

Kurzverriss: Hülsberg u.a. Anti-Fraud-Management

Frank Hülsberg, Partner bei einer Wirtschaftsprüfungsgesellschaft, schreibt mit zwei Kollegen zum Thema Anti-Fraud-Management (AFM) – Reduzierung von Haftungsrisiken und Vermögensschädigungen (ZRFG 5/07, S. 204 – 208). Die Autoren gliedern nach der Einführung, in der sie sich mit der zunehmenden medialen Aufmerksamkeit für das Thema Wirtschaftskriminalität sowie den internationalen und nationalen Normen (ein Lieblingsthema von Wirtschaftsprüfern) beschäftigen, ihren Kerntext in folgende Teilelemente:

- Fraud Risk Assessment
- Prevention & Detection
- Monitoring & Reporting

Sie führen aus, dass *‘ein wirksam implementiertes und kontinuierlich durchgeführtes AFM (Anti Fraud Management, Anmerkung des Verfassers) der Vermeidung, Aufdeckung und Verfolgen von Verstößen gegen Unternehmensrichtlinien und bewussten Gesetzesverstößen von Organen, Mitarbeitern oder Unternehmensfremden, die eine Schädigung der Vermögensinteressen eines Unternehmens zur Folge haben’, dienen soll.*¹

Ein Anti-Fraud-Management System hat nach Auffassung der Autoren folgende Komponenten:

- Risiko- und Kontrollkultur (Control Environment)
- Risikoerfassung und -beurteilung (Fraud Risk Assessment)
- Präventions- und Aufklärungsmaßnahmen (Prevention und Detection)
- Berichtswesen (Reporting)
- Monitoring

Der Text ignoriert die von den Autoren genannte erste Komponente der Risiko- und Kontrollkultur, auch soft controls genannt, völlig und setzt unvermittelt mit dem Fraud Risk Assessment ein. Ein Fraud Risk Assessment führt man nach Ansicht der Autoren als von externen Beratern moderiertes Self Assessment durch (Schritt eins), dem eine Validierung in Workshops nachfolgen kann (Schritt zwei).

Die Autoren nutzen in ihrem Text den Begriff der potentiellen Realisierbarkeit für das Eintreten doloser Handlungen, ein Begriff, der weder hergeleitet noch hinsichtlich der Notwendigkeit seiner Einführung begründet wird.²

Alternative Konzepte für ein Assessment werden nicht angesprochen, obwohl sie zweifelsohne existierten (beispielsweise spezielle Audits zur Identifizierung von Einfallstoren für Fraud). Auch eine Einbindung interner Stellen (Unternehmenssicherheit, Recht, Interne Revision, u.a.) wird nicht angedacht, es wirkt so, als agierten die Berater alleine.

Im Bereich der Fraud Prevention und Detection (zweite Komponente) würden dann auf der Basis des Assessments korrespondierende Maßnahmen implementiert, um die wesentlichen Fraud-Risiken zu steuern. Ziel sei die proaktive Vermeidung und Aufklärung an Stelle eines zufälligen Bekannt werdens von Fraud. Die Autoren nennen hier ethische Richtlinien (die sie offensichtlich nicht in den Bereich der Kontrollumgebung einordnen, was falsch ist), die Einführung von Fraud-Richtlinien (wir wissen allerdings nicht, was das ist und erfahren es aus dem Text auch nicht) sowie Geschenkerichtlinien.

Dazu kommen ein wenig [Corporate Intelligence](#) (Open Source Analysen) sowie Vertragsklauseln mit Lieferanten. Im Bereich der Fraud Detection kommen die typischen Produkte der Wirtschaftsprüfer zu Ehren: IT-gestützte Tools (hier auch wieder der immer gern strapazierte Benford), aber von Continuous Auditing oder Lernenden Systemen wissen die Autoren wohl nichts – oder sie schreiben es nicht. Dafür aber konzentrieren sie sich auf digitale Signaturen und Zeitstempel, klassische Felder der IT-gestützten Prüfung der so genannten Großen Vier. Das wirksamste und wichtigste Instrument

¹ Hülsberg u.a., S. 206

² Hülsberg u.a. S. 207

zur Aufdeckung von Fraud wird gar nicht erwähnt (das machen wir dann aber unten in unseren Anmerkungen).

Im Bereich des Monitoring und Reportings (schon die Reihenfolge in der Überschrift scheint uns falsch herum zu sein) sprechen die Autoren von Erst- und Folgeaufnahmen sowie von einer Inventarisierung von Fraud-Risiken. Die Autoren empfehlen eine Vergabe der Verantwortung des AFM an den Chief Compliance Officer und haben damit wohl wieder mal nur die Großunternehmen im Blick.

Wen wundert es dann, dass anschließend (allerdings richtiger Weise!) auf eine systematische Aufarbeitung von Fraud-Fällen verwiesen wird, dies aber bitte nicht durch die Interne Revision, sondern externe Forensiker, *da diese über die gesetzlichen Bestimmungen der gerichtssicheren Datenerhebung in der Regel besser ausgebildet sind und über entsprechende Systeme und Programme verfügen.*³ So was kann man sich ja als Interner Revisor weder aneignen noch kaufen...

Anmerkungen:

Die eingangs gewählte Fokussierung auf Unternehmen ist unseres Erachtens falsch, so gilt für gemeinnützige Organisationen oder Körperschaften des öffentlichen Rechts ([BAFIN-Skandal als ein Beispiel](#)), dass diese Organisationen nicht ausgeklammert werden dürfen, weil dort Fraud-Risiken die gleichen finanziellen und schädigenden Auswirkungen haben und der Reputationsschaden ungleich höher und langwirkend ist und damit noch dringender vermieden werden muss: Wenn eine Aufsichtsbehörde keine internen Kontrollen über Aufwendungen für IT in Millionenhöhe hat, dann ist das jenseits der Peinlichkeit, es ist eben ein Skandal.

Ebenfalls nicht richtig ist die implizite Fokussierung auf Großunternehmen, denn im Mittelstand sind Instrumente wie Compliance Officers oder manchmal sogar eine Interne Revision nicht durchgängig vorhanden. Damit stellt sich die Frage, wo das Thema dort denn zu verankern wäre. Diese wichtige Frage lassen die Autoren offen.

Wir möchten aber darauf hinweisen, dass die Frage von wesentlicher Bedeutung ist, denn eine falsche organisatorische Zuordnung, wie sie beispielsweise bei der Internen Revision im Mittelstand nicht unbedingt selten sein dürfte, führt zu einer fehlenden oder zumindest eingeschränkten Wirksamkeit des gesamten Systems.

Wenn Ihnen die oben dargelegte Struktur des AFM verdächtig bekannt vorkommt, haben Sie Recht: Das ist die Struktur des COSO-Modells, eines grundlegenden Modells zur Etablierung von Internen Kontrollsystemen (COSO I) oder von Risikomanagement-Systemen (COSO II). Man hat hier offensichtlich nicht mehr getan, als die Begrifflichkeiten auszutauschen und das Modell entsprechend anders zu verpacken. Dementsprechend ist der Text auch in seinem materiellen Gehalt schwachbrüstig, wie dieser KurzVerriss auch zeigt.

In der uns bekannten Praxis ist es so, dass Ethische Kodizes der Kontrollumgebung zugeordnet werden – wir empfehlen den Fachleuten, die diesen Text verfasst haben, einen gelegentlichen Blick in das COSO-Modell. Dort heißt es etwa zum Bereich Internal Environment, dass hier beispielsweise zu subsumieren seien:

- Aufsicht durch das Kontrollorgan
- Integrität, ethische Werte und die Kompetenz der Mitarbeiter
- Die Art und Weise, wie Kompetenz und Verantwortung delegiert wird⁴

Auch werden die von den Autoren künstlich getrennten Elemente (Geschenke, Fraud, Werte) in der Regel in einer Richtlinie zusammengefasst, was ohne Zweifel auch sinnvoll ist. Dies gilt selbst dann, wenn nicht jeder Mitarbeiter von jedem dort geregelten Punkt betroffen sein wird, etwa weil er keine Spenden an andere Organisationen anweisen wird, weil dies der Geschäftsführung vorbehalten ist.

³ Hülsberg u.a., S. 208

⁴ The Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework. Executive Summary Framework, 2004, S. 27

Das wirksamste Instrument der Aufdeckung von Fraud – noch vor spezifischen Assessments, (leider) vor der Internen Revision oder dem Abschlussprüfer oder CAATs – ist ein funktionierendes Hinweisgebersystem. Dies erwähnen die Autoren nicht, vielleicht deswegen, weil es nicht im Produktportfolio der Wirtschaftsprüfer enthalten ist und man damit also nichts verdienen kann. Auch der Ombudsmann, bei einigen der deutschen Topadressen der Wirtschaft bereits lange etabliert, findet keine Würdigung.

Diese Verkaufbarkeit ist bei Risk Assessments, Workshops und anderen Leistungen allerdings gegeben. Das kann aber nur ein Zufall sein. Wir sind der Meinung, dass Anti-Fraud-Management originäre Aufgabe der Organisationen und ihrer Führungsebene selbst ist. Wohl brauchen viele dieser Organisationen wirklich Be-Ratung in der Aufbauphase, aber niemand sollte den Fehler machen und von externen Beratern abhängig werden.

Know-how muss intern aufgebaut werden, und dies betrifft v.a. die Interne Revision, denen die Autoren hier nur eine Rolle einräumen, die auf uns die eines staunenden und unwissenden Beobachters macht. Wenn man weiß, wie viel verbrannte Erde durch externe Berater in diesem Bereich in der Praxis bereits hinterlassen worden ist, wird die Auffassung der Autoren auch nicht teilen wollen.

Zusammenfassend sind wir der Meinung, dass dieser Text eher eine Verkaufshilfe denn ein zweckmäßiger fachlicher Abriss für die genannten Services ist:

- Risk Assessments und Workshops
- CAATs
- Forensische Dienstleistungen, v.a. Sonderuntersuchungen

Er vergibt die Chance, die Grundzüge eines wirksamen Anti-Fraud-Managements zu skizzieren, weil er leider nur fahrlässig geschrieben und offensichtlich ebenso fahrlässig redaktionell geprüft worden ist. Sonst wären solche schweren Mängel wie das Fehlen von Hinweisgebersystemen nicht unentdeckt geblieben. Die ZRFG läuft damit Gefahr, ähnliche Gutenachtgeschichten zu bringen wie andere Publikationen aus dem gleichen Haus.

Selbstverständlich teilen wir nicht die Auffassung der Autoren, dass forensische Untersuchungen nicht durch eine etablierte Interne Revision durchgeführt werden sollten; da gibt es nur ganz wenige Ausnahmen, bei denen es zwingend notwendig ist, etwa wenn es um Management Fraud auf der höchsten Managementebene geht. Hier geriete die Interne Revision in einen nicht lösbaren Konflikt hinsichtlich ihrer Objektivität, weil sie ihren fachlichen und in der Regel auch disziplinarischen Vorgesetzten in einem sehr sensiblen Bereich prüfen muss. Die fachliche Kompetenz muss allerdings bei einer etablierten Internen Revision vorhanden sein, beziehungsweise projektbegleitend ausgebildet werden.

Eine weitere wichtige Konsequenz aus einem Fraud Risk Assessment bleibt übrigens auch unerwähnt: Die identifizierten Einfallstore für dolose Handlungen müssen in die Prüfungsplanung der Internen Revision als besonders zu berücksichtigende Bereiche eingebracht werden. Der Prüfungsdruck in diesen Prüffeldern ist zu erhöhen, um hier neben der Etablierung von Kontrollen wirksame Prävention und Aufdeckung leisten zu können.

Elmar Schwager, [The AuditFactory](http://www.auditfactory.de)

Kontakt:

The AuditFactory
Geschäftsleitung
Elmar Schwager

' 07142 7748 331 (Backoffice)
* Info@AuditFactory.de
www.auditfactory.de