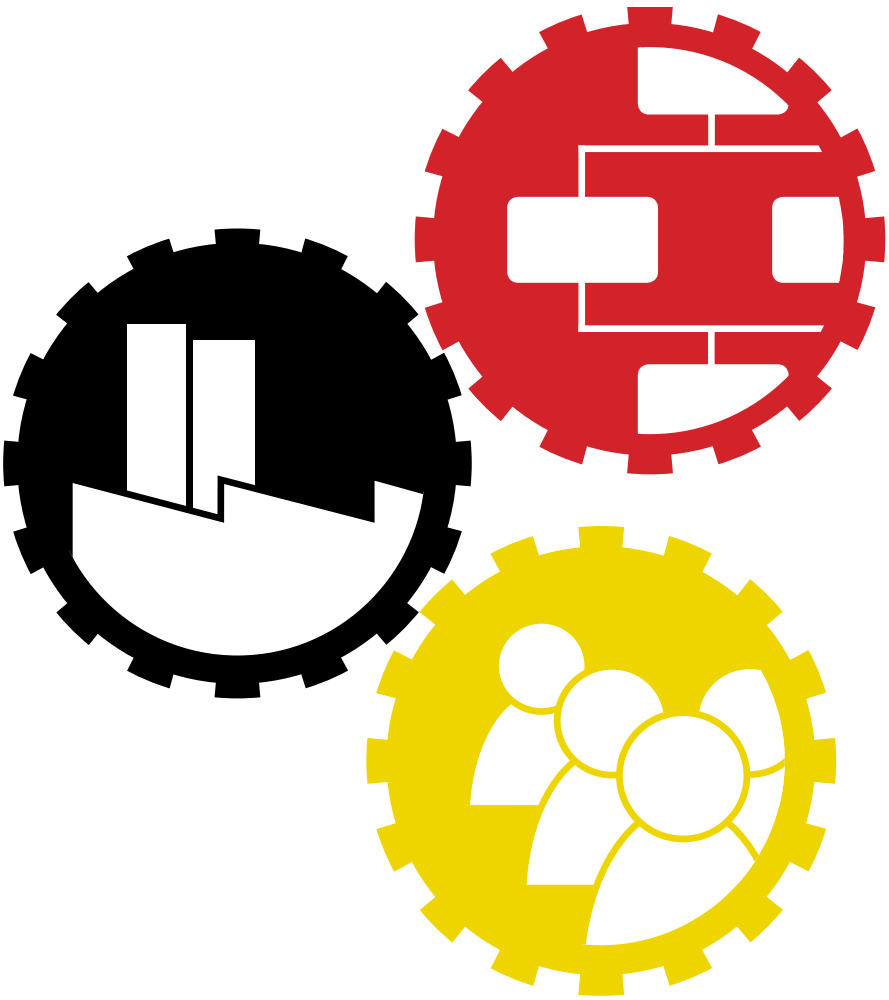
Bundesamt für Verfassungsschutz

Bundesamt für Sicherheit in der Informationstechnik

ASW Bundesverband

Wirtschaftsgrundschutz

Baustein ÜA5 Umgang mit Wirtschaftskriminalität



1 Relevanzentscheidung für diesen Baustein

1. Ist die **Institution aufgefordert oder** sogar – **aufgrund nationaler und internationaler rechtlicher Bestimmungen – verpflichtet**, ein Risikomanagementsystem zu betreiben?
2. Hat die Institution **nationalen und internationalen Zahlungsverkehr**?
3. Hat die Institution **werthaltige Güter für den Eigenbedarf** oder **produziert** sie **Güter, deren Verlust** (im Sinne von Diebstahl) **für Dritte von Interesse** ist?
4. Kann der **Schaden** aus einer (wirtschafts-)kriminellen Handlung gegen die Institution **existenzbedrohende Ausmaße** annehmen?
5. Hat die Institution ihre **Risiko- und Gefährdungslage** aufgrund von (wirtschafts-)kriminellen Handlungen zu ihren Lasten **strukturiert analysiert und** entsprechende zielgerichtete **Präventionsmaßnahmen** zu deren Vermeidung **implementiert**?
6. Hat die Institution bei ihren **Mitarbeitern** ein **angemessenes Bewusstsein für** die vielfältigen **Gefahren aus wirtschaftskriminellen Handlungen** zulasten der Institution geschaffen und hält dieses auf einem hohen Niveau aufrecht?
7. Hat die Institution ausreichende **Vorkehrungen für** das **Eintreten eines Schadensereignisses/Vorfalls** getroffen?
8. Ist sich die **Leitung** der Institution **etwaiger persönlicher Haftungsrisiken aufgrund** eines **Organisationsverschuldens** bewusst (z. B. durch ein nicht angemessenes Manage-

ment von operationellen Risiken aus (wirtschafts-)kriminellen Handlungen gegen die Institution)?

Die Polizeiliche Kriminalstatistik der letzten Jahre für Deutschland, das Bundeslagebild Wirtschaftskriminalität des Bundeskriminalamts sowie alle Analysen und Erhebungen bekannter Wirtschaftsprüfungsgesellschaften und Vertrauensschadenversicherer national wie auch international zeigen deutlich:

Wirtschaftskriminalität ist ein ernsthaftes und größer werdendes Problem mit einer **hohen Dunkelziffer**, das **branchenunabhängig** alle Institutionen betrifft und angeht.

Allein die bekannt gewordenen Schäden gehen für die Unternehmen in eine mehrstellige Milliardenhöhe, ganz abgesehen von der immensen Dunkelziffer, von der auch die Ermittlungsbehörden ausgehen und auf die in allen anderen Statistiken und Lagebilddarstellungen ausdrücklich hingewiesen wird.[1] Dabei ist besonders auffällig, dass **ein einzelner Fall** oftmals einen **erheblichen materiellen und immateriellen Schaden verursacht und** nicht selten die **wirtschaftliche Substanz** eines Unternehmens **gefährden** kann.

Keineswegs handelt es sich zudem um ein jeweils nationales Problem, sondern der **Täter oder** ganze **Tätergruppen operieren** - nicht zuletzt auch begünstigt durch die technische Entwicklung der letzten Jahre - **länder- und kontinentübergreifend** sowie mit einer Geschwindigkeit, die es teilweise erheblich erschwert, sich hiervor als einzelnes Land oder Unternehmen angemessen zu schützen.

Zum **Täterkreis** von (wirtschafts-)kriminellen Handlungen gehören sowohl **Mitarbeiter eines Unternehmens als auch Externe** bzw. teilweise auch beide gemeinsam in kollusivem Handeln. Motiviert werden die Täter durch vielschichtige persönliche Gründe wie beispielsweise angespannte finanzielle Verhältnisse, Gier oder Illoyalität. Auch Unzufriedenheit, u. a. aus Enttäuschung aufgrund nicht ausreichend geförderter Karriereentwicklung , kann ein Motiv sein.

[1] Die Dunkelziffer in den polizeilichen Statistiken ist zweigeteilt. Einerseits beinhaltet diese noch nicht aufgedeckte Fälle, anderseits aber auch all die Fraud-Fälle, die von Unternehmen oder Privatpersonen zwar aufgedeckt, nicht aber gegenüber den Ermittlungsbehörden angezeigt wurden und demzufolge ebenfalls nicht statistisch erfasst werden können. Die aktuellen Entwicklungen werden jeweils im jährlichen „Bundeslagebild Wirtschaftskriminalität“ des Bundeskriminalamts abgebildet.

Wirtschaftskriminelle Handlungen sind außerordentlich vielfältig, beispielhaft sind dabei Kapitalanlage-/Kreditbetrug, Korruption/Bestechlichkeit, Begünstigung, Betrug, Untreue, Diebstahl, Unterschlagung, Datenmissbrauch oder Geldwäsche zu nennen. Häufig treten mehrere dieser Tatbestände in Kombinationen auf. Sie verursachen allein in Deutschland jedes Jahr Schäden in Höhe von mehreren Milliarden Euro, wobei das tatsächliche Schadensvolumen aufgrund der hohen Dunkelziffer noch beträchtlich größer ist. Neben dem materiellen Ausmaß kommen für die geschädigten Unternehmen aufgrund der oftmals **unvermeidlichen Publizität** dieser Vorkommnisse ein massiver Vertrauensverlust und eine **deutliche Beeinträchtigung** ihrer **Reputation** hinzu.

Zielstellung des Bausteins

Dieser Baustein liefert Verantwortlichen einer Institution eine Hilfestellung für eine strukturierte Vorgehensweise zur Implementierung eines insbesondere auf die Vermeidung von (wirtschafts-)kriminellen Handlungen („vor die Tat bzw. den Schaden kommen“) ausgerichteten Managementsystems und zeigt die wesentlichen Aktivitäten eines entsprechenden ganzheitlichen Managementsystems.

Anwendungsbereich

Dabei ist die Vielzahl der Einzelmaßnahmen im Rahmen des Managements von Wirtschaftskriminalität so umfangreich und komplex, dass sich dieser Baustein auf die wesentlichen Kernprozesse gemäß Kapitel 3 fokussiert. Die unter diesen Kernprozessen liegenden zahlreichen Einzelmaßnahmen werden demzufolge nachfolgend zwar genannt, die dazugehörigen detaillierten Prozess-/Ablaufbeschreibungen sind jedoch den ergänzenden Literaturwerken zu entnehmen.

2 Beschreibung

Die Bekämpfung sowie die Vermeidung von Schäden aus wirtschaftskriminellen Handlungen als ein Teil des operationellen Risikos ist ein wichtiger Bestandteil des **Risikomanagements** innerhalb eines Unternehmens.

Dabei beginnt die **Bekämpfung von wirtschaftskriminellen Handlungen** nicht erst „nach der Tat", d. h. wenn der hieraus resultierende Schaden bereits realisiert und bestenfalls durch geeignete Maßnahmen minimiert werden kann, sondern sinnvollerweise **„vor der Tat"**, also bevor ein Schaden entsteht. Dies bedeutet, dass der **Prävention** ein besonderes Augenmerk zu schenken ist. Dabei ist entscheidend, dass bei allen Mitarbeitern ein entsprechend ausgeprägtes Bewusstsein für die **Risiken und Gefährdungen** vorhanden ist, die **durch** potentielle **interne und externe Täter** entstehen. Hierdurch werden die entsprechenden Risiken reduziert und der Institution gelingt es, „vor die Tat" zu kommen.

Demzufolge stellt das Management von Wirtschaftskriminalität innerhalb einer Institution eine **Querschnittsaufgabe** dar, in die neben den Organmitgliedern nahezu **alle Bereiche** und Organisationseinheiten sowie jeder einzelne Mitarbeiter in allen Teilen **der Institution** eingebunden sind und die ihren Beitrag **zur Verhinderung von materiellen Schäden, Reputationsschäden** oder sonstigen Schäden für das Unternehmen zu leisten haben.

Unter dem Management von Wirtschaftskriminalität werden somit alle (Einzel-)Maßnahmen zusammengefasst, die geeignet sind, gegen wirtschaftskriminelle Handlungen zu Lasten der Institution

- **präventiv** zu wirken
- diese zu vermeiden bzw. **proaktiv** aufzudecken
- diese nach Eintreten eines Vorfalls **effizient** sowie **effektiv** zu managen

Ungeachtet einer umfassenden und allgemeingültigen bzw. anerkannten Definition sind die Formen und Begehungsmöglichkeiten und somit die **Gefährdungslage** von (wirtschafts-)kriminellen Handlungen sehr **vielschichtig und vielfältig**. Nachstehend wird daher eine Aufteilung nach Tätergruppen aus der Sicht einer Institution dargestellt.

Kategorisierung von (wirtschafts-)kriminellen Handlungen

Institutionen sind grundsätzlich aus zwei unterschiedlichen Richtungen und daraus resultierend in drei verschiedenen Arten von (wirtschafts-)kriminellen Handlungen betroffen:

1. **von innen** durch eigene Mitarbeiter
2. **von außen** durch Kunden, Lieferanten, Geschäftspartner oder externe Dritten
3. durch ein **Zusammenspiel** (kollusives Handeln) **von internen und externen** Tätern

Daneben lassen sich die (wirtschafts-)kriminellen Handlungen in die jeweiligen „Prozessschritte“ eines Täters unterteilen und diesen zuordnen. Hierzu zählen insbesondere:

1. **vorbereitende** Tatbestände
2. **Vermögensschädigungstat**
3. **Verschleierungstat**
4. **begleitende oder übergreifende** Tatbestände

In Deutschland existiert zur Beschreibung der Wirtschaftskriminalität unverändert keine Legaldefinition. Die Polizei bedient sich daher bei der Zuordnung von Straftaten zur Wirtschaftskriminalität des Katalogs von § 74c Abs. 1 Nr. 1 bis 6b Gerichtsverfassungsgesetz(GVG).[2]

[2] Ausführungen in den Vorbemerkungen der „pressefreien Kurzfassung“ des „Bundeslagebilds Wirtschaftskriminalität“ des Bundeskriminalamts der letzten Jahre.

Definition des DIIR

Das Institut für Interne Revision e. V. (DIIR) hat in seinen Standards folgende Definition des Begriffs formuliert: „Illegale Handlungen, die sich in vorsätzlicher Täuschung, Verschleierung oder Vertrauensmissbrauch ausdrücken. Diese Handlungen sind nicht abhängig von Gewaltandrohung oder Anwendung körperlicher Gewalt. Dolose Handlungen werden von Beteiligten und Organisationen begangen, um in den Besitz von Geldern, Vermögensgegenständen oder Dienstleistungen zu gelangen, um Zahlungen oder den Verlust von Leistungen zu vermeiden oder um sich einen persönlichen oder geschäftlichen Vorteil zu verschaffen."

Schlüsselfaktoren

Betrachtet man die drei ausschlaggebenden Faktoren für die Eintrittswahrscheinlichkeit wirtschaftskrimineller Handlungen genauer, wird sehr schnell deutlich, dass sowohl der Aspekt „Motivation/Anreiz" als auch der Aspekt „Rechtfertigung" unmittelbar vom „Schlüsselfaktor Mensch" abhängen, während lediglich der dritte Aspekt „Gelegenheit" auch von der Gestaltung von Arbeits- und Kontrollprozessen beeinflusst wird.

Ausgehend hiervon ist demzufolge die **Förderung bzw.** der **Erhalt** einer **möglichst hohen Eigenmotivation bei** allen **Mitarbeitern** ein **wesentlicher Faktor** sowohl für die langfristige Sicherung des Erfolgs einer Institution als auch für ein hohes Maß an Integrität.

Somit ist der **„Schlüsselfaktor Mensch"** die wichtigste Komponente sowohl für die Prävention und die Bekämpfung und Verhinderung von Wirtschaftskriminalität als auch für die Ursachen von gegen eine Institution gerichteten wirtschaftskriminellen Handlungen. Folgerichtig ist dies der Faktor, dem im Rahmen des Managements von Wirtschaftskriminalität die höchste Aufmerksamkeit zu widmen ist.

Um die Zielsetzung dieses Bausteins zu erreichen, ist die Voraussetzung, dass in einer Institution ein **strukturiertes Management von Wirtschaftskriminalität** zur Verhinderung, Aufdeckung und Bearbeitung von auftretenden wirtschaftskriminellen Handlungen gemäß den nachfolgenden Inhalten dieses Bausteins etabliert ist bzw. wird.

Die Basis für einen angemessenen Schutz vor wirtschaftskriminellen Handlungen ist ein System zum Management von Wirtschaftskriminalität, das die zu implementierenden Verfahrensweisen und **Methoden zur Planung, Umsetzung sowie** permanenten **Anpassung und Verbesserung** der einzelnen Komponenten eines Systems zum Management von Wirtschaftskriminalität abbildet.

internes Kontrollsystem

Ungeachtet der elementaren Bedeutung des „Schlüsselfaktors Mensch“ sowie aller Bestrebungen zur Stärkung der Eigenmotivation und des Bewusstseins für Mitarbeiter – auch für die Risiken wirtschaftskriminellen Handelns durch Kollegen und/oder externe Dritte – ist auch ein **effektives internes Kontrollsystem** (IKS) eine **elementare Grundlage** für ein effizientes Management von Wirtschaftskriminalität. Dies ist nicht zuletzt deswegen notwendig, um bei allem Grundvertrauen und ggf. langjährigen positiven Erfahrungen durch entsprechende Kontrollen regelmäßig sowie **immer wieder erneut** zu **überprüfen** (und damit auch den Risiken von für Täter berechenbaren Routinen entgegenzuwirken), inwieweit das entgegengebrachte Vertrauen gegenüber eigenen Mitarbeitern und/oder Dritten (unverändert) gerechtfertigt ist. Allerdings reicht ein funktionierendes und von allen Mitarbeitern/Verantwortlichen auch „gelebtes“ internes Kontrollsystem allein nicht aus, um wirtschaftskriminelles Handeln zu verhindern bzw. sehr frühzeitig aufzudecken.

Das **interne Kontrollsystem** ist in Bezug auf die Thematik **„proaktive Aufdeckung/Erkennung von Wirtschaftskriminalität“** so anzupassen und auszurichten, dass vorhandene Unregelmäßigkeiten möglichst zeitnah und unmittelbar aufgedeckt werden können („zeitnah nach der Tat“).

Prävention und deren Grundanforderungen

Die **Prävention** vor Wirtschaftskriminalität ist dagegen darauf ausgerichtet, unmittelbar **auf** den **„Schlüsselfaktor Mensch“** und somit „vor der Tat“ zu **wirken**, das heißt die Motivation und die Anreize für deliktisches Handeln möglichst erst gar nicht entstehen zu lassen sowie Tätern auch keine entsprechende Rechtfertigung zu geben. Neben der Prävention liegt ein Schwerpunkt im Umgang mit eintretenden („nach der Tat“) Vorfällen (Deliktfällen).

Hieraus resultiert, dass ein wirksames Management von Wirtschaftskriminalität die **drei Grundanforderungen** „**Prävention** von Wirtschaftskriminalität“, „**Aufdeckung** von Wirtschaftskriminalität“ und „**Bearbeitung** von Wirtschaftskriminalitäts(vor-)fällen“ sowie deren permanente Optimierung in einem ganzheitlichen, integrierten Ansatz einschließlich einer permanenten Evaluierung und kontinuierlichen Verbesserung miteinander verknüpft.

Ein **ganzheitliches und integriertes Management** von Wirtschaftskriminalität ist dabei sowohl ein **elementarer Bestandteil des Risikomanagements** als auch in die sonstigen internen Kontrollverfahren ausreichend eingebettet. Ein entsprechendes Regelwerk allein schafft allerdings noch kein (nachhaltiges) Werte- und/oder Kontrollbewusstsein. Wesentliche übergreifende Erfolgsfaktoren sind gelebte und praktizierte „Corporate Governance“[3] sowie „Compliance“ (regelkonformes Verhalten) bzw. „Unternehmensethik“. Dies bedeutet, dass das Management von Wirtschaftskriminalität in sehr starkem Maße eine **verhaltensbezogene** und damit den „Schlüsselfaktor Mensch“ in den Mittelpunkt stellende **Komponente** beinhaltet.

Voraussetzung

Ausgehend hiervon sind die wesentlichen Voraussetzungen bzw. die Basis für erfolgreiches und nachhaltiges Management von Wirtschaftskriminalität neben der Vorbildfunktion der Leitung der Institution ein **Unternehmensleitbild** sowie ein (Wohl-)**Verhaltenskodex**, die ein **uneingeschränktes Bekenntnis zu ethisch-moralisch einwandfreiem Verhalten und Geschäftsgebaren** der Institution sowie zu „Corporate Social Responsibility“[4] beinhalten.

[3] „Corporate Governance“ umfasst die Gesamtheit aller internationalen und nationalen Werte und Grundsätze für eine gute und verantwortungsvolle Unternehmensführung; konkrete Regelungen und Vorschriften sind im „Deutschen Corporate Governance Kodex“ in der aktuellen Fassung vom 05.05.2015 dargestellt.

[4] „Corporate Social Responsibility” umschreibt den freiwilligen Beitrag der Unternehmen zu einer nachhaltigen Entwicklung, der über die gesetzlichen Forderungen („Compliance“) hinausgeht. Es steht für verantwortliches unternehmerisches Handeln in der eigentlichen Geschäftstätigkeit (Markt), über ökologisch relevante Aspekte (Umwelt) bis hin zu den Beziehungen mit Mitarbeitern (Arbeitsplatz) und dem Austausch mit den relevanten Anspruchsgruppen wie zum Beispiel den Anteilseignern, vgl. Kommission der europäischen Gemeinschaften, 2001, Grünbuch Europäische Rahmenbedingungen für die soziale Verantwortung der Unternehmen.

3 Gefährdungslage

Das Management dieser **komplexen Gefährdungslage** liegt in der Verantwortung einer jeden Institution selbst und hier insbesondere bei deren Leitung.

Folgende Gefährdungen aus (wirtschafts-)kriminellen Handlungen treten häufig im Zusammenhang mit Institutionen auf und sind daher von besonderer Bedeutung:

G 1	Verletzung des persönlichen Lebens- und Geheimbereichs (§§ 201 bis 204 StGB)
G 2	Diebstahl (§§ 242 und 243 StGB)
G 3	Unterschlagung (§ 246 StGB)
G 4	Geldwäsche (§ 261 StGB)
G 5	Betrug (§ 263 StGB)
G 6	Computerbetrug (§ 263a StGB)
G 7	Subventionsbetrug (§ 264 StGB)
G 8	Kapitalanlagebetrug (§ 264a StGB)
G 9	Versicherungsbetrug (§ 265 StGB)
G 10	Erschleichen von Leistungen (§ 265a StGB)
G 11	Kreditbetrug (§ 265b StGB)
G 12	Untreue (§ 266 StGB)
G 13	Urkundenfälschung (§§ 267 bis 281 StGB)
G 14	Insolvenzstraftaten (§§ 283 bis 283d StGB)
G 15	Wettbewerbsbeschränkende Absprachen bei Ausschreibungen (§ 298 StGB)

G 16	Bestechlichkeit im geschäftlichen Verkehr (§§ 299 und 300 StGB)
G 17	Bestechlichkeit im Gesundheitswesen (§§ 299a und 300 StGB)
G 18	Bestechung im Gesundheitswesen (§§ 299a und 300 StGB)
G 19	Datenveränderung (§ 303a StGB)
G 20	Computersabotage (§ 303b StGB)
G 21	Vorteilsannahme (§ 331 StGB)
G 22	Bestechlichkeit (§§ 332 und 335 StGB)
G 23	Vorteilsgewährung (§ 333 StGB)
G 24	Bestechung (§§ 334 und 335 StGB)
G 25	Unbefugte Ausgabe und Verwendung von Geldzeichen (§§ 35 und 36 BBankG)

4 Maßnahmen

Die vorgenannten **Rahmenbedingungen** und Faktoren sind durch entsprechende **aufbau- und ablauforganisatorische Regelungen** zu flankieren sowie durch entsprechende **Kontrollmaßnahmen** zu überwachen, die auch **mitarbeiterbezogene Sicherungsmaßnahmen** umfassen. Dabei hängt der Erfolg aller Maßnahmen innerhalb eines Unternehmens insbesondere davon ab, dass auch die vorhandene Unternehmenskultur/-philosophie sowie alle weiteren unternehmensspezifischen Faktoren entsprechende Berücksichtigung finden.

Das nachstehende Schaubild veranschaulicht diesen ganzheitlichen prozessualen Ansatz eines Systems zum Management von Wirtschaftskriminalität, das sich an dem so genannten **„Plan-Do-Check-Act-Modell“** (Qualitätsmanagementmodell) orientiert und wodurch die zuvor zu definierenden grundsätzlichen Zielsetzungen und Anforderungen für eine (institutionsweite) Integration aller Aktivitäten zum Management von Wirtschaftskriminalität innerhalb der Institution geplant, umgesetzt und somit erfüllt werden können. Die Maßnahmen unterteilen sich in diese drei wesentlichen Prozessblöcke:

1. **Führungsprozess**
2. **Betriebsprozess** (Planung, Umsetzung, Überprüfung, Verbesserung)
3. **Berichts-/Kontrollwesen**

Abbildung 1 stellt dies grafisch dar.

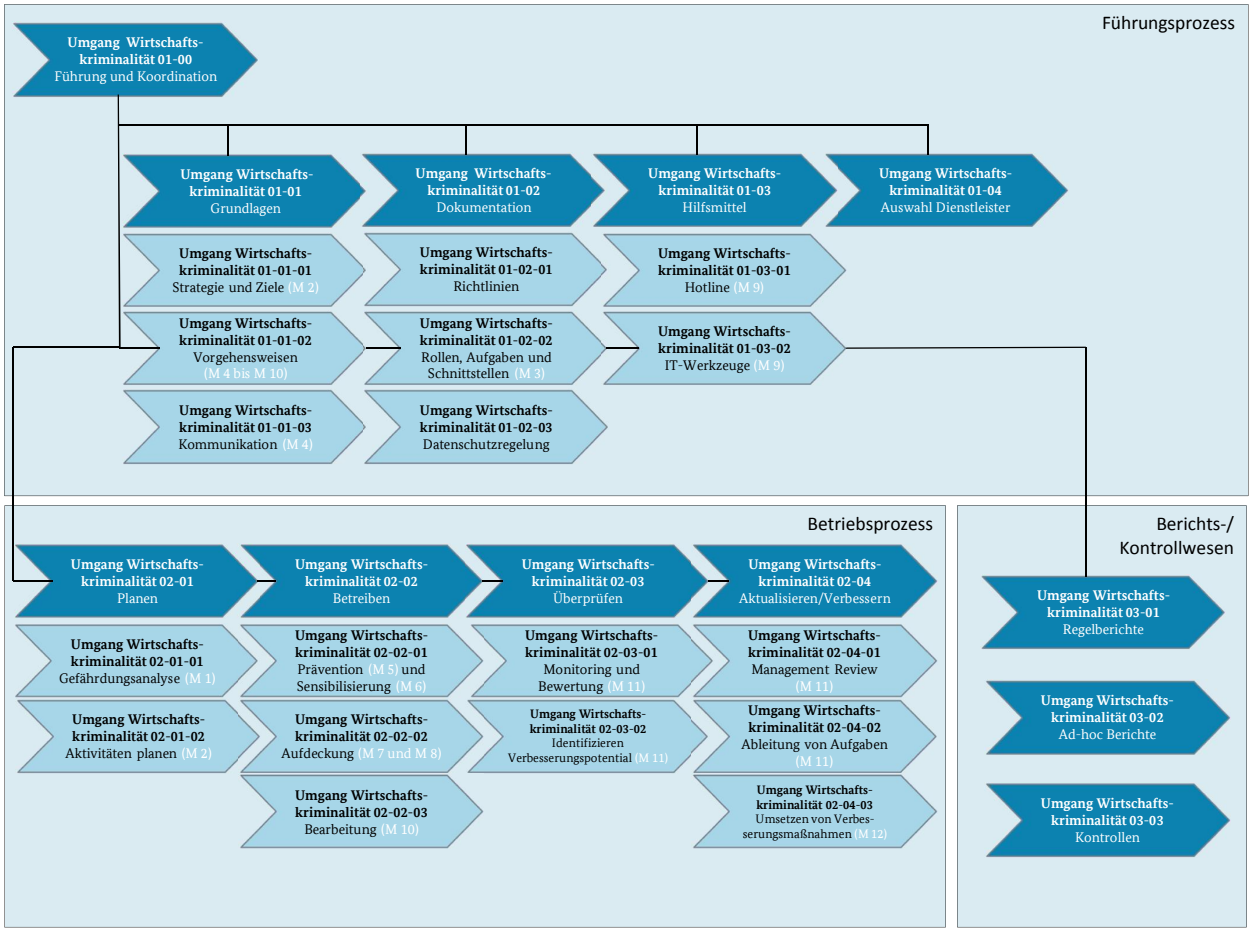


Abbildung 1: Prozessschaubild Management von Wirtschaftskriminalität

Die Führungsprozesse sowie teilweise auch das Berichts- und Kontrollwesen entsprechen dabei weitgehend den bereits im Standard 2000-1 beschriebenen Grundansätzen. Dabei ist ein **konsequentes Berichts- und Kontrollwesen** sowohl für alle Führungsprozesse als auch für alle nachstehend näher dargestellten Betriebsprozesse von großer Bedeutung.

Die spezifischen, konkret auf das Management von Wirtschaftskriminalität ausgerichteten und nachstehend dargestellten Maßnahmen M 1 bis M 12 dieses Bausteins, die in der vorstehenden Abbildung auch entsprechend bezeichnet sind, sind in drei Kategorien eingeteilt. Sie richten sich nach dem erforderlichen Detailgrad bzw. der gewünschten Ausprägung (siehe Relevanzentscheidung) auf Basis der Anwendungsentscheidung gemäß Wirtschaftsgrundschutzstandard 2000-1:

A-Kategorie – Basismaßnahmen: unabdingbarer Wirtschaftsgrundschutz

B-Kategorie – Standardmaßnahmen: vollständiger Wirtschaftsgrundschutz
C-Kategorie – erweiterte Maßnahmen: erweiterter Schutz bei hohem Risikopotential

M 1 Identifikation der Gefährdungs- bzw. Ausgangslage für das Management von Wirtschaftskriminalität (A)

Die Institution führt eine **institutionsspezifische Gefährdungsanalyse** zur Identifizierung aller relevanten wirtschaftskriminellen Gefährdungspotentiale durch.

Auf Grundlage des ermittelten individuellen Gefährdungspotentials leitet die Institution die **erforderlichen Präventions- und Kontrollmaßnahmen** sowie die konkreten Aktivitäten zur Aufrechterhaltung ab. Dabei ergänzen bzw. spezifizieren die (Kontroll-)Maßnahmen die ohnehin durch die (sofern vorhanden) Interne Revision einer Institution vorzunehmenden Prüfungshandlungen zur allgemeinen Einhaltung und Wirksamkeit von Unternehmensprozessen sowie die des internen Kontrollsystems.

mögliche Einzelmaßnahmen

Mögliche Einzelmaßnahmen zur Erhebung der Gefährdung- oder Ausgangslage können sein:

1. Wirtschaftskriminalitätsgefährdungs**potential ermitteln**
2. institutionsspezifische **Gefährdungsanalyse** durchführen

M 2 Planen eines Systems zum Management von Wirtschaftskriminalität (A)

Die Institution führt ein System zum Management von Wirtschaftskriminalität ein. Hierzu berücksichtigt sie alle Aktivitäten, die sich mit der Planung von (Einzel-)Maßnahmen befassen, um ein wirkungsvolles und institutionsweites (Präventions-)System gegen (wirtschafts-)kriminelle Handlungen zu implementieren. Dieser Planungsprozess definiert im Sinne des **Plan-Do-Check-Act-Zyklus** alle Aktivitäten, die sich mit der Verhinderung und Aufdeckung von (wirtschafts-)kriminellen Handlungen sowie den daraus abgeleiteten Optimierungsaktivitäten innerhalb der Institution befassen.

mögliche Einzelmaßnahmen

Mögliche Einzelmaßnahmen des Planungsprozesses können sein:

1. **wesentliche Zielsetzungen** für das Management von Wirtschaftskriminalität der Institution festlegen (vgl. Auflistung am Ende dieser Maßnahme)
2. **Leitlinie und Regelwerk für das Management** von Wirtschaftskriminalität entwickeln und aktualisieren
3. **Maßnahmen/Aktivitäten** planen
4. **Bedarf für IT-Programme/Tools zur Prävention, Aufdeckung und Bearbeitung** von Wirtschaftskriminalität ermitteln
5. **Kompetenzen, Aufgaben und Verantwortlichkeiten** festlegen
6. **Zeitplan** festlegen und **benötigte Mitarbeiterkapazitäten/-expertise** ermitteln
7. **Informations- und Kommunikationskonzept** für das Management von Wirtschaftskriminalität entwickeln (einschließlich der Regelung von Melde- und Informationspflichten sowie der Eingangskanäle für eingehende Meldungen/Hinweise)
8. **Berichterstattung** für das System zum Management von Wirtschaftskriminalität festlegen

Zielsetzung

Wesentliches Ziel eines ganzheitlichen Managements von Wirtschaftskriminalität ist es, innerhalb der Institution Rahmenbedingungen zu schaffen und Maßnahmen zu entwickeln sowie diese zu implementieren, damit die Motivation und der Anreiz, die Gelegenheiten sowie die eigene Rechtfertigung der Mitarbeiter und externen Täter für unredliches Handeln, insbesondere zu Lasten der Institution, nachhaltig reduziert werden.

beispielhafte Prozessziele und Anforderungen

Ausgehend hiervon sollten die Prozessziele und Anforderungen für ein System zum Management von Wirtschaftskriminalität innerhalb einer Institution (einschließlich aller Tochtergesellschaften der Institution) beispielhaft wie nachfolgend dargestellt definiert werden:

1. Alle **gesetzlichen und aufsichtsrechtlichen Anforderungen** sind **eingehalten** bzw. umgesetzt.
2. Das **Gefährdungspotential** durch Wirtschaftskriminalität innerhalb der Institution (einschließlich aller

Tochtergesellschaften) ist **minimiert**.

3. Alle **Mitarbeiter** der Institution verfügen über die **erforderliche Sensibilität** und ein **angemessenes Bewusstsein** für den Umgang mit Gefährdungspotentialen durch wirtschaftskriminelle Handlungen.
4. Die **Aufdeckung und Bearbeitung von eingetretenen Vorfällen** (Deliktfälle bzw. Schadensereignisse) erfolgt **unverzüglich, umfassend und nachhaltig**.
5. Gegen aus aufgedeckten Delikt-/Schadensfällen und aus wirtschaftskriminellen Handlungen identifiziertem Gefährdungspotential werden **zeitnah wirksame Maßnahmen zur Prävention und Risikominimierung** eingeleitet.
6. Eine **regelmäßige und umfassende Kommunikation** sowie **Berichterstattung** sind durch ein entsprechendes **Managementinformationssystem** sichergestellt.
7. Die **institutionsspezifische Gefährdungsanalyse** erfüllt die definierten Anforderungen und wird regelmäßig aktualisiert.

M 3 Identifizieren der relevanten Schnittstellen (B)

Ein weiterer wichtiger Aspekt des Managements von Wirtschaftskriminalität ist das Management der aus den dargestellten diversifizierten Zuständigkeiten zwangsläufig resultierenden zahlreichen **Schnittstellen bei der effektiven Umsetzung der Querschnittsaufgabe** „Management von Wirtschaftskriminalität". Dieses Schnittstellenmanagement stellt erfahrungsgemäß in allen Institutionen sowohl eine große Herausforderung als auch mögliche Fehlerquellen bzw. -ursachen dar. Daher sollte die **Regelung aller Schnittstellen** mit besonderer Sorgfalt erfolgen und selbstverständlich auch **konsequent und verlässlich** eingehalten werden. Sinnvolle und abgestimmte Schnittstellenregelungen, die auch persönlichen Fähigkeiten von Mitarbeitern Rechnung tragen und beispielsweise mittels einer entsprechenden Matrix oder einer Checkliste dokumentiert werden können, stellen dagegen eine unverzichtbare Basis und ein wesentliches Element eines effektiven Managements von Wirtschaftskriminalität und insbesondere eines **Delikt-/Schadensfallmanagements** im Rahmen des Prozesses „Wirtschaftskriminalitäts(vor-)fälle bearbeiten" dar.

M 4 Festlegen eines Informations- und Kommunikations-managements (B)

Wesentliche Voraussetzung für ein wirksames und effektives Management von Wirtschaftskriminalität ist ein entsprechend etabliertes und „gelebtes“ **Kommunikations- und Informationsmanagement**. Dieses ist so zu gestalten, dass es sowohl innerhalb der Institution als auch – insbesondere im Krisenfall – nach außen gerichtet gegenüber Kunden, Partnern und Behörden im Besonderen sowie gegenüber der Öffentlichkeit im Allgemeinen wirkt.

Eine große Rolle im Rahmen des Schnittstellenmanagements spielt dabei auch der effiziente Umgang mit eingehenden Informationen. Die nachstehende graphische Darstellung veranschaulicht beispielhaft die Vielzahl von Eingangskanälen für Hinweise und Informationen auf einen möglichen Vorfall (Delikt-/Schadensfall):

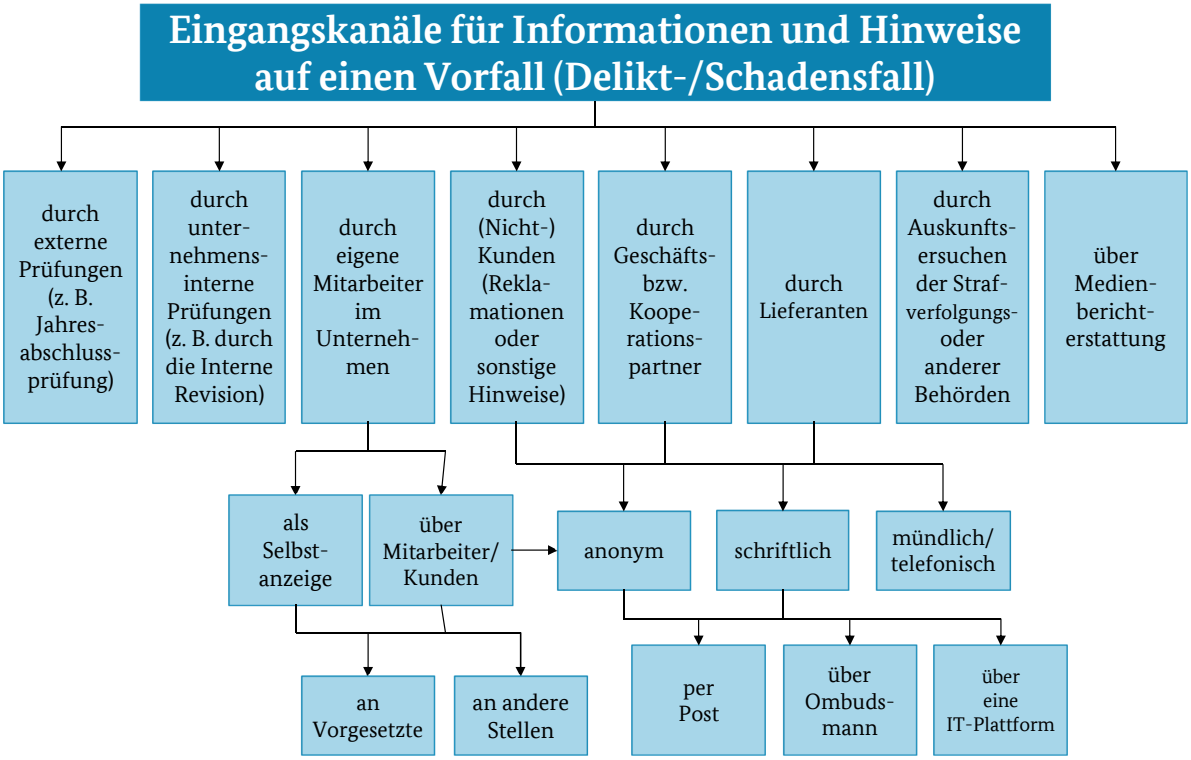


Abbildung 2: Eingangskanäle für Informationen und Hinweise auf einen Vorfall (Delikt-/Schadensfall)

Weitere Informationsquellen können u. a. **Warnhinweise** diverser Stellen (z. B. branchenspezifische Verbände und Interessenvertretungen, Verbraucherschutzverbände, Aufsichts- und Ermittlungsbehörden), **Presse-/Internetinformationen** oder **bilaterale Gespräche** auf Veranstaltungen sein.

Da diese **Hinweise und Informationen** in unterschiedlicher Form und Qualität sowie an verschiedenen Stellen innerhalb eines Unternehmens eingehen, müssen diese **institutionalisiert und zeitnah an** für eine fundierte Bewertung und weitere Bearbeitung ausgebildete **Verantwortungsträger weitergeleitet** werden. Damit dies möglichst reibungslos erfolgt, bedarf es wiederum eines professionellen Kommunikations- und Informationsmanagements.

M 5 Planen und Durchführen von Präventionsmaßnahmen (A)

Bei der Prävention vor Wirtschaftskriminalität sind alle Maßnahmen zu berücksichtigen sowie umzusetzen, die sich mit der Verhinderung von (wirtschafts-)kriminellen Handlungen durch zeitlich „vor der Tat“ erfolgende Aktivitäten befassen. Mögliche Einzelmaßnahmen sind bspw.:

mögliche Einzelmaßnahmen

1. **Präventionsprogramm** (weiter-)entwickeln bzw. aktualisieren
2. **Notfallkonzept** aktualisieren
3. **Präventionsmaßnahmen** identifizieren
4. **Präventionsvorkehrungen** treffen
5. **Versicherungsschutz** prüfen bzw. möglichen zusätzlichen/optimierten Versicherungsbedarf feststellen
6. Durchführung von **Penetrationstests** prüfen

M 6 Sensibilisieren der Mitarbeiter (A)

Ein wesentlicher Bestandteil der Präventionsmaßnahmen ist das **Steigern des Bewusstseins aller Mitarbeiter** für die Risiken und Gefahren aus (wirtschafts-)kriminellen Handlungen. Die Institution fördert dies mit angemessenen **Schulungen und Sensibilisierungsmaßnahmen** für die Mitarbeiter und nutzt hierfür eigene bestehende Regelungen oder die des Wirtschaftsgrundschutzes[5]. Die einzelnen Maßnahmen

mögliche Einzelmaßnahmen

[5] Der Wirtschaftsgrundschutz stellt hierfür mit dem Baustein Schulung und Sensibilisierung einen Leitfaden bereit.

können bspw. nachfolgende Aktivitäten sein:

1. **Schulungs- und Sensibilisierungsmaßnahmen** durchführen (z. B. Schulungen, Web-Based-Trainings, Ratgeber/Merkblätter)
2. **Abstimmung** zwischen **Beschwerdemanagement und Reklamationsbearbeitung** optimieren sowie entsprechend **für** mögliche **Auffälligkeiten sensibilisieren**
3. **Kommunikation über erfolgte Präventionsmaßnahmen** durchführen

M 7 Umsetzen von Maßnahmen zur Aufdeckung von Wirtschaftskriminalität (A)

Die Institution setzt Maßnahmen um, sodass **Vorfälle** (im Sinne von wirtschaftskriminellen Handlungen zu Lasten der Institution) möglichst **zeitnah identifiziert und aufgedeckt** werden.

Durch Implementierung von Aktivitäten, die sich von der Identifikation einer generellen Ebene (institutionsspezifische Gefährdungsanalyse) bis zur Einzelgeschäftsvorfallebene (Datenanalytik auffälliger Geschäftsvorgänge) durchziehen, soll die Aufdeckungsquote insgesamt erhöht sowie ein möglichst frühzeitiger Aufdeckungszeitpunkt erreicht werden. Der Institution stehen hier bspw. nachfolgende Maßnahmen zur Verfügung:

mögliche Einzelmaßnahmen

1. (fortlaufende) institutionsspezifische **Gefährdungs- und Risikoanalyse**
2. Prozesse/Handlungsfelder mit **Gefährdungspotential analysieren**
3. **Aufdeckungsprogramm**(e) für Wirtschaftskriminalität **aktualisieren**
4. **Muster-/Standardanalysen**
5. (auffällige) **Sachverhalte prüfen und aufklären** (weitere Einzelmaßnahmen siehe nachstehend unter M 10)

M 8 Umsetzen von erweiterten Maßnahmen zur Aufdeckung von Wirtschaftskriminalität (B)

Erweiterte Maßnahmen beziehen nicht nur die Standardanalysen ein, sondern umfassen weitere, ggf. gezielte Analysen. Diese setzt die Institution regelmäßig oder bei Bedarf und ausreichendem Anfangsverdacht ein. Der Institution stehen hier bspw. nachfolgende Maßnahmen zur Verfügung:

mögliche Einzelmaßnahmen

1. spezifische oder tiefergehende **Analysen**
2. **Datenbestände scannen**
3. **IT-Forensik-Maßnahmen** durchführen
4. (auffällige) **Sachverhalte prüfen und aufklären** (weitere Einzelmaßnahmen siehe nachstehend unter M 10)

M 9 Vorbereiten von Hilfsmitteln und Reaktionsoptionen (B)

Die Institution bestimmt, welche **Hilfsmittel** und **vorbereitenden Maßnahmen für** eine **Reaktion auf** einen **Verdachtsfall** erstellt werden. Dies können bspw. sein:

mögliche Einzelmaßnahmen

1. **Analysen und Vorgehensweisen** festlegen
2. (Warn-)**Meldungen/Informationen** erstellen
3. (anonyme) **Hotline** einrichten
4. **Konsequenzen und Maßnahmen** ableiten
5. **Kommunikation und Informationsweitergabe** von identifizierten bzw. möglichen Vorfällen (Delikt-/Schadensfälle) **sicherstellen**

M 10 Bearbeiten von Wirtschaftskriminalitäts(vor-)fällen (A)

Bei einem Vorfall bzw. einer auftretenden potentiellen wirtschaftskriminellen Handlung stellt die Institution eine **professionelle Bearbeitung** der (Vor-)Fälle sicher. Hierzu gehören u. a. die sorgfältige **Prüfung und Bewertung des Vorgangs** aus den verschiedenen rechtlichen gesetzlichen Sichtweisen (insbesondere **Straf-, Zivil-, Arbeits- und Datenschutzrecht**) sowie in aufsichtsrechtlicher Hinsicht, die **gerichtsverwertbare Sicherung von Beweismitteln** und die **Einleitung** sowie Umsetzung **von (Sofort-)Maßnahmen** bis hin zu (Rückgewinnungs-)Maßnahmen, um den bereits entstandenen oder auch erst

drohenden Schaden zu minimieren. Der Institution stehen hier bspw. nachfolgende Maßnahmen zur Verfügung:

mögliche Einzelmaßnahmen

1. (Erst-)**Bewertung von eingehenden Meldungen/Hinweisen** organisieren und vornehmen
2. notwendige **Sofortmaßnahmen** durchführen
3. **Prüfungen/Ermittlungen** durchführen
4. **Sachverhalte aufklären, Beweise und Unterlagen/Informationen gerichtsverwertbar sichern**
5. Einsatz von **kriminalpsychologischen Methoden** sowie von **Datenanalytikmethoden** erwägen und ggf. umsetzen
6. **rechtliche Bewertung** der Sachverhalte vornehmen
7. **Befragungen involvierter Personen** durchführen
8. **Maßnahmen** nach Ermittlung bzw. Überführung des Täters **einleiten und umsetzen**
9. **Krisenmanagement und -kommunikation**[6] durchführen
10. Information an die und **Zusammenarbeit mit den Ermittlungsbehörden** entscheiden (einschließlich Entscheidung über die Erstattung einer Strafanzeige)
11. **Schadenrückgewinnung** betreiben
12. (Ad-hoc-)**Berichterstattung** erstellen
13. (Warn-)**Meldungen/Informationen** erstellen
14. angemessene **Kommunikation intern und extern** durchführen

Die nachstehende Abbildung veranschaulicht den Prozess bei der institutionsinternen Bearbeitung von wirtschaftskriminellen Handlungen einschließlich der wesentlichen Zielsetzungen.

[6] Der Wirtschaftsgrundschutz stellt hierfür mit dem Standard 2000-3 einen Leitfaden bereit.

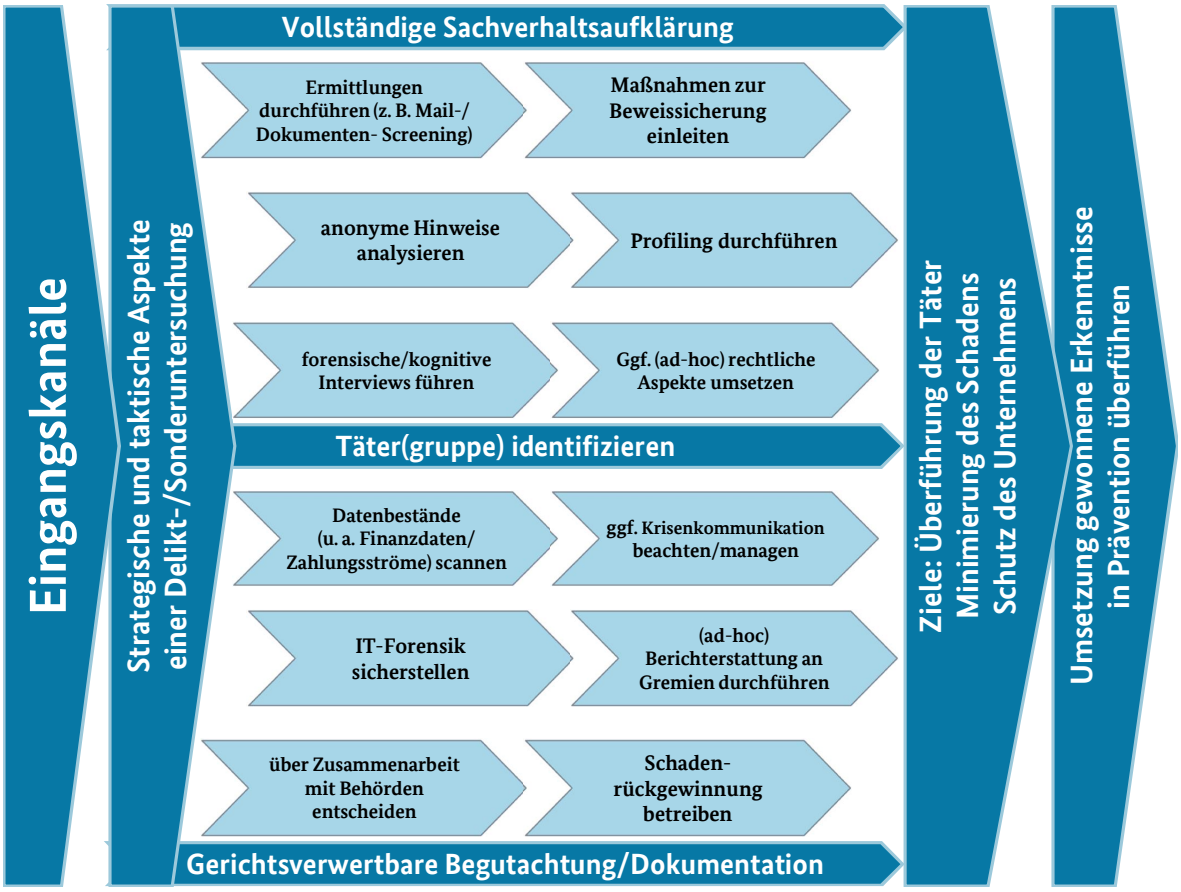


Abbildung 3: Bearbeitung von bzw. institutionsinterne Ermittlungen bei wirtschaftskriminellen Handlungen

Bei der Bearbeitung von wirtschaftskriminellen Vorfällen ist stets auch eine mögliche Einschaltung der bzw. eine Zusammenarbeit mit den Ermittlungsbehörden zu erwägen. Diese kann in vielerlei Hinsicht sinnvoll und mehrwertschöpfend sein.

M 11 Kontrolle und Bewertung des Systems zum Management von Wirtschaftskriminalität vornehmen (B)

Die Summe der Aktivitäten zur Vermeidung von wirtschaftskriminellen Handlungen zu Lasten der Institution wird seitens der Institution einem **ständigen Monitoring- und Qualitätsverbesserungsprozess** unterzogen, damit eine Aussage darüber getroffen werden kann, inwieweit die implementierten Maßnahmen ausreichend sind – beispielsweise auch zur Einhaltung der gesetzlichen Pflichten und Regularien – sowie ggf. optimiert werden müssen.

Mögliche Einzelmaßnahmen können sein:

mögliche Einzelmaßnahmen

1. **Monitoring** durchführen
2. Wirksamkeit der **Präventions- sowie Aufdeckungsmaßnahmen überprüfen** (auch für alle Teile der Institution)
3. identifizierte und aufgeklärte wirtschaftskriminelle Vorfälle auf **Verbesserungsmaßnahmen prüfen**
4. **Bewertung der Wirksamkeit vorhandener Präventionsmaßnahmen** bei neu auftretenden unredlichen/manipulativen/deliktischen Vorgehensweisen vornehmen
5. **Verbesserungsmaßnahmen ableiten** bzw. gegebenenfalls beauftragen
6. **Umsetzung** der Verbesserungsmaßnahmen **überwachen**
7. **Wirksamkeit** umgesetzter Verbesserungsmaßnahmen **prüfen**

M 12 Verbesserung des Systems zum Management von Wirtschaftskriminalität vornehmen (B)

Die Institution optimiert regelmäßig alle Maßnahmen und Aktivitäten zum Management von Wirtschaftskriminalität im Sinne eines kontinuierlichen Verbesserungsprozesses. Die Notwendigkeit hierzu erwächst aus der (regelmäßigen/ständigen) **Analyse und Bewertung der Wirksamkeit des Systems** zum Management von Wirtschaftskriminalität sowie aufgrund der permanenten Veränderungen der Vorgehensweisen der Täter. Somit entsteht hieraus das Bindeglied zum (ursprünglichen) Planungsprozess (M1) für nunmehr neue, veränderte oder zusätzliche Aktivitäten und somit ein **Regelkreislauf**, der als Ziel die **permanente Optimierung des Betrugsmanagements** hat, um bestmöglich „vor die Tat“ bzw. „vor den Schaden“ zu kommen und hierdurch einen wichtigen Beitrag zur Wettschöpfungskette der Institution zu leisten.

Mögliche Einzelmaßnahmen können sein:

mögliche Einzelmaßnahmen

1. (neue) **Szenarien/Muster erarbeiten, in** der institutionsspezifischen **Gefährdungsanalyse berücksichtigen und kommunizieren** sowie entsprechende **mögliche Indizien/Warnhinweise** („Red Flags“) **ableiten**
2. **zusätzliche/geänderte Präventionsmaßnahmen** zur

Verhinderung von Wirtschaftskriminalität **implementieren**

3. neue bzw. aktualisierte **Aufdeckungsprogramme** für wirtschaftskriminelle Handlungen **implementieren**
4. **Optimierung der Information und Kommunikation** innerhalb der Institution durchführen

5 Weiterführende Informationen

Weiterführende Informationen zum Thema „Umgang mit Wirtschaftskriminalität“ können den nachfolgenden Veröffentlichungen entnommen werden:

- *Bundeskriminalamt, jährliches Lagebild Wirtschaftskriminalität 2015*
- *Deutsches Institut für Interne Revision e. V. (DIIR), 2017, Internationale Grundlagen für die berufliche Praxis der Internen Revision 2017, Stand: 07.12.2016*
- *Institut der Wirtschaftsprüfer (IDW), 2012, Aufdeckung von Unregelmäßigkeiten im Rahmen der Abschlussprüfung (IDW PS 210), Stand: 12.12.2012*
- *Institut der Wirtschaftsprüfer (IDW), 2011, Grundsätze ordnungsgemäßer Prüfung von Compliance Management Systemen (IDW PS 980), Stand: 11.03.2011*
- *International Organization for Standardization (ISO), 2014, Zertifizierungsstandard ISO 19600 für Compliance Management-Systeme, 15.12.2014*
- *International Organization for Standardization (ISO), 2016, Zertifizierungsstandard ISO 37001 für Anti-Korruptions-Systeme, 15.10.2016*
- *Jackmuth, Hans-Willi/de Lamboy, Christian/Zawilla, Peter (Hg.), 2012, Fraud Management - Der Mensch als Schlüsselfaktor gegen Wirtschaftskriminalität, Frankfurt School Verlag, Frankfurt am Main*
- *Jackmuth, Hans-Willi/de Lamboy, Christian/Zawilla, Peter (Hg.), 2013, Fraud Management in Kreditinstituten - Praktiken, Verhinderung, Aufdeckung, Frankfurt School Verlag, Frankfurt am Main*
- *Jackmuth, Hans-Willi/de Lamboy, Christian/Zawilla, Peter (Hg.), 2017, Fraud & Compliance Management - Trends, Entwicklungen, Perspektiven, Frankfurt School Verlag, Frankfurt am Main*
- *Kopetzky, Dr. Matthias, 2010, Standard „Sonderuntersuchung“, Zeitschrift für Interne Revision, Nr. 5, S. 211 - 221*
- *Wells, Joseph T./Kopetzky, Dr. Matthias, 2012, Handbuch Wirtschaftskriminalität in Unternehmen, LexisNexis ARD Orac, Wien*
- *Zawilla, Peter/Hoffmann, Jens, 2016, Sonderuntersuchung 2.0: Kriminalpsychologie und Profiling erweitern revisorische Betrachtungsweisen, RevisionsPraktiker, 08-09/2016, S. 163 - 168*

6 Anlage

Das Wichtigste auf einen Blick (Themenübersicht)

Analyse

Erhebung von Risiken

Identifizierung von Vorgehensmustern/Modi Operandi

Klassifizierung und Bewertung von Risiken

Informationsquellen

Datenbestände scannen und analysieren

Monitoring durchführen

Organisation

Aufbau- und Ablauforganisation für das Management von Wirtschaftskriminalität festlegen und implementieren

Festlegen von Zuständigkeiten und Kompetenzen

Melde- und Berichtswege festlegen

Bereitstellen notwendiger personeller, technischer und sonstiger notwendiger Ressourcen

Versicherungsschutz herstellen

Dokumentation

Ziele dokumentieren

Melde- und Berichtswege dokumentieren

Stellenbeschreibungen erstellen

identifizierte Risiko- und Gefährdungspotentiale dokumentieren

Leitfaden zur Durchführung von internen Ermittlungen erstellen

Reaktionspläne und Notfallkonzept dokumentieren

Kommunikation

Kommunikations- und Informationsweitergabe von identifizierten bzw. möglichen Fällen

Krisenkommunikation durchführen

(Ad-hoc-)Berichterstattung über bearbeitete Fälle

(Warn-)Meldungen erstellen

Sensibilisierung

Schulungs- und Sensibilisierungsmaßnahmen für alle Mitarbeiter durchführen

kontinuierliche Weiterbildung der für das Management von Wirtschaftskriminalität zuständigen Mitarbeiter durchführen

kontinuierlicher Verbesserungsprozess

Wirksamkeit des Systems zum Management von Wirtschaftskriminalität überprüfen und bewerten und Optimierungspotential identifizieren und umsetzen

neue Szenarien/Muster identifizieren, bewerten und Präventionsmaßnahmen ableiten und umsetzen

aktuelle Entwicklungen erkennen und Präventionsmaßnahmen entwickeln und umsetzen

Maßnahmenübersicht und -kategorien

A - Basismaßnahmen	B - Standardmaßnahmen	C - erweiterte Maßnahmen
M1 Identifikation der Gefährdungs- bzw. Ausgangslage für das Management von Wirtschaftskriminalität M2 Planen eines Systems zum Management von Wirtschaftskriminalität M5 Planen und Durchführen von Präventionsmaßnahmen M6 Sensibilisieren der Mitarbeiter M7 Umsetzen von Maßnahmen zur Aufdeckung von Wirtschaftskriminalität M10 Bearbeiten von Wirtschaftskriminalitäts(vor-)fällen	A + M3 Identifizieren der relevanten Schnittstellen M4 Festlegen eines Informations- und Kommunikationsmanagements M8 Umsetzen von erweiterten Maßnahmen zur Aufdeckung von Wirtschaftskriminalität M9 Vorbereiten von Hilfsmitteln und Reaktionsoptionen M 11 Kontrolle und Bewertung des Systems zum Management von Wirtschaftskriminalität vornehmen M 12 Verbesserung des Systems zum Management von Wirtschaftskriminalität vornehmen	A und B +

Danksagung

Wir bedanken uns bei den vielen Experten, die ihr Fachwissen bei der Erstellung dieses Bausteins einfließen ließen und durch ihr Engagement die Entstehung erst ermöglicht haben. Insbesondere gilt unser Dank folgendem Autor und Mitwirkenden: Herr Peter Zawilla (FMS Fraud & Compliance Management Services GmbH).

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
www.verfassungsschutz.de

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn
www.bsi.bund.de

Herausgeber
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Rosenstraße 2, 10178 Berlin
asw-bundesverband.de

Redaktion/Bezugsquelle/Ansprechpartner
Prof. Timo Kob (Gesamtprojektleitung)

Gestaltung, Produktion
HiSolutions AG

Stand
April 2017

Auflage
1. Auflage