

Whitepaper

Anti-Fraud-Management

Wirtschaftskriminelle Handlungen zu Lasten von
Finanzinstituten effektiv vermeiden



Stand: Juli 2015

Disclaimer

Die Inhalte der folgenden Seiten wurden von ORO mit größter Sorgfalt angefertigt. ORO übernimmt jedoch keinerlei Gewähr für die Aktualität, Korrektheit und Vollständigkeit der bereitgestellten Informationen. Haftungsansprüche gegenüber ORO, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen, sofern vonseiten OROs kein nachweislich vorsätzliches oder grob fahrlässiges Verschulden vorliegt. ORO behält sich ausdrücklich vor, Teile der Seiten ohne gesonderte Ankündigung zu verändern, zu ergänzen und/oder zu löschen. Alle Rechte vorbehalten. Die Reproduktion oder Modifikation ganz oder teilweise ohne schriftliche Genehmigung von ORO ist untersagt.

Inhaltsverzeichnis

1	Management Summary	6
2	Herausforderung Wirtschaftskriminalität	8
2.1	Die Notwendigkeit einer effektiven Betrugsbekämpfung steigt	8
2.2	Gesetzliche und aufsichtsrechtliche Grundlagen	9
2.3	Entwicklung wirtschaftskrimineller Verhaltensweisen	11
2.4	Risiken wirtschaftskrimineller Handlungen gefährden Institute	13
2.5	Einfallstore für deliktische Handlungen in Unternehmen	14
2.6	Identifikation von fraudspezifischen Risikofaktoren	15
3	AFM als Teil des unternehmensweiten Risikomanagements	17
3.1	Fraud Auditing	17
3.2	Fraud Prevention	18
3.3	Fraud Detection	18
4	Unser methodischer Lösungsansatz	19
4.1	Etablierung eines ganzheitlichen Anti-Fraud-Managements	19
4.2	Institutsbewertung mittels Fraud-Quick-Check	20
4.3	Implementierung und Durchführung einer Fraud-Risiko-Analyse	22
4.4	Entwicklung und Umsetzung einer Anti-Fraud-Management Strategie.....	24
4.5	Erfolgsfaktoren für eine wirksame Etablierung	26
5	Vorteile eines wirksamen Anti-Fraud-Management Systems	27
6	Anhang	28
6.1	Aufsichtsrechtliche Grundlagen (Auszug)	28
6.2	Einfallstore betrügerischer Handlungen	29
6.3	Glossar	32
7	Ihr Partner	33

Abkürzungsverzeichnis

AFM	Anti-Fraud-Management
BKA	Bundeskriminalamt
DK	Deutsche Kreditwirtschaft
IKS	Internes Kontrollsystem
PKS	Polizeiliche Kriminalstatistik
Wikri	Wirtschaftskriminalität

Abbildungsverzeichnis

Abbildung 1: Rechtliche und regulatorische Vorgaben zur Betrugs-bekämpfung	10
Abbildung:2 Polizeilich registrierte Fälle von Wirtschafts-kriminalität.	11
Abbildung:3 Polizeilich registrierte Fälle von Wirtschafts-kriminalität	12
Abbildung 4: Übersicht Risiken aus wirtschafts-kriminellen Handlungen für Institute. .	13
Abbildung 5: Interner vs. Externer Betrug.	14
Abbildung 6: Sieben Einfallstore für betrügerische Handlungen im Unternehmen.	15
Abbildung 7: Wie die Unternehmen ihr Risikomanagement nach der Krise anpassten	16
Abbildung 8: Lösungsansatz für die Etablierung eines institutsweiten Anti-Fraud- Managements.	19
Abbildung 9: Vorgehensweise im Rahmen des Fraud-Quick-Check.	20
Abbildung 10: Visualisierung der Risikosituation mittels Fraud-Risk-Map.	21
Abbildung 11: Standortbestimmung der Anti-Fraud-Organisation.	22
Abbildung 12: Fraud-relevante Risikobereiche der Gefährdungsanalyse.	22
Abbildung 13: Systemgestützte Fraud-Risiko-Analyse mit ANTALIS.....	23
Abbildung 14: Kritische Faktoren für die erfolgreiche Etablierung eines Anti-Fraud- Managements.	26

1 Management Summary

Auch Statistiken belegen, wovon Medien immer häufiger berichten: Der Anteil der Wirtschaftskriminalität nimmt an Bedeutung zu. Für das Jahr 2013 betrug der Anteil 50 % an sämtlichen in der polizeilichen Kriminalstatistik (PKS) ausgewiesenen Gesamtschäden von rund 8 Mrd. Euro. Bedeutende Großunternehmen – darunter zahlreiche Banken – wurden in der jüngeren Vergangenheit durch Betrugsfälle belastet, einige von ihnen gerieten dadurch in geschäftsgefährdende Krisen. Nicht erst die Medienberichterstattung macht klar: Schäden durch wirtschaftskriminelle Handlungen bleiben eine ernst zu nehmende Herausforderung für jedes Finanzinstitut, auch wenn die Aufklärungsquote in 2013 mit 93% deutlich höher liegt als bei der Gesamtkriminalität (55%) über alle Branchen hinweg.

Die Zunahme der Komplexität der Geschäftsbereiche, technische Infrastrukturen, bereichsübergreifende Arbeitsprozesse und Umbrüche in der Organisationsstruktur von Instituten führen dazu, dass sich das Entdeckungsrisiko (Wahrscheinlichkeit des Nichtentdeckens von wirtschaftskriminellen Handlungen) weiter erhöht. Die Gefahren wirken an unterschiedlichen Stellen und sind durch existierende Kontrollsysteme oft kaum zu identifizieren. Die sich daraus ergebenden gravierenden Risiken gefährden Institute in vielfacher Hinsicht. Finanzielle Schäden sind nur eine der Konsequenzen betrügerischer Aktivitäten – häufig erleidet ein Unternehmen durch die Wirtschaftskriminalität auch einen enormen Image- und Vertrauensschaden (Reputationsrisiko), welches für den zukünftigen Erfolg der Institution viel schwerer wiegt als der erlittene monetäre Schaden durch die kriminelle Handlung an sich.

Betrachtet man eine Organisation näher, finden sich oftmals Schwachstellen in der Aufbau- und/oder Ablauforganisation sowie den Prozessen, die nicht den regulatorischen Anforderungsansprüchen genügen und damit Gelegenheit bieten für eine Vielzahl betrügerischer Handlungen. Dazu kommt meist noch ein nicht ausreichendes internes Kontrollsystem (IKS), das mit seinen Lücken den Angriffswellen krimineller Energien widerstandslos gegenübersteht.

Erst ein unternehmensweites und einheitliches Anti-Fraud-Management hilft, materielle und immaterielle Werte im Unternehmen wirkungsvoll zu schützen. Eine erfolgreiche, zielgerichtete Strategie zur Bekämpfung wirtschaftskrimineller Handlungen und zum aktiven Umgang mit ihren Auswirkungen basiert auf den drei Komponenten: Fraud Auditing, Fraud Prevention und Fraud Detection.

Die Compliance-Awareness sowie die Compliance-Kommunikation sind stark zu beachtende Faktoren, um die Funktionsweise des unternehmensweiten Management-Systems zu gewährleisten. Das setzt voraus, dass die Mitarbeiter Kenntnisse über die maßgeblichen Compliance-Vorgaben besitzen und ein Bewusstsein hinsichtlich relevanter Compliance-Sachverhalte entwickelt haben. Erst wenn die Compliance-Kultur derart im Unternehmen verankert ist, wird jeder einzelne Mitarbeiter feststellen, dass Compliance kein „Geschäftsverhinderer“ ist sondern im Gegenteil, ein jeder Mitarbeiter durch sein aufgebautes Compliance-Bewusstsein ein risikoorientierter Berater innerhalb seines eigenen Unternehmens wird, wenn er es noch nicht ist. Diesen Status für Ihre Compliance-Kultur im Unternehmen zu bewirken ist ein wesentliches Hauptziel unserer Beratungsleistung.

Um ein wirksames Anti-Fraud-Management im Institut zu etablieren, ist eine methodische Vorgehensweise erforderlich, die analytische Instrumente mit indikativen Risikoansätzen verbindet. Ein ausgereifter Best-Practice-Ansatz zeigt konkrete Handlungsfelder auf, indem das Gefährdungspotenzial der verschiedenen

bankspezifischen Bereiche genau analysiert wird. Die risikobasierte Betrachtung von Geschäftsabläufen lässt die Schwachstellen in Prozessen, Produkten, Systemen oder gar auf Kontenbasis deutlich werden. Die Analyse der institutsspezifischen Gefährdungssituation bringt Ergebnisse, die der Definition konkreter Präventivmaßnahmen dienen. Ein solch ganzheitlicher Lösungsansatz berücksichtigt gleichermaßen die Unternehmensbedürfnisse wie auch die Erfüllung aufsichtsrechtlicher Anforderungen. Einen absoluten Schutz gegen wirtschaftskriminelle Handlungen gibt es allerdings nicht. Ein sinnvolles Präventionskonzept, das wirksam etabliert ist, kann aber entscheidend dazu beitragen, Risiken aus Betrugshandlungen aktiv zu minimieren und potenzielle Schäden für das Institut zu vermeiden.

2 Herausforderung Wirtschaftskriminalität

2.1 Die Notwendigkeit einer effektiven Betrugsbekämpfung steigt

Medienwirksame Fälle von Wirtschaftskriminalität und die stetig zunehmenden wirtschaftlichen und finanziellen Schäden für Institute haben das öffentliche Interesse an einer aktiven Betrugsbekämpfung verstärkt. Eine Vielzahl von Initiativen und Gesetzesnovellen verfolgen unter anderem dieses gemeinsame Ziel: Die Transparenz im Unternehmen zu verbessern und damit die Grundlage für Verfahren zu schaffen, die geschäftsgefährdende Risiken aus wirtschaftskriminellen Handlungen wirksam reduzieren bzw. vermeiden.

Mangels begrifflicher Definition wird sich an den in § 74c Abs. 1 Nr. 1-6b Gerichtsverfassungsgesetz (GVG) aufgeführten Straftaten orientiert, um Wirtschaftskriminalität zu spezifizieren.

Sämtliche Formen des Betrugs aus dem Strafgesetzbuch sowie Strafnormen aus anderen Gesetzen, die verschiedene Bereiche des Wirtschaftslebens regeln, wie den gewerblichen Rechtsschutz, das Kapitalgesellschaftsrecht und das Insolvenzrecht sind somit inbegriffen. Sämtliche Phasen des Wirtschaftslebens sind von Delikten betroffen; vom Anfang (z.B. Gründungsschwindel durch Angabe falscher Vermögensverhältnisse) bis zum Ausscheiden aus dem Wirtschaftsleben (z.B. Insolvenzdelikte).

Die Bandbreite der Wirtschaftskriminalität spiegelt sich exemplarisch in folgenden Tätigkeiten wieder: Betrug und Untreue im Zusammenhang mit Kapitalanlagen sowie Straftaten im Anlage- und Finanzierungsbereich, Delikte von Insiderhandel und Kursmanipulationen an den Börsen über betrügerisches Anbieten von unseriösen Anlageobjekten am "Grauen Kapitalmarkt" bis hin zu Wettbewerbsdelikten, Produktpiraterie und zum Vorenthalten und Veruntreuen von Arbeitsentgelt.

Im Unternehmen ein Problembewusstsein zu schaffen und unternehmensweit die Erkenntnis durchzusetzen, dass eine wirksame Betrugsbekämpfung unerlässlich ist, ist aus vielfältigen Gründen nötig:

- _ Vermehrtes Auftreten von internem und externem Betrug in Unternehmen aller Größenordnungen;
- _ Deutlich gestiegenes Öffentlichkeitsinteresse und wachsende Medienaufmerksamkeit für aufgedeckte Betrugsfälle;
- _ Signifikant hohe Schadenssummen können betroffene Unternehmen unvorhergesehen in finanzielle Schwierigkeiten bringen;
- _ Erhöhter Druck durch Gesetzgeber, Aufsichtsbehörden und Wirtschaftsprüfer zur aktiven Auseinandersetzung mit Betrugsprävention;
- _ Verstärkte Konsequenzen für Unternehmen und handelnde Personen, die von aufgedeckten Betrugsfällen betroffen sind;

Deutlicher Reputationsschaden für Unternehmen durch die öffentlichen Diskussionen um potenzielle oder tatsächliche Betrugsfälle.

Tatsächlich ist der Markt zunehmend sensibilisiert, was wirtschaftskriminelle Handlungen und ihre Auswirkungen angeht. Zum Stakeholderkreis gehören nicht mehr nur die Unternehmen und ihre organisatorischen Einrichtungen, vielmehr haben auch externe Dritte wie etwa Kapitalgeber oder Analysten ein Interesse an Sicherungssystemen in den Unternehmen. Darüber hinaus treten die Risiken der Wirtschaftskriminalität und die Maßnahmen, die zu ihrer Vermeidung ergriffen werden, mehr denn je in den Fokus der Wirtschaftsprüfer und Regulatoren. Aufsichtsrechtliche Vorgaben werden ausgeweitet und die Prüfungsgrundsätze von Abschlussprüfungen gleichzeitig an einem stärker risikoorientierten Ansatz ausgerichtet – beides belegt den wachsenden Informationsbedarf der potenziellen Stakeholder.

2.2 Gesetzliche und aufsichtsrechtliche Grundlagen

Gem. § 91 Abs. 2 AktG hat der Vorstand ein Früherkennungssystem einzurichten, um dem Going Concern-Prinzip Rechnung zu tragen. Weiterhin appellieren die Grundsatznormen § 93 Abs. 1 AktG sowie § 43 Abs. 1 GmbHG an die allgemeinen Sorgfaltspflichten und Verantwortlichkeiten der Vorstände respektive Geschäftsführer.

In Verbindung mit der Spezialnorm § 25a Abs. 1 KWG, die eine ordnungsgemäße Geschäftsorganisation vorsieht – insbesondere durch die Ausgestaltung eines angemessenen und wirksamen Risikomanagements – sowie der § 25c Abs. 3 und 4a KWG, die explizit ein wirksames Risikomanagement charakterisieren, sind die Institute verpflichtet, ein risikobasiertes Anti-Fraud-Management aufzubauen. Zudem muss die Wirksamkeit von internen Sicherungsmaßnahmen zur Verhinderung sonstiger strafbarer Handlungen nach § 25h KWG gegeben sein, damit das Vermögen des Instituts nicht gefährdet ist.

Die Aufsichtsbehörden achten verstärkt darauf, dass diese Anforderungen exakt erfüllt werden und Institute interne risikoorientierte Analyse- und Steuerungsverfahren zur Verhinderung von Betrugsrisiken implementieren.¹ Nicht zuletzt sind durch das RS 7/2011 /GW) der BaFin die Auslegungs- und Anwendungshinweise der deutschen Kreditwirtschaft (DK) zu § 25 h KWG (sonstige strafbare Handlungen) zwecks Konkretisierung als Leitlinien anerkannt worden und entsprechen somit der Verwaltungspraxis der BaFin.

Zur Einhaltung der Anforderung stehen die Geschäftsleiter in der Pflicht; bei Zuwiderhandlungen greifen die Haftungsnormen, mit denen sich die Vorstände und Geschäftsführer konfrontiert sehen.

Seit April 2011 ist der Prüfungsstandard 980 des IDW veröffentlicht worden. Hiermit werden die Anforderungen an ein Compliance-Management-System (CMS) konkretisiert und den Unternehmen wird die Möglichkeit gegeben, im Rahmen einer Zertifizierung durch einen Wirtschaftsprüfer ihrer Verantwortung als Geschäftsleitung nachzukommen. Zertifizierte CMS erleichtern zum einen die Kommunikation mit der Aufsicht

¹ Vgl. a. BaFin-Rundschreiben 8/2005 „Institutsinterne Implementierung angemessener Risikomanagementsysteme zur Verhinderung der Geldwäsche, Terrorismusfinanzierung und Betrug zu Lasten der Institute.

(Anforderungserfüllung) und zum anderen wirken sie als institutsspezifisch angepasste Systeme schadenshemmend und somit exkulpierend für die Heranziehung von Haftungsnormen gegenüber Vorständen und Geschäftsführern.

Abbildung 1:
Rechtliche und regulatorische Vorgaben zur Betrugsbekämpfung



Neben den zahlreich bestehenden nationalen Vorgaben erhöhen auch grenzüberschreitende Neuregelungen den Druck auf die Finanzinstitute, effektive Verfahren für den Umgang mit Betrugsrisiken umzusetzen. Mit der Umsetzung der dritten EU-Geldwäscherichtlinie² in nationales Recht wurden die Anforderungen an die internen Sicherungsmaßnahmen – insbesondere zur Verhinderung betrügerischer Handlungen zu Lasten der Institute (jetzt: sonstige strafbare Handlungen) – verschärft. Nicht zuletzt die mit der europaweiten Richtlinie verbundene Neufassung des § 25h KWG hebt die Bedeutung des Umgangs mit sonstigen strafbaren Handlungen im Institut und die Notwendigkeit angemessener Sicherungsmaßnahmen gegen Betrugsrisiken stärker als bisher hervor.

Über die Bankenlandschaft hinaus richtet sich der Fokus von Aufsichtsbehörden auch auf Unternehmen der Assekuranz. Die MaRisk VA³ konkretisieren bestehende gesetzliche Grundlagen – insbesondere den § 64a VAG. Zielsetzung der MaRisk VA ist es, durch die Einrichtung unternehmensinterner Leitungs-, Steuerungs- und Kontrollprozesse im Rahmen Solvency II die Wirksamkeit eines internen Risikomanagementsystems

² Richtlinie 2005/60/EG vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung.

³ MaRisk VA: Mindestanforderungen an das Risikomanagement von Versicherungsgesellschaften, der BaFin 3/2009,.

innerhalb von Versicherungsgesellschaften weitreichend zu unterstützen. Untrennbar gehört damit auch der Umgang mit Risiken aus sonstigen strafbaren Handlungen zu einem risikoorientierten Rahmenwerk in diesem Segment.

Kernelement dieser Initiativen ist die aufsichtsrechtliche Verpflichtung zur Einführung des risikobasierten Ansatzes, der eine erhöhte Wirksamkeit interner Kontrollmechanismen gewährleisten muss. Auch die aktuellen Entwicklungen im Schadensaufkommen unterstreichen, wie wichtig es für die Institute ist, im Hinblick auf Betrugsrisiken adäquate Managementverfahren einzuführen.

Ihr Partner

Reduzierung der Komplexität im Umgang mit regulatorischen Anforderungen



Die ORO Services GmbH („Outsourced Regulatory Office“) wurde mit dem Ziel gegründet, mit einem neuen innovativen Ansatz Banken bei der Bewältigung regulatorischer Anforderungen zu unterstützen.

ORO verfügt über ein eigenes Expertenteam mit langjähriger Erfahrung im Risikomanagement, in der Umsetzung regulatorischer Anforderungen, in den Themenstellungen Compliance und Geldwäsche sowie im Management komplexer Großprojekte.

Zur Ergänzung unserer internen Expertise und um gezielt Best-Practice-Ansätze in unser Serviceangebot aufzunehmen, arbeiten wir eng mit ausgewählten externen Kooperationspartnern zusammen, die über ausgewiesene und anerkannte Kernkompetenzen verfügen.

Autoren:

Norman Nehls (Partner Severn Consultancy GmbH)

Michael Otto (Manager)

ORO Services GmbH
Hansa Haus, Berner Straße 74
60437 Frankfurt am Main
T +49 (0)69 / 950 900-0
F +49 (0)69 / 950 900-50
Redaktion@oro-services.de
www.regupedia.de