DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner

AUSGABE 2/2020

Gemeinsam Herausforderungen annehmen

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 23, 2/2020
ISSN: 2194-9514
Herausgeber: DZ CompliancePartner GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.dz-cp.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter, Norbert Schäfer

Verantwortlich i. S. d. P.: Jens Saenger
Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: DZ Compliance-Partner GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@dz-cp.de
Weitere Autoren dieser Ausgabe:
Andreas Arendt, Marco Becker, Christina Fiedler, Thomas Grebe, Dennis Heinemeyer, Martin Hierlemann, Marc Hübner, Andreas Marbeiter, Lars Schinnerling, Michael Switalla, Dominik Tiburtius, Thomas Wagener

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto (Titel, Seite 22)
Gestaltung: EGENOLF DESIGN, Wiesbaden, studio@egenolf-design.de
Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktionsschluss: 3. August 2020
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc

Wenn uns Corona eines lehrt,

dann ist es, Herausforderungen anzunehmen.

Jens Saenger
Sprecher der Geschäftsführung

Risiken zu erkennen und zu steuern, haben wir lange eingeübt. Nun ist genau das unsere stabile Planke über unsicheres Gelände. Schritt für Schritt lernen wir alle – gemeinschaftlich – die vielen und auch vielfältigen Herausforderungen der Krise zu erkennen und darauf zu reagieren. Wir erleben eine große Partnerschaft in der Zusammenarbeit mit Ihnen, unseren Kunden, mit unseren Mitarbeiterinnen und Mitarbeitern und auch unseren Lieferanten. Wenn in der Krise das wahre Gesicht zum Vorschein kommt, so sieht dieses kreativ, lösungsorientiert und miteinander verbunden aus. Das ist in der aktuellen Pandemie die positive Erfahrung, für die wir uns bei Ihnen allen bedanken möchten.

Unser **gemeinsamer** „Erfahrungsschatz" lässt belastbare Erkenntnisse, schnelles Handeln und valide Prognosen zu. Gleichzeitig bündeln wir auch und die gemeinsamen Interessen und können als starke Gesprächspartner auftreten. Das hilft.

Wie das im Einzelnen aussieht, davon möchten wir im vorliegenden Heft sprechen.

Bleiben Sie gesund.

Ihr Jens Saenger

▶ **Compliance**

Wirecard und seine Folgen

Es vergeht seit Wochen kaum ein Tag, an dem nicht irgendwelche Informationen zu dem Fall Wirecard viral gehen. Aktualität und Tragweite des Vorgangs erscheinen geeignet, sich mit dem bislang Bekannten und seinen möglichen Folgen für die Compliance-Management-Systeme im Allgemeinen zu beschäftigen.

Unbestritten ist, dass dieser Vorfall erhebliche Wellen schlägt. Dies ist umso relevanter, da sich hier mehr oder weniger alle Stakeholder, die im Umfeld der Finanzdienstleistungsindustrie eine Rolle spielen, im Rahmen ihrer Aufgabenstellungen hinterfragen und dies auch durchaus kritisch tun. Dies betrifft nicht nur den Vorstand des Unternehmens Wirecard AG und potenziell betrügerisch tätige Führungskräfte, sondern tangiert auch den Aufsichtsrat des Unternehmens, die Finanzdienstleistungsaufsicht BaFin sowie die nach Bundes- und Landesrecht zuständige Stelle, den Abschlussprüfer, die Compliance-Funktion, die Investoren sowie die Finanzanalysten, die das Unternehmen über Jahre hinweg analysiert haben.

Aufgrund der hohen Komplexität des Vorfalls und der Notwendigkeit zur Durchführung einer gründlichen Analyse ist zwar nicht mit Schnellschüssen zu rechnen. Dennoch ist es aufgrund des erheblichen Reputationsschadens für den Finanzplatz Deutschland sehr wahrscheinlich, dass dieser Fall ein Impulsgeber für die aktuellen Normen, deren Gestaltung sowie die Maßnahmen zu deren Einhaltung sein wird.

Welche Normen könnten betroffen sein?

Immer wieder fallen hier der Begriffe des Corporate-Governance- Systems sowie der Einhaltung gesetzlicher Vorgaben inkl. der Transparenz in der Berichterstattung. Ob bzw. wo es in der Umsetzung der aktuellen Vorgaben systemische Mängel gegeben hat oder ob bzw. wo es auch die Notwendigkeit zu gestalterischen Anpassungen in den aufsichtlichen Rahmenbedingungen gibt, werden die nächsten Monate zeigen. Bereits jetzt wird aber deutlich, dass ein bloßes Vorhalten eines Compliance-Management-Systems per se keine Garantie für die Einhaltung gesetzlicher Normen ist.

Jedes System muss in der Praxis den Beweis antreten, dass es in gleichem Maße angemessen ausgestaltet wie auch in der Sache tatsächlich wirksam ist. Nicht umsonst gehört die unabhängige Testierung des Internen Kontrollsystems in der DZ CompliancePartner GmbH seit Jahren durch die Wirksamkeitsprüfung nach IDW PS 951 Typ II zum Standard in unserer Dienstleistungspalette.

Der Begriff der Angemessenheit lässt sich auch für die Betrachtung der Berichterstattung verwenden. Wenn die Aufsichtsorgane an ihre Kontrollverpflichtung erinnert werden, sollte auch Art und Inhalt der vorgelegten Berichterstattung darauf ausgerichtet sein, alle wesentlichen Entwicklungen sowie die damit verbundenen Risikoeinschätzungen kompakt und sachgerecht erkennen zu können. In der DZ CompliancePartner GmbH arbeiten wir fortlaufend in Zusammenarbeit mit unseren Kunden und Beiräten an einer sachgerechten Ausgestaltung unseres Berichtswesens von Risikoberichten über Quartals- und Ad-hoc-Berichten bis hin zum Jahresbericht. Wir werden daher den Fortgang der Berichterstattung und den Erkenntnisgewinn sehr genau verfolgen und unseren eigenen Prozess damit abgleichen.

Aktuell verdichten sich die Hinweise, dass es im Fall Wirecard auch umfassende Betrugsmuster gibt. Es ist Stand heute nicht davon auszugehen, dass es DAS perfekte Betrugspräventionssystem gibt, mit dem jedwede betrügerische Handlung identifiziert oder gar im Vorfeld verhindert werden könnte. Und dennoch erhöht das Vorhandensein jeder wirksamen Kontrolle die Wahrscheinlichkeit, das Eintreten betrügerischer Handlungen sowie des damit verbundenen Vermögens- und Reputationsschadens zu reduzieren.

Wichtig ist in diesem Zusammenhang auch die Vielfalt der hierfür vor allen Dingen hierarchie- und risikobasiert einzusetzenden Instrumente und Maßnahmen. Das geht vom reinen Anweisungswesen über manuelle und maschinelle Kontrollsystematiken bis hin zu persönlichen Vor-Ort-Wirksamkeits- und Penetrationstests oder gar forensischen Ansätzen. Flexibilität und Erfahrung werden umso wichtiger, je höher in den Hierarchieebenen eines Hauses die Mechanismen anzusetzen sind. Bisweilen ist es da sogar sehr hilfreich, sich auch der Expertise externer Fachleute im Rahmen z. B. des Beauftragtenwesens zu bedienen. Damit können sich zumindest einige bestimmte Interessenkonfliktkonstellationen vermeiden lassen.

Neben den betrügerischen Handlungen, z. B. im Bereich der Geldwäscheprävention, werden auch die marktmanipulativen Sachverhalte des Unternehmens durch Aktienkäufe/-verkäufe per se, aber auch insbesondere in Verbindung mit der entsprechenden Unternehmenskommunikation angesprochen. Auch wenn Volksbanken und Raiffeisenbanken selbst keine börsennotierten Gesellschaften sind, besteht dennoch die Verpflichtung zur Prävention und Überwachung von marktmanipulativem Verhalten auch im Rahmen der eigenen Kundschaft und bei den Mitarbeitern. Diese Thematik hat bereits nachgewiesene Relevanz für die Genossenschaftliche FinanzGruppe. Daher werden wir unser aktuelles Angebot im dritten Quartal 2020 mit einer fachlich und inhaltlich überarbeiteten Dienstleistung, MAR Kompakt Plus, für Sie erweitern.

AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter
Geschäftsführung,
E-Mail: andreas.marbeiter@dz-cp.de

Fazit

Bereits jetzt zeichnen sich vielfache Impulse für eine optimierte Ausgestaltung der Compliance-Management-Systeme in Bezug auf Effektivität und Effizienz ab. Dennoch wird dabei eines sehr deutlich: Sich ausschließlich auf das betrügerische Verhalten einzelner Menschen oder das Versagen von Kontrollsystemen infolge bestehender oder noch nicht vorhandener Kontrollvorgaben zu beschränken, wäre ein Schritt zu wenig gegangen.
Am Ende braucht es eine ausgewogene Symbiose zwischen der angemessenen Ausgestaltung wirksamer Kontrollsysteme und einem persönlichen Compliance-Bewusstsein der handelnden Personen aller Hierarchieebenen bei allen „Stakeholdern". Dieses Zusammenspiel entscheidet über Erfolg und Misserfolg. Nur so kann sich der Aufwand der Investitionen in die Regulatorik auch nachhaltig auszahlen. ▬

IT-Revision

IT-Revision aus dem Homeo

Durch die noch anhaltende Corona-Pandemie gewinnt die digital gestützte Vernetzung von Ressourcen und Unternehmensprozessen inzwischen eine greifbare reale Bedeutung. Grundlegende Veränderungen des Arbeitsalltags stellen Mitarbeiter und Unternehmen vor große Herausforderungen: Plötzlich im Homeoffice.

Die Verlagerung von Tätigkeiten vor Ort hin zu Tätigkeiten im Homeoffice beeinflusst den bisherigen Ablauf von Prüfungshandlungen der IT-Revision bei unseren Kunden in mehrfacher Hinsicht.

Herausforderung

Die IT-Revision als Teil der Internen Revision bleibt, unabhängig von Covid-19, ein wichtiges Element der Unternehmensleitung zur Unterstützung aufsichtsrechtlich bedingter Kontroll- und Überwachungspflichten, um den damit verbundenen Sorgfaltspflichten nachkommen zu können.

Auch die IT-Audit der DZ CompliancePartner GmbH sah sich mit ihrem Angebot zur Auslagerung der IT-Revision vor die Herausforderung gestellt, Lösungen in der Krise zu finden. Erlassene Kontaktsperren, Reiseverbote und die Beachtung föderaler Unterschiede im bundesweiten Einsatz setzten den Rahmen, in dem – sehr schnell – eine neue, sichere Vorgehensweise zur Prüfungsdurchführung gefunden werden musste. Dabei durften die aktuelle Terminplanung und die bestehenden personellen Ressourcen unter dem Blickwinkel der Wirtschaftlichkeit nicht aus den Augen verloren werden.

Neben Logistik und Technik mussten auch die Belange der Mitarbeiter beachtet werden. Der zunehmende Mangel an sozialen Kontakten und die damit einhergehende Isolation in häuslicher Büroarbeit machten Maßnahmen erforderlich, die Orientierung, Vertrauen und Wertschätzung vermittelten.

Zielgerichtete Unterstützung

Nicht zuletzt dürfen und können unsere Kunden von uns, ihrem Auslagerungspartner, erwarten, dass wir – gerade in Krisensituationen – eine zielgerichtete Unterstützung durch sensibles Serviceverhalten und praktische Lösungsansätze anbieten. Denn auch sie müssen sich ihrerseits in dieser Krisenzeit mehr denn je auf die Bedürfnisse und Erwartungen ihrer Kunden und Mitglieder fokussieren können. Da macht es sich bezahlt, dass die Mitarbeiter der IT-Audit die Infrastruktur ihrer Kunden kennen und Weiterentwicklungen im Rahmen von Prüfungshandlungen der IT-Revision seit vielen Jahren begleiten.

Die DZ CompliancePartner GmbH hat den Anspruch, insbesondere in solchen Krisen ihren Kunden kompetent zur Seite zu stehen. Wie sich dies in der Praxis zeigt, skizziert das nachfolgende Interview mit dem IT-Leiter der Raiffeisenbank HessenNord eG in Wolfhagen, Herrn Andreas Arendt:

Herr Arendt, die Raiffeisenbank HessenNord eG beschäftigt rund 150 Mitarbeiter an elf Standorten. Wie intensiv war Ihre Bank seit März durch die Pandemie beeinträchtigt?
A. Arendt: Wir haben uns schon frühzeitig mit dem Thema Corona beschäftigt, insbesondere im Hinblick auf den Schutz der Mitarbeiter. Neben der Bereitstellung von Desinfektionsmitteln, Schutzmasken für jeden Mitarbeiter und die Beschaffung von Trennwänden lag ein weiteres Augenmerk natürlich auf der Aufrechterhaltung des Geschäftsbetriebes. Hier mussten wir, insbesondere im Hinblick auf zentralisierte Abteilungen und Bereiche, für uns neue Wege gehen. In einem ersten Schritt wurde vom gebildeten Krisenteam aus Vorstand und Abteilungsleitung das „Inselprinzip“ beschlossen. Der sonst übliche Austausch von Personal zwischen den Geschäftsstellen im Rahmen von Urlaubs- und Krankheitsvertretungen wurde vollständig eingestellt. Als weiteres ernsthaftes Problem wurden die zentralisierten Abteilungen identifiziert, da hier die Gefahr bestand, durch die Infizierung einer einzelnen Person die gesamte Abteilung zu verlieren. Neben der Reaktivierung von bankeigenen Räumlichkeiten in SB-Geschäftsstellen hat das Thema „Homeoffice“ einen ungeahnten Schub bekommen. Alle in unserem Haus zur Verfügung stehenden Notebooks wurden umgehend, sofern nicht ohnehin schon als mobiler Arbeitsplatz genutzt, technisch umgestellt und entsprechende VPN-Zugänge

office – ein Praxisbericht

AUTOREN UND ANSPRECHPARTNER

Andreas Arendt
Leiter IT-Orga/Allg. Verwaltung
Raiffeisenbank HessenNord eG,
E-Mail: andreas.arendt@rb-hessennord.de

Thomas Grebe
Leiter IT-Audit,
E-Mail: thomas.grebe@dz-cp.de

beauftragt. Im weiteren Verlauf konnten wir zusätzliche Homeoffice-Arbeitsplätze generieren, da die Fiducia & GAD IT AG als zuständige Rechenzentrale auch die Nutzung von Desktop- Arbeitsplätzen für die VPN-Nutzung freigegeben hat. Schlussendlich sind im Moment etwa ein Drittel unserer Bankarbeitsplätze Homeoffice-fähig.

In welchem Umfang war Homeoffice denn vorher schon möglich?
A. Arendt: Wir nutzen die Möglichkeit der alternierenden Telearbeit schon seit einigen Jahren, im Wesentlichen war die Möglichkeit allerdings dem Vorstand und den Führungskräften vorbehalten. Durch die Corona-Problematik ist hier ganz sicher ein Umdenkprozess angestoßen worden. Inzwischen nutzen Mitarbeiter aus den Bereichen Marktfolge Aktiv, Revision, Firmen- und Privatkunden sowie weitere interne Abteilungen die neuen Möglichkeiten. Erste Tests mit den Mitarbeitern unserer bankeigenen Telefonfiliale verlaufen vielversprechend. Als willkommener Nebeneffekt kann sich unser Haus auch als moderner und attraktiver Arbeitgeber präsentieren.

Sie haben also bisher gute Erfahrungen in Ihrem Hause gemacht?
A. Arendt: Die bisherigen Erfahrungen sind weitgehend positiv. Zur Risikogruppe gehörende Mitarbeiter stehen dem Unternehmen weiterhin voll zur Verfügung, für einen weiteren Personenkreis ergeben sich Chancen, Familie und Engagement im Beruf unter einen „Hut“ zu bringen. Durch die räumliche Trennung sind neue Gedankenwelten hinsichtlich Übermittlung und Verteilung von Informationen und Unterlagen entstanden, viele althergebrachte Vorgehensweisen stehen jetzt auf dem Prüfstand. Sehr hilfreich ist dabei der in unserem Haus schon vorhandene hohe Digitalisierungsgrad. Wichtig bei der Umsetzung ist ein absolut transparenter Austausch zwischen Vorstand, Führungskräften und Mitarbeitern über auftretende Probleme. Nur so können Lösungen gefunden werden, um gesetzlichen Vorschriften, Anforderungen der Bank und Bedürfnissen der Mitarbeiter zu entsprechen.

Ihr Unternehmen hat die IT-Revision an die DZ CompliancePartner GmbH ausgelagert. Wie bewerten Sie die Zusammenarbeit?
A. Arendt: Ja, die DZ CompliancePartner GmbH ist mit ihren Dienstleistungen ein langjähriger verlässlicher Partner unseres Hauses. Insbesondere der Bereich IT-Audit unterstützt uns in vertrauensvoller Zusammenarbeit mit seinen Praktikern über die Auslagerung der IT-Revision seit fast zwanzig Jahren. Die Mitarbeiter sind hoch qualifiziert und bieten im Rahmen der getroffenen Prüfungsfeststellungen auch praktische Lösungsansätze an. >

Durch die Pandemie musste auch die IT-Revision aus dem Homeoffice für Ihre Bank erbracht werden. Wie sah die praktische Umsetzung aus?
A. Arendt: Zunächst wurde in einem Vorgespräch die jeweilige Arbeits- bzw. Ausgangssituation in unserem Hause mit dem Bereich IT-Audit erörtert, um notwendige personelle und räumliche Ressourcen festlegen zu können. Auch wir hatten den größten Teil unserer Mitarbeiter in das Homeoffice geschickt bzw. die vorhandenen Räumlichkeiten auf Einzelpersonen aufgeteilt.

Vor dem Prüfungstermin erhielten wir eine Liste zur Vorbereitung der notwendigen Prüfungsunterlagen. Diese Unterlagen wurden durch ausgewählte Mitarbeiter in einen sicheren, durch die DZ CompliancePartner GmbH eingerichteten virtuellen Raum zur Datenübertragung hochgeladen und so dem IT-Revisor zu den Prüfungshandlungen zur Verfügung gestellt. Sonstige Fragen, Informationen oder fehlende Unterlagen wurden telefonisch geklärt oder per E-Mail übermittelt.

Wie erfolgte das Abschlussgespräch?
A. Arendt: Das Abschlussgespräch wurde mittels einer Telefonkonferenz abgebildet. Im Vorfeld erhielten wir das vorläufige Prüfungsergebnis, sodass wir im Rahmen des Gespräches auf dem aktuellen Informationsstand waren.

Welche Erkenntnisse konnten Sie bei der IT-Prüfung aus dem Homeoffice gewinnen?
A. Arendt: Die diesjährige Prüfung aus dem Homeoffice hat sich als sehr gute Alternative dargestellt. Natürlich ist es ein nicht ganz einfacher Schritt von der Präsenz-Kultur zur Ergebnis-Kultur, aber unser bewährter Partner in Sachen IT-Revision hat diese Krisensituation mit gewohnter Kompetenz gemeistert. Es wurde der volle Service geboten.

Könnten Sie sich vorstellen, auch zukünftig aus dem Homeoffice heraus geprüft zu werden?
A. Arendt: Ich kann mir für die Zukunft Prüfungshandlungen aus dem Homeoffice heraus sehr gut vorstellen. Natürlich sollte der soziale Kontakt vor Ort dadurch nicht vollständig abgebaut werden, allerdings hat diese Prüfungsvariante auch eine finanzielle Komponente. Es reduzieren sich sonst anfallende Reise- und Übernachtungskosten.

Herr Arendt, vielen Dank für das Gespräch!

Ausblick

Die Corona-Pandemie hat uns alle in den letzten Monaten gefordert und beschäftigt uns auch jetzt noch immer. Mit Blick auf die in diesem Zeitraum durchgeführten IT-Prüfung zeigt sich, dass der Prüfungsort nicht grundsätzlich entscheidend ist. **Wichtig ist die Erkenntnis: Prüfen aus dem Homeoffice funktioniert.**

Notwendige Prüfungsunterlagen können sicher und zeitnah zur Verfügung gestellt werden. Die Erstellung der Prüfungsdokumente sowie der Berichtsversand erfolgen elektronisch und Abschlussgespräche können auch über Telkos, GoTo-Meeting oder adäquate Medien durchgeführt werden.

Das Homeoffice erspart beiden Partnern Kosten. Anfahrzeiten verringern sich und dadurch gewonnene Zeiten können intensiver in den Prüfungsauftrag eingebracht werden. Aber Vor-Ort-Kontrollen werden trotz Krise weiter notwendig bleiben. Nicht alle Prüfungshandlungen lassen sich aus dem Homeoffice heraus abbilden. Und auch der soziale Kontakt vor Ort bei den Kunden darf nicht vernachlässigt werden. Eine Kombination aus Homeoffice und Vor-Ort-Tagen schafft eine Win-win-Situation für beide.

Der Bereich IT-Audit der DZ CompliancePartner GmbH wird die gewonnenen positiven Erfahrungen aus dieser Krise im Rahmen eines internen Projektes bewerten und gegebenenfalls in den vorhandenen Prozesskreislauf des Prüfungsalltags zur Erbringung der IT-Revision mit einbinden. ▬

Geldwäsche- und Betrugsprävention

Aktualisierung der Risikoanalyse

Die Erstellung bzw. Aktualisierung der Risikoanalyse in Bezug auf die Prävention von Geldwäsche, Terrorismusfinanzierung und strafbaren Handlungen stellt die Verpflichteten jedes Jahr aufs Neue vor eine große Herausforderung. Zum einen ist dies sehr zeitintensiv, zum anderen müssen neue und aktualisierte (aufsichts)rechtliche Vorschriften regelmäßig beachtet werden.

So waren bei der diesjährigen Aktualisierung der Risikoanalyse insbesondere die Hinweise aus der Ersten Nationalen Risikoanalyse (NRA) sowie die weiteren Faktoren für ein potenziell höheres Risiko aus der Anlage 2 der GwG-Novelle vom 1. Januar 2020 zu berücksichtigen. Dies machte zusätzlich auch eine methodische Überarbeitung der Risikoanalyse erforderlich.

Blicken Sie nachträglich ein wenig „hinter die Kulissen" unserer Arbeit, indem wir Aufbau und Struktur sowie neue rechtliche Grundlagen der Risikoanalyse näher erläutern.

Aufbau und Struktur der Risikoanalyse

Die Auslegungs- und Anwendungshinweise (AuA) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) Stand 05/2020 geben den grundsätzlichen Rahmen der Risikoanalyse vor. Daraus leitet sich eine strukturierte Vorgehensweise zur Erstellung der Risikoanalyse sowie zu deren Nachvollziehbarkeit ab.

Zunächst musste die Gliederung der Risikoanalyse angepasst werden. Diese ist nun nach den einzelnen Risikofeldern strukturiert, anhand derer die konkrete Bewertung der jeweiligen Risikofaktoren ersichtlich wird.

Nachstehende Abbildung zeigt die strukturierte Vorgehensweise mit den einzelnen Prozessschritten auf und konkretisiert diese anhand eines Beispiels.

Bestandsaufnahme und Erfassung der Risiken

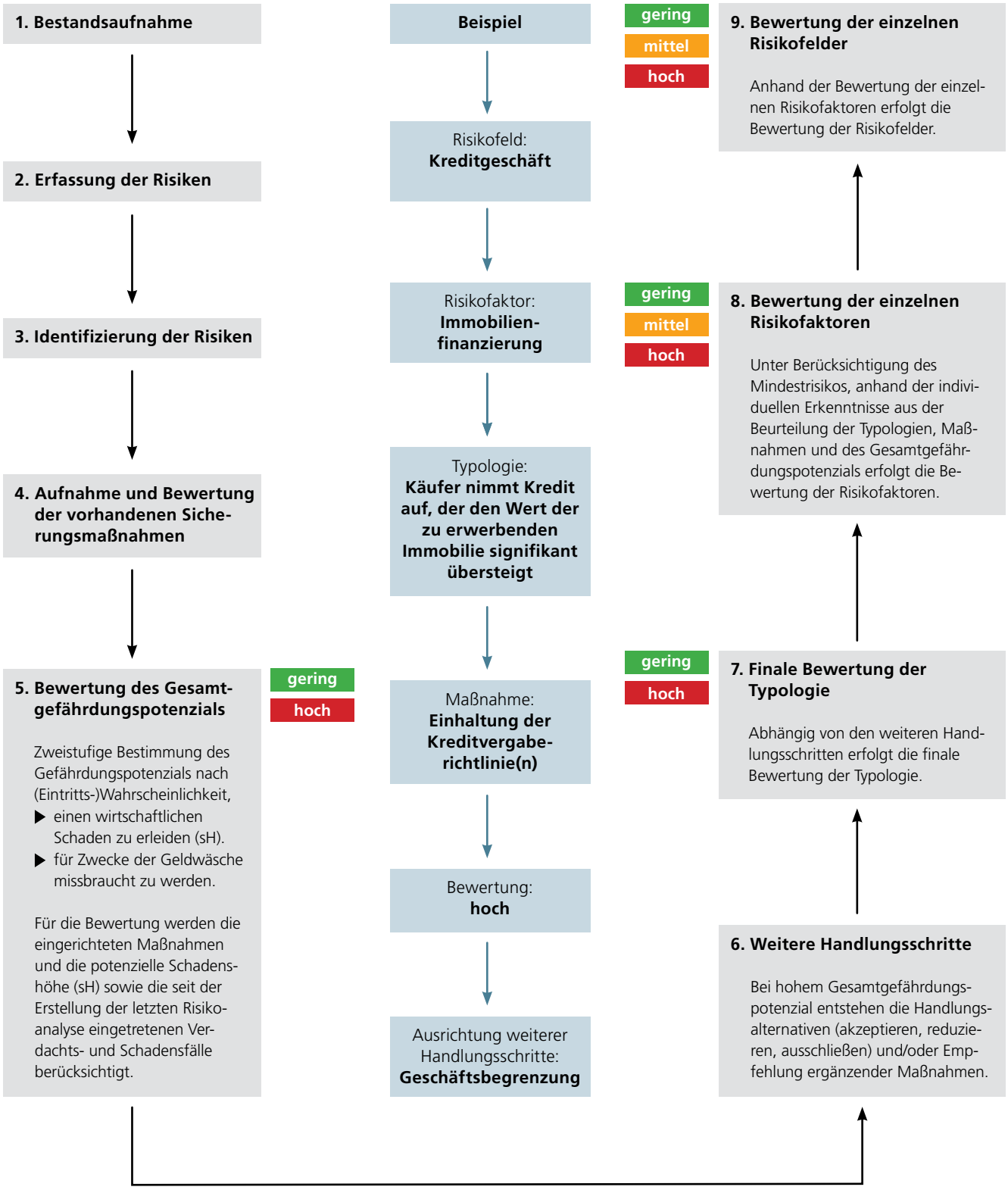
Jede Risikoanalyse startet mit einer umfassenden **„Bestandsaufnahme"** der institutsspezifischen Situation und der **„Erfassung der Risiken"** (Schritte 1 und 2 in der Abbildung). Hierbei sind u. a. folgende Aspekte zu berücksichtigen:

- Geschäftsgebiet
- Produkte und Dienstleistungen
- Erwerbssituation
- Kundenstruktur
- Kriminalität
- Kundensegmente
- Risikoerhöhende Faktoren
- Versicherungsschutz
- Unternehmensstrategie
- Politisch exponierte Personen
- Unternehmenskultur
- Korrespondenzbankbeziehungen
- Gruppenweite Pflichten
- Kundenannahmeprozess
- Organisationsstruktur
- Zahlungsverkehrsstatistiken
- Wirtschaftliche Situation
- Vertriebswege
- Auslagerungen
- Geschäftsbegrenzungen

Zur Bestandsaufnahme nutzen wir eine browserbasierte Anwendung, die Compliance-Management-Plattform (CMP). Dort werden alle institutsspezifisch relevanten Angaben und Risiken anhand eines Fragenkatalogs erfasst bzw. auf ihre Aktualität hin überprüft. Eine Rückschau auf vormals erteilte Antworten ist jederzeit möglich. Das Tool gibt insofern auch die notwendige Revisionssicherheit. Die Einträge werden regelmäßig von dem Geldwäschebeauftragten überprüft bzw. plausibilisiert.

>

DARSTELLUNG DER STRUKTURIERTEN VORGEHENSWEISE



Neben der CMP generieren wir weitere Informationen und Daten über die institutsindividuelle Einstellung des Typologien-Raster-Cockpits in Geno-SONAR®.

Abgerundet wird die Bestandsaufnahme durch folgende zur Erstellung der Risikoanalyse herangezogene Datenquellen:

- Soziodemografische Daten zum Geschäftsgebiet des Instituts
- Interne und Externe Revisionsberichte
- Organigramm des Instituts
- Schadensfall-Übersicht – OP Risik
- Versicherungspolice OP Risk
- Eigene Auswertungen des Beauftragten zum Kundenbestand sowie zum Verdachtspool
- Sonstige externe Datenquellen, wie z. B zur Kriminalitätsstatistik

Identifizierung der Risiken

Ausgehend von der Bestandsaufnahme erfolgt die **„Identifizierung der Risiken“** (Schritt 3 in der Abbildung) in den nachstehenden Risikofeldern, wodurch mögliche Eintrittsszenarien (Typologien) aufgedeckt werden:

- Geografische Risiken
- Unternehmensrisiken
- Produktrisiken
- Transaktionsrisiken
- Kundenrisiken
- Vertriebswegerisiken

Bei diesem Vorgang werden rund 370 Geldwäsche- und 110 Betrugs-Typologien einzeln analysiert und beurteilt.

Den weiteren Ablauf führen wir anhand des beispielhaften Risikoträgers **Kreditgeschäft** näher aus, der bei Kreditinstituten regelmäßig innerhalb des Risikofeldes Produktrisiken einschlägig ist. Das Kreditgeschäft bringt dabei u.a. folgende potenzielle Risiken mit sich:

- Erpressung eines Mitarbeiters zur Erlangung eines Darlehens durch einen Kunden (hier Bewilligung)
- Käufer nimmt Kredit auf, der den Wert der zu erwerbenden Immobilie signifikant übersteigt
- Kunde zahlt Eigenkapital als größeren Betrag in bar ein, ohne dass die Mittelherkunft plausibel und nachprüfbar erklärt werden kann

Aufnahme und Bewertung der vorhandenen Sicherungsmaßnahmen

Anhand der für das Institut relevanten Typologien erfolgt eine Bewertung der relevanten Risiken. Hierbei werden die im Institut **„vorhandenen Sicherungsmaßnahmen“** (Schritt 4 in der Abbildung) berücksichtigt, sofern sich nicht Anhaltspunkte für deren Unwirksamkeit und/oder deren Unangemessenheit ergeben.

Mögliche vorhandene Sicherungsmaßnahmen könnten beispielweise sein:

- Einhaltung der Kreditvergaberichtlinie(n)
- Know-Your-Customer-Prinzip
- Kreditvergabe im Kreditgeschäft in Funktionstrennung
- Sorgfältige Prüfung von Sicherheiten (insbesondere bei Hereinnahme)

Bewertung des Gesamtgefährdungspotenzials

Unter Berücksichtigung der installierten Sicherungsmaßnahmen erfolgt nun eine Bewertung der Risiken und somit des Gesamtgefährdungspotenzials (Schritt 5 in der Abbildung).

Neben den bereits installierten Sicherungsmaßnahmen werden nun weitere Faktoren in die Bewertung einbezogen, wie beispielsweise die potenzielle Schadenshöhe und die zurückliegenden Verdachtsfälle, die im Betrachtungszeitraum aufgetreten sind.

Ebenso werden unterjährig an den Beauftragten gemeldete Schadensfälle, sogenannte „strafbare Handlungen“, bei denen >

AUTOREN UND ANSPRECHPARTNER

Marco Becker
Leiter Geldwäsche- und Betrugsprävention,
E-Mail: marco.becker@dz-cp.de

Dominik Tiburtius
Leiter Geldwäsche- und Betrugsprävention,
E-Mail: dominik.tiburtius@dz-cp.de

- Mitarbeiterinnen und Mitarbeiter des Institutes involviert sind, oder
- bei denen bei Beschäftigten die Zuverlässigkeit im Sinne des § 1 Abs. 20 GwG in Frage zu stellen ist, oder
- bei denen die tatsächliche oder mögliche Schadenshöhe (hierzu zählt auch ein etwaiger Reputationsschaden) 10 % der vom Institut festgelegten Wesentlichkeitsgrenze übersteigt,

bearbeitet und fließen unabhängig von etwaigen Ad-hoc-Maßnahmen in die Erstellung der Risikoanalyse mit ein. Dies geschieht insbesondere vor dem Hintergrund, dass gemäß den gesetzlichen und aufsichtsrechtlichen Bestimmungen solche Fälle in die Betrachtung der strafbaren Handlungen einzubeziehen sind, die zu einer „wesentlichen Vermögensgefährdung" des Instituts führen können.

Weitere Handlungsschritte

Die Ableitung der weiteren Handlungsschritte (Schritt 6 in der Abbildung) basiert auf den Ergebnissen der Risikobewertung und den vorhandenen Sicherungssystemen. Gegebenenfalls werden ergänzende Sicherungsmaßnahmen definiert und Monitoringmaßnahmen angepasst bzw. ergänzt, um nicht ausreichend abgeschirmten Risiken zu begegnen.

Im Falle des Kreditgeschäfts könnten dies bspw. zusätzlich folgende Maßnahmen sein:

- Sorgfältige Prüfung von Sicherheiten (insbesondere bei Hereinnahme)
- Unterrichtung der relevanten Beschäftigten über die Pflichten zur Verhinderung von Geldwäsche und Terrorismusfinanzierung
- Verfahren in Bezug auf zweifelhafte oder ungewöhnliche Sachverhalte

Finale Bewertung der Risikoträger (Typologien, Risikofaktoren und Risikofelder)

Nachdem die jeweiligen Typologien final bewertet wurden (Schritt 7 in der Abbildung), erfolgt anhand dieser eine Bewertung der einzelnen Risikofaktoren (Schritt 8 in der Abbildung) und letztendlich auch des jeweiligen Risikofeldes (Schritt 9 in der Abbildung). Hierzu werden die finalen Bewertungen der Typologien je Risikoträger zusammengefasst und unter Berücksichtigung des Mindestrisikos abschließend beurteilt. Das Mindestrisiko beinhaltet dabei die einschlägigen Aufsichtsrechtlichen Vorgaben. Zu diesem Zweck wird, wie in den Auslegungs- und Anwendungshinweisen der BaFin beispielhaft dargestellt, eine Dreistufigkeit gewählt:

gering Ein geringes Risiko liegt vor, wenn das Geldwäsche- oder Betrugsrisiko unter Berücksichtigung der einschlägigen Vorgaben und der jeweils verbundenen Typologien als gering angesehen wird.

mittel Ein mittleres Risiko liegt vor, wenn das Geldwäsche- oder Betrugsrisiko unter Berücksichtigung der einschlägigen Vorgaben und der jeweils verbundenen Typologien nicht als gering oder hoch angesehen wird.

hoch Ein hohes Risiko liegt vor, wenn das Geldwäsche- oder Betrugsrisiko unter Berücksichtigung der einschlägigen Vorgaben und der jeweils verbundenen Typologien als hoch angesehen wird.

Dieser Schritt dient dazu, anhand der tatsächlich einschlägigen Risiken eine Bewertung über das konkrete Risiko des jeweiligen Risikoträgers für das Institut zu treffen. Gleichzeitig entsteht durch dieses Vorgehen Transparenz über die Risikoträger im Institut. Gleiches gilt für die Aussage des jeweiligen Risikofeldes.

Somit lässt sich für den Leser der Risikoanalyse zusammenfassend erkennen, welche Risiko-„Hotspots" vorhanden sind. Auf Basis der Ergebnisse der Risikoanalyse sowie unter Berücksichtigung der geldwäscherechtlichen Anforderungen werden dann für das laufende Berichtsjahr die weiteren Tätigkeiten und Kontrollhandlungen seitens des Beauftragten geplant. Diese werden in einem Kontrollplan zusammengefasst, der den Instituten nach der Zusendung der Risikoanalyse zur Verfügung gestellt wird.

Inhaltliche Faktoren

In der jüngsten Vergangenheit ergaben sich eine Vielzahl von gesetzlichen Änderungen und wichtigen Publikationen.

So wurde im Oktober 2019 die NRA veröffentlicht, auf die im April 2020 ein Rundschreiben des BVR mit Hinweisen zu den Inhalten der NRA und zur Berücksichtigung in der bankspezifischen Risikoanalyse folgte.
Nach umfassender Analyse haben wir die Erkenntnisse in unsere bestehenden Prozesse implementiert und für die Erstellung der bankspezifischen Risikoanalyse berücksichtigt. Damit verbunden war auch eine vollständige Überarbeitung und Ergänzung aller relevanten Risiken, die wir bereits im Rahmen der Bestandsaufnahme berücksichtigt haben.

So wurden beispielsweise zahlreiche neue Risikoträger geschaffen und die Bewertungsroutinen der vorhandenen Risikoträger aktualisiert.

Daran schloss sich noch die Subnationale Risikoanalyse 2019/2020 der BaFin an, die den Genossenschaftssektor grundsätzlich mit einem mittleren Risiko versehen hat.

Zudem veröffentlichte die Zentralstelle für Finanztransaktionen (FIU) ein Eckpunktepapier (operative Risikoschwerpunkte der FIU im Rahmen der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung) und zu guter Letzt wurde zum 1. Januar 2020 das GwG novelliert. Hierbei wurden u. a. die Risikofaktoren der Anlage 2 (Faktoren für ein potenziell höheres Risiko) überarbeitet, die zwingend bei der Erstellung einer Risikoanalyse berücksichtigt werden müssen.

Fazit

Die Erstellung bzw. Aktualisierung der institutsspezifischen Risikoanalyse muss sowohl die bankindividuellen Gegebenheiten im Hinblick auf die jeweilige Risikolage als auch die aktuellen gesetzlichen und aufrichtrechtlichen Anforderungen berücksichtigen. Wir übernehmen diese Aufgabe für unsere Mandanten und stehen auch anderen Instituten, die die Funktion des Geldwäschebeauftragten nicht an uns ausgelagert haben, gerne beratend zur Seite. ▬

Datenschutz und Informationssicherheit

Virtuelle Jahreshaupt-versammlung

Mit Blick auf die Kontakteinschränkungen ist die virtuelle Hauptversammlung eine viel diskutierte Alternative. Doch welche datenschutzrechtlichen Aspekte sind zu beachten?

Mit der Corona-Notfallgesetzgebung vom 28. März 2020 besteht erstmalig die Möglichkeit, eine Jahreshauptversammlung virtuell – ohne physische Präsenz der Mitglieder oder Aktionärsvertreter – durchzuführen. Hierzu müssen jedoch neben technischen Herausforderungen auch rechtliche Anforderungen, etwa die der Datenschutz-Grundverordnung (DSGVO), bewältigt werden.

Verarbeitung personenbezogener Daten

Im Rahmen der virtuellen Jahreshauptversammlungen werden (in der Regel) über eine Videokonferenzlösung vielfältige Daten gespeichert. Dazu zählen insbesondere die folgenden Daten:

- Konfigurationsdaten der Komponenten
- Benutzerdaten
- Protokolldaten zu durchgeführten Videokonferenzen (typische Metadaten)
- (persistente) Chat-Nachrichten-Dateien, die von den Nutzern in einer Dateiablage gespeichert werden
- Aufzeichnungen von Videokonferenzen

Dabei werden auch personenbezogene Daten gespeichert. Dies trifft insbesondere auf Verbindungsinformationen sowie sämtliche nutzerbezogenen Daten zu.

Die Speicherung der Daten kann in Abhängigkeit von der Architektur und der jeweiligen Komponente, die die Daten speichert, innerhalb der Videokonferenzlösung oder mittels externer Dienste und Speicherorte geschehen. Dabei kann es sich bei den Datensätzen sowohl um flüchtige Daten, die nur während einer Konferenz gespeichert werden, als auch um persistente, d. h. dauerhaft gespeicherte Daten handeln.

Rechtliche Herausforderungen beim Abstimmungsverhalten und bei Fragen durch Teilnehmer

Aus Sicht des Datenschutzes und der Informationssicherheit sind insbesondere Online-Formulare bzw. ähnliche digitale Eingabemöglichkeiten zur Wahrnehmung der Abstimmungs- und Fragerechte zu prüfen.

Dabei ist zu beachten, dass – im Gegensatz zu einer „analogen“ Jahreshauptversammlung – schon beim Stellen einer Frage eine Verarbeitung von personenbezogenen Daten im Sinne der DSGVO vorliegt, da die Frage digital übertragen wird.

Die zugrunde liegende Technik hat damit zwei sich teilweise widersprechende Anforderungen zu erfüllen:

1. Gewährleistung verpflichtender Nachweisbarkeit, etwa der Anwesenheit, aber auch gestellter Fragen, und
2. Gewährleistung von bestehenden Ansprüchen auf Anonymität, etwa bei geheimen Wahlen.

Einhaltung der Datenschutzgrundsätze

Die Datenschutzgrundsätze dienen als allgemeine fundamentale Regeln, die anderen Regeln zugrunde liegen (Art. 5 Abs. 1 DSGVO). Im Rahmen einer virtuellen Jahreshauptversammlung ist entsprechend darauf zu achten, dass die Datenschutzgrundsätze gewährleistet werden und deren Einhaltung auch schriftlich dokumentiert wird. Namentlich sind dies:

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Erfüllung der Anforderungen an die Transparenz
- Zweckbindung der erhobenen Daten
- Datenminimierung
- Garantie der Richtigkeit der Daten
- Speicherbegrenzung
- Integrität und Vertraulichkeit der Daten

Einhaltung der Betroffenenrechte

Im Rahmen der virtuellen Jahreshauptversammlung ist auch darauf zu achten, dass die Rechte der betroffenen Personen gewahrt werden.

Betroffenenrechte regeln das Recht der von der Datenverarbeitung betroffenen Personen. Folgende Aspekte sind zwingend zu berücksichtigen:

- Transparente und vollumfängliche Hinweise gem. Art. 13/14 DSGVO vor Beginn der virtuellen Jahreshauptversammlung
- Erfüllung von Auskunftsansprüchen gem. Art. 15 DSGVO
- Gegebenenfalls die Berichtigung oder Löschung falscher Informationen gem. Art. 16 – 18 DSGVO
- Möglicherweise die Erfüllung des Anspruchs auf Datenübertragbarkeit gem. Art. 20 DSGVO

Vertrag mit dem IT-Dienstleister

Die DSGVO setzt bei der Auslagerung von Aufgaben im Rahmen der Auftragsverarbeitung eine vertragliche Grundlage für die Verarbeitung dieser Daten voraus. Das heißt, wenn ein IT-Dienstleister hinzugezogen wird, sind die entsprechenden Anforderungen des Art. 28 DSGVO in einem Vertrag festzuhalten. Im Rahmen dieser Vereinbarung müssen technische und organisatorische Maßnahmen festgelegt, dokumentiert und überprüft werden.

Vereinfacht ausgedrückt, obliegt es dem Auftraggeber, den IT-Dienstleister sorgfältig auszuwählen. Er muss sich sowohl vor Beginn der Datenverarbeitung (Erstkontrolle) als auch regelmäßig im laufenden Betrieb von der Einhaltung der Veinbarungen überzeugen.

Verzeichnis der Verarbeitungstätigkeiten

Jede Verarbeitung von Daten verpflichtet zum Führen eines Verzeichnisses (DSGVO). Dieses muss u. a. enthalten:

- den Namen und die Kontaktdaten der Verantwortlichen und gegebenenfalls von deren Vertretern sowie eines etwaigen Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind/offengelegt werden,
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1.

Durchführung einer Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung nach DSGVO ist eine Risikomanagementaufgabe und zugleich eine Risikominimierungsverpflichtung. Gegenstand der Datenschutz-Folgenabschätzung ist eine „Form der Verarbeitung“ bzw. ein oder mehrere „Verarbeitungsvorgänge“.

Als einzelne Vorgänge kommen dabei das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten in Betracht (Art. 4 Nr. 2 DSGVO). Es kommen aber auch bestimmte Technologien oder spezielle Hard- oder Software in Frage. >

AUTOREN UND ANSPRECHPARTNER

Dennis Heinemeyer
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: dennis.heinemeyer@dz-cp.de

Michael Switalla
Leiter Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

In der Datenschutz-Folgenabschätzung zur virtuellen Jahreshauptversammlung wäre in einem ersten Schritt zu ermitteln, ob überhaupt eine Datenschutz-Folgenabschätzung erforderlich ist. Hierzu sind in jedem Fall die geplanten Verarbeitungsvorgänge und deren Zwecke zu ermitteln. Zudem muss eine Bewertung des Verfahrens unter Bezugnahme auf die einzusetzende Technologie erfolgen.

Das Bundesamt für Sicherheit in der Informationstechnik rechnet u. a. mit nachfolgenden Gefährdungen bei der Nutzung von Videokonferenzsystemen:

- Abhören von Videokonferenzen
- Manipulation der Signalisierung
- Gezieltes Ausspähen von Räumen
- Verlust der Vertraulichkeit durch Kompromittierung von Video-Endpunkten
- Unzureichende Prüfung der Identität von Kommunikationspartnern
- Fehlverhalten und Missbrauch von Sprachsteuerung und KI-Funktionen
- Missbrauch von Administrations- und Wartungszugängen
- Unzureichendes Identitäts- und Berechtigungskonzept
- Unzureichend abgesicherte Aufzeichnung, Protokollierung und Dateiablage
- Unzureichende Kenntnis von Technik und Regelungen

Technische und organisatorische Maßnahmen

Die DSGVO verlangt auch vom Verantwortlichen die Umsetzung bzw. Kontrolle ausgelagerter geeigneter technischer und organisatorischer Maßnahmen. Vom Begriff der Maßnahme werden alle Handlungen erfasst, die in geeigneter Weise dazu dienen, das auferlegte Ergebnis einer Datenschutzkonformität zu erzielen. Hierzu können z. B. folgende Maßnahmen gehören:

- Hinweise auf Videokameras, Einsehbarkeit aller Personen im Raum
- Verschlüsselung
- Absicherung von Konferenzräumen
- Erstellung eines Rollen- und Berechtigungskonzepts
- Sicherer Umgang mit Konferenzaufzeichnungen
- Schulungen zur sicheren Nutzung von Videokonferenzen

Fazit

Die derzeitige Krise eröffnet insbesondere mit Blick auf virtuelle Jahreshauptversammlungen viele neue Möglichkeiten, aber auch neue rechtliche Herausforderungen. Gerade im Datenschutz sind viele Maßnahmen zum Schutz der Betroffenen zu treffen. Das Auslassen dieser Themen kann schnell zu hohen Geldbußen in Höhe von bis zu 20 Millionen Euro führen. Daher empfehlen wir, das Thema der virtuellen Jahreshauptversammlung mit der nötigen Aufmerksamkeit zu verfolgen und geeignete Maßnahmen zum Schutz der personenbezogenen Daten zu ergreifen. ▬

Weiterführende Informationen

- Leitfaden „Datenschutz in einer virtuellen Jahreshauptversammlung“: https://www.dz-cp.de/dateien/pdf/flyer/leitfaden-datenschutz-in-einer-virtuellen-jahreshauptversammlung
- Überblick über Videokonferenzsysteme: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4

Geldwäsche- und Betrugsprävention

Transparenzregister

Kein Lockdown für unsere Kunden – ein Beispiel aus der Praxis

Das Jahr 2020 hat uns alle vor ungeahnte Herausforderungen gestellt. COVID-19 zwang und zwingt viele Unternehmen aus der altbekannten Routine auszubrechen. Eine Herausforderung, mehr noch, ein Wagnis mit Blick auf das Aufsichtsrecht, dessen Umsetzung eng an definierte Zuständigkeiten mit festgezurrten Prozessen geknüpft ist. Doch wie sich zeigt, sind auch hier praxisbezogene Lösungen möglich.

An dem Beispiel „Transparenzregister" wird deutlich, dass Regulatorik flexibel und kreativ sowie lösungs- bzw. bedarfsorientiert umgesetzt werden kann.

Transparenzregister – Worum geht es?

Mit dem Inkrafttreten des Umsetzungsgesetzes zur vierten EU-Geldwäscherichtlinie Mitte des Jahres 2017 hat der Gesetzgeber auf nationaler Ebene ein zentrales Register geschaffen, in das bestimmte Angaben zu den wirtschaftlich Berechtigten

- juristischer Personen des Privatrechts,
- eingetragener Personengesellschaften und
- bestimmter Rechtsgestaltungen einzutragen sind.

Hierdurch sollen insbesondere Geldwäsche und Terrorismusfinanzierung eingedämmt werden, die vielfach durch verschachtelte Unternehmensstrukturen begünstigt werden. Daher der Name Transparenzregister.

Warum ist das Thema von Banken zu beachten?

Als Verpflichtete im Sinne des Geldwäschegesetzes sind Banken im Rahmen der Erfüllung ihrer Sorgfaltspflichten (§ 11 Abs. 5 Satz 2 GwG) verpflichtet, bei Begründung einer Geschäftsbeziehung mit bestimmten Kunden einen Nachweis der Registrierung nach § 20 Abs. 1 GwG oder § 21 GwG oder einen Transparenzregisterauszug einzuholen. Zusätzlich hat die Bank Prüfungspflichten, die bei Feststellung sogenannter Unstimmigkeiten die verpflichtende Abgabe einer Unstimmigkeitsmeldung auslösen.

Verstöße gegen die Erfüllung der Sorgfaltspflichten stellen eine Ordnungswidrigkeit dar, die sowohl auf Kundenseite (vom Bundesverwaltungsamt) als auch auf Bankenseite (von der BaFin) mit teils hohen Geldbußen geahndet werden kann. Wichtig zu wissen: Das Bundesverwaltungsamt veröffentlicht unanfechtbare Bußgeldentscheidungen auf seiner Internetseite[1].

Herausforderungen für die Banken

Die Banken sehen sich aufgrund der zum 1. Januar 2020 in Kraft getretenen gesetzlichen Regelungen mit inhaltlichen und organisatorischen Herausforderungen konfrontiert.

Die **inhaltlichen Herausforderungen** ergeben sich vor allem im Bereich der Bestimmung des wirtschaftlich Berechtigten. Denn nur wer in diesem Bereich „sattelfest unterwegs" ist, kann letztlich eine sachgerechte Beurteilung im Prozess „Transparenzregister" vornehmen. Weitere Herausforderungen sind mit den Begriffen „Mitteilungsfiktion" und „Leermeldung" verbunden. Was muss eine Bank beispielsweise beim Vorliegen einer Leermeldung tun? Abbildung 1 erläutert den Prozess.

Die **organisatorischen Herausforderungen** liegen vornehmlich in der angemessenen und rechtskonformen Einrichtung eines Prozesses zum Thema Transparenzregister. In der Bank werden mehrere Mitarbeiter/-innen benötigt, die über fundierte Fachkenntnisse verfügen. Die Bank muss organisatorisch in der Lage sein, eine Unstimmigkeitsmeldung **unverzüglich, d. h. ohne schuldhafte Verzögerung (Lies: ohne schuldhaftes Zögern),** abzugeben.

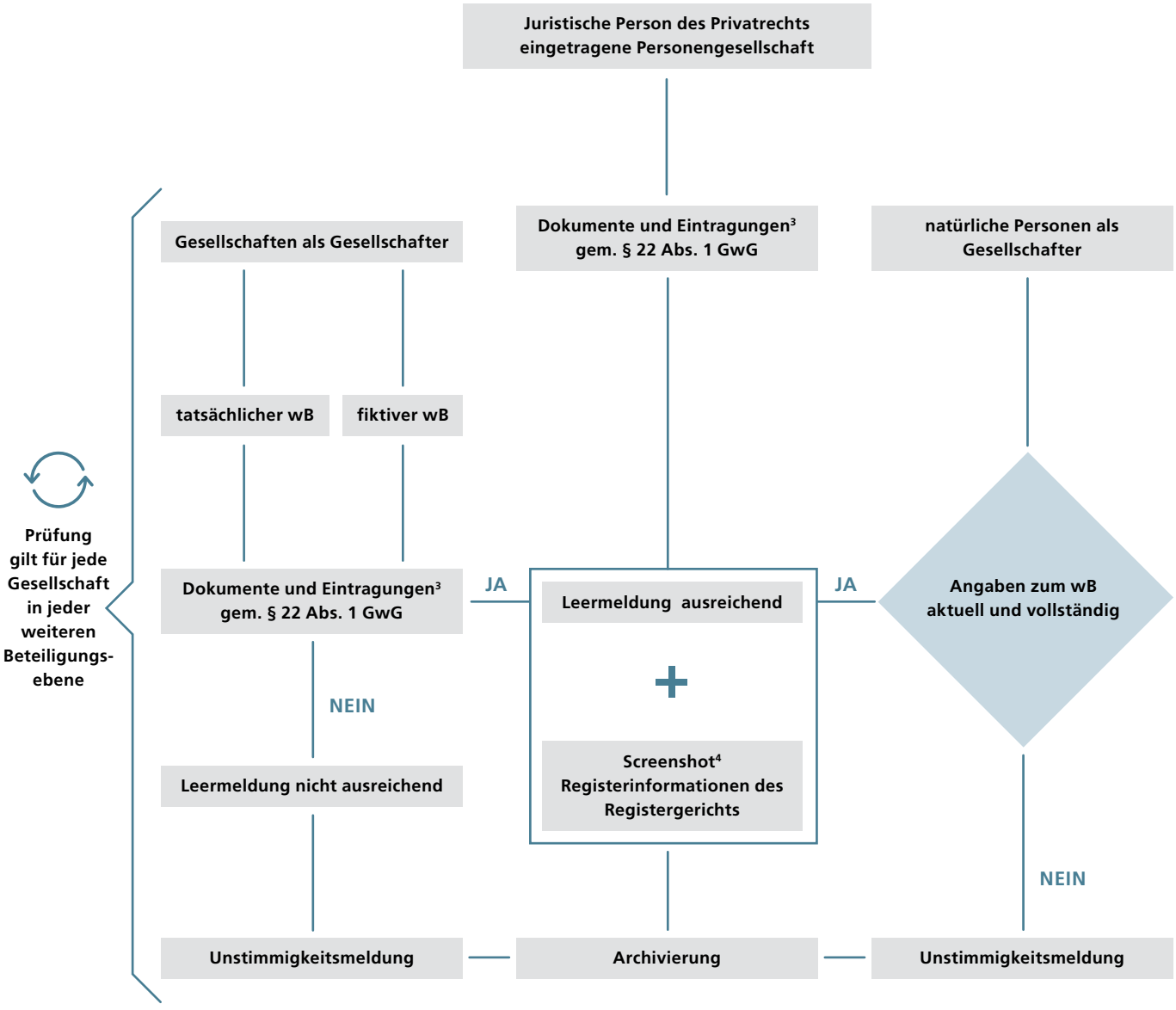
Flexible und bedarfsgerechte Lösungen

Konnten wir unsere ursprünglich als Workshop konzipierte Beratung zum Thema Transparenzregister bis Anfang März dieses Jahres noch persönlich und bei den Banken vor Ort durchführen, so war dies mit dem COVID-19-bedingten Lockdown nicht mehr möglich.

Wir freuen uns sehr, dass wir unmittelbar und ohne zeitlichen Verzug den Schalter von analoger auf digitale Beratung umlegen konnten. >

[1] https://www.bva.bund.de/DE/Das-BVA/Aufgaben/T/Transparenzregister/Bussgeldentscheidungen/bussgeldentscheidungen_node.html;jsessionid=6FA2F23D9FA7F97D823600D966FB54A9.intranet662

1 PROZESS BEI VORLIEGEN EINER LEERMELDUNG[2]



[2] Eine Leermeldung enthält keine Angaben zu den wirtschaftlich Berechtigten (wB).

[3] Die Angaben zu den wirtschaftlich Berechtigten des Kunden müssen elektronisch aus den in § 22 Abs. 1 GwG genannten Quellen (abschließende Aufzählung) abrufbar sein.

[4] Empfehlung, bislang keine Verpflichtung auf rechtlicher Basis

Die Voraussetzungen dafür waren gut:

- Die Dienstleistungserbringung basiert auf einem zeit- und ortsunabhängig abrufbaren Compliance-Management-System.
- Auch organisatorisch ist Homeoffice schon immer ein fester Bestandteil unserer Arbeitsweise,
- Nicht zuletzt ist die Offenheit und Akzeptanz beim Kunden hervorzuheben.

So war es uns möglich, eine qualitativ hochwertige, bedarfsgerechte und auch kostengünstige Dienstleistung für unsere Kunden zu erbringen. Die Präsenzveranstaltungen wurden durch Webinare ersetzt. Mehr noch. Termine konnten viel schneller vereinbart werden. Ergaben sich Änderungen beim Kunden, konnten wir flexibel reagieren. Auch der Workshop-Charakter ging nicht verloren. Viele praxisrelevante Fragen wurden von den Teilnehmern gestellt und durch uns anhand konkreter Fälle erläutert.

Was sagen unsere Kunden? Lesen Sie selbst!

„Das Webinar hat uns viele hilfreiche und vor allem praxisnahe Informationen gegeben. Die Inhalte wurden gut vermittelt und unsere Fragen konnten direkt beantwortet werden. Die Zeit war sehr gut investiert." (Volksbank Brilon-Büren-Salzkotten eG)

„Das von DZ CompliancePartner durchgeführte Webinar zu den neuen Transparenzregisterpflichten brachte uns wichtige Erkenntnisse zur hausinternen Umsetzung. Insbesondere die zahlreichen Praxisfälle, die konkreten Handlungsempfehlungen und die Betreuung im Nachgang lieferten uns einen echten Mehrwert. In Ergänzung zu den veröffentlichten Rundschreiben und Informationen des Bundesanzeigers ist dies absolut empfehlenswert." (Raiffeisen – meine Bank eG, Hilpoltstein)

„Die DZ CompliancePartner GmbH hat uns bei der Einführung eines für uns geeigneten Prozesses bei den Anforderungen des Transparenzregisters gut begleitet. Das kompakte Webinar hat uns – auch in Zeiten von Corona – zielgerichtet das notwendige Wissen an die Hand gegeben, uns unsere Handlungsoptionen aufgezeigt und damit die richtigen Impulse zur schnellen Einführung unseres individuellen Prozesses gegeben."
(VR-Bank Mitte eG)

Als Ihr Dienstleister im Bereich der Geldwäsche- und Betrugsprävention sind wir für Sie da! Sprechen Sie uns gerne an. ▬

AUTOREN UND ANSPRECHPARTNER

Thomas Wagener
Leiter Compliance-Spezialisten,
E-Mail: thomas.wagener@dz-cp.de

Christina Fiedler
Compliance-Spezialistin,
E-Mail: christina.fiedler@dz-cp.de

▶ **Auslagerung**

Was bedeutet Qualität bei Auslagerungen?

Neben monetären Motivationen für eine Auslagerung sind zwei Entscheidungsfaktoren maßgeblich: Kernkompetenzen und Qualität. Der Faktor „Kernkompetenz" unterliegt der gesetzlichen bzw. aufsichtsrechtlichen Normierung und kann daher nicht als Wettbewerbsvorteil aufgebaut werden. Damit bleibt nur die „Qualität" als entscheidender nichtmonetärer Faktor für die Auslagerungsprüfung und -entscheidung übrig. Aber was heißt nun Qualität?

Wie lässt sich Qualität bestimmen oder operationalisieren?

Umgangssprachlich ist die Qualität das Gegenstück zur Quantität. Während Letztere gut messbar ist, bleibt Erstere verschwommen. Meist wird Qualität im Alltag als Gütesiegel gebraucht. Etwas ist von „guter" oder „schlechter" Qualität. Letztlich eine subjektive, individuelle Nutzer- oder Kundenbewertung, die sich nur schwer erfassen oder vergleichen lässt. Das hat zu den Einschätzungen geführt: „Qualität liegt immer im Auge des Betrachters" oder „Qualität ist, wenn der Kunde wiederkommt und nicht die Ware".

Qualitätsmessung ist wie der Versuch, einen Pudding an die Wand zu nageln

Auch ökonomisch wird seit langer Zeit versucht, den Mythos der Qualität zu entschlüsseln. Bereits Henry Ford führte um 1900 eine „Qualitätskontrolle" ein, um fehlerhafte Produkte auszusortieren. Auch die PIMS-Studien (1960er Jahre) und die Vergleichsstudien Japan – USA (1980er Jahre) stellten fest, dass die Qualität ein entscheidender Hebel ist, sich am Markt zu behaupten und erfolgreich zu sein. Das hat national wie international zu einer Konzept- und Wettbewerbs- bzw. Auszeichnungsflut geführt, die bis heute anhält. Six Sigma, EFQM-Modell, TQM-Modell bzw. der Ludwig-Erhard-Preis in Deutschland oder der Malcolm Baldrige National Quality Award in den USA sind nur die prominentesten Beispiele. Letztlich ähneln sich viele dieser Ansätze und Preise, aber sie haben bis heute kein ge-meinsames und allgemein akzeptiertes Verständnis von Qualität hervorgebracht.

Wie erreichen wir trotzdem eine pragmatische und praktikable Definition der Dienstleistungsqualität von Auslagerungen im aufsichtsrechtlichen Beauftragtenwesen?

Eine Definition von Bruhn zur Dienstleistungsqualität im Allgemeinen kommt den genannten Anforderungen nahe. Sie besagt: „Dienstleistungsqualität ist die Fähigkeit eines Anbieters, die Beschaffenheit einer primär intangiblen und der Kundenbeteiligung bedürfenden Leistung gemäß den Kundenerwartungen auf einem bestimmten Anforderungsniveau zu erstellen." Und wenn es sich um aufsichtsrechtliche Dienstleistungen handelt, ist neben den Kundenerwartungen auch die Erfüllung gesetzlicher Pflichten ein unverzichtbarer Qualitätsmaßstab.

Für die Dienstleistungsqualität im aufsichtsrechtlichen Beauftragtenwesen sind also zwei Komponenten entscheidend:

- die Erfüllung der Kundenerwartungen und
- die Erfüllung der gesetzlichen Pflichten.

Und getreu dem Grundsatz „You can only manage what you can measure" muss nun versucht werden, die Kundenerwartungen und gesetzlichen Pflichten operabel und messbar zu machen.

Dienstleistungsqualität für Auslagerungen im Beauftragtenwesen ist konkret messbar, erfahrbar und prüfbar

Dies erfolgt am besten über die Festlegung von sogenannten Service-Levels oder Güte-Vereinbarungen.

Beispielsweise werden für die Auslagerungsdienstleistungen der DZ CompliancePartner GmbH für drei Segmente solche Gütekriterien vorgegeben:

1. Erstellung und Lieferung von Berichten und Dokumenten
2. Durchführung von Vor-Ort-Kontrollen
3. Durchführung von Web Based Trainings/Schulungen

Die erste Gruppe ist die umfangreichste und größte Gruppe. In ihr werden insgesamt bis zu 13 unterschiedliche Berichte und Dokumente aufgezählt. Für jedes Dokument wird festgelegt, wie oft es im Jahresverlauf erstellt wird und bis wann es dem Kunden geliefert wird.

Die 13 Berichte und Dokumente beleuchten dabei jeweils die Auslagerungsdienstleistung aus drei unterschiedlichen Perspektiven:

- aus der prozessualen Sicht des externen Beauftragten (Risikoanalysen, Quartalsberichte, Tätigkeits- und Jahresberichte, Ad-hoc-Berichte),
- aus der Sicht des gesamten Unternehmens (Prüfungsberichte der internen Revision, IT-Revision, Quartals- und Risikoberichte, Notfallvorsorgekonzept),
- aus der Sicht von externen Prüfern (Bescheinigung nach IDW PS 951 und/oder PS 331 und/oder PS 880).

Die zweite Gruppe legt fest, wann mit Routinekontrollen zu rechnen ist und wann mit „Gefahr-in-Verzug-Kontrollen".

Und die dritte Gruppe dokumentiert die zeitliche Verfügbarkeit von Web Based Trainings/Schulungen für jeden Bankarbeitstag.

Damit wird die Dienstleistungsqualität für Auslagerungen konkret messbar, erfahrbar und prüfbar. Und damit auch eine wesentliche Anforderung aus den MaRisk für das zentrale Auslagerungsmanagement erfüllt. In AT 9 Satz 13 wird gefordert, dass eine „ institutsinterne Bewertung der Dienstleistungsqualität der Auslagerungsunternehmen" zu erfolgen hat und „eine Aussage darüber zu treffen ist, ob die erbrachten Dienstleistungen der Auslagerungsunternehmen den vertraglichen Vereinbarungen entsprechen".

Diese Aussage zu treffen, dürfte mit der Vielzahl der vorgestellten Kriterien problemlos möglich sein.

Vergleich Eigenfertigung – Auslagerung

Um nun die Qualität der Eigenfertigung mit jener der Auslagerung vergleichen zu können, sollten ähnliche Bewertungsmaßstäbe auch an die hauseigene Erbringung von aufsichtsrechtlichen Beauftragtenfunktionen angelegt werden.

Ein umfassender Vergleich von eigener und gekaufter Beauftragtenleistung berücksichtigt sowohl monetäre als auch nichtmonetäre Faktoren.

AUTOR UND ANSPRECHPARTNER

Martin Hierlemann
Leiter Vertrieb,
E-Mail: martin.hierlemann@dz-cp.de

Beispielsweise wäre am konkreten Beispiel der WpHG-Compliance-Funktion zu prüfen, was die eigene Erstellung im Vergleich zur gekauften Leistung kostet.

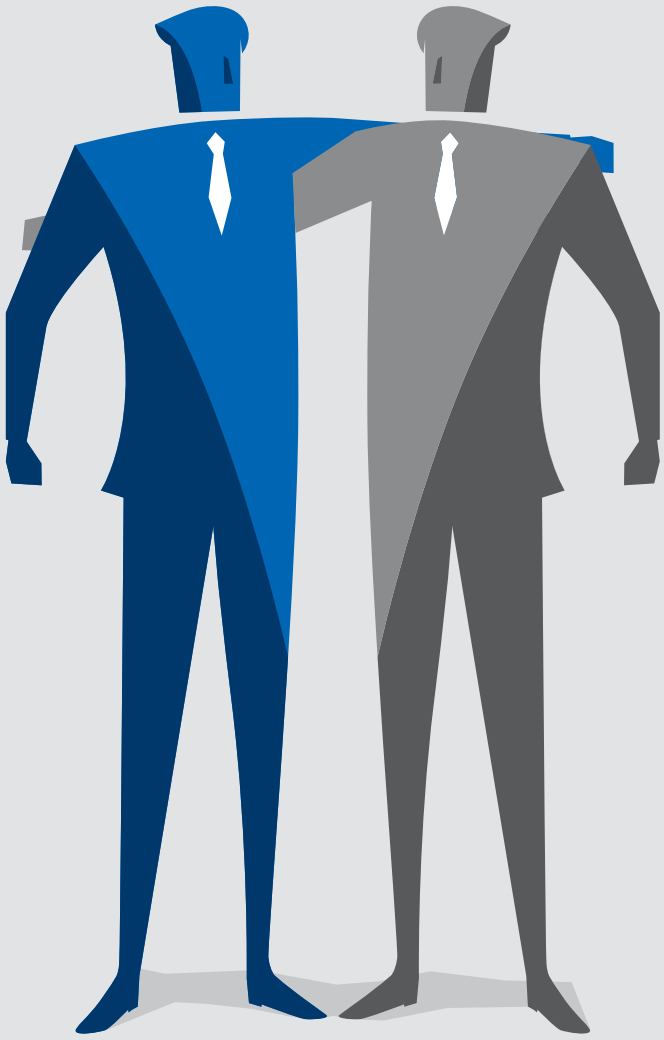
Ergänzt werden muss dieser Preis-Check aber durch den Qualitäts-Check. Welche Qualität erhalte ich bei der Selbsterstellung der WpHG-Compliance-Funktion und welche bei der zugekauften Leistung?

Erst wenn beide Komponenten, Preis und Qualität, berücksichtigt werden, kann eine fundierte und nachvollziehbare Entscheidung zur Gestaltung von aufsichtsrechtlichen Beauftragtenfunktionen in der Bank getroffen werden.

Messbare Qualitätskriterien sind also das unverzichtbare zweite Standbein für den Vergleich Eigenfertigung versus Auslagerung. Denn bekanntlich steht man auf zwei Beinen länger, sicherer und komfortabler als auf einem Bein. ▬

In eigener Sache

CompliancePartner vor, während und nach Corona



Sicherheit und Gesundheitsschutz haben seit dem Beginn der Corona-Pandemie oberste Priorität. Dabei kommt uns eine dezentrale und auch weitgehend digitalisierte Arbeitsorganisation zugute: Unsere Mitarbeiter und Mitarbeiterinnen können nahezu ohne Einschränkungen aus dem Homeoffice heraus arbeiten. Gleichzeitig nutzen wir in Abstimmung mit den Kunden und natürlich unter Beachtung der notwendigen Hygiene- und Abstandsregeln die aktuellen Lockerungen, um Vor-Ort-Kontrollen und auch -Beratungen durchzuführen.

Aufsichtsrecht

Grundsätzlich zeichnen sich mit Blick auf das Aufsichtsrecht Erleichterungen in Bezug auf Durchführung, Dokumentationen und Meldungen für den Zeitraum Corona-bedingter Einschränkungen ab. Fristen laufender Verfahren werden „ausgedehnt“ und Termine vertagt. Im Bereich Geldwäscheprävention wird angeregt, die „Flexibilität des von der FATF angewendeten risikoorientierten Ansatzes bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu nutzen“. Novellierungsarbeiten, wie z. B. bei den MaRisk, werden zwar nicht ausgesetzt, aber die BaFin hat klargestellt, dass die neuen Vorgaben nicht zum Stichtag 31. Dezember 2020 gelten und auch nicht für das Jahr 2020 prüfungsrelevant sein werden[1]. Insgesamt ist also erkennbar,

dass die Aufsicht sich zu einer gewissen „Entspannung“ der Lage verpflichtet fühlt.

Wir begrüßen die Maßnahmen, nehmen aber auch eine gewisse Überforderung infolge einer Gesetzes-, Verordnungs-, Auslegungs- und Hinweisflut wahr.

Fakt ist, gerade weil

- sich mit und in der Krise die Arbeitsorganisation (Stichwort Informationssicherheit & Datenschutz) und auch das Marktverhalten ändern (Stichwort WpHG-Compliance),
- die Bundesregierung mit den Gesetzen zur Abmilderung der Pandemiefolgen den Banken besondere Aufgaben zuweist und
- neue Betrugsmuster (Stichwort Geldwäsche- und Betrugsprävention) auftreten,

wird jenseits aller Erleichterungen eine erhöhte Aufmerksamkeit – auch aufsichtsrechtlich – eingefordert. Eine besondere Herausforderung in allen Beauftragtenthemen sehen wir dabei

- in der Etablierung neuer, aufsichtskonformer Prozesse und Organisationen,
- in der Abarbeitung de facto steigender Verdachtsfälle/Treffer sowie
- in der zeitnahen Anpassung der Risikoszenarien und damit auch der Risikoanalysen.

Ein Beispiel unter vielen für „Corona-bedingten Mehraufwand“ ist die Warnung des LKA NRW vom 15. April 2020 im Zusammenhang mit der Beantragung von Corona-Soforthilfe-Zahlungen: Das Land NRW hatte eine Internetseite zur Beantragung von Soforthilfen eingerichtet, die von einer inkriminierten Webseite nachgeahmt wurde. Dadurch kamen Betrüger an Unternehmensdaten, die zu kriminellen Zwecken genutzt werden konnten. In der Folge wies die BaFin darauf hin, dass bestimmte – neue – Verdachtskriterien auf eine möglicherweise betrügerisch erwirkte Auszahlung von Geldern durch die Bezirksregierungen NRW an Unberechtigte hindeuten könnten. In diesen Fällen wurde eine Prüfung der Zahlung angeregt, was wiederum zu einer Vielzahl von zu bearbeitenden Treffern führte.

Fragen zu unseren Corona-bedingten Maßnahmen beantwortet Ihnen gerne Ihr Beauftragter; allgemeine Informationen finden Sie darüber hinaus auch auf unserer Homepage unter https://www.dz-cp.de/ueber-uns/presse

Mehrmandantenansatz als Chance

In der Krise hat sich der Mehrmandantenansatz in allen Beauftragtenthemen – in der Geldwäsche- und Betrugsprävention, in der Informationssicherheit und dem Datenschutz, der MaRisk- und WpHG-Compliance und der IT-Audit – bewährt.

Der konsequent prozess- und risikoorientierte Steuerungsansatz ist nicht nur belastbar, sondern auch außerordentlich flexibel: Neue oder angepasste Anforderungen können nahezu reibungslos integriert werden. Dabei spielt auch der hohe Digitalisierungsgrad eine entscheidende Rolle: Er ist die Basis für eine zügige, transparente und nachvollziehbare Umsetzung.

Einen wesentlichen Vorteil haben unsere Kunden auch durch die Bündelung des Wissens – immerhin das Wissen und die Erfahrung aus über 700 Mandaten – in einem Dienstleister erfahren: Gerade in Krisenzeiten ist eine schnelle, fundierte Orientierung entscheidend, um den Überblick zu erhalten.

Schlussendlich offenbart sich in der Krise, wie wichtig es ist, eine Stimme zu haben, das heißt, überhaupt gehört zu werden. Wir haben in den vergangenen Monaten in nahezu allen Bereichen sowohl mit den Verbänden als auch mit der Aufsicht „gangbare Wege“ abstimmen können. Der Nutzen dieser Gespräche liegt teilweise in konkreten Entlastungen. Wichtiger aber ist fast, dass diese Gespräche zu Klarheit, einem gemeinsamen Verständnis und damit letztlich auch zu mehr (Umsetzungs-)Sicherheit führen.

Internes Projekt

Die gemachten Erfahrungen haben uns ermutigt, den Mehrmandantenansatz, die Standardisierung und Automatisierung noch einmal zu hinterfragen und auch weiter auszubauen. Intern haben wir dazu ein Projekt aufgesetzt, in dem die Erfahrungen und Effekte der letzten sechs Monate gesammelt und analysiert werden. Ziel ist es, sowohl fachlich als auch betriebswirtschaftlich jene Maßnahmen in den Teilprojekten „Aufsichtsrecht“, „Kundenbedarf“ und „Mitarbeiter“ zu identifizieren, die nun weiter ausgebaut werden sollen bzw. müssen.

Wenn Sie Anregungen haben oder uns in diesem Zusammenhang ein Feedback geben möchten, freuen wir uns sehr, gerne per Mail über poc@dz-cp.de oder aber über Ihren Beauftragten. (red.)

[1] https://www.bafin.de/DE/Aufsicht/CoronaVirus/CoronaVirus_node.html

Informationssicherheit

ISI kompakt – Update

Erweiterter Funktionsumfang und Umsetzung aufsichtsrechtlicher Anforderungen: Neu ist die Darstellung der Recovery Time Objective, des Schutzniveaus, einer möglichen Unterdeckung und die Wiedervorlage.

Die Corona-Zeit wurde intensiv genutzt, um weitere Funktionen und Ansichten zu ergänzen, aber auch die aufsichtsrechtlichen Anforderungen bestmöglich umzusetzen. So ist ISI kompakt eines der ersten Tools, das auch die seitens der BAIT in den Erläuterungen Tz. 46 geforderte Bewertung des maximal tolerierbaren Datenverlusts (RPO) bietet.

RPO – RTO

Die Recovery Point Objective (RPO) ist Bestandteil der Business-Impact-Analyse (BIA) zur Bewertung der Verfügbarkeit eines Geschäftsprozesses. Die RPO betrachtet für ein IT-System oder eine IT-Infrastruktur den Zeitraum, der maximal zwischen zwei Datensicherungen liegen darf. Im Prinzip geht es hier also um die Frage, wie viele Daten oder Transaktionen zwischen der letzten Sicherung und einem Systemausfall höchstens verloren gehen dürfen.

Andererseits gilt es in der Business-Impact-Analyse, die maximal tolerierbare Ausfallzeit (RTO) zu berücksichtigen.

Die Recovery Time Objective (RTO) beschreibt die benötigte Zeit für den Wiederanlauf eines Geschäftsprozesses im Rahmen eines Notfalls. Also: Wie viel Zeit darf vergehen, bis nach einem Ausfall eines Geschäftsprozesses wieder der Normalbetrieb hergestellt ist und auf die Daten zugegriffen werden kann?

Die Darstellung in ISI kompakt erfolgt über die doppelte Anzeige der Verfügbarkeit („A“ = Availability) bei der Darstellung des Schutzbedarfs sowie des Schutzniveaus. Die übrigen Buchstaben stellen die weiteren Bestandteile der Schutzbedarfseinstufungen dar für die Schutzziele Vertraulichkeit (C = Confidentiality), Integrität (I = Integrity) und Authentizität/Verbindlichkeit (N = Non repudiation).

Im Beispiel (Tabelle 1) wird die Verfügbarkeit mit A1:3 bewertet. Dies ist wie folgt zu interpretieren:

- Der erste Teil vor dem Doppelpunkt stellt – wie bisher in ISI kompakt ausgewiesen – die RTO dar, hier A1 = 1 Woche maximal tolerierbare Ausfallzeit.
- Der zweite Teil nach dem Doppelpunkt stellt – und dies ist neu – die RPO dar, hier 3 = 1-4 Stunden darf der Zugriff auf die Daten maximal ausfallen.

Erreichtes Schutzniveau

Ein weiteres Novum ist die Darstellung des Umsetzungsstands der relevanten Sicherheitsmaßnahmen bei den einzelnen Objekten in ISI kompakt. Aus den zugeordneten Maßnahmen wird unter Berücksichtigung der vollständig umgesetzten Maßnahmen eine entsprechende Umsetzungsquote ermittelt. Aus dieser Quote kann direkt abgelesen werden, bei welchen Objekten noch Bedarf hinsichtlich der Bearbeitung bzw. Umsetzung der relevanten Sicherheitsmaßnahmen besteht.

Im Rahmen des Abgleichs des erforderlichen Schutzniveaus mit dem Schutzbedarf, also den geforderten Sicherheitsmaßnahmen, wurde bislang in einigen Fällen eine Differenz ausgewiesen: Die umgesetzten Maßnahmen reichten nicht aus, um den Bedarf an Sicherheit, den die Bank in dem Schutzniveau darstellt, zu decken.

TABELLE 1

Schutzbedarf	Schutzniveau	Unterdeckung	Schutzniveau (E)	Quote
A1:3 C3 I2 N2	A3:4 C3 I3 N3	–	A3:4 C3 I3 N3	100 % 31/31

TABELLE 2

Schutzbedarf	Schutzniveau	Unterdeckung	Schutzniveau (E)	Quote
A1:3 C3 I2 N2	A3:4 C3 I3 N3	–	A3:4 C3 I3 N3	100 % 31/31
A1:3 C3 I2 N2	A3:4 C2 I2 N2	C3 I3 N3	A3:4 C3 I3 N3	81 % 25/31

Unklar war dabei häufig,

- ob einfach nur offene Maßnahmen nicht in der Bank umgesetzt wurden, oder
- ob die zugeordneten Maßnahmen nicht ausreichen, um das Schutzniveau mit dem Schutzbedarf in Einklang zu bringen.

Mit der Darstellung des erwarteten Schutzniveaus („Schutzniveau (E)“) bietet ISI kompakt nun die Möglichkeit, bereits anhand der noch zu bearbeitenden Maßnahmen zu erkennen,

- ob eine Unterdeckung beseitigt werden kann, oder
- ob noch weitere Maßnahmen getroffen werden müssen.

Das erwartete Schutzniveau ermittelt sich aus den für das jeweilige Objekt relevanten Maßnahmen und zeigt das Schutzniveau an, das erreicht werden kann, wenn sämtliche für das Objekt relevanten Maßnahmen in der Bank umgesetzt werden. Im Beispiel (Tabelle 2) wurden bei einer Erfüllungsquote von 100 % sämtliche 31 von 31 relevanten Maßnahmen in der Bank umgesetzt (Zeile 1).

Im zweiten Fall wurden bisher nur 25 Maßnahmen von 31 Maßnahmen in der Bank umgesetzt. Dies entspricht einer Erfüllungsquote von ca. 81 % (Zeile 2). Es ist aber durch das erwartete Schutzniveau („Schutzniveau (E)“) erkennbar, dass die derzeit ausgewiesene Unterdeckung durch die weitere Umsetzung der noch offenen bzw. nicht vollständig erfüllten Maßnahmen geschlossen werden kann.

Unterdeckung

Nicht immer können sämtliche Maßnahmen in der Bank tatsächlich umgesetzt werden. Auch Kosten-Nutzen-Aspekte spielen häufig eine Rolle.

In einer neu gestalteten Ansicht sehen Sie nun, bei welchen Objekten das aufgrund der Maßnahmenumsetzung im Haus erreichte Schutzniveau nicht für den Schutzbedarf ausreichend ist, also eine Unterdeckung besteht (siehe Tabelle 3, Zeile 2).

Wenn Sicherheitsmaßnahmen eine Unterdeckung nicht abwenden können, ist dies regelmäßig entsprechend zu kommentieren bzw. zu dokumentieren. Das gilt insbesondere dann, wenn die hinterlegten Maßnahmen auch bei einer vollständigen Bearbeitung bzw. Umsetzung nicht ausreichen, um die Unterdeckung zu beheben. Damit wird die Unterdeckung zwar nicht aufgehoben. Aber über eine Begründung kann und muss dokumentiert werden, weshalb trotz der bestehenden (theoretischen) Unterdeckung das Schutzobjekt weiterhin eingesetzt wird. >

TABELLE 3

Schutzbedarf	Schutzniveau	Unterdeckung	Schutzniveau (E)	Quote
A1:3 C3 I2 N2	A3:4 C3 I3 N3	–	A3:4 C3 I3 N3	100 % 31/31
A1:3 C3 I2 N2	A3:4 C2 I2 N2	C3 I3 N3	A3:4 C3 I3 N3	81 % 25/31

Sollte aufgrund neuer Maßnahmenumsetzungen die Unterdeckung entfallen, so wird der Kommentar automatisch archiviert und zukünftig nicht mehr in der Ansicht angezeigt.

Wiedervorlage

Unabhängig von dem in der Bank für das Informationssicherheitsmanagement genutzten Standard ist eine regelmäßige Überprüfung des Informationssicherheitsmanagementsystems erforderlich. Sowohl der SOIT als auch das BSI oder die ISO 27001 fordern einen entsprechenden Regelkreislauf.

Mit ISI kompakt ist die technische Möglichkeit für die Abbildung eines Regelkreislaufs gegeben.

In den Vorgaben kann festgelegt werden, wie die Wiedervorlage mandantenindividuell ausgestaltet wird. Sowohl der Wiedervorlageturnus für Prozesse, Objekte und Objektmaßnahmen als auch die Frequenz der Erinnerungen an den Prozesseigentümer bzw. Verantwortlichen kann individuell eingestellt werden.

Damit sich der Aufwand zur Bearbeitung der Wiedervorlagen im Rahmen hält, gibt es in ISI kompakt jetzt auch die Möglichkeit, mit Hilfe des Buttons „Bestätigen“ die Richtigkeit eines Prozesses, eines Objektes bzw. einer Maßnahmen zu bestätigen. Dies kann im Rahmen der Wiedervorlagen auch über mehrere Objekte, Maßnahmen und Prozesse hinweg erfolgen: schnell und unkompliziert mit einem Klick.

AUTOREN UND ANSPRECHPARTNER

Michael Switalla
Leiter Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

Marc Hübner
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: marc.huebner@dz-cp.de

Ausblick

Die Arbeiten an ISI kompakt sind bei weitem noch nicht abgeschlossen. Informationssicherheit lebt und erfährt stetig Änderungen. Entsprechend wird ISI kompakt weiterentwickelt: Einerseits bedingt durch die regelmäßige Aktualisierung des Standards für Ordnungsmäßigkeit der IT-Verfahren der Fiducia & GAD (SOIT) oder der Einführung des Sicherheitsmaßnahmenkatalogs der Fiducia & GAD (SiMaKat). Andererseits veranlasst durch Anregungen, die uns von Anwendern oder Prüfern erreichen. ▬

Interne Revision

Seit der letzten Berichterstattung in der Point of Compliance (1/2020, S. 23) wurde entsprechend der Jahresprüfungsplanung 2019 der Bericht für den Bereich „IT-Audit“ an die Mandantschaft verschickt. Nach der Jahresprüfungsplanung 2020 wurden Berichte zu den Prüffeldern „Hinweisgebersystem“, „Vertriebsmanagement“, „WpHG-Compliance“, „Fakturierung von Debitorenrechnungen“ und „MaRisk-Compliance“ abgeschlossen und veröffentlicht.

Die Berichte zu den Bereichen „Hinweisgebersystem“, „WpHG-Compliance“ und „MaRisk-Compliance“ wurden jeweils als dienstleistungsbezogene Berichte an unsere Mandantschaft versandt.

Der Jahresbericht der Internen Revision für 2019 und die Quartalsberichte zum ersten und zweiten Quartal 2020 wurden turnusgemäß erstellt und ebenfalls unserer Mandantschaft zur Verfügung gestellt.

Die externe Prüfung der Geschäftsbereiche „MaRisk-Compliance“, „WpHG-Compliance“ und „Geldwäsche- und Betrugsprävention“ nach IDW PS 951 (Typ 2) sowie die externe Prüfung der Geschäftsbereiche „Datenschutz“ und „Informationssicherheit“ nach IDW PS 951 (Typ 1) wurde von der AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft vorgenommen und an die Mandantschaft versandt.

Die externe Prüfung der Funktion „Hinweisgebersystem“ nach IDW PS 331 erfolgt ebenfalls durch die AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft. Auch hier wurde der Prüfungsbericht bereits versandt.

Für das Softwareprodukt „Auslagerungsmanagement kompakt“ erfolgte eine Zertifizierung nach IDW PS 880 durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft. Die Bescheinigung wurde an die Kunden dieses Produkts versandt.

Darüber hinaus wurde turnusgemäß je ein Follow-up-Quartalsbericht für das erste und zweite Quartal 2020 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Maßnahmen/Empfehlungen dokumentiert. Offene Punkte werden durch die Interne Revision konsequent nachgehalten.

Als weiterer Informationsaustausch finden zwischen dem Sprecher der Geschäftsführung der DZ CompliancePartner GmbH und der Internen Revision regelmäßige Jours fixes statt. ▬

Ansprechpartner: ***Lars Schinnerling,*** *Leiter Interne Revision, E-Mail: lars.schinnerling@dz-cp.de*

Wirtschaftliche Lage

Das Halbjahresergebnis der DZ CompliancePartner GmbH liegt bei +516 T€ (vor Steuern) und damit –184 T€ unter Plan. Die starken Kontaktbeschränkungen der Monate März bis Mai/Juni führten zu einem Rückgang der Vor-Ort Präsenz, die nur teilweise durch elektronische Medien ersetzt werden konnte. Unter anderem hierdurch wurden –318 T€ weniger Erträge im ersten Halbjahr erzielt als geplant (7.631 T€ im Ist zu 7.949 T€ im Plan). Zwar konnten auch die Kosten gesenkt werden (–7.110 T€ im Ist zu –7.249 T€ im Soll), durch die Einsparungen konnten die Erlösrückgänge jedoch nicht vollends kompensiert werden.

Es wird erwartet, dass im zweiten Halbjahr Aufholeffekte realisiert werden können. Deren Höhe ist jedoch vom Fortgang der Corona-Pandemie abhängig. Zur Ertragssicherung hat die DZ CompliancePartner GmbH ein Projekt zur weiteren Entwicklung geeigneter und kundenorientierter Instrumente in der „neuen Normalität“ aufgesetzt.

Die Risikosituation der DZ CompliancePartner GmbH wird durchgehend als „gering“ bewertet. Auch die Folgen der Corona-Pandemie konnten durch Homeoffice-Regelungen aufgefangen werden; die Fortführung des ordentlichen Geschäftsbetriebs wurde durch die Kontaktbeschränkungen nicht beeinträchtigt. Vor-Ort-Termine wurden entweder verschoben oder durch elektronische Instrumente ersetzt. Die regulativ vorgegebenen Aufgaben und Kontrollmaßnahmen konnten sicher erbracht werden. ▬

Ansprechpartner: ***Jens Saenger,*** *Sprecher der Geschäftsführung, E-Mail: jens.saenger@dz-cp.de*