DIIR Deutsches Institut für Interne Revision e.V.

DIIR Revisionsstandard Nr. 5

STANDARD ZUR PRÜFUNG DES ANTI-FRAUD-MANAGEMENT-SYSTEMS DURCH DIE INTERNE REVISION

Herausgegeben vom DIIR unter Federführung des DIIR Arbeitskreises „Abwehr wirtschaftskrimineller Handlungen in Unternehmen “

Projektleitung
RA Lars Riether

Download unter

http://www.diir.de/fachwissen/veroeffentlichungen/standards

Veröffentlicht im Mai 2012 und geändert im September 2015 (Version 1.1), Frankfurt am Main

Inhaltsverzeichnis

1 EINLEITUNG

In Zeiten steigender Wirtschaftskriminalität und komplexer wirtschaftskrimineller Methoden sind immer mehr Unternehmen und öffentliche Institutionen (nachfolgend: Organisationen) der Gefahr ausgesetzt, durch wirtschaftskriminelle Handlungen eigener Mitarbeiter - z. T. auch durch das Zusammenwirken mit Externen - finanziell geschädigt zu werden. Verbesserte Aufdeckungsmethoden und eine präventive organisationsweite Erfassung von Fraud Risiken führen hier zu einer höheren organisationsinternen Aufklärungsquote doloser Handlungen.

Zur Vermeidung von Haftungsrisiken und Reputationsschäden ist es daher Aufgabe der Organisation, ein wirksames Anti-Fraud-Management-System (nachfolgend: AFM) zu installieren und Maßnahmen zur Abwehr wirtschaftskrimineller Handlungen zu implementieren. Dies geschieht sowohl im eigenen Interesse als auch aufgrund entsprechender gesetzlicher Verpflichtungen sowie sich daraus ergebenden Ausführungsbestimmungen.

1.1 Ziel des Standards

Das vorliegende Dokument beschreibt den ***Standard zur Prüfung des Anti-Fraud-Management-Systems*.**

Ziel ist es, auf Basis der aktuellen wissenschaftlichen und praktischen Erkenntnisse ein Rahmenwerk für die Prüfung des AFM in Organisationen durch die Interne Revision zu schaffen. Der Standard dient vor allem zur Planung durchzuführender AFM-Prüfungen und zur Konkretisierung des Prüfungsauftrags. Für Revisionsmitarbeiter ist der Standard somit ein „roter Faden“, der ihnen grundsätzliche Orientierung bietet und einheitliche Qualitätskriterien zur Beurteilung des AFM vorgibt. Im Rahmen einer notwendigerweise auf das Wesentliche beschränkten Darstellung berücksichtigt der Standard die Kernelemente eines risikoorientierten Prüfungsansatzes des AFM, der jeweils auf die konkreten organisationsspezifischen Gegebenheiten auszurichten ist. Der Standard erhebt insoweit keinen Anspruch auf Vollständigkeit.

1.2 Adressaten

Dieser Standard richtet sich operativ vorrangig an Leiter und Mitarbeiter der Internen Revision sowie an Compliance-, Risikomanagement-, Sicherheits- und Anti-Fraud-Beauftragte.

Für die Leitungsebene von Organisationen gibt der Standard mit Blick auf die Managementverantwortung und im Kontext der Corporate–Governance-Anforderungen Hinweise zur Erfassung, zur Bewertung und zum sachgerechten Umgang mit Fraud-Risiken.

Er soll weiterhin Grundlage für mit Fragestellungen des AFM befasste externe Dritte - wie zum Beispiel Wirtschaftsprüfer, Ermittlungs- oder Aufsichtsbehörden - sein.

1.3 Verbindlichkeit des Standards

Dieser Revisionsstandard wurde vom DIIR – Deutsches Institut für Interne Revision e.V. in einem sorgfältigen Verfahren entwickelt und verabschiedet. Er ergänzt als lokale Leitlinie das International Professional Practice Framework (IPPF). Die Anwendung dieses Revisionsstandards wird für Interne Revisoren in Deutschland dringend empfohlen.

Sind organisationsindividuelle Anpassungen notwendig, so ist der Standard sinngemäß anzuwenden.

2 BEGRIFFE UND GESETZLICHE RAHMENBEDINGUNGEN

Für die Wirksamkeit des AFM einer Organisation ist zunächst eine für diese Organisation inhaltliche Konkretisierung des Begriffes „Fraud“ vorzunehmen und zu dokumentieren. Dies ist notwendig, weil der deutsche Rechtsraum keine Legaldefinition des Begriffs „Fraud“ kennt. Zudem besteht auch in der Literatur keine abschließende Rechtsauffassung darüber, welche Tatbestände unter den Begriff „Fraud“ zu subsumieren sind.

2.1 Der Begriff „Fraud“

Allgemein werden unter „Fraud“ bewusst begangene unerlaubte Handlungen verstanden, die direkt oder indirekt zur Schädigung oder Gefährdung des Vermögens einer Organisation und/oder zu operationellen Risiken in den Geschäftsprozessen der Organisation führen können.

Vor diesem Hintergrund wird im vorliegenden Standard „Fraud“ als beabsichtigte Handlung einer oder mehrerer Personen - Mitglieder des für die Leitung und Überwachung einer Organisation verantwortlichen Managements, (sonstige) Mitarbeiter oder Dritte - bezeichnet, mit der ein ungerechtfertigter oder rechtswidriger Vorteil erlangt werden soll.

Derartige Handlungen können durch Mitglieder der Organisation (interner Fraud), Geschäftspartner der Organisation und durch nicht mit der Organisation verbundene Dritte (externer Fraud) begangen werden. Sie besitzen oftmals strafrechtliche Relevanz. Beispielhaft zu nennen sind hier Straftatbestände wie Diebstahl (§ 242 Strafgesetzbuch (StGB)) und Unterschlagung (§ 246 StGB), Betrug und Untreue (§§ 263, 266 StGB), Urkundenfälschung (§ 267 StGB), Geld- und Wertzeichenfälschung (§ 152 StGB), Begünstigung (§ 257 StGB), Geldwäsche (§ 261 StGB), Straftaten gegen den Wettbewerb (§§ 298, 299 StGB), Amtsdelikte (§§ 331 - 334 StGB) und Sachbeschädigung (§ 303 StGB).

Die organisationsindividuelle Ausprägung des Fraud-Begriffs sollte an den Vermögensgegenständen der Organisation sowie an ihren Sachzielen, den zur Erreichung dieser Ziele notwendigen Prozessen und den internen Richtlinien ansetzen. Es sollte systematisch mittels einer Risikoanalyse untersucht und dokumentiert werden, durch welche Art von Handlungen welche Personenkreise unter Nutzung welcher Hilfsmittel Vermögensgefährdungen oder -schädigungen konkret verursachen können. Die so festgestellten Handlungsmöglichkeiten zum Nachteil der Organisation sowie die Zuordnung der Handlungen zu Einzelpersonen bzw. Personenkreisen bilden den Inhalt des organisationsindividuellen Fraud-Begriffs. Im Sinne eines organisationsweit einheitlichen Verständnisses ist es insoweit erforderlich, das jeweilige AFM in seiner konkreten Ausprägung zu beschreiben.

2.2 Der Begriff „Anti-Fraud-Management“

Allgemein werden unter „Anti-Fraud-Management“ alle Maßnahmen einer Organisation verstanden, mit deren Hilfe

- Fraud vorgebeugt (Fraud Prevention),
- Fraud aufgedeckt (Fraud Detection),

- Fraud bei Hinweisen oder im Verdachtsfall strukturiert aufgearbeitet sowie auf offenbar gewordene Fraud-Fälle angemessen reagiert werden soll (Fraud Investigation).

Das AFM enthält somit grundsätzlich eine präventive, eine proaktiv und eine reaktiv prüfende Komponente und ist integraler Bestandteil eines organisationsweiten Compliance-Managements und des IKS.

Die organisationsindividuelle Ausgestaltung des AFM erfordert die Klärung aufbau- und ablauforganisatorischer Fragestellungen sowie Risiko- bzw. Wirtschaftlichkeitsabwägungen. Die Entscheidung über die konkrete Ausgestaltung des AFM sollte unter Berücksichtigung der organisatorischen Rahmenbedingungen und der Gestaltungsvorstellungen der Organisationsleitung getroffen werden. Hierbei sind die für die Organisation festgestellten möglichen nachteiligen Handlungen, die Personenkreise, die diese Handlungen begehen können, sowie die Gelegenheiten, die sich für diese Handlungen bieten, zu berücksichtigen.

Die der Ausgestaltung des AFM zugrundeliegenden Erwägungen (Risiko- und Wirtschaftlichkeitsabwägungen) sollten nachvollziehbar dokumentiert sein. Als Ergebnisse des Entscheidungsprozesses sollten eine verbindlich in der Organisation kommunizierte Beschreibung der Aufgaben und Befugnisse des AFM sowie eine Beschreibung seiner aufbauorganisatorischen Eingliederung vorliegen.

2.3 Gesetzliche und rechtliche Grundlagen, Standards und Risiken

Die Anforderungen für die Umsetzung eines AFM als wesentlicher Bestandteil des Risikomanagementsystems ergeben sich mittelbar aus den nachfolgend angeführten gesetzlichen Bestimmungen.

2.3.1 Allgemeine Anforderungen

Die im Zuge des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) eingeführte Vorschrift des § 91 Abs. 2 Aktiengesetz (AktG) bestimmt unter anderem, dass der Vorstand geeignete Maßnahmen zu treffen hat, insbesondere ein Überwachungssystem einzurichten hat, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Korrespondierend hierzu ist die Einhaltung der Maßnahmen nach § 91 Abs. 2 AktG im Hinblick auf das Bestehen und den Betrieb eines Risikomanagementsystems und der zugehörigen Maßnahmen im Bereich der Internen Revision nach § 317 Abs. 4 Handelsgesetzbuch (HGB) bei börsennotierten Aktiengesellschaften Gegenstand der Prüfung des Abschlussprüfers.

Der nach dem Wortlaut des § 91 Abs. 2 AktG nur für die Aktiengesellschaft geltende erweiterte Pflichtenkreis entfaltet nach der Begründung des Regierungsentwurfs zum KonTraG eine „Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen“. Aus den §§ 76 Abs. 1 und 93 Abs. 1 AktG wird darüber hinaus die Pflicht des Vorstands zur Legalitätskontrolle der im Unternehmen tätigen Mitarbeiter und der Ergreifung von geeigneten organisatorischen Maßnahmen abgeleitet.

Ziffer 4.1.3 des Deutschen Corporate Governance Kodex (DCGK) sieht dementsprechend vor, dass der Vorstand für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und auf deren Beachtung durch die Konzernunternehmen hinzuwirken hat (Compliance). Des Weiteren hat der Vorstand

den Aufsichtsrat nach Ziffer 3.4 Satz 2 DCGK regelmäßig, zeitnah und umfassend über alle für das Unternehmen relevanten Fragen der Risikolage, des Risikomanagements und der Compliance zu informieren. Zwar entfaltet der DCGK keine unmittelbare Rechtsbindung für Organisationen, da es diesen frei steht, die Regelungen des Kodex zu befolgen. Die im Zuge des Gesetzes zur weiteren Reform des Aktien- und Bilanzrechts, zu Transparenz und Publizität (TransPuG) eingefügte sog. Entsprechenserklärung des § 161 AktG bildet allerdings die Grundlage für die Implementierung der Corporate-Governance-Grundsätze in das Aktienrecht. Hiernach sind Vorstand und Aufsichtsrat verpflichtet, jährlich eine Erklärung darüber abzugeben, ob dem DCGK entsprochen wurde bzw. auch weiterhin entsprochen wird. Im Zuge der Neufassung des § 161 AktG besteht für börsennotierte Unternehmen die weitere Verpflichtung, Abweichungen von den Empfehlungen des DCGK in der Entsprechenserklärung zu begründen (sog. "comply or explain"-Prinzip).

2.3.2 Spezifische Anforderungen für Kredit- und Finanzdienstleistungsinstitute sowie Versicherungsunternehmen

Nach § 25a Abs. 1 Sätze 2, 3 des Gesetzes über das Kreditwesen (Kreditwesengesetz - KWG) sind bereichspezifisch die Geschäftsleiter von Kredit- und Finanzdienstleistungsinstituten für eine ordnungsgemäße Geschäftsorganisation verantwortlich, die insbesondere ein angemessenes und wirksames Risikomanagement umfassen muss. Nach § 25c Abs. 1 KWG müssen die Institute unbeschadet der in § 25a Absatz 1 KWG und der in § 9 Absatz 1 und 2 Geldwäschegesetz (GwG) aufgeführten Pflichten über ein angemessenes Risikomanagement sowie über Verfahren und Grundsätze verfügen, die der Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstiger strafbarer Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können, dienen. Die § 25a KWG konkretisierenden Mindestanforderungen an das Risikomanagement (MaRisk (BA)) geben dabei im Einzelnen den Rahmen für die Umsetzung des institutsinternen Risikomanagements, insbesondere die Festlegung von Strategien sowie die Einrichtung interner Kontrollverfahren, vor. § 64a Abs. 1 des Gesetzes über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz – VAG) enthält die § 25a Abs. 1 KWG, § 80d Abs. 1 VAG die § 25c Abs. 1 KWG entsprechende Regelung für Versicherungsunternehmen. § 64a VAG und § 104s VAG werden durch die aufsichtsrechtlichen Anforderungen an das Risikomanagement (MaRisk (VA)) konkretisiert.

Die Prüfung der Angemessenheit und Effektivität des nach den o. g. gesetzlichen Vorgaben einzurichtenden Risikomanagementsystems sowie die Beurteilung der Wirksamkeit der Maßnahmen zur Verhinderung und Aufdeckung doloser Handlungen, d. h. die Bewertung der Effektivität des AFM, stellt eine wesentliche Aufgabe der Internen Revision dar.

2.3.3 Spezifische Anforderungen für Öffentliche Institutionen

Für öffentliche Institutionen gibt es zum Teil spezifische Regelungen im Hinblick auf Fraud. So regelt zum Beispiel die Richtlinie der Bundesregierung (gemäß Artikel 86 Satz 1 GG) zur Korruptionsprävention in der Bundesverwaltung vom 7. Juli 2004, dass Risikoanalysen für besonders korruptionsgefährdete Arbeitsgebiete durchzuführen sind. Nr. 6 der Richtlinie führt aus, dass der Internen Revision die Aufgabe der Korruptionsprävention übertragen werden kann.

2.3.4 Rechtliche Risiken bei fehlender Implementierung eines AFM

Die Implementierung eines AFM dient neben der Verhinderung und der Aufdeckung von Fraud einerseits dem Zweck, Schadenersatzansprüche Dritter gegen die Organisation zu vermeiden (Außenhaftung). Andererseits besteht die Zielsetzung des AFM darin, Ansprüche der Organisation gegen die Mitglieder der Organisationsleitung und des Aufsichtsgremiums zu vermeiden (Innenhaftung). Ferner sollen auch Schadensersatzansprüche der Organisation gegen Dritte gewahrt werden, um (Reputations-)Schäden der Organisation zu verhindern. Bei fehlender Implementierung eines AFM bestehen neben zivilrechtlichen Schadensersatzansprüchen bei Compliance Verstößen sowohl straf- und ordnungswidrigkeitenrechtliche Haftungsrisiken für die verantwortlich handelnden natürlichen Personen als auch für die juristischen Personen bzw. Organisationen. Überblicksartig ergeben sich dabei vor allem die nachfolgenden Risiken:

- **Strafrechtliche Risiken**
  Die strafrechtliche persönliche Haftung verantwortlich handelnder Personen kann sich aus Täterschaft (§ 25 StGB) oder Teilnahme in Form der Anstiftung (§ 26 StGB) oder Beihilfe (§ 27 StGB) i. V. m. dem jeweiligen Straftatbestand ergeben.

- **Ordnungswidrigkeitenrechtliche Risiken**

  Das Ordnungswidrigkeitsrecht sieht im Vergleich zum StGB entsprechend § 14 Abs. 1 Satz 1 OWiG keine Unterscheidung zwischen Täterschaft und Teilnahme vor. Aus Gründen der Vereinfachung wird keine Beurteilung vorgenommen, inwiefern der jeweilige Tatbeitrag des Beteiligten als Täterschaft oder Teilnahme zu werten ist. Art und Umfang des Tatbeitrags sind vielmehr Grundlage für die Bußgeldbemessung.

  Zentrale Haftungstatbestände für juristische Personen sind die §§ 30, 130 OWiG. Der Inhaber eines Betriebes oder Unternehmens handelt gem. § 130 OWiG ordnungswidrig, wenn er vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die ihn treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist. § 30 OWiG erweitert diese Pflichten auf Geschäftsführer, Vorstände, leitende Angestellte sowie Aufsichtsräte und rechnet ihre Pflichtverletzungen dem Unternehmen zu (sog. Verbandsbuße). Im Falle einer vorsätzlichen Straftat kann die gegen das Unternehmen verhängte Geldbuße gem. den §§ 30 Abs. 2 S. 1, 130 Abs. 3 S. 1 OWiG bis zu einer Million Euro betragen. Ferner kann auch der für das Unternehmen angefallene Gewinn im Wege des Verfalls oder der Einziehung abgeschöpft werden (§§ 73 ff. StGB, 29a OWiG).

- **Kartellrechtliche Risiken**

  § 81 Abs. 4 Satz 2 GWB beinhaltet zudem eine praktisch bedeutsame Sonderregelung für Kartellbußen. Bei schwerwiegenden Verstößen gegen das deutsche oder europäische Recht kann gegen ein Unternehmen oder eine Unternehmensvereinigung eine den Grundbetrag von einer Million Euro überschreitende Geldbuße verhängt werden. Die Geldbuße darf 10% des in dem vorausgegangenen Geschäftsjahr erzielten Gesamtumsatzes des Unternehmens oder der Unternehmensvereinigung nicht übersteigen. Bei der Ermittlung des Gesamtumsatzes ist der weltweite Umsatz aller natürlichen und juristischen Personen zugrunde zu legen, die als wirtschaftliche Einheit operieren. Die Höhe des Gesamtumsatzes kann geschätzt werden.

3 AUFGABEN DER INTERNEN REVISION BEIM AFM

Die zentrale Aufgabe der Internen Revision mit Blick auf das AFM besteht darin, dessen Ordnungsmäßigkeit, Angemessenheit und Wirksamkeit zu prüfen und die Organe der Organisation - Organisationsleitung und Aufsichtsorgane – hierüber regelmäßig zu informieren.

Eine Besonderheit für die Interne Revision ergibt sich bei der Durchführung verdachtsbezogener Sonderuntersuchungen zu internem und externem Fraud. Hier fungiert die Interne Revision als aufklärende Instanz. Darüber hinaus wirkt sie aufgrund ihrer Prüfungsergebnisse als Impulsgeber für die kontinuierliche Weiterentwicklung präventiver Maßnahmen in den Geschäftsprozessen der Organisation. Ihre hierbei gewonnenen Erfahrungen nutzt sie zur Optimierung revisionsspezifischer Prüfungsansätze. Dies setzt voraus, dass die AFM-Prüfungshandlungen durch Revisionsmitarbeiter durchgeführt werden, die über entsprechende Berufserfahrung sowie die AFM-spezifischen Fachkenntnisse und persönlichen Fähigkeiten verfügen. Damit erfüllt die Interne Revision sowohl ihre präventive als auch ihre aufklärende Funktion im AFM.

Für eine ordnungsgemäße Geschäftsorganisation ist die eindeutige Zuordnung aller wesentlichen Verantwortlichkeiten notwendig. Ziel ist eine redundanzfreie Aufgabenwahrnehmung. Alle im AFM beteiligten Organisationseinheiten müssen ihre Aufgaben, Kompetenzen, Verantwortlichkeiten und Kommunikationswege kennen; bei allen Beteiligten muss Transparenz hierüber herrschen.

Um die Aufgabenzuordnung im AFM zu verdeutlichen, wird exemplarisch das „Three Lines of Defense (Drei Verteidigungslinien)“-Modell erläutert:

Bei dieser Betrachtung ist das AFM integraler Bestandteil des IKS. Betrachtungsgegenstände des AFM können z. B. folgende Teilbereiche sein:

- Einhaltung gesetzlicher und regulatorischer Vorgaben (bspw. zur Geldwäsche),
- Sicherheit von IT-Systemen und –verfahren,
- Effekte von personellen Veränderungen.

Fraudgefährdete Organisationseinheiten sind für Fraud-Risiken ausreichend zu sensibilisieren. Für die Geschäftsprozesse sind die erforderlichen Kontrollen zu definieren und durch die Geschäftsbereiche zu überwachen **(1. Verteidigungslinie)**. Dies bedingt ein grundlegendes Verständnis über die relevanten Prozesse und die prozessinhärenten Risiken. Insbesondere muss den beteiligten Mitarbeitern bewusst sein, welche konkrete Verantwortung sie bei der Gestaltung der Geschäftsprozesse sowie bei der Bearbeitung und Kontrolle der Geschäftsvorfälle haben.

Damit die Implementierung und die Durchführung der Kontrollmaßnahmen funktionsfähig und wirksam sind, muss eine laufende Überwachung der bestehenden Kontrollen durch die Überwachungsbereiche erfolgen. So ist innerhalb der Organisation durch ein Risk-Control-Self-Assessment sicherzustellen, dass angewiesene Kontrollen zu den identifizierten Risiken auch tatsächlich durchgeführt werden. Ergänzend muss der für das AFM Verantwortliche (AFM-Beauftragte) das AFM funktionsfähig implementieren und überwachen **(2. Verteidigungslinie)**.

Die Interne Revision **(3. Verteidigungslinie)** überprüft wiederum die Aufgabenerfüllung der Geschäfts- und Überwachungsbereiche und damit insgesamt die organisationsweite Ordnungsmäßigkeit, Angemessenheit und Wirksamkeit der getroffenen Kontrollmaßnahmen (System- und Verfahrensprüfung). Soweit AFM-Beauftragte benannt sind, erstreckt sich die Prüfung der Internen Revision insbesondere auf deren angemessene Aufgabenerfüllung. Einzelfallprüfungen bzw. analytische Prüfungshandlungen können

stichprobenartig erfolgen. Sie sind dann erforderlich, wenn die Überwachungsaufgaben nicht adäquat wahrgenommen oder bestehende Risiken bisher nicht erfasst wurden. Die Interne Revision kann zudem bei der Ausgestaltung und Anpassung des AFM durch die Organisationsleitung beratend einbezogen werden und Empfehlungen zur Verbesserung des AFM aussprechen.

4 PRÜFUNGSSTRATEGIE UND -VORGEHENSWEISE

Bei der Planung einer Prüfung des AFM sind die organisationsspezifischen Anforderungen und die darauf basierenden AFM-Maßnahmen und Prozesse systematisch zu erfassen. Diese sind unter Berücksichtigung der inhärenten Fraud-Risiken und der Fraud-Kontrollrisiken und im Hinblick auf ihre Praktikabilität zu analysieren. Insbesondere sind hierbei die Möglichkeiten des Auftretens doloser bzw. deliktischer Handlungen sowie die dadurch für die Organisation entstehenden Haftungs- und Reputationsrisiken in die Prüfungsstrategie einzubeziehen.

Ziel der Prüfung ist es, eine Gesamtaussage zur Ordnungsmäßigkeit, Angemessenheit und Wirksamkeit des implementierten AFM und möglicher bestehender Schwachstellen auf Basis der Beurteilung der Fraud-Risiken und der dazugehörigen AFM-Maßnahmen innerhalb der Organisation zu treffen. Hierzu muss eine nachvollziehbare und konsistente Dokumentation vorliegen, der die Aufbau- und Ablauforganisation des AFM zu entnehmen ist.

4.1 Prüfung der Aufbauorganisation des AFM

Die Basis für jede Prüfung ist das Organigramm, das im Einzelnen die am AFM-Prozess beteiligten Organisationseinheiten darstellt. Daraus lassen sich anhand von Rollen-, Stellen- bzw. Funktionsbeschreibungen die festgelegten Aufgaben und Zuständigkeiten sowie die Berichtswege entnehmen. Hierzu gehören auch die Rechte und Pflichten der jeweils am AFM beteiligten Personen. Voraussetzung für die Festlegung ist eine seitens der Unternehmensleitung festgelegte ausreichende personelle und sachliche Ressourcenzuordnung.

Die Prüfung muss sich insbesondere auf die neben der Internen Revision regelmäßig beteiligten Organisationseinheiten, wie beispielweise AFM-Beauftragter, Rechtsabteilung, Compliance, Personal, Sicherheit, Datenschutz und Risikocontrolling beziehen. Innerhalb der Organisation sind die bestehenden länder-, produkt-, kunden-, vertriebs- und transaktionsspezifischen Risiken jeweils hinsichtlich der Verantwortlichkeit nachvollziehbar zuzuordnen.

Dabei ist zu prüfen, ob zur Vermeidung von Überwachungslücken bzgl. bestehender Fraud-Risiken und von Redundanzen bei der organisationsweiten Risikoerfassung eine frühzeitige Schnittstellenanalyse zwischen den Organisationseinheiten durchgeführt wurde. Das AFM ist in die bestehenden Risikomanagementsysteme zu integrieren.

Zur Sicherstellung zeitnaher und organisationsspezifischer Entscheidungen sollte bei Fraud-Fällen ein Gremium (z. B. Compliance-/Fraud-Committee/Lenkungs-Ausschuss) unter Beteiligung der maßgeblichen Entscheidungsträger der vorgenannten Organisationseinheiten gebildet werden.

Prüfungsmaßstab für die prozessuale Ausgestaltung eines wirksamen AFM ist der organisationsspezifisch festgelegte Regelungsrahmen, der sich aus den schriftlich fixierten Rahmenkonzepten ergibt. Zu nennen sind insbesondere das für die jeweilige Organisation formulierte Leitbild und die ethischen Verhaltensgrundsätze („Code of Conduct“) sowie die darauf aufbauenden Richtlinien, Handbücher, Prozessbeschreibungen und Arbeitsanweisungen.

4.2 Prüfung der Ablauforganisation des AFM

4.2.1 AFM-Ziele

Ausgangspunkt der Prüfung der Ablauforganisation ist zunächst die Ausgestaltung von AFM-Prozessen dahingehend, ob die beabsichtigten AFM-Ziele mit den zuvor in dem organisationsspezifischen Regelungsrahmen vorgegebenen Zielen (z. B. Vermeidung von Interessenkonflikten, Korruption) übereinstimmen. Dies bedingt, dass die vereinbar ten Ziele an der Organisationskultur, dem Werteverständnis sowie der Vorbildfunktion der Organisationsleitung (z. B. „Tone at the Top“ und „Zero-Tolerance-Strategy“) ausgerichtet sind. Hierzu gehört neben der organisationsinternen Akzeptanz der AFM-Umsetzung das Vorhandensein einer angemessenen Risikokultur und eines entsprechenden Kontrollbewusstseins. Die Prüfungshandlungen erstrecken sich dabei auf die Analyse der von der Organisationsleitung schriftlich festgelegten Organisationsziele und Verhaltensgrundsätze, die Festlegung der Aufgaben, Kompetenzen und Verantwortlichkeiten der jeweiligen Organisationseinheiten sowie deren interdisziplinäre Kommunikations- und Berichtswege. Die organisationsinterne Akzeptanz wird dabei einerseits durch Anreizsysteme für regelkonformes Verhalten und andererseits durch Sanktionierung von Fehlverhalten gefördert.

Im Folgenden ist die Umsetzung der organisationsweit festgelegten AFM Ziele in den einzelnen Organisationseinheiten im Hinblick auf ihre jeweilige Zielerreichung, z. B. auf Basis der sog. SMART-Kriterien (**S**pezifisch, **M**essbar, **A**usführbar, **R**ealistisch, **T**erminiert), zu analysieren.

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

Prüfungsgegenstand ist, inwieweit eine angemessene Risikoerfassung (Risk-Assessment) integraler Bestandteil des AFM ist und in festgelegten regelmäßigen Abständen durchgeführt wird. Im Vordergrund steht dabei, inwieweit eine organisationsweite systematische und methodische Risikoerfassung erfolgt ist. Maßgebliche Prüfungskriterien sind die im Rahmen der Risikoanalyse zugrunde gelegten Informationsquellen und Kriterien, wie z. B. Geschäftsmodell, Organisationsstruktur, Mitarbeiter- und Kundenstruktur, Korruptionsindex (CPI-Index Transparency International), länder- und branchenspezifische Informationen (Presse, Internet, öffentliche Datenbanken etc.) sowie bekannte (interne/externe) Schadensfälle.

Ferner ist zu beurteilen, inwieweit zur kontinuierlichen Weiterentwicklung des AFM sichergestellt ist, ob aktuelle Veränderungen innerhalb und außerhalb der Organisation sachgerecht in die Risikoidentifikation einbezogen worden sind bzw. werden (Gesetzesänderungen, neue Geschäftsfelder, Handlungsmuster bei aufgetretenen Schadensfällen aus dolosen Handlungen, Mitarbeiter-Wechsel etc.).

Einzubeziehen ist ebenfalls die Erfassungsmethodik der Risiken. Als solche kommen in Betracht Interviews, Workshops, Fragebögen, Vertrags- und Dokumenteneinsicht, IT-gestützte Datenanalysen sowie branchenspezfische Hintergrundrecherchen zu ausgewählten Fraud-Risiken.

Nach der erfolgten Verifizierung der Risikoerhebung ist die durch das AFM erfolgte Bewertung der Fraud-Risiken zu prüfen. Ziel ist hier die Beurteilung der erfolgten Priorisierung der Fraud-Risiken. Diesbezüglich sind sowohl die angesetzten Bewertungsmaßstäbe der Einzelrisiken als auch die Gewichtungskriterien untereinander und bzgl. ihrer Relevanz für die Gesamtorganisation zu betrachten. Basis für die Risikoklassifizierung

ist eine matrixbasierte Darstellung der Parameter „Schadenshöhe“ und „Eintrittswahrscheinlichkeit. Im Anschluss ist zu prüfen, inwieweit durch das AFM auf dieser Grundlage eine organisationsrelevante Risikokategorisierung vorgenommen wurde. Zielrichtung sollte hier die Priorisierung möglicher materieller und immaterieller Haftungsfolgen sein. Hierauf basierend sind die durch das AFM festgelegten organisatorischen Zuordnungen der Risiken auf Ihre Zweckmäßigkeit zu beurteilen.

Als Ergebnis der Prüfung sind die vom AFM aufgestellte Risikolandkarte verifiziert und etwaige prozessuale und methodische Schwachstellen im AFM-Prozess identifiziert.

4.2.3 Fraud-Risiko-Steuerung und Risiko-Begrenzung

Zur Beurteilung des Wirkungsgrades des AFM hat die Interne Revision festzustellen, ob und in welchem Umfang ein systematischer Abgleich zwischen den identifizierten Fraud-Risiken und den bereits implementierten risikoreduzierenden Maßnahmen und Prozessen (Fraud-Performance-Assessment) vorgenommen wurde. Hierbei ist einzubeziehen, wie das AFM Warnsignale (Red-Flags) insbesondere bei identifizierten Hochrisiko-Bereichen bewertet und welche Maßnahmen daraufhin eingeleitet wurden.

Prüfungsgegenstand ist, ob im Sinne eines kontinuierlichen Verbesserungsprozesses die ermittelten Fraud-Risiken (sog. Bruttorisiken) dem vorhandenen Kontrollumfeld i. S. aller implementierten risikominimierenden Maßnahmen - wie z. B. Richtlinien, IKS (4-Augen-Prinzip, Funktionstrennung), Kompetenzregelungen, AFM-Schulungen etc. - zur Ermittlung der verbleibenden Risiken (sog. Nettorisiken) gegenübergestellt wurden.

Die Prüfung der Risikosteuerung beinhaltet, inwiefern eine Entscheidung hinsichtlich des Umgangs mit dem Nettorisiko in Form möglicher weiterer Risiko begrenzender und vermeidender Maßnahmen (z. B. weitere Kontrollen), der Verlagerung auf Dritte (z. B. Versicherung, Subunternehmen) oder der Risikoakzeptanz getroffen worden ist. Diese Entscheidung ist durch eine Lücken- (GAP-)Analyse auf ihre organisationsspezifische Angemessenheit hin zu prüfen. Zur Schließung identifizierter Schwachstellen sind Verbesserungsmaßnahmen auf Basis der von der Internen Revision ausgesprochenen Empfehlungen einzuleiten.

4.2.4 AFM-Kommunikation

Es ist darüber hinaus festzustellen, inwieweit die Entwicklung und Umsetzung eines wirksamen und den Organisationsbedürfnissen angepassten Kommunikationskonzeptes Bestandteil des AFM ist. Dieses beinhaltet zielgruppen- und aufgabenorientierte Schulungs- und Sensibilisierungsmaßnahmen in Form von Präsenz- oder webbasierten Trainings für die Organisationsleitung und die Mitarbeiter - soweit erforderlich - einschließlich eines Teilnahmenachweises. Hierbei muss deutlich werden, welche AFM-Inhalte intern an welche Personen in welchem Umfang kommuniziert werden.

Zudem ist turnusmäßig sicherzustellen, dass die erstellten Schulungskonzepte und eingeleiteten Trainingsmaßnahmen fortlaufend aktualisiert werden im Hinblick auf neue Mitarbeiter, Mitarbeiter-Wechsel innerhalb der Organisation oder veränderte Aufgaben und Organisationsänderungen. Die Aktualisierung umfasst in gleicher Weise anlassbezogene (aktuelle Fraud-Fälle) und wiederkehrende Ereignisse (z. B. Hinweis auf Geschenke-Richtlinie zu Weihnachten). Die Wahl des Kommunikationsmittels (z. B. Meetings, Newsletter, Merkblätter, Emails, Intranet) ist organisationsspezifisch und anlassbezogen festzulegen.

Die externe Komponente der Kommunikation beinhaltet die Bekanntgabe der spezifischen Anforderungen und Regeln für Dritte, z. B. gegenüber Kunden und Lieferanten.

4.2.5 Hinweisgebersystem

Ergänzender Bestandteil der AFM-Prüfung ist, inwieweit ein organisationsspezifisches Hinweisgebersystem implementiert ist. Als solches ist ein vertraulicher Kommunikationskanal zur Erlangung von Informationen zu verstehen, der Mitarbeitern und Dritten die Möglichkeit eröffnet, anonym mögliche Verstöße gegen interne und externe Regelungen und Gesetze zu melden. Als Formen von einzurichtenden Hinweisgebersystemen kommen IT-gestützte Verfahren, Ombudsleute sowie in- und externe Telefonhotlines in Betracht. Die Prüfung beinhaltet, ob die an ein Hinweisgebersystem zu stellenden grundlegenden Anforderungen, wie z. B. Anonymität des Hinweisgebers, Erreichbarkeit, Dokumentation der Meldung, Reaktion und eingeleitete Maßnahmen auf eingehende Meldungen, erfüllt sind.

4.2.6 Forensische Sonderuntersuchungen

Im Falle eines bestehenden Anfangsverdachts im Hinblick auf Handlungen, die dem organisationsspezifischen Fraud-Begriff entsprechen, ist es Aufgabe der Internen Revision, die Sachverhaltsklärung im Rahmen einer forensischen Sonderuntersuchung durchzuführen. Dabei sind im Wege eines zielgerichteten Vorgehens gerichtsverwertbare Erkenntnisse insbesondere auf der Basis von forensischen Interviews, IT-gestützten Dokumentenanalysen und fallbezogenen Hintergrundrecherchen zu gewinnen. Bei den beabsichtigten Prüfungshandlungen sind insbesondere die Anforderungen nach dem Bundesdatenschutzgesetz im Hinblick auf den Beschäftigtendatenschutz (BDSG) und mögliche Beteiligungsrechte des Betriebs- bzw. Personalrats nach dem Betriebsverfassungsgesetz (BetrVG) bzw. Bundespersonalvertretungsgesetz (BPersVG) zu beachten.

Im Ausland sind darüber hinaus länderspezifische rechtliche Rahmenbedingungen (z. B. Foreign Corrupt Practices Act (FCPA), UK Bribery Act) bereits bei der Prüfungsplanung zu berücksichtigen. Ferner ist gegebenenfalls eine Entscheidung über die Einbeziehung weiterer interner und externer Stellen (z. B. Strafanzeige bzw. Abstimmung mit den Ermittlungsbehörden bei anhängigen Verfahren, Information der Pressestelle, Beauftragung externer Rechtsanwälte bzw. Prüfungsteams, organisationsintern abgestimmte Schadensmeldung bei der Versicherung) zu treffen. Um mögliche weitere Schäden der Organisation zu verhindern, sind in Einklang mit dem AFM-Reaktionsplan (s. u. 4.2.7) einzelfallbezogen rechtzeitige Sicherungsmaßnahmen (z. B. Freistellung des verdächtigen Mitarbeiters, Einleitung von Maßnahmen zum vorläufigen Rechtsschutz, Sperrung von IT-Zugängen, Aushändigung mitarbeiterbezogener Betriebsmittel (Firmenausweis, PC/Laptop, Kreditkarte, Mobilfunktelefon etc.) in Abstimmung mit den weiteren beteiligten Organisationseinheiten (v. a. Personal, Recht, IT) zu veranlassen.

Ziel ist es, neben der Ermittlung der Tatbeteiligten insbesondere eine Aussage zur Höhe des eingetretenen oder zu erwartenden Schadens treffen zu können. Darüber hinaus dienen die Prüfungsergebnisse der kontinuierlichen Verbesserung des AFM und der Einleitung weiterer präventiver Maßnahmen.

4.2.7 AFM-Reaktionsplan

Die Prüfung der Internen Revision bezieht sich darauf, inwieweit das AFM einen organisationsspezifischen Reaktionsplan vorsieht, der die systematische allgemeine Vorgehensweise im Falle auftretender Fraud-Fälle oder eingeleiteter Maßnahmen von Ermittlungs- und Aufsichtsbehörden beschreibt. Ziel des Reaktionsplans ist es, die im Zusammenhang mit einem Fraud-Fall zu beteiligenden Organisationseinheiten zu identifizieren, eine kurze Reaktionszeit zu gewährleisten und die Zusammenarbeit der Beteiligten festzulegen. Dazu sind im Reaktionsplan die Verantwortlichkeiten, der zeitliche Ablauf einzuleitender Maßnahmen, die Abstimmung mit der Organisationsleitung und eventuellen externen Stellen sowie die Informationspflichten der am Prozess beteiligten Organisationseinheiten festzulegen.

Darüber hinaus sind die Angemessenheit und Wirksamkeit des Reaktionsplans, der darin festgelegten Prozesse und Kommunikationsabläufe zu analysieren sowie Verbesserungsmöglichkeiten aufzuzeigen. Die Prüfung der Angemessenheit beinhaltet vor allem den Abgleich des Sollplans hinsichtlich Konsistenz und Bekanntheit bei den einzubeziehenden Organisationseinheiten. Die Wirksamkeit sollte anhand einer ex post Betrachtung eingetretener Fraud-Fälle anhand analysefähiger Faktoren (z. B. Reaktionsdauer, Zeitpunkt der Weiterleitung fallbezogener Erstinformationen, Einbeziehung aller notwendig zu beteiligender Einheiten) erfolgen.

4.2.8 AFM-Berichtspflichten

Weiterer Prüfungsbestandteil für die Beurteilung des AFM ist, inwieweit das AFM in der Organisation Prozesse definiert hat, um bestehende Informations- und Berichtspflichten regelmäßig und zeitnah zu erfüllen. Dies beinhaltet eine institutionalisierte Kommunikation sowohl an die Organisationsleitung und die Aufsichtsorgane als auch an den AFM-Beauftragten. Dadurch wird einerseits sichergestellt, dass diese ihre gesetzlichen Aufsichts- und Überwachungspflichten erfüllen und im Falle von AFM-Verstößen angemessen reagieren können. Andererseits werden die Organisationsleitung und die Aufsichtsorgane regelmäßig oder anlassbezogen über den Zustand und die Wirksamkeit des AFM inkl. etwaiger Verbesserungsvorschläge in Kenntnis gesetzt.
Um auf aktuelle organisationsinterne (z. B. Fraud-Fall) und -externe Einflüsse (z. B. Gesetzesänderungen) mit entsprechenden Maßnahmen in angemessener Form reagieren zu können, ist eine anlassbezogene Kommunikation notwendig.

5 BERICHTERSTATTUNG DER INTERNEN REVISION

Die Prüfung des AFM schließt mit der Erstellung eines Prüfungsberichtes ab. Empfänger dieses Berichtes sind die Organisationsleitung sowie die Leitungsebenen der an dem AFM-Prozess beteiligten Organisationseinheiten. Der Bericht beinhaltet eine zusammenfassende Darstellung des Prüfungsgegenstandes, der gewählten Prüfungsmethodik und der getroffenen Feststellungen zum aktuellen Status des AFM. Insbesondere ist vor dem Hintergrund der organisationsinternen und -externen Anforderungen eine Bewertung der Ordnungsmäßigkeit, Angemessenheit und Wirksamkeit des AFM vorzunehmen. Ergänzend sind notwendige Maßnahmen und Empfehlungen zu formulieren. Diese sollten im Vorfeld mit den jeweils Verantwortlichen innerhalb der Organisation abgestimmt werden. Besondere Berichtspflichten infolge regulatorischer Vorgaben sind zu beachten. Die fristgerechte Umsetzung einzuleitender Verbesserungsmaßnahmen ist im Rahmen der Nachverfolgung bzw. einer Nachschauprüfung (Follow-Up Audit) zu überwachen.