Anti-Fraud-Management zur Minimierung von Betrugsrisiken

Risikobasierung als Chance

Laut Statistik ist jedes zweite Finanzinstitut Opfer wirtschaftskrimineller Handlungen, einige Banken geraten durch Betrugsfälle sogar in existenzgefährdende Krisen. Während der durchschnittliche Schaden aus wirtschaftskriminellen Handlungen in großen Unternehmen mit mehr als 5.000 Mitarbeitern im Jahr 2005 pro Fall noch bei ca. 3,4 Mio. Euro lag [vgl. PwC 2005], verloren diese im Jahr 2007 im Schnitt schon 6,7 Mio. Euro pro Wirtschaftsdelikt [vgl. PwC 2007]. Somit sollte jedes Finanzinstitut gut beraten sein, Schäden durch wirtschaftskriminelle Handlungen als sehr ernste Herausforderung zu verstehen, zumal ein Großteil aller betrügerischen Aktivitäten unentdeckt bleibt. Unmittelbare finanzielle Schäden sind dabei nur eine Konsequenz betrügerischer Aktivitäten – häufig erleidet eine Bank durch Fälle von Wirtschaftskriminalität auch einen enormen Image- und Vertrauensschaden.

Die Risiken der Wirtschaftskriminalität rücken in den Instituten nicht nur wegen der massiven finanziellen Auswirkungen und der verschärften aufsichtsrechtlichen Anforderungen stärker in den Vordergrund – auch Geschäftsleiter von Finanzinstituten standen noch nie so sehr persönlich im Fokus von Betrugsskandalen wie jetzt. Zudem zeigen Kapitalgeber und auch interne Kontrollgremien ein wachsendes Interesse an wirksamen Sicherungssystemen. Insbesondere der Aufsichtsrat legt sein Augenmerk zunehmend auf die Effizienz der Maßnahmen zur Bekämpfung von Betrugs- und Korruptionsdelikten. Zudem haben auch externe Dritte wie etwa Analysten ein Interesse an effektiven Sicherungsmaßnahmen gegen betrügerische Handlungen. Schließlich treten die Risiken der Wirtschaftskriminalität und die Maßnahmen, die Institute zu ihrer Vermeidung ergreifen, mehr denn je in den Fokus der Wirtschaftsprüfer und Regulatoren.

Der risikobasierte Ansatz zur institutsindividuellen Betrugsbekämpfung

Das qualitativ Neue an den aktuellen aufsichtsrechtlichen Vorgaben und an den modernen Prüfungsgrundsätzen für Abschlussprüfungen ist der Wandel hin zu einem risikobasierten Ansatz, wie er im angelsächsischen Raum schon etwas länger angewandt wird. Der Kern des risikobasierten Ansatzes ist die institutsindividuelle Risikoanalyse und Schadensabwehr: Die Regulatoren und Wirtschaftsprüfer verlangen von den Instituten nicht, dass sie einen fest definierten Maßnahmenkatalog umsetzen, sondern dass sie ihre unternehmensindividuellen Maßnahmen sinnvoll und nachvollziehbar an der institutsspezifischen Risikolage ausrichten. Unternehmensgröße, Organisationsstruktur sowie Geschäftskomplexität sind also die treibenden Faktoren für die Etablierung eines risikobasierten Anti-Fraud-Managements. Für die Institute bedeutet diese Ausweitung ihrer Eigenverantwortung nicht nur ein Mehr an Aufwand bei ihrer individuellen Betrugsbekämpfung, sondern auch eine beachtliche Chance: Ein unternehmensweites und einheitliches Anti-Fraud-Management trägt ganz entscheidend dazu bei, materielle und immaterielle Werte im Unternehmen wirkungsvoll zu schützen. Dies ist im Interesse der Finanzinstitute selbst, im Interesse ihrer Shareholder und im Interesse der Aufsichtsbehörden.

Dementsprechend wurden in den letzten Jahren auch zahlreiche gesetzliche Vorschriften geschaffen, die für das Anti-Fraud-Management relevant sind: So behandelt schon AktG § 91 Abs. 2 die Verpflichtung des Vorstandes zur Einrichtung eines Früherkennungs- und Risiko-Managementsystems. Aus KWG § 1 Abs. 2 Satz 1 in Verbindung mit § 25a Abs. 1 Satz 2 ergeben sich die „Verantwortung der Geschäftsleitung für ein angemessenes und wirksames Risikomanagement“ und „besondere organisatorische Pflichten“. Entsprechend fordert auch die BaFin in ihrem Rundschreiben 8/2005 eine „institutsinterne Implementierung angemessener Risikomanagementsysteme zur Verhinderung der Geldwäsche, Terrorismusfinanzierung und Betrug zu Lasten der Institute gemäß § 25 a Abs. 1 Satz 3 Nr. 6, Abs. 1a KWG, § 14 Abs. 2 Nr. 2 GwG“. Das erst kürzlich in Kraft getretene neue Geldwäschebekämpfungsergänzungsgesetz (GwBekErgG) führt ebenfalls dazu, dass die Aufsichtsbehörde verstärkt in den Bereich des Managements von Geldwäsche- und auch Betrugsrisiken eingreift. Nicht zuletzt die mit dem GwBekErgG verbundene Neufassung des § 25c KWG hebt die Bedeutung des Umgangs mit betrügerischen Handlungen im Institut und die Notwendigkeit angemessener Sicherungsmaßnahmen gegen Betrugsrisiken stärker als bisher hervor.

Typische Einfallstore für deliktische Handlungen

Betrachtet man eine Organisation näher, finden sich häufig Strukturen und Prozesse, die einer Vielzahl betrügerischer Handlungen Angriffspunkte bieten und die regulatorische Anforderungen nicht oder nur unzureichend abdecken. Ein zentrales Einfallstor für deliktische Handlungen in Unternehmen stellen die eigenen Mitarbeiter dar. Wie statistische Erhebungen belegen, sind dem internen Betrug circa 69 Prozent aller registrierten Fälle zuzuordnen [vgl. KPMG 2007]. Hinzu kommen Taten, die im Zusammenspiel von Mitarbeitern und Dritten begangen werden (so genannte Kollusivdelikte). Ein erhebliches Maß wirtschaftskrimineller Taten ereignet sich auf höheren Hierarchieebenen im Unternehmen. Die Häufung von Betrugshandlungen auf Führungsebene macht deutlich, dass dezidierte Kenntnisse von Mitarbeitern über das Unternehmen und das Wissen über interne Kontrollen und Maßnahmen die Gelegenheiten zum Betrug entscheidend vergrößern. Forensische Erfahrungswerte zeigen, dass dem Internal Fraud eine wesentliche Bedeutung zukommt – in Gestalt von Betrug, Untreue,

und Unterschlagung, aber auch in Verbindung mit externen Tätern, beispielsweise durch Korruption.

Untersucht man die Risikofaktoren in einem Unternehmen unabhängig voneinander, haben sie nur eine geringe Aussagekraft darüber, wie stark wirtschaftskriminelle Handlungen begünstigt werden. Es ist daher unerlässlich, die Risikofaktoren gesamthaft und bezogen auf die institutsspezifischen Strukturen zu bewerten. Typische Faktoren für Betrugsrisiken sind beispielsweise:

- Fehlende Richtlinien und Arbeitsanweisungen,
- Manipulationsmöglichkeiten für Mitarbeiter an Geschäftsvorgängen oder Systemen,
- mangelnde interne Kontrollmöglichkeiten,
- fehlende Prüfungsroutinen,
- manuelle Geschäftsvorgänge mit Ermessens- und Entscheidungsspielräumen,
- Kompetenzkonzentration und Rollenballung,
- fehlende Funktionstrennung sowie
- mangelnde Integrität einzelner Mitarbeiter – etwa ein mit der Position unvereinbarer Lebensstil.

Demnach stellen zahlreiche Faktoren Warnsignale für Betrugsrisiken dar. Sind einige Indizien stark ausgeprägt oder liegen sie gar in Kombination vor, führt dies zu einem deutlich erhöhten Gefährdungspotenzial für das Institut (vgl. ► **Abb.** 01 sowie ► **Tab.** 01).

Fraud Auditing, Fraud Prevention, Fraud Detection

Das Ziel eines Finanzinstituts muss es daher sein, ein Anti-Fraud-Management-System zu etablieren, das der Gesetzeslage Rechnung trägt und wirtschaftskriminelle Handlungen nicht nur wirkungsvoll aufdeckt und analysiert, sondern auch präventiv verhindern kann. Wichtig ist dabei eine sorgfältige organisatorische Integration in bereits bestehende Management- und Kontrollsysteme. Das Anti-Fraud-Management-System selbst basiert auf drei Komponenten: Fraud Auditing, Fraud Prevention und Fraud Detection. Die risikoorientierten Ansätze dieser drei Kernelemente und ihre Wirkungsweisen gilt es aufeinander abzustimmen und in einem gesamthaften Unternehmensansatz zusammenzuführen.

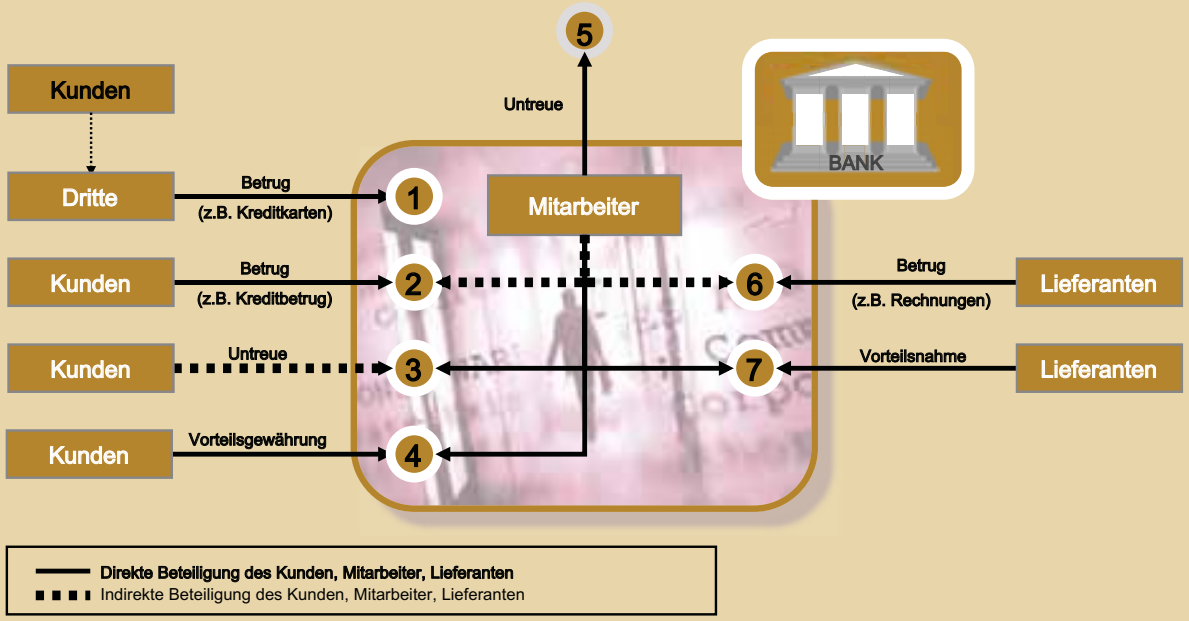
Fraud Auditing ermöglicht es mittels moderner forensischer Verfahren, das Risiko wirtschaftskrimineller Handlungen für alle Geschäftsbereiche und Funktionen innerhalb des Instituts einzuschätzen. Konkrete Fragestellungen sind unter anderem: Wie anfällig ist meine bestehende Organisation für Betrugsdelikte und wo befinden sich signifikante Kontrollschwächen? In welchem Umfang werden bisher die aufsichtsrechtlichen Anforderungen erfüllt? Welche Risikofaktoren sind innerhalb der Organisation vorhanden, die Gefahren aus vorsätzlichen wirtschaftskriminellen Handlungen signifikant erhöhen?

Fraud Prevention soll die direkten oder indirekten Schäden aus wirtschaftskriminellen Handlungen proaktiv verhindern oder minimieren. Hierbei stehen die Entwicklung und organisatorische Etablierung von Maßnahmen im Mittelpunkt. Präventive Maßnahmen bauen auf der umfassenden Risikoanalyse von Geschäftseinheiten, Geschäftsprozessen und Finanzprodukten des Instituts auf.

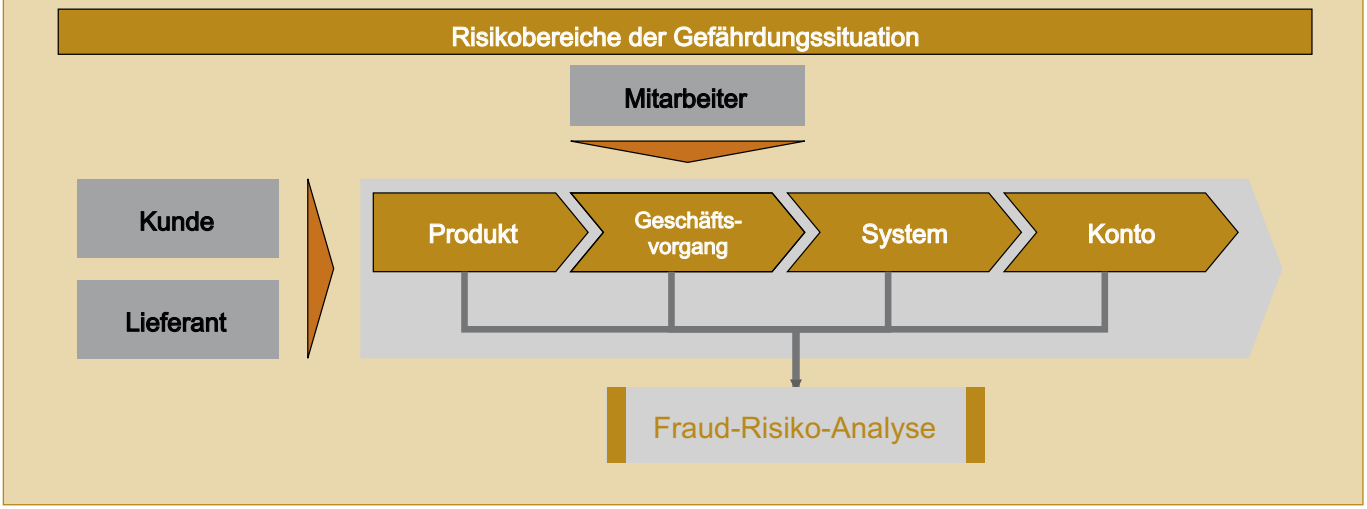
Fraud Detection umfasst alle Maßnahmen und Verfahren, die geeignet sind, Betrug und wirtschaftskriminelle Handlungen im Unternehmen aufzudecken, weitere Schäden zu verhindern und die Täter zu sanktionieren. Zu einer wirkungsvollen Fraud Detection gehört die Entwicklung eines adäquaten internen Kontrollsystems (IKS).

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

Sieben Einfallstore für Betrugshandlungen ► **Abb.** 01



Risikobereiche der Gefährdungsanalyse ▶ Abb. 02



Gefährdungspotenzial der verschiedenen bankspezifischen Bereiche genau analysiert wird. Die risikobasierte Betrachtung von Geschäftsabläufen lässt Schwachstellen in Prozessen, Produkten, Systemen oder gar auf Kontenbasis deutlich werden. Die Analyse der institutsspezifischen Gefährdungssituation bringt Ergebnisse, die der anschließenden Definition konkreter Präventivmaßnamen dienen.

Fraud-Quick-Check und Fraud-Risiko-Analyse als Basis

Ein initialer Fraud-Quick-Check als Teil des Gesamtkonzepts erlaubt einen ersten Grobüberblick über die Gefährdungssituation im Institut und über seine risikobehafteten Geschäftsbereiche. Im Rahmen dieser Standortbestimmung werden einige grundlegende Fragen beantwortet, wie etwa:

- Welche Schäden im Unternehmen sind auf wirtschaftskriminelle Handlungen zurückzuführen?
- Welche Unternehmensbereiche und Funktionen sind besonders anfällig für Betrugshandlungen?
- Ist meine Organisation darauf ausgerichtet, Fraud-Risiken präventiv zu vermeiden?
- Wie wirkungsvoll sind bereits vorhandene Maßnahmen?

Des Weiteren liefert der Fraud-Quick-Check mit einer Schwachstellenanalyse erste forensische Informationen. Hierzu dienen vor allem interne wie externe Revisionsberichte, Schadensdatenbanken des Risikomanagements, Typologiepapiere, Einschätzungen von Experten etc. Der Abgleich von Schadensmustern mit idealtypischen Risikobereichen gemäß forensischer Erfahrungswerte liefert dabei wertvolle Erkenntnisse über die institutsspezifischen Einfallstore und Gefahrenschwerpunkte für internen und externen Betrug. Aus den Ergebnissen des Fraud-Quick-Checks lassen sich so fundamentale Informationen für die weiteren Schritte bei der Etablierung des institutsindividuellen Anti-Fraud-Managements – beispielsweise für die Fraud-Risiko-Analyse – gewinnen.

Die anschließende detaillierte Fraud-Risiko-Analyse – auch als Fraud-Gefährdungsanalyse bezeichnet – identifiziert die Einfallstore für externe oder interne Betrugshandlungen in Gestalt verschiedener Risikobereiche. Einzelne Mitarbeiter und auch externe Dritte (wie Kunden oder Lieferanten) sind prinzipiell in der Lage, die Schwächen interner Organisationsstrukturen und Kontrollmechanismen systematisch auszunutzen – sei es als Einzeltäter oder in Kollusion. Den vier Risikobereichen Produkt, Geschäftsvorgang, System und Konto kommt daher in der Fraud-Risiko-Analyse eine besondere Bedeutung zu: Organisatorische oder technische Schwachstellen in diesen Bereichen erhöhen das Potenzial für wirtschaftskriminelle Handlungen drastisch (vgl. ▶ **Abb. 02**).

Die fundierte Prüfung und Bewertung bankspezifischer Geschäftsprozesse zeigt zudem konkrete Gefährdungspotenziale in den täglichen Arbeitsabläufen auf. Es ist ein Nebeneffekt der Fraud-Risiko-Analyse, dass sie auch regulatorische Anforderungen (beispielsweise an die Anfertigung einer institutsweiten Gefährdungsanalyse) erfüllt und den derzeit geltenden Wirtschaftsprüfungsstandards gerecht wird. Die Fraud-Risiko-Analyse stellt somit das tragende Element des risikobasierten Ansatzes dar und liefert den verantwortlichen Compliance- oder Risikomanagern wertvolle Erkenntnisse, wie ein Präventionskonzept auszugestalten ist, damit es bestehende Risiken effektiv reduziert.

Das institutsindividuelle Anti-Fraud-Management

Die Erkenntnisse aus dem Fraud-Quick-Check und aus der detaillierten Fraud-Risiko-Analyse bilden das Fundament einer risikoorientierten Prävention. Die grundlegende Idee des risikobasierten Ansatzes ist es ja, dass die Institute alle notwendigen Einzelmaßnahmen aus der Bewertung ihrer individuellen Gefährdungssituation ableiten können. So gestaltet ein Institut auf der Basis seiner Gefährdungsanalyse die geeigneten Maßnahmen zur Optimierung seiner internen Prüfungsroutinen aus (vgl. Tab 02). Die Implementierung eines funktionsfähigen Kontroll- und Überwachungssystems für die Risiken aus wirtschaftskriminellen Handlungen (eines Anti-Fraud-IKS), erfüllt die gesetzlichen Anforderungen und vermeidet zugleich wirtschaftliche Schäden. Im Mittelpunkt eines unternehmensweiten Anti-Fraud-Managements aber steht die Entwicklung einer Präventionsstrategie – als Summe effizienter Einzelmaßnahmen, die struk-

turell auf die Organisation und ihre Risiken abgestimmt sind. Im Rahmen der organisatorischen Verankerung im Institut ist es besonders wichtig, auch die Wechselwirkungen der Präventivmaßnahmen zu berücksichtigen. Nur wenn das System insgesamt eine hohe Wirksamkeit entwickelt, erreicht ein Institut einen effektiven Schutz gegen Wirtschaftskriminalität. Einige Einzelaktivitäten wie beispielsweise die Anwendung eines anonymen Hinweisgeber- oder Whistle-Blowing-Systems können ihre Wirkung in mehr als nur einem Unternehmensprozess entfalten. Mitunter erhöhen solche Synergien die Effektivität des gesamten Systems beträchtlich.

Die Ansatzpunkte für spezifische Präventionsmaßnahmen, die auf die institutsindividuelle Gefährdungssituation reagieren und eine organisationsübergreifende Betrugsbekämpfung erlauben, sind viel-

Sieben Einfallstore für Betrugshandlungen ▶ Tab. 01

Einfallstor	Konkretes Beispiel
1. Betrug durch Dritte an Kunden Dritte Personen gelangen illegal an relevante Kundendaten, um diese missbräuchlich zu verwenden. Den Kunden des Instituts entsteht dabei ein teilweise beträchtlicher Schaden, der meist durch das Institut ersetzt werden muss. Im Vordergrund der häufig durch die organisierte Kriminalität durchgeführten Aktionen stehen u. a. das Skimming von Debitkarten, die Fälschung von Kreditkarten und der Überweisungsbetrug im Zahlungsverkehr. Hinzu kommen Schäden durch Kartenverlust oder -diebstahl.	**Skimming von Kredit- oder Bankkarten** Durch den Einsatz von technischen Einrichtungen werden über Bankautomaten gleichzeitig der Magnetstreifeninhalt der Kredit- oder EC-Karte und die PIN ausgespäht. Dritte gelangen so an die Zugangsdaten der Karte. Nachdem die Betrüger diese Informationen auf einen Kartenrohling (sog. „White-Plastic“) aufgebracht haben, sind sie durch Kenntnis der PIN in der Lage, Bargeld an Geldautomaten abzuheben. Eine ähnliche Verfahrensweise wird bei Kreditkarten angewandt, indem hier die Karte des Kunden (etwa beim Bezahlvorgang im Einzelhandel) durch ein manipuliertes Kartenlesegerät ausgespäht wird.
2. Betrug durch den Kunden Tathandlung ist die Angabe falscher Informationen durch den Kunden, um wirtschaftliche Vorteile zu erzielen. Die Schwächen im System werden dabei von Kunden bewusst ausgenutzt, um entscheidungsrelevante Informationen zum eigenen Vorteil zu manipulieren. Wegen mangelnder Prüfung, fehlender Kontrollen oder unzureichender forensischer Expertise entsteht dem Institut durch die Disposition ein Vermögensschaden. Folgende betrugsrelevante Handlungen können dabei unterschieden werden: • Vorlage von unrichtigen und unvollständigen Unterlagen (etwa Bilanzen) • Schriftliche Falschangaben • Verschweigen von eingetretenen Veränderungen gegenüber den vorgelegten Unterlagen (Unterlassungsdelikt).	**Kreditbetrug** Ein Kreditnehmer erlangt einen Kredit auf der Basis falscher Angaben zur Bonität seines Unternehmens. Das Kreditinstitut entscheidet auf der Grundlage der gefälschten Bilanzen positiv über die Gewährung eines Kredites. Darüber hinaus werden Dokumente gefälscht, die insbesondere Angaben zu wertlosen Sicherheiten enthalten. Eine Prüfung der Sicherheiten hinsichtlich ihrer Werthaltigkeit auf der Grundlage der gefälschten Informationen des Kreditnehmers wurde durch den Mitarbeiter zwar durchgeführt – eine Kontrolle der Dokumentationen auf ihre Echtheit fand allerdings nicht statt.
3. Betrug durch den Mitarbeiter zu Lasten des Kunden Der Mitarbeiter nutzt das über die Jahre hergestellte Vertrauensverhältnis zum Kunden aus und gelangt so an sensible Daten und Informationen des Kunden, die er zum eigenen Vorteil nutzen kann. Mögliche Formen des Mitarbeiterbetrugs zu Lasten des Kunden können sein: • Nicht autorisierte Überweisungen auf das eigene Konto • Bewusst unrichtige Informationsweitergabe an den Kunden • Erschleichen von nicht freigegebenen Informationen	**Kontoeröffnungs- und Überweisungsbetrug** Der Mitarbeiter veranlasst nicht autorisierte Überweisungen von Kundengeldern auf das eigene Konto. Da für den Kunden ein Postverwahrungsvermerk vorhanden ist, werden Konto- und Depotauszüge vom Institut – bzw. vom Mitarbeiter – zurückgehalten. Aktuelle Kontenbewegungen werden dadurch verschleiert und können so erst sehr spät entdeckt werden.
4. Betrug durch den Kunden in Zusammenarbeit mit dem Mitarbeiter (kollusiv) Es findet eine aktive Zusammenarbeit zwischen Mitarbeiter und Kunden statt – mit der Absicht, die Bank zu schädigen. Die beiden Parteien nutzen dabei die internen Prozesse für sich aus. Kennzeichnend für die Tathandlung ist die Gewissheit, den internen Kontrollen ausweichen zu können, da die wirtschaftskriminelle Handlung von beiden bewusst eingegangen und entsprechend verschleiert wird.	**Kreditvermittlungsbetrug (Gegenseitige Vorteilsgewährung, „Korruption“)** Der Firmenkundenbetreuer bekommt die interne Anweisung, einem langjährigen Kunden keine weitere Kreditlinie zu gewähren, da dem Unternehmen durch diverse Immobilienprojekten bereits die Insolvenz mit potenziellen Schäden im mehrstelligen Millionenbereich droht. Nach Annahme einer wertvollen Armbanduhr genehmigt der Betreuer eine weitere Überziehung der Firmen-/Privatkonten und stellt eine neue Kreditkarte für den Firmeninhaber aus. Der Schaden für die Bank aus den nach der Insolvenz nicht rückzahlbaren Krediten wird auf mehrere Millionen geschätzt.
5. Betrug durch den Mitarbeiter zu Lasten des Instituts Der in langjähriger Zusammenarbeit gewachsene Informationsstand des Mitarbeiters birgt die Gefahr, dass er Schwachstellen des internen Kontrollsystems bewusst zu seinem Vorteil ausnutzt. Das dem Mitarbeiter entgegengebrachte Vertrauen schützt ihn vor intensiven Kontrollvorgängen. Mögliche Formen des direkten Mitarbeiterbetrugs zu Lasten des Instituts sind: • Abrechnung von privaten Rechnungen • Erschleichen von Leistungen • Manipulation bestehender Computersysteme • Entwenden von Firmeneigentum	**Computerbetrug** Ein Bankmitarbeiter manipuliert ein Buchungsprogramm in der Form, dass immer ein Teil der Abbuchungen auf sein eigenes Konto gutgeschrieben wird. Da der Mitarbeiter selbst für die Prüfung dieser Buchungsvorgänge verantwortlich ist und ein geeignetes Vier-Augen-Prinzip fehlt oder nur unzureichend umgesetzt ist, werden diese Kontobewegungen vorerst nicht entdeckt.

Fortsetzung

▶ Tab. 01

6. Betrug durch Lieferanten Der Lieferant/Provider macht sich die Gutgläubigkeit bzw. die Fahrlässigkeit von Mitarbeitern zunutze. Die Tathandlung konzentriert sich meist auf die zu liefernde Ware oder vereinbarte Dienstleistungen. Die Ware/Leistung wird dem gutgläubigen Mitarbeiter entweder nicht in der richtigen Menge oder in einer minderen Qualität zur Abnahme präsentiert. Darüber hinaus missbraucht der Lieferant die Infrastruktur des Instituts zum eigenen Vorteil. Die Tathandlung konzentriert sich bspw. auf nicht ausreichend umgesetzte Informations- und IT-Sicherheitskonzepte. Mögliche Formen des direkten Lieferantenbetrugs zu Lasten des Instituts können etwa sein: • Manipulation technischer Systemen • Erschleichung von Datensätzen • Missbrauch von Identitäten • Missbrauch der Telekommunikations-Infrastruktur	**Überhöhte Rechnungsstellung durch externe Dienstleister** Die Zusammenarbeit des Instituts mit einem externen IT-Dienstleister im Rahmen eines Outsourcing-Vertrags basiert auf definierten Service-Level-Agreements (SLA). Durch den IT-Dienstleister werden die vereinbarten Leistungen allerdings nur unzureichend erbracht, aber in voller Höhe in Rechnung gestellt. Darüber hinaus wird der Wert der Rechnungsbeträge erhöht. Der Dienstleister macht sich die mangelnde Nachvollziehbarkeit der Rechnungsaufstellung zunutze, um sich finanzielle Vorteile zu verschaffen. **Warenbetrug** Ein Lieferant liefert mit Absicht defektes oder gebrauchtes Verbrauchsmaterial an und gibt vor, dass es sich dabei um neue Ware handelt oder um Güter, die den gewünschten Qualitätsanforderungen entsprechen. Der Mitarbeiter nimmt die Ware ohne eingehende Kontrolle ab.
7. Betrug durch Lieferanten in Zusammenarbeit mit Mitarbeitern (kollusiv) Zwischen dem Lieferanten/Provider und dem Mitarbeiter findet eine aktive Zusammenarbeit statt – mit der Absicht, das Institut zu schädigen. Hier werden insbesondere fehlende Kontrollen bei Logistik- und Einkaufsprozessen wie auch bei der Rechnungslegung ausgenutzt. Im Fokus des Lieferantenbetrugs in Zusammenarbeit mit dem Mitarbeiter stehen fingierte bzw. überhöhte Rechnungen: Quantitativ oder qualitativ nicht erbrachte oder schlecht ausgeführte Dienstleistungen/Produkte werden durch den beteiligten Mitarbeiter dennoch abgenommen.	**Leistungserschleichung in Form von fingierten Rechnungen** Der Lieferant erstellt fingierte Rechnungen für nicht erbrachte Dienstleistungen/Produkte, die vom zuständigen Mitarbeiter bewusst ohne Prüfung akzeptiert werden. Als Gegenleistung erhält der Mitarbeiter materielle bzw. immaterielle Vermögensvorteile. **Korruption im IT-Einkauf eines Finanzdienstleisters** Ein leitender Mitarbeiter der Einkaufsabteilung einer Bank wird von einem langjährigen IT-Lieferanten zu einem mehrtägigen Formel-1-Wochenende mit vollständiger Kostenübernahme ins Ausland eingeladen. So gelingt es dem Lieferanten, die anstehenden Vertragsverhandlungen für die Hardwareausstattung der Bank in einer „entspannten Atmosphäre“ durchzuführen.

Organisationsübergreifende Präventionsmaßnahmen

▶ Tab. 02

Präventionsmaßnahme	Organisationsübergreifender Nutzen
Ethische Leitlinien und Standards als unternehmensweites Wertemanagement	Akzeptanz einer unternehmensweiten Kultur zur Verhinderung wirtschaftskrimineller Handlungen
Verfahren und Richtlinien, beispielsweise als „Gift and Entertainment“-Policy, „Anti-Fraud-Policy“ etc.	Einheitliches Rahmenwerk zur Kontrolle und Prävention von Wirtschaftskriminalität
Prüfungskonzept als Bestandteil des konzernweiten Kontrollsystems (Anti-Fraud-IKS)	Effiziente und risikoorientierte Kontrollen zur Aufdeckung von Betrugsdelikten und Ableitung weiterer präventiver Maßnahmen
Unabhängiges, anonymes Hinweisgebersystem („Whistle Blowing System“)	Effektive Früherkennung von Betrugshandlungen und aktive Verhinderung von Vermögensschaden durch Risikoidentifizierung in einem frühzeitigen Deliktstadium
Untersuchungsprozess für wirtschaftskriminelle Delikte	Strukturierte Vorgehensweise im Schadensfall (Beweissicherung) und Reduzierung von finanziellen Schäden und Reputationsrisiken
Fraudspezifische Mitarbeitertrainings	Sensibilisierung der Mitarbeiter und Schaffung eines bereichsübergreifenden Bewusstseins für die Risiken aus wirtschaftskriminellen Handlungen („Fraud-Awareness“)
Eindeutige Berichts- und Informationswege	Verbesserung der Transparenz über potenzielle Gefahren aus Betrugsdelikten durch „Fraud Reporting“
Konzept zur Prüfung der Mitarbeiter auf ihre Zuverlässigkeit gegenüber Betrug (Integritätstest)	Reduzierung potenzieller Täterprofile schon im Rahmen der Personalauswahl durch einen „Know Your Employee“-Ansatz
Kommunikationskonzept im Außenverhältnis gegenüber Aktionären, Providern etc.	Schaffung eines unternehmensübergreifenden Bewusstseins für Betrugsrisiken und präventive Stärkung der Reputation am Markt

fältig. So können explizite ethische Leitlinien und Standards dazu dienen, eine unternehmensweite Kultur zur Verhinderung wirtschaftskrimineller Handlungen zu etablieren. Verfahren und Richtlinien, etwa als „Gift and Entertainment"-Policy oder als Anti-Fraud-Policy, können ein einheitliches Rahmenwerk zur Kontrolle und Prävention schaffen. Effiziente und risikoorientierte Kontrollen im Rahmen des Anti-Fraud-IKS dienen der Aufdeckung von Betrugsdelikten und der Ableitung weiterer präventiver Maßnahmen. Ein definierter Untersuchungsprozess für wirtschaftskriminelle Delikte sorgt für eine strukturierte Vorgehensweise im Schadensfall und garantiert die Beweissicherung. Fraudspezifische Trainings können der Sensibilisierung der Mitarbeiter dienen und dazu beitragen, ein bereichsübergreifendes Risikobewusstsein zu schaffen. Die Liste der potenziell geeigneten Maßnahmen ist vielfältig – die im konkreten Fall indizierten Maßnahmen hängen entscheidend von der institutsspezifischen Gefährdungssituation ab. In jedem Fall gilt, dass für den Erfolg der Maßnahmen eine bereichsübergreifende Sicht auf das Thema essenziell ist. Zudem ist es einer erfolgreichen Implementierung überaus förderlich, wenn die Verantwortung für die Anti-Fraud-Thematik auf oberster Führungsebene im Institut wahrgenommen wird. □

Fazit

Der risikobasierte Ansatz zur Betrugsbekämpfung stellt für Finanzinstitute eine beträchtliche Chance dar. Durch die Ausrichtung der individuellen Präventivmaßnahmen an der konkreten Risikosituation – fundiert durch die Ergebnisse der Gefährdungsanalyse – können Institute wirtschaftskriminelle Handlungen zielgerichteter und wirkungsvoller verhindern. Die Verantwortlichen aus der Compliance-Abteilung, der internen Revision oder dem Risikomanagement haben nun die Möglichkeit, konzentrierter und ressourcensparender zu agieren. Zugleich haben sie einen ausreichenden Nachweis gegenüber Aufsichtsbehörden, Wirtschaftsprüfern und Kontrollgremien, dass eine institutsspezifisch angemessene Betrugsbekämpfung etabliert ist.

Indem sich ein Institut auf seine tatsächlich risikobehafteten Bereiche fokussiert, kann es beispielsweise auch nicht-risikorelevante Prüfungstätigkeiten identifizieren, die zukünftig überflüssig sind. Präventivmaßnahmen werden nicht mehr nach einem generell geltenden Leitfaden und mit dem „Gießkannenprinzip" angewandt. Der risikobasierte Ansatz hilft den Instituten, mit geringerem Aufwand mehr zu erreichen. Ein Anti-Fraud-Management, das sich auf einen ganzheitlichen, risikobasierten Ansatz stützt, erfüllt gleichermaßen die ökonomischen Unternehmensbedürfnisse und die aufsichtsrechtlichen Anforderungen einer größeren Eigenverantwortung. Ein institutsindividuelles, sinnvolles Präventionskonzept genügt nicht nur den verschärften Regularien – es trägt entscheidend dazu bei, die Risiken aus Betrugshandlungen zu minimieren und potenzielle Schäden für das Institut aktiv zu vermeiden.

Quellenverzeichnis:

***PwC [Hrsg.] (2006)**: Wirtschaftskriminalität 2005 – Internationale und deutsche Ergebnisse, Studie von PriceWaterhouseCoppers in Zusammenarbeit mit der Martin-Luther-Universität Halle-Wittenberg und TNS Emnid, Frankfurt (Main) 2006.*

***PwC [Hrsg.] (2008)**: Wirtschaftskriminalität 2007 – Sicherheitslage der deutschen Wirtschaft, Studie von PriceWaterhouseCoppers in Zusammenarbeit mit der Martin-Luther-Universität Halle-Wittenberg und TNS Emnid, Frankfurt (Main) 2008.*

***KPMG [Hrsg.] (2007)**: Profile of a Fraudster – Studie zu Täterprofilen, Frankfurt (Main) 2007.*

Autor:
Christian Moerler ist Geschäftsführer der Severn Consultancy GmbH, Frankfurt/Main