DZ CompliancePartner

Point of Compliance

Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner

AUSGABE 1/2020

Beauftragten-wesen 2020

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 22, 1/2020
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:
Thomas Grebe, Axel Hofmeister, Silke Lenhart, Marc Linnebach, Jörg Scharditzky, Björn Scherer, Lars Schinnerling, Thomas Schröder, Dominik Tiburtius, Benjamin Wellnitz.

Bildnachweise: DZ CompliancePartner GmbH, iStockphoto (Titel, Seite 6, Seite 21)
Gestaltung: EGENOLF DESIGN, Wiesbaden, studio@egenolf-design.de
Druck: odd GmbH & Co. KG · Print und Medien, www.odd.de

Redaktionsschluss: 14. Februar 2020
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.dz-cp.de/poc

Chancen sind jene Faktoren,

die einen positiven Einfluss auf den Erfolg haben können und somit ein unternehmerisches Handeln nahelegen. Risiken dagegen zwingen Unternehmen zum Handeln, da sie den Erfolg gefährden können.

Jens Saenger
Sprecher der Geschäftsführung

In 2020 werden Chancen und Risiken nah aneinanderrücken. So ist die Digitalisierung ohne Zweifel eine Chance, doch in ihrer Komplexität birgt sie Gefahren. Andererseits macht der bewusste Umgang mit ebendiesen Risiken den Unterschied zwischen traumtänzerischer Unbedarftheit und verantwortungsvollem Handeln. Und auch die Nachhaltigkeitsdebatte – samt der ESG-Kriterien Environmental, Social und Governance – verweist auf immense Unsicherheitsfaktoren und öffnet doch zugleich neue Perspektiven.

Das Beauftragtenwesen, namentlich der risikoorientierte, präventive Ansatz, wird vor diesem Hintergrund zum Erfolgsfaktor. In 2020 wird das Beauftragtenwesen mehr denn je in gesamtunternehmerische Aufgabenstellungen eingebunden sein. Der Umgang mit Betrugs-, Datenschutz- oder IT-Risiken wird zur Chance in einer Gesellschaft im Umbruch. Hier sehen wir unseren Beitrag, um Ihre Position vor Ort zu stärken.

In diesem Sinne wünsche ich eine spannende Lektüre.

Ihr Jens Saenger

Geldwäsche- und Betrugsprävention

Kundendatenaktualisie

Mit der Vierten EU-Geldwäscherichtlinie sind die Anforderungen zur Aktualisierung der Kundendaten signifikant angestiegen. Konnte bislang zwischen einem anlassbezogenen und einem periodischen Ansatz gewählt werden, sind Kundendaten künftig sowohl anlassbezogen als auch periodisch auf ihre Aktualität zu überprüfen.

2014 war die Welt der Kundendatenaktualisierung vergleichsweise einfach und gleichzeitig eindeutig. Damals sahen die „Auslegungs- und Anwendungshinweise der Deutschen Kreditwirtschaft zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und ‚sonstigen strafbaren Handlungen'" (DK-Hinweise) vor, dass die Aktualisierung der Kundendaten entweder anlassbezogen oder periodisch erfolgen konnte. Gleichzeitig wurde ein Mindestmaß an Kundendaten festgelegt, die entsprechend zu aktualisieren waren. Hierbei handelte es sich „nur" um Name, Adresse und, sofern vorhanden, wirtschaftlich Berechtigte des Kunden.

Statt „Entweder-oder"

Der **anlassbezogene Ansatz** stellte stark auf die tatsächliche Aktualität der Kundendaten ab bzw. auf Hinweise, dass Aktualisierungsbedarf besteht. Die Institute hatten hierdurch laufenden Aufwand, mussten sich aber zu keiner Zeit projektmäßig mit diesem Thema auseinandersetzen. Einzige Voraussetzung, damit dieser Ansatz verfolgt werden konnte, war, dass die entsprechenden Daten alle vorhanden waren. Etwaige fehlende wirtschaftlich Berechtigte aus dem Altbestand mussten sofort aufgearbeitet werden. In den DK-Hinweisen wurden seinerzeit einige Anhaltspunkte für mögliche anlassbezogene Aktualisierungsmaßnahmen definiert:

- Anzeige von Veränderungen der Kundendaten durch die Vertragspartner im Rahmen der Mitwirkungspflicht nach GwG bzw. AGB (Kunde meldet Änderungen von diversen Daten)
- Auffälligkeiten im Rahmen der kontinuierlichen Überwachung
- Erkenntnisse aus der laufenden Geschäftsbeziehung (beispielsweise im Rahmen der allgemeinen Korrespondenz, in Form von Saldenmitteilungen und Rechnungsabschlüssen, ggf. unzustellbare Post)
- Anlässe zur Erfassung bzw. Prüfung von Kundendaten im Laufe der Geschäftsbeziehung (beispielsweise bei Bonitätsabfragen, 18. Geburtstag, Beratungsgesprächen, Eröffnung zusätzlicher Konten, Rücksendung verschickter Zwangskontoauszüge)

Der **periodische Ansatz** sah diese Dringlichkeit – anlassbezogene/unmittelbare Aufarbeitung fehlender Daten – nicht vor. Demgegenüber verlangte der periodische Ansatz die regelmäßige – periodische – Aktualisierung der Kundendaten, abhängig von der Risikoklasse des einzelnen Kunden. Dies hatte zu den jeweiligen Stichtagen einen entsprechenden (Projekt-)Aufwand zur Folge. Die DK-Hinweise sahen damals folgende Aktualisierungszeiträume vor:

- Niedriges Risiko – bis zu zehn Jahre (und bis zu drei Jahre für Maßnahmen/Nachfassen)
- Normales Risiko – bis zu sieben Jahre (und bis zu drei Jahre für Maßnahmen/Nachfassen)
- Hohes Risiko – bis zu zwei Jahre

Daneben ließen die DK-Hinweise auch eine Kombination zwischen dem anlassbezogenen und periodischen Ansatz zu.

„Sowohl-als-auch"

Die Auslegungs- und Anwendungshinweise der BaFin (AuA) in ihrer aktuellen Fassung schreiben heute vor, dass die „Erfüllung der Aktualisierungspflicht […] **periodisch und anlassbezogen** zu erfolgen" hat.

Zudem fordert das Geldwäschegesetz in § 10 Abs. 1 Nr. 5, „dass die jeweiligen Dokumente, Daten oder Informationen unter Berücksichtigung des jeweiligen Risikos im Rahmen der kontinuierlichen Überwachung im angemessenen zeitlichen Abstand aktualisiert werden" müssen.

Durch das zum 1. Januar 2020 in Kraft getretene Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie wurde mit dem neu eingefügten § 10 Abs. 3a

rung – Quo vadis?

GwG nochmal konkretisiert, wann die allgemeinen Sorgfaltspflichten bei bestehenden Geschäftsbeziehungen erneut erfüllt werden müssen: „Bei bereits bestehenden Geschäftsbeziehungen müssen sie [die Verpflichteten] die allgemeinen Sorgfaltspflichten zu geeigneter Zeit auf risikobasierter Grundlage erfüllen, insbesondere dann, wenn

1. sich bei einem Kunden maßgebliche Umstände ändern,
2. der Verpflichtete rechtlich verpflichtet ist, den Kunden im Laufe des betreffenden Kalenderjahres zu kontaktieren, um etwaige einschlägige Informationen über den wirtschaftlich Berechtigten zu überprüfen, oder
3. der Verpflichtete gemäß der Richtlinie 2011/16/EU des Rates vom 15. Februar 2011 über die Zusammenarbeit der Verwaltungsbehörden im Bereich der Besteuerung und zur Aufhebung der Richtlinie 77/799/EWG (ABl. L 64, vom 11. 3.2011, S. 1) dazu verpflichtet ist."

Zurzeit ist nicht eindeutig geklärt, was mit den „maßgeblichen Umständen" aus Nummer 1 gemeint ist. Im „Allgemeinen Teil" der AuA werden aktuell folgende Anlässe genannt:

- Unzustellbare Post
- Kunde meldet Änderung von Stammdaten wie Namensänderung, Adressänderung, Familienstandsänderung
- Zweifel an der Aktualität der Kundendaten

Insofern bleibt auch hier die Veröffentlichung des sogenannten „Besonderen Teils" der BaFin-AuA abzuwarten. Dies gilt auch für die in den Nummern 2 und 3 genannten Aktualisierungsverpflichtungen. Bis zur Klarstellung können die Regelungsinhalte aus den DK-Hinweisen vom 1. Februar 2014 daher weiter angewandt werden. Dies gilt insbesondere für die anlassbezogene Aktualisierung.

Für die periodische Aktualisierung wurden bereits in dem „Allgemeinen Teil" der BaFin-AuA **neue Zeiträume** definiert:

- Geringes Risiko – bis 15 Jahre
- Normales Risiko – bis zehn Jahre
- Hohes Risiko – bis zwei Jahre

Eine weitere Herausforderung stellt auch die Risikoklassifizierung selbst dar. Hierbei gilt es zu beachten, dass die technischen Risikoklassen in den Verfahren (u. a. Geno-SONAR®) nicht mit den in den AuA vorgesehenen Risikoklassifizierungen (jeweils in Verbindung mit den entsprechenden Sorgfaltspflichten) gleichzusetzen sind. Beispielsweise ist die Risikoklasse 0 „Geringes Risiko" in Geno-SONAR® nicht mit den vereinfachten Sorgfaltspflichten im Sinne des § 14 GwG zu verwechseln.

Im Kundenannahmeprozess erfolgt die Risikoklassifizierung im Sinne der AuA anhand verschiedener Risikofaktoren. Das führt unmittelbar zu der Frage, welches Maß der Sorgfaltspflichten (vereinfachte, allgemeine oder verstärkte) angewandt werden muss. Nachdem die Geschäftsbeziehung begründet ist, erfolgt technisch eine regelbasierte Zuordnung der Risikoklasse in Geno-SONAR®. Im weiteren Verlauf der Geschäftsbeziehung kann, beispielsweise nach Erkenntnissen aus dem sogenannten „Know-your-Customer-Prinzip", die technische Risikoklassen-einstufung manuell korrigiert werden.

Fazit

Durch die gesetzlichen Änderungen und die von der BaFin im Rahmen ihrer Auslegungshinweise festgelegte Verwaltungspraxis steigt der administrative Aufwand in den Banken: Die gesetzlich geforderte Aktualisierungspflicht sieht nun eine Verknüpfung von anlassbezogenem und periodischem Ansatz vor. Die DZ CompliancePartner wird die Entwicklungen verfolgen, um auch hier weiterhin die bestmögliche Unterstützung im Rahmen der angebotenen Dienstleistungen in der Geldwäsche- und Betrugsprävention zu gewährleisten. ▬

AUTOREN UND ANSPRECHPARTNER

Thomas Schröder
Beauftragter Geldwäsche- und Betrugsprävention,
E-Mail: thomas.schroeder@dz-cp.de

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

Informationssicherheit

Monetäre Bewertung von IT-Restrisiken

Auf welcher Grundlage muss eine monetäre Bewertung der IT-Restrisiken durchgeführt werden? Welche Bewertungsansätze sind möglich?

Die aufsichtsrechtlichen Anforderungen in der Informationssicherheit sind in den letzten Jahren immer weiter gestiegen. Vor Veröffentlichung der Bankaufsichtlichen Anforderungen an die IT (BAIT) lag in vielen Banken der Fokus zunächst auf der qualitativen Bewertung der IT-Risiken. Eine quantitative Bewertung wurde hingegen zumeist vernachlässigt bzw. erfolgte in den Banken, ohne nachweisbaren Bezug zu den qualitativ erhobenen IT-Risiken, in Form einer Expertenschätzung. Doch auf welcher Grundlage kann eine nachvollziehbare monetäre Bewertung der IT-Restrisiken erfolgen? Welche Bewertungsansätze sind hierzu möglich?

Erhebung der qualitativen IT-Risiken

In der Informationssicherheit werden den Geschäftsprozessen sogenannte IT-Schutzobjekte (Datenklassen, Anwendungen, Systeme und Infrastrukturkomponenten) zugeordnet und hinsichtlich ihres Schutzbedarfs und Schutzniveaus bewertet. Der Schutzbedarf ergibt sich zumeist aus den Verfügbarkeitsanforderungen der zugeordneten Geschäftsprozesse sowie den hierin verwendeten Datenklassen. Das Schutzniveau hingegen wird aus den umgesetzten und für wirksam befundenen technischen und organisatorischen Maßnahmen (TOM) der jeweiligen Schutzobjekte bestimmt. Die IT-Risiken orientieren sich an dem Bedrohungskatalog und werden bestimmten Bedrohungsfeldern zugeordnet (vgl Abb. 1).

1 ZUORDNUNG ZU BEDROHUNGSFELDERN

Kategorie und Bezeichnung	Schutzziele
B 1 Interne Verfahren	
B1-1 Fehler von Anwendern/Benutzern	A C I N
B1-2 Fehler im Betrieb	A C I N
B1-3 fehlerhafte Prozesse	A C I N
B 2 Menschen	
B2-1 Missbrauch und Diebstahl	A C I N
B2-2 Angriffe auf Verfügbarkeit und Angriffe durch Schadprogramme	A C I N
B2-3 Angriffe auf Menschen (Social Engineering, Erpressung, …)	A C I N
B 3 Infrastruktur/Systeme	
B3-1 Ausfall von Systemen	A
B3-2 Ausfall von Kommunikationsinfrastruktur	A I
B3-3 Ausfall von Infrastrukturkomponenten	A
B 4 Externe Einflüsse	
B4-1 Gebäudeausfall	A
B4-2 Personalausfall	A
B4-3 Urteile, Beschlagnahmung, Reputation	A C I N

A C I N:
A = availability/Verfügbarkeit
C = confidentiality/Vertraulichkeit
I = integrity/Intigrität
N = non-repudiation/Authenzität

Dabei werden die IT-Risiken in Brutto- und Nettorisiken eingeteilt. Die Bruttorisiken weisen meist ein höheres Risiko aus als die Nettorisiken. Um das Risiko zu minimieren, werden Maßnahmen (z. B. Sollberechtigungskonzepte, Zugriffsregelungen) hinterlegt. Das durch die Maßnahmen reduzierte Risiko wird als Nettorisiko bezeichnet.

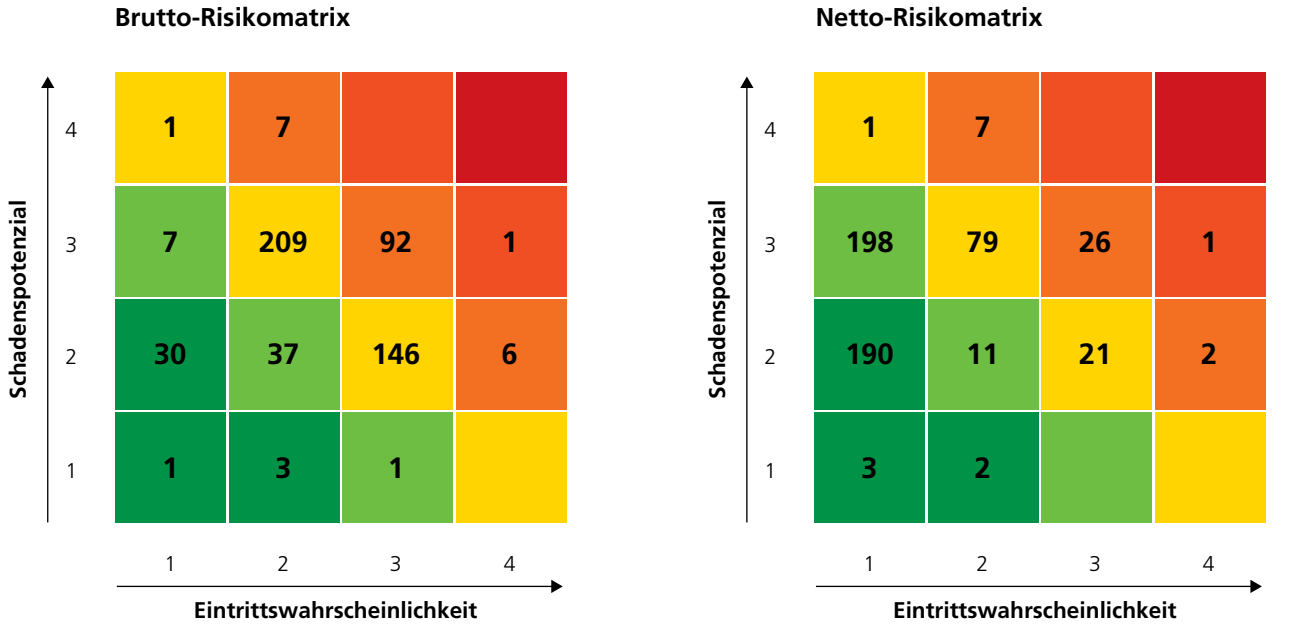
Die hinterlegten Nettorisiken lassen sich je nach Höhe des Risikos wiederum in drei Bereiche kategorisieren:

- Genehmigungspflichtige Risiken
- Meldepflichtige Risiken
- Akzeptable Risiken

Eine Auswertung aller IT-Risiken lässt sich in der Regel über eine Risikomatrix darstellen (vgl. Abb. 2).

Mit der beschriebenen Vorgehensweise werden die qualitativen IT-Risiken erhoben. Doch wie lassen sich die Ergebnisse der qualitativen in eine quantitative Betrachtung überführen? >

2 BEISPIELHAFTE AUSWERTUNG EINER RISIKOMATRIX AUS DER FACHANWENDUNG „ISI KOMPAKT“



Schadenspotenzial
1 = niedrig
2 = mittel
3 = hoch
4 = sehr hoch

Eintrittswahrscheinlichkeit
1 = unwahrscheinlich
2 = möglich
3 = wahrscheinlich
4 = sehr wahrscheinlich

Risikoklassen
- nicht relevant
- vernachlässigbar
- gering
- relevant
- äußerst relevant
- existenzbedrohend

Risikokategorie
- akzeptabel
- akzeptabel
- meldepflichtig
- genehmigungspflichtig
- genehmigungspflichtig
- genehmigungspflichtig

Grundlage zur quantitativen (=monetären) Bewertung der IT-Restrisiken

Zunächst ist zu klären, auf welcher rechtlichen Grundlage eine monetäre IT-Restrisikobewertung durchzuführen ist.

Die Grundlagen finden wir in den BAIT Tz. 13 i. V. m. MaRisk BTR 4: „Die Risikoanalyse auf Basis der festgelegten Risikokriterien hat auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen zu erfolgen. Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern. Die Ergebnisse der Risikoanalyse sind zu genehmigen und in den Prozess des Managements der operationellen Risiken zu überführen." Erläuternd heißt es weiter dazu: „Risikokriterien enthalten bspw. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit." (Auszug aus den BAIT 10/2017[1])

In den MaRisk (Fassung vom 27.10.2019[2]) wird der Umgang mit den operationellen Risiken klar definiert (siehe Abb. 3).

3 BTR 4 – OPERATIONELLE RISIKEN

1 Das Institut hat den operationellen Risiken durch angemessene Maßnahmen Rechnung zu tragen. Für diese Zwecke ist eine institutsintern einheitliche Festlegung und Abgrenzung der operationellen Risiken vorzunehmen und an die Mitarbeiter zu kommunizieren.	**Definition von operationellen Risiken** Die Festlegung sollte auch eine möglichst klare Abgrenzung zu anderen vom Institut betrachteten Risiken enthalten. **Umgang mit nicht eindeutig zuordenbaren Schadensfällen oder Beinaheverlusten** Die Prozesse zum Management operationeller Risiken sollten auch den Umgang mit nicht eindeutig zuordenbaren Schadensfällen („boundary events"), Beinaheverlusten und zusammenhängenden Ereignissen umfassen. Als sogenannte „boundary events" können Verluste eingestuft werden, die zwar einem Risiko zugerechnet werden oder bereits wurden (z. B. Kreditverluste), die aber ihren Ursprung in Ereignissen wie z. B. mangelhaften Prozessen und Kontrollen haben oder hatten. Als „Beinaheverluste" können durch Fehler oder Mängel ausgelöste Ereignisse bezeichnet werden, die zu keinem Verlust geführt haben (z. B. fehlerhafte Zahlung an falschen Kontrahenten; Rückzahlung durch den Kontrahenten).
2 Es muss gewährleistet sein, dass wesentliche operationelle Risiken zumindest jährlich identifiziert und beurteilt werden.	
3 Das Institut hat eine angemessene Erfassung von Schadensfällen sicherzustellen. Bedeutende Schadensfälle sind unverzüglich hinsichtlich ihrer Ursachen zu analysieren.	**Erfassung von Schadensfällen** Größere Institute haben hierfür eine Ereignisdatenbank für Schadensfälle eingerichtet, bei welcher die vollständige Erfassung aller Schadensereignisse oberhalb angemessener Schwellenwerte sichergestellt ist.
4 Auf Basis der Risikoberichterstattung gemäß BT 3.2 Tz. 6 ist zu entscheiden, ob und welche Maßnahmen zur Beseitigung der Ursachen zu treffen oder welche Risikosteuerungsmaßnahmen (z. B. Versicherungen, Ersatzverfahren, …) zu ergreifen sind.	

ISI kompakt

Mit der Anwendung „ISI kompakt" wird der aufsichtsrechtlich geforderte Informationsverbund zum Informationsrisikomanagement abgebildet:

- Geschäftsprozesse,
- Objekte/Ressourcen,
- Risikoanalysen und
- Maßnahmen der entsprechend verwendeten Standards (SOIT, BSI etc.).

Die Maßnahmen sind selbstverständlich mit den Risiken verknüpft und bilden so das tatsächlich realisierte Schutzniveau am Objekt/an der Ressource ab und sorgen für eine Reduzierung der jeweiligen Risiken. Des Weiteren verfügt die Anwendung über diverse Auswertungsfunktionen zum Informationsrisikomanagement.

Bewertungsansatz der monetären IT-Restrisiken

Bisher gibt es seitens der BAIT und MaRisk keine konkreten Vorgaben, wie die Bewertung durchzuführen ist. Dies eröffnet den Banken die Möglichkeit, ein für sie passendes Verfahren zu nutzen. Als Mehrmandantenanbieter nutzen wir das in unserem Haus entwickelte Tool „ISI kompakt". Es ermöglicht uns eine umfassende Betrachtung und zugleich eine nachvollziehbare Bewertung der IT-Risiken. Die IT-Restrisiken werden übersichtlich dargestellt.

Bei der Bewertung der monetären Restrisiken sollte unabhängig vom eingesetzten Tool immer auch der Risiko-Controller aktiv mit einbezogen werden.

Gleichzeitig sollte jedes Tool die Arbeitsanweisung „100.04.06 RB zum Management operationeller Risiken" – genauer der Anlage 2. – gemäß den Musterarbeitsanweisungen des Genossenschaftsverbands – Verband der Regionen e.V. berücksichtigen. Praktisch heißt das, dass die o. g. Bedrohungen mit der entsprechenden Kategorie „Ereigniskategorie (3. Ebene)" verknüpft werden. Eine Zuordnung sieht dann wie folgt aus (siehe Abb. 4).

4 ZUORDNUNGSTABELLE

Bedrohung aus SOIT	Ereigniskategorie der Anlage 2
B1-1 Fehler von Anwendern/ Benutzern	7.1.2 Fehler bei der Dateneingabe, -pflege oder -speicherung
B1-2 Fehler im Betrieb	7.1.4 fehlerhafte Anwendung von Modellen/Systemen
B1-3 fehlerhafte Prozesse	7.1.5 Buchführungsfehler/ falsche Prozesszuordnung
B2-1 Missbrauch und Diebstahl	2.2.2 Diebstahl von Informationen (mit finanziellem Schaden)
B2-2 Angriffe auf Verfügbarkeit und Angriffe durch Schadprogramme	2.2.1 Schäden durch Hackeraktivitäten
B2-3 Angriffe auf Menschen (Social Engineering, Erpressung, …)	2.1.1 Diebstahl/Raub
B3-1 Ausfall von Systemen	6.1.1 Hardware
B3-2 Ausfall von Kommunikations-infrastruktur	6.1.3 Telekommunikation
B3-3 Ausfall von Infrastruktur-komponenten	6.1.4 Versorgungsausfall/ -störung
B4-1 Gebäudeausfall	6.1.2 Software
B4-2 Personalausfall	3.1.1 Ausgleichszahlungen, Zuwendungen, Abfindungen
B4-3 Urteile, Beschlagnahmung, Reputation	4.2.2 unzulässige Geschäfts-/ Marktpraktiken

>

AUTOREN UND ANSPRECHPARTNER

Björn Scherer
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: bjoern.scherer@dz-cp.de

Benjamin Wellnitz
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

Diese Zuordnung soll als Beispiel für die weitere Bearbeitung der Risiken dienen.

Nach entsprechender Auswertung aus dem Informationssicherheitsmanagementsystem werden die gebildeten Mittelwerte zur Eintrittswahrscheinlichkeit (EW) und zum Schadenspotenzial (SP) über alle im jeweiligen Bedrohungsbereich liegenden Einzelrisiken an das Self-Assessment/die Risikoinventur übergeben (vgl. Abb. 5).

Bereits getroffene Aussagen der Fachbereiche zu den Eintrittswahrscheinlichkeiten und den Schadenspotenzialen können abgeglichen werden. Hier empfehlen wir das Maximalwertprinzip (konservativer Bewertungsansatz): Je nachdem, welcher Wert höher ist, wird dieser übernommen. Ist die getroffene Aussage des Fachbereiches höher als der Wert aus der Informationssicherheit, so ist der Wert des Fachbereichs beizubehalten. Sofern der Fachbereich einen niedrigeren Wert veranschlagt hat, so ist der Wert aus der Informationssicherheit zu verwenden.

Nach Übertragung aller Positionen erfolgt eine Monte-Carlo-Simulation (Verfahrensmethode aus der Stochastik), um den entsprechenden individuellen Schadenswert zu berechnen. Hierzu sollte der Risiko-Controller eingebunden werden, um die Berechnung durchzuführen.

Fazit

Aufsichtsrechtlich ist spätestens mit den BAIT die monetäre Bewertung der IT-Restrisiken – neben der qualitativen Analyse – zwingend erforderlich. Welche Bewertungsmethoden gewählt werden, sollte seitens der Bank gut überlegt werden und nachvollziehbar (für Dritte) dokumentiert werden. Dabei ist der Weg – wie die Bewertung für die Bank erfolgt – gut zu begründen. ▬

5 BEISPIEL EINER RISIKOINVENTUR IN ISI KOMPAKT

B1 Interne Verfahren	150	BE	SW	EW	SP
B1-1 Fehler von Anwendern/Benutzern	**60**	**2**	**1**	**2**	**2**
agree mobile WLAN-V-R2.1.1. Ungeeignete Aufstellung der WLAN-Access-Points		1	1	1	3
agree21Banking-V-R2.1.1: Versehentliche Falscheingaben durch den Bankmitarbeiter		3	3	3	2
agree21Banking-V-R2.1.1: Versehentliche Falscheingaben von Konditionen oder Kreditlimits durch den Bankmitarbeiter, die einen erweiterten Schaden verursachen können		3	3	3	2
agree21Banking-V-R2.1.1: Versehentliche Falscherfassung bei Zahlungsverkehrsdaten durch den Bankmitarbeiter, die einen erweiterten Schaden verursachen können		1	1	1	2

[1] BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9 (Stand: 28.10.2019)

[2] BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&v=5 (Stand: 28.10.2019)

WpHG-Compliance

Single Officer

Ein weiterer Beauftragter hat die Bühne betreten: der Beauftragte zum „Schutz von Finanzinstrumenten und Geldern von Kunden". Doch bedeutet das unweigerlich auch die Einrichtung einer neuen Stelle? Und muss wirklich jede Bank das ganze Aufgabenspektrum abdecken? Die Antwort lautet: Es kommt drauf an.

Mit der MiFID II trat zum 3. Januar 2018 auch die Pflicht zur Ernennung eines „Beauftragten zum Schutz von Finanzinstrumenten und Geldern von Kunden" (englisch: single officer) in Kraft (Art. 7 delegierte Richtlinie EU 2017/953). In deutsches Recht wurde die Richtlinie mit § 81 Abs. 5 WpHG und § 10 WpDVerOV umgesetzt.

Eine Konkretisierung zum Schutz von Finanzinstrumenten der Kunden findet sich in dem am 16. August 2019 veröffentlichten Rundschreiben 07/2019 (WA) – Mindestanforderungen an die ordnungsgemäße Erbringung des Depotgeschäfts und den Schutz von Kundenfinanzinstrumenten für Wertpapierdienstleistungsunternehmen (MaDepot).

Weitere Regelungen zu den allgemeinen Verhaltenspflichten sind im Depotgesetz (DepotG) enthalten. Laut 1.1 Abs. 5 der MaDepot sind einzelne Bestimmungen des DepotG relevant für die Beurteilung, ob das Wertpapierdienstleistungsinstitut die allgemeinen Verhaltenspflichten im Sinne des § 63 Abs. 1 WpHG eingehalten hat.

Welches sind die Pflichten des Single Officers?

Der Single Officer trägt die Verantwortung dafür, dass das Wertpapierdienstleistungsunternehmen seine Verpflichtung in Bezug auf den Schutz von Finanzinstrumenten und Geldern von Kunden einhält (2.1.5.1 MaDepot).

In der MaDepot wird klargestellt, dass es sich beim Single Officer um eine Funktion der „zweiten Verteidigungslinie" handelt (2.1.5.1 MaDepot). Das bedeutet, dass der Single Officer eine überwachende und beratende Funktion innehat.

Die Wahrnehmung der Verantwortung des Single Officers erfolgt gemäß 2.1.5.2 MaDepot durch folgende Tätigkeiten:

1. Erstellung einer Risikoanalyse,
2. ständige Überwachung (auf Basis der Risikoanalyse) der organisatorischen Vorkehrungen,
3. Beratung und Unterstützung der zuständigen Personen,
4. Berichterstattung (Jahresbericht und Ad-hoc-Bericht bei erheblichen Feststellungen).

Vor diesem Hintergrund sind die vom Gesetzgeber verwendeten Begriffe „Gesamtverantwortung" (5. Erwägungsgrund delR EU 2017/593); „spezielle Verantwortung" (Art. 7 delR 2017/593); „der die Verantwortung dafür trägt"(§ 81 Abs. 5 WpHG) zu lesen. Die Veranwortung und die Tätigkeiten des Single Officers beziehen sich – analog derjenigen des Beauftragten WpHG-Compliance (i.S.d. Art. 22 delVO 2017/565) – auf die Überwachung und Bewertung der organisatorischen Grundsätze. Er trägt demnach nur für die eigenen, ordnungsgemäß auszuführenden Aufgaben und Tätigkeiten und für den Hinweis auf Missstände die Verantwortung.

Die eigentliche Verantwortung zur Einhaltung der rechtlichen Pflichten obliegt dagegen den operativen Bereichen („erste Verteidigungslinie").

Kann der Single Officer gleichzeitig durch den Beauftragten WpHG-Compliance wahrgenommen werden?

Laut MaDepot (2.1.5.5) kann (aber muss nicht) die Aufgabe des Single Officers auch durch den Beauftragten WpHG-Compliance wahrgenommen werden.

Dies wird sich in vielen Fällen aufgrund der vergleichbaren systematischen Vorgehensweise auch anbieten. Der Vorteil: Die Aufgaben des Single Officers (Risikoanalyse/Überwachung/Berichtswesen) können in die bereits vorhandene Organisationsstruktur der Compliance-Funktion integriert werden. Voraussetzung ist, dass die zusätzlich notwendigen Ressourcen in diesem Fall der Compliance-Funktion zur Verfügung gestellt werden.

Sofern die Aufgabe von einem anderen Mitarbeiter/einer anderen Funktion wahrgenommen wird, ist zu beachten, dass

1. die notwendigen Befugnisse, Ressourcen und Fachkenntnisse vorhanden sind, >

2. er nicht selbst an den zu überwachenden Dienstleistungen und Tätigkeiten beteiligt ist,
3. der Single Officer seine Aufgaben weisungsfrei und unabhängig ausüben kann und
4. eine klare Abgrenzung zum Zuständigkeitsbereich des Beauftragten WpHG-Compliance erfolgt.

A. Risikoanalyse

Zunächst hat sich der Beauftragte einen Überblick über das Geschäftsmodell und den damit notwendigen organisatorischen Regelungen zu verschaffen. Diese Analyse könnte man auch als „Betroffenheitsanalyse" bezeichnen.

Um die notwendigen Pflichten des Instituts identifizieren zu können, empfiehlt es sich, die Risikoanalyse wie einen Entscheidungsbaum aufzubauen. Die erste Ebene ließe sich beispielsweise auf folgende Fragen reduzieren:

1. Hat das Institut das Depotgeschäft (Wertpapierabwicklung und -verwahrung) auf einen Dienstleister ausgelagert?
2. Unterhält die Bank (darüber hinaus) eigene Lagerstellen oder bestehen eigene (direkte) Verbindungen zu Lagerstellen?
3. Ist die Bank selbst Handelsteilnehmer im Sinne der CSDR („Drittbankclearing")?
4. Werden Sicherungsübereignungen („SÜ") (Vollrechtsübertragung) von Finanzinstrumenten professioneller Kunden/geeigneter Gegenparteien angeboten bzw. durchgeführt?
5. Betreibt die Bank Wertpapierleihgeschäft mit Kundenfinanzinstrumenten?
6. Nutzt die Bank standardisierte geprüfte Kundeninformationen im Sinne des Art. 47 Abs. 1 g) und Art. 49 delVO 2017/565?
7. Gab es in Prüfungsberichten (Interne Revision, externe Prüfung nach § 89 Abs. 1 WpHG, Jahresabschlussprüfung) einschlägige Mängel (insbesondere zum Depotgeschäft, der Depotbuchführung)?

Je nach Beantwortung der Fragen entsteht möglicherweise weiterer Klärungsbedarf. Auf der zweiten Ebene wären beispielsweise folgende Fragestellungen relevant:

8. Gibt es Feststellungen in Bezug auf den Auslagerungsdienstleister (siehe oben Frage 1) bzw. liegen die notwendigen Prüfungsberichte vor? Ist die Überwachung des Dienstleisters Gegenstand des zentralen Auslagerungsmanagements?
9. Welche Regelungen zur eigenen Lagerstelle liegen vor? Welche Regelungen im Hinblick auf die Verbindung zu einer (ausländischen) Lagerstelle liegen vor?
10. Welche Regelungen liegen in Hinblick auf die Sicherungsübereignung von Finanzinstrumenten von professionellen Kunden/geeigneten Gegenparteien vor?

B. Überwachung

Aus den Erkenntnissen der Risikoanalyse ergeben sich die individuell notwendigen Überwachungstätigkeiten des Single Officers. Diese Überwachungstätigkeiten sollten auf einem schriftlich fixierten Überwachungsplan basieren.

Sofern sich aus der Risikoanalyse ergibt, dass ein bestimmtes – mit weiteren Pflichten behaftetes – Geschäftsmodell nicht angeboten wird (z. B. Wertpapierleihe, Sicherungsübereignung), genügt es, zu prüfen, ob dies schriftlich geregelt ist.

Je höher sich das Risiko von Verletzungen von kundenschützenden Regelungen darstellt, desto detaillierter müssen die Überwachungstätigkeiten sein.

So kann es beispielsweise notwendig sein, zu prüfen, welche konkreten Verwahrrisiken sich bei einer direkten Verbindung zu einer ausländischen Lagerstelle ergeben, welche Maßnahmen zur Reduktion des Risikos von den operativen Bereichen ergriffen wurden, ob die Kunden entsprechend informiert sind und ob die aufsichtskonforme Vorgehensweise und die Zuständigkeiten schriftlich fixiert sind.

Neben den risikoorientierten Überwachungshandlungen empfiehlt es sich – zumindest einmalig – zu prüfen und sicherzustellen, dass die Informationen, die gemäß § 10 Abs. 10 WpDVerOV auf Anfrage der BaFin einem bestellten Insolvenzverwalter und, sofern zutreffend, der zuständigen Abwicklungsbehörde auf Anfrage zur Verfügung zu stellen sind, ohne zeitlichen Verzug geliefert werden können (2.1.4 MaDepot). Hierzu

AUTOR UND ANSPRECHPARTNER

Marc Linnebach
Leiter WpHG-Compliance,
E-Mail: marc.linnebach@dz-cp.de

sollte ein Fragebogen/eine Checkliste verwendet werden, in der

- die Informationen des § 10 Abs. 10 WpDVerOV aufgelistet werden und
- jeweils vermerkt wird, wo die jeweiligen Informationen zu erhalten sind.

Dieser Fragebogen sollte für das laufende Jahr einmal als Muster ausgefüllt werden.

§ 10 Abs. 10 WpDVerOV

1. Aufzeichnungen interner Konten und Aufzeichnungen, aus denen Salden der für Kunden gehaltenen Gelder und Finanzinstrumente hervorgehen
2. Angaben zu Konten bei der Zentralbank oder Dritten, auf denen Kundengelder gehalten werden, die diesbezüglichen Vereinbarungen mit den Wertpapierdienstleistungsunternehmen (WpDIU)
3. Konten und Depots bei Dritten, wenn dort Kunden-Finanzinstrumente verwahrt werden, und die diesbezüglichen Vereinbarungen mit den WpDIU
4. Angaben zu ausgelagerten Aufgaben und die diesbezüglichen Vereinbarungen mit den WpDIU
5. Angaben zu Mitarbeitern, die für die Verwahrung von Gel-dern und Finanzinstrumenten verantwortlich oder daran beteiligt sind und zu den Mitarbeitern, die für den Schutz verantwortlich sind (SO)
6. die Vereinbarungen, die zur Feststellung der Eigentumsverhältnisse an den Vermögensgegenständen der Kunden relevant sind

C. Beratung und Unterstützung

Der Single Officer ist der Ansprechpartner für die zuständigen operativen Einheiten und steht für Fragen zur Verfügung. Darüber hinaus gibt er Empfehlungen zu notwendigen Maßnahmen ab, die er aus seiner Risikoanalyse oder den Überwachungshandlungen gewonnen hat. Bei aufsichtsrechtlichen Änderungen unterstützt er bei der Anpassung der organisatorischen Maßnahmen.

D. Berichtswesen

Über seine Tätigkeit berichtet der Single Officer mindestens jährlich an die Geschäftsführung. Darüber hinaus berichtet er ad hoc bei wesentlichen Feststellungen (2.1.5.2 MaDepot). Da die MaDepot keine konkreten Vorgaben zum Inhalt des Berichtes des Single Officers enthalten, können die Vorgaben für den Beauftragten WpHG-Compliance BT 1.2.2 MaComp analog herangezogen werden.

Unser Angebot

Als unser Kunde haben Sie die Möglichkeit, entweder die Funktion des Single Officers durch einen Ihrer Mitarbeiter wahrzunehmen oder – neu – sie an Ihren Beauftragten WpHG-Compliance zu übertragen. Dabei wird die Leistung des „Single Officers“ in Personalunion durch Ihren Beauftragten WpHG-Compliance durchgeführt. Ihr Vorteil: Sie haben einen zentralen Ansprechpartner, die Kommunikationswege und Zuständigkeiten sind klar geregelt. Darüber hinaus wird die Leistung selbstverständlich auch nach IDW PS 951 geprüft. Sie profitieren also auch mit Blick auf den Single Officer von einer sicheren, gesetzes- und MaDepot-konformen Umsetzung.

Fazit

Der Aufwand und das notwendige fachliche Know-how des Beauftragten richten sich auch bei der Funktion Single Officer nach dem konkreten Geschäftsmodell der Bank.

Unabhängig von der individuellen Komplexität der Tätigkeit hilft eine systematische und standardisierte Vorgehensweise dabei, Risiken korrekt zu bewerten und die Funktion möglichst effizient auszuüben. ▬

MaRisk-Compliance

Kann Auslagerungsmanagement noch einfach sein?

Die Anzahl der Vorgaben, die bereits heute in Zusammenhang mit dem Auslagerungsmanagement von jedem Institut zu beachten sind, ist hoch. Zur Beurteilung, ob und wie Auslagerungsmanagement einfach sein kann, müssen zunächst die aktuell gültigen Vorgaben betrachtet werden.

Maßgeblich sind die in § 25b KWG vorgeschriebenen Grundsätze sowie die Einhaltung der AT 9 MaRisk. Demnach sind die mit wesentlichen Auslagerungen verbundenen Risiken angemessen zu steuern und ist die Ausführung der ausgelagerten Aktivitäten und Prozesse ordnungsgemäß zu überwachen. Dies umfasst auch die regelmäßige Beurteilung der Leistung des Auslagerungsunternehmens anhand vorzuhaltender Kriterien. Für die Steuerung und Überwachung hat das Institut klare Verantwortlichkeiten festzulegen.

Darüber hinaus hat ein Institut gemäß § 25a Abs. 1 KWG die Ordnungsmäßigkeit der Geschäftsorganisation sicherzustellen. Dies beinhaltet unter anderem ein angemessenes und wirksames Risikomanagement. Die zeitnahe Risikoanalyse zu den wesentlichen Auslagerungen mit entsprechender Dokumentation ist hierbei in jedem Fall notwendig. Zusätzlich wird erwartet, dass auch die mit den sogenannten „sonstigen Fremdbezügen" in Verbindung stehenden Risiken gemäß § 25a Abs. 1 KWG ins Risikomanagement des Instituts mit einbezogen werden. Gleiches gilt auch für Auslagerungen, die im Rahmen einer Risikoanalyse als unwesentlich eingestuft werden.

Grundlagen des Auslagerungsmanagements

Die MaRisk setzen – in Abhängigkeit von der Art, dem Umfang und der Komplexität der Auslagerungsaktivitäten – die Einrichtung eines zentralen Auslagerungsmanagements voraus. Auch mit Blick auf die Informationstechnik erwartet die Aufsicht ein zentrales Auslagerungsmanagement. Weiterhin verlangen interne und externe Prüfer bei Prüfungshandlungen in der Regel eine Übersicht der ausgelagerten Geschäftsprozesse, weshalb die jeweiligen Ergebnisse in einer Gesamtliste zusammenzufassen sowie Änderungen eindeutig und nachvollziehbar zu dokumentieren sind. Neben einer stetig steigenden Anzahl an Auslagerungen werden auch die Informationen bzw. Unterlagen, die die Auslagerungsunternehmen bereitstellen, immer mehr und umfangreicher. Desto mehr ist es geboten, das Auslagerungsmanagement mit den folgenden wesentlichen Fragen auf den Prüfstand zu stellen:

- Sind die ausgelagerten Aktivitäten und Prozesse (inklusive Weiterverlagerungen) in einem Register vollständig erfasst und dokumentiert?
- Wurden klare Verantwortlichkeiten festgelegt?
- Sind die wesentlichen Vertragsbestandteile zu Prüfungs-/Informations- und Durchgriffsrechten enthalten?
- Gibt es nachvollziehbare und transparente Risikoanalysen?
- Werden die mit den wesentlichen Auslagerungen verbundenen Risiken angemessen gesteuert?
- Sind nachvollziehbare Kontroll- und Überwachungsprozesse installiert, um die ausgelagerten Aktivitäten und Prozesse ordnungsgemäß überwachen zu können?
- Ist eine jährliche Berichterstattung vorgesehen?

Prozess Risikoanalyse

Vor Beginn einer Vertragsbeziehung mit einem Dienstleister ist darauf zu achten, dass eine Risikoanalyse erstellt wird. So muss sich das auslagernde Institut über die Risiken informieren können, um hieraus abgeleitet den Prozess der Risikoanalyse anzu-

AUTORIN UND ANSPRECHPARTNERIN

Silke Lenhart
Beauftragte MaRisk-Compliance,
E-Mail: silke.lenhart@dz-cp.de

stoßen. Dies kann aber nur erfolgen, wenn dem Institut entsprechende Informationen vorliegen, um Auslagerungsrisiken, Prozessrisiken und dienstleistungsspezifische Risiken bewerten zu können. Aus diesem Grund sind vom Dienstleister entsprechende Unterlagen einzufordern, zu sichten und innerhalb der Risikoanalyse zu bewerten. Hierzu gehört beispielsweise der externe Prüfungsbericht (z. B. IDW PS 951 n.F.).

In die Erstellung der Risikoanalyse sind bei den Instituten neben dem Auslagerungskoordinator weitere Stellen zwingend einzubinden. In der Risikoanalyse selbst wird die Fachabteilung bzw. der fachlich Verantwortliche die Auslagerungsrisiken aufgrund der Nähe zum Thema am besten bewerten können. Gleichfalls können die risikomindernden Maßnahmen durch eine Fachabteilung gezielt definiert werden. Unabhängig davon sind die maßgeblichen Organisationseinheiten (z. B. Risikocontrolling, Compliance-Funktionen) einzubeziehen und auch die Interne Revision ist im Rahmen ihrer Aufgaben zu beteiligen. Die Herausforderung besteht insbesondere darin, den Überblick zu behalten, sodass keine Organisationseinheiten vergessen werden.

Risikosteuerung/Überwachungsprozess

Die Risikoanalysen sind regelmäßig und anlassbezogen zu überprüfen. Für wesentliche Auslagerungen ist regelmäßig von einem jährlichen Turnus auszugehen. Damit besteht eine Differenzierung zu unwesentlichen Auslagerungen mit einem dreijährigen Turnus. Darüber hinaus empfiehlt sich der Blick auf die sonstigen Fremdbezüge, die zwar keine Auslagerungen darstellen, aber aufgrund von Leistungserweiterungen sich zu solchen entwickeln können.

Von der anlassbezogenen Risikoanalyse spricht man, wenn kein regulärer Turnus vorliegt, sondern ein Grund für eine ad hoc einberufene Analyse, beispielsweise ein Fall von eklatanter Schlechtleistung, vorliegt.

Die Steuerung der Risiken wird insbesondere durch die vertraglichen Regelungen unterstützt. So sehen beispielsweise die Musterklauseln des BVR Leistungs- und Qualitätsstandards vor. Die konkreten Steuerungs- und Überwachungsmechanismen hängen wiederum von Art, Umfang, Komplexität und Risikogehalt der Auslagerungsmaßnahme ab. Aus den sich aus der Risikoanalyse ergebenden Risiken wird abgeleitet, welche Berichte zur Steuerung und Überwachung der Risiken erforderlich sind.

Die Überwachung erstreckt sich insbesondere auf die Ergebniskontrolle und die dafür eingerichteten Prozesse und Strukturen. Beispielhafte Überwachungsmaßnahmen sind die Auswertung regelmäßig eingereichter Berichte des Dienstleisters oder Soll-Ist-Vergleiche auf Basis von Leistungsbeschreibungen. Die Dokumentation der Auswertung von Informationen und Berichten im Rahmen der Risikoüberwachung von Dienstleistungsunternehmen ist dabei wesentlich.

Durch die stetig steigende Anzahl an Auslagerungen werden auch die Informationen beziehungsweise Unterlagen, die die Auslagerungsunternehmen bereitstellen, immer mehr und umfangreicher. Dadurch und durch die gestiegenen Anforderungen wird ein transparentes und organisiertes Auslagerungsmanagement und -controlling erschwert.

Unsere Erfahrung als Mehrmandantendienstleister zeigt, dass häufig bei der Durchsicht von Berichten (und auch bei vielen anderen Themen, wie z. B. der Überprüfung der Risikoanalyse) nicht bzw. nicht ausreichend dokumentiert wird (etwa in Form von Kurzdarstellung, Zusammenfassung des Ergebnisses oder zu ergreifender Maßnahmen, sofern erforderlich). >

Die Dokumentation ist sehr aufwendig. Zuerst müsste eine Infrastruktur in jedem Institut geschaffen werden, was sich als sehr zeitaufwendig und kostenintensiv gestaltet. Die Übersicht zu wahren und die Überprüfungen sowie Auswertungen gegenüber Aufsicht und Prüfern nachweisen zu können, stellt eine große Herausforderung dar, die mit steigender Anzahl an Auslagerungen zunehmend unmöglich erscheint.

Zusammenfassend ist das Auslagerungsmanagement für eine einzige Auslagerung trotz der vielen zu erfüllenden Vorgaben nach wie vor einfach. Die Komplexität steigt jedoch mit zunehmender Anzahl an Auslagerungen und beteiligten Organisationseinheiten massiv an.

Geeignete Infrastruktur

Ohne eine geeignete Infrastruktur und implementierte Prozesse besteht das nicht zu unterschätzende Risiko, dass Organisationseinheiten nicht einbezogen, Tätigkeiten nicht durchgeführt und Unterlagen bzw. Dokumentationen nicht nachgewiesen werden können. Gleichzeitig steigt das Risiko, dass auf Schlechtleistung eines Dienstleisters nicht (rechtzeitig) reagiert werden kann. Dieser Umstand manifestiert sich in der wachsenden Anzahl an Feststellungen zum Auslagerungsmanagement in den Berichten von Aufsicht, Prüfern und Compliance.

Spätestens mit dem Inkrafttreten der neuen EBA-Leitlinien am 30. September 2019 steht im Auslagerungsmanagement die Bewertung und Steuerung der Risiken der jeweiligen Dienstleistung wieder einmal im Vordergrund. Ausgelöst durch die EBA-Leitlinien zum Umgang mit Auslagerungen ist bei den zukünftig anstehenden Anpassungen der MaRisk und des KWG mit gesteigerten Überwachungstätigkeiten zu rechnen. Um alledem auch in Zukunft gerecht zu werden, muss ein Tool so konzipiert sein, dass es auch zukünftige regulatorische Anforderungen integrieren kann. Es sollte Vertragsprüfung, Risikoanalyse, abgeleitete Maßnahmen, Exit-Optionen und Leistungsmessung miteinander verbinden und den Vorgaben des BVR und des DGRV entsprechen.

Fazit

Ja, Auslagerungsmanagement kann auch einfach sein. Voraussetzung hierfür ist jedoch, dass entweder nur sehr wenige Auslagerungen bestehen oder das Auslagerungsmanagement durch geeignete Hilfsmittel unterstützt wird. Da in der Regel jedoch nicht wenige Auslagerungen vorliegen, wird in Zukunft der Einsatz einer toolbasierten Lösung für das Auslagerungsmanagement zur Reduzierung der Risiken unumgänglich sein.

Gerne beraten wir Sie bei der Implementierung eines angemessenen Auslagerungsmanagements. ▬

IT-Revision

Digitale Transformation im Kontext der IT-Revision

Der Anpassungsdruck auf Geschäftsmodelle und auf die dazugehörenden unterstützenden Geschäftsprozesse wächst und unterliegt immer kürzeren Zeitintervallen. Eine zentrale Rolle nimmt dabei die Digitalisierung ein. Sie ändert nahezu alle Unternehmensbereiche und -prozesse und somit auch die Anforderungen an die IT-Revision.

Unternehmen unterliegen einem zunehmenden Wettbewerbsdruck. Die Interaktion mit den Kunden ist im Rahmen der Globalisierung entscheidend für den Unternehmenserfolg und erfordert einen Abschied von bewährten Unternehmensstrukturen. Das Zauberwort lautet Digitalisierung. Die digitale Vernetzung ist eine grundlegende Voraussetzung für die Verbindung von Menschen, Maschinen und Dingen, denn notwendige Informationen müssen in einer sich stetig verändernden IT-Landschaft verlässlich ausgetauscht werden können.

Waren die Desktop-Anwendungen, web-basierten Interfaces und nativen Oberflächen für z. B. Smartphones noch überschaubar, so verwischt inzwischen die Grenze zwischen Mensch und Maschine, beispielsweise durch Weiterentwicklungen wie HTML 5. Eingabegeräte wie Maus, Tastatur und Touchscreen werden sukzessive durch die direkte Verarbeitung von Gesten, Sprache, Augen- und Körperbewegungen überflüssig. Die Interaktion zwischen Mensch und Maschine verändert sich in einem fortlaufenden digitalen Prozess.

Damit hat die digitale Transformation auch Auswirkungen auf die IT-Revision. Es konkretisieren sich alte Prüffelder, neue Prüffelder entstehen und bisherige Prüfungsansätze und Prüfungshandlungen werden mehr und mehr von technologischen Prüfverfahren unterstützt. Die IT-Revision muss sich den technischen und auch organisatorischen Herausforderungen der digitalen IT-Transformation stellen.

Was ist Digitalisierung?

Doch was ist Digitalisierung? Unter dem Begriff der Digitalisierung versteht man das „Umwandeln von analogen Werten in digitale Signale zur Verarbeitung oder Speicherung in einem digitaltechnischen System“. Die dabei gewonnenen Daten können dann informationstechnisch verarbeitet werden.

Nachdem die ersten industriellen Revolutionen noch die Mechanik vorantrieben, entwickelt das Zeitalter der vierten industriellen Revolution (Industrie 4.0) eine ganz neue Form wirtschaftlicher und sozialer Prozesse mit einer zunehmenden Vernetzung hin zur Globalisierung. Unternehmen nutzen immer mehr IT. Die innovativen Entwicklungen der letzten 15 Jahre belegen dies. So werden inzwischen

– Daten aus dem Web über Facebook, Google Suche, YouTube erhoben,
– Online-Handel wird z. B. über Amazon, Expedia, Zalando, iTunes betrieben,
– virtuelle soziale Kontakte werden über Plattformen wie Facebook, Flickr, Instagram, WhatsApp geknüpft oder gar
– Wissen und Nachrichten über Wikipedia, Twitter, Nachrichten- und Zeitungsportale verteilt.

Das Online verlagert sich zu Mobile mittels Smartphones, Tablets oder über die Nutzung digitaler Assistenten wie Amazon Echo. Die Entwicklung neuer Geschäftsmodelle wie Uber, Airbnb oder im privaten Bereich die Nutzung neuer User Interfaces wie Siri, Alexa, Cortana oder E-Book-Reader und nicht zuletzt die Möglichkeit, große Mengen von Daten in virtuellen Speicherplätzen bei Cloud Services wie z. B. Dropbox, Amazon und Microsoft zu parken, bereichern den digitalen Markt. Begleitet werden all diese Entwicklungen durch eine globale >

technische Vernetzung von Personen sowie physikalischen und virtuellen Objekten miteinander über das Internet.

RegTech (Regulatory Technology)

Der Zusammenhang zwischen Compliance und neuen Technologien wird immer öfter mit dem Begriff „RegTech" beschrieben. RegTech bezeichnet Unternehmen, die versuchen, neue Regulierungen, z. B. Gesetze oder Verordnungen, effizient umzusetzen. Sie positionieren sich quasi als technische Untergruppe der FinTechs (Financial Technology). Während FinTechs nach Lösungen oder neuen Produkten im Finanzsektor suchen, wird der Schwerpunkt bei RegTechs auf die Regulatorik gelegt.

Im Folgenden werden Technologien aufgezeigt, die im regulatorischen Umfeld einzeln oder in Kombination eingesetzt werden können:

- **Machine Learning**
  Versetzt IT-Systeme in die Lage, aus strukturierten und unstrukturierten Datenmengen und Algorithmen, Muster und Gesetzmäßigkeiten zu erkennen und Lösungen zu entwickeln.
- **Predictive Analytics**
  Unter Verwendung von Big Data und Machine-Learning-Technologien werden Datenbestände analysiert, um zukünftige Ereignisse und Resultate vorhersagen zu können.
- **Blockchain**
  Blockchain ermöglicht es, jede Art von Information in einer öffentlich einsehbaren Datenbank (z. B. Handelsplattformen, Zahlungssysteme) verfälschungssicher zu speichern, zu verarbeiten, zu teilen und zu verwalten.
- **Big Data**
  Tools, Werkzeuge und Programme zur schnellen und effizienten Auswertung komplexer, ggf. schwach strukturierter und heterogener Datenbestände
- **Robotic Process Automation (RPA)**
  Digitale Software-Roboter, die strukturierte Geschäftsprozesse automatisiert bearbeiten
- **Smart Contracts**
  Computerprotokolle, die (digitale) Verträge abbilden oder überprüfen oder die Verhandlung oder Abwicklung eines Vertrags technisch unterstützen können
- **Cloud Computing**
  Dynamische und bedarfsgerechte Bereitstellung von IT-Infrastruktur, IT-Plattformen und Services über ein Netzwerk zum Austausch von Daten oder zur Verarbeitung von Informationen
- **Application Interface (API)**
  Eine für Software zugeschnittene und maschinenlesbare (standardisierte) Programmschnittstelle zum Austausch und zur Weiterverarbeitung von Daten und Inhalten

Künstliche Intelligenz (KI)

Dazu gehört auch die Künstliche Intelligenz (KI) als eine Art Schlüsseltechnologie. Es handelt sich hier um den menschlichen Denkprozessen nachempfundene „intelligente" Problemlösungsverfahren zur Bewältigung komplexer Herausforderungen.

Während herkömmliche IT-Systeme vollständig programmiert werden mussten, lernen KI-Systeme selbstständig. Sie können sich und andere programmieren und damit entsprechend weiterentwickeln. Digitale Inhalte werden durch KI inhaltlich verstanden und nicht einfach nur maschinenlesbar gespeichert, übertragen und verarbeitet. Entscheidungen können so mit mehr Basiswissen unterstützt werden.

KI gehört zu den Technologien, die in unserem privaten und beruflichen Leben immer mehr an Bedeutung gewinnen. Bei der Internetsuche sowie der Nutzung von Online-Shops oder eines Sprachassistenten – „Hallo Alexa" – werden beispielsweise Verfahren der KI genutzt.

Wir Menschen nutzen KI in modernen Anwendungen so regelmäßig, dass es uns schon gar nicht mehr auffällt: auf großen Datenmengen basierende Wettervorhersagen, kontextbasiertes Suchen im Internet, biometrische Authentifizierung, teilautonomes Fahren, lernfähige Abwehr von Cyberangriffen, automatisierte Diagnose von Krankheiten anhand von Bilddaten etc.

AUTOR UND ANSPRECHPARTNER

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

Die Bundesregierung hat auf ihrem Digital-Gipfel im Juni 2017 wichtige Weichenstellungen in Richtung Big Data und KI vorgenommen. Offen ist, wie sich beispielsweise unsere Arbeitswelt in Zukunft mit KI-Systemen verändern wird und wie die Wahrung unserer persönlichen Freiheit und Selbstbestimmung aussehen wird sowie welche ethischen Grundprinzipien beachtet werden müssen.

Genossenschaftliche FinanzGruppe?

Auch in der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken hat das Zeitalter der Digitalisierung begonnen. Die in 2019 gestartete Digitalisierungsoffensive reagiert auf die Anforderungen der Digitalisierung und die sich ändernden Kundenbedarfe. Die Offensive zielt auf den Erhalt der Wettbewerbsfähigkeit ab. Über ein durchgängiges Omnikanal-Modell soll das „Digitale Banking" im Privat- und Firmenkundengeschäft als zukunftsfähiges Angebot ausgebaut werden. So können die Kunden schon seit längerem eine VR-BankingApp in den gängigen App-Stores downloaden und damit über ihre Smartphones Bankgeschäfte abwickeln.

Transformation der IT-Revision?

Regelmäßige Berichte über Datenklau oder Cyberspionage bezüglich Unternehmensdaten weisen darauf hin, dass Informationssicherheit und Datenschutzaspekte eine wichtige Rolle spielen, um die Sicherheit in den Unternehmen und ihre Positionierung am Markt zu gewährleisten.

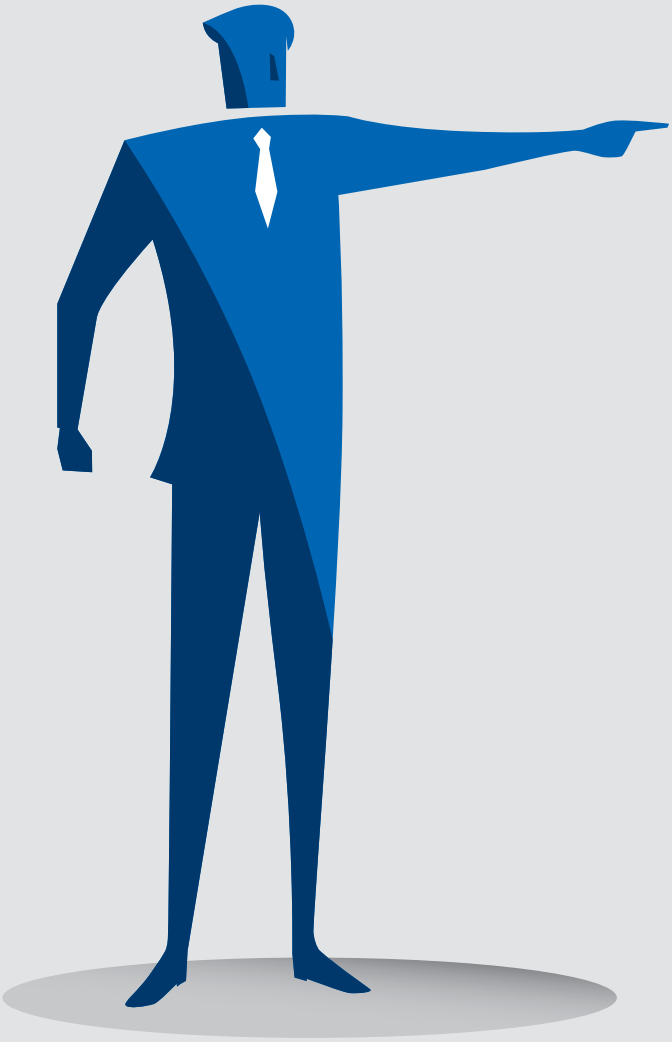
Das Aufgabenfeld der Internen Revision und hier explizit der IT-Revision wird durch die digitale Transformation komplexer und erweitert das Audit Universe mit seinen prüfungsrelevanten Inhalten. Dabei spielt die Prüfungsplanung eine zentrale Rolle, in der die DSGVO und die Informationssicherheit sich regelmäßig in den Managementprozessen wiederfinden. Schon bei der Analyse kann das im Unternehmen vorhandene Verarbeitungsverzeichnis Aufschluss geben, in welchen Geschäftsprozessen besonders schutzbedürftige, personenbezogene Daten digitalisiert verarbeitet werden.

Die Herausforderung zur Weiterbildung der IT-Revision im Hinblick auf die digitalen Veränderungen erfordert von den Unternehmen somit eine ständige Investition in zeitliche und finanzielle Ressourcen ihrer Internen Revision. Denn nur durch prozess- und risikoorientierte IT-Audits gelingt es, Risiken in der IT-Organisation und den IT-Anwendungen frühzeitig zu erkennen.

Mit unserem Angebot zur Auslagerung der IT-Revision eröffnet die DZ CompliancePartner GmbH einen sicheren Übergang in das digitale Zeitalter. ▬

In eigner Sache

Unterstützung Ihres Aus



Belastbares Vertragswerk

Die Bewertung einer Auslagerung setzt voraus, dass bereits im Vertragswerk Regelungen zu Service Level Agreements, Maßnahmen zur Nichterfüllung, zum Reporting und andere, in den MaRisk geforderte Parameter enthalten sind. Sie münden in ein geregeltes Berichtswesen, das eine valide Bewertung und Dokumentation unseres Unternehmens und der vereinbarten Dienstleistung zusammenfasst.

Als Ihr Compliance-Partner mit einem Angebotsportfolio, das überwiegend **wesentliche Auslagerungen** im Bereich des Beauftragtenwesens umfasst, prüfen wir regelmäßig unser Vertragswerk und auch unser Reporting auf die Erfüllung regulatorischer Anforderungen bzw. aufsichtsrechtlicher Prüfungspraxis und passen sie ggf. an.

Unsere Verträge entsprechen den Anforderungen der MaRisk (AT9) und der BAIT. Sie dokumentieren die

- Spezifizierung und ggf. Abgrenzung der von uns zu erbringenden Leistung,
- Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer,
- Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der gemäß § 25b Absatz 3 KWG zuständigen Behörden bezüglich der ausgelagerten Aktivitäten und Prozesse,
- Weisungsrechte, soweit erforderlich,
- Regelungen, die sicherstellen, dass wir datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachten,
- Kündigungsrechte und angemessene Kündigungsfristen,
- Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung, die sicherstellen, dass die bankaufsichtsrechtlichen Anforderungen weiterhin eingehalten werden,
- Verpflichtung, dass wir rechtzeitig über Entwicklungen informieren, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen könnten.

Die genannten Punkte dienen nicht nur dazu, den regulatorischen Anforderungen gerecht zu werden. Sie geben uns, und

lagerungsmanagements

damit auch Ihnen, einen Überblick über die Risikosituation. Zugleich monitoren sie die Leistungserfüllung.

Hinweis: Wir lassen derzeit unser Vertragswerk von dem Arbeitskreis Vertragsprüfung (DGRV) überprüfen. Sofern Änderungen erforderlich werden, werden wir diese natürlich umsetzen und ihnen Geltung verschaffen.

Abgesichert – interne und externe Prüfung

Vertrauen ist gut, Kontrolle besser: Diesen Gedanken verfolgen wir nicht erst seit der MaRisk-Novelle. Mit der internen und externen Prüfung möchten wir für Sie mehr Transparenz schaffen. Um Ihr Auslagerungsmanagement aktiv zu unterstützen,

- lassen wir unsere Dienstleistungen regelmäßig prüfen/testieren durch einen unabhängigen Wirtschaftsprüfer nach IDW 951 Typ II,
- lassen wir unsere Tools bzw. Module (u. a. Gefährdungsanalysen, Kontrollpläne und Kontrolldurchführungen) regelmäßig prüfen/testieren durch einen unabhängigen Wirtschaftsprüfer nach IDW PS 880,
- stimmen wir unsere Dienstleistungen, Produkte und Tools mit den Regionalverbänden über den Fachbeirat Beauftragtenwesen ab,
- werden unsere Dienstleistungen von der eigenen Internen Revision geprüft, und nicht zuletzt
- lassen wir bedarfsorientierte Musterrisikoanalysen von einem unabhängigen Wirtschaftsprüfer durchführen (z. B. zum Kauf durch die DZ BANK oder zur Integration des DZ BANK-Angebots in der Geldwäsche- und Betrugsprävention),
- lassen wir bedarfsorientiert Gutachten erstellen, so z. B. anlässlich des Rechenzentrumswechsels von der AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft.

Vernetzt

Schlussendlich sind wir ein Teil der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken und als solcher vernetzt über den

- **Aufsichtsrat der DZ CompliancePartner**
  Vorsitzender des Aufsichtsrats ist Michael Speth, Mitglied des Vorstandes der DZ BANK AG. Stellvertretende Vorsitzende ist Ulrike Brouzi, Mitglied des Vorstandes der DZ BANK AG. Weiteres Aufsichtsratsmitglied ist Monika van Beek, Mitglied des Vorstandes des Baden-Württembergischen Genossenschaftsverbandes.
- **Fachbeirat Beauftragtenwesen**
  Der Fachbeirat will verbandsübergreifend Sicherheit für Banken, Prüfer sowie Leiter Compliance und Beauftragte durch die „Validierung von Fachvorgaben“ und eine „ex ante prüferische Begleitung“ schaffen. Gleichzeitig werden (praktische) Erkenntnisse aus der Regulatorik und den Prüfungen thematisiert mit dem Ziel, auch gegenüber Ämtern und Behörden eine gemeinsame Auffassung zu festigen. Mitglieder des Fachbeirats sind die verantwortlichen Bereichsleiter der Grundsatzabteilungen der Regionalverbände sowie der Bereichsleiter Compliance der DZ BANK AG.
- **Kundenbeirat**
  Der Kundenbeirat bezieht aktiv und regelmäßig die Kunden der DZ CompliancePartner in die Produkt- und Dienstleistungsentwicklung ein. Durch seine beratende Funktion sollen mögliche Entwicklungspotenziale der Gesellschaft aufgezeigt und eine nachhaltige, marktorientierte Positionierung der Gesellschaft sichergestellt werden.

Zusammenfassend lässt sich festhalten, dass die aufsichtsrechtlich geforderten Regelungen Klarheit in der Zusammenarbeit und der gegenseitigen Vertragserfüllung geben. Für beide Vertragsparteien bieten sie Transparenz. Zudem dient der jährliche Bericht dazu, sich Gedanken zu machen, in welcher Beziehung Auftragnehmer und -geber stehen. Ein Punkt, der im Übrigen beiden Vertragspartnern auch Entwicklungschancen aufzeigen kann. (red.) ▬

MaRisk-Compliance

Nachhaltigkeit – und nun?

Am 20. Dezember 2019 wurde das „Merkblatt zum Umgang mit Nachhaltigkeitsrisiken“ auf der BaFin-Homepage veröffentlicht. Das Merkblatt setzt sich auf rund 40 Seiten mit sogenannten Nachhaltigkeitsrisiken auseinander. Unter Nachhaltigkeitsrisiken versteht die BaFin Ereignisse oder Bedingungen aus den Bereichen Umwelt, Soziales oder Unternehmensführung, deren Eintreten tatsächlich oder potenziell negative Auswirkungen auf die Vermögens-, Finanz- und Ertragslage sowie die Reputation eines beaufsichtigten Unternehmens haben kann. Auch geht das Merkblatt auf physische und transitorische Risiken ein. Die BaFin betont hierbei, dass die bestehenden gesetzlichen Vorgaben durch die MaRisk, MaGo und KAMaRisk in jedem Fall zu beachten sind und Nachhaltigkeitsrisiken auf die bekannten Risikoarten einwirken.

Im Vergleich zum Konsultationspapier (vgl. PoC 3/2019, S. 15) stellt die BaFin nun deutlicher heraus, dass es sich bei den im Merkblatt aufgezeigten Grundsätzen und Prozessen um sinnvolle, unverbindliche Verfahrensweisen handelt (Good-Practice-Ansätze), an denen sich die Unternehmen bei der unternehmensindividuellen Behandlung von Nachhaltigkeitsrisiken orientieren können.

Dies wird im Merkblatt auch dadurch deutlich, dass an verschiedenen Stellen die Formulierungen entschärft werden und wiederholt im Konjunktiv formuliert wird bzw. Wörter wie „sollte“, „könnte“ oder „erscheine“ verwendet werden. Auch wurden diverse Passagen aus dem Konsultationspapier gelöscht. So ist insbesondere unter Ziffer 4.1 nicht mehr von einer speziellen Nachhaltigkeitseinheit die Rede. Darüber hinaus obliegt der Compliance-Funktion nicht mehr die Überwachung der Implementierung wirksamer Verfahren zur Einhaltung der gesetzlichen Anforderungen im Hinblick auf die Nachhaltigkeit, sondern sie soll nur noch ihre Aufgaben im Sinne der MaRisk auch mit Blick auf die rechtlichen Anforderungen zur Nachhaltigkeit ausführen. Grundsätzlich sind die Struktur und die Themenblöcke, von minimalen Ausnahmen abgesehen, im Vergleich zum Konsultationspapier nicht geändert wurden.

Breiten Raum nimmt nach wie vor das Risikomanagement ein. Hier ist der Absatz 6.1.3 aus dem Konsultationspapier gelöscht worden, der auf die Identifizierung von Nachhaltigkeitsrisiken auch in den Risikobereichen operationelles Risiko, Reputationsrisiko und strategisches Risiko einging. Gleichwohl beschreibt das Merkblatt ausführlich Risikoidentifikations-, -steuerungs- und Controllingprozesse sowie klassische Methoden und Verfahren in Bezug auf Nachhaltigkeitsrisiken. Weiterhin werden Stresstests einschließlich Szenarioanalysen beschrieben.

Auch wenn das Merkblatt als Kompendium unverbindlicher Verfahrensweisen vorgestellt wird, so betont die BaFin zugleich, „sie erwarte, dass die beaufsichtigten Unternehmen eine Auseinandersetzung auch mit Nachhaltigkeitsrisiken sicherstellen und dies nachweislich dokumentieren.“

Der quasi verbindliche Anspruch wird auch dadurch deutlich, dass Felix Hufeld als Präsident der BaFin in Interviews die Erwartung der BaFin geäußert hat, „dass Unternehmen schon jetzt ihre Angemessenheitsrisiken angemessen steuern“, und prognostiziert, „dass in den kommenden Jahren entsprechende Standards auf europäischer Ebene verbindlich festgelegt werden“. Daher ist es nicht überraschend, dass die BaFin das Merkblatt ebenfalls in englischer Sprache veröffentlicht hat. Fast zeitgleich veröffentlichte die BaFin die Aufsichtsschwerpunkte für das Jahr 2020. Von den vier Prüfungsschwerpunkten befassen sich zwei Aufsichtsschwerpunkte mit der Thematik „Nachhaltige Geschäftsmodelle“ und „Nachhaltige Finanzwirtschaft, Sustainable Finance“.

Gerne unterstützen wir Sie bei der Umsetzung. Auf Wunsch stellen wir Ihnen einen Quick-Check zur Verfügung. Sprechen Sie uns an. ▬

AUTOREN UND ANSPRECHPARTNER

Axel Hofmeister
Beauftragter MaRisk-Compliance,
E-Mail: axel.hofmeister@dz-cp.de

Jörg Scharditzky
Beauftragter MaRisk-Compliance,
E-Mail: joerg.scharditzky@dz-cp.de

Interne Revision

Seit der letzten Berichterstattung in der Point of Compliance (3/2019, S. 30) wurden entsprechend der Jahresprüfungsplanung 2019 die Berichte zu den Prüffeldern „MaRisk-Compliance“, „Geldwäsche- und Betrugsprävention und Compliance-Spezialisten“, Unternehmenssteuerung – Vertragswesen – Interne Compliance“, „IT & Projekte – IT-Systeme“, „Unternehmenssteuerung – Rechnungswesen & Controlling“, „Informationssicherheit & Datenschutz“ und „Unternehmenssteuerung – Risikomanagement“ abgeschlossen und veröffentlicht.

Die Berichte zu den Bereichen „MaRisk-Compliance“, „Geldwäsche- und Betrugsprävention und Compliance-Spezialisten“, „IT & Projekte – IT-Systeme“ und „Informationssicherheit & Datenschutz“ wurden jeweils als dienstleistungsbezogener Bericht an unsere Mandantschaft versandt. Der Bericht für den Bereich „IT-Audit“ ist derzeit in der Endabstimmung. Die Quartalsberichte zum dritten und vierten Quartal 2019 wurden turnusgemäß erstellt und ebenfalls unserer Mandantschaft zur Verfügung gestellt.

Der interne Jahresprüfungsplan für 2019 wurde vollständig erfüllt. Für das Jahr 2020 wurde eine risikoorientierte Jahresplanung erstellt und der Geschäftsführung zur Genehmigung vorgelegt.

Die externe Prüfung der Geschäftsbereiche „MaRisk-Compliance“, „WpHG-Compliance“ und „Geldwäsche- und Betrugsprävention“ nach IDW PS 951 (Typ 2) sowie die externe Prüfung des Geschäftsbereichs „Informationssicherheit & Datenschutz“ nach IDW PS 951 (Typ 1) wird derzeit von der AWADO GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft vorgenommen. Die Endfassungen der Berichte zur externen Prüfung wurden von der Prüfungsgesellschaft für Ende Februar 2020 angekündigt und werden danach 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 für Ende Februar 2020 angekündigt und wird danach versandt.

Darüber hinaus wurde turnusgemäß je ein Follow-up-Quartalsbericht für das dritte und vierte Quartal 2019 erstellt und der Geschäftsführung der DZ CompliancePartner GmbH vorgelegt. In den Follow-up-Berichten wird die Abarbeitung der von internen und externen Prüfern getroffenen Empfehlungen dokumentiert. Die Anzahl der offenen Punkte ist erfreulicherweise rückläufig – auch unter Einbeziehung der neuen Prüfungsergebnisse (s. o.). 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

Die wirtschaftliche Entwicklung der DZ CompliancePartner GmbH ist weiterhin positiv. Das Jahresergebnis 2019 nach Steuern liegt bei ca. 1,4 Mio. Euro bei einem Umsatz von ca. 15 Mio. Euro. Die Integration des DZ BANK-Angebots „Geldwäsche- und Betrugsprävention“ in die DZ CompliancePartner GmbH war zum Teil mit Mehraufwendungen verbunden. Hierzu zählt beispielsweise der Betrieb eines neuen Standorts, aber auch notwendige Investitionen in Hardware, Software und Möbel. Gleichzeitig haben wir ein Wachstum in allen Beauftragtenthemen wahrnehmen können. Insbesondere der Bereich Geldwäsche- und Betrugsprävention entwickelte sich sehr positiv: Mittlerweile betreut die DZ CompliancePartner GmbH in diesem Thema gut die Hälfte aller Genossenschaftsbanken. Aber auch die übrigen Fachbereiche haben zu einer Erlösüberschreitung von insgesamt 6 % über Plan beigetragen.

In 2020 sind vor allem Investitionen in Personal und IT geplant. Eine Herausforderung stellt die schwierige Situation am Arbeitsmarkt dar. Sie wirkt sich unmittelbar auf unsere Aufnahmekapazitäten für Neumandate aus. Wir sind deshalb beständig auf der Suche nach geeigneten Fachkräften in allen Beauftragtenbereichen, aber auch im Backoffice (insbesondere IT). ▬

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