungen austauschen.

Die genannten Funktionen sind gleichwohl vollumfänglich Gegenstand der Prüfungstätigkeit der Internen Revision.

Die Prüfungs- / Kontrollergebnisse sollten zwischen den Parteien bekannt sein. Die Interne Revision kann die Kontrollergebnisse der Einheiten der zweiten Verteidigungslinie im Rahmen der Risikoorientierung der Prüfungsplanung / -tätigkeit berücksichtigen.

Ziel muss es sein, im Interesse des jeweiligen Hauses immer eine so weit wie möglich abgestimmte und effiziente Vorgehensweise zu implementieren und sicherzustellen, so dass sich an der (positiven) Schnittstelle zwischen Interner Revision und den Einheiten der zweiten Verteidigungslinie eine für das Institut mehrwertstiftende und effiziente Zusammenarbeit im Einklang mit dem Modell der Drei Verteidigungslinien ergibt. Als

Kommunikations-, Koordinations- und Überwachungsinstrument wird im IPPF hierfür eine Prüfungsübersicht (= Assurance Map) vorgeschlagen[20]

15.2.3 Einordnung des im Juli 2021 veröffentlichte „Three Lines Model – An update of the Three Lines of Defense“ (Three Lines Model)

Durch das Three Lines Model[21] (TLM) sollen unter anderem folgende Kritikpunkte am Modell der Drei Verteidigungslinien beseitigt werden:

- Ein „Silo-Denken“ zwischen den Linien wird gefördert und damit erfolgt zu wenig Kommunikation, Koordination und Zusammenarbeit.
- Die Linien suggerieren eine sequenzielle Abfolge der Tätigkeiten – zuerst die erste Line, dann die zweite Linie und abschließend die Linie.

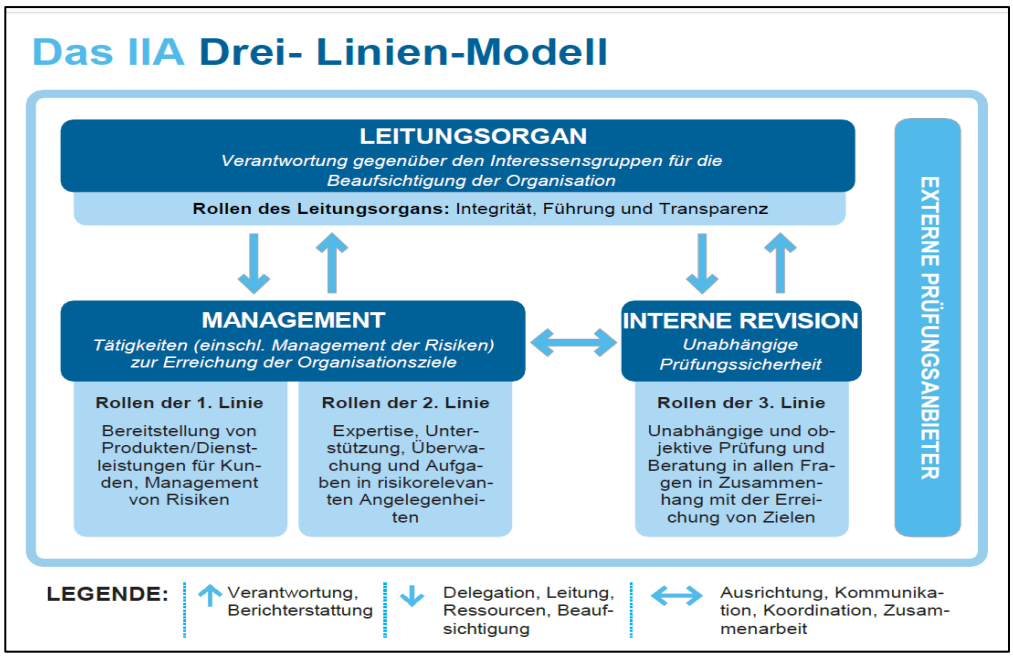


Abb. 23: Das IIA - Drei Linien-Modell

Das TLM versteht sich als Governance-Modell und nicht nur wie das Modell der Drei Verteidigungslinien als Risikomanagementmodell. Es geht nun insbesondere auch um Wertsteigerung und nicht nur Werterhaltung. Die Grundpfeiler des TLM sind eine Prinzipienorientierung mit der Einführung von sechs Grundsätzen, das neue Rollenmodell mit dem Fokus auf die drei Strukturelementen (Leitungsorgan, Management und Interne Revision)

---

[20] Praxisleitfaden Koordination und Vertrauen – Entwicklung einer Prüfungsübersicht, DIIR, 2020 (Version1).

[21] Formulierungen im Abschnitt 11.2.3 anlehnend an den grundlegenden Beitrag zum TLM Wissenschaftlicher Beirat des DIIR e.V., WPg 22/2021

innerhalb der internen Governance und die nachfolgende überarbeitete graphische Darstellung.

Das TLM besteht aus drei internen Strukturelementen ergänzend um externe Prüfungsanbieter. Abweichend zum Modell der Drei Verteidigungslinien wird der Regulierer nicht mehr berücksichtigt. Im Gegensatz zum Modell der Drei Verteidigungslinien steht nicht mehr die Struktur im Vordergrund, sondern es geht um „Rollen und Beziehungen, die zugewiesen, kombiniert oder getrennt werden können, und um Wechselbeziehungen“[22].

Es bleibt abzuwarten, wie die Aufsicht die Impulse aus dem TLM aufnimmt. Bis jetzt ist aufsichtsrechtlich das Modell der Drei Verteidigungslinien verankert. Die stärkere Vermischung bzw. Kombination von Erster und Zweiter Verteidigungslinie könnte aufsichtsrechtlich als problematisch betrachtet werden.

15.3 Schnittstelle Interne Revision Jahresabschlussprüfer

Die Schnittstellen zum Jahresabschlussprüfer sind eindeutig zu definieren und festzulegen. Dies betrifft insbesondere die internen Ansprechpartner und die Zuständigkeiten für die Vorbereitung und Begleitung der Jahresabschlussprüfung.

Die Interne Revision sollte einer der Ansprechpartner für die Jahresabschlussprüfer sein und diesen durch einen konstruktiven Austausch bei der Ausführung seines Prüfungsauftrags unterstützen. Die Prüfungsvorbereitung und die Prüfungskoordination auf Seiten des Instituts können, müssen aber nicht zwingend von der Internen Revision übernommen werden.

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.

Es sollte standardisiert ein regelmäßiger Austausch zwischen der Internen Revision und dem Jahresabschlussprüfer stattfinden. Gegenstand der Gespräche sollten 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. Für den Abschlussprüfer ist insbesondere IDW PS 321 (Interne Revision und Abschlussprüfung) relevant.

---

[22] So IIA/DIIR, Global Perspectives and Insights: Das Drei-Linien-Modell – ein wichtiges Instrument für den Erfolg jeder Organisation, Seite 6.

15.4 Schnittstelle Interne Revision (weitere) Externe Prüfer

In Bezug auf die Schnittstelle zwischen der Internen Revision und (sonstigen / weiteren) Externen Prüfern, sollte eine eindeutige Zuständigkeit für den Informationsaustausch/ -fluss festgelegt werden.

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. Hierbei sind auch Kommunikationswege an die Prüfer und im Haus zu definieren. Ferner sollte eine Eskalationsschwelle definiert werden, ab welcher der Vorstand eingeschaltet werden muss / sollte. Die Federführung für den Jahresabschlussprozess hierzu kann, muss aber nicht zwingend bei der Internen Revision liegen.

Zusammengefasst sollten dabei zumindest folgende Aspekte berücksichtigt und geregelt sein:

- Ansprechpartner in der Internen Revision
- Ansprechpartner in dem Kreditinstitut (sofern relevant)
- Informationsweitergabe (Was durch wen? Dokumentation der Unterlagen, Interviewdokumentation, Austausch telefonisch zulässig oder nur schriftlich, Fristen für Rückmeldungen, etc.)
- Wesentlichkeits-/Eskalationsstufen
- Abstimmungsprocedere von Feststellungen / des Berichtes
- Koordination / Durchführung notwendiger Berichterstattung & Beantwortung von Anfragen

15.5 Interaktion der Internen Revision mit Aufsichtsinstitutionen

Es finden bei (EZB-)beaufsichtigten Häusern 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 kleineren Häusern 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
- 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.

Darüber hinaus sollte der Leiter der Internen Revision grundsätzlich an allen Gesprächen zwischen dem Kreditinstitut und dem JST teilnehmen. Gleiches gilt für Gespräche des Kreditinstituts mit der Bundesbank und / oder der BaFin.

Sofern Prüfungsberichte der Internen Revision von einer Aufsichtsbehörde angefordert werden, so sollten diese durch den Leiter der Internen Revision zur Verfügung gestellt werden.

Es erfolgt ferner eine Information des Vorstandes 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 den Vorstand integriert werden.

15.6 Follow-up von Feststellungen aus externen Prüfungen

Es empfiehlt sich das Follow-up von Feststellungen aus externen Prüfungen (z. B. Aufsichtsbehörden, Jahresabschlussprüfer, etc.) in den Mängelbeseitigungsprozess der Internen Revision aufzunehmen.

Die Details hierzu sind im Abschnitt 4.6.1.4 (Behandlung anderer externer Prüfungsberichte) beschrieben.

IV. Autoren

Das Online-Revisionsbuch 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
Christopher Ecks	Kreditanstalt für Wiederaufbau
Anja Engel	UBS Beteiligungs- GmbH & Co. KG
Gert Eßer	TARGOBANK AG
Bernd Hombach	DZ BANK AG
Ulrich Hurmer	BMW Group
Lutz Kranzbühler	FORD BANK GmbH
Horst Ulrich Kremer	Stadtsparkasse Düsseldorf
Oliver Martens	Hamburg Commercial Bank AG
Thomas Maurer	Münchner Bank eG
Jan Meyer im Hagen	Finanz Colloquium Heidelberg GmbH
Thomas Millitzer	DekaBank
Rudolf Moschitz	Aareal Bank AG
Sabine Nakath	Deutsche Apotheker- und Ärztebank eG
Insa Redenius	ING-DiBa AG
Anna Reich	Landesbank Hessen-Thüringen Girozentrale
Jürgen Rohrmann	Union Investment
Jan T. Saul	DEG - Deutsche Investitions- und Entwicklungsgesellschaft mbH
Thorsten Schmidt	Deutsche Bank AG
Ines Schröder	Bayerische Landesbank
Sabine Schrödl	UniCredit Bank AG

Michael Seifert	Bausparkasse Schwäbisch-Hall AG
Sandra Strelow	Deutsche WertpapierService Bank AG
Monika Wiffel	NRW.BANK
Steve Wilkens	Commerzbank AG

An früheren Fassungen haben mitgewirkt:

Jochen Bender
Hubert Breuer
Gabriele Fischer
Jürgen Jung
Michael Helfer
Patricia Kordesch
Thomas Ramke
Günter Ruck
Holger Scharmann
Steffen Schöffler
Arne Schreiber
Manuela Straube
Oliver Terhorst
Holger Wagner