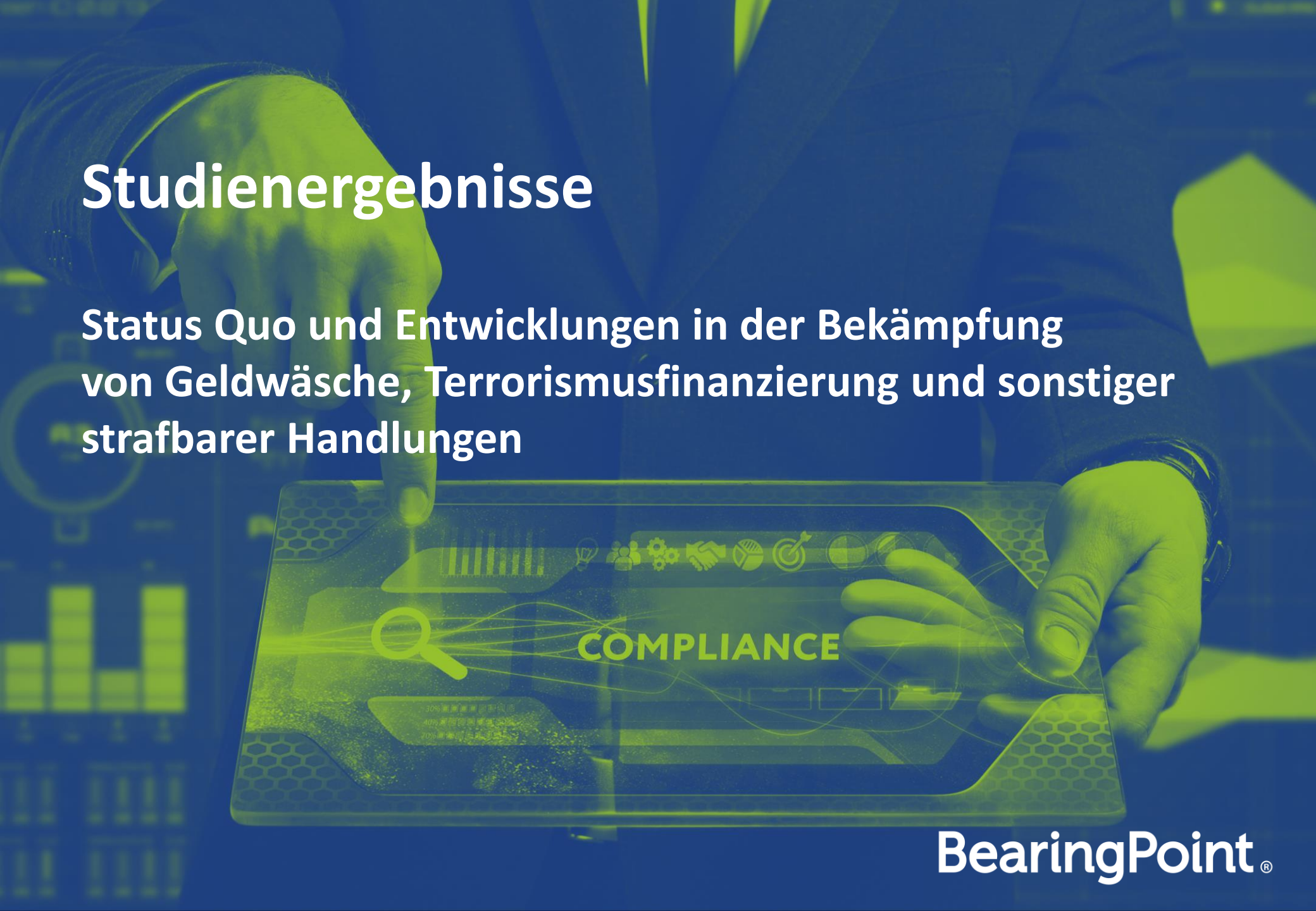
Studienergebnisse

Status Quo und Entwicklungen in der Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstiger strafbarer Handlungen



BearingPoint®

Agenda

I. **Studienvorstellung & Teilnehmerangaben**

II. Handlungsempfehlungen

III. Fragen zur Geldwäschebekämpfung - Umsetzung „GwG-Neu“

IV. Fragen zur Digitalisierung von Compliance Prozessen

V. Fragen zu „sonstigen strafbaren Handlungen“ (§ 25h KWG)/Betrugsbekämpfung/Zentrale Stelle

Studie “Status quo und Entwicklung der Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstige strafbare Handlungen”

Übersicht zur Zielsetzung, Ablauf und Hintergrund der Studie

Ziel

Die Studie soll einen …

- allgemeinen und aktuellen Überblick über die angewandte Marktpraxis geben.
- Beitrag zur sinnvollen Gestaltung von Maßnahmen zur Bekämpfung der Geldwäsche, Terrorismusfinanzierung und Betrug leisten.

Hintergrund

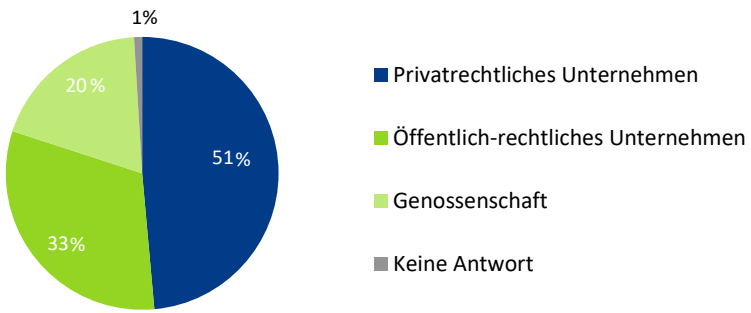
- BearingPoint publiziert seit 2005 in regelmäßigen Abständen Studien zum Thema Geldwäsche- und Betrugsbekämpfung. Unsere Studien haben sich mittlerweile bei vielen Banken als wertvolle Übersicht zur Marktpraxis entwickelt.
- In 2017 erfolgt die 5. Neuauflage mit neuen regulatorischen Entwicklungen, wie z.B. "GwG-Neu", Auswirkungen der Digitalisierung auf Compliance-Risiken, etc., die beleuchtet werden sollen.

Vorgehen, Inhalt und Zeitraum der Durchführung

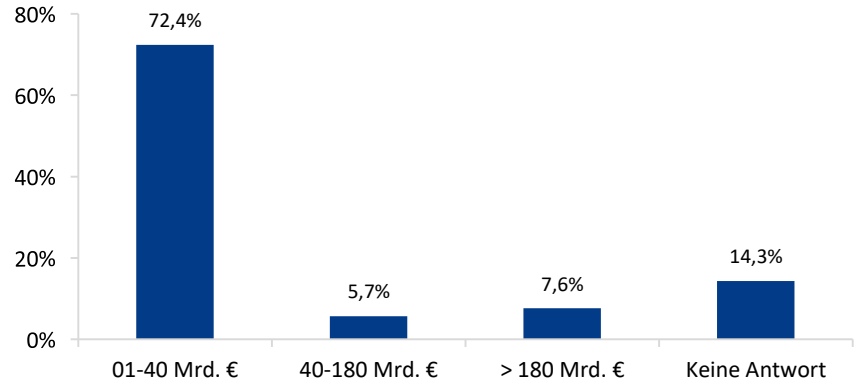
- An der vorliegenden Studie haben über 100 Kreditinstitute aus dem privaten, öffentlich-rechtlichen und genossenschaftlichen Sektor teilgenommen, womit der deutsche Bankenmarkt repräsentativ abgebildet wird.
- Die Teilnehmerwerbung erfolgte im Zeitraum zwischen August 2016 und Februar 2017.
- Die Umfrage erfolgte auf Basis eines Online-Fragebogens mit Fragen zu aktuellen Entwicklungen im Bereich der Geldwäsche-bekämpfung, Terrorismusfinanzierung, Betrugsbekämpfung und Digitalisierung in Compliance.
- Die Teilnahme wurde streng vertraulich behandelt und die Antworten waren anonym.

Eine der größten Studien, mit insgesamt 105 Teilnehmern, zum Status Quo und Trends im Bereich der Geldwäsche-, Terrorismusfinanzierung- und Betrugsbekämpfung

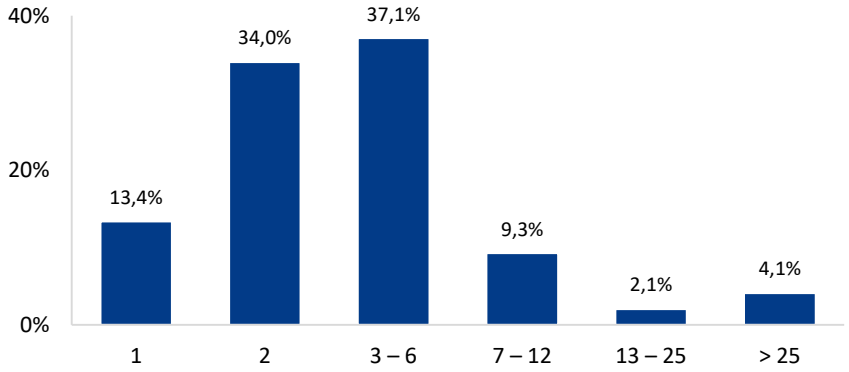
Bankensektoren der Teilnehmer



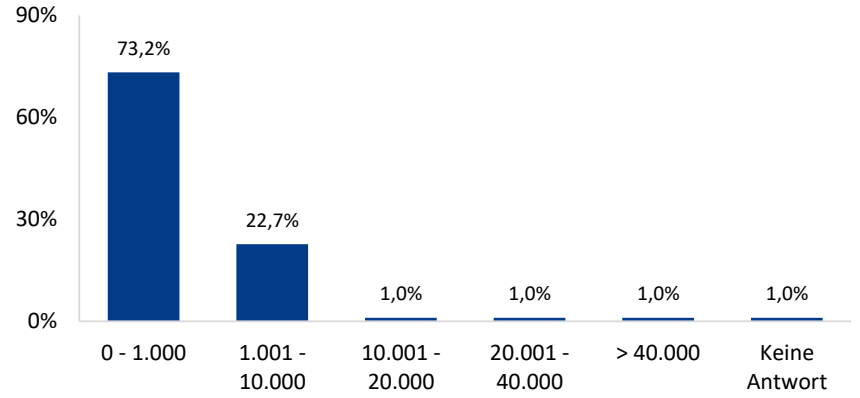
Wie hoch ist Ihre Bilanzsumme (€ Mrd.)?



Wie viele Mitarbeiter arbeiten im Bereich Geldwäsche-, Betrugs-, Terrorismusbekämpfung (Deutschland)?



Wie viele Mitarbeiter hat Ihr Institut in Deutschland?



BearingPoint

Agenda

I. Studienvorstellung & Teilnehmerangaben

II. Handlungsempfehlungen

III. Fragen zur Geldwäschebekämpfung - Umsetzung „GwG-Neu“

IV. Fragen zur Digitalisierung von Compliance Prozessen

V. Fragen zu „sonstigen strafbaren Handlungen“ (§ 25h KWG)/Betrugsbekämpfung/Zentrale Stelle

Die wichtigsten Kernaussagen und Handlungsempfehlungen der Studie auf einem Blick (1/2)

Im Fokus steht das „GwG-Neu“ und die „Digitalisierung von Compliance Prozessen“

Kernaussagen für die Umsetzung „GwG-Neu“

1. Hauptantriebsfaktoren der Geldwäschebekämpfung sind die Minimierung des Reputations-, Bußgeld- und Sanktionsrisikos.
2. Ein Großteil sieht eine Verbesserung der Gesetze im Kampf gegen die Geldwäsche. Gleichzeitig hat sich die Wertschätzung und Akzeptanz für Geldwäschebekämpfung verdoppelt.
3. Die Mehrheit schätzt die erforderlichen Aufwände für die „GwG-Neu“-Umsetzung mittel bis hoch ein. Des Weiteren werden zunehmende Aufwände bei neuen Geschäfts-modellen gesehen, sodass regulatorische Anforderungen eine zunehmende strategische Rolle spielen.
4. Die Einführung des zentralen Registers wird als sinnvoll gesehen, jedoch wird dessen Verlässlichkeit angezweifelt.
5. Ein erhöhtes Risiko für Banken entsteht durch das unzureichende Einbinden des Bereichs Geldwäschebekämpfung bei der Votumsvergabe bzgl. Hochrisikokunden.
6. Hinsichtlich des Risikomanagements findet eine zunehmende Vernetzung insbesondere mit der IT-Sicherheit sowie Datenschutz statt.
7. Primär werden standardisierte Aktivitäten und fachliche Niedrigrisiken ausgelagert. Ein Durchschnitt der Teilnehmer sieht weiteres Auslagerungspotential, empfindet aber den Datenschutz als Restriktion.

Handlungsempfehlungen für die Umsetzung „GwG-Neu“

- Unter Beachtung des Reputationsrisikos und der zunehmenden internen Wertschätzung müssen Banken weiterhin die Geldwäschebekämpfung ernsthaft vorantreiben.
- Die unterschiedlichen Aufwandsbereiche (IT-Systeme, Prozesse, Dokumentation, etc.) machen es unerlässlich, dass die Mitarbeiter für eine effiziente Umsetzung der vielseitigen Anforderungen über ein breitgestreutes fachliches und technisches Wissen verfügen müssen.
- Banken sollten verstärkt dazu übergehen, die Potentiale bei der Auslagerung zur Kostenreduzierung weiter auszubauen. Hierbei sollten auch potentielle Datenschutzrestriktionen Hinterfragt werden.
- Durch die stärkere Einbindung des Geldwäschebereichs bei Hochrisikokunden sowie eine stärkere prozessuale Vernetzung hinsichtlich Steuerthemen können Banken ihr Risikoprofil verbessern.

Die wichtigsten Kernaussagen und Handlungsempfehlungen der Studie auf einem Blick (2/2)

Im Fokus steht das „GwG-Neu“ und die „Digitalisierung von Compliance Prozessen“

Kernaussagen zur „Digitalisierung von Compliance Prozessen“

1. Die größten Digitalisierungspotentiale liegen primär im Bereich Sorgfaltspflichten, Fallbearbeitung und automatisierte Reports für Risikoanalysen.
2. Die neuen Legitimationstechnologien werden positiv aufgenommen, jedoch wird die Legitimation vor Ort den neuen Verfahren vorgezogen.
3. Instant Payments wird von einem Großteil der Banken noch nicht verfolgt. Eine GWG-konforme Prüfung wird als Herausforderung gesehen.
4. Die Mehrheit verwendet keine Blockchain-Technologie, in welcher nur eine Minderheit ein erhöhtes Geldwäsche- oder sonstiges Risiko sieht.
5. Bei der Digitalisierung im Zusammenhang mit PSD 2 werden insbesondere die Bereiche Datensicherheit und Betrugsbekämpfung als die größten Risiken eingeschätzt.
6. Die Digitalisierung birgt bei einer Mehrheit ein erhöhtes Risiko im Zusammenhang mit Geldwäsche und betrügerischen Handlungen.
7. Im Rahmen der Digitalisierung sieht die Hälfte der Banken große Prozess-optimierungspotentiale in der elektronischen Verdachtsfallübermittlung an die FIU.

Handlungsempfehlungen zur „Digitalisierung von Compliance Prozessen“

- Banken sollten verstärkt auf die Möglichkeiten der Digitalisierung insbesondere im Bereich der Sorgfaltspflichten, Fallbearbeitung und automatisierte Risikoanalysen zurückgreifen. Neue Technologien, wie z.B. Robotics und AI-Lösungen können helfen, die Aufwände zu reduzieren und Risiken besser einschätzen zu können.
- Banken müssen sich verstärkt mit neuen Technologien, wie z.B. Blockchain, Instant Payments, etc. auseinandersetzen, damit Chancen für interne Prozessoptimierungen genutzt und Compliance-Risiken frühzeitig z.B. im Rahmen des NPM-Prozesses identifiziert werden können.

Kernaussagen zu „Sonstige strafbare Handlungen, Betrugsbekämpfung und Zentrale Stelle“

1. Es besteht immer noch ein schwacher Rücklauf seitens der FIU.
2. Der überwiegende Teil der Betrugsfälle wird durch Mitarbeiterhinweise aufgedeckt. Allerdings werden oftmals Schadensfälle erst nach Eintritt identifiziert.

Handlungsempfehlungen „Sonstige strafbare Handlungen, Betrugsbekämpfung und Zentrale Stelle“

- Zur Vermeidung von Verlusten sollten sich die Sicherungsmaßnahmen auf Mitarbeiterschulungen und effizientere IT-System zur Betrugsbekämpfung fokussieren.

Agenda

I. Studienvorstellung & Teilnehmerangaben

II. Handlungsempfehlungen

III. Fragen zur Geldwäschebekämpfung - Umsetzung „GwG-Neu“

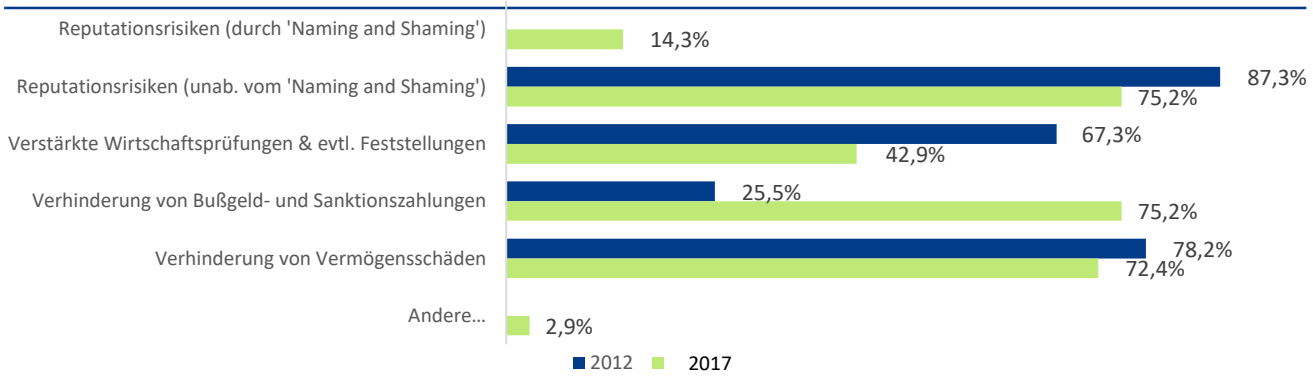
IV. Fragen zur Digitalisierung von Compliance Prozessen

V. Fragen zu „sonstigen strafbaren Handlungen“ (§ 25h KWG)/Betrugsbekämpfung/Zentrale Stelle

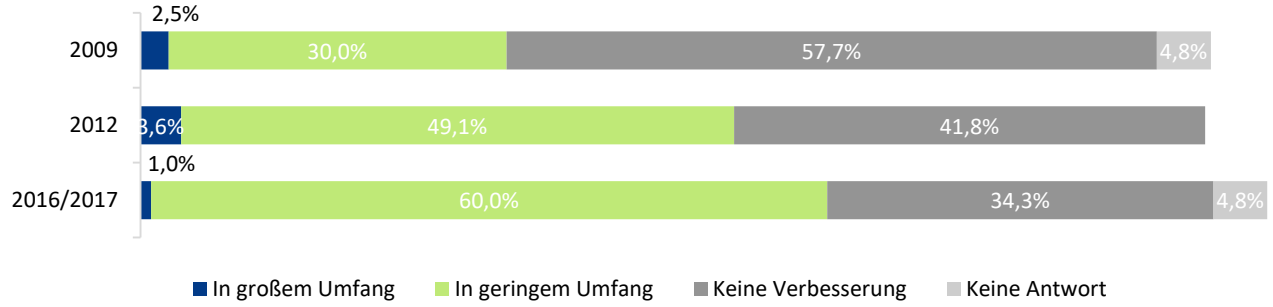
Der Schutz der Reputation bleibt nach wie vor einer der Haupttreiber für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung

- Bereits in der Studie von 2012 wurden Reputationsrisiken als wichtigster Treiber zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Betrug identifiziert.
- Ein weiterer wesentlicher Treiber zur Umsetzung des „GwG-Neu“ sind die neuen „Bußgeld- und Sanktionszahlungen“ (bis zu 10% des Gesamtumsatzes) und „Vermögensschäden“.

Was sind die Einflussfaktoren für Ihr Institut zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und Betrug?



In welchem Umfang, schätzen Sie, führt das „GwG-Neu“ zu einer Verbesserung der Geldwäschebekämpfung?

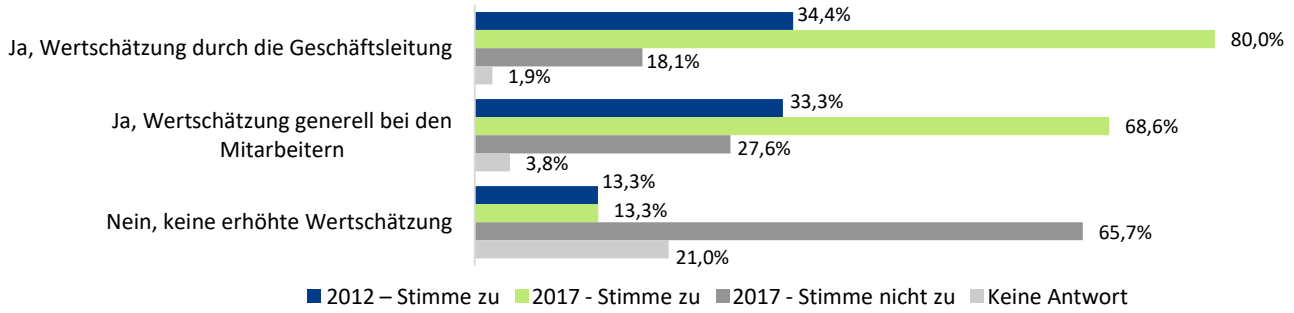


- Nach wie vor werden die neuen Richtlinien mit Skepsis bewertet, jedoch werden seit 2009 vermehrt Verbesserungen (z.B. das wB-Register) wahrgenommen.
- In 2017 schätzen 60%, dass die neuen Gesetze zu einer Verbesserung im geringem Umfang führen, während in 2009 zum größten Teil keine Verbesserung gesehen wurde.

BearingPoint

Zunehmende Wertschätzung für die Terrorismusfinanzierung, Geldwäsche- und Betrugsbekämpfung

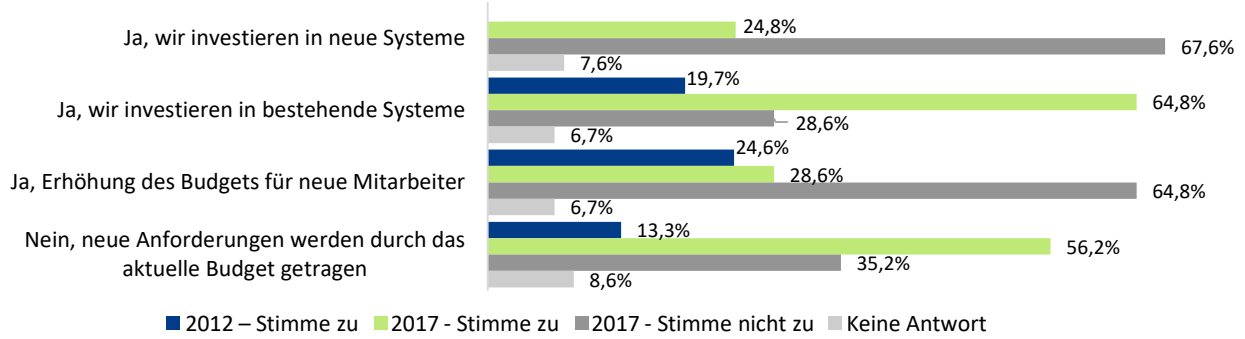
Hat es eine Aufwertung (z.B. größere Akzeptanz, stärkere Prozesseinbindung, etc.) über die letzten 4 Jahre Geldwäschebekämpfung/Terrorismusfinanzierung innerhalb der Bank gegeben?



- Seit 2012 hat sich die Wertschätzung für Geldwäschebekämpfung durch die Geschäftsleitung (>75%) und den Mitarbeitern (> 65%) verdoppelt.

- Die zunehmenden Anforderungen müssen zum Großteil vom bestehenden Budgets getragen werden (> 55%).
- Es wird eher in bestehende Systeme und in neue Mitarbeiter als in neue Systeme investiert.

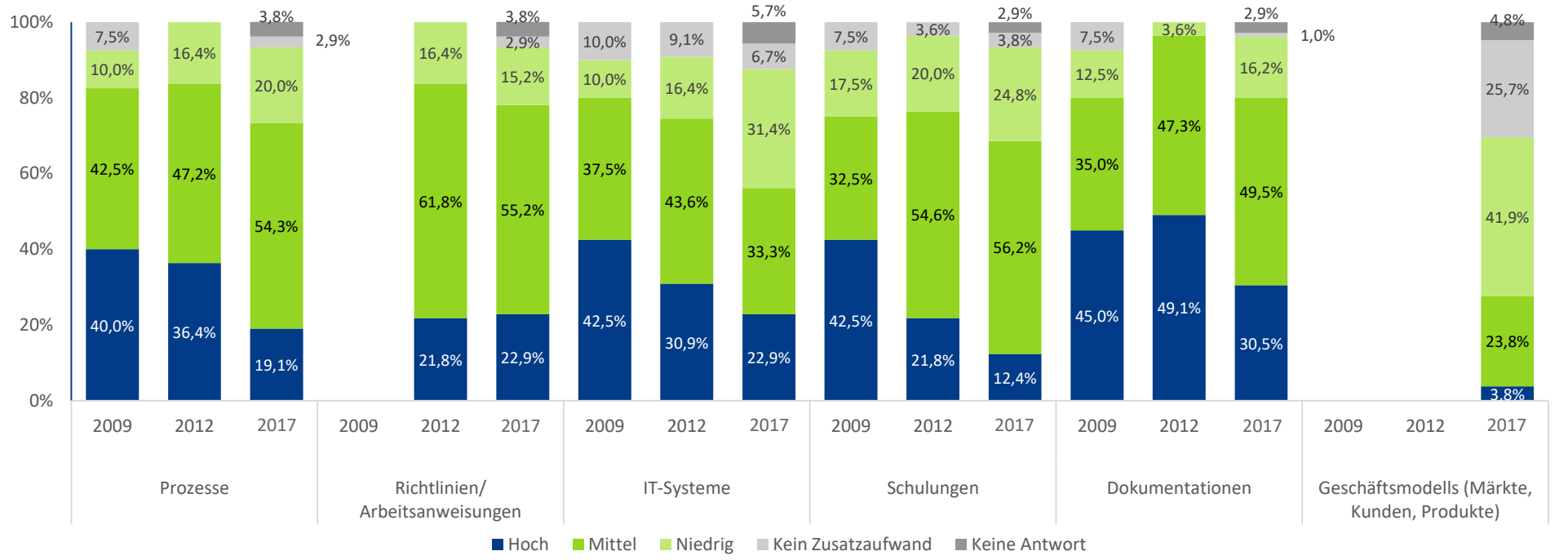
Hat es eine Erhöhung des Budgets (z.B. größere Akzeptanz, stärkere Prozesseinbindung, etc.) über die letzten 4 Jahre für Geldwäschebekämpfung/Terrorismusfinanzierung innerhalb der Bank gegeben?



BearingPoint

Nach wie vor sieht ein Großteil der Banken durch das „GwG-Neu“ mittel bis hohe Aufwände bei der Umsetzung der neuen gesetzlichen Anforderungen

Welche der nachfolgenden Umsetzungsbereiche, bedingt durch das „GwG-Neu“, werden die größten Aufwände nach sich ziehen (inkl. Aufwandskategorisierung)?

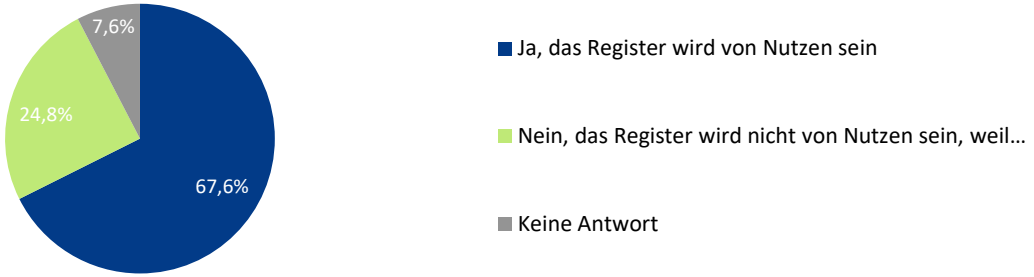


- Zwischen 50-70% der Teilnehmer schätzen die Gesamtaufwände für die Umsetzung der neuen Anforderungen mittel bis hoch ein.
- Die Einschätzung der „hohen“ Aufwände nimmt über fast alle Bereiche hinweg ab, wohingegen die „mittleren“ Aufwände zugenommen haben.
- Tendenziell gehen die Aufwände seit 2009 langsam zurück.
- Bei rund einem Viertel der Banken muss das Geschäftsmodell regulatorische Anforderungen berücksichtigen, sodass die Geldwäschebekämpfung eine zunehmend strategische Rolle einnimmt.

BearingPoint

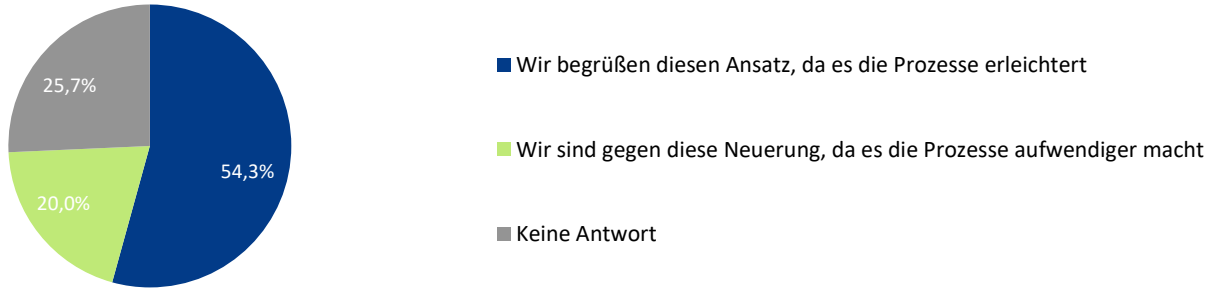
Fast zwei Drittel der Teilnehmer begrüßen die Einführung des Zentralregisters und die Abschaffung der White-List im Rahmen des „GwG – Neu“

Denken Sie, dass das im Rahmen der "GwG-Neu" geplante zentrale Register für wirtschaftlich Berechtigte für die Erfüllung der Sorgfaltspflichten von Nutzen sein wird?



- 67% der Befragten halten die Einführung des zentralen Registers für wirtschaftlich Berechtigte (Transparenzregister) für sinnvoll, obwohl dessen Verlässlichkeit von den Teilnehmern angezweifelt wird.
- In den Freitextfeldern wurde Folgendes als Gegenargumente genannt:
  - Es geniest keinen öffentlichen Glauben und
  - der Verpflichtete bleibt für die korrekte Datenerhebung und den Mehraufwand verantwortlich.

Was halten Sie von der Abschaffung der White-List für Länder und der Etablierung einer Black-List für Hochrisikoländer?

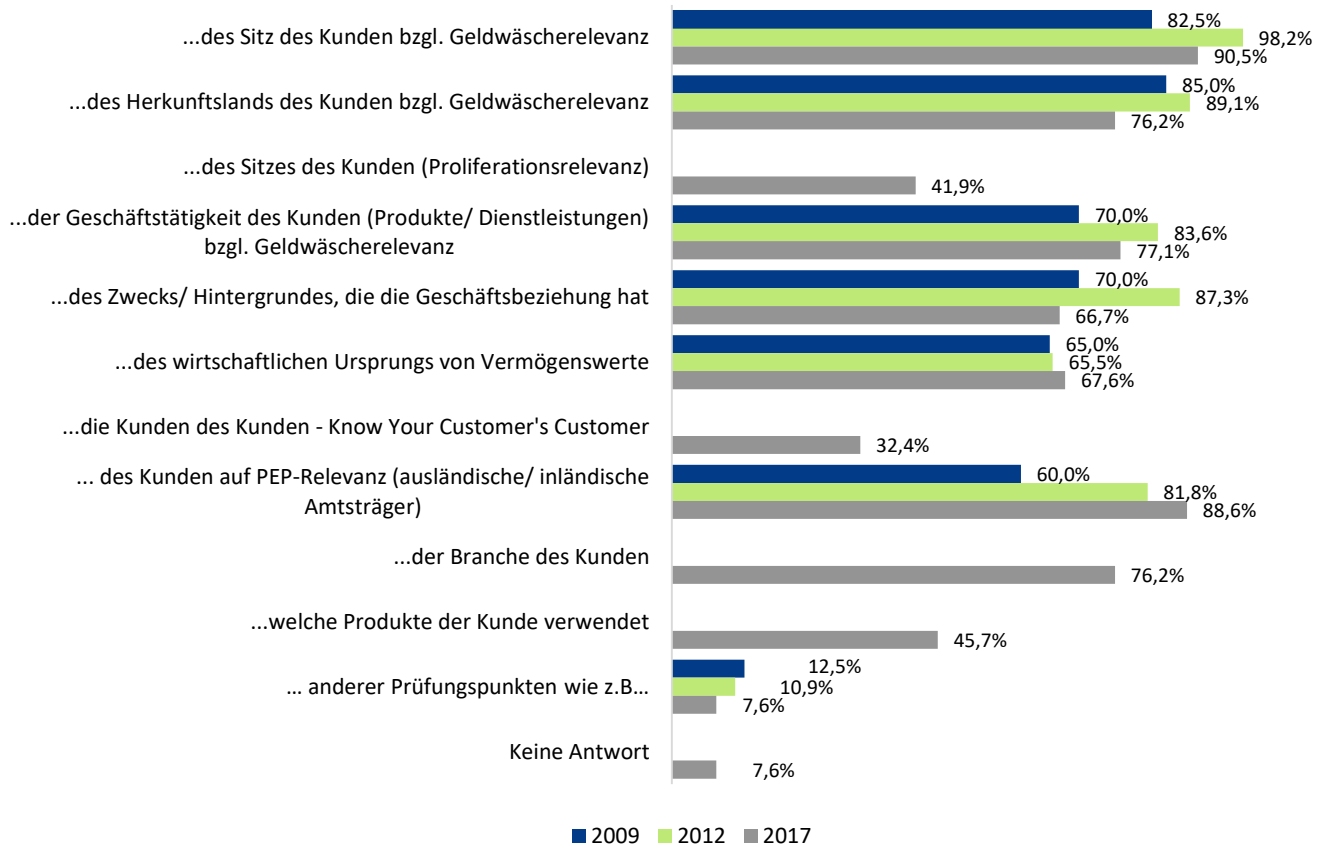


- 54% der Befragten empfinden die Etablierung einer Black-List für Hochrisikoländer durch die Delegierte Verordnung (EU) 2016/1675 für KYC-Prozesse erleichternd.
- Die Black-List enthält jedoch keine Angaben über Länder, die als Steueroasen eingeordnet werden. Aus diesem Grund sollte jedes Kreditinstitut zusätzlich eigene Länder-Bewertungskriterien hinsichtlich Steuerflucht ableiten.

BearingPoint

Der Prozess der Kundenrisikobewertung (KYC) für den risikobasierten Ansatz gemäß des „GwG – Neu“ ist etablierte Marktpraxis

Die in unserem Hause durchgeführte Kundenrisikobewertung umfasst die Prüfung…

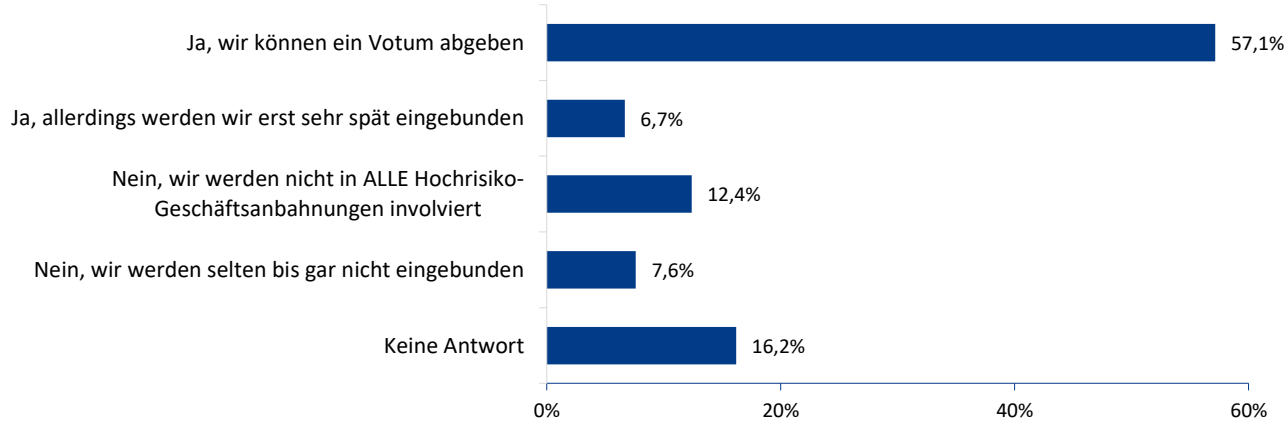


- Das Risikomodell zur Kundenbewertung wird von ca. 95% der Teilnehmer angewandt.
- Entgegen dem RS 05/2008 der BaFin werden die Produkte bei weniger als 50% der Teilnehmer in die Bewertung aufgenommen.
- Länderinformationen bilden den Schwerpunkt der Risikobewertung.
- Weitere Aspekte, die in die Risikomodelle individuell mit aufgenommen werden, sind u.a.:
  - Kundengruppe, Identifizierungsart;
  - Publizitätsanforderungen an die Rechtsform des Kunden, Einhaltung von Standards (z.B. Umwelt-vorschriften), Abwesenheit von Vorverurteilungen;
  - Herkunft des hinterlegten Referenzkontos;
  - Dauer der Geschäftsbeziehung und
  - Negative Informationen.

BearingPoint

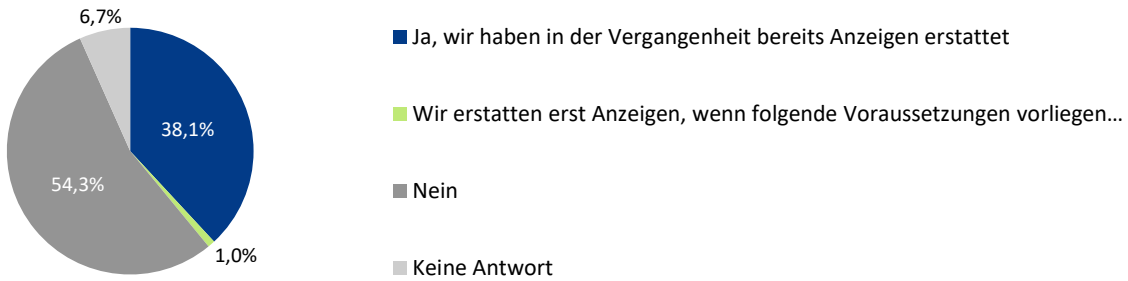
Bei Hochrisikokunden werden ca. 25% der Teilnehmer nur unzureichend in den Votumsprozess eingebunden, was ein erhöhtes Risiko für die Bank darstellt

Können Sie im Rahmen der Geschäftsanbahnung ein Votum für ALLE Hochrisiko-Geschäftsbeziehungen abgeben?



- 57% der Teilnehmer können ein uneingeschränktes Votum bei Hochrisikogeschäftsbeziehungen abgeben.
- 20% der teilnehmenden Banken kann beim Abschluss von Geschäftsbeziehungen nur in Teilen ein eingeschränktes Votum abgeben, wodurch ggf. zusätzliche Risiken eingegangen werden.
- Mehr als 25% der Geldwäschebeauftragten haben keine all umfassende Sicht auf die Hochrisikokunden innerhalb ihres Hauses.

Mussten Sie im Rahmen der Erfüllung von Sorgfaltspflichten bereits eine Anzeige (§ 43 Abs. 1 TP 3 GWG) aufgrund eines Verstoß gegen die Offenlegungspflicht gemäß § 11 Abs. 6 S. 2 GWG erstatten?

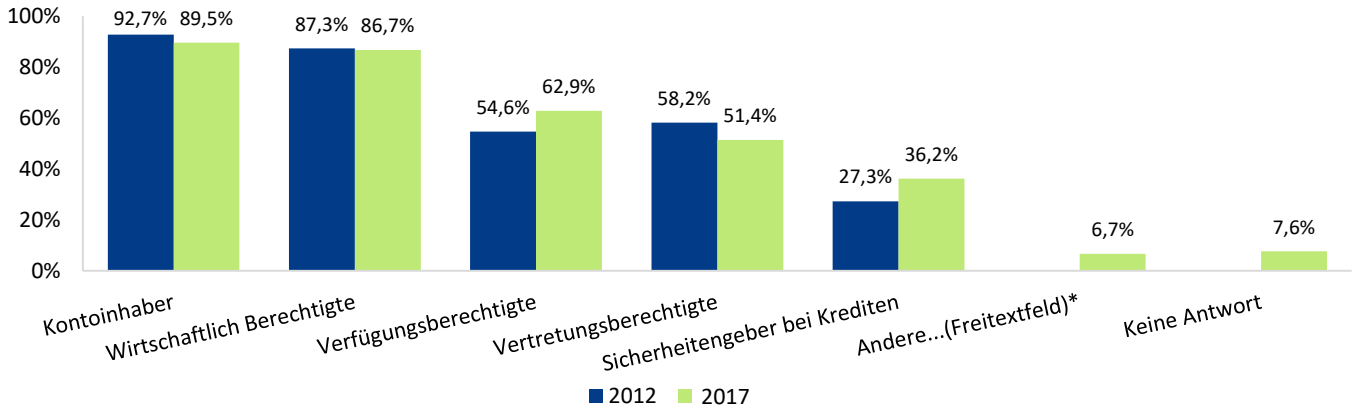


- Ein Drittel der Teilnehmer setzen die gesetzlich geforderten Sorgfalts-pflichten auch unter Erstattung einer Anzeige durch.
- Bei rund 55% der teilnehmenden Institute kommen die Kunden ihren Offenlegungsspflichten nach.

BearingPoint

Fast alle Banken kommen den gesetzlichen Anforderungen der PEP-Prüfung nach, allerdings bleiben einige Risikobereiche ungeprüft

Wer wird bei den Kontoverbindungen Ihres Institutes auf PEP geprüft?



- Ähnlich wie in der Studie von 2012, kommen Banken den gesetzlichen Sorgfaltspflichten hinsichtlich der PEPs nach.
- Weitere Vertragspartner (z.B. Sicherheitengeber) werden zunehmend freiwillig geprüft, was allerdings nur für eine Minderheit zutrifft.

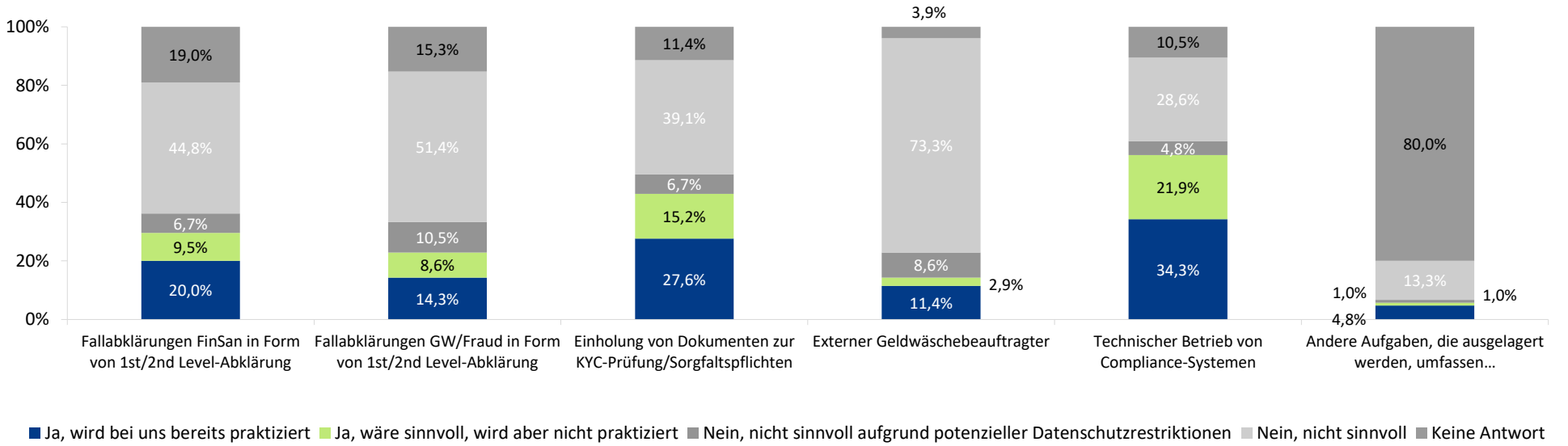
Wie schätzen Sie im Rahmen der "GwG-Neu" die Aufwände für die Umsetzung der PEP-Konkretisierung für Ihre KYC-Prozesse ein?

- Nur wenige Teilnehmer halten die Umsetzung der PEP-Konkretisierung nach der 4. EU-Geldwäscherichtlinie für sehr aufwendig.

BearingPoint

Fast 43% der Teilnehmer sehen Auslagerungspotential im Bereich der KYC-Prüfung/Sorgfaltspflichten oder haben diese bereits ausgelagert

Erachten Sie die Auslagerung von Tätigkeiten im Zusammenhang mit Geldwäsche- (GW), Terrorismusfinanzierungs-, Betrugsprävention (Fraud) und Embargo/Finanz Sanktionen (FinSan) für die nachstehenden Aufgaben als sinnvoll?

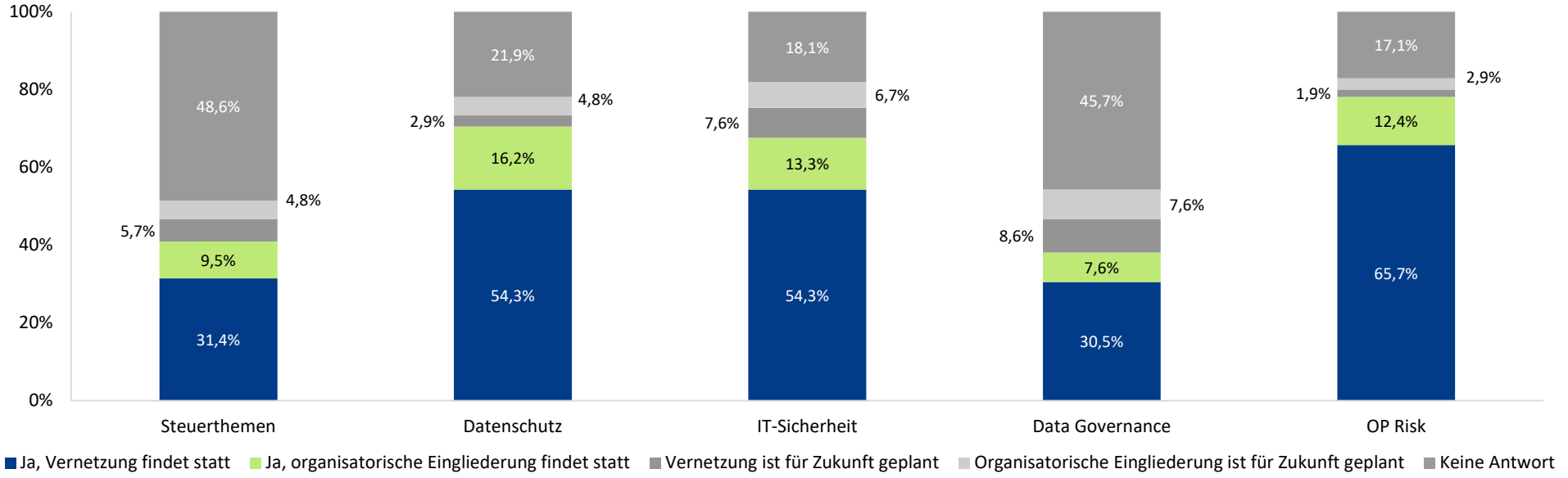


- In Bereichen der standardisierten Bearbeitung (Fallbearbeitung, KYC) halten fast 25-45% der Teilnehmer internes/externes Sourcing/Auslagerung für sinnvoll.
- Die teilnehmenden Institute lagern am häufigsten den technischen Betrieb verschiedener Compliance-Systeme aus.
- Die Auslagerung größerer Aufgabenbereiche (z.B. externer Geldwäschebeauftragter) wird teilweise bei >70% als nicht sinnvoll eingestuft: "Das Problem der Auslagerung ist, dass sich Externe nicht mit dem Unternehmen identifizieren und ausschließlich entsprechend der vereinbarten Leistungsscheine arbeiten. Darüber hinaus gehende Auffälligkeiten werden nicht oder nur unzureichend an das Institut zurückgemeldet, sodass eine Weiterentwicklung der Präventionsarbeit nur schleppend erfolgt“ (Feedback eines Teilnehmers).

BearingPoint

Banken favorisieren eine Verschmelzung des unternehmensweiten Risikomanagements und sind hierzu bereits gut vernetzt

In Anbetracht der Themen, wie z.B. „Panama Papers“, der geforderten „Risikokultur“ gemäß der MaRisk und unternehmensweiten Risikomanagements, findet in Ihrer Organisation eine stärkere Vernetzung oder sogar organisatorische Zusammenführung mit der Geldwäschebekämpfung/Zentralen Stelle mit den folgenden Themen statt?

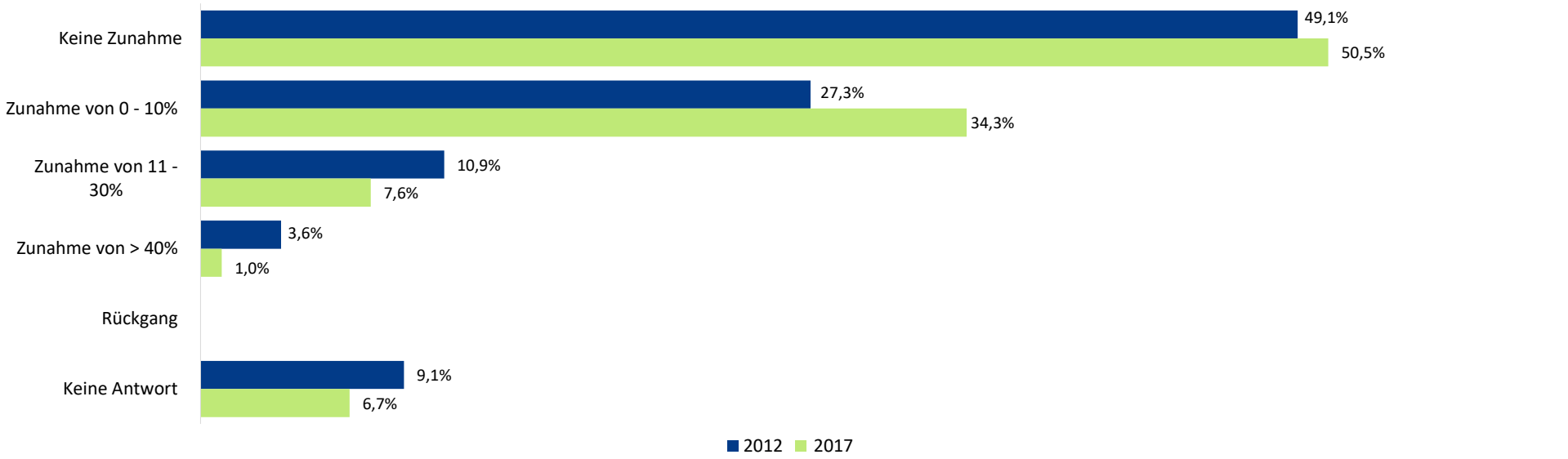


- Bei ca. 54-66% findet eine Vernetzung in den Kernbereichen Datenschutz, IT-Sicherheit und OP-Risk statt.
- Eine organisatorische Zusammenführung dieser Bereichen findet bei ca. 8-16% der teilnehmenden Institute statt.
- Keine starke Berücksichtigung bei Banken findet Data Governance und Steuerthemen mit negativen Implikationen auf die Risikosituation.
- Einige Teilnehmer sehen einen Interessenskonflikt zwischen Datenschutz und Geldwäschebekämpfung (z.B. bei der Einführung des Zentralregisters für wirtschaftlich Berechtigte), wodurch auch die Komplexität einer gesetzeskonformen Risikoanalyse zunehmen kann (siehe Datenschutzgrundverordnung).

BearingPoint

Eine Erhöhung der Verdachtsfallmeldung wird von der Hälfte der Teilnehmer auch für die Zukunft erwartet

Wie wird sich Ihrer Einschätzung nach die Anzahl der Verdachtsmeldungen nach § 43 GWG u.a. im Hinblick auf die Umsetzung der "GwG-Neu" für Ihre Bank entwickeln?

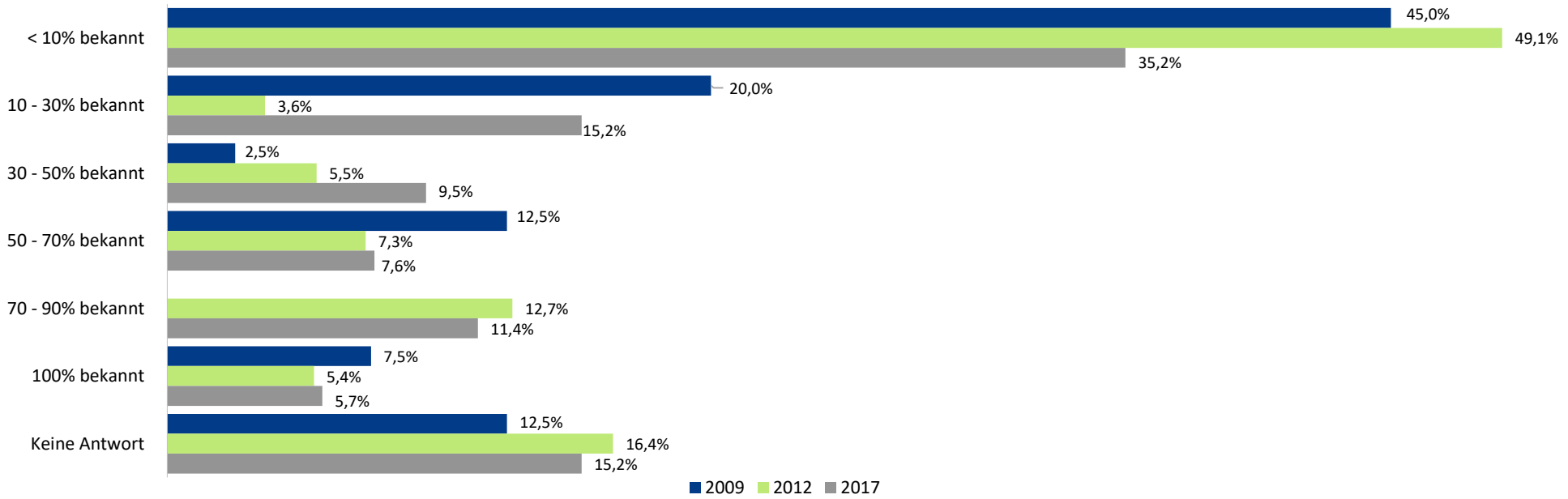


- Fast die Hälfte der Teilnehmer erwarten weiterhin eine Zunahme der Verdachtsmeldungen (tatsächliche Anzahl an eingereichten Verdachtsfallmeldungen: 2014 = 24.054; 2015 = 29.108; 2016 = 40.690), wobei lediglich eine Zunahme in geringerem Umfang im Vergleich zu 2012 erwartet wurde.

BearingPoint

Rückläufe seitens der FIU zu Verdachtsmeldungen sind nach wie vor gering

In wie vielen Fällen ist Ihnen der Ausgang von Ermittlungen aufgrund Ihrer Verdachtsmeldung bekannt?

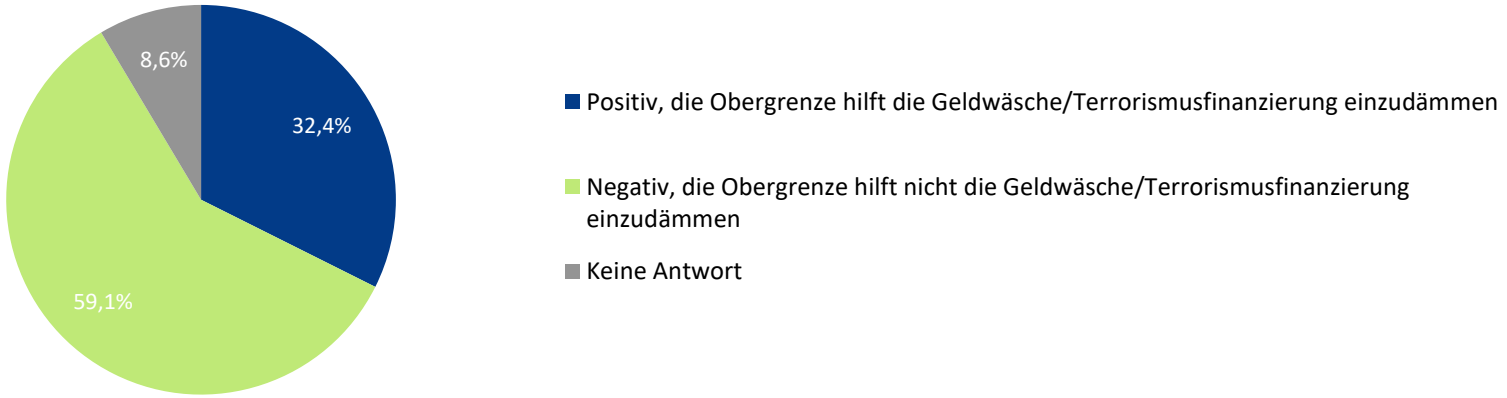


- Ein Drittel aller Teilnehmer erhält weniger als 10% Rückmeldung seitens der FIU auf die von ihnen eingereichten Verdachtsmeldungen, sodass die Finanzinstitute mit Schwierigkeiten in der Anpassung ihrer Prozesse und Systeme konfrontiert sind.
- Es konnte eine Verschlechterung der getätigten Rückläufe seitens der FIU zwischen 2012 und 2017 beobachtet werden.

BearingPoint

Bargeldobergrenzen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung wird von mehr als der Hälfte der Teilnehmer angezweifelt

Die Bundesregierung erwägt eine Obergrenze für Bargeldzahlungen (z.B. 5.000€). Wie schätzen Sie den Nutzen dieser Maßnahme im Hinblick auf eine Verbesserung der Geldwäsche- und Terrorismusfinanzierungsbekämpfung ein?



- Fast 60% der Teilnehmenden finden eine Bargeldobergrenze zur Eindämmung von Geldwäsche- und Terrorismusfinanzierung als nicht hilfreich.

BearingPoint

Agenda

I. Studienvorstellung & Teilnehmerangaben

II. Handlungsempfehlungen

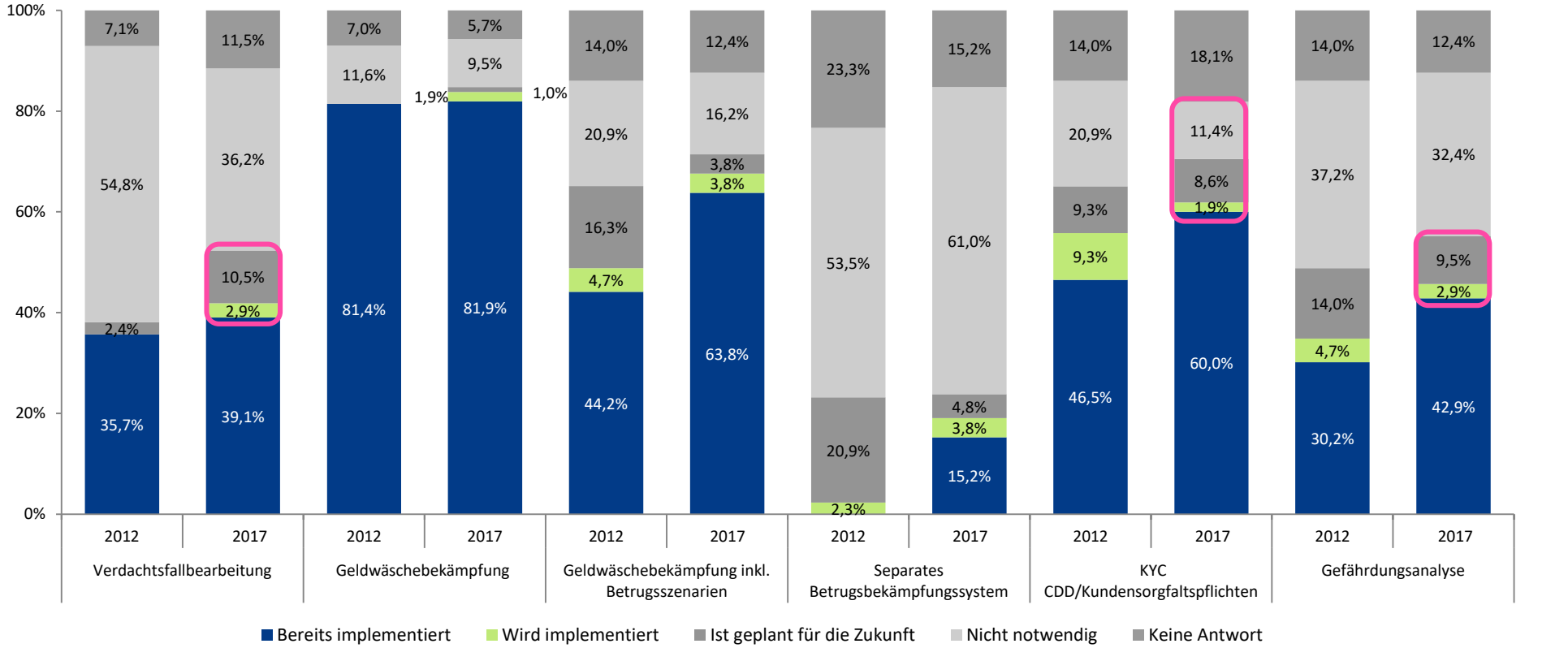
III. Fragen zur Geldwäschebekämpfung - Umsetzung „GwG-Neu“

IV. Fragen zur Digitalisierung von Compliance Prozessen

V. Fragen zu „sonstigen strafbaren Handlungen“ (§ 25h KWG)/Betrugsbekämpfung/Zentrale Stelle

Banken planen ihre Prozesse im Bereich der Fallbearbeitung, Sorgfaltspflichten und Risikoanalyse zunehmend zu digitalisieren (1/2)

Was sind die Hauptsysteme und Listen, die Sie in der Geldwäschebekämpfung/Zentralstelle verwenden?

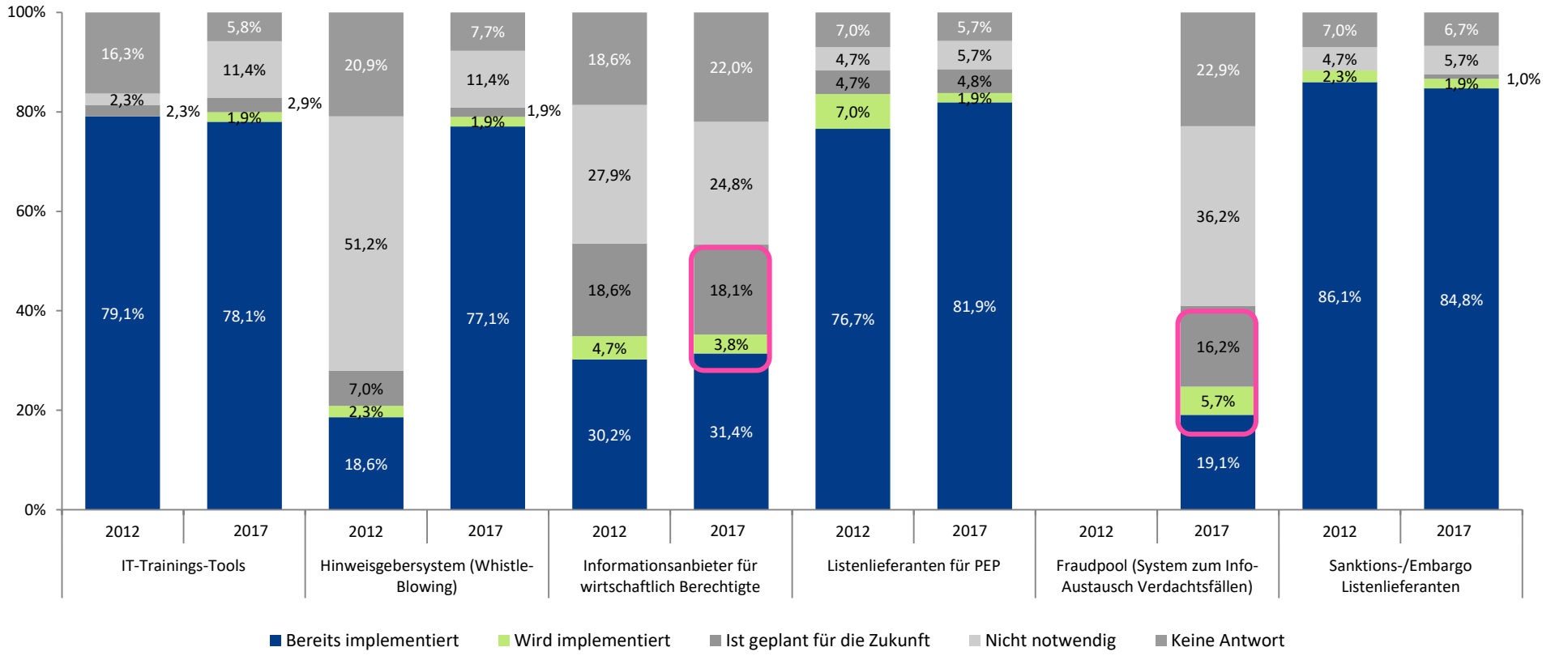


- Die Aussagen hinsichtlich „für die Zukunft“ Geplantes in 2012 und nun bis 2017 „implementiert“ wurde, sind relativ präzise.
- Zukünftig werden verstärkt Prozesse im Bereich Verdachtsfallbearbeitung, Kundensorgfaltspflichten und Risikoanalyse digitalisiert, um neue bzw. bestehende Systeme auf- bzw. auszubauen.
- Die maschinelle Betrugsbekämpfung hat eine geringe Priorität bei den Banken.

BearingPoint

Banken planen ihre Prozesse im Bereich der Fallbearbeitung, Sorgfaltspflichten und Risikoanalyse zunehmend zu digitalisieren (2/2)

Was sind die Hauptsysteme und Listen, die Sie in der Geldwäschebekämpfung/Zentralstelle verwenden?

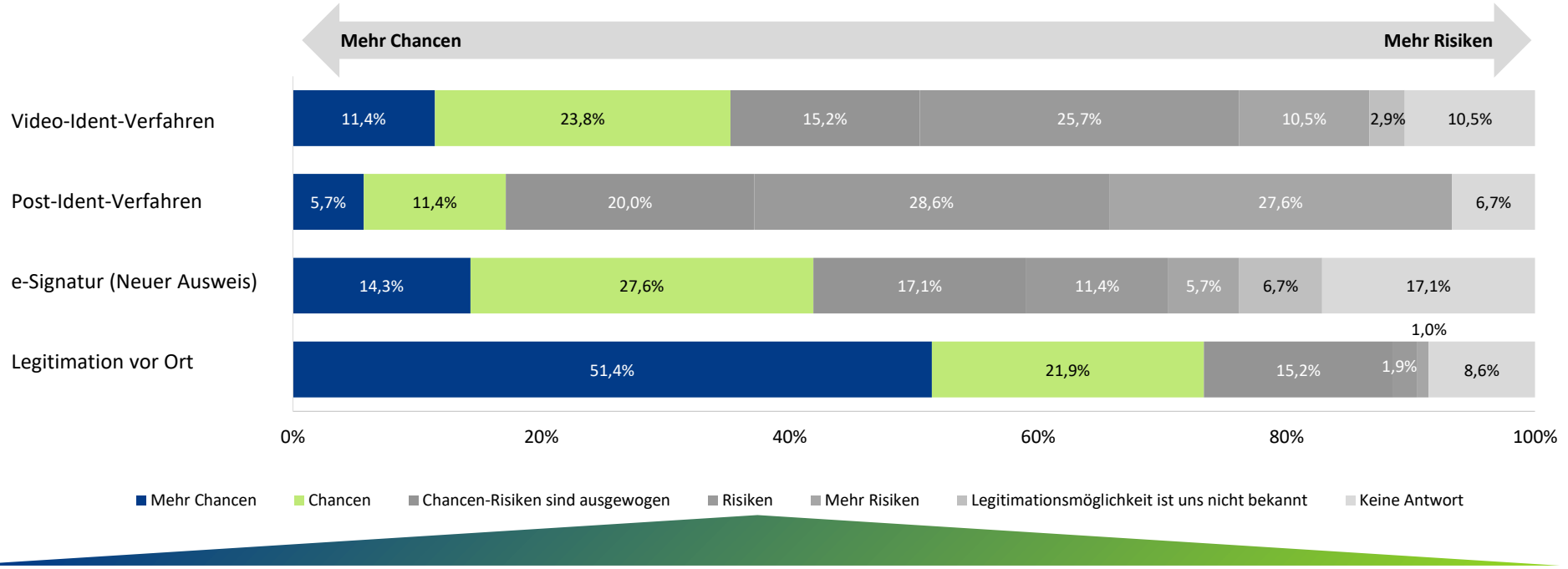


- IT-Trainings-Tools, Sanktions-/Embargolistenlieferanten und Listenlieferanten für PEPs wurden zum größten Teil bereits 2012 implementiert und weisen daher ein geringes Potential für eine zukünftige Implementierung auf.
- Im Gegensatz dazu konnten Whistle-Blowing-Systeme von 2012 bis 2017 einen starken Zuwachs in der Implementierung verzeichnen. Aus diesem Grund hatten in 2017 drei Viertel aller Studienteilnehmer solche Systeme bereits implementiert, was u.a. durch §25a KWG veranlasst wurde.
- Informationsanbieter z.B. für wBs, Fraudpool, etc. haben teilweise ein starkes Wachstumspotential, welches u.a. durch die steigende Relevanz einer Überprüfung des geschäftlichen Hintergrundes von Geschäftsbeziehungen begründet wird.

BearingPoint

Die Möglichkeit der Verwendung von neuen Legitimationstechnologien wird allgemein von den Teilnehmern der Studie als positiv wahrgenommen

In welchen der bestehenden bzw. neuen Möglichkeiten zur Identitätsprüfung, sehen Sie mehr Chancen bzw. Risiken für die Geldwäschebekämpfung? Wir sehen in den folgenden Legitimationsmöglichkeiten, …

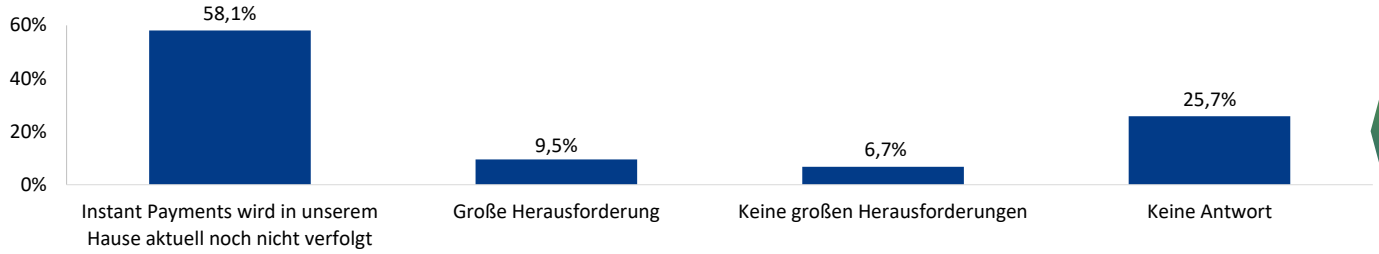


- Trotz der raschen Digitalisierung im Onboarding-Prozess wird die Kundenlegitimation vor Ort als die sicherste Legitimationsform eingestuft.
- Die e-Signatur folgt der Legitimation vor Ort, da insgesamt über 40% der Studienteilnehmer diesem Verfahren Chancen bzw. mehr Chancen einräumen.
- Das Post-Ident-Verfahren wird bei über 50% der Teilnehmer als risikobehaftet eingeschätzt, währenddessen dem Video-Ident-Verfahren lediglich nur 35% der Institute skeptisch gegenüber stehen.
- Laut einem Drittel der Studienteilnehmer birgt das Video-Ident-Verfahren ein höheres Geldwäscherisiko als das Post-Ident-Verfahren.

BearingPoint

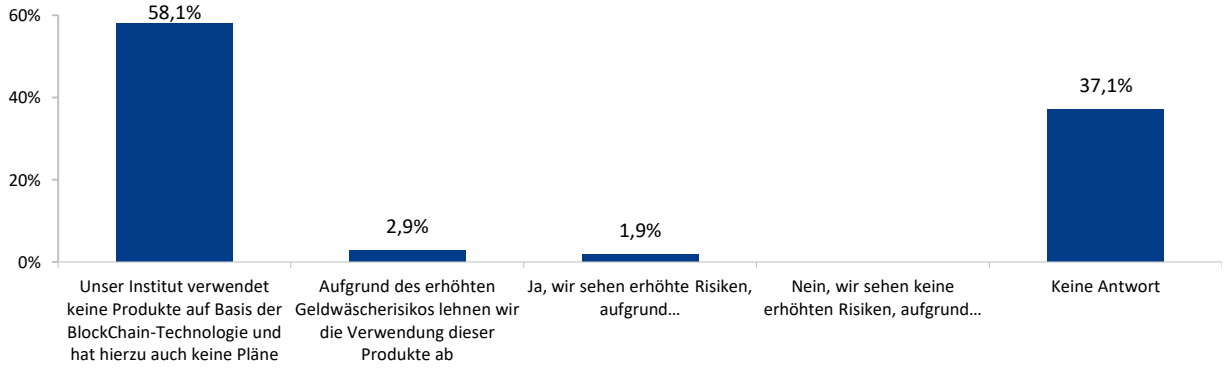
Obwohl Instant Payment bereits seit November 2017 zur Verfügung steht, befassen sich fast 60% der Teilnehmer noch nicht mit dem Thema

Wie bewerten Sie die aktuellen Entwicklungen zur Umsetzung von Instant Payments in Bezug auf die Einbindung der Geldwäsche-, Terrorismus- und Embargoprüfungen in den Zahlungsverkehrsprozess?



- Fast 60% der Teilnehmer befassen sich nicht mit Instant Payments.
- Zusatzangaben zu „Große Herausforderung“:
  - Gewährleistung der Real-Time Prüfungen,
  - undurchsichtiger Zahlungsverkehr,
  - Erfüllung GwG Anforderungen und
  - eine weitere Plattform für Betrug.
- Zusatzangaben zu „Keine große Herausforderung“:
  - Bereits in bestehenden Überwachungssysteme implementiert.

Sofern Ihr Institut Produkte auf Basis der neuen Technologie Blockchain anbietet oder plant, erwarten Sie erhöhte Geldwäscherisiken?

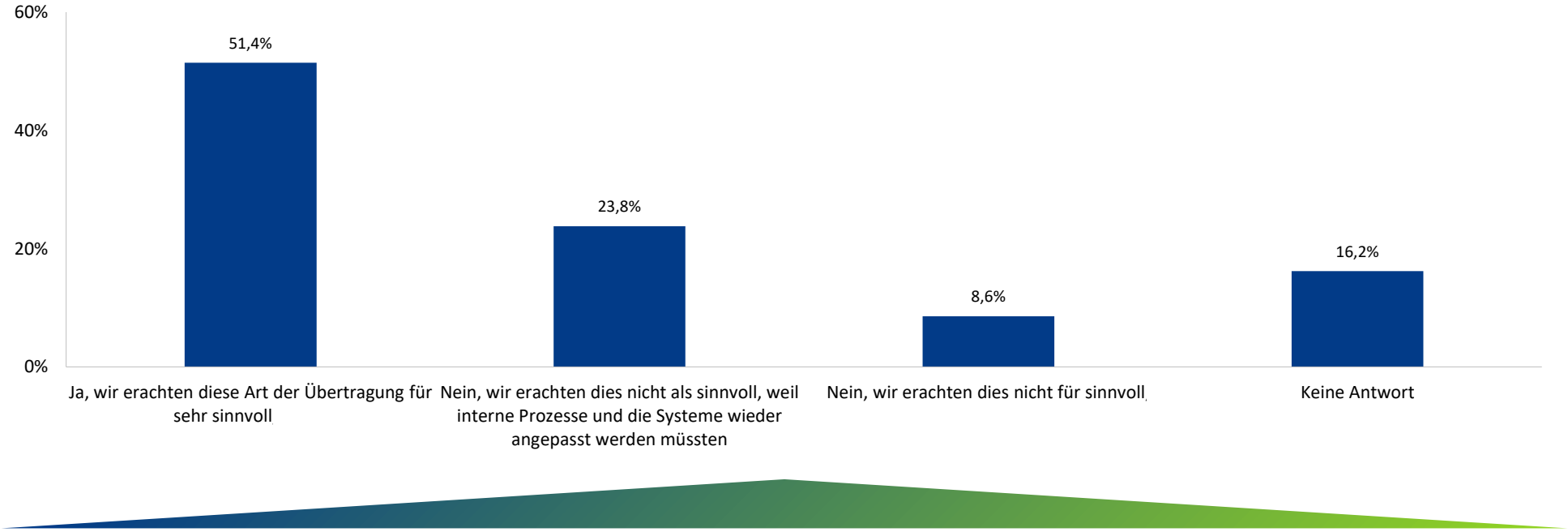


- Obwohl Blockchain nun mehr als innovative Technologie angesehen wird, haben sich Finanzinstitute noch nicht intensiv mit der Thematik auseinandergesetzt.
- Die Verwendung der Blockchain-Technologie schätzen einige Teilnehmer als riskant in Bezug auf erhöhtes Geldwäscherisiko ein. Als Gründe hierfür wurde folgendes genannt:
  - Transaktionsgeschwindigkeit,
  - Anonymität, sowie
  - fehlende Regulierung des Markts auf Basis von Blockchain.

BearingPoint

Im Rahmen der Digitalisierung sieht die Hälfte der Banken große Prozessoptimierungs-potentiale in der elektronischen Übermittlung von Verdachtsmeldungen an die FIU

Erachten Sie eine elektronische Verdachtsmeldung (gesicherter Übertragungsweg, Übermittlung von Anlagen, strukturierte Datenanlieferung, etc.) gemäß § 43 GWG an die FIU als sinnvoll?

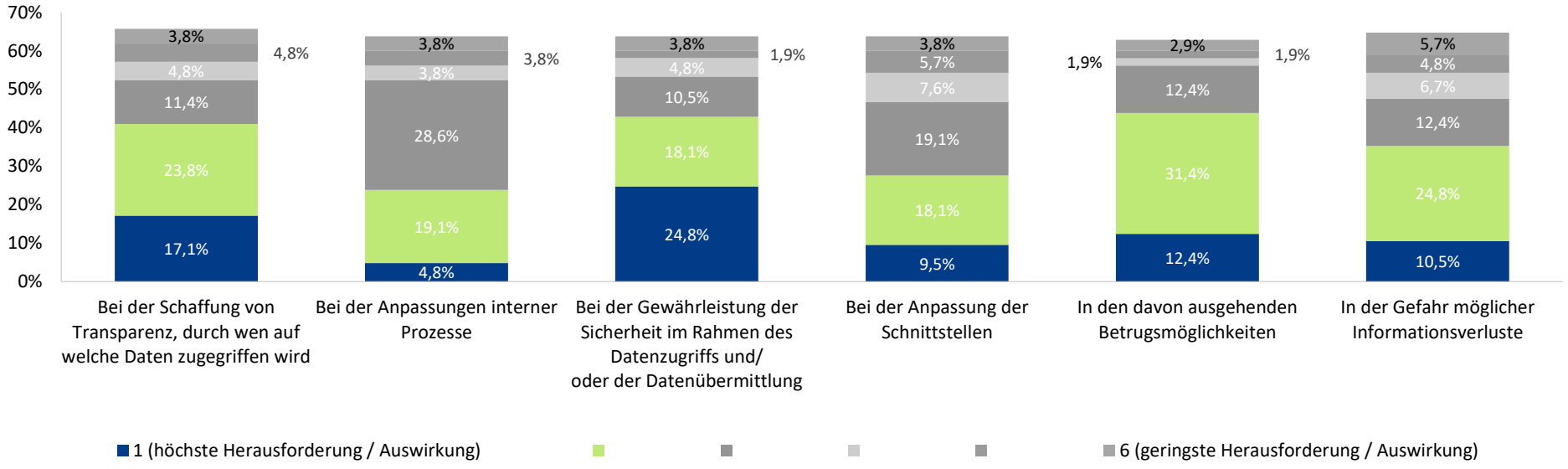


- Die elektronische Datenübermittlung an die FIU wird vom Großteil der Befragten (51%) für sehr sinnvoll gehalten.
- Begründung für elektronische Meldungen sind u.a.: schnelle Übermittlung und Rückmeldung der Ermittlungsbehörden, Verhinderung des Medienbruchs, papierloses Büro, Prozessstraffung, Effizienzsteigerung, Vereinheitlichung der Vorgehensweise, Vereinfachte Auswertung der Daten bei FIU etc.
- Für die Implementierung der elektronischen Meldungen wurde im Jahr 2009 von der Bundesregierung ein Pilotprojekt (eVA) im Rahmen des Programm „E-Government 2.0“ initiiert. Innerhalb dieses Projekts wurden die technischen und fachlichen Grundlagen (Datenstruktur, Übermittlungswege, Verarbeitung) für den Datenaustausch zwischen Banken, Finanzdienstleistern, Unternehmen und Polizeibehörden entwickelt.

BearingPoint

Bei der Digitalisierung im Rahmen von PSD 2 werden insbesondere Betrug, Datensicherheit und Übersicht über Datenzugriffe als größte Herausforderungen eingeschätzt

Durch die zweite EU-Zahlungsdienstrichtlinie werden Dritte Zahlungsdienstleister zukünftig über neue, erweiterte Schnittstellen einen Zugang zu Kontoinformationen ihrer Kunden erhalten sowie direkt Zahlungen für ihre Kunden auslösen können. Wo sehen Sie die höchsten bzw. niedrigsten Herausforderungen?

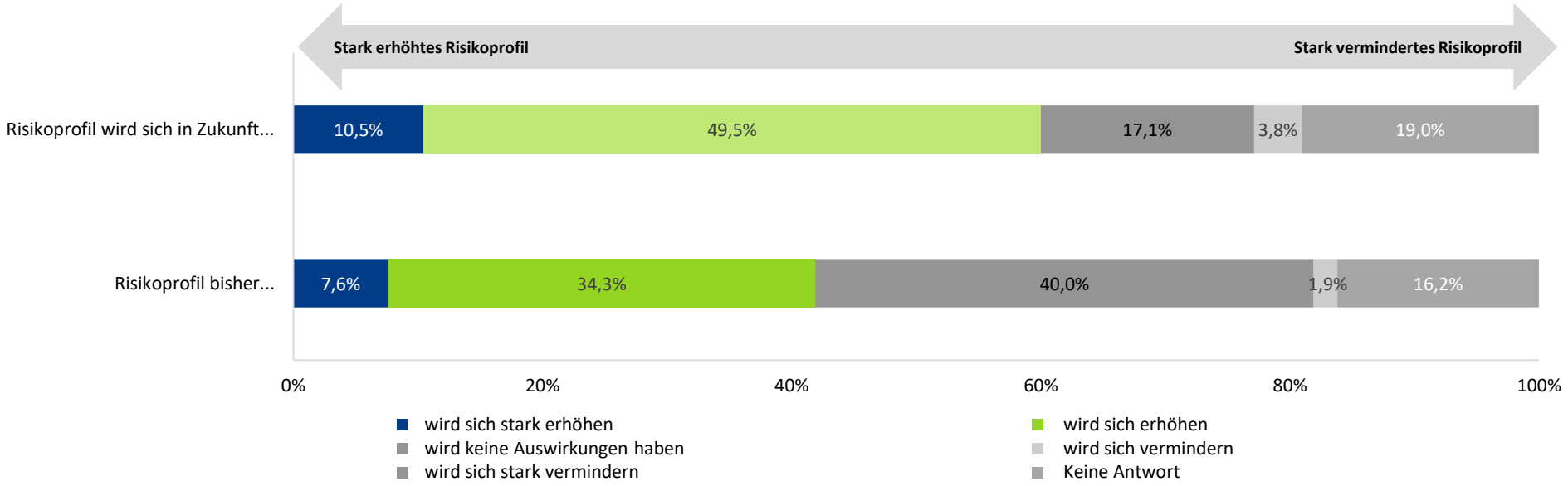


- Die „Gewährleistung der Sicherheit beim Datenzugriff“ oder der „Datenübermittlung“ wird als höchste Herausforderung für Finanzinstitute bei der PSD 2 identifiziert.
- Die zweithöchste Herausforderung wird der „Schaffung von Transparenz“ bezüglich des Datenzugriffs zugeordnet, gefolgt von der Anpassung interner Prozesse.
- Bei der geplanten „Gewährleistung des Zugangs durch Dritte“, bei „möglichen Informationsverlusten“, sowie bei den davon „ausgehenden Betrugsmöglichkeiten“ sehen die meisten Institute hohe Herausforderungen.
- Aus den Freitextantworten geht hervor, dass die Teilnehmer höhere Herausforderungen in den Bereichen „Kommunikation mit dem Kunden“, „datenschutzrechtliche Risiken“ und „Ertragsverluste“ bezüglich der Gewährleistung des Zugangs für Dritte sehen.

BearingPoint

Aus Sicht der Geldwäsche und Betrug birgt die Digitalisierung verstärkt Risiken mit denen die Banken in Zukunft umgehen müssen

Im Zuge der Digitalisierung, wie sehen Sie die bisherige und zukünftige Entwicklung Ihrer Wertschöpfungsprozesse hinsichtlich der Auswirkungen auf das Risikoprofil für Geldwäsche-, FinSan-Verstöße und betrügerische Handlungen?



- Über 60% der Teilnehmer sehen eine zukünftige Erhöhung der Compliance-Risiken im Zusammenhang mit der Digitalisierung.
- Die Digitalisierung wird für die Banken ein verstärktes Compliance-Risiko darstellen.

BearingPoint

Agenda

I. Studienvorstellung & Teilnehmerangaben

II. Handlungsempfehlungen

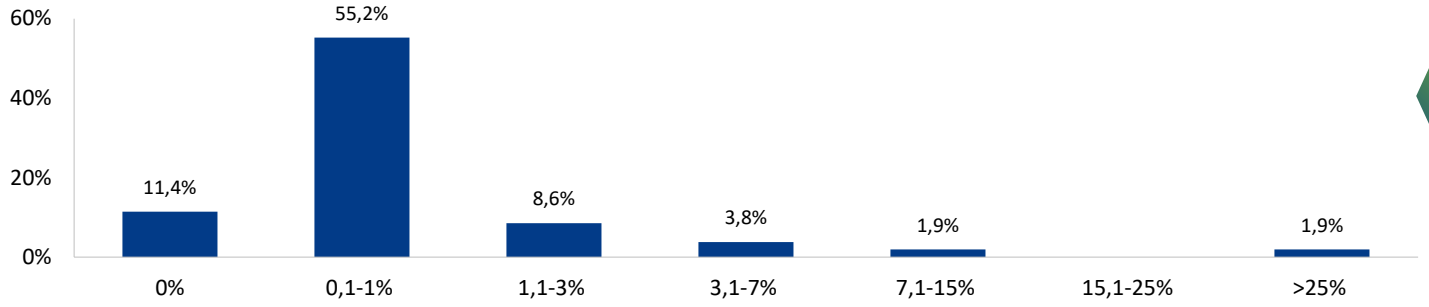
III. Fragen zur Geldwäschebekämpfung - Umsetzung „GwG-Neu“

IV. Fragen zur Digitalisierung von Compliance Prozessen

V. Fragen zu „sonstigen strafbaren Handlungen“ (§ 25h KWG)/Betrugsbekämpfung/Zentrale Stelle

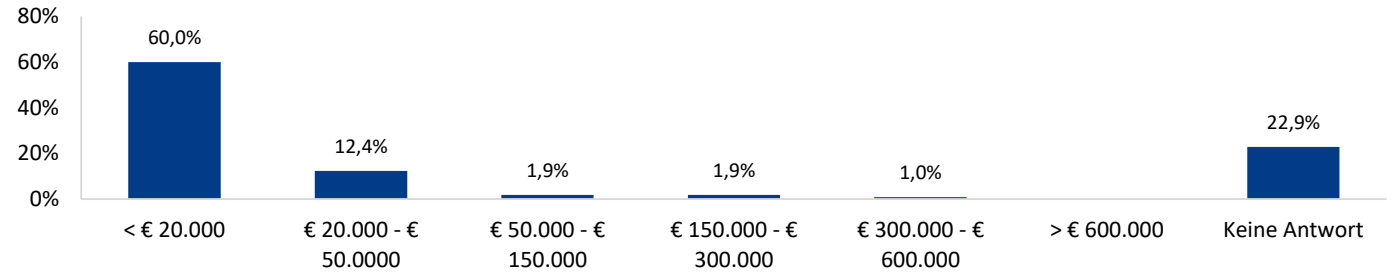
Banken verzeichnen ein überschaubares Maß an Netto-Betrugsschäden

Wie hoch schätzen Sie den relativen Anteil am Portfolio des Geschäftsvolumens der Schadensfälle pro Jahr aus sonstigen strafbaren Handlungen in % ein?



- Der Großteil der Teilnehmer sieht die Schadenshöhe aus „sonstigen strafbaren Handlung“ in der Größenordnung von 0,1% - 1% des Geschäftsvolumens.

Wie hoch schätzen Sie den durchschnittlichen Schaden pro Schadensfall aus sonstigen strafbaren Handlungen?



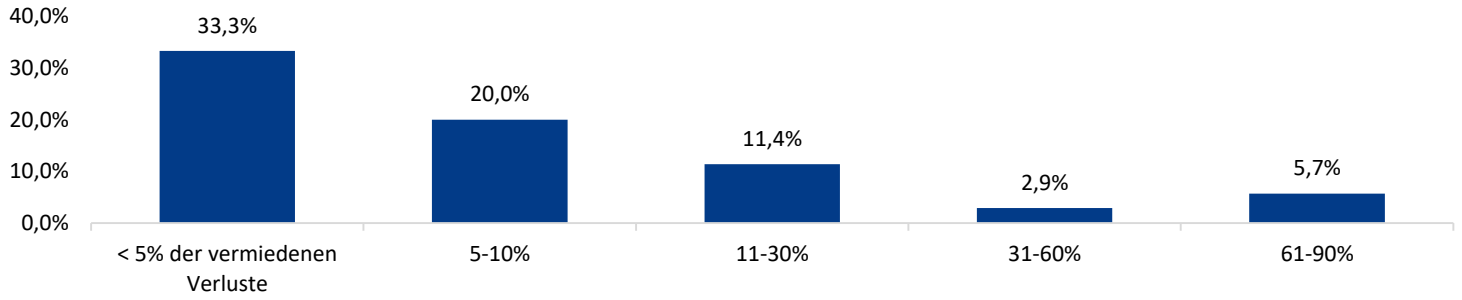
- Bei über 60% der Befragten beträgt die durchschnittliche Schadenshöhe weniger als EUR 20.000.
- Hierbei müssen klare „Kosten-Nuten“- Analysen durchgeführt werden, in denen die Präventionskosten dem Nutzen durch die Vermeidung von finanziellen Schäden gegenüber gestellt werden müssen.

BearingPoint

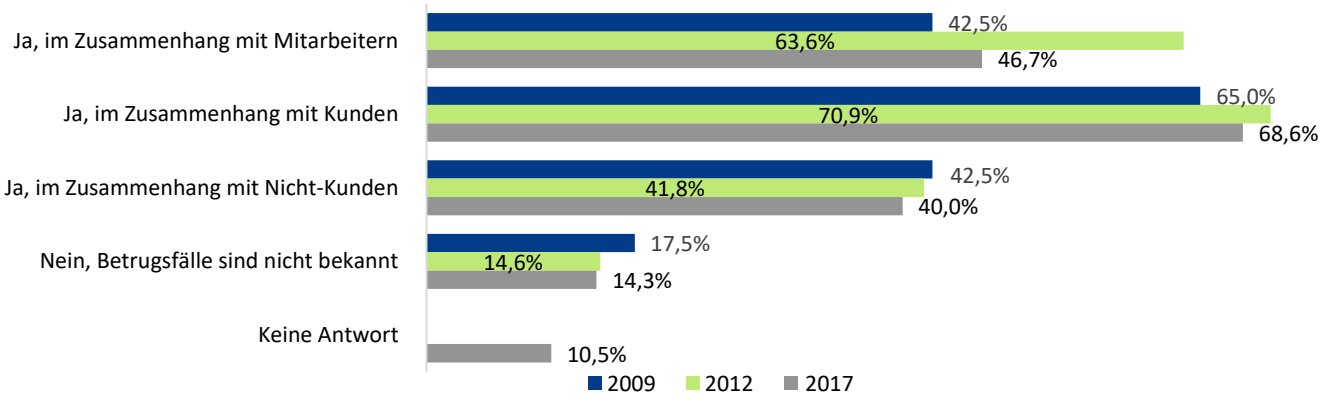
Maßnahmen zur Betrugsbekämpfung greifen in weiten Teilen nicht, da bei knapp 50% der Banken gerade mal max. 10% der Verluste vermieden werden können

- Bei einem Großteil der Banken greifen die Präven-tionsmaßnahmen sehr begrenzt max. – 10% sonstiger strafbarer Handlungen vermieden.
- Daraus lässt sich schließen, dass bei einem Großteil der Banken Maßnahmen nicht greifen.

Wie hoch schätzen Sie den relativen Anteil am Portfolio der vermiedenen Verluste (z.B. durch Systeme, Kontroll-Prozesse, Schulungen, etc.) pro Jahr aus sonstigen strafbaren Handlungen in %?



Sind in Ihrem Institut in der Vergangenheit Betrugsfälle aufgetreten?

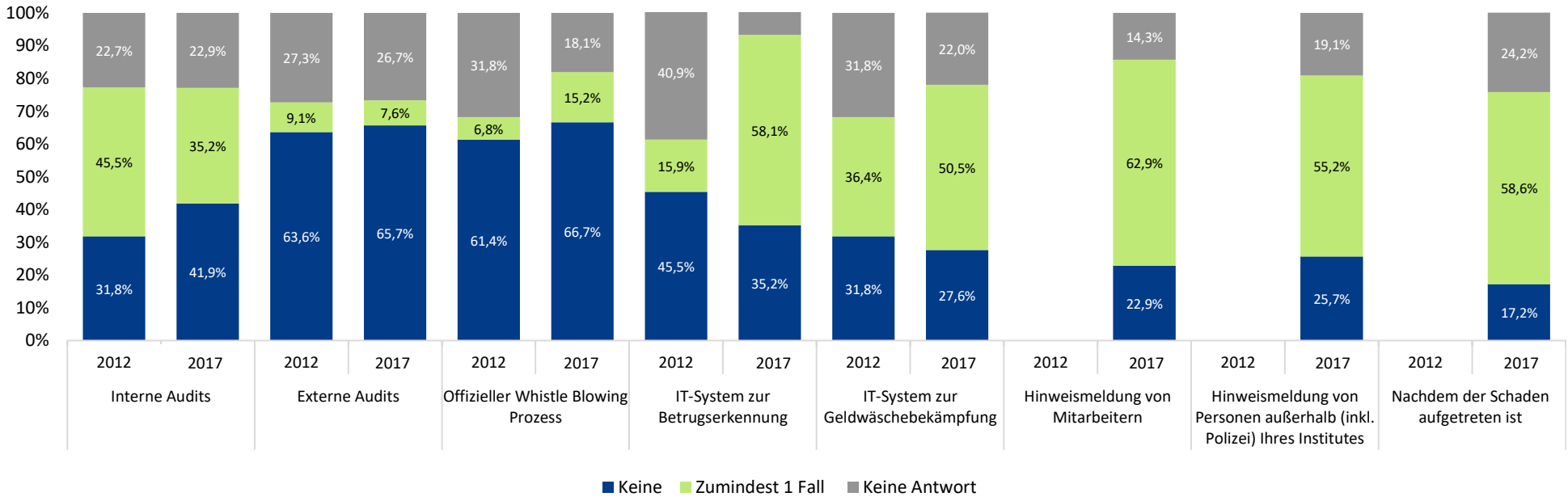


- Ca. 85% der Teilnehmer waren bis dato von Betrug betroffen.
- Als Hauptgrund für das Betrugs-auftreten wird der Kunde identifiziert.
- Fast 50% der Betrugsfälle stehen in 2017 im Zusammenhang mit Mitarbeitern, wo bei es in 2012 ein Drittel mehr war.
- Die wenigsten Betrugsfälle sind durch Nicht-Kunden (40%) entstanden.

BearingPoint

Am häufigsten wird Betrug durch Mitarbeiter-Hinweise identifiziert

In welcher Weise sind in Ihrem Institut Betrugsfälle identifiziert worden?

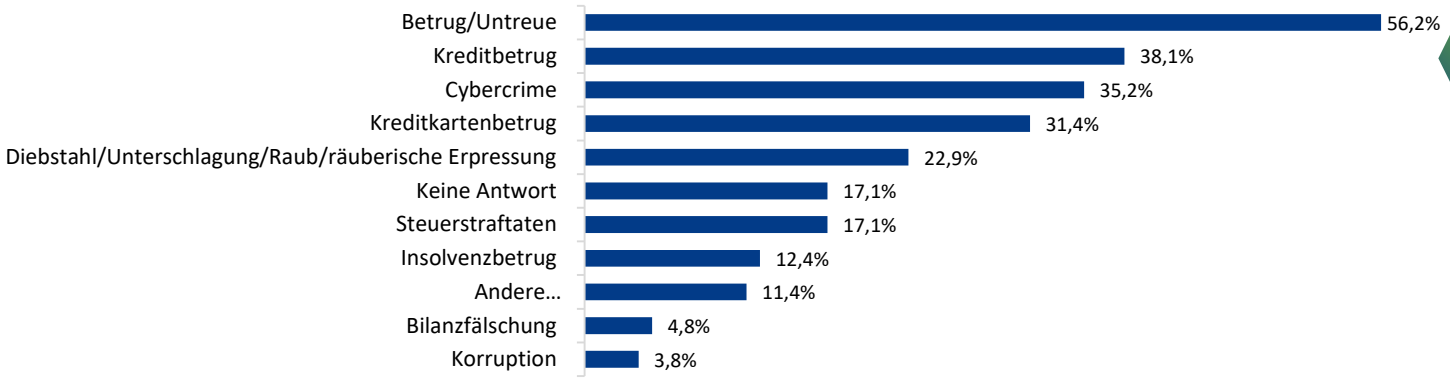


- Gemäß zwei Drittel der Teilnehmer hilft der Whistle-Blowing Prozess zur Betrugsbekämpfung nicht.
- Stattdessen führt eine Kombination von Mitarbeiter-Hinweismeldung und IT-gestützten Prüfungen zu größerem Erfolg (ca. 58-63%).
- Externe Audits sind im Vergleich zu anderen Informationsquellen am wenigsten behilflich. Nur ca. 8 % der Betrugsfällen wurden mit Hilfe von externen Audits entdeckt.
- Ein Großteil der Betrugsfälle werden erst nach Auftreten des Schadens identifiziert.

BearingPoint

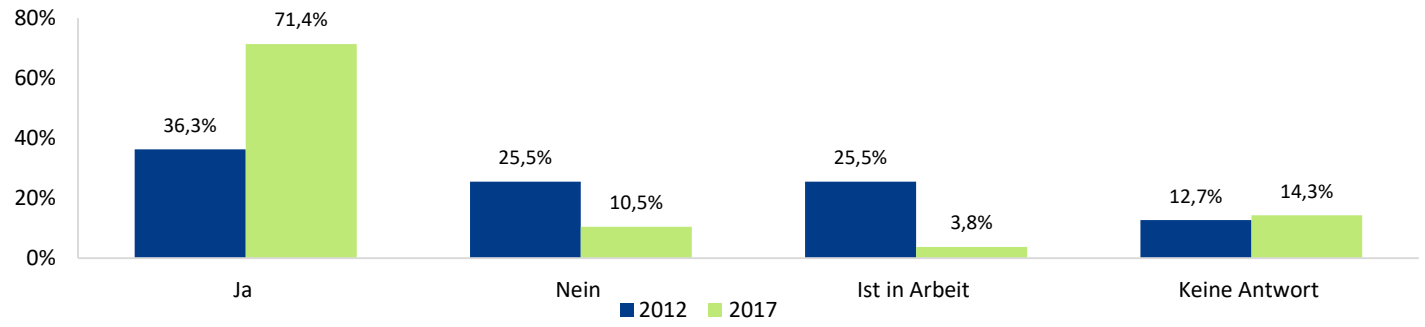
Betrug/Untreue, Kredit(-karten)betrug und Cybercrime konnten als am häufigsten aufgetretene strafbare Handlung identifiziert werden

Welche strafbaren Handlungen sind bis dato am häufigsten in Ihrem Institut aufgetreten?



- Betrug, Untreue, Cybercrime sowie Kredit (-karten)-Betrug sind die am häufigsten aufgetretenen strafbaren Handlungen.

Gibt es einen "Notfallplan" für das Vorgehen in Betrugsfällen? (Kommunikationskonzept)

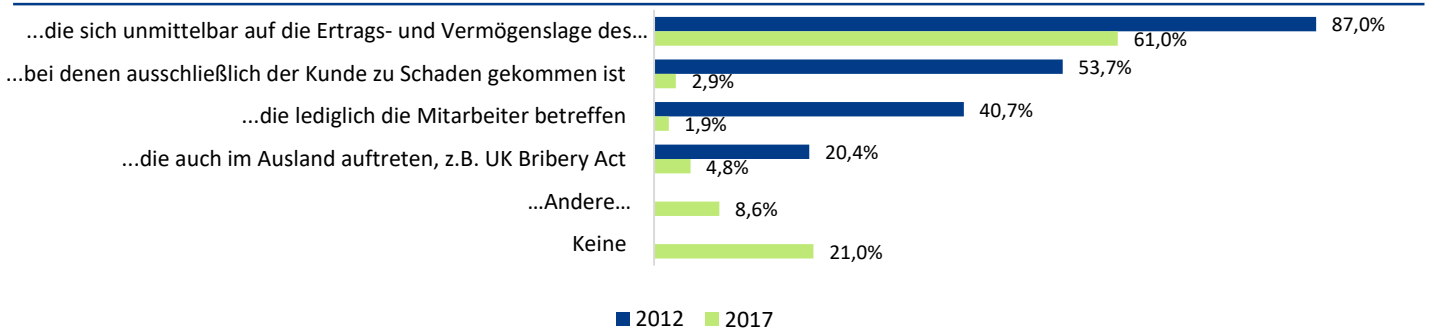


- Über zwei Drittel der teilnehmenden Institute (70%) haben vorsorglich ein Kommunikationskonzept zur Minderung des Reputationsrisikos ausgearbeitet.
- In 2012 waren es erst ein Drittel, dass einen Notfallplan hatte.

BearingPoint

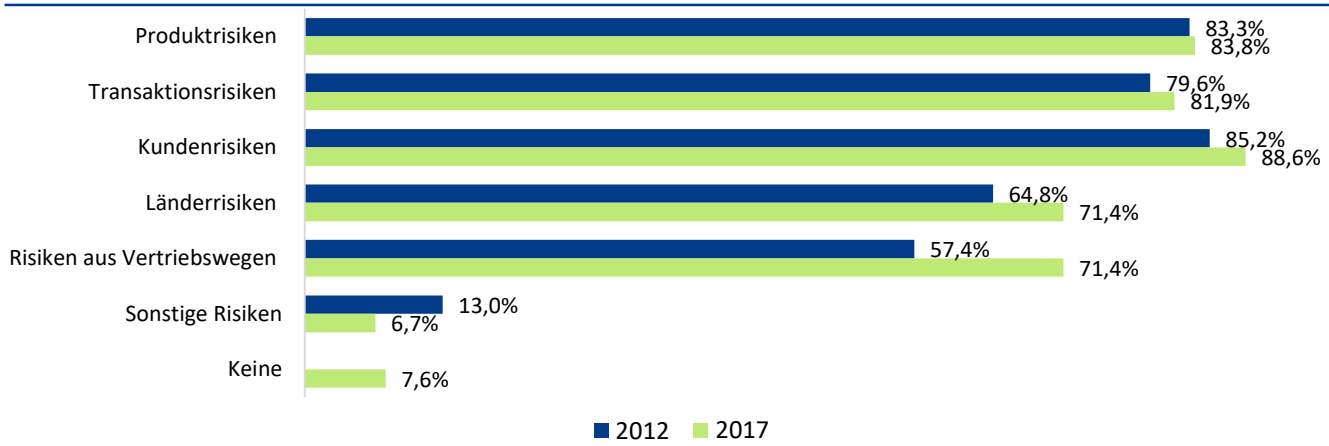
Banken fokussieren sich bei der Betrugsprävention eher auf Risiken, die die Vermögenslage des Institutes betreffen

Auf welche Vermögensgefährdungen fokussiert sich Ihr Institut im Hinblick auf die Regelungen des § 25h KWG? Auf Vermögensgefährdungen…



- Die Institute legen bei der Bekämpfung der "sonstigen strafbaren Handlungen" nach wie vor primär Wert auf den Schutz des eigenen Vermögens.
- Betrugsschäden bei Kunden spielen eine stark untergeordnete Rolle.

Welche Risikobereiche umfasst Ihre Risikoanalyse (vormals Gefährdungsanalyse) für "sonstige strafbare Handlungen"?



- Die wichtigsten in der Risikoanalyse für "sonstige strafbare Handlungen" einbezogenen Risikoarten sind Kundenrisiken, Transaktionsrisiken, Produktrisiken und Länderrisiken. Bezeichnend ist darüber hinaus, dass im Vergleich zu 2012 vermehrt Vertriebswegrisiken einbezogen werden.

BearingPoint

Kontakt

Oliver Engelbrecht
Partner
oliver.engelbrecht@bearingpoint.com

Autoren:
Christopher Offe, Corinna Sieglin,
Johanna Wenk und Janina Schießl

BearingPoint®

Über BearingPoint

BearingPoint ist eine unabhängige Management- und Technologieberatung mit europäischen Wurzeln und globaler Reichweite. Das Unternehmen agiert in drei Bereichen: Consulting, Solutions und Ventures. Consulting umfasst das klassische Beratungsgeschäft, Solutions fokussiert auf eigene technische Lösungen in den Bereichen Digital Transformation, Regulatory Technology sowie Advanced Analytics, und Ventures treibt die Finanzierung und Entwicklung von Start-ups voran. Zu BearingPoints Kunden gehören viele der weltweit führenden Unternehmen und Organisationen. Das globale Netzwerk von BearingPoint mit mehr als 10.000 Mitarbeitern unterstützt Kunden in über 75 Ländern und engagiert sich gemeinsam mit ihnen für einen messbaren und langfristigen Geschäftserfolg.

Für weitere Informationen: www.bearingpoint.com

BearingPoint®

BearingPoint®