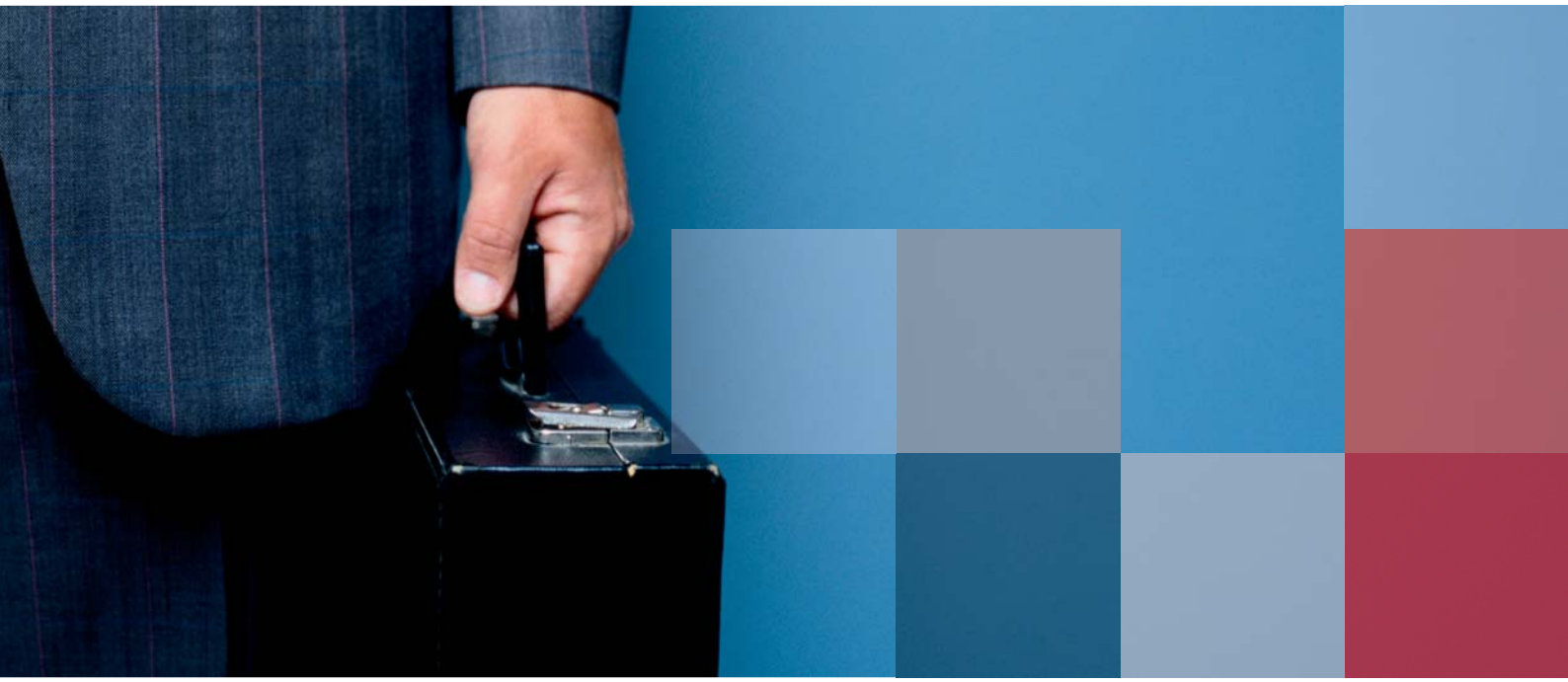
BearingPoint
Management
&Technology
Consultants

Status quo und Entwicklung zur Bekämpfung von Geldwäsche, Betrug und Terrorismus-finanzierung 2009



Inhaltsverzeichnis

Abkürzungsverzeichnis 4

1 Executive Summary 5

2 Ausgangslage und Zielsetzung der Studie 7

3 Die Ergebnisse der Studie im Detail 8

3.1 Teilnehmer der Studie 8

3.2 Stimmungsbild zum neuen Geldwäschebekämpfungsergänzungsgesetz 10

3.3 Umsetzung der Risikokategorisierung, Sorgfaltspflichten, Prozesse und Informationssysteme 18

3.4 Entwicklungen im Bereich der Gefährdungsanalyse und Verdachtsmeldungen 22

3.5 Status im Bereich der Betrugsbekämpfung 26

Über BearingPoint 31

Autoren 31

BearingPoint. Management & Technology Consultants

Abkürzungsverzeichnis

4. FMFG	Das vierte Finanzmarktförderungsgesetz
AML	Anti Money Laundering
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
CDD	Customer Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GwBekErgG	Geldwäschebekämpfungsergänzungsgesetz (GwG-Neu)
GwG	Geldwäschegesetz
KWG	Kreditwesengesetz
NCCT	Non-Cooperative Countries and Territories
OECD	Organization for Economic Cooperation and Development
OFAC	Office of Foreign Assets Control
PEP	Politisch exponierte Person
RS	Rundschreiben
VA	Verdachtsanzeigen
ZKA	Zentraler Kreditausschuss

1 Executive Summary

Das Aufgabengebiet der Geldwäschebekämpfung hat sich über die Jahre hinweg stetig ausgedehnt und erstreckt sich mittlerweile über eine Vielzahl von Themen, die u. a. Finanzsanktionen, Know-Your-Customer, Terrorismusfinanzierung, Politisch exponierte Personen und verstärkt auch das Thema der Betrugsbekämpfung umfassen. Die Umsetzung der 3. EU Anti-Geldwäsche-Richtlinie[1] durch das Geldwäschebekämpfungsergänzungsgesetz (GwBekErgG)[2] vom 21. August 2008 hat nun den Arbeitsbereich des Geldwäschebeauftragten um einige zusätzliche Aufgaben erweitert, die es erforderlich machen, Prozesse, Anweisungen, IT-Systeme, Schulungen, etc. neu zu überdenken und risikoorientiert anzupassen. Die Anpassungen müssen mit Auslauf der Übergangsfrist bis zum Mai diesen Jahres erfolgen, wobei die derzeitige wirtschaftliche Situation, zwangsläufige Sparmaßnahmen und viele offene operative Fragen die Umsetzung erschweren. Arbeitsgruppen und auch die Entwicklung der Industriestandards innerhalb des Zentralen Kreditausschusses (ZKA) durch die kreditwirtschaftlichen Spitzenverbände helfen, Klarheit in die rechtlichen Anforderungen zu bringen. Nichtsdestotrotz muss jedes Institut für sich selbst den richtigen risikobasierten Ansatz finden und damit die Feuerprobe durch die Wirtschaftsprüfer bestehen.

Vor diesem Hintergrund wurde durch BearingPoint nach den Geldwäschestudien in 2002, 2003 und 2005 nun eine weitere Studie zum Thema „Bekämpfung der Geldwäsche und Terrorismusfinanzierung“ durchgeführt. Die Studie wurde aufgrund der zunehmenden Bedeutung auch um den Themenbereich der Betrugsbekämpfung erweitert.

Ziel dieser Studie ist es, einen Überblick über den Status quo und die Entwicklung zur Bekämpfung von Geldwäsche, Betrug und Terrorismusfinanzierung zu geben. Die folgende Übersicht listet die wesentlichen Ergebnisse auf:

Stimmungsbild zum neuen Geldwäschebekämpfungsergänzungsgesetz

- Auch nach Inkrafttreten des aktuellen Gesetztes wird von Dreiviertel der Teilnehmer eine weitere Zunahme des Handlungsdrucks erwartet.
- Die Wirksamkeit der zusätzlichen gesetzlichen Regelungen wird von den Studienteilnehmern zunehmend in Zweifel gezogen.
- Die Umsetzung des „GwG-Neu“ hat maßgeblichen Einfluss auf die Aufgabengebiete des Geldwäschebeauftragten mit erheblichen prozessualen und IT-technischen Aufwänden.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:01:DE:HTML, Januar 2009
[2] Bundesgesetzblatt Jahrgang 2008, Teil 1 Nr. 37 ausgegeben zu Bonn am 20. August 2008

- Das Verständnis der Mitarbeiter für die fachlichen Anforderungen des „GwG-Neu“ sowie die Anforderungen an die IT-Systeme im Rahmen der Umsetzung des „GwG-Neu“ stellen die größten Herausforderungen dar.
- Die Einhaltung der „regulatorischen bzw. gesetzlichen Anforderungen“ ist für die meisten Institute der Hauptantrieb bei der Umsetzung von Geldwäschebekämpfungsmaßnahmen.

Umsetzung der Risikokategorisierung, Sorgfaltspflichten, Prozesse und Informationssysteme

- Bei der rechtzeitigen Erfüllung der erforderlichen Kundensorgfaltspflichten bis Mai 2009 wird es für viele Banken zeitlich sehr knapp werden. Bei Neukunden haben lediglich 37,5 % der Institute diese Vorgaben bereits umgesetzt; bei Bestandskunden liegt die Umsetzungsquote gar nur bei 27,5 %.
- 37 % *der* befragten Teilnehmer sehen keine Notwendigkeit einer IT-gestützten CDD-Lösung zur Risikokategorisierung der Kunden.

Entwicklungen im Bereich der Gefährdungsanalyse und Verdachtsmeldungen

- Die Ergebnisse aus der Gefährdungsanalyse werden bei vielen Banken aktiv im Indizienmodell der IT-Tools umgesetzt.
- Abweichend zum Jahresbericht 2007 der FIU Deutschland gibt knapp die Hälfte der befragten Teilnehmer an, dass die Rückmeldequote durch die Staatanwaltschaft bei Verdachtsanzeigen unter 10 % liegt.

Status im Bereich der Betrugsbekämpfung

- Neben den Kunden sehen fast die Hälfte der Institute ihre Mitarbeiter als die größte Gefahrenquelle bei Betrug.
- Trotz der Synergiemöglichkeiten sehen nur knapp die Hälfte der Befragten einen Sinn in einer kombinierten Gefährdungsanalyse von Geldwäsche und Betrugsbekämpfung.
- Die befragten Institute legen zur Zeit ihren systemtechnischen Fokus primär auf den Bereich der Geldwäschebekämpfung und weniger auf die Betrugsbekämpfung.

Die Details zu den Kernaussagen sind in der folgenden Sektion dargestellt.

2 Ausgangslage und Zielsetzung der Studie

Die Umsetzung des GwBekErgG macht es für den Geldwäschebeauftragten erforderlich, Prozesse, Anweisungen, Systeme, Dokumentation und Schulungen, etc. mit den neuen Anforderungen abzugleichen und gegebenenfalls risikoorientiert anzupassen. Hierbei sind die Vielzahl der Themengebiete und auch der Zeitrahmen eine große Herausforderung, wobei der risikobasierte Ansatz der Gesetzgebung den Instituten mehr Spielraum und somit eine Vereinfachung der Umsetzung erlauben soll. Nichtsdestotrotz stellt sich bei vielen Geldwäschebeauftragten nach wie vor die Frage, ob der Aufwand und Nutzen in einem sinnvollen Verhältnis steht und was die Implikationen für die einzelnen Aufgabengebiete des Geldwäschebeauftragten sind.

Vor diesem Hintergrund beleuchtet die BearingPoint Studie „Status quo und Entwicklung zur Bekämpfung von Geldwäsche, Betrug und Terrorismusfinanzierung 2009“ folgende Themenbereiche:

- Stimmungsbild zum neuen GwBekErgG
- Umsetzung der Risikokategorisierung, Sorgfaltspflichten, Prozesse und Informationssysteme
- Entwicklungen im Bereich der Gefährdungsanalyse und Verdachtsmeldungen
- Status im Bereich der Betrugsbekämpfung

Insgesamt haben 40 Institute aus dem privaten, genossenschaftlichen und öffentlichen Sektor an der Studie teilgenommen. Die Teilnahme erfolgte per Online-Befragung, Fax bzw. Email. Ein Großteil der teilnehmenden Institute hat bereits an den vorangegangenen Befragungen teilgenommen.

Die zugrunde liegenden Daten der aktuellen Studie wurden Ende 2008 erhoben. Angesichts der sehr hohen Anzahl von Banken in Deutschland reicht die Zahl der Teilnehmer nicht für eine repräsentative Aussage aus. Trotzdem lassen sich aufgrund der Zusammensetzung der befragten Banken aussagekräftige Trends erkennen.

BearingPoint. Management & Technology Consultants

3 Die Ergebnisse der Studie im Detail

Im Folgenden sind die Ergebnisse der Studie dargestellt. Die Beantwortung der Fragen erfolgte anonym. Den Teilnehmern stand bei der Beantwortung der Fragen offen, gegebenenfalls Zusatzkommentare zu erfassen. Auf Zusatzkommentare wird an den jeweiligen Stellen beispielhaft eingegangen. In diesem Zusammenhang sind auch einige Software-Produkte und Unternehmen erwähnt worden, wobei die Erwähnungen keinerlei Wertung darstellen.

3.1 Teilnehmer der Studie

Die Zahl der Teilnehmer beläuft sich auf 40 Institute. Von den Teilnehmern waren 20 aus dem privaten (inkl. deutsche Tochtergesellschaften oder Niederlassungen internationaler Großbanken), 15 aus dem öffentlich-rechtlichen und fünf Institute aus dem genossenschaftlichen Sektor.

Die Bilanzsumme der befragten Institute variierte von 0,5 bis über 250 Mrd. Euro. Besonders stark vertreten sind Banken mit einer Bilanzsumme von 1–9 Mrd. Euro und über 250 Mrd. Euro. Die Mehrzahl der teilnehmenden Institute beschäftigt weniger als 1.000 Mitarbeiter. Die Anzahl der Mitarbeiter im Bereich der Geldwäsche-, Betrugsbekämpfung und Terrorismusfinanzierung beträgt bei knapp über der Hälfte der Institute zwischen ein und drei Mitarbeiter. Das nächste Viertel der befragten Institute beschäftigt vier bis sieben Mitarbeiter in diesem Bereich.

Abbildung 1:
Bilanzsumme der teilnehmenden Institute

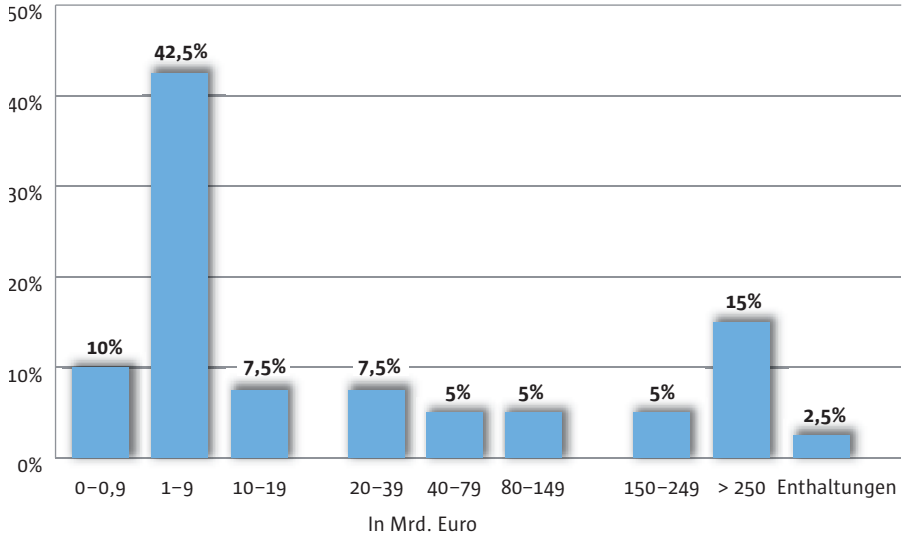
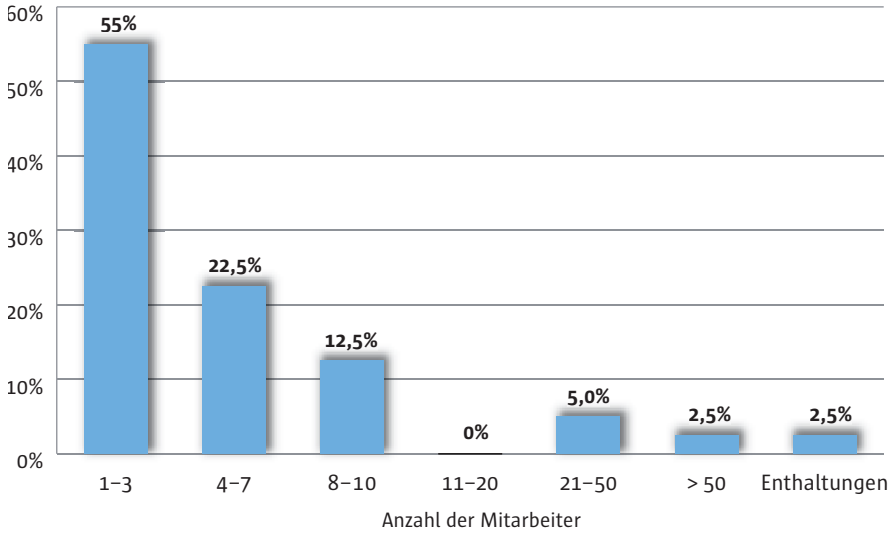


Abbildung 2:
Anzahl der Mitarbeiter im Bereich Geldwäsche-, Betrugsbekämpfung und Terrorismusfinanzierung



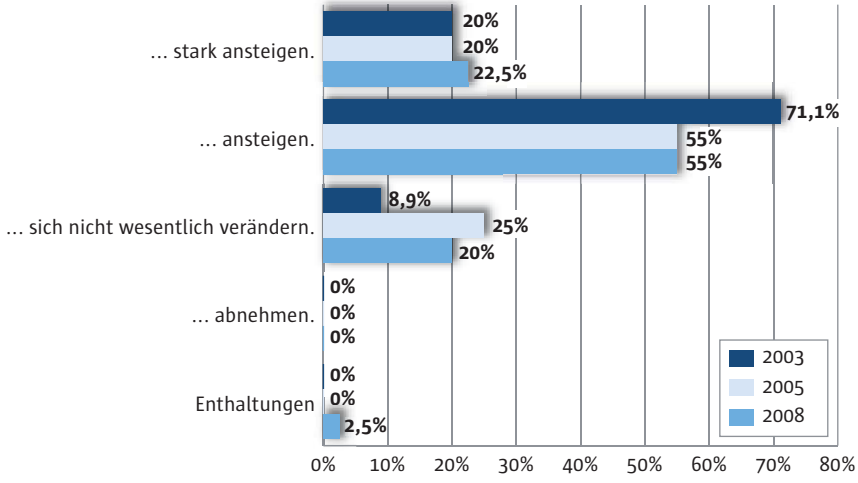
3.2 Stimmungsbild zum neuen Geldwäschebekämpfungsergänzungsgesetz

In der Umfrage von 2003[3] waren insgesamt ca. 90 % der Teilnehmer der Meinung, dass der Handlungsdruck im Zeitverlauf weiterhin zunehmen wird (70 % erwarteten einen Anstieg, weitere 20 % erwarteten einen starken Anstieg). Die Vorhersage war im Hinblick auf die Einführung der 3. EU Anti-Geldwäsche-Richtlinie begründet, da hier in der Tat ein verstärkter Handlungsdruck erzeugt wird.

Kernaussage 1:
Auch nach Inkrafttreten des aktuellen Gesetzes wird von Dreiviertel der Teilnehmer eine weitere Zunahme des Handlungsdrucks erwartet.

In 2008 sind mehr als Dreiviertel (77,5 %) der Teilnehmer der Meinung, dass der Handlungsdruck weiterhin steigen wird, wobei sich dieses Stimmungsbild konstant seit 2005[4] gehalten hat. Dies bedeutet, dass die Institute hier einen fortwährenden Drang zur Regulierung befürchten und den Prozess mit Einführung des „GwG-Neu" noch nicht für abgeschlossen halten. Die konkrete Ausgestaltung des weiteren Handlungsbedarfs für die einzelnen Institute wird u. a. maßgeblich durch die anstehenden Wirtschaftsprüfungen getrieben werden.

Abbildung 3:
Entwicklung des erwarteten Handlungsdrucks bei der Umsetzung von Maßnahmen zur Bekämpfung von Geldwäsche, Betrug und Terrorismusfinanzierung



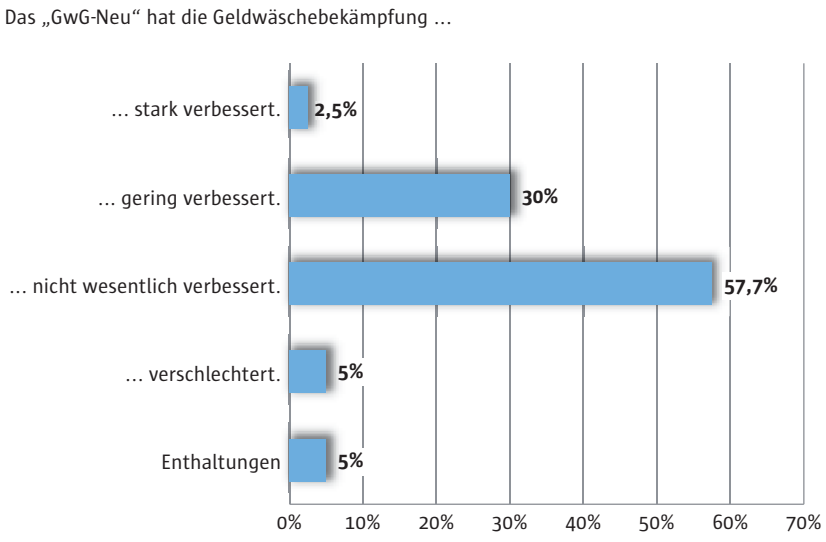
[3] BearingPoint Studie, Geldwäschebekämpfung – Umsetzung bei den deutschen Finanzinstituten, 2003.
[4] BearingPoint Studie, Geldwäschebekämpfung in Europa – Status quo und zukünftige Entwicklung, 2005.

Kernaussage 2:
Die Wirksamkeit der zusätzlichen gesetzlichen Regelungen wird von den Studienteilnehmern zunehmend in Zweifel gezogen.

Bei der erwarteten Zunahme des Handlungsdrucks, der durch die Gesetzgebung, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und Wirtschaftprüfer ausgeübt wird, stellt sich die Frage, ob man hier wirklich dem Ziel der effektiven Bekämpfung der Geldwäsche und Terrorismusfinanzierung näher gekommen ist. Bei dieser Frage waren 2003 noch ca. 68 % der Befragten der Meinung, dass die gesetzlichen Änderungen zu einer Verbesserung der Geldwäschebekämpfung[5] führen würden. Im Jahr 2005 lag dieser Anteil bei ca. 50 % und in 2008 liegt der Wert bei ca. 32 %. Mehr als die Hälfte der befragten Institute waren der Meinung, dass die Geldwäschebekämpfung sich nicht wesentlich verbessert hat.

Das negative Stimmungsbild ist auch dadurch bedingt, dass die Zusatzaufwände als erheblich eingestuft werden und aus Sicht vieler Teilnehmer in keinem guten Verhältnis zum Nutzen stehen.

Abbildung 4:
Meinungen zum „GwG-Neu" in der Bekämpfung von Geldwäsche, Betrug und Terrorismusfinanzierung



[5] BearingPoint Studie, Geldwäschebekämpfung – Umsetzung bei den deutschen Finanzinstituten, 2003

Kernaussage 3:
Die Umsetzung des „GwG-Neu“ hat maßgeblichen Einfluss auf die Aufgabengebiete des Geldwäschebeauftragten mit erheblichen prozessualen und IT-technischen Aufwänden.

Bei der Betrachtung der erwarteten Zusatzaufwände lässt sich ablesen, dass alle Befragten die „GwG-Neu“-Umsetzungen im operativen Geschäft als hoch bzw. mittel einstufen. Fast alle Aufgabengebiete des Geldwäschebeauftragten sind maßgeblich von der Umsetzung betroffen und ziehen teilweise einen erheblichen Arbeitsaufwand nach sich.

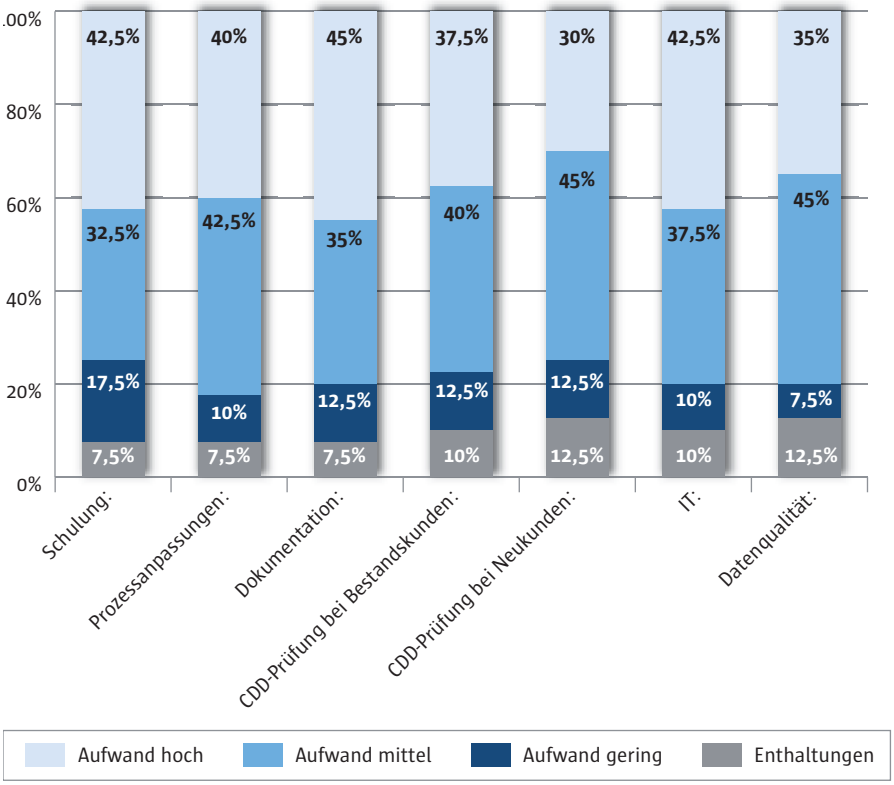
In den Arbeitsbereichen „Dokumentation“ (45 %), „IT“ (42,5%) und „Schulungen“ (42,5 %) vermuten die Studienteilnehmer am häufigsten einen hohen Aufwand. In den Bereichen „Datenqualität“ (45 %) „CDD-Prüfungen bei Neu- (42,5 %) und Bestandskunden (40 %)“ sowie „Prozessen“ (42,5 %) vermuten die meisten Teilnehmer mittlere Aufwände.

Insbesondere die enge Verzahnung und Abhängigkeit der Aufgabenbereiche untereinander macht die Umsetzung komplex. Erschwerend kommt auch noch hinzu, dass die Interpretation der rechtlichen Anforderungen zwischen den Instituten unterschiedlich vorgenommen wird. Hinsichtlich der Interpretation sollte der ZKA-Industriestandard, der zum Zeitpunkt der Umfrage noch nicht finalisiert war, klarere Vorgaben machen.

In England gibt es eine ähnliche Vorgehensweise hinsichtlich der rechtlichen Interpretation durch einen Industriestandard. Die Joint Money Laundering Steering Group (JMLSG)[6], ein Gremium, welches aus den Spitzenverbänden der englischen Finanzwirtschaft besteht, produziert die sog. „JMLSG Guidance“. Diese Richtlinien geben klare Vorgaben hinsichtlich der Umsetzung wieder. Die „JMLSG Guidance“ sind mit der ‚Financial Services Authority‘ (FSA) abgestimmt[7] und geben somit den Rahmen zur risikobasierten Umsetzung vor.

[6] http://www.jmlsg.org.uk/bba/jsp/polopoly.jsp?d=749, Januar 2009
[7] http://www.jmlsg.org.uk/content/1/c4/98/21/FSA_letter_of_comfort_on_guidance.pdf, Januar 2009

Abbildung 5:
Aufwandsschätzungen für die Erfüllung des „GwG-Neu“ in den Arbeitsbereichen des Geldwäschebeauftragten



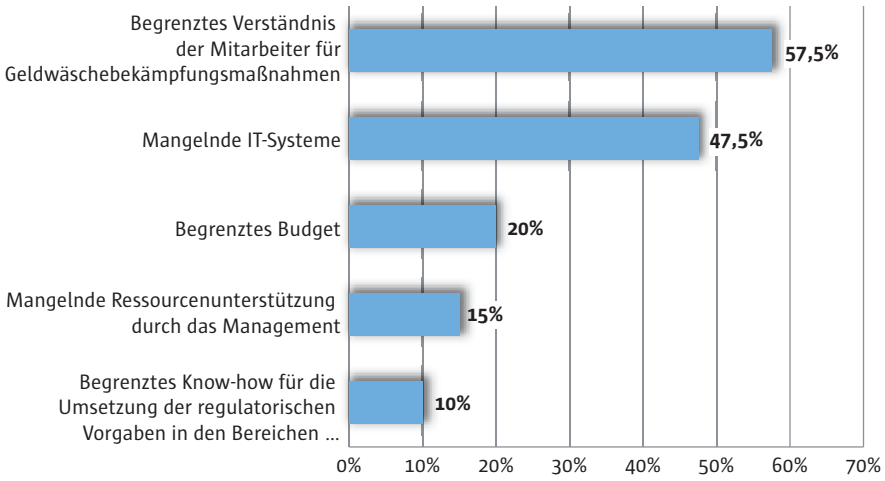
Kernaussage 4:
Das Verständnis der Mitarbeiter für die fachlichen Anforderungen des „GwG-Neu“ sowie die Anforderungen an die IT-Systeme im Rahmen der Umsetzung des „GwG-Neu“ stellen die größten Herausforderungen dar.

Bei der Umsetzung des „GwG-Neu“ sehen sich die Geldwäschebeauftragten mit einer Reihe von Herausforderungen konfrontiert. Das begrenzte Verständnis der Mitarbeiter für Geldwäschebekämpfungsmaßnahmen stellt hierbei das größte Problem dar (57,5 %). Um dem Problem des begrenzten Verständnisses bei den Kolleginnen und Kollegen besser entgegenwirken zu können, haben einige Geldwäschebeauftragte die Schulungsmaßnahmen erfolgreich dazu genutzt, ihre Abteilungen als wertschaffenden bzw. werterhaltenden Dienstleister innerhalb der Bank zu positionieren. Die Schulungsmassnahmen zielten insbesondere darauf ab, die Funktion des Reputationsschutzes und Möglichkeiten der Risikominimierung hervorzuheben, um eine größere Akzeptanz innerhalb der Institute zu erreichen.

Mangelnde IT-Systeme (47,5 %) u. a. bedingt durch schlechte Datenqualität, fehlende Auswertungen sowie die fehlerhafte Ermittlung von Kundeninformationen werden von vielen Instituten als kritisch betrachtet.

Die Budgetsituation (20 %) sowie die Ressourcensituation und Unterstützung durch das Top Management (jeweils 15 %) wird nur von wenigen als Risikofaktor genannt.

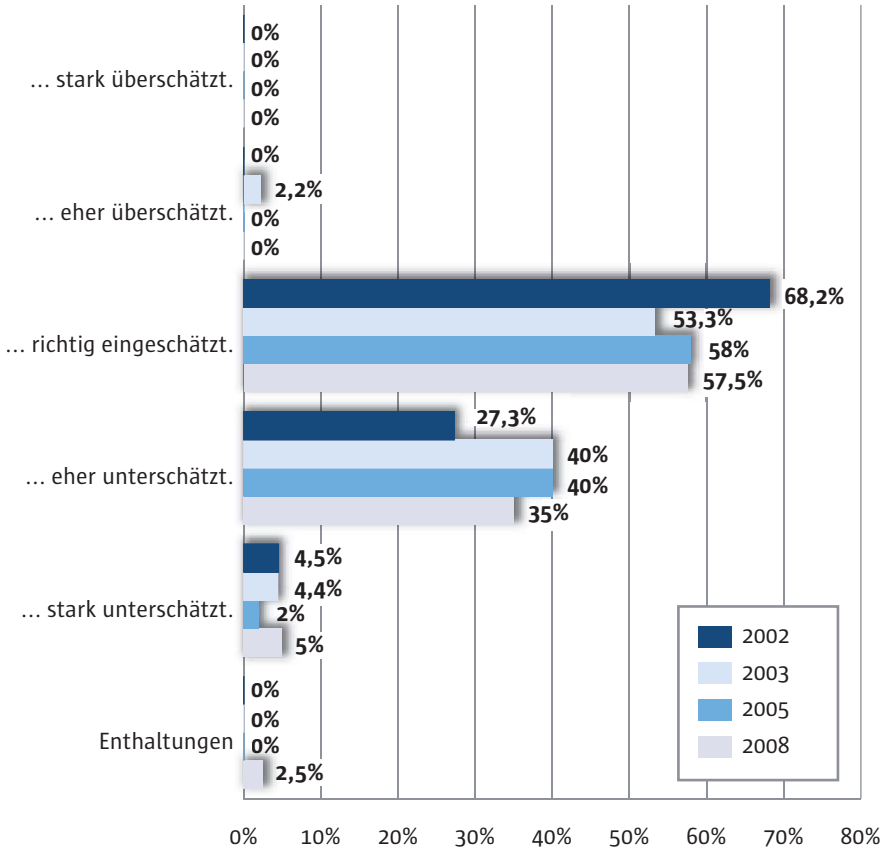
Abbildung 6:
Die größten Herausforderungen bei der Umsetzung des „GwG-Neu“



Trotz der Zunahme der gesetzlichen Anforderungen sowie der zahlreichen Herausforderungen des Geldwäschebeauftragten hat die Unterstützung des Top Managements bzw. deren Einschätzung des Themas Geldwäschebekämpfung und Terrorismusfinanzierung sich nicht verbessert, so dass der Geldwäschebeauftragte hier nach wie vor primär auf sich alleine gestellt ist.

So sind weiterhin ca. 40 % der Geldwäschebeauftragten der Meinung, dass das Top Management die Situation „unterschätzt" bzw. sogar „stark unterschätzt". Dies überrascht, da nur wenige Teilnehmer – wie oben erwähnt – die Unterstützung durch das Management und die Ressourcenausstattung als kritisch einstufen.

Abbildung 7:
Einschätzung der Bedeutung des Themas Geldwäsche-, Betrugsbekämpfung und Terrorismusfinanzierung durch das Top Management

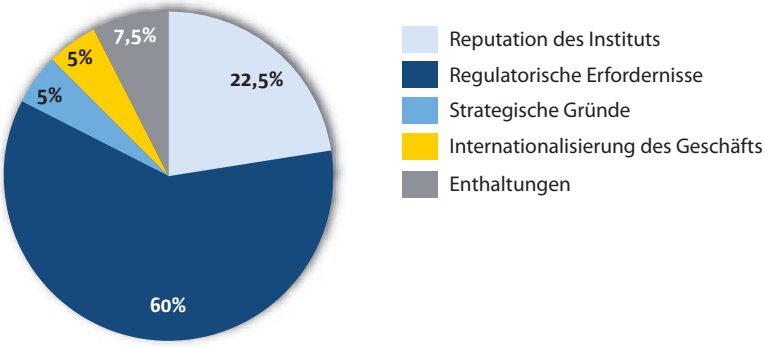


Kernaussage 5:
Die Einhaltung der „regulatorischen bzw. gesetzlichen Anforderungen“ ist für die meisten Institute der Hauptantrieb bei der Umsetzung von Geldwäschebekämpfungsmaßnahmen.

Beim Ausbau der Sicherungsmaßnahmen gegen Geldwäschevorfälle und Terrorismusfinanzierung ist bei den befragten Instituten nach wie vor seit 2005 das Hauptthema ‚Erfüllung der regulatorischen bzw. gesetzlichen Anforderungen‘ (60 %) unangefochten an der Spitze. Diese Statistik lässt darauf schließen, dass auch in Zeiten, in denen die Bankenbranche im Zuge der Finanzkrise stark kritisiert wird, eine gut funktionierende Bekämpfung von Geldwäsche, Betrug und Terrorismusfinanzierung nicht als publikumswirksame, vertrauensfördernde Aufgabe gesehen wird, die auch dem Ruf des Institutes zu Gute kommt. Lediglich 22,5 % sehen die ‚Reputation des Institutes‘ als Haupttreiber für die Umsetzung von Geldwäschebekämpfungsmaßnahmen.

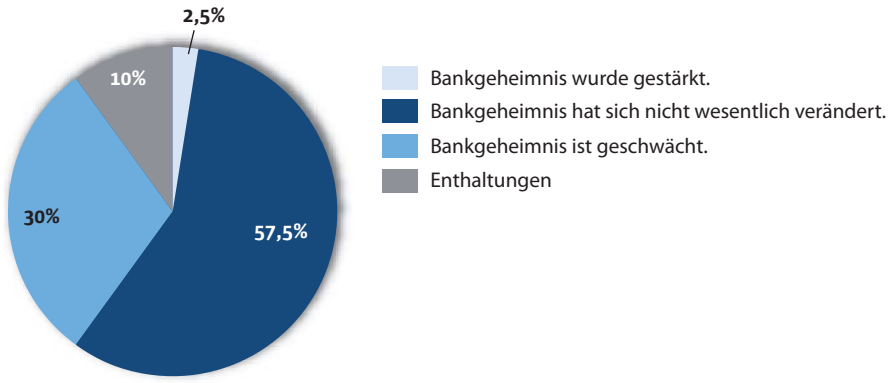
Bei Instituten, die mit ihren Niederlassungen stärker global agieren und bspw. in den USA oder England aktiv sind, ist eine funktionierende Organisation zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung als Marktzulassungsvoraussetzung und somit zur Wettbewerbsfähigkeit unerlässlich. Dementsprechend sind strategische Gründe und die Internationalisierung des Geschäfts mit jeweils 5 % als Haupttreiber vertreten.

Abbildung 8:
Haupttreiber für die Umsetzung von Maßnahmen zur Bekämpfung von Geldwäsche, Betrug und Terrorismusfinanzierung



Die verschärften Geldwäschebestimmungen führen nach Einschätzung der meisten Befragten zu keiner weiteren Schwächung des Bankgeheimnisses. Während im Jahr 2003 noch 72 % der Teilnehmer den Standpunkt vertraten, dass eine Schwächung des Bankgeheimnisses stattgefunden hat, teilten im Jahr 2008 nur noch 30 % diese Meinung. Ungefähr Zweidrittel waren der Ansicht, dass das „GwG-Neu“ keine Auswirkung auf das Bankgeheimnis hat. Nach Einschätzung der Studienteilnehmer führte die Kontenabfrage (vgl. § 24c KWG) zur größten Schwächung des Bankgeheimnisses.

Abbildung 9:
Stärkung oder Schwächung des deutschen Bankgeheimnisses 2008

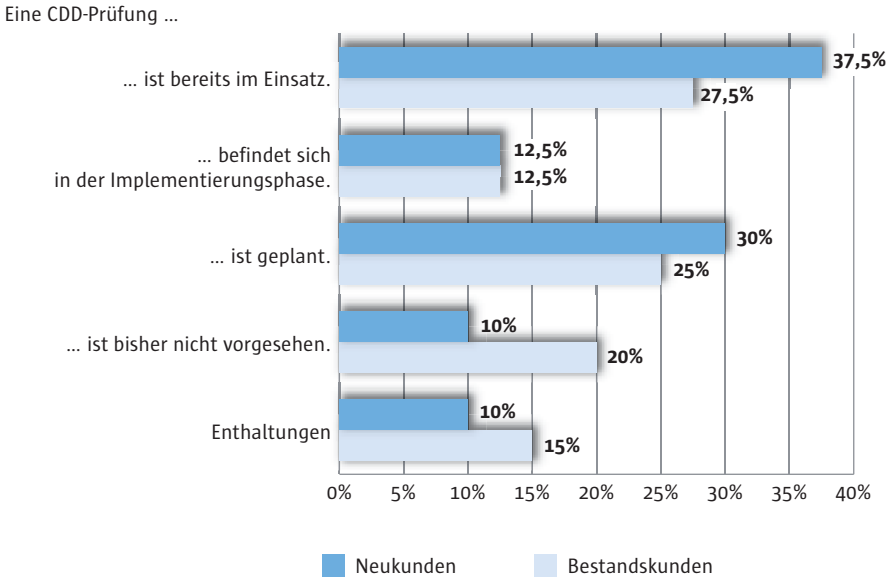


3.3 Umsetzung der Risikokategorisierung, Sorgfaltspflichten, Prozesse und Informationssysteme

Kernaussage 6:
Bei der rechtzeitigen Erfüllung der erforderlichen Kundensorgfaltspflichten bis Mai 2009 wird es für viele Banken zeitlich sehr knapp werden. Bei Neukunden haben lediglich 37,5 % der Institute diese Vorgaben bereits umgesetzt; bei Bestandskunden liegt die Umsetzungsquote gar nur bei 27,5 %.

Ein Großteil der Befragten plant, die gesetzlich geforderten ‚Sorgfaltspflichten und internen Sicherungsmaßnahmen'[8] im Rahmen von CDD-Prüfungen abzubilden. Der geplante Abdeckungsgrad ist bei Neukunden mit 80 % deutlich höher als bei Bestandkunden mit 65 %. Zu Berücksichtigen ist die hohe Anzahl von Enthaltungen.

Abbildung 10:
CDD-Prüfungen bei Kunden



[8] Geldwäschebekämpfungsergänzungsgesetz, http://dejure.org/gesetze/GwG, Februar 2009

Der Schwerpunkt der CDD-Prüfungen bei Neukunden ist z. T. dadurch zu erklären, dass die Prozessanpassungen bei Neukunden leichter aufzusetzen sind, denn hier können die relevanten Aspekte gleich bei der Erfassung der Kundeninformationen aufgenommen werden.

Bei Bestandskunden gestaltet sich dieser Prozess schwieriger, da hierbei auf alte Kundendaten zurückgegriffen werden muss und gegebenenfalls eine Nacherfassung bestimmter Informationen erforderlich ist. Zusätzlich sind die typischen Datenqualitätsprobleme (z. B. veraltete und/oder falsche Einträge, Dubletten, etc.) zu berücksichtigen. Diverse Institute haben zur Bewältigung des Datenqualitätsproblems mit Erfolg dedizierte Datentools und Methodiken angewendet, um eine verlässlichere Datengrundlage für die Priorisierung der Risiken zu schaffen.

Kritisch anzumerken ist, dass der aktuelle Umsetzungsstand noch deutlich hinter den Planzahlen liegt. Bei Neukunden haben lediglich 37,5 % der Institute diese Vorgaben bereits umgesetzt; bei Bestandskunden liegt die Umsetzungsquote gar nur bei 27,5 %. Für viele Institute kann die fristgerechte Einhaltung der Umsetzung des „GwG-Neu" bis Mai 2009 daher nur über den erhöhten Einsatz von Ressourcen oder „work arounds" dargestellt werden.

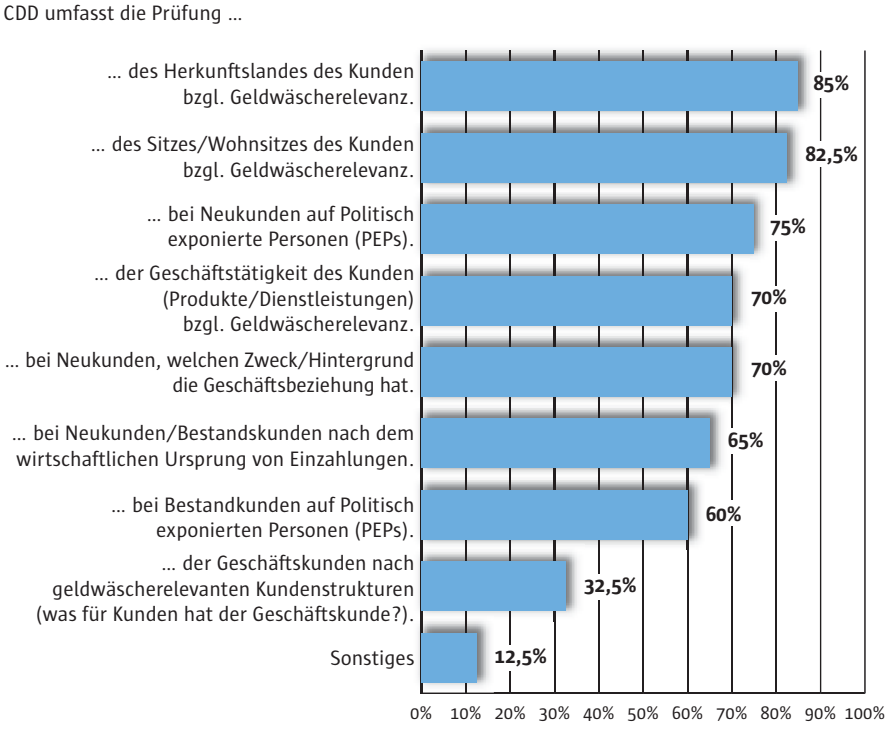
Ein Großteil der Befragten verwendet zur Kundenrisikoklassifizierung Kriterien, die u. a. in der publizierten BaFin-Übersetzung des „Leitfadens zum risikoorientierten Ansatz zur Bekämpfung von Geldwäsche" der Financial Action Task Force (FATF)[9] und der „Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität"[10] des Baseler Bankenausschusses veröffentlich sind. Bei der Anwendung der einzelnen Kriterien werden von den einzelnen Instituten geschäfts-, kunden- und produktspezifische Faktoren berücksichtigt. Von ca. 80 % der Befragten werden ‚Unternehmens-/Wohnsitz' und ‚Herkunftsland' des Kunden verwendet. Eine Überprüfung auf Politisch exponierte Personen (PEP) findet insbesondere bei Neukunden (75%) statt. Bei Bestandskunden wird diese Prüfung jedoch nur bei ca. 60 % der Institute durchgeführt. Fast Dreiviertel der Befragten bewertet die beanspruchten Produkte und Dienstleistungen ihrer Vertragspartner hinsichtlich potenzieller Geldwäscherisiken (z. B. Kunde hat internationales Geschäft und benötigt weitläufige Korrespondenzbankbeziehungen) sowie die Hintergründe der Branche des Kunden. In diesem Zusammenhang begutachten 65 % der Teilnehmer auch den wirtschaftlichen Ursprung von Einzahlungen.

Bei der Überprüfung der Kunden hinsichtlich ihrer Kundenstrukturen (Know Your Customer's Customer) liegt der Anteil bei 32,5 %. Dies hängt damit zusammen, dass diese tiefergehende Analyse aufgrund des größeren Aufwandes unter Begründung der risikobasierten Verhältnismäßigkeit lediglich bei „High Risk Kunden" angewendet wird.

[9] „Leitfaden zum risikoorientierten Ansatz zur Bekämpfung von Geldwäsche und Terrorismusbekämpfung" (Übersetzung), Juni 2007, Financial Action Task Force, Paris, Frankreich

[10] „Customer Due Diligence for Banks", Oktober 2001, Baseler Ausschuss für Bankenaufsicht, Basel, Schweiz

Abbildung 11:
Prüfkriterien bei der CDD-Risikoklassifizierung

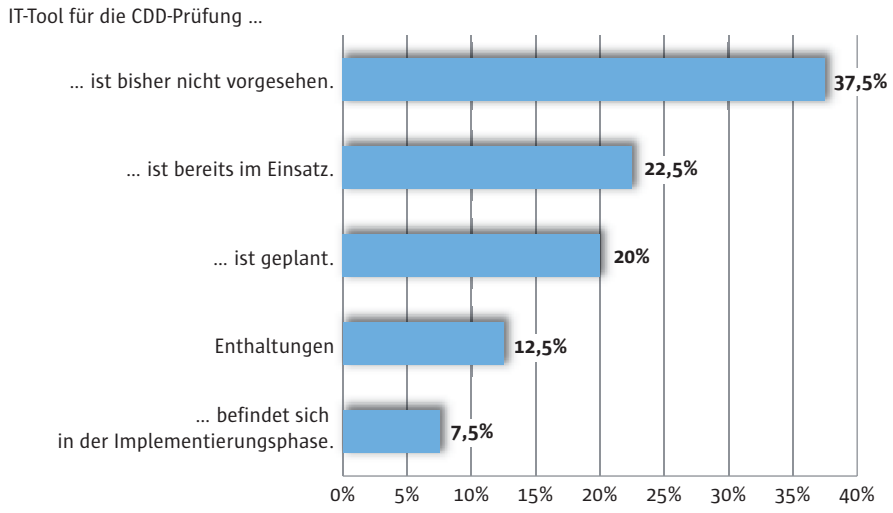


Im Rahmen der Identifizierung von Politisch exponierten Personen (PEP) werden bei der Hälfte der Befragten die Kundenstammdaten mit extern verfügbaren Informationen abgeglichen. Eine Reihe von Instituten verwendet jedoch keinen automatischen externen Listenabgleich, sondern fragt im Rahmen eines Fragebogens/Kundengesprächs, ob der Vertragspartner oder der wirtschaftlich Berechtigte PEP zutreffende politische Funktionen ausübt. Weitere Faktoren, die bei der Anwendung der verstärkten bzw. vereinfachten Sorgfaltspflicht in Betracht gezogen werden, sind u. a. beschränktes Geldwäscherisiko bei Produkten (z. B. Bausparprodukte), Berufsgruppen, Rechtsform der Unternehmung (z. B. börsennotierten Gesellschaften), aktenkundige Personen oder Gesellschaften. Bei 15 % der Umfrageteilnehmer werden die Kundenstammdaten mit der Liste des Office of Foreign Assets Control (OFAC), Dies trifft insbesondere für Institute zu, die eine verstärkte Präsenz in den USA haben.

Kernaussage 7:
37 % der befragten Teilnehmer sehen keine Notwendigkeit einer IT-gestützten CDD-Lösung zur Risikokategorisierung ihrer Kunden.

Bei der Frage, ob bei der CDD-Risikokategorisierungs-Prüfung IT-Tools zur Hilfe genommen werden sollen, bejahte fast die Hälfte der Teilnehmer die Frage (22,5 % haben eine CDD-Lösung im Einsatz, 7,5 % befinden sich in der Implementierung, 20 % haben eine IT-basierte CDD-Unterstützung geplant). Weitere 37,5 % haben den Einsatz eines CDD-Tools nicht vorgesehen, etwa 13 % sind noch unentschieden. Unter der Berücksichtigung der erforderlichen Umsetzung kann man davon ausgehen, dass im ersten Umsetzungsschritt die CDD-Prüfungen von diversen Instituten manuell durchgeführt werden müssen. Die manuelle Umsetzung wird verstärkt von kleinern Instituten mit einer Bilanzsumme kleiner 10 Mrd. Euro präferiert.

Abbildung 12:
Verwendung von IT-Tools für die Customer Due Diligence (CDD)



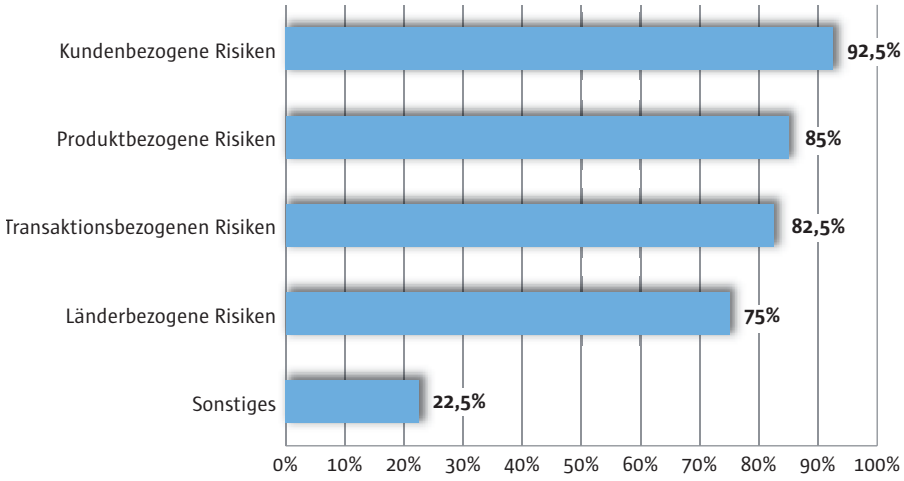
25 % der befragten Institute verwenden die bestehende Research/Monitoring Plattform für eine IT-gestützte CDD-Prüfung. Dies bietet u. a. die Möglichkeit Synergien im Bereich der technischen Infrastruktur und Systembetreuungsressourcen zu nutzen. Ein Viertel der Befragten verwendet getrennte Systeme. Dabei sind u. a. folgende Systeme im Einsatz: FIDUCIA IT AG ‚agree Bankarbeitsplatz' (BAP) und Geno-Sonar, Tonbeller AG „Siron AML" und Innovations GmbH „Compliance Suite".

3.4 Entwicklungen im Bereich der Gefährdungsanalyse und Verdachtsmeldungen

Nachdem 2003 bereits 86 % der befragten Institute eine Gefährdungsanalyse für ihre Kunden durchführten, liegt der aktuelle Abdeckungsgrad bei nahezu 100 %. Bei der Betrachtung der Gefährdungsanalyse nimmt mittlerweile ein Großteil der Umfrageteilnehmer (82,5 % bis 92,5 % – je nach Risikokategorie) die Leitlinien gemäß des BaFin Rundschreibens 8/2005 (GW) als Grundlage und betrachtet die kunden-, produkt- und transaktionsbezogenen Risiken hinsichtlich der potenziellen Geldwäschegefahr. Länderrisiken werden bei 75 % der Befragten berücksichtigt.

Darüberhinaus berücksichtigen einige Institute folgende Aspekte: Personalbezogene Risiken, Branchen- und Standortrisiken, Risiken im Zusammenhang mit der Rechtsform sowie Prozess-, Mitarbeiter- und Technologierisiken.

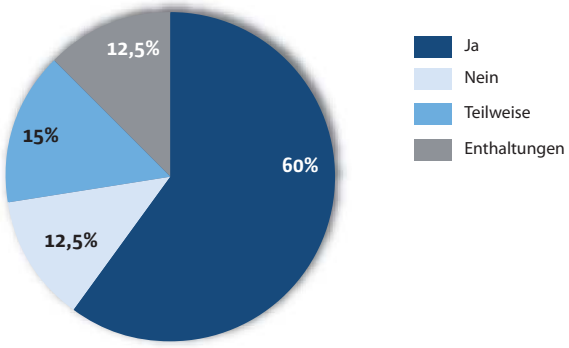
Abbildung 13:
Risikoaspekte der Gefährdungsanalyse



Kernaussage 8:
Die Ergebnisse aus der Gefährdungsanalyse werden bei vielen Banken aktiv im Indizienmodell der IT-Tools umgesetzt.

60 % der befragten Institute gaben an, dass die Ergebnisse der Gefährdungsanalyse in das Indizienmodell der IT-Lösung übernommen werden. 15 % der Teilnehmer gaben an, dass sie bedingt die Ergebnisse ihrer Gefährdungsanalyse im Indizienmodell abbilden. 12,5 % gaben an, keine Abstimmung zwischen ihrer Gefährdungsanalyse und ihrem Indizienmodell vorzunehmen. Weitere 12,5 % haben hierzu keine Antwort gegeben. Dies hat zur Folge, dass die Risikobewertung gemäß Gefährdungsanalyse nicht im Anti Money Laundering (AML)-Tool umgesetzt wird. Mit den Konsequenzen, dass die Ergebnisse der AML-Tools bei ca. einem Drittel der Teilnehmer nur begrenzt zur Identifizierung von Geldwäscherisiken genutzt werden können, da die zugrunde liegenden Indizienmodelle nicht gemäß der Gefährdungsanalyse institutsspezifisch angepasst sind.

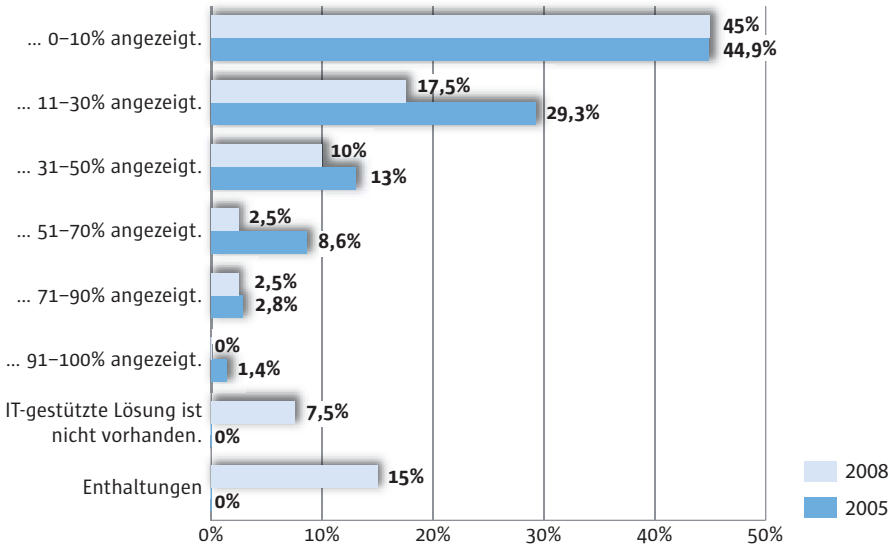
Abbildung 14:
Verwendung der Erkenntnisse aus der Gefährdungsanalyse im Risikoscoring des Indizienmodells



Die Anzahl der Verdachtsfälle, die durch IT-Tools generiert und an die Strafverfolgungsbehörden weitergegeben worden sind, ist im Vergleich zum Jahre 2005 in etwa gleich geblieben. In den beiden Vergleichzeiträumen wurden von fast der Hälfte der Banken lediglich ca. 10 % der Meldungen angezeigt (2005: 45 % bzw. 2008: 45 %). 17,5 % der Teilnehmer meldeten 11–30 % der gesamten Treffer, mehr als 30 % der Meldungen werden lediglich von 2–7 % der Teilnehmer angezeigt (15 % wollten zu dieser Frage keine Stellung nehmen).

Im Jahresbericht 2007 der Financial Intelligence Unit Deutschland (FIU)[11] wird eine rückläufige Entwicklung der Verdachtsanzeigen explizit erwähnt. Die Erwartungshaltung der Zentralstelle hinsichtlich der Anzahl der Anzeigen ist, dass Geldwäscheverhaltensformen mit Hilfe von EDV-Lösungen leichter zu identifizieren seien und somit für ein erhöhtes Anzeigenaufkommen sorgen sollten. Die Annahme der Zentralstelle ist, dass die Nachforschungen bei sich ergebenden komplexeren „Verdachtslagen demnach zunehmend weniger angezeigt“[12] werden. Die FIU vermerkt, dass sie die weitere Entwicklung beobachten und eine „entsprechende Ursachenforschung betreiben“ wird.

Abbildung 15:
Anteil der Verdachtsanzeigen aus dem Research/Monitoring Tool, die an die Strafverfolgungsbehörden gemeldet werden



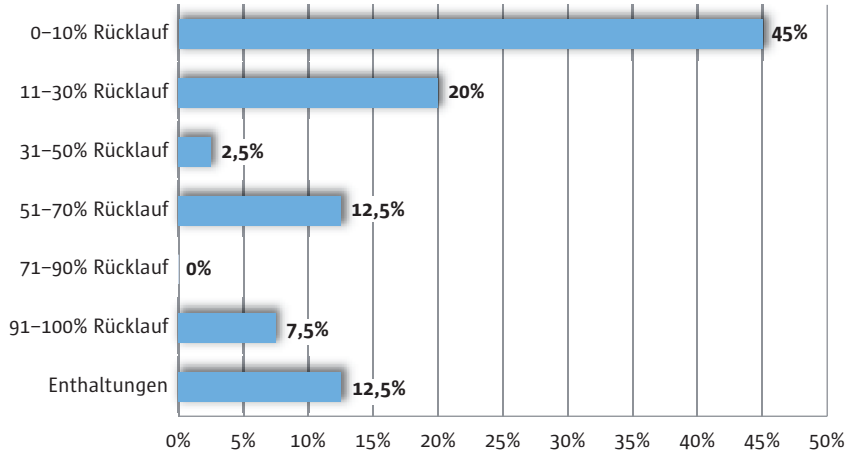
[11] http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2007.pdf, Januar 2009
[12] http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2007.pdf, Januar 2009

Kernaussage 9:
Abweichend zum Jahresbericht 2007 der FIU Deutschland gibt knapp die Hälfte der befragten Teilnehmer an, dass die Rückmeldequote durch die Staatanwaltschaft bei Verdachtsanzeigen unter 10 % liegt.

Bei den Verdachtsanzeigen (VA) ist die mangelnde Rücklaufquote ein häufig kritisierter Punkt. In unserer aktuellen Umfrage gab fast die Hälfte (45 %) der Teilnehmer an, dass für lediglich 0–10 % ihrer gemachten Anzeigen eine Rückmeldung erfolgt. Eine Rückmeldung in 11–30 % der VAs erhalten 20 % der Teilnehmer. 22,5 % der befragten Institute gaben an in mehr als 30 % der Fälle eine Rückmeldung erhalten zu haben. 12,5 % machten diesbezüglich keine Angaben.

Im Gegensatz hierzu spricht der FIU Jahresbericht 2007 von einer durchschnittlichen 45 %igen staatsanwaltschaftlichen Rückmeldungsquote (generell steigende Tendenz der Rücklaufquoten seit 2003), was den obigen Aussagen der befragten Institute widerspricht.

Abbildung 16:
Rücklaufquote der angezeigten Fälle

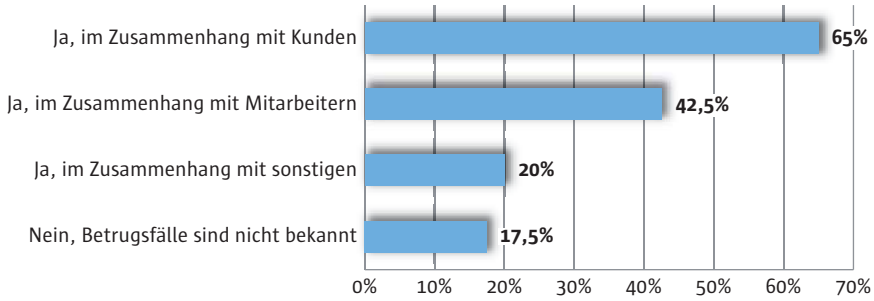


3.5 Status im Bereich der Betrugsbekämpfung

Kernaussage 10:
Neben den Kunden sehen fast die Hälfte der Institute ihre Mitarbeiter als die größte Gefahrenquelle bei Betrug.

82,5 % der befragten Institute gaben an, bis dato von Betrugsfällen betroffen gewesen zu sein. 65 % der Institute wurden bisher von Kunden und 42,5 % wurden von Mitarbeitern betrogen, wobei die Kollaboration zwischen Mitarbeitern und Kunden als Betrugsszenario ebenfalls von einzelnen Instituten genannt worden ist.

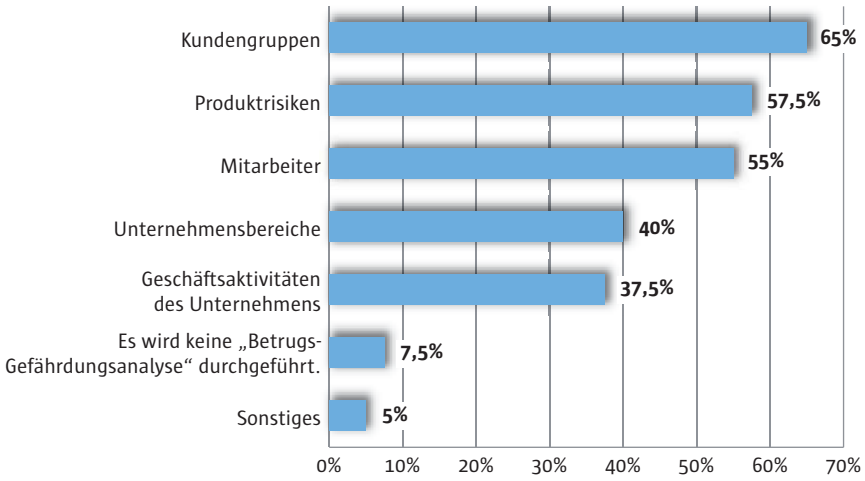
Abbildung 17:
Aufgetretene Betrugsfälle



Die Institute legen im Rahmen der Betrugs-Gefährdungsanalyse das Hauptaugenmerk auf die Überwachung der Kunden. Auf diese Weise werden soziale und lokale Gegebenheiten miteinbezogen. Neukunden, die außerhalb des eigenen Geschäftsgebietes liegen, werden dabei generell besonders sorgfältig überprüft.

Bei den Produkten werden speziell Bar-, Kredit-, Garantie- und Akkreditivgeschäfte sowie Wechsel als besonders risikoreich eingestuft. Darüber hinaus sind im Bereich der Girokonten Risiken, wie z. B. im Zusammenhang mit Kontoeröffnungs-, Überweisungs- und Lastschriftbetrug genannt worden. Bei den Mitarbeitern werden kundennahe Bereiche, wie z. B. mit Kassierern und Kundenbetreuern als besonders riskant eingestuft. Die Geschäftsaktivitäten und Branchen der Kunden werden ebenfalls in die Gefährdungsanalyse aufgenommen. Bei 7,5 % der Institute wird generell keine Gefährdungsanalyse für den Betrug durchgeführt. Bei 5 % der befragten Institute befindet sich der Prozess noch im Aufbau.

Abbildung 18:
Risikoaspekte in der „Betrugs-Gefährdungsanalyse“



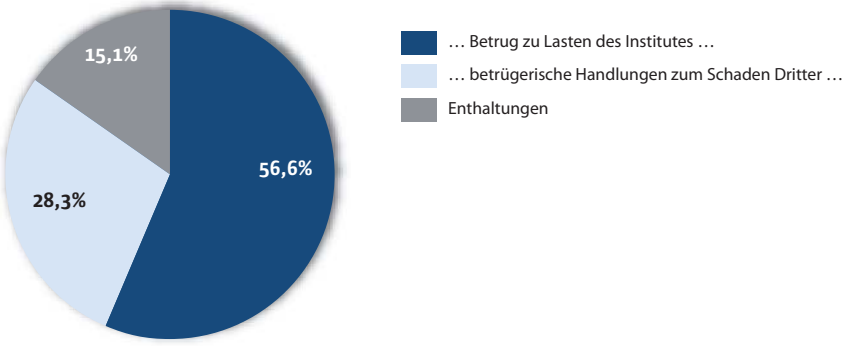
Kernaussage 11:
Trotz der Synergiemöglichkeiten sehen nur knapp die Hälfte der Befragten einen Sinn in einer kombinierten Gefährdungsanalyse von Geldwäsche und Betrugsbekämpfung.

Die BaFin (siehe RS 8/2005) sieht zwischen Geldwäsche und Betrug diverse verwandte Aspekte hinsichtlich des Risikos, der Verhaltensformen und der erforderlichen Präventionsmaßnahmen. Aufgrund dieser Überlappungen kann eine gemeinsame Gefährdungsanalyse erstellt werden, was den Instituten auch die Möglichkeit bietet Synergien zu nutzen. Lediglich 45 % der befragten Institute nutzen bzw. planen eine kombinierte Gefährdungsanalyse von Geldwäsche und Betrug. 20 % der befragten Institute haben bereits eine getrennte Lösung umgesetzt, 17,5 % planen für Betrug und Geldwäsche eine eigenständige Lösung. 10 % der Befragten wollten hierzu keine Angaben machen.

Eine getrennte Gefährdungsanalyse, wird z. T. dann durchgeführt, wenn die Institute aufgrund ihres breiten Produktportfolios eine starke organisatorische Trennung der Unternehmensbereiche haben. Eine organisatorische Trennung hat zur Folge, dass es nur bedingte Überlappungen bei den Verhaltensformen und insbesondere Maßnahmen gibt, so dass Synergien nur begrenzt zu erreichen sind. Die Synergien beschränken sich hier nur auf eine abgestimmte Systematik.

§ 25c KWG fordert interne Sicherungsmaßnahmen zur Verhinderung von betrügerischen Handlungen zu Lasten des Instituts. Ungefähr 28 % der Befragten versuchen über die gesetzlichen Anforderungen hinaus auch Betrugsfälle zu identifizieren, die zu Lasten Dritter gehen. Die Motivation zur Übererfüllung ist damit zu erklären, dass die Reputation der Bank bei Betrugsfällen zu Lasten Dritter in Gefahr gerät. Zahlreiche Banken sehen es als ihre ureigenste Pflicht, den Kunden vor entsprechenden Schäden zu schützen.

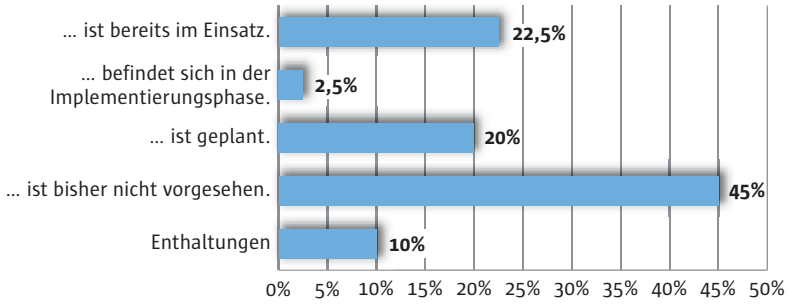
Abbildung 19:
Fokus der Betrugsprävention



Kernaussage 12:
Die befragten Institute legen zur Zeit ihren systemtechnischen Fokus primär auf den Bereich der Geldwäschebekämpfung und weniger auf die Betrugsbekämpfung.

Gemäß den rechtlichen Anforderungen bei „Internen Sicherungsmaßnahmen“ müssen betroffene Finanzdienstleister „angemessene Datenverarbeitungssysteme“ einsetzen. Aktuell scheint die Umsetzung der rechtlichen Anforderungen sich in zwei Lager zu teilen, wobei die eine Hälfte bereits IT-Tools zur Betrugsbekämpfung im Einsatz hat (22,5 %), in der Implementierung ist (2,5 %) oder plant (20 %). Bei 45 % ist ein Einsatz von IT-Tools zur Betrugsbekämpfung derzeit nicht vorgesehen. Im Vergleich dazu sind zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung bei 82,5 % entsprechende IT-Tools im Einsatz. Das zeigt, dass die Geldwäschebekämpfung momentan noch eine deutlich höhere Priorität hat.

Abbildung 20:
Verwendung von IT-Tools zur Betrugsbekämpfung



Bei den rein regelbasierenden Betrugsbekämpfungsystemen erfolgt die technische Umsetzung ähnlich der Umsetzung der Typologien im Bereich der Geldwäschebekämpfung. Dementsprechend basiert bei fast Zweidrittel (insgesamt 57 %, wovon 20 % ein Modell bereits produktiv haben, 15 % haben es in Arbeit, 22,5 % haben es geplant) der Institute die Methodik der Betrugsindizienentwicklung auf der „Geldwäsche-Gefährdungsanalyse“. Insofern haben viele Institute ihre bestehenden AML-Plattformen ausgebaut bzw. werden diese weiter ausbauen.

Viele der ursprünglich geldwäscheorientierten Systeme haben sich auch bereits in der Praxis bei der Betrugsbekämpfung bewährt, allerdings muss man im Kontext der diversen Betrugsarten berücksichtigen, dass für eine effiziente Betrugsprävention u. a. die Datenverarbeitungszeit und eine hochwertige Analytik starke Erfolgsfaktoren sind. Der typische „Geldwäscher" legt es, unseres Erachtens, auf eine langfristige, möglichst unauffällige Vertragsbeziehung an, im Verlaufe dessen er seinen Geschäften in Ruhe nachgehen kann, ohne dass er der Bank oder ihren Kunden einen direkten Schaden zufügt. Bei der Analyse der Daten kann die zeitliche Verarbeitung über Nacht stattfinden, um die Kundenhistorie (Profile) zu aktualisieren und entsprechende Abfragen ablaufen zu lassen.

Im Gegensatz zum „Geldwäscher" schlägt der „Betrüger" in den meisten Fällen einmal zu und verursacht in einem meist sehr kurzem Zeitraum einen erheblichen finanziellen Schaden. Aufgrund der zwangsläufigen Auffälligkeit durch den entstandenen Schaden, versucht sich der Betrüger dem Zugriff schnellstmöglich zu entziehen. Systemseitig stellt dies andere Anforderungen an die Analytik und auch an die zeitliche Verarbeitung, die z. T. Real-Time durchgeführt werden muss. Diverse Systeme bieten hier analytische Methodiken an, die eine höhere Qualität und schnellere Identifizierung von potenziellen Betrugsfällen zur Folge haben und somit helfen, die Betrugsverluste stark zu reduzieren.

In anbetracht des verstärkten Augenmerks der Prüfer ist eine Zunahme von Systemen zur Betrugsbekämpfung (oder Ausdehnung der bestehenden AML-Systeme) wahrscheinlich.

BearingPoint. Management & Technology Consultants

Wir helfen unseren Kunden, messbare und nachhaltige Ergebnisse zu erzielen

BearingPoint wendet sich als ein führendes Management- und Technologieberatungsunternehmen an die Forbes Global 2.000-Unternehmen sowie viele der weltweit größten öffentlichen Einrichtungen. Unsere rund 15.000 engagierten und erfahrenen Mitarbeiter unterstützen Organisationen rund um den Globus bei der Lösung ihrer dringendsten und wichtigsten Aufgaben – und das tagein, tagaus. Durch unseren kooperativen und flexiblen Ansatz helfen wir unseren Kunden, praktische, nachhaltige und messbare Ergebnisse zu erzielen, die richtigen strategischen Entscheidungen zu treffen und die passenden Lösungen umsetzen zu können.

Insbesondere in den Bereichen Risk, Compliance & Security (RCS) hat sich BearingPoint mit einem tiefgehenden Lösungsportfolio etabliert. Das ‚RCS' Lösungsportfolio ist bereits bei einer Vielzahl von Kunden im Financial Services Bereich sowohl in Deutschland als auch weltweit erfolgreich umgesetzt worden.

Weitere Informationen finden Sie auf unserer Webseite unter www.bearingpoint.de oder www.bearingpoint.com.

BearingPoint. Management & Technology Consultants

Autoren:

Stefan Schütt
Christopher Offe
Timir Choudhuri

Kontakt:

fsmarketingeurope@bearingpoint.com | +49.69.13022.1565

BearingPoint GmbH
Speicherstraße 1
60327 Frankfurt am Main – Deutschland

www.bearingpoint.de | www.bearingpoint.com

WP 0484 DE