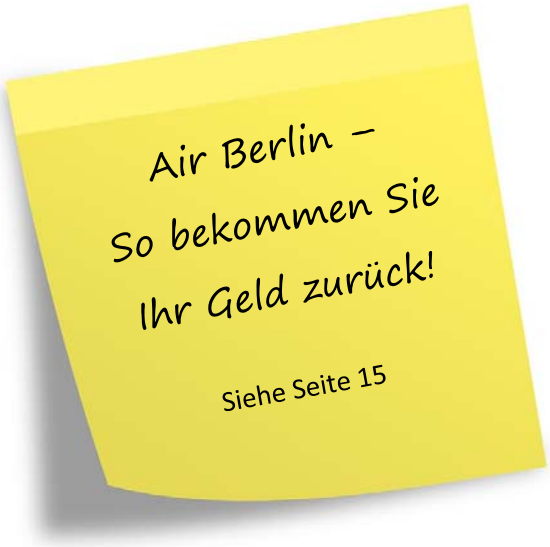
NEWSletter

Ausgabe 3/2017

CASIS

WIRTSCHAFTSPRÜFUNG



Wir wünschen Ihnen
eine fröhliche Adventszeit,
besinnliche Weihnachten und
einen guten Rutsch
ins neue Jahr!

Inhalt

I. Bankenübergreifende Themen

IT-Sicherheit: Note 4. Setzen, Nachhilfe! – Die neuen BAIT 4
Überarbeitete Fassung des BaFin-Leitfadens zur Risikotragfähigkeit 6
Endlich! Die neuen MaRisk treten in Kraft 7

II. Prüfung

Bilanzpolizei veröffentlicht Prüfungsschwerpunkte 2018 8

III. Beauftragtenwesen

How to deal with Geldwäsche 9
Fröhliche Weihnacht' und Datenschutz überall? – Die neue ePrivacy-Verordnung 10

IV. Unternehmensführung und Steuern

Paradise Papers – Ein Leben in der Grauzone? 11
Die neuen EBA-Leitlinien sind da! Über Risiko, Kommunikation und Verantwortung 12
Beurteilung von Mitgliedern des Leitungsorgans: Neue Leitlinien! 13
Steuernews 14

V. CASIS intern 15

VI. Impressum 16

IT-Sicherheit: Note 4. Setzen, Nachhilfe! – Die neuen BAIT

Empfängerkreis

- Vorstand/Geschäftsführung, IT-Sicherheitsbeauftragte, Führungskräfte IT

Hintergrund

Am 3. November 2017 wurde die offizielle Neufassung der „Bankaufsichtlichen Anforderungen an die IT (BAIT)“ veröffentlicht. Ende des Vorjahres hatten Europäische Zentralbank (EZB), Bundesbank und BaFin die IT-Systeme großer Banken untersucht und zum Teil erhebliche Sicherheitslücken festgestellt, was im Februar 2017 zum Konsultationsentwurf der BAIT führte. Mitte März 2017 fand zum vierten Mal die Konferenz „IT-Aufsicht bei Banken“ statt, auf der Raimund Röseler, der BaFin-Exekutivdirektor für Bankenaufsicht, von schwerwiegenden Mängeln in der IT-Sicherheit sprach: „Gemessen an Schulnoten, ist kein Institut besser als Vier.“

Die zunehmende Digitalisierung stellt Banken vor große Herausforderungen: Die Kunden vertrauen ihnen ihr Geld und ihre Daten an. Sie müssen sich darauf verlassen können, dass die Institute in angemessener Weise vor Finanzbetrug und Cyberangriffen geschützt sind. Kritisch betrachtet wurde bis dato, dass die IT-relevanten Anforderungen nur unzureichend in den „Mindestanforderungen an das Risikomanagement“ (MaRisk) abgebildet werden. Die BAIT schließen diese Lücke. Sie schärfen das Bewusstsein für IT-Risiken und wollen sie minimieren – sowohl innerhalb der Finanzinstitute als auch im Hinblick auf Auslagerungen.

Inhalt

Die BAIT verdeutlichen die IT-spezifische Erwartungshaltung der Finanzaufsicht gegenüber den Instituten. Sie präzisieren § 25a Abs. 1 KWG und § 25b KWG und konkretisieren die MaRisk. Das Ziel ist die Schaffung eines flexiblen und praxisnahen Rahmens für die Ausgestaltung der IT, das Management der IT-Ressourcen und das IT-Risikomanagement, im Rahmen dessen die Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der verarbeiteten Informationen sicherzustellen ist.

Die prinzipienorientierten Anforderungen unterliegen dem Proportionalitätsprinzip und betreffen die Themenkomplexe:

- IT-Strategie
- IT-Governance
- Informationsrisikomanagement
- Informationssicherheitsmanagement

I. Bankenübergreifende Themen

- Benutzerberechtigungsmanagement
- IT-Projekte und Anwendungsentwicklung
- IT-Betrieb
- Auslagerung und sonstigen Fremdbezug von IT-Diensten (Hier ist vor allem die Abgrenzung spannend.)

Die Anforderungen der BAIT sind mit Veröffentlichung in Kraft getreten und umzusetzen. Umsetzungsfristen hat die Aufsicht nicht eingeräumt.

Anforderungen/Konkrete Erfordernisse

- Bestellung eines Informationssicherheitsbeauftragten
  - der, um Interessenkonflikte zu vermeiden, organisatorisch und prozessual unabhängig agiert
  - der nicht mit dem IT-Verantwortlichen oder dem netzbetreuenden Dienstleister identisch sein darf
  - in kleineren Instituten Zusammenlegung mit der Compliance- oder Risikocontrolling-Funktion möglich
- Erarbeitung und Weiterentwicklung einer Informationssicherheitsrichtlinie
  - Definition von Maßnahmen zum Schutz der Daten
- Entwicklung eines Datensicherungskonzepts
  - Definition der zu sichernden Daten; Festlegung von anzuwendender Technik, Häufigkeit und Aufbewahrungsort
- Fortbildung der Mitarbeiter
  - IT-Sicherheit wird nicht nur durch Technik erreicht, sondern auch von entsprechend sensibilisierten und agierenden Mitarbeitern getragen.

Handlungsbedarf

Ganzheitlich denken

- Entwicklung einer Prozessdenkweise mit Überblick über die Systemlandschaft sowie die einzelnen Geschäftsprozesse mit allen relevanten Abhängigkeiten

Gewissenhaft planen

- Definition eines mit der Geschäftsstrategie konsistenten IT-Konzepts inklusive IT-Auslagerungsstrategie und Informations-sicherheitsorganisation, IT-Architektur und Notfallmanagement

Systematisch und überlegt handeln

- Einrichtung der nötigen Strukturen für Steuerung, Überwachung und Weiterentwicklung des IT-Konzepts
- Methodik zur Definition von Schutzbedarfen und Soll-Anforderungen sowie zur Durchführung von Risikoanalysen
- vor Produktivsetzung von neuer/geänderter Software Durchführung von Tests hinsichtlich Funktionalität, Sicherheit und Systemleistung
- Einordnung der eigenentwickelten und betriebenen Anwendungen (IDV) in Schutzbedarfsklassen

Compliant umsetzen

- Sicherstellen, dass die BAIT-Anforderungen angemessen umgesetzt werden
- Einbindung der Beauftragten (besondere Funktionen) und externen Unterstützer mit Expertise in Projektdurchführung

Überarbeitete Fassung des BaFin-Leitfadens zur Risikotragfähigkeit

Empfängerkreis

- Vorstand/Geschäftsführung, Risikocontrolling, Interne Revision

Hintergrund

Mit ihrem am 6. September 2017 veröffentlichten **Diskussionspapier** „Aufsichtliche Beurteilung bankinterner Risikotragfähigkeitskonzepte und deren prozessualer Einbindung in die Gesamtbanksteuerung (ICAAP) – Neuausrichtung" stellt die Aufsicht eine überarbeitete Fassung des Risikotragfähigkeitsleitfadens von 2011 vor. Es ist eine Reaktion auf elementare Veränderungen in der europäischen Aufsichtsstruktur und -praxis (Single Supervisory Mechanism – SSM und Supervisory Review and Evaluation Process – SREP), die sich wiederum auf die aufsichtliche Beurteilung bankinterner Risikotragfähigkeitskonzepte (Internal Capital Adequacy Assessment Process – ICAAP) auswirken. Das führt dazu, dass Institute ihre Verfahren zur Sicherstellung der Risikotragfähigkeit (RTF) nach Verabschiedung den neuen Gegebenheiten und Beurteilungskriterien des SSM anpassen müssen. Zur Orientierung enthält das Diskussionspapier entsprechende Grundsätze, Prinzipien und Kriterien, die von der Aufsicht genutzt werden, um bankinterne Risikotragfähigkeitskonzepte zu beurteilen.

Was ist neu?

Mit dem Diskussionspapier geht es der Aufsicht hauptsächlich darum, dass die beiden Schutzziele gemäß AT 4.1 Tz. 2 MaRisk, einerseits die Institutsfortführung, andererseits der Gläubigerschutz, hinreichend berücksichtigt werden. Um dies zu gewährleisten, fordert die Aufsicht, dass den bankinternen Risikotragfähigkeitskonzepten – anders als bislang – eine normative und eine ökonomische Perspektive zugrunde gelegt werden. Als Übergangslösung darf der „Going-Concern-Ansatz alter Prägung" bis auf Weiteres beibehalten werden; jedoch gelten auch für diese Institute bestimmte Anforderungen (Grundsätze, ICAAP, Stresstests).

Normative Perspektive

- Kapitalgrößen und strukturelle Anforderungen als Steuerungsgrößen
- auf Basis regulatorischer und aufsichtlicher Kennzahlen sowie ihrer Berechnungslogik
- Risikodeckungspotenzial (RDP): regulatorische Eigenmittel + aufsichtlich anerkannte Kapitalbestandteile
- Risikoquantifizierung nach regulatorischen Vorgaben
- Kapitalplanung mit Basis- und adversem Szenario

Ökonomische Perspektive

- umfasst in Rechnungslegung/aufsichtlichen Eigenmittelanforderungen nicht (hinreichend) erfasste Bestandteile
- Risikodeckungspotenzial daher unabhängig von Abbildung in der externen Rechnungslegung
- konservative Messung der Risiken, wobei in Anlehnung an die internen Modelle der Säule 1 ein Konfidenzniveau von 99,9 Prozent gefordert wird
- drei mögliche Ansätze bzw. Verfahren:
  1. Barwertige RTF: barwertige Messung des RDP gegenüber barwertiger Messung der Risiken
  2. Barwertnahe RTF: bilanzielles Eigenkapital +/− stille Lasten/Reserven gegenüber barwertnaher Messung der Risiken
  3. „Säule 1 +" RTF: RDP analog zu 2. gegenüber Risikowerten aus Säule 1 und quantifizierten Risikowerten aus Säule 2

Handlungsbedarf

- Überprüfung und Anpassung bestehender Risikotragfähigkeitskonzepte
- Umgestaltung der Risikotragfähigkeitsrechnung mit Auswirkungen auf Kapitalplanung und Stresstests
- Dokumentation, wie normative und ökonomische Perspektive in der Risikosteuerung berücksichtigt werden
- Prüfen Sie die Steuerungsansätze und erfassen Sie Schnittstellen/Abhängigkeiten mit/von anderen bankinternen Bereichen, um Inkonsistenzen bei der Kombination verschiedener Ansätze zu vermeiden.
- Überprüfen Sie, ob Sie die Übergangslösung – den Going-Concern-Ansatz alter Prägung – beibehalten dürfen.

Endlich! Die neuen MaRisk treten in Kraft

Empfängerkreis

- Vorstand/Geschäftsführung, Risikocontrolling-Funktion, Interne Revision, Compliance

Hintergrund

Durch die Veröffentlichung der finalen Fassung der MaRisk am 27. Oktober 2017 hat die BaFin den seit Februar 2016 andauernden Konsultationsprozess beendet. Die neuen MaRisk sind damit in Kraft und anzuwenden.

Wichtige Änderungen, Neuerungen und „Klarstellungen“

Das Rundschreiben 09/2017 (BA) beinhaltet wesentliche Neuerungen der MaRisk, vor allem zu folgenden Bereichen:

- Risikokultur
- Datenaggregation/Risikodatenmanagement
- Risikoberichterstattung
- Auslagerungen
- sonstige Anpassungen

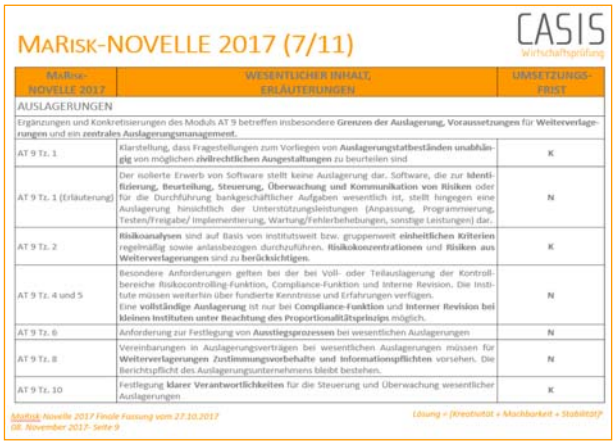
Außerdem bietet die jüngste MaRisk-Novelle einige Konkretisierungen/„Klarstellungen“. Eine nicht exemplarische, aber praxisrelevante Folge solcher „Klarstellungen“ zum Bereich Outsourcing (jetzt „Auslagerungen“) betrifft Weiterverlagerungen und die Abgrenzung vom Fremdbezug in Hinblick auf IT-Unterstützungsleistungen durch Externe. In der Fachöffentlichkeit herrscht nun Unsicherheit in Bezug auf die Tragweite der IT-spezifischen Anforderungen, beispielhaft dazu die Fragen:

- Vervielfachen sich wesentliche Auslagerungen bei (bestehenden) Verträgen mit IT-Dienstleistern?
- Im Zusammenspiel mit den Regelungen der BAIT zu Risikoanalysen bei IT-Fremdbezug: Auch rückwirkend?
  Diesbezüglich wird ein erläuternder Prüfungshinweis durch das IDW gewünscht und erwartet.

Umsetzungsfristen

Mit der Veröffentlichung sind die MaRisk anzuwenden. Dazu werden im Rundschreiben – teilweise indirekt – verschiedene Umsetzungsfristen bekannt gegeben, die von „unmittelbar verpflichtend“ bis „binnen drei Jahren“ reichen. Die CASIS Wirtschaftsprüfung hat für ihre Mandanten eine Übersicht zur finalen Fassung der MaRisk erstellt, die neben Erläuterungen zu den Neuerungen und Konkretisierungen auch eine prüferische Einschätzung der entsprechenden Umsetzungsfristen enthält.

Kontaktieren Sie uns! Gern besprechen wir mit Ihnen unsere Einschätzung zu Umsetzungsfristen, -aufwand und Konsequenzen für Ihr Institut.


MaRisk-NOVELLE 2017 (7/11)

CASIS Wirtschaftsprüfung

MaRisk-NOVELLE 2017	WESENTLICHER INHALT, ERLÄUTERUNGEN	UMSETZUNGS-FRIST
AUSLAGERUNGEN		
Ergänzungen und Konkretisierungen des Moduls AT 9 betreffen insbesondere **Grenzen der Auslagerung, Voraussetzungen für Weiterverlagerungen** und ein **zentrales Auslagerungsmanagement**.		
AT 9 Tz. 1	Klarstellung, dass Fragestellungen zum Vorliegen von **Auslagerungstatbeständen unabhängig** von möglichen **zivilrechtlichen Ausgestaltungen** zu beurteilen sind	K
AT 9 Tz. 1 (Erläuterung)	Der isolierte Erwerb von Software stellt keine Auslagerung dar. Software, die zur **Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation von Risiken** oder für die Durchführung bankgeschäftlicher Aufgaben wesentlich ist, stellt hingegen eine Auslagerung hinsichtlich der Unterstützungsleistungen (Anpassung, Programmierung, Testen/Freigabe/ Implementierung, Wartung/Fehlerbehebungen, sonstige Leistungen) dar.	N
AT 9 Tz. 2	**Risikoanalysen** sind auf Basis von institutsweit bzw. gruppenweit **einheitlichen Kriterien** regelmäßig sowie anlassbezogen durchzuführen. **Risikokonzentrationen** und **Risiken aus Weiterverlagerungen** sind zu **berücksichtigen**.	K
AT 9 Tz. 4 und 5	Besondere Anforderungen gelten bei der bei Voll- oder Teilauslagerung der Kontrollbereiche Risikocontrolling-Funktion, Compliance-Funktion und Interne Revision. Die Institute müssen weiterhin über fundierte Kenntnisse und Erfahrungen verfügen. Eine **vollständige Auslagerung** ist nur bei **Compliance-Funktion** und **Interner Revision bei kleinen Instituten unter Beachtung des Proportionalitätsprinzips** möglich.	N
AT 9 Tz. 6	Anforderung zur Festlegung von **Ausstiegsprozessen** bei wesentlichen Auslagerungen	N
AT 9 Tz. 8	Vereinbarungen in Auslagerungsverträgen bei wesentlichen Auslagerungen müssen für **Weiterverlagerungen Zustimmungsvorbehalte und Informationspflichten** vorsehen. Die Berichtspflicht des Auslagerungsunternehmens bleibt bestehen.	N
AT 9 Tz. 10	Festlegung **klarer Verantwortlichkeiten** für die Steuerung und Überwachung wesentlicher Auslagerungen	K

Handlungsbedarf

- Vermeiden Sie ein DilemMaRisk! Die Aufsicht hat betont, dass Erfahrungen „bei der täglichen Aufsicht und bei Prüfungen“ in die Novelle eingeflossen sind. Mit einer entsprechenden Aufmerksamkeit der Aufsicht in Bezug auf die Umsetzung der (im Wesentlichen seit Februar 2016) bekannten Anforderungen sollten Sie rechnen.
- Die Umsetzung der komplexen Regulierungsvorschriften bindet – gerade in kleineren Instituten – interne Ressourcen und sollte in ihren Folgen frühzeitig bedacht werden.
- Die Erfahrungen mit vergangenen MaRisk-Novellen sowie aktuell den BAIT haben gezeigt, dass auf die Bekanntgabe klarer Vorgaben und Fristen zunächst verzichtet wird, da eine im Wesentlichen vollumfängliche Umsetzung mit Inkrafttreten erwartet wird. – *Die Lehre daraus*: Eine frühzeitige Auseinandersetzung mit Auswirkungs- und Umsetzungsanalysen lohnt sich schon während der Konsultationsphasen, um die (spätere) konforme Umsetzung zu erleichtern und zu gewährleisten.

Bilanzpolizei veröffentlicht Prüfungsschwerpunkte 2018

Empfängerkreis

- Vorstand/Geschäftsführung, Aufsichtsrat, Leiter Rechnungswesen

Hintergrund

Zur Prüfung der Jahres- und Konzernabschlüsse sowie der entsprechenden Lageberichte kapitalmarktorientierter Unternehmen veröffentlichte die Deutsche Prüfstelle für Rechnungslegung e. V. (DPR) am 23. November 2017 ihre Prüfungsschwerpunkte für 2018; die ersten drei wurden von der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) übernommen.

Prüfungsschwerpunkte

- Anhangangaben zu den erwarteten Auswirkungen aufgrund erstmaliger Anwendung neuer Standards (IAS 8.30)
- spezifische Vorgaben zu Ansatz, Bewertung und Anhang in Bezug auf Unternehmenszusammenschlüsse (IFRS 3)
  - im Fokus: immaterielle Vermögenswerte, Anpassungen im Bewertungszeitraum, verpflichtende Übernahmeangebote, günstige Unternehmenskäufe, Zusammenschlüsse von Unternehmen unter gemeinsamer Beherrschung, bedingte Gegenleistungen, fair-value-bezogene Anhangangaben
- ausgewählte Aspekte zu Kapitalflussrechnungen (IAS 7)
  - im Fokus: Überleitungsrechnung, Angaben zur Berücksichtigung von Überziehungskrediten und Beträgen aus cash-pool-Vereinbarungen in Zahlungsmittelbestand, Angaben zu eingeschränkt verfügbaren Zahlungsmittelbeständen
- Ansatz und Bewertung von Rückstellungen und entsprechenden Anhangangaben (IAS 37), wichtige Einzelaspekte:
  - Verzicht auf Ansatz, weil verlässliche Schätzung unter Beachtung der Angabepflichten nicht möglich
  - Verzicht auf reguläre Berichterstattung wegen Inanspruchnahme der Schutzklausel mit Beachtung der Mindestangaben
  - Angaben zu Schätzungsunsicherheiten
  - Gruppierung der Rückstellungen
  - Angabe rückstellungsspezifischer Ertrags- und Aufwandsposten
- Konzernlagebericht und -erklärungen (§ 315 HGB)
  - Berichterstattung zu alternativen Leistungskennziffern als finanzielle Leistungsindikatoren
  - Darstellung möglicher Brexit-Auswirkungen auf künftige Vermögens-, Finanz- und Ertragslage des Konzerns
  - Angaben zum Diversitätskonzept (Konzernerklärung zur Unternehmensführung) und nichtfinanzielle Konzernerklärung

Handlungsbedarf

- im Hinblick auf die Anwendung neuer Standards auf unternehmensspezifische Ausgestaltung der Angaben achten
- Vorhalten einer aussagefähigen Dokumentation inkl. Nachweisen zu den erforderlichen Anhangangaben, vor allem in Bezug auf Rückstellungen
- Prüfung der Berichterstattung im Anhang auf Transparenz, Verständlichkeit und Übereinstimmung mit dem Lagebericht

How to deal with Geldwäsche

Empfängerkreis

- Vorstand/Geschäftsführung, Geldwäschebeauftragte/Zentrale Stelle

Hintergrund

Mit der Einführung des Gesetzes (23. Juni 2017) zur Umsetzung der 4. EU-Geldwäscherichtlinie (Richtlinie (EU) 849/2015), zur Ausführung der EU-Geldtransferverordnung (Verordnung (EU) 847/2015) und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen wurde es notwendig, die Prüfungsberichtsverordnung (PrüfbV) den neuen geldwäscherechtlichen Vorschriften anzupassen, sodass am 18. August 2017 der Entwurf für eine Änderungsverordnung zur Konsultation gestellt wurde. Die IDW-Arbeitsgruppe „Geldwäscheprüfung bei Instituten“ hat sich am 7. Juli 2017 mit Vertretern der BaFin (GW) in Bonn getroffen, um wesentliche Aspekte zu erörtern.

Im Fokus der Aufsicht

Aufgrund von Erfahrungen aus Geldwäscheprüfungen 2016/17 sieht die BaFin Verbesserungsbedarf in den Bereichen Gefährdungsanalyse, wirtschaftlich Berechtigter, Darstellung der Monitoring-Systeme, Korrespondenzbankwesen und gruppenweite Umsetzung. Für die Prüfungen 2017/18 leitet die Aufsicht daraus die folgenden Prüfungsfelder als besonders relevant ab:

- gruppenweite Umsetzung
- Korrespondenzbankwesen
- wirtschaftlich Berechtigter
- Effektivität von Risikoprävention/-kultur
- Stand der Umsetzung von Pflichten aus 4. EU-Geldwäscherichtlinie

Darüber hinaus verweist die BaFin auf die Notwendigkeit der Darstellung etwaiger Brexit-Folgen.

Neue GwG-Anforderungen – Die BaFin äußert sich.

Die Aufsicht macht ihre Erwartungen deutlich: Der Prüfer soll im Rahmen der Jahresabschlussprüfung über den konkreten Umsetzungsstand des neuen GwG bzw. den jeweiligen Projektstatus berichten. Sofern einzelne Anforderungen noch nicht umgesetzt wurden, fordert die Aufsicht eine entsprechende Klassifizierung/Wertung im Fragebogen nach § 27 PrüfbV.

Weitere bedeutende Aspekte und wie die BaFin sie auslegt:

- Fiktiver wirtschaftlich Berechtigter (wB): Frage nach zu erfassender Anzahl im Neukundengeschäft, nach der Identität bei Behörden und danach, ob im Fall vereinfachter Sorgfaltspflichten von einer Identifizierung abgesehen werden kann. – Nach Auffassung der BaFin reicht es aus, nur ein Mitglied der Geschäftsführung als fiktiven wB zu erfassen. Bei Behörden ist kein fiktiver wB zu bestimmen, wohl aber die auftretende Person zu identifizieren (derzeit noch Prüfung auf Ressortebene). Auf Letzteres kann auch bei vereinfachten Sorgfaltspflichten nicht verzichtet werden.
- Aufzeichnungs- und Aufbewahrungspflicht: Frage, ob fünfjährige Aufzeichnungspflicht dem Anspruch auf Löschung personenbezogener Daten gemäß Art. 17 der 4. EU-DSGVO vorgeht. – Dazu befindet die BaFin, dass die Spezialvorschrift (im GwG) regelmäßig vorgeht.
- Allgemeine Sorgfaltspflichten: Frage zur Prüfungspflicht hinsichtlich der Identifizierung „auftretender Personen“ und der Eigentums- und Kontrollstruktur. – Die BaFin stellt heraus, dass eine bloße „Plausibilisierung“ nicht ausreicht. Bei jeder auftretenden Person, die im Namen eines Kunden zu handeln vorgibt (z. B. Prokurist, Organe), sind ihre Berechtigung und Identität zu überprüfen; auch die Prüfung der Eigentums- und Kontrollstruktur hat regelmäßig zu erfolgen.

Handlungsbedarf

- Durchführung einer GAP-Analyse
- Erstellung eines Projektplans (inkl. Zielbestimmung, Darstellung der Entwicklung, Meilensteine, Umsetzungsdatum)

Fröhliche Weihnacht' und Datenschutz überall? – Die neue ePrivacy-Verordnung

Empfängerkreis

- Geschäftsführer, Führungskräfte IT, Datenschutzbeauftragte, Marketing-Abteilung, Recht

Hintergrund

Während die Banken sowohl die Umsetzung der Datenschutzgrundverordnung (DSGVO) bis zum Inkrafttreten am 25. Mai 2018 als auch die neuen BAIT beschäftigen, hat das Europäische Parlament Ende Oktober 2017 die ePrivacy-Verordnung (2. Reform der ePrivacy-Richtlinie, auch „Cookie-Richtlinie“ genannt) mit großer Mehrheit zugunsten eines schärferen Datenschutzes beschlossen. Diese wird nun mit der Kommission verhandelt. Vor dem Hintergrund, dass die PSD II-Richtlinie es (amerikanischen, chinesischen etc.) Großkonzernen ermöglicht, detaillierte Kontoinformationen der Kunden zu erhalten und Nutzerprofile zu erstellen, steht die ePrivacy-Verordnung für schärfere Datenschutzregeln. Ob die Verordnung zeitgleich mit der DSGVO in Kraft treten wird, ist noch nicht absehbar.

Anwendungsbereich DSGVO und ePrivacy-Verordnung

Die DSGVO schafft umfassende und europäisch einheitliche Regelungen zum Datenschutz in Bezug auf personenbezogene Daten im Allgemeinen und regelt das Verhältnis von Unternehmen zu Verbrauchern und Datenschutzbehörden. Die ePrivacy-Verordnung flankiert die DSGVO und weitet den Schutz personenbezogener Daten auf Kommunikationsdienste (z. B. Apps für Online-Banking) aus. Dieser Bereich ist im Telekommunikationsgesetz (TKG), im Telemediengesetz (TMG) und in § 7 des UWG derzeit unvollständig geregelt; er umfasst nur die Vertraulichkeit von Telefon- und E-Mail-Kommunikation.

Neuerungen der ePrivacy-Verordnung im Einzelnen

Die ePrivacy-Verordnung vereinheitlicht die Wettbewerbsbedingungen für Telekommunikationsanbieter. Sie führt das *Marktortprinzip* ein, wonach alle in der EU tätigen Unternehmen, unabhängig von ihrem Sitz, den EU-Regeln unterworfen sind. Die Vertraulichkeit der Kommunikation wird erhöht, indem *Nachrichten zukünftig verschlüsselt* werden müssen. Das soll auch für bereits *ausgelieferte Nachrichten* gelten, sofern sie noch auf einem Server liegen.

Browser und Apps müssen über *datenschutzfreundliche Voreinstellungen* verfügen (privacy by default), wie dies die DSGVO auch für Software fordert. Das Erstellen von *Nutzerprofilen* durch Google Analytics, Like-Buttons und andere E-Tracker über viele Seiten hinweg ist nur noch mit vorheriger Einwilligung möglich. *Zwingend wird das Opt-in-Verfahren.* Das Opt-out-Verfahren (in AGB) ist nicht ausreichend, was eine *Änderung der AGB (zur Online-Nutzung) und des Impressums* erfordern wird. Der „Do Not Track“-Standard des Internets wird europaweit eingeführt und Cookies dürfen weiterhin nur mit Einwilligung gesetzt werden. Nur eine *rein statistische Reichweitenmessung* wird möglich sein, sofern dies nicht zu individuellen Profilen führt und die Daten nur sehr kurz gespeichert werden. Zur Durchsetzung dieser neuen Regeln wurden die *Bußgelder auf das Niveau der DSGVO angehoben* (bis zu 20 Mio. Euro oder vier Prozent des weltweiten Jahresumsatzes).

Handlungsbedarf

- Abstimmung zwischen Datenschutzbeauftragten, IT-Abteilung, Produktverantwortlichen und Marketing, inwieweit z. B. bei Geschäftsauftritt/Werbung/Kundenakquise Online-Dienste genutzt werden, die unter die e-Privacy-Verordnung fallen
- daran anschließend gegebenenfalls Bewertung, welche Dienste unverändert verwendet werden können und wo Anpassungsbedarf besteht
- Informationen an Vorstand/Geschäftsführung über die identifizierten Auswirkungen vor dem Hintergrund des Umsetzungsstands der Verordnung

Paradise Papers – Ein Leben in der Grauzone?

Tom und Jerry reloaded

Lug und Betrug sind angesagt:
Untreue bei Schlecker; Dieselskandal bei VW; Swiss Leaks; Lux Leaks; Panama Papers; Steuervermeidung durch Amazon, Apple, Google und Co.; Steuerhinterziehung à la Hoeneß und Fahrenschon … Die Aufzählung ließe sich fortführen.

Solche Skandale stehen auf der Tagesordnung, betreffen nicht selten die Steuerpflicht. Jüngster Steuerskandal sind die Paradise Papers, die alles andere als paradiesische Zustände schildern. Dass Steueroasen genutzt werden, um Geld vor dem Fiskus zu verstecken und sich offiziell arm zu rechnen, ist nichts Neues, brisant aber die Tatsache, dass eine Anwaltskanzlei im Zentrum der Paradise Papers steht und viele deutsche Firmen auftauchen, was zeigt, dass Steuerdumping hierzulande gängige Praxis ist.

Die dargelegten Steuergeschäfte sind zwar höchst bedenklich, bewegen sich aber in einer rechtlichen Grauzone, sodass Konsequenzen unwahrscheinlich sind. In der Folge wird ein gerechteres Steuersystem gefordert und es kommt zu einer buchstäblichen Regulierungsflut – einem ewigen Katz-und-Maus-Spiel. Im Dezember 2017 hat die EU-Kommission eine „Schwarze Liste" mit Steueroasen veröffentlicht; ein weiterer Regulierungsvorschlag intendiert, dass Wirtschaftsprüfer, Steuerberater und Rechtsanwälte der Finanzverwaltung „potenziell aggressive" Steuergestaltungsmodelle ihrer Mandanten melden – allerdings ohne dass genau definiert wird, wie ein Modell aussehen muss, um „potenziell aggressiv" zu sein.

Global denken!

Sobald sich Regulierungsbemühungen auf nicht erwünschte, aber legale Steuergestaltungen innerhalb einer Grauzone richten, führt Regulierungswut allein zu einem nicht überschau- und organisierbaren bürokratischen Aufwand. Es ist falsch, auf den „großen Regulator" zu warten, wenn der „kleine Einzelne" schon etwas tun kann. Globales Denken erfordert lokales Handeln.

Gemäß AT 3.1 MaRisk ist die Rede von einer Verantwortung der Geschäftsleitung, die auch „die Entwicklung, Förderung und Integration einer angemessenen Risikokultur" mit einschließt. Eine ethisch vertretbare Risikokultur zu leben, heißt nicht nur, Gesetze zu befolgen, sondern auch, dass wir unsere Arbeit an solchen Grundsätzen und Werten ausrichten, die kein Ausreizen jeglicher Grauzonen bedeuten. Steuermoral trägt unser demokratisches Gemeinwesen.

In diesem Zusammenhang gerät auch der persönliche Handlungsspielraum in den Blick. Wenn ein Konzern wie Amazon mithilfe von Luxemburger Tochterfirmen in Deutschland kaum Steuern zahlt, kann man sich dagegen entscheiden, seine Dienstleistungen in Anspruch zu nehmen. „Schönen" lassen sich entsprechende Zahlen mit einer Steuerquote auf Basis des Gewinns – die zudem nur wenig aussagekräftig ist. Nehmen Sie deshalb eine Steuerquote auf Basis der Umsatzerlöse. Die folgende Tabelle informiert Sie über Steuerquoten ausgewählter Branchen sowie unsere eigene Steuerquote auf Basis der jeweiligen Jahresabschlüsse (JA) für 2015.

Branche	alle Wirtschaftszweige (alle Rechtsformen)	Einzelhandel (alle Rechtsformen)	Rechts- und Steuerberatung, Wirtschaftsprüfung, PR- und Unternehmensberatung	Amazon	CASIS
Steuerquote in Prozent der Umsatzerlöse	0,5	0,5	0,5	keine JA publiziert	0,5

Uns interessiert Ihre Meinung zu dem Thema. Schreiben Sie an info@casis-wp.de und diskutieren Sie mit!

Individueller Handlungsspielraum

- Leisten Sie einen Beitrag zur gesellschaftlichen Verantwortung durch eine gelebte Risikokultur und Steuermoral?
- Wie steht es um Ihre Fairness und Ihr Wettbewerbsverhalten gegenüber Kunden?
- Beauftragen Sie Dienstleister mit niedrigen Steuerquoten?
- Untersuchen und publizieren Sie Ihre eigene Steuerquote?

Die neuen EBA-Leitlinien sind da! Über Risiko, Kommunikation und Verantwortung

Empfängerkreis

- Vorstand/Geschäftsführung, Aufsichtsorgane

Hintergrund

Am 26. September 2017 hat die European Banking Authority (EBA) ihre finalen „Guidelines on internal governance“ (EBA-GL-2017-11) veröffentlicht. Sie definieren die Anforderungen der Bankenaufsicht an die interne Governance, die vor allem die Verantwortung der Leitungsorgane für eine effiziente Unternehmensführung betreffen. Die Guidelines beschreiben – unter Berücksichtigung des Proportionalitätsprinzips – einen Handlungsrahmen für das ausgewogene Verhältnis von internen Steuerungsmechanismen und -prozessen sowie deren Überwachung, um eine bessere Risikokontrolle zu erreichen. Originär richten sich die Guidelines an Leitungsorgane einschließlich Ausschüssen (Board-System). Übertragen auf das Two-Tier-System deutscher Prägung betrifft dies die Verwaltungs- oder Aufsichtsorgane inländischer Institute. Aufgrund der Ausstrahlungswirkungen der europäischen Vorgaben sind diese auch für nicht EZB-beaufsichtigte Institute relevant. Am 30. Juni 2018 treten die Leitlinien in Kraft.

Erwartungen an die interne Governance

Was von den Aufsichtsorganen der Banken gefordert wird, ist für BaFin-beaufsichtigte Institute schon größtenteils im nationalen Recht verankert sowie Bestandteil von Prüfungen – und daher nicht grundsätzlich neu. Deutlich wird aber, dass die bankinterne Überwachung als Funktion stärker in den Fokus gerät. Als besonders wichtig für eine ausgewogene Aufsichtsfunktion treten dabei folgende Punkte hervor:

- Größe des Leitungsorgans: Sicherstellen von sowohl Diversität als auch direkter und reger Kommunikation
- Zusammensetzung des Leitungsorgans: klare Struktur mit deutlich voneinander abgegrenzten Verantwortlichkeiten
- Mitglieder des Leitungsorgans betreffend: Nachfolgeplanung, Unabhängigkeit, Rotationsempfehlung, bankenspezifisches Fachwissen – individuell sowie im Kollektiv (z. B. in den Bereichen IT oder Rechnungswesen)
- Förderung der Interaktion, eines offenen und kritischen Dialogs zwischen Leitungsorganmitgliedern
- Sitzungsorganisation: Tagesordnung, rechtzeitige Aushändigung von Informationen/Unterlagen, Dokumentation
- direkter Informationsfluss zwischen dem Leitungsorgan und internen Kontrollfunktionen (Risikomanagement, Compliance, Interne Revision): regelmäßige Berichterstattung an Leitungsorgan, Zugang desselben zu internen Kontrollfunktionen
- Risikokultur mit klarer Definition angemessener Verhaltensweisen und transparenter Kommunikation
- hoher Anspruch an Leitung und Mitarbeiter bei der Identifizierung und Meldung von Interessenkonflikten
- Vorgaben zum Umgang mit internen Hinweisen, zum Schutz beteiligter Personen, z. B. bei Whistleblowing
- Festlegung und Überwachung konzernweiter Governance-Regelungen durch das konsolidierende Institut

Handlungsbedarf

- Analyse, ob bzw. inwieweit Ihr Institut den Anforderungen an die interne Governance gerecht wird
- Einschätzung der Aufsichtsorgane, ob ein offener und kritischer Dialog im Sinne der Risikokultur gepflegt wird bzw. wie dieser gefördert werden könnte
- Überprüfung der Berichterstattung und Gremiensitzungs-Dokumentation auf Leitlinienkonformität
- Überarbeitung der regelmäßigen (Selbst-)Evaluierungen von Aufsichtsorganen gemäß Vorgaben aus den Leitlinien

Beurteilung von Mitgliedern des Leitungsorgans: Neue Leitlinien!

Empfängerkreis

- Vorstand/Geschäftsführung, Aufsichtsorgane

Hintergrund

Ende Oktober 2016 hatten die European Banking Authority (EBA) und die European Securities and Markets Authority (ESMA) ihre gemeinsamen „Guidelines on the assessment of the suitability of members of the management body and key function holders“ zur Konsultation gestellt (EBA-CP-2016-17).

In der Folge erarbeitete die Europäische Zentralbank (EZB) den „Leitfaden zur Beurteilung der fachlichen Qualifikation und persönlichen Zuverlässigkeit“, der sich präzise auf das Konsultationspapier bezieht. Mittlerweile haben die Europäischen Bankenaufsichtsbehörden ihre finalen Guidelines veröffentlicht (EBA-GL-2017-12 vom 26. September 2017).

Wesentliche Anforderungen und Neuerungen

Im Einklang mit CRD IV und MiFID II intendieren die neuen Leitlinien, die Beurteilung der Eignung von Management-Mitgliedern zu vereinheitlichen, indem entsprechende Kriterien und Verfahren zur Überprüfung festgelegt werden.

Für die Dokumentation werden den Instituten Unterlagen zur Verfügung gestellt. Es steht ihnen aber frei, ob sie die angehängte Matrix („Annex I: Suitability Matrix“) oder eigene Dokumentations-Tools nutzen. Inhaltlich werden über den „Annex II: Skills“ Konkretisierungen der anzulegenden Maßstäbe genannt; beispielsweise sind bei der Eignungsbeurteilung der Leitungsorgane nunmehr auch Kenntnisse in der Rechnungslegung und Prüfung heranzuziehen.

Geltung/Umsetzung

Die gemeinsamen Leitlinien gelten ab dem 30. Juni 2018, sodass im Sinne eines „comply or explain“ mit einer Anpassung – zumindest des Merkblatts zu den *Geschäftsleitern* gemäß KWG, ZAG und KAGB – zu rechnen ist. Allerdings hat die BaFin in ihrem Journal vom Oktober 2017 angekündigt, dass sie die Anforderungen an eine formelle Unabhängigkeit von *Aufsichts- und Verwaltungsräten* „als zu weitreichend“ erachtet und deshalb nicht beabsichtigt, die Leitlinien „in diesem Punkt“ umzusetzen.

Handlungsbedarf

- Überarbeitung der regelmäßigen (Selbst-)Evaluierungen von Aufsichtsorganen gemäß Vorgaben aus den Leitlinien
- Überprüfung der Eignungsbeurteilungen in Bezug auf Leitlinienkonformität und regelmäßige Dokumentation
- Einschätzung zum kollektiven Wissen hinsichtlich ausreichender Kenntnisse in der Rechnungslegung und Prüfung
- Beobachtung der Haltung der BaFin zur Untersuchung der Leitungsebene in Bezug auf Unabhängigkeit und die Vermeidung von Interessenkonflikten

Steuernews

1. Bemessungsgrundlage für Pauschalversteuerung bei Veranstaltungen

Sie möchten eine gute Zeit mit Ihren Mitarbeitern oder Geschäftsfreunden verbringen? Tun Sie das! Gemeinsame Erlebnisse schaffen gemeinsame Erinnerungen an ein „Wir“, dem man sich zugehörig fühlt. Und Zugehörigkeit tut gut. Doch achten Sie darauf, die Pauschalversteuerung nach § 37b Einkommenssteuergesetz (EStG) richtig anzuwenden, denn was in die Bemessungsgrundlage mit einzubeziehen ist, hängt von der Art der Veranstaltung ab. Dazu gibt die Oberfinanzdirektion Nordrhein-Westfalen in ihrer Kurzinformation Lohnsteuer Nr. 01/2017 vom 7. September 2017 Auskunft.

- Incentive-Veranstaltungen zum privaten Vergnügen:
  Aufwendungen können als Betriebsausgaben abgesetzt oder – um die Mitarbeiter von der Lohnsteuer zu entlasten – pauschal versteuert werden (außer der Bewirtungsanteil)
- Incentive-Reisen (mindestens eine Übernachtung) zum privaten Vergnügen:
  Aufwendungen für die Bewirtung fließen in die Bemessungsgrundlage mit ein
- Veranstaltungen zu betrieblichen Zwecken, z. B. Produktpräsentationen, fachliche Besprechungen, Fortbildungen:
  Aufwendungen sind keine geldwerten Vorteile und können nicht unter § 37b EStG gefasst werden
- gemischte Veranstaltungen mit sowohl betrieblich veranlassten als auch Incentive-Bestandteilen:
  bei unsicherer sachgerechter Einschätzung zeitanteilige Aufteilung, die von einem 8-Stunden-Arbeitstag ausgeht

2. Teilzeitbeschäftigung eines Gesellschafter-Geschäftsführers in Pension

Mitteilung des Finanzgerichts Schleswig-Holstein am 2. Oktober 2017 zum Urteil 1 K 201/14 vom 4. Juli 2017

In dem Streitfall ging es um die zivil- und steuerrechtlichen Auswirkungen der Teilzeitbeschäftigung eines Gesellschafter-Geschäftsführers nach seinem 65. Lebensjahr mit laufenden Pensionszahlungen. Diese waren ihm knapp zwei Jahre vor Pensionsbeginn mit 75-Prozent-Klausel zugesagt worden. Daraufhin war fraglich, ob sein Versorgunganspruch trotz vorheriger Zusage auf 75 Prozent der Teilzeitvergütung zu begrenzen ist und ob er aufgrund einer Teilzeitvergütung, deren Betrag unter der Pensionszahlung liegt, aufzuschieben ist. Das entsprechende Finanzamt hatte beides bejaht.

Im Ergebnis wurde jedoch festgehalten, dass der vertragliche Pensionsanspruch aufgrund späterer Teilzeitbeschäftigung nicht gekürzt werden darf. Mit Vollendung des 65. Lebensjahrs gilt die Pension des Gesellschafter-Geschäftsführers als erdient, unabhängig davon, ob er zu geringeren Bezügen weiter arbeitet. Der neue Vertrag ist nicht als Reduzierung der vorherigen Vergütung zu verstehen, sondern stellt eine eigenständige Neuregelung des Dienstverhältnisses dar. Vertragsklauseln, die besagen, dass Pensionsleistungen erst erbracht werden, wenn der Gesellschafter-Geschäftsführer keine Gehalts- oder entsprechenden Zahlungen mehr enthält, gilt es so auszulegen, dass nur ein erdienter Pensionsanspruch in Höhe des neu gezahlten (Teilzeit-) Gehalts aufgeschoben ist.

3. Umsatzsteuer 2018

Änderungen zum 1. Januar 2018

- punktuelle Erweiterung der Steuerbefreiung für die Verwaltung von Sondervermögen nach § 4 Nr. 8 Buchst. h UStG
- Steuerfrei ist demnach die Verwaltung von
  - Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) i. S. d. § 1 Abs. 2 Kapitalanlagegesetzbuch (KAGB),
  - mit diesen vergleichbaren alternativen Investmentfonds (AIF) i. S. d. § 1 Abs. 3 KAGB sowie von
  - Versorgungseinrichtungen i. S. d. Versicherungsaufsichtsgesetzes (VAG).
- geringfügige Änderungen der Formulare (betreffend Vordrucke für die Umsatzsteuererklärung, Muster für Umsatzsteuer-Voranmeldung) und verlängerte Fristen (31. Juli bzw. 31. Dezember 2019)

Beratungsangebote und weitere Dienstleistungen (Auszug)

- Umsetzung MaRisk 6.0
- Umsetzung BAIT
- Umsetzung Datenschutzanforderungen
- Umsetzung BCBS 239 Risikoreporting
- SREP Quick Scan
- Simulation und Change Management einer Sonderprüfung nach § 44 KWG
- Umsetzung AnaCredit
- Nachhaltigkeitsmanagement und -berichterstattung
- Optimierungsprozesse im Rahmen von aufsichtsrechtlichen Umsetzungsprojekten
- Leasingbilanzierung nach IFRS 16
- Validierung von Ratingsystemen
- Prüfung von Compliance-Management-Systemen (CMS)
- Prüfungen von Internen Revisionssystemen (IRS)
- Kreditportfolioanalysen
- Rechtliche Gestaltungsberatung (CASIS Rechtsanwaltsgesellschaft)
- Marken- und Lizenzanmeldungen (CASIS Rechtsanwaltsgesellschaft)

Aus unserem Seminar- und Workshop-Angebot (Auszug)

- MaRisk 6.0
- Schulungen für Aufsichtsorgane
- Aufsichtsenglisch für nationale/lokale Banken
- Vorbereitung auf Sonderprüfungen der Aufsicht
- § 44 KWG reloaded – SREP, AQR, Challenger Model in der Bankpraxis
- Gestaltungsansätze und Fallstricke: Wertberichtigungen im Straf-, Handels-, Steuer- und Aufsichtsrecht
- Zielgruppenorientierte Seminare für Aufsichtsrecht, z. B. Aufsichtsrecht für
  - Mitarbeiter in der Organisation
  - Mitarbeiter der IT-Abteilung
  - Mitarbeiter des Personalbereichs
  - Mitarbeiter in Marktbereichen

An alle Flugkunden von Air Berlin!

Unser Tipp für Sie:

Trotz Insolvenz gibt es eine Möglichkeit, dass Sie Ihr Geld zurück bekommen – und zwar über die Versicherung der Kreditkartengesellschaften. Sie bieten ihren Kunden Schutz, falls eine Leistung nicht erhalten wurde.

Wenn Sie also einen Air-Berlin-Flug über Kreditkarte bezahlt haben und ihn aufgrund der Insolvenz nicht mehr wahrnehmen können, wird Ihnen die Versicherung der Kreditkartengesellschaft die Kosten rückerstatten.

Es ist also auch in Zukunft ratsam, solche Zahlungen mittels Kreditkarte abzuwickeln.

VI. Impressum

Herausgeber dieser Ausgabe sind:

CASIS Heimann Buchholz Espinoza
Partnerschaft
Wirtschaftsprüfungsgesellschaft

Esplanade 41
20354 Hamburg
T: +49 40 808011020
F: +49 40 808011029
E-Mail: info@casis-wp.de

CASIS Heimann Espinoza
Partnerschaft
Steuerberatungsgesellschaft

Bollhörnkai 1
24103 Kiel
T: +49 431 98280330
F: +49 431 98268476
E-Mail: info@casis-wp.de

CASIS Rechtsanwaltsgesellschaft mbH

Esplanade 41
20354 Hamburg
T: +49 40 808011024
F: +49 40 808011029
E-Mail: info@casis-ra.de

CASIS Servicegesellschaft mbH

Esplanade 41
20354 Hamburg
T: +49 40 80801100
F: +49 40 808011029
E-Mail: info@casis-wp.de

Wenn Sie Fragen zu unseren Themen haben und weitergehende Hinweise wünschen, freuen wir uns auf Ihre Kontaktaufnahme.

Dr. Antje Buchholz
Projektleiterin
T: +49 160 2545882

Redaktionsschluss: 4. Dezember 2017

CASIS Newsletter im Online-Abo unter **www.casis-wp.de/aktuelles**