Hinweise zur Prüfung des Anti-Fraud-Management-Systems durch die Interne Revision auf Basis des DIIR Revisionsstandards Nr. 5

Arbeitskreis Abwehr wirtschaftskrimineller Handlungen in Unternehmen

DIIR Deutsches Institut für Interne Revision e.V.

Präambel

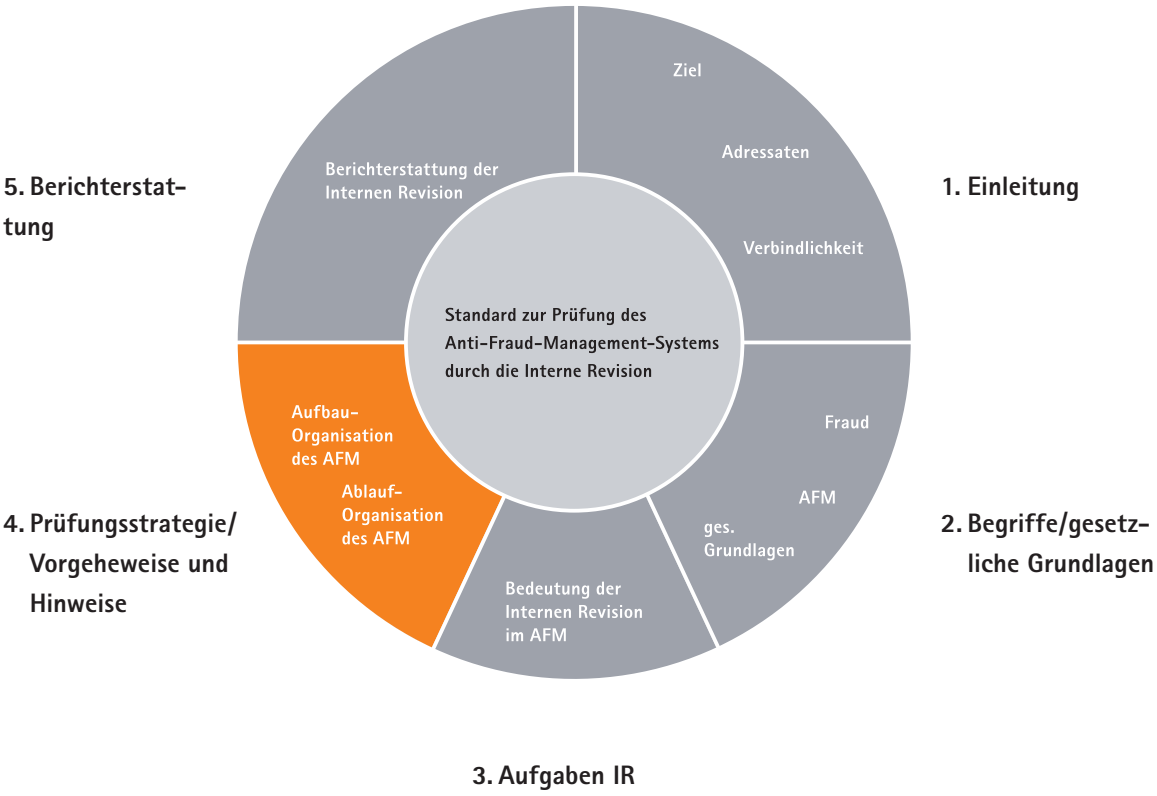
Die vorliegenden Hinweise wurden auf Basis des Revisionsstandards Nr. 5 erstellt und sollen Hinweise zur Vorgehensweise bei der Prüfung des Anti-Fraud-Management-Systems (AFM) durch die Interne Revision geben.
Im Rahmen einer notwendigerweise auf das Wesentliche beschränkten Darstellung berücksichtigen die Hinweise die Kernelemente eines risikoorientierten Prüfungsansatzes des AFM.

Die Hinweise erheben insoweit keinen Anspruch auf Vollständigkeit und sind jeweils auf die konkreten organisationsspezifischen Gegebenheiten auszurichten.

Insbesondere stellt sich die Frage, in wie fern angemessene Maßnahmen getroffen wurden, um bestehende Fraud-Risiken zu minimieren (Proportionalitätsprinzip).

Rechtliche Grundlagen, aus denen sich Hinweise für die Umsetzung eines AFM ergeben, enthält der DIIR Revisionsstandard Nr. 5. Für im internationalen Umfeld tätige Unternehmen sind ferner internationale Regelungen und Abkommen in Betracht zu ziehen.

DIIR Prüfungsstandard Nr. 5



4.1 Prüfung der Aufbauorganisation

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Ist auf Geschäftsleitungsebene die Zuständigkeit für das AFM festgelegt?	■ Geschäftsverteilungsplan, Organigramme ■ Rollen-, Stellen- bzw. Funktionsbeschreibungen ■ AFM-Prozesshandbuch ■ Flussdiagramm ■ Prozesshandbuch ■ Richtlinie zum AFM
Sind Rollen und Verantwortlichkeiten der am AFM beteiligten Personen definiert und umgesetzt? Gibt es eine personelle und sachliche Ressourcenzuordnung?	
Sind die Berichtswege ausreichend definiert?	
Ist ein AFM-Gremium oder ein sonstiges Gremium, das diese Funktionen übernimmt, eingerichtet?	■ Vorstandsbeschluss zur Einrichtung eines AFM-Gremiums (z. B. Compliance Committee) bzw. zur Benennung eines Fraud-Beauftragten ■ Charta/Geschäftsordnung des Gremiums ■ Protokolle von Sitzungen

4.2 Prüfung der Ablauforganisation

4.2.1 Anti-Fraud-Management-Ziele

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Gibt es eine Festlegung von Anti-Fraud-Zielen? (z. B. Verankerung im Leitbild der Organisation oder im Verhaltenskodex)	■ Fraud-Definition ■ Leitbild der Organisation ■ Unternehmensgrundsätze ■ Verhaltenskodex/Code of Conduct
Hat sich die Unternehmensleitung klar positioniert? Wird Fehlverhalten konsequent sanktioniert und kommuniziert? Sind eingeleitete Maßnahmen transparent und nachvollziehbar? Gibt es z. B. eine Zero-Tolerance-Regelung?	■ Videobotschaften/Artikel der Geschäftsleitung im Intranet ■ Rundschreiben der Geschäftsleitung ■ Richtlinien (beispielsweise zum Thema Anti-Korruption) ■ Dokumente zum Umgang mit Geschenken/ Einladungen/Hospitality

4.2.2 Fraud-Risiko-Erfassung und Fraud-Risiko-Bewertung

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Werden Risiken qualitativ strukturiert und regelmäßig erfasst? Werden die erfassten Risiken systematisch quantitativ bewertet? Liegen Bewertungskriterien vor? (z. B. Eintrittswahrscheinlichkeit und Einschätzung mögliche Schadenshöhe).	■ Methodik, Rollen und Verantwortlichen beschreibendes Regelwerk, z. B. Fraud Risk Assessment-Konzept, Handbuch, Verfahrensgrundsätze ■ Risikokategorisierung anhand Risikomatrix oder Risikocluster (Risikolandkarte) ■ Risikoinventur, Risikoworkshops ■ Risikointerviews, Risikofragebögen
Welche internen/externen Informationsquellen und Kriterien werden zu Grunde gelegt?	■ Geschäftsmodell, Organisationsstruktur, Mitarbeiter- und Kundenstruktur ■ branchen¬spezifische Hintergrundrecherchen, Datenanalysen ■ öffentlich verfügbare Informationen ■ aufgetretene Fraud Fälle/Anzahl bekannter Schadensfälle (Schadensfalldatenbank, Revisionsberichte etc.) ■ Meldungen einzelner Bereiche/Einheiten ■ Quartalsberichte ■ Meldung an Ermittlungs- und Aufsichtsbehörden ■ CPI-Index
Werden aktuelle Veränderungen (intern und extern) bei der Erfassung und Bewertung berücksichtigt? Gibt es unterjährige bzw. regelmäßige Reviews?	Dokumentation über die Überprüfung und ggf. Anpassung von Richtlinien (z. B. Versionierung)

4.2.3 Fraud-Risiko-Steuerung und Risiko-Begrenzung

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Gibt es eine Steuerung von Fraud-Risiken? Sind insbesondere die folgenden Elemente enthalten? a) Festlegung der Wesentlichkeit von Risiken durch die Geschäftsleitung, bei deren Erreichen mitigierende Maßnahmen zu ergreifen sind b) Implementierung geeigneter Maßnahmen zur Vermeidung/Verminderung wesentlicher Fraudrisiken	siehe auch 4.2.2 ■ Dokumentation des Internen Kontrollsystems ■ Dokumentierte Entscheidung über getroffene Maßnahmen bzw. Risikoakzeptanz (Protokolle, Ergebnisberichte) ■ Nachweis über neue Kontrollen (Arbeitsanweisungen, o. ä.)
Erfolgt ein Abgleich der Ergebnisse aus 4.2.2 (identifizierte Risiken) mit bereits getroffenen Maßnahmen? Werden neue Maßnahmen aus erkannten (und noch nicht gesteuerten) Risiken abgeleitet?	■ Dokumentation zum Abgleich zwischen identifizierten Fraud Risiken und bestehenden Kontrollen/Prozessen (GAP-Analyse) ■ Dokumentation zum Umgang mit verbleibenden Risiken
Wird die Umsetzung der Maßnahmen überwacht?	■ Meldungen zum Umsetzungsstand einzelner Maßnahmen ■ Quartalsberichte, sonstige Reportings an Entscheidungsgremien bzw. Vorstand/ Geschäftsführung

4.2.4 Anti-Fraud-Management-Kommunikation

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Werden die Mitarbeiter ausreichend über das AFM informiert?	■ Veröffentlichungungen der Geschäftsleitung im Intranet (z. B. Artikel, Videobotschaften) ■ Rundschreiben der Geschäftsleitung, Sensibilisierungsmails (z. B. anlassbezogen zum Weihnachts-/Neujahrsgeschäft) ■ Protokolle von Teammeetings
Werden zielgruppen- und aufgabenorientierte Schulungen und Sensibilisierungsmaßnahmen durchgeführt?	■ Verankerung von AFM in Personalentwicklung, Aus- und Weiterbildung ■ Einbindung von AFM in Kommunikationskonzept ■ Dokumentation über Schulungsteilnehmer und durchgeführte Schulungen (z. B. Einladungen, Teilnehmer- bzw. Signaturlisten, Zertifikate/ Teilnahmebestätigungen ■ Dokumentation der Inhalte (z. B. Präsentation, Ordner mit Schulungsunterlagen) ■ webbasierte Trainings, Präsenzschulungen ■ Teammeetings
Wie werden Mitarbeiter für die Schulungen ausgewählt?	Dokumentation über Auswahl der Zielgruppen
Werden Schulungskonzepte und Trainings regelmäßig aktualisiert? Erfolgt eine Anpassung der Zielgruppen bei Organisationsänderungen?	■ Versionierung der Schulungsunterlagen ■ Updatedokumentation, Änderungsdokumentation
Werden auch Externe (z. B. Lieferanten oder Kunden) in die Kommunikation eingebunden?	■ Übersendung von Merkblättern an Externe ■ Teilnahme Externer an Schulungen oder Trainings

4.2.5 Hinweisgebersystem

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Ist es organisationsspezifisches Hinweisgebersystem implementiert?	■ Telefonhotline ■ Ombudsmann ■ Vertrauensperson ■ elektronisches Postfach
Ist das Hinweisgebersystem geeignet und angemessen?	■ Gewährleistung der Anonymität des Hinweisgebers ■ Erfassung/Nutzung aller organisationsrelevanten Sprachen ■ Erreichbarkeit (im Idealfall 24h/7T) ■ Dokumentation der Meldung ■ Möglichkeit des Zugriffs von Dritten (z. B. Kunden oder Lieferanten) auf das System
Ist ein Prozess für den Umgang mit Hinweisen/ Hinweisgebern definiert, der auch die Erfordernisse des BetrVerfG, Arbeitnehmerschutzes, Datenschutzes, etc. miteinbezieht?	■ Dokumentation zur Abstimmung mit dem Datenschutz und dem Betriebsrat, **bei externen Anbietern:** Zertifikat des Anbieters, **bei IT-Anwendungen:** Systembeschreibungen, Berechtigungskonzepte, Prozess- oder Verfahrenshandbuch
Werden Meldungen dokumentiert und in angemessener Zeit bearbeitet? Werden entsprechende Maßnahmen eingeleitet?	■ Dokumentation des Prozesses: Eingang, Bearbeitung bis Abschluss (z. B. durch fortlaufende Nummernvergabe, Statusbogen, Fallbegleitbogen) ■ Ggf. Überprüfung des Prozesses anhand einer Testmeldung

4.2.6 Forensische Sonderuntersuchungen

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Im Rahmen des Standards wird davon ausgegangen, dass die Sachverhaltsaufklärung im Rahmen einer forensischen Sonderuntersuchung durch die Interne Revision durchgeführt wird. Insofern besteht hier keine Prüfungsnotwendigkeit der Internen Revision mit Bezug zum AFM. Nachfolgend werden zur Orientierung dennomögliche Fragestellungen und Vorschläge zur Erbringung von Nachweisen aufgeführt:	
Gibt es einen Prozess für Durchführung von forensischen Sonderuntersuchungen? **Wenn ja:** Ist dieser, sofern rechtlich erforderlich, mit Arbeitnehmervertretern oder/und Datenschutz und ggf. weiteren Bereichen abgestimmt? **Wenn nein:** Ist sichergestellt, dass bei konkreten Prüfungshandlungen insbesondere die Datenschutz-Anforderungen sowie Beteiligungsrechte nach dem BetrVG/BPersVG und dem TKG beachtet werden?	▪ Richtlinien (z. B. Anti-Fraud-Richtlinie Ermittlungsrichtlinie) ▪ Prüfungsleitfaden ▪ Datenschutz- oder Mitbestimmungscheckliste Siehe auch 4.2.7
Liegt eine Grundsatzentscheidung hinsichtlich der Einbindung von Strafverfolgungsbehörden/ Aufsichtsbehörden sowie anderer externer Stellen (z. B. externe Dienstleister) vor? Ist bei Sonderuntersuchungen ein adäquater Entscheidungsprozess zur Einbeziehung Strafverfolgungsbehörden/Aufsichtsbehörden/ externer Stellen etabliert? Werden die Entscheidungen aureichend dokumentiert?	▪ Schriftliche Strafanzeige ▪ Auftragsschreiben an externe Berater/ juristischen Beistand ▪ Presseerklärung ▪ Schadensmeldung an Versicherung
Wurden Sicherungsmaßnahmen getroffen? Ist bei Sonderuntersuchungen gewährleistet, dass zeitnah die erforderlichen Sicherungsmaßnahmen getroffen werden? Wird die Durchführung von Sicherungsmaßnahmen ausreichend dokumentiert?	▪ Dokumentation über Rückgabe von Betriebsmitteln (z. B. Laufzettel) ▪ Freistellungsmeldung ▪ Sperrungsmitteilung Kreditkarte/SIM-Karte ▪ Sperrungsbenachrichtigung Gebäudezutritt und IT-Systeme

Wurden Sicherungsmaßnahmen getroffen? Ist bei Sonderuntersuchungen gewährleistet, dass zeitnah die erforderlichen Sicherungsmaßnahmen getroffen werden? Wird die Durchführung von Sicherungsmaßnahmen ausreichend dokumentiert?	■ Dokumentation über Rückgabe von Betriebsmitteln (z. B. Laufzettel) ■ Freistellungsmeldung ■ Sperrungsmitteilung Kreditkarte/SIM-Karte ■ Sperrungsbenachrichtigung Gebäudezutritt und IT-Systeme
Sind die Ergebnisse für Dritte nachvollziehbar/ gerichtsverwertbar dokumentiert?	■ Schriftlicher verständlicher Prüfungsbericht (Inhalt: Prüfungsgegenstand, Prüfungsmethodik, Feststellungen und Ergebnisse der Prüfung, ggf. Empfehlungen und Maßnahmen) ■ Dokumentation zur Herleitung der Feststellungen ■ Interviewprotokolle ■ Dokumentation über Personalanhörungsgespräche

4.2.7 Anti-Fraud-Management-Reaktionsplan

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Existiert ein Reaktionsplan, der eine systematische Vorgehensweise bei Fraud-Fällen vorsieht? Sind die im Fraud-Fall zu beteiligenden Organisationseinheiten identifiziert? Ist durch die festgelegten Abläufe eine kurze Reaktionszeit gewährleistet? Ist eine zielgerichteteinterne und externe Kommunikation in einem Fraud-Fall gewährleistet?	■ Richtlinien (z. B. Anti-Fraud-Richtlinie, Ermittlungsrichtlinie) ■ Notfallplan mit Benennung zuständiger Gremien/ Personen/Verantwortlichkeiten ■ Prozess-/Ablaufchart/Folgepläne ■ Telefonliste mit Verfügbarkeiten ■ interne „Notrufnummer" Siehe auch 4.2.6
Ist der Reaktionsplan wirksam?	Stichprobe anhand ex post Betrachtung von Fraud-Fällen (Dokumentation der zeitlichen Ereignisse, Kommunikationswege, beteiligte Personen)

4.2.8 Berichtspflichten durch das Anti-Fraud-Management

Mögliche Fragestellungen	**Beispiele für Nachweise, Hinweise**
Besteht eine institutionalisierte Berichterstattung, die gewährleistet, dass die Geschäftsleitung und die Aufsichtsorgane ihre Aufsichts- und Überwachungspflichten erfüllen können?	Definierte Berichtslinien: Fraud-Beauftragter an Geschäftsleitung und jeweilige Aufsichtsgremien
Wird regelmäßig/anlassbezogen über laufende Fraud-Fälle berichtet? Wenn ja, an wen?	Regelmäßige/anlassbezogene Berichterstattung an Geschäftsführung, Fraud-Beauftragten, Aufsichtsgremien
Wird regelmäßig über laufende Maßnahmen im AFM berichtet? Wenn ja, an wen?	Regelmäßige Berichterstattung an Geschäftsführung, Fraud-Beauftragten, Aufsichtsgremien

5 Berichterstattung der Internen Revision

Mögliche Fragestellungen	Beispiele für Nachweise, Hinweise
Wird über die Prüfung des AFM ein Bericht erstellt? Sind wesentliche Punkt beschrieben? Insbesondere Darstellung des Prüfungsgegenstandes, der Prüfungs-methodik, getroffene Feststellungen, Maßnahmen	Schriftliche Berichterstattung (Prüfbericht) Aussagen haben Bewertung der Ordnungsmäßigkeit, Angemessenheit und Wirksamkeit des AFM zu enthalten
Wer ist Empfänger dieses Berichts?	Organisationsleitung, Leitungsebenen der am AFM-Prozess beteiligten Organisationseinheiten
Follow-Up der Maßnahmen	■ Dokumentation zur fristgerechten Maßnahmen-umsetzung (Maßnahmenverfolgung) ■ Nachschauprüfung