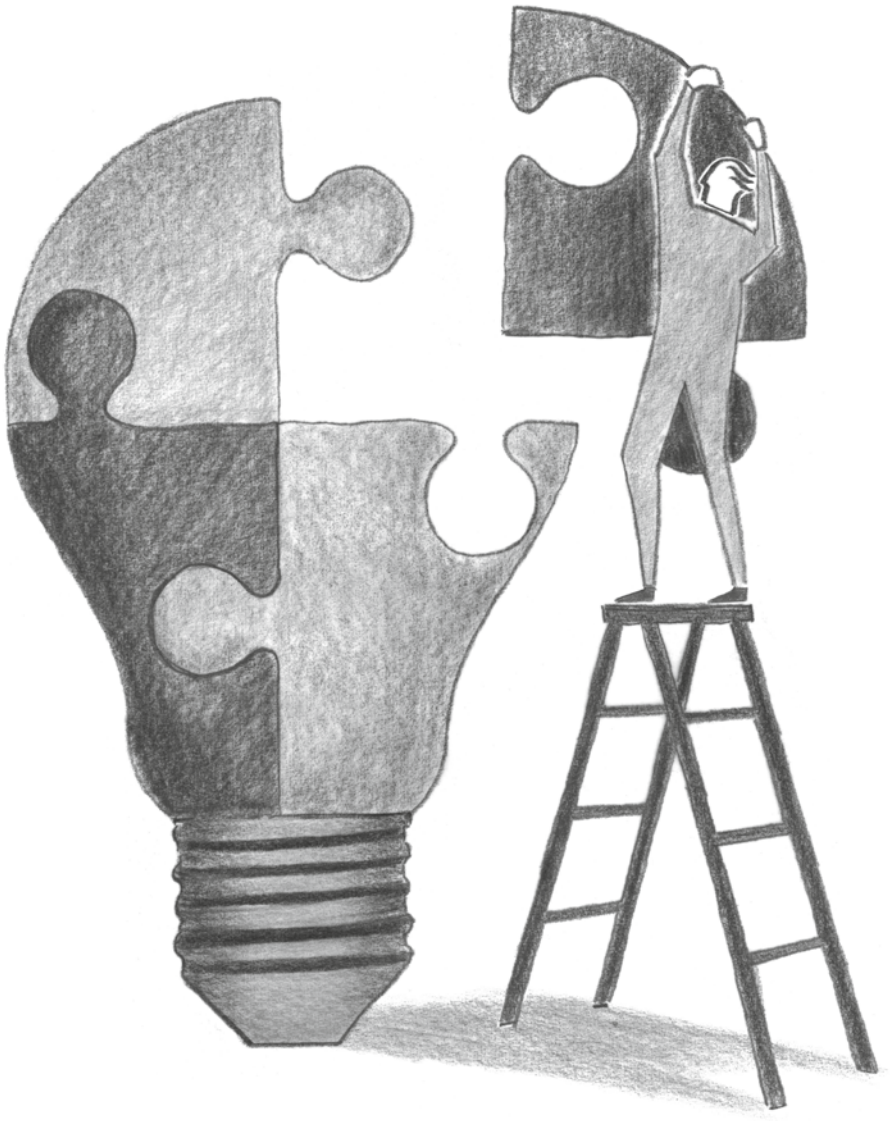
Ausgabe 2 / 2018

GenoTec GmbH

Point of Compliance

Das Risikomanagement-Magazin
für unsere Kunden und Geschäftspartner



Integrierte Compliance

IMPRESSUM

Point of Compliance
Das Risikomanagement-Magazin für unsere Kunden und Geschäftspartner, Ausgabe 19, 2/2018
ISSN: 2194-9514
Herausgeber: GenoTec GmbH, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3324, Telefax 069 6978-3322, www.geno-tec.de
Handelsregister HRB 11105, Amtsgericht Offenbach, USt.-IdNr.: DE201150917
Geschäftsführung: Jens Saenger (Sprecher), Andreas Marbeiter
Verantwortlich i. S. d. P. :
Jens Saenger

Redaktion: Gabriele Seifert, Leitung (red.)
Redaktionsanschrift: GenoTec GmbH, Redaktion Point of Compliance, Wilhelm-Haas-Platz, 63263 Neu-Isenburg, Telefon 069 6978-3188, Telefax 069 6978-3322, E-Mail: poc@geno-tec.de
Weitere Autoren dieser Ausgabe:
Klaus Bellmann, Thomas Grebe, Iris Hauptführer, Martin Hierlemann, Michael Müller, Martin Reglinski, Jens Saenger, Norbert Schäfer, Sandra Sitter, Michael Switalla, Dominik Tiburtius
Bildnachweise: GenoTec GmbH, iStockphoto
Gestaltung und Titelillustration:
EGENOLF DESIGN, Wiesbaden
studio@egenolf-design.de
Druck: odd GmbH & Co. KG · Print und Medien
www.odd.de

Redaktionsschluss: 17. September 2018
Auflage: 2.600 Exemplare
Die aktuellen Mediadaten finden Sie im Internet unter www.geno-tec.de/poc

Jens Saenger
Sprecher der Geschäftsführung

Das Beauftragtenwesen war lange Zeit eine Kontrollfunktion. Stichprobenartig wurden die Aufbau- und Ablauf-organisation untersucht. Im Wesentlichen implizierte das Beauftragtenwesen viel, mitunter redundanten Aufwand in marktfernen Bereichen ohne nennenswerten Mehrwert.

Die Schutzansprüche und damit auch die aufsichtsrechtlichen Anforderungen sind allerdings in den vergangenen Jahren enorm gestiegen. Heißt das aber automatisch auch mehr Aufwand?

Ob Zentrale Stelle, MaRisk-Compliance, WpHG-Compliance, Informationssicherheit oder Datenschutz, sie alle folgen heute der gleichen Logik: In allen Bereichen bestimmt eine Risikoanalyse den Kontrollplan und die abzuleitenden Kontrollmaßnahmen. In allen Bereichen wird eine systemische Unterstützung nicht nur von der Aufsicht akzeptiert, sondern gefordert.

Heute bedarf es eines Compliance Management System, das die Anforderungen integriert und automatisiert umsetzt und in stabile und nachvollziehbare Prozesse überführt. Nur so können die Schutzinteressen effektiv gewahrt werden. Und nur so lässt sich der Aufwand im Tagesbetrieb bzw. bei der Einspielung neuer aufsichtsrechtlicher Anforderungen in einem betriebswirtschaftlich sinnvollen Maß darstellen.

Faktisch geht mit dem Ausbau der Schutzmaßnahmen ein Schulterschluss der Fachdisziplinen und eine veränderter Perspektive einher. Es zeichnet sich ein integrierter und prozessorientierter Ansatz ab, der das (frühere) Beauftragtenwesen in eine „Integrierte Compliance" überführt. Unter dem Strich erlangt die Bank nicht nur mehr regulatorische Souveränität, sondern sie gewinnt auch ein Stück unternehmerische Freiheit zurück.

Ich wünsche Ihnen eine anregende Lektüre.

Ihr Jens Saenger

Grußwort

Ein sicheres und betriebswirtschaftlich sinnvolles Beauftragtenwesen

von Dipl.-Ök. Klaus Bellmann

Die DZ BANK AG und die Gesellschafter der GenoTec GmbH – der Genossenschaftsverband Verband der Regionen e.V., der Baden-Württembergische Genossenschaftsverband e.V., der Genossenschaftsverband Weser-Ems e.V. und die Fiducia & GAD IT AG – haben am 17. September 2018 den Verkauf der GenoTec-Gesellschaftsanteile an die DZ BANK vereinbart.

Damit ist die GenoTec 100-prozentige Tochtergesellschaft der DZ BANK. In einem zweiten Schritt werden die Auslagerungsangebote für Compliance- und Beauftragtentätigkeiten der DZ BANK mit denen der GenoTec zusammengeführt. Wir, die bisherigen Gesellschafter der GenoTec, werden die Entwicklung der Gesellschaft in Zukunft über die Einbindung in die Gremien weiter eng begleiten.

Die Zusammenführung zielt auf eine Bündelung der Kräfte im Beauftragtenwesen ab. Seit Ende 2017 befanden wir uns im Gespräch mit der DZ BANK, um die Dienstleistungen zur Erfüllung regulatorischer Anforderungen zu bündeln und einen leistungsstarken, auf die spezifischen Interessen der Genossenschaftsbanken ausgerichteten Lösungsanbieter zu etablieren. Ziel ist es, die Bank vor Ort qualifiziert zu unterstützen.

Sowohl die DZ BANK als auch die GenoTec sind seit vielen Jahren als Auslagerungspartner im Bereich Compliance- und Beauftragtenwesen tätig. Beide Unternehmen haben sich den immer komplexer werdenden Herausforderungen der Bankenregulierung in den vergangenen Jahren erfolgreich gestellt. Der Handlungsdruck im regulatorischen Umfeld wird jedoch weiter steigen und künftig deutlich höhere (Umsetzungs-) Aufwendungen für die Genossenschaftsbanken mit sich bringen.

schaftlich auf lange Sicht

Dipl.-Ök. Klaus Bellmann
Vorsitzender der Gesellschafterversammlung
der GenoTec GmbH
Vorstandsmitglied des Genossenschaftsverbands –
Verband der Regionen e.V.

Wir sind davon überzeugt, dass die Zusammenführung des Know-hows notwendig ist, um den wachsenden Anforderungen adäquat begegnen zu können.

Der steigenden Komplexität setzen wir einen gemeinsamen, prozessorientierten und integrierten Ansatz entgegen, der die Bank vor Ort entlastet. Gleichzeitig werden wir vereint unsere spezifischen Interessen auch gegenüber der Aufsicht besser wahrnehmen können.

Die GenoTec hat sich in den 20 Jahren ihres Bestehens zu einem Spezialisten im Beauftragtenwesen entwickelt. Heute führt sie als Mehrmandantenanbieter das Know-how aus über 500 Mandaten zusammen. Gleichzeitig hat sie ein Compliance Management System aufgebaut, das die standardisierte, nachvollziehbare und sichere Umsetzung regulatorischer Anforderungen ermöglicht. Ihr Auftrag war (und wird es auch künftig sein), sichere und betriebswirtschaftlich sinnvolle Beauftragtendienstleistungen anzubieten und die Auslagerungsoption offenzuhalten. Dies ist ihr in hervorzuhebender Weise gelungen.

Wir, die bisherigen Gesellschafter, bedanken uns für das Geleistete: Dem Team um Jens Saenger und Andreas Marbeiter gehört unsere Anerkennung. ▬

Gastbeitrag

Ein Jahr FIU

Die Bilanz nach einem Jahr ist durchwachsen: Die Verlagerung der Zuständigkeit für die Bearbeitung von Geldwäsche-Verdachtsmeldungen stellt nach Auffassung vieler Experten in ihrer derzeitigen Ausgestaltung ein Hindernis für eine wirksame Bekämpfung von Geldwäsche- und Terrorismusfinanzierung in Deutschland dar.

Die Financial Intelligence Unit (FIU) – Zentralstelle für Finanztransaktionsuntersuchungen – wurde zum 26. Juni 2017 unter dem Dach der Generalzolldirektion eingerichtet. Kerntätigkeit der FIU ist u.a. die Entgegennahme von Verdachtsmeldungen und deren erste Bewertung. Der geplante Aus- und Aufbau des Personalbestandes ist nach wie vor nicht abgeschlossen.

Standardisierte Meldewege

Für die Verpflichteten ist die neue FIU seit Ende Juni 2017 insbesondere durch veränderte Meldewege bei der Abgabe einer Verdachtsmeldung erlebbar geworden. Mit Einrichtung des elektronischen Portals goAML und der standardisierten Abgabe von Verdachtsmeldungen ab dem 1. Februar 2018 über diesen Meldeweg wurde das Verdachtsmeldewesen sowohl für Verpflichtete als auch für die FIU effizienter gestaltet.

Der bürokratische Aufwand durch Übermittlung per Fax wurde durch den internetbasierten Meldeweg zwar deutlich verringert. Gleichzeitig ist die FIU aber bisher nicht von ihrer (nicht nachvollziehbaren) Anforderung abgewichen, alle nach gleichem Muster verlaufenden verdächtigen Transaktionen einzeln durch die Verpflichteten umständlich erfassen zu lassen. Wünschenswert wäre, zu erlauben, eine entsprechende Anlage beizufügen. Auch der Prozess einer Folge- bzw. Nachmeldung müsste für die Verpflichteten deutlich schlanker gestaltet sein.

Leider sind auch die Anfangsschwierigkeiten der neuen FIU noch nicht gelöst. Mehrere Medien berichten über deutliche Rückstände bei der Verdachtsfallbearbeitung auch in der jüngeren Vergangenheit. Und auch wir, als Insourcing-Partner im Bereich Geldwäsche- und Betrugsprävention, beobachten mit Sorge, dass noch nicht alle Verdachtsmeldungen auf Behördenseite zeitnah bearbeitet werden. Hinzu tritt die Problematik, dass entgegen der rechtlichen Verpflichtung aus § 41 Abs. 2 GwG eine Rückmeldung der FIU an die Verpflichteten hinsichtlich der Relevanz der jeweiligen Verdachtsmeldung derzeit faktisch nicht erfolgt.

Tatsächlich ist die FIU Medienberichten zufolge weiterhin personell unterbesetzt. Danach werden über 100 studentische Hilfskräfte und Langzeitarbeitslose sowie zahlreiche Zollbedienstete auf Abordnungsbasis im Bereich der Datenerfassung eingesetzt. Zudem kann die FIU auch strukturell ihrer „Filterfunktion“ noch nicht in dem eigentlich vorgesehenen Umfang nachkommen.

Wirksamkeit von Verdachtsmeldungen

Insbesondere bei der Beurteilung von Verdachtsmeldungen durch die FIU und ihrer zügigen Weiterleitung an die zuständigen Landeskriminalämter scheint es noch „Luft nach oben“ zu geben. So berichtete Spiegel Online Anfang August 2018 von immer noch bestehenden massiven Schwierigkeiten. Landeskriminalämter und Staatsanwaltschaften – so die Kritik aus den Landesbehörden – bekämen Verdachts-

AUTOR UND ANSPRECHPARTNER

Norbert Schäfer
Abteilungsdirektor – Abteilungsleiter
Insourcing Finanzkriminalität,
DZ BANK AG,
E-Mail: norbert_schaefer@dzbank.de

meldungen zum Teil verspätet oder nur unzureichend aufbereitet. Das LKA Thüringen wird von Spiegel Online (20. März 2018) sogar wie folgt zitiert: „Es sei im Einzelfall zu prüfen, ob die zögerliche Bearbeitung der Geldwäsche-Verdachtsanzeigen nicht den Tatbestand der Strafvereitelung im Amt erfülle, heißt es in dem Papier in Erfurt."

Politisch wird die Diskussion zusätzlich angefacht, weil Deutschland als „Paradies für Geldwäscher" gilt. Beispielsweise gibt es hierzulande – anders als in anderen EU-Ländern – keine Restriktionen bei der Bezahlung mit Bargeld. Es fehlt zudem eine bundeseinheitliche, wirksame Aufsicht für Verpflichtete aus dem Nichtfinanzsektor (u. a. Immobilienmakler, Autohändler, Kunsthandel), analog der BaFin.

Unterm Strich stellt sich manch einer die Frage nach Wirksamkeit und Sinnhaftigkeit von Verdachtsmeldungen. Dies umso mehr, als Verpflichtete aufgrund fehlender Rückmeldungen durch die Behörde derzeit nur mutmaßen können, ob eine Verdachtsmeldung mehr oder weniger wertvoll für die Strafverfolgung gewesen ist. Diesbezüglich hat die FIU allerdings auf ihrer ersten Geldwäschetagung mit Verpflichteten und Verbänden des Finanzsektors am 26. Februar 2018 eine erste Lösung in Aussicht gestellt: Mit verpflichtender elektronischer Meldungsabgabe zum 1. Februar 2018 sind auch die Arbeiten für ein Rückmeldungskonzept intensiviert worden. Es werden Indikatoren erarbeitet, anhand derer über verschiedene Kategorien schrittweise Rückmeldungen an die Verpflichteten erfolgen werden.

Fakt ist: Es obliegt jedem einzelnen nach GwG Verpflichteten, für die Einhaltung der geldwäscherechtlichen Pflichten Sorge zu tragen. Liegen Auffälligkeiten im Hinblick auf ein oder mehrere Transaktionen oder Geschäftsbeziehungen vor, ist unmittelbar der Geldwäschebeauftragte zu informieren. Er entscheidet über weitere Maßnahmen, insbesondere über die Abgabe einer Verdachtsmeldung nach § 43 GwG. Dabei dürfen mögliche Bearbeitungsengpässe oder andere Hindernisse auf Behördenseite keinerlei Rolle spielen.

Fazit

Die Verdachtsmeldungen nach dem GwG lassen sich von den Verpflichteten heute grundsätzlich einfacher und schneller übermitteln als noch vor einem Jahr. Leider scheint eine zügige Weiterverarbeitung nicht in jedem Fall garantiert. Medienberichte lassen bei den Verpflichteten mitunter ein unbefriedigendes Gefühl zurück: die Angst, dass das eigene Institut für Geldwäsche missbraucht wird – ohne effektiv dagegen vorgehen zu können. Experten äußern weiterhin Zweifel, inwieweit es überhaupt gelingen wird, die FIU in ihrer aktuellen Konzeption funktionsfähig auszubauen.

Umso wichtiger ist es, die den Verpflichteten obliegenden Pflichten konsequent zu erfüllen. Das heißt insbesondere auch, den Geldwäschebeauftragten bei Auffälligkeiten und Fragen unverzüglich zu kontaktieren. Er kennt die notwendigen Schritte. ▬

Geldwäscheprävention

Update Geldwäscheprävention

Mit der 5. Geldwäscherichtlinie stellt sich der Gesetzgeber der digitalen, global vernetzten Realität und schafft mehr Transparenz. Banken müssen mit erhöhtem Aufwand rechnen – auch wenn dieser verglichen mit der 4. Geldwäscherichtlinie vergleichsweise gering ausfallen dürfte.

Am 19. Juni 2018 ist die 5. Richtlinie zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung im Amtsblatt der EU veröffentlicht worden. Bereits am 9. Juli 2018 ist sie in Kraft getreten und von den Mitgliedsstaaten bis 10. Januar 2020 umzusetzen.

Unterdessen stehen die Anwendungs- und Auslegungshinweise der BaFin sowie letzte Umsetzungsmaßnahmen, wie beispielsweise die Nationale Risikoanalyse, für die vor einem Jahr im Juni 2017 in nationales Recht umgesetzte 4. Geldwäscherichtlinie nach wie vor aus.

Nun also noch im laufenden Prozess die 5. Geldwäscherichtlinie, die die Geldewäscherichtlinien erneut ergänzt bzw. ändert. Sie bezieht insbesondere die bei den jüngsten Terroranschlägen aufgetretenen Tendenzen, wie beispielsweise die Nutzung von alternativen Finanzsystemen, mit ein. Sie will darüber hinaus die Transparenz von Transaktionen erhöhen und die Vernetzung von Personen und Gesellschaften nachvollziehbarer machen. Des Weiteren stellt die zunehmende Annäherung von organisierter Kriminalität und Terrorismus eine erhöhte Sicherheitsbedrohung dar. Auch auf diese reagiert die 5. Geldwäscherichtlinie.

Erfreulicherweise sind einige Punkte, die in der Praxis sehr aufwandsintensiv gewesen wären, nicht in die finale Richtlinie eingeflossen. Die im Vorfeld diskutierte Herabsetzung der relevanten Beteiligungsschwelle auf 10 % bei wirtschaftlich Berechtigten wurde beispielsweise nicht aufgenommen. Nachfolgend erhalten Sie einen ersten Überblick über die maßgeblichen Änderungen, die Hintergründe und die damit verfolgten Intentionen.

Letztlich bleibt jedoch der erste Referentenentwurf im Rahmen der nationalen Gesetzgebung abzuwarten. Erst dann sind die tatsächlichen Auswirkungen adäquat zu beurteilen. Die nachfolgenden Wertungen verstehen sich daher auch nur als erste Einschätzungen.

1. Erweiterung des Anwendungsbereichs auf virtuelle Währungen

Die zunehmende Anonymisierung durch die Möglichkeiten von Kryptowährungen (siehe auch Beitrag in der PoC 1/2018 „Bitcoin – Mythos und Realität“) verändert auch die Geldwäsche und die Terrorismusfinanzierung. Mit der neuen Richtlinie wird die Regulierung von virtuellen Währungen initiiert, indem entsprechende Dienstleistungsanbieter (u. a. Tauschbörsen und E-Wallet-Anbieter) nun ebenfalls die Anforderungen aus dem Geldwäschegesetz erfüllen müssen.

Ein weiterer Aspekt sind anonyme Guthabenkarten. Um den Missbrauch von anonymen Guthabenkarten einzuschränken, wird der Schwellenwert zur Sorgfaltspflichtenerfüllung auf 150 Euro abgesenkt. Bei Fernzahlungsvorgängen, bei denen der Betrag mehr als 50 Euro beträgt, ist die Identität des Kunden künftig zu identifizieren.

2. Identitätsprüfung bei wirtschaftlich Berechtigten, sofern diese Mitglied der Führungsebene sind

Wenn der ermittelte wirtschaftlich Berechtigte gleichzeitig ein Angehöriger der Führungsebene (in der Regel Geschäftsleitung) des Unternehmens ist, wird die Identität dieser Person künftig zu überprüfen sein.

In der Praxis werden die Mitglieder der Geschäftsleitung in den meisten Fällen ohnehin als vertretungsberechtigte Personen identifiziert. Somit wird es entscheidend sein, wie groß der Umfang dieser neuen „Identitätsprüfung“ sein soll.

3. Ermittlung des wirtschaftlich Berechtigten bei Geschäftsbeziehungen zu Drittstaaten mit hohem Risiko

Bei Geschäftsbeziehungen zu Personen in Drittstaaten mit hohem Risiko müssen bereits heute die verstärkten Sorgfaltspflichten gemäß § 15 GwG erfüllt werden.

Diese Thematik soll nun dahingehend erweitert werden, dass auch Informationen über die Mittelherkunft (Herkunft des Vermögens) der wirtschaftlich Berechtigten eingeholt werden müssen. Auch wenn die Anwendungsfälle vergleichsweise selten sein sollten, bleibt die Frage offen, wie diese Anforderung in der Praxis umgesetzt werden könnte.

4. Erstellung einer nationalen PEP-Funktionsliste durch den jeweiligen Mitgliedsstaat

Damit politisch exponierte Personen länderübergreifend in der EU praxisnah identifiziert werden können, haben die Mitgliedsstaaten entsprechende Listen/Register zu erstellen.

Diese müssen mindestens die Definition/Aufstellung wichtiger öffentlicher Ämter enthalten und sind stets auf dem neuesten Stand zu halten.

5. Erstellung eines nationalen Immobilienregisters

Der nationale Gesetzgeber wird dazu verpflichtet, sicherzustellen, dass zentrale Meldestellen (FIU/Zoll) und andere zuständige Behörden Abfragemöglichkeiten zu Immobilieneigentum erhalten. Das Register soll die zeitnahe Identifizierung aller natürlichen und juristischen Personen ermöglichen, die Eigentümer von Immobilien sind.

6. Öffnung des Transparenzregisters für die Öffentlichkeit

Um die Transparenz der Eigentumsverhältnisse bei Kapital-, Personengesellschaften und Stiftungen zu erhöhen, ist ein besserer Zugang zu den Registern der wirtschaftlichen Eigentümer (in Deutschland: Transparenzregister) vorgesehen. Die Registerinformationen sollen künftig zugänglich sein für die

- zuständigen Behörden und zentralen Meldestellen (keine Einschränkung),
- Verpflichteten im Rahmen der Erfüllung der Sorgfaltspflichten,
- Öffentlichkeit (mit Einschränkungen).

Wichtig ist, dass die Verpflichteten im Rahmen der Erfüllung der Sorgfaltspflichten die Registerdaten verwenden dürfen, ohne diese durch weitere eigene Maßnahmen plausibilisieren zu müssen. Die nationale Gesetzgebung muss also sicherstellen, dass die Daten im Register verbindlich nutzbar sind.

Ebenso soll ein öffentlicher Zugang zu Informationen über die wirtschaftlichen Eigentümer von Trusts bei berechtigtem Interesse oder auf schriftlichen Antrag (Trusts, die im Besitz einer nicht in der EU registrierten Gesellschaft sind) geschaffen werden.

Nach Löschung einer Gesellschaft oder einer anderen juristischen Person aus dem Register müssen die Daten für mindestens fünf Jahre öffentlich zugänglich bleiben.

Die Daten, die der Öffentlichkeit zugänglich gemacht werden, sollen allgemeiner Art sein, damit mögliche Beeinträchtigungen für wirtschaftlich Berechtigte auf ein Mindestmaß beschränkt werden. Im Wesentlichen sind die Stellung der wirtschaftliche Berechtigten sowie die Tätigkeit von Interesse. Bei den fiktiven wirtschaftlich Berechtigten, ist eine entsprechende Kennzeichnung vorgesehen.

7. Definition von Rechtsgestaltungen hinsichtlich der Einordnung als Trust

Weil sich die gesetzlichen Anforderungen innerhalb der einzelnen Mitgliedsstaaten zum Teil erheblich unterscheiden, werden Trusts und ähnliche Rechtsgestaltungen heute nicht zentral registriert. Künftig ist auch hierfür ein entsprechendes Register zu schaffen. Dies soll u. a. Mehrfachregistrierungen in unterschiedlichen Ländern unterbinden.

8. Einrichtung umfassender Statistiken zur Wirksamkeitsüberprüfung

Jeder Mitgliedsstaat wird dazu verpflichtet, umfassende Statistiken über Faktoren zu führen, die einerseits für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung und andererseits für die Wirksamkeit solcher Bekämpfungssysteme relevant sind. Inhaltlich umfasst dies folgende Angaben:

- Mess- und Größendaten zu Sektoren des Verpflichtetenkreises
- Mess- und Größendaten zu Verdachtsmeldungen, Untersuchungen und behördlichen Verfahren
- Informationen zum Nutzen, zu Maßnahmen und Jahresberichten

>

AUTOREN UND ANSPRECHPARTNER

Michael Müller
Geldwäschebeauftragter,
E-Mail: michael.mueller@geno-tec.de

Dominik Tiburtius
Leiter Überwachung & Kontrolle,
E-Mail: dominik.tiburtius@geno-tec.de

- Daten zum (grenzüberschreitenden) Informationsaustausch
- Daten zum eingesetzten Personal der zuständigen Behörden
- Kennzahlen zu festgestellten Verstößen und deren Sanktionen

9. Erweiterung der Faktoren für ein potenziell höheres Risiko

Hinsichtlich der im GwG aufgeführten Risikofaktoren ist ebenfalls von einer Anpassung auszugehen. Hinzu kommen beispielsweise bestimmte Situationen von Drittstaatsangehörigen (z. B. Antrag auf Aufenthaltsrechte in Verbindung mit Kapitalüberträgen (‚Investoren')) oder Transaktionen in Bezug auf Öl, Waffen, Edelmetalle, Tabakerzeugnisse, Kulturgüter und andere Artikel von archäologischer, historischer, kultureller oder religiöser Bedeutung oder von außergewöhnlichem wissenschaftlichem Wert sowie Elfenbein und geschützte Arten.

Fazit

Die Änderungen, die durch die 5. Geldwäscherichtlinie zu erwarten sind, erscheinen im Vergleich zur 4. Geldwäscherichtlinie hinsichtlich der Auswirkungen auf die Verpflichteten zunächst weniger umfangreich. Wie bereits eingangs erwähnt, bleiben natürlich dennoch die nationale Gesetzgebung und die damit verbundene Auslegung abzuwarten. Wir werden über die anstehenden Veränderungen selbstverständlich laufend informieren.

Zusammenfassend haben wir eine Übersicht zusammengestellt, inwiefern die vorgenannten Themen Auswirkungen auf das operative Geschäft haben könnten (vgl. untenstehenden Kasten). ■

Wie wird sich der Aufwand entwickeln? Wo wird die Umsetzung schwieriger, wo sind Entlastungen zu erwarten? Nach dem heutigen Erkenntnisstand gehen wir davon aus, dass die 5. GwR zumindest geringere Auswirkungen auf die Banken haben wird als noch die 4. GwR. Auch wenn der Aufwand voraussichtlich unter dem Strich noch einmal steigen wird, so wird es doch auch Hilfen durch die Vorhaltung zentraler Register geben.

	Der Aufwand wird voraussichtlich		
	steigen	unverändert bleiben	sinken
1. Neu: virtuelle Währungen		■	
2. Erweiterung: Identitätsprüfung	■		
3. Erweiterung: wirtschaftlich Berechtigter	■		
4. Neu: PEP-Funktionsliste			■
5. Neu: Immobilienregister		■	
6. Öffnung: Transparenzregister			■
7. Neu: Trusts		■	
8. Neu: Statistiken		■	
9. Erweiterung: Risikofaktoren	■		

BAIT

IT-Strategie: Bestens vernetzt

Die Einführung der neuen MaRisk und der BAIT liegt jetzt schon einige Monate hinter uns. Zeit für den Lackmustest: Welche Umsetzungsstrategie hat sich bewährt? Wie geht man es am besten an? Wie kann man sicherstellen, den Ansprüchen zu genügen?

Die Änderungen in der MaRisk (27. Oktober 2017), die die Anforderungen an die Informationstechnologie (IT) betreffen, sind nicht besonders umfangreich. Die meisten Neuerungen betreffen das Auslagerungsmanagement. Die Bankaufsichtlichen Anforderungen an die IT (BAIT, 3. November 2017) werden dagegen konkreter in den Forderungen.

Sie befassen sich mit acht Hauptthemen:

1. IT-Strategie,
2. IT-Governance,
3. Informationsrisikomanagement,
4. Informationssicherheitsmanagement,
5. Benutzerberechtigungsmanagement,
6. IT-Betrieb,
7. IT-Projekte/Anwendungsentwicklungen und
8. Auslagerung/sonstiger Fremdbezug.

Beschäftigt man sich näher mit den Themen der BAIT, wird der ‚große Wurf', das notwendige Zusammenspiel der einzelnen Themen, schnell sehr deutlich.

1. IT-Strategie

Am Anfang steht die Unternehmensstrategie. In ihr sollten Aussagen zur IT getroffen werden. Anders ausgedrückt: Die strategischen IT-Ziele müssen konsistent zur Geschäfts- und Risikostrategie des Unternehmens aufgebaut sein und sich an diesen ausrichten.

Die IT-Strategie sollte darüber hinaus Antworten auf alle sieben weiteren Themen der BAIT geben.

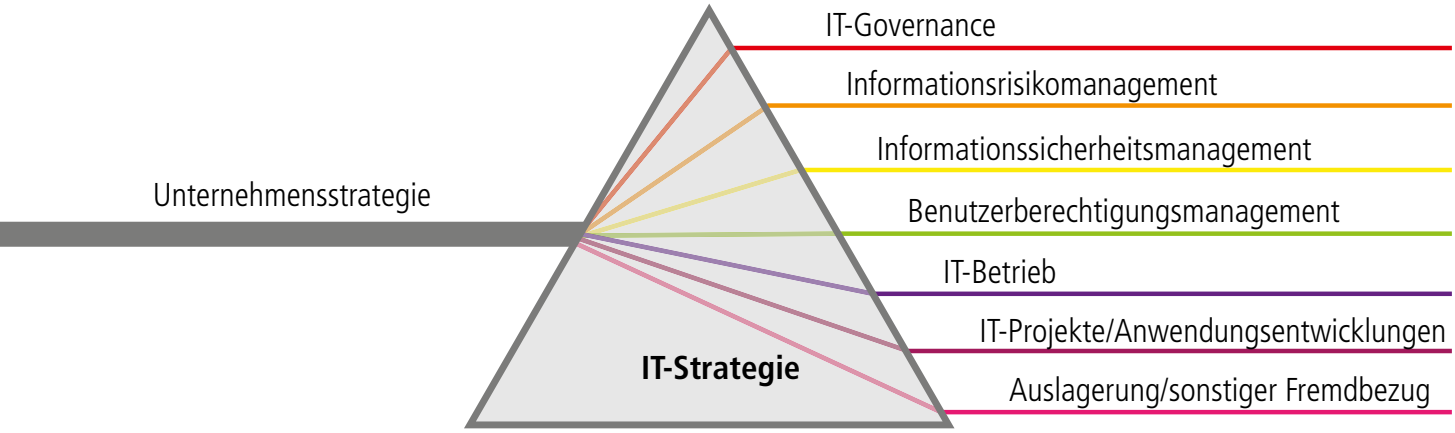
Sie beschreibt die strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation, der IT-Architektur sowie die dazugehörigen IT-Prozesse. Neben einer Aussage zu Sicherheitsstandards und Eckpunkten der Informationssicherheitsorganisation sollte sie das Notfallmanagement im IT-Betrieb berücksichtigen.

Wenn das Unternehmen auf eigenbetriebene und -entwickelte IT-Systeme oder auf Auslagerung setzt, sind in der IT-Strategie auch Aussagen zu diesen Themen aufzunehmen.

Die Messung und Erreichung der strategischen Ziele sollte mit Maßnahmen konkretisiert und die Erreichung der Ziele überprüft werden.

2. IT-Governance

Die in der IT-Strategie getroffenen Aussagen finden direkten Eingang in die IT-Governance. Hier wird geprüft, ob die Steuerung und Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der IT-Prozesse auf Basis der IT-Strategie geschehen.



Zur Steuerung des Betriebs und der Entwicklung der IT-Systeme sollten quantitative und qualitative Kriterien festgelegt und überwacht werden. Bei Veränderungen an IT-Aufbau oder IT-Ablauf müssen Aktivitäten und Prozesse direkt angepasst werden.

Regelungen zum Informationsrisikomanagement und Informationssicherheitsmanagement sind zu treffen und schriftlich zu fixieren, ebenso wie Regelungen zu IT-Aufbau und IT-Ablauf.

3. Informationsrisikomanagement

IT-Systeme und IT-Prozesse müssen Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit sicherstellen.

Dafür sind klare Verantwortlichkeiten, Kontrollen, Kommunikationswege und Kompetenzen zu definieren. Um das Informationsrisikomanagement sauber zu betreiben, müssen zudem Überwachungs- und Steuerungsprozesse eingesetzt, Berichtspflichten eingehalten und Schutzbedarfe ermittelt werden.

4. Informationssicherheitsmanagement

Das Informationssicherheitsmanagement legt feste Aufgaben und Verantwortliche fest.

So hat der Informationssicherheitsbeauftragte die Aufgabe, eine Informationssicherheitsleitlinie zu erstellen. IT-Dienstleister werden nach den Vorgaben der Leitlinie überwacht. Jede Auslagerung ist im Rahmen eines IT-Projektes zu steuern und zu dokumentieren.

Darüber hinaus muss eine vierteljährliche Berichterstattung bei wesentlichen Auslagerungen vereinbart werden.

5. Benutzerberechtigungsmanagement

Im Rahmen des Benutzerberechtigungsmanagements werden die Kompetenzen definiert, aufeinander abgestimmt und gepflegt. Benutzerberechtigungen müssen regelmäßig und auch anlassbezogen überprüft werden. Das gilt auch bezüglich der Schnittstelle bei Auslagerungen. Technische User müssen jederzeit zweifelsfrei zuzuordnen sein.

Grundsätzlich dürfen Berechtigungen nur nach einer dokumentierten Genehmigung und Kontrolle vergeben werden. Die Vergabe, Änderung, Deaktivierung, Löschung und Rezertifizierung von Benutzerrechten sind nachvollziehbar zu dokumentieren. Dazu muss jedes Unternehmen außerdem einen Prozess etablieren, der den Soll-Ist Abgleich der Berechtigungen prüft.

Zudem muss sichergestellt werden, dass das Benutzerberechtigungskonzept eingehalten wird und nicht umgangen werden kann (technisch-organisatorische Maßnahmen).

6. IT-Betrieb

Nach den BAIT muss der IT-Betrieb zwingend mit den Anforderungen der IT-Strategie übereinstimmen.

Es muss dokumentiert werden, welche IT-Systeme eingesetzt werden und wie deren Beziehungen untereinander sind. Diese Aufstellung ist zu verwalten, zu erfassen und regelmäßig zu aktualisieren.

AUTORIN UND ANSPRECHPARTNERIN

Sandra Sitter
Leiterin IT & Projekte,
E-Mail: sandra.sitter@geno-tec.de

Die BAIT setzen weiter voraus, dass Prozesse zu Änderungen an IT-Systemen, abhängig von Art, Umfang, Komplexität und Risikogehalt, festgelegt sind und dann auch angewandt werden. Änderungen an IT-Systemen müssen dokumentiert, bewertet, priorisiert, genehmigt, koordiniert und sicher umgesetzt werden.

Die BAIT fordern zudem, dass Störungen und Ausfälle sauber dokumentiert, Ursachen analysiert, Maßnahmen eingeleitet und überwacht werden.

Nicht nur die DSGVO, sondern auch die BAIT fordern ein Datensicherungskonzept. Das Datensicherungskonzept muss Anforderungen zur Verfügbarkeit, Lesbarkeit, Aktualität der Kunden- und Geschäftsdaten sowie deren Verarbeitung ableiten. Datensicherungen müssen regelmäßig, mindestens jährlich getestet werden.

7. IT-Projekte und Anwendungsentwicklungen

Alle IT-Projekte und Anwendungsentwicklungen sind sauber und nachvollziehbar zu dokumentieren.

Aus einer Dokumentation müssen die Ziele und Anforderungen klar hervorgehen. Sowohl der Projektverlauf als auch die Umsetzung einer Entwicklung sind festzuhalten. Bei Entwicklungen liegt dabei insbesondere das Augenmerk auf einem zu installierenden Test- und Freigabeverfahren. Dabei ist zu dokumentieren, dass die Anforderungen an Funktion und Leistung richtig umgesetzt werden.

8. Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen

Als IT-Dienstleistungen werden alle Ausprägungen des IT-Bezugs definiert. In dieser Definition wird der AT 9 MaRisk nochmal konkreter gefasst.

Die Gesamtverantwortung der Auslagerung bleibt immer bei der Geschäftsleitung. Die BAIT fordern explizit Risikoanalysen. Änderungen müssen bewertet werden. Zu einer Auslagerung bedarf es regelmäßig auch einer Exit-Strategie. Zudem muss der Auslagerungsdienstleister überwacht werden.

Fazit

Um den Anforderungen der BAIT gerecht zu werden, müssen die einzelnen Punkte ineinandergreifen. Nur wenn sie aufeinander abgestimmt sind, erfüllt ein Unternehmen die gesetzlichen Anforderungen.

Zu ergänzen wäre, dass auch nur dann das Unternehmen mit Blick auf die IT sicher aufgestellt ist.

In der Praxis punktet langfristig eine ganzheitliche Herangehensweise ausgehend von der Unternehmensstrategie. Sie allein gewährleistet die erforderlichen Sicherheitsstandards und ermöglicht darüber hinaus die notwendige Flexibilität hinsichtlich einer künftigen Unternehmens(-IT-)entwicklung. ▬

MaRisk

Auslagerungsmanagement

Die Umsetzungsfrist für das Auslagerungsmanagement nach MaRisk (AT 9) läuft Ende Oktober aus. Das neue Verbund-Tool „Auslagerungsmanagement kompakt“ unterstützt Sie in der Umsetzung.

Genossenschaftliche Primärbanken müssen zwar nicht zwingend ein zentrales Auslagerungsmanagement einrichten. Gleichwohl hat jedes Institut die mit einer Auslagerung verbundenen Risiken zu analysieren und zu steuern.

Diese Aufgabe umfasst u. a.:

- Bankweite Umsetzung der gesetzlichen Anforderungen an Auslagerungen
- Implementierung und Organisation eines Auslagerungsmanagements im Unternehmen
- Dokumentation von Auslagerungen und Weiterverlagerungen
- Risikoanalysen nach einheitlichen und transparenten Maßstäben
- Leistungsüberwachung der Dienstleistungsqualität
- Dokumentation und Berichterstattung

Wie unterstützt Sie das „Auslagerungsmanagement kompakt“ bei Umsetzung dieser Aufgaben konkret?

Vollständige Erfassung von Auslagerungen und Weiterverlagerungen

Gemäß AT 9 Tz. 1 MaRisk liegt eine Auslagerung i. S. v. § 25b KWG i. V. m. AT 9 Tz. 1 MaRisk vor, wenn ein Institut ein anderes Unternehmen mit der Wahrnehmung von Aktivitäten und Prozessen in Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen und sonstigen institutstypischen Leistungen beauftragt, die ansonsten vom Institut selbst erbracht würden.

Im ersten Schritt des Tools werden daher die von der Bank ausgelagerten Aktivitäten erfasst. Dazu steht eine Vorauswahl der üblicherweise innerhalb der Genossenschaftlichen FinanzGruppe genutzten Dienstleistungen als Auswahlliste zur Verfügung. Durch Auswahl des Anbieters und der erbrachten Dienstleistung sind Adressdaten und Kurzbeschreibungen zur Dienstleistung direkt vorhanden. Das vereinfacht und verkürzt die Erfassungsarbeiten enorm.

Institute, die unsere Anwendung „ISI kompakt“ zur Umsetzungsunterstützung in der Informationssicherheit nutzen, profitieren darüber hinaus von einer individualisierten und angepassten Auswahlliste der bereits erfassten Auslagerungen.

Die im Aufnahmeprozess gewonnenen Erkenntnisse werden in einer komprimierten Ansicht abgebildet. Alle relevanten Daten sind auf einen Blick erkennbar (vgl. Abbildung 1).

Abb. 1 ÜBERSICHT AUSLAGERUNGEN

Bezeichnung	Beginn	Art	Wesentlichkeit	Dienst	Dienstleister
DZ Bank					
EGon-Limite	01.01.2018	Auslagerung	nicht wesentliche Auslagerung	EGon-Limite	DZ Bank
Genossenschaftsverband					
Unterstützung IT Test	01.01.2016	Sonstiger Fremdbezug		Unterstützung IT Test	Genossenschaftsverband
GenoTec					
Auslagerung MaRisk Compliance	01.07.2018	Auslagerung	wesentliche Auslagerung	Auslagerung MaRisk Compliance	GenoTec

kompakt – alles im Blick

Risikoanalyse und -beurteilung: einheitliche Kriterien, Nachvollziehbarkeit und Transparenz

Die MaRisk gibt in AT 9 Tz. 2 vor, dass das Institut auf der Grundlage einer Risikoanalyse eigenverantwortlich festlegen muss, welche Auslagerungen von Aktivitäten und Prozessen unter Risikogesichtspunkten wesentlich sind (wesentliche Auslagerungen). Diese ist auf der Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben durchzuführen.

Die Erfüllung dieser Vorgabe führt in der Praxis zu einem Balanceakt zwischen Standardisierung und individuell nachvollziehbarer Begründung inklusive Dokumentation.

Die in „Auslagerungsmanagement kompakt“ integrierte Risikoanalyse gibt den Rahmen durch einheitliche Fragen und einen festen Beurteilungsstandard vor. Dabei werden die jeweils aktuellen verbundkonformen Vorgaben und Standards für das Auslagerungsmanagement berücksichtigt. Nach unserer Auffassung werden die Anforderungen an den „Auslagerungs-Risikomanager“ künftig noch weiter steigen: Seine Entscheidungen und Einordnungen müssen nachvollziehbar begründet und dokumentiert sein. Ein einfaches Ankreuzen ohne weitere Kommentierung dürfte den Anforderungen an die Nachvollziehbarkeit nicht genügen.

Um Ihren Auslagerungs-Risikomanager in der Risikobeurteilung zu unterstützen, sind in „Auslagerungsmanagement kompakt“ die einzelnen Beurteilungsparameter mit umfangreichen Hilfestellungen für die Kommentierung versehen. Für die finale Risikobeurteilung macht das System auf der Basis der getroffenen Einschätzungen einen Beurteilungsvorschlag. Die Parameter für den Vorschlag werden transparent und nachvollziehbar angezeigt. Letztlich obliegt die Beurteilung dem Auslagerungs-Risikomanager: Er kann den Vorschlag bestätigen oder auch abändern.

Prüfung, Überwachung und Steuerung der Dienstleistungsqualität

Die Steuerung und Überwachung der ausgelagerten Aktivitäten und Prozesse gemäß AT 9 Tz. 9 MaRisk umfasst die regelmäßige Beurteilung der Leistung des Auslagerungsunternehmens anhand vorzuhaltender Kriterien.

Zur Leistungsbeurteilung sind im Vertrag zunächst die vom Auslagerungsunternehmen zu erbringenden Leistungen spezifiziert. Weiterhin werden vertraglich die Informations- und Kontrollmöglichkeiten für das einlagernde Institut geregelt. Vereinbart werden können z. B. Tätigkeitsberichte, Berichte über interne und externe Prüfungen, Reportings zur Erfüllung von Service-Level-Agreements oder Zertifizierungen.

Für die Durchführung und Dokumentation der Leistungsmessung haben wir die Vertragsprüfung mit der Leistungsmessung verknüpft.

Aus der Aufnahme der vereinbarten Informationspflichten (Art und Turnus) werden automatisiert einzelne Wiedervorlagen zur weiteren Bearbeitung und Dokumenta- >

tion erstellt. Auch hier sind einheitliche Kriterien für die Beurteilung von Leistungen und Berichten vorhanden. Somit haben Sie zu jeder Zeit die Vollständigkeit von Unterlagen im Blick und erfüllen die Anforderung an eine ordnungsgemäße Überwachung des Auslagerungsunternehmens (vgl. Abbildung 2).

Umsetzung und Dokumentation der BAIT

Mit den Bankaufsichtlichen Anforderungen an die IT (BAIT) vom 3. November 2017 sollen die in den MaRisk enthaltenen Anforderungen in Bezug auf die IT konkretisiert und das Bewusstsein für IT-Risiken erhöht werden. In diesem Zusammenhang ergeben sich über die MaRisk hinaus weitere Anforderungen an jeden sonstigen Fremdbezug von IT-Dienstleistungen. Hier ist gemäß BAIT-Modul 8 Tz. 53 vorab eine Risikobewertung durchzuführen, sofern die IT-Dienstleistungen entsprechend den Erläuterungen zu AT 9 Tz. 1 MaRisk seitens der Bank nicht bereits als wesentliche oder unwesentliche Auslagerung einer regelmäßigen Risikoanalyse unterliegen.

Aus diesem Grund enthält „Auslagerungsmanagement kompakt“ auch eine Risikoanalyse gemäß den Anforderungen des Moduls 8 der BAIT. In Verbindung mit den weiteren Funktionen wie der Vertragsprüfung und der Möglichkeit zur Leistungsüberwachung können die in der im Juli 2018 veröffentlichten Interpretation der Genossenschaftlichen FinanzGruppe beschriebenen Handlungsfelder erfüllt werden. Diese sind:

- Überprüfung der Kategorisierung von IT-Dienstleistungen als Auslagerungen bzw. sonstigen Fremdbezug
- Überprüfung der Vorgaben zur Vertragsgestaltung
- Erstellung einer strukturierten Vertrags-/Leistungsübersicht
- Festlegung des Prozesses zur Durchführung von Risikobewertungen beim sonstigen Fremdbezug
- Festlegung der Prozesse zum Abgleich mit der IT-Strategie der Bank sowie zur Überwachung der Leistungserbringung
- Festlegung der Prozesse zur regelmäßigen und anlassbezogenen Überprüfung der Leistungserbringung

Abb. 2 ÜBERSICHT LEISTUNGSÜBERWACHUNG

GenoTec				
Auslagerung MaRisk Compliance				
Bericht Jahresabschlussprüfung 2017				
	offen			
Ergebnisbericht				
	eingegangen	01.05.2018	25.07.2018	25.07.2018
Ergebnisbericht 2018				
	offen	01.02.2019		
Jahresbericht WpHG-Compliance 2017				
	eingegangen	28.02.2018	27.02.2018	27.02.2018
Jahresbericht WpHG-Compliance 2018				
	offen	28.02.2019		
Sonderprüfungsbericht Interne Revision				
	eingegangen		30.05.2018	31.05.2018

Erstellung eines jährlichen Berichts über die wesentlichen Auslagerungen

Der AT 9 Tz. 13 der MaRisk fordert, dass das zentrale Auslagerungsmanagement mindestens jährlich einen Bericht über die wesentlichen Auslagerungen verfasst und der Geschäftsleitung zur Verfügung stellt. Der Bericht hat unter Berücksichtigung der dem Institut vorliegenden Informationen bzw. der institutsinternen Bewertung der Dienstleistungsqualität der Auslagerungsunternehmen folgende Antworten zu liefern:

- Entsprechen die erbrachten Dienstleistungen der Auslagerungsunternehmen den vertraglichen Vereinbarungen?
- Können die ausgelagerten Aktivitäten und Prozesse angemessen gesteuert und überwacht werden?
- Sind weitere risikomindernde Maßnahmen zu ergreifen?

Die Berichterstattung erfolgt in erster Linie an die Geschäftsleitung. Aber auch weitere Adressaten wie z. B. interne und externe Prüfer, Mitarbeiter mit Beauftragten-Funktionen oder das Risikocontrolling haben einen Anspruch auf eine aussagekräftige Berichterstattung und Informationen. Im Rahmen der Entwicklung des Tools „Auslagerungsmanagement kompakt“ wurde berücksichtigt, dass im Zusammenhang mit der Tätigkeit und der Dokumentation die Ergebnisse so festgehalten werden, dass diese für eine automatisierte und aussagekräftige Berichterstellung genutzt werden können.

Vorgesehen sind adressatengerechte Standardreports mit unterschiedlicher Detailtiefe. Diese reichen vom Gesamtüberblick der ausgelagerten Aktivitäten und Prozesse in Tabellenform bis zur Auswahl von Details zu einzelnen Auslagerungen. Durch regelmäßigen Austausch mit unseren Kunden, Prüfungsverbänden und Beauftragten werden wir diese Standardreports an die praktischen Erfordernisse immer weiter anpassen.

AUTOREN UND ANSPRECHPARTNER

Iris Hauptführer
Leiterin Produktentwicklung,
E-Mail: iris.hauptfuehrer@geno-tec.de

Martin Hierlemann
Leiter Vertrieb,
E-Mail: martin.hierlemann@geno-tec.de

Fazit

Mit „Auslagerungsmanagement kompakt“ kann jede Bank den neuen und alten Anforderungen der MaRisk an das Risikomanagement von Auslagerungen und dem Modul 8 der BAIT gelassen entgegensehen. Alle zentralen bzw. inhaltlichen Ansprüche werden erfüllt.

Die Option zur Auslagerung und damit auch die Option auf die qualitativen und betriebswirtschaftlichen Vorteile einer arbeitsteiligen Organisation bleiben erhalten – dank eines einfachen und sicheren Auslagerungswerkzeugs. ▬

WpHG-Compliance

Bedarfsorientierte Sachkundeschulung

Sachkundeschulung ist heute eine regelmäßig durchzuführende Maßnahme, die einen erweiterten Personenkreis einbezieht. Die Einheitsschulung für jedermann funktioniert längst nicht mehr, erforderlich ist ein gezieltes Training.

Das Thema Sachkunde ist nicht neu. Und doch hat sich seit dem 3. Januar 2018 einiges geändert. So ist nun schriftlich fixiert, dass die Sachkunde gemäß § 87 WpHG/WpHGMaAnzV kontinuierlich zu wahren, jährlich zu überprüfen und regelmäßig auf den neuesten Stand zu bringen ist (§ 1 Abs. 1 Satz 2 WpHGMaAnzV).

Des Weiteren sind neue Mitarbeitergruppen hinzugekommen, die so vorher im Gesetz noch nicht definiert waren, wie beispielsweise die Mitarbeiter der Finanzportfolioverwaltung und Vertriebsmitarbeiter. Auch die Anforderung, dass speziell Anlageberater, sofern sie bis zum 3. Januar 2018 nicht bei der BaFin gemeldet waren und kein duales Studium bzw. keine duale Ausbildung durchlaufen haben, einen Praxisnachweis erbringen müssen, ist neu (siehe auch ausführlich beschrieben im Abschnitt B.I.6. des BVR-Umsetzungsleitfadens). Ähnlich die maßgeblich beteiligten Mitarbeiter in der Product Governance: Sie unterliegen ebenfalls besonderen Ansprüchen.

Als Auslagerungspartner WpHG-Compliance für Volksbanken Raiffeisenbanken führen wir seit Jahren Schulungen durch. Im Rahmen der MiFID-II-Einführung haben wir in erheblichem Umfang bei der Sachkundevermittlung an die Bankmitarbeiter innerhalb der Genossenschaftlichen FinanzGruppe und auch im Privatbanksektor mitgewirkt.

In unseren Schulungen forcieren wir einerseits einen zielgruppenorientierten Ansatz. Das heißt, dass die Schulungen spezifisch für die jeweiligen Anforderungen der Zielgruppen ausgelegt sind. Andererseits legen wir viel Wert auf Praxisnähe. Diese resultiert aus unserer Mehrmandantentätigkeit und findet ihren Ausdruck in einem umfassenden Erfahrungswissen. Schlussendlich ist es uns wichtig, dass die Schulungsunterlagen bankindividuell gestaltet sind. Letztlich wollen und müssen sie alltagstauglich sein.

Nicht jeder muss alles wissen

Die vielen positiven Rückmeldungen haben uns in der Vorgehensweise bestätigt, so dass wir nun, nach Einführung von MiFID II, unser Schulungskonzept ausgebaut haben (vgl. auch untenstehende Abbildung 1) durch eine

- WpHG-Compliance-Grundlagenschulung,
- MiFID-II-Updateschulung und
- WpHG-Compliance-Zielgruppenschulung.

Die Schulungen für Auszubildende, MiFID-II-Nachzügler und diverse andere Zielgruppen (u.a. Anlageberater, Vertriebsmitarbeiter, Vertriebsbeauftragte, Product Governance, Marktfolge, IR, Führungskräfte) können sowohl als Präsenzschulung als auch per Webinar durchgeführt werden. Zukünftig werden alle Schulungen auch per E-Learning angeboten. Derzeit ist ein E-Learning bereits für die WpHG-Compliance-Grundlagenschulung (WpHG-Compliance Grundlagen/MAR/Insidergeschäfte/persönliche Geschäfte) buchbar.

AUTOR UND ANSPRECHPARTNER

Martin Reglinski
Beauftragter WpHG-Compliance,
E-Mail: martin.reglinski@geno-tec.de

Für den Alltag gewappnet

Ihren Nutzen sehen wir darin, dass in unseren Schulungen nur die für die Zielgruppen relevanten Informationen vermittelt werden. Ihre Mitarbeiter können ihre volle Konzentration auf das Wesentliche richten.

Darüber hinaus profitieren Ihre Mitarbeiter und damit Ihre Bank von unseren bankübergreifenden Erfahrungen, Praxis-tipps und fachkompetenten Dozenten. ▬

Abb. 1 ÜBERSICHT SCHULUNGEN

WpHG-Compliance-Grundlagenschulung	**MiFID-II-Updateschulung**	**WpHG-Compliance-Zielgruppenschulungen**
inkl. MAR/Insidergeschäfte/persönliche Geschäfte	Welche Änderungen haben sich durch MiFID II ergeben?	Sachkundeschulung in aufsichtsrechtlichen Grundlagen
▶ **Auszubildende** ▶ **Neue Bankmitarbeiter** (nicht Berater) ▶ **Ausgewählte Mitarbeiter:** Auffrischung und Updateschulung	▶ **Nachzügler** (nach längerer Abwesenheit, etwa Mutterschutz, Elternzeit oder Krankheit) ▶ **Ausgewählte Mitarbeiter:** Auffrischungsschulung Voraussetzung: MiFID-I-Sachkundeschulung	▶ **Vertriebsbeauftragte** ▶ **Product Governance** (für maßgeblich beteiligte Mitarbeiter) ▶ **Compliance-Funktionen** (Marktfolge, IR) ▶ **Berater/Vertriebsmitarbeiter** ohne vorherige gleichartige Tätigkeit

Interne Revision

IT-Revision – Herausforderung für Banken

Informationstechnologie bestimmt nicht nur alle Bereiche in der Bank, sie ist auch hochkomplex. Zu glauben, man könne alle Prüfungsgebiete und die dazugehörenden Prozesse eines Unternehmens in gleicher Qualität prüfen, ist unrealistisch. Relevanz und Komplexität machen daher eine Spezialisierung innerhalb der Revision notwendig.

Beständige Neuentwicklungen und immer kürzere Änderungszyklen in der Informationstechnik (IT) stellen die Banken immer schneller vor immer größere Herausforderungen. Cloud-Services, die steigende Anzahl von mobil genutzten Endgeräten, digitale Zahlungsmöglichkeiten per Karte oder Apps, um nur einige zu nennen, gewinnen in allen Unternehmensbereichen und -prozessen an Bedeutung.

Das hat auch Folgen für die interne Revision in den Banken. Sie steht vor der Tatsache, sich mit dem daraus resultierenden Risikopotenzial auseinandersetzen zu müssen. Die Identifizierung, Analyse und Beseitigung der IT-Risiken gewinnt stetig an Bedeutung.

Die interne Revision muss sich somit zunehmend auf diese Risiken bzw. dieses Prüffeld konzentrieren und sicherstellen, dass die „richtigen" Fachkenntnisse angewandt werden.

Auch die rasante Entwicklung ständiger gesetzlicher Veränderungen lässt inzwischen den Generalisten in der internen Revision regelmäßig ins Schwitzen kommen: Es kostet schlicht Zeit, die umfangreichen Bestimmungen zu durchdringen und in die Prüfungspraxis umzusetzen.

Eine Spezialisierung auf ein Prüfungsgebiet bietet hier die Möglichkeit, sowohl dem Prüfungsgegenstand als auch den gesetzlichen und aufsichtsrechtlichen Prüfungsanforderungen gerecht zu werden.

Doch vielerorts fehlen die notwendigen (personellen) Ressourcen. In der Realität findet sich die IT-Revision deshalb meist nur als ein Teil der internen Revision wieder und muss von dieser mit umgesetzt werden.

Ohne Spezialwissen wird es schwer

Alle für das Prüffeld IT zuständigen Mitarbeiter in der internen Revision müssen die notwendigen Grundlagenkenntnisse für ihre IT-bezogenen Prüfungen gesondert erwerben. Dazu gehören Grundlagenkenntnisse

- in der Informatik,
- über Netzwerkkomponenten,
- über IT-Konzepte und Virtualisierung,
- über das IT-Notfallmanagement,
- in Datenbank- und Speichertechnologien und
- über mobile Endgeräte wie Laptops, Smartphones etc.

Diese Kenntnisse werden benötigt, um im Rahmen der Prüfung eine angemessene und wirtschaftliche Nutzung der IT beurteilen zu können.

Dabei gilt es auch, wesentliche gesetzliche Grundlagen zu kennen

- wie HGB, AO, KonTraG, EU-DSGVO, BDSG neu, GoBD, MaRisk, BAIT,
- fachliche Stellungnahmen für Wirtschaftsprüfer IDW RS FAIT 1–3, IDW PS 330 und PS 880 sowie
- sonstige Normen, Standards und Empfehlungen wie BSI, ITIL, ISO 27001, COBIT, SOIT.

Hinzu kommen schließlich noch interne Grundsatzdokumente, Richtlinien und Anwendungsanweisungen, die es im Rahmen der Prüfungshandlungen zu berücksichtigen gilt.

Während Themen wie IT-Steuerung, Cybersicherheit, Qualitätssicherung nach wie vor Schwerpunkte bilden, werden künftig auch neue Themen wie Social Media, Cloud-Computing und Virtualisierung etc. im Fokus stehen.

Es ist somit von wesentlicher Bedeutung, dass Unternehmen in fachspezifisches Wissen und Fähigkeiten investieren, um in diesen Bereichen Sicherheit zu gewinnen.

Das Wissen und sich die entsprechenden Fähigkeiten zu erarbeiten, zu erhalten bzw. zu erweitern, sind unabdingbare Voraussetzungen zur Umsetzung einer ordnungsgemäßen IT-Prüfung. Der mit der IT-Prüfung beauftragte Revisor sollte deshalb auch eine ständige Bereitschaft zur Weiterbildung zeigen. Er sollte neuen Technologien aufgeschlossen begegnen. Das betrifft insbesondere die Beurteilung der Informationssicherheit, die – mit Fragen nach der Verfügbarkeit, Integrität, Vertraulichkeit und Verbindlichkeit der IT – inzwischen eine wesentliche Rolle einnimmt.

AUTOR UND ANSPRECHPARTNER

Thomas Grebe
Leiter Informationssicherheit & Datenschutz,
E-Mail: thomas.grebe@geno-tec.de

IT-Audit

Die GenoTec unterstützt seit 20 Jahren die Volksbanken Raiffeisenbanken mit Leistungen zur IT-Revision, sei es im Rahmen einer Auslagerung oder im Rahmen ausgewählter Prüffelder in Personalgestellung für die interne Revision. Die Prüfung und Beurteilung der Angemessenheit, Vollständigkeit und Funktionsfähigkeit des Internen Kontrollsystems bildet dabei ein zentrales Ziel.

Im Rahmen einer risikoorientierten Prüfungsplanung, die in der Regel auf ein bis drei Jahre ausgelegt ist, werden die Prüffelder in Abstimmung mit der internen Revision festgelegt und nach der Genehmigung der Unternehmensführung entsprechend umgesetzt. Dabei kommen je nach Prüffeld oder Prüfungsauftrag verschiedene Revisionsverfahren wie Einzelfallprüfungen, Systemprüfungen etc. zur Anwendung.

Fazit

Die Aufgabenstellung und die Anforderungen an die Kompetenz von IT-Revisoren haben sich in den vergangenen 20 Jahren rasant weiterentwickelt. Der historische DV-Revisor und der heutige IT-Revisor haben nur noch wenige gemeinsame Ansätze. Die Entwicklungen in der IT, insbesondere die der digitalen Revolution, implizieren hohe Anforderungen an die Prüfungssystematik und vor allem an die Kompetenz des IT-Revisors. Nicht zuletzt ist die IT-Revision damit auch zu einem Kostenfaktor geworden.

Die Lösung ist bankindividuell. Sie liegt zwischen einem bankinternen Kompetenzaufbau und einer (teilweisen) Auslagerung. Was für Ihr Haus der richtige Weg ist, hängt im Wesentlichen von Ihrer strategischen Ausrichtung ab. Gerne beraten wir Sie hier, sprechen Sie uns an.

EU-DSGVO – Ein Zwischenfazit

Die Umsetzung der Anforderungen aus der DSGVO hat branchenübergreifend enorme Ressourcen in Anspruch genommen und beschäftigt uns nach wie vor intensiv.

Die neue Datenschutz-Grundverordnung ist nun bereits über drei Monate in Kraft. Mal bemerkbar durch kleine Scharmützel, wenn man an der Fleischtheke im Supermarkt ironisch gefragt wird, ob man denn noch namentlich angesprochen werden dürfe. Mal bemerkbar, wenn wir Verbraucher viele, viele Seiten Text – mal papierhaft, mal im Internet – durchlesen, na ja, zumindest zur Kenntnis nehmen sollen.

Dessen ungeachtet ist und bleibt die DSGVO ein wichtiger Meilenstein zur Harmonisierung des in der EU geltenden Rechts. Schon das ist eine Leistung. Die eigentliche Bedeutung liegt jedoch darin, dass die DSGVO den Umgang mit unseren persönlichen Daten regelt. Sie sind heute, in einer digitalen Welt, ein bedeutender Wirtschaftsfaktor und müssen geschützt werden. Es gilt, das Recht auf informationelle Selbstbestimmung hochzuhalten.

Erfreulich ist, dass die befürchtete Abmahnwelle ausgeblieben ist. Die Rechte der Betroffenen wie z. B. das Auskunftsrecht oder das Recht auf Löschung wurden im Mai und Juni dieses Jahres deutlich öfters in Anspruch genommen, man könnte auch sagen: wurden getestet. Auch die eine oder andere Beschwerde ist bei den durch uns betreuten Banken eingegangen. Dabei waren aber insgesamt keine nennenswerten Verstöße festzustellen.

Auch wenn sich die Lage zwischenzeitlich wieder normalisiert hat, so sehen wir doch, dass Bankkunden deutlich sensibler im Hinblick auf den Umgang mit ihren Daten geworden sind.

Die Banken haben sich aus unserer Wahrnehmung heraus darauf gut einstellen können. So kam beispielsweise aufgrund technischer Komplikationen bei einem zentralen Dienstleister der neue Meldeprozess zum Einsatz. Die Frist von 72 Stunden konnte bei den durch uns betreuten Kunden durchgehend gehalten werden.

Eine besondere Herausforderung stellte die datenschutzrechtliche Prüfung von Verträgen dar. Während üblicherweise im Jahr 20 bis 30 verschiedene Verträge geprüft werden, gingen bei uns in diesem Jahr rund um den Stichtag weit über 200 verschiedene Vereinbarungen ein. Hier kam es bei den Rückmeldungen mitunter zu deutlichen Verzögerungen. Für diese bitten wir auch an dieser Stelle ausdrücklich um Entschuldigung. Zwischenzeitlich sind die Spitzen jedoch größtenteils abgearbeitet.

Der zeitliche Aufwand für den Datenschutz hat sich dessen ungeachtet insgesamt deutlich erhöht. Allein die nun anstehenden regelmäßigen, umfangreicheren Aufgaben, wie das Betreiben eines Datenschutzmanagementsystems nebst der dazugehörenden Dokumentation, nehmen viel Zeit ein. Wir entwickeln deshalb eine systemische Lösung. Sie wird den unvermeidlichen Mehraufwand bei unseren Mandanten, aber auch bei uns als Mehrmandenatenanbieter, künftig möglichst gering gestalten. ▬

Ansprechpartner: ***Michael Switalla,*** *Stv. Leiter Informationssicherheit & Datenschutz, E-Mail: michael.switalla@geno-tec.de*

Wirtschaftliche Lage

Für 2018 erwarten wir plangemäß einen Jahresüberschuss von rund 600 TEUR. Im kumulierten Ergebnis Ende Juli lag die Gesellschaft ca. 11 % über den Ertragserwartungen. Dies resultiert aus Sondereffekten in den Bereichen Datenschutz und Geldwäscheprävention.

Dem gegenüber stehen allerdings auch Mehraufwände, die in der Projektarbeit zur EU-DSGVO und vor allem auch in dem außerordentlichen Aufwand im Zusammenlang mit der Zusammenführung der GenoTec und DZ BANK (siehe S. 4) begründet sind.

Die Liquiditätssituation war durchweg entspannt und lag ca. 70 % über dem eingezahlten Kapital. Die wirtschaftliche Lage der GenoTec ist stabil.

Besonders erfreulich ist, dass die Nachfrage im Bereich Informationssicherheit und Datenschutz ungebrochen hoch ist. Wir tragen dem Rechnung, indem wir die Prozesse weiter standardisieren und auch die Spezialisierung in den einzelnen Kompetenzen vorantreiben. Dies ist auch deshalb zwingend erforderlich, weil es hier im ersten Halbjahr im Rahmen der DSGVO-Umsetzung zu Performanceeinbrüchen gekommen ist.

Darüber hinaus bereiten wir derzeit die Integration der DZ BANK- und GenoTec-Angebote vor. Die Prämisse ist, dass kundenseitig ein möglichst geräuschloser Übergang möglich wird. Wir werden frühzeitig auf die betroffenen Kunden zukommen. ▬

Ansprechpartner: Jens Saenger, Sprecher der Geschäftsführung, E-Mail: jens.saenger@geno-tec.de

Interne Revision

Seit der letzten Berichterstattung in der Point of Compliance (1/2018, S. 27) wurde der Revisionsbericht zum Vertriebsmanagement intern veröffentlicht. Darüber hinaus wurden die Revisionsberichte zum Hinweisgebersystem, zur WpHG-Compliance, zur MaRisk-Compliance und die Revisions-Quartalsberichte 1/2018 und 2/2018 erstellt und an die jeweiligen Kunden versandt.

Die Abarbeitung des internen Jahresprüfungsplans für 2018 verläuft weiterhin planmäßig.

Die externe Prüfung der Geschäftsbereiche MaRisk-Compliance, WpHG-Compliance und Zentrale Stelle nach IDW PS 951 (Typ 2) wurde von der Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft vorgenommen und abgeschlossen. Es wurde jeweils ein **Testat ohne wesentliche Einschränkung erteilt.**

Die externe Prüfung der Funktion Hinweisgebersystem nach IDW PS 331 – ebenfalls durch die Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft – wurde mit einem **uneingeschränkten Testat** beendet.

Alle Berichte zu den obigen Bereichen wurden den entsprechenden Kunden im Juni 2018 zur Verfügung gestellt.

Des Weiteren wurde quartalsmäßig ein Follow-up-Bericht erstellt, in dem die Abarbeitung der getroffenen Maßnahmen/Empfehlungen dokumentiert wird. In vorausgegangenen Prüfungen getroffene Feststellungen wurden weitestgehend abgearbeitet. Der Follow-up-Bericht wird regelmäßig mit der Geschäftsführung besprochen und dem Vorsitzenden der Gesellschafterversammlung, Verbandsdirektor Klaus Bellmann, übermittelt.

Darüber hinaus fand am 11. Juli 2018 das regelmäßige Jahresgespräch zwischen dem Vorsitzenden der Gesellschafterversammlung als Aufsichtsgremium der GenoTec und dem Leiter der Internen Revision statt. ▬

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

Wir gratulieren …

unseren Mitarbeiterinnen und Mitarbeitern zur erfolgreich bestandenen Prüfung:

- Sascha Bullwinkel, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Astrid Euskirchen, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Jan Fleischer, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Jan Fleischer, Certified Information Systems Auditor (CISA)
- Thomas Grebe, Betrieblicher Datenschutzbeauftragter (GDDcert. EU; Ergänzungsprüfung zur EU-Erweiterung)
- Marc Hübner, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Philip Kärsten, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Pia Kaufmann, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Pinkas Müller, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Monika Salomon, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Jörg Scharditzky, Certified Audit Professional (CAP)
- Reiner Schmidt, Betrieblicher Datenschutzbeauftragter (GDDcert. EU)
- Michael Switalla, Betrieblicher Datenschutzbeauftragter (GDDcert. EU; Ergänzungsprüfung zur EU-Erweiterung)
- Dr. Wolfgang Weimer, Betrieblicher Datenschutzbeauftragter (GDDcert. EU; Ergänzungsprüfung zur EU-Erweiterung)