NEWSletter

Ausgabe 3/2015

CASIS

WIRTSCHAFTSPRÜFUNG

„Der Herbst ist die Jahreszeit, in der die Natur die Seite umblättert.“

(Pavel Kosorin, *1964)

Inhalt

I. Schwerpunkthema

Anforderungen an die IT-Sicherheit — ein Fokus der Aufsicht 4

II. Kurz notiert

Individuelle Datenverarbeitung — ein Prozessrisiko 7

Einlagensicherung — das neue Gesetz ist in Kraft getreten 8

Neuer EU-weiter Standard für Produktinformationen für Verbraucher 9

Neues zur Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen 10

EB veröffentlicht work programm 11

„Zahlungsrichtlinie“ - Sind Ihre Prozesse zur Kontenwechselhilfe schnell genug? 12

Lageberichterstattung nach DRS 20 — Update 13

Vor dem Stresstest ist nach dem Stresstest — Was kommt in 2016? 14

III. CASIS intern

Beratungsangebote und weitere Dienstleistungen 15

Seminar– und Workshop-Angebote 15

IV. Impressum 16

Anforderungen an die IT-Sicherheit—ein Fokus der Aufsicht

Empfängerkreis

- Vorstände, IT-Sicherheitsbeauftragte, Leiter IT und Organisation

1. Hintergrund

Anforderungen an die IT-Sicherheit werden weiter zunehmen, insbesondere da auch die wesentlichen Geschäftsprozesse der Banken im Kern IT-gestützt ablaufen. Digitalisierung und innovative Prozesse, vorangetrieben durch Start-Up-Unternehmen und FinTechs stellen dabei nicht nur Anforderungen an die IT-Sicherheit, sondern an sämtliche vernetzte Prozesse des Bankenmanagements. Cyber-Angriffe werden ausgefeilter und professioneller und fordern Vorkehrungen zur Informationssicherheit heraus und erfordern ein wirksames Risikomanagement. Die Entwicklung des kriminellen Potenzials und der innovativen Entwicklung in der Bereitstellung von Informationstechnik (Cloud Computing, Bring Your Own Device, Industrial Control Systems) fordern eine stetige Anpassung der IT-Sicherheit an die aktuellen Herausforderungen.

In diesem Umfeld führte die BaFin mit Schreiben vom 15. Mai 2015 an die Deutsche Kreditwirtschaft ihren Standpunkt zur Auslagerbarkeit der Funktion des IT-Sicherheitsbeauftragten aus. Kernaussage ist, dass die Verantwortung eines zentralen Ansprechpartners (IT-Sicherheitsbeauftragter) nicht ausgelagert werden kann. Die BaFin begründet dies in der Aufgabenbeschreibung des IT-Sicherheitsbeauftragten, wonach er den IT-Sicherheitsprozess im Institut auch gegenüber IT-Dienstleistern zu überwachen hat und bei allen damit zusammenhängenden Aufgaben mitzuwirken hat. Die zentrale Verantwortung für die Gewährleistung der IT-Sicherheit auf einen externen Dienstleister zu übertragen würde dazu führen, dass das Institut über kein eigenes Know-how mehr verfügt und sich vollständig in die Abhängigkeit des Dienstleisters begibt. Vor dem Hintergrund der Bedeutung der IT-Sicherheit für die Reputation und den wirtschaftlichen Erfolg eines Instituts und der stetig steigenden Bedrohungslage wird die BaFin eine Auslagerung aufsichtsrechtlich nicht akzeptieren.

Detaillierungen der regulatorischen Anforderungen werden sich aus den Bankaufsichtlichen Anforderungen an die IT (BAIT) ergeben, die derzeit durch die BaFin erarbeitet werden. Ein Datum für die Veröffentlichung ist noch nicht bekannt. Hilfestellungen finden sich in der aktualisierten Fassung des BSI IT-Grundschutzkatalogs des Bundesamtes für Sicherheit in der Informatik.

2. Auslagerung des IT-Sicherheitsbeauftragten

Die Deutsche Kreditwirtschaft erstellte im September 2015 Anmerkungen und Vorschläge zu den Ausführungen der BaFin. Sie begrüßt die Initiative der BaFin, mittels eines Merkblatts die Funktion des IT-Sicherheitsbeauftragten zu beschreiben und damit aufzuwerten, teilt die Auslegung der BaFin zur Nichtauslagerbarkeit des IT-Sicherheitsbeauftragten jedoch nicht und begründet dies insbesondere durch die Erläuterungen zu AT 9 Tz. 4 MaRisk. Hiernach kann die Geschäftsleitung sich an Funktionen oder Organisationseinheiten zur Ausübung ihrer Leitungsaufgaben bedienen, welche sowohl nach innen als auch durch Auslagerung nach außen delegiert werden.

Darüber hinaus beinhaltet der BSI IT-Grundschutzkatalog die Maßnahme M 2.475 zur „Vertragsgestaltung bei Bestellung eines externen Sicherheitsbeauftragten“. Aus Sicht der DK kann gerade bei kleinen Instituten durch die Auslagerung eine kompetente und unabhängige Ausführung dieser Funktion sichergestellt werden (Funktionsausübung). Einigkeit besteht darin, dass eine Auslagerung der Verantwortung der Geschäftsleitung nicht möglich ist. Mit der bisherigen Schlussfolgerung könnte die Auslagerbarkeit von vielen weiteren Bereichen (z. B. Geldwäsche, Datenschutz) in Frage gestellt werden.

Auf der Informationsveranstaltung „IT-Aufsicht bei Banken“ am 7. Oktober 2015 teilte die BaFin mit, aufgrund des Feedbacks an einer trennscharfen Formulierung der Inhalte („klare Botschaft“) zu arbeiten, wobei die BaFin an der Auffassung festhalte, dass der IT-Sicherheitsbeauftragte nicht auslagerbar ist. Es muss sichergestellt sein, dass auf Fragen der Aufsicht sowie von Kunden Antworten gegeben werden können und nicht nur ein Verweis auf einen externen Dienstleister stattfindet. Insofern ist in naher Zukunft eine Konkretisierung seitens der BaFin zu erwarten.

Handlungsbedarf

- Monitoring des Erscheinens des geplanten Merkblatts nebst Schreiben der BaFin zum IT-Sicherheitsbeauftragten um
  - ⇒ die genaue Beschreibung der Funktionen des IT-Sicherheitsbeauftragten zu untersuchen,
  - ⇒ die Möglichkeit, externe Dienstleister einzubinden, zu beurteilen
- Analyse der Umsetzung im Institut auf Aufsichtsrechtskonformität und gegebnenfalls Nutzung von Umsetzungsfristen zur Anpassung der Organisation
- Untersuchung der Möglichkeit, inwieweit die Funktionen des IT-Sicherheitsbeauftragten, des betrieblichen Datenschutzbeauftragten und des Compliance-Beauftragten in einer Person zusammengefasst werden können

3. Aktualisierung des BSI Grundschutzkatalogs

Das BSI bietet mit seinem aktualisierten IT-Grundschutz im Katalog und in Standards Methoden an, um eine Mindestanforderung an die Informationssicherheit zu gewährleisten. Verschiedene Einsatzumgebungen, Sicherheitsmaßnahmen sowie die Methodik zur Auswahl und Anpassung geeigneter Maßnahmen zum sicheren Umgang mit Informationen wurden dabei überarbeitet. Betrachtet werden typische Geschäftsprozesse, Anwendungen und IT-Systeme unter personellen, organisatorischen, infrastrukturellen und technischen Aspekten, um ein dem Geschäftsbetrieb angemessenes Sicherheitsniveau zu gewährleisten.

Mit der Modernisierung des IT-Grundschutzkatalogs verfolgt das BSI folgende Ziele:

- Skalierbarkeit an Unternehmensgröße und Schutzbedarf
- Flexibilisierung der Vorgehensweise
- Stärkere Berücksichtigung von anwenderspezifischen Anforderungen (Profilbildung)
- Bessere Strukturierung und Verschlankung der IT-Grundschutzkataloge
- Beschleunigung der Umsetzung von Sicherheitsmaßnahmen
- Dynamisierung durch Adaption von Lageinformationen

4. Bankaufsichtliche Anforderungen an die IT (BAIT)

Zur Detaillierung ihrer Anforderungen erarbeitet die BaFin die bankaufsichtlichen Anforderungen an die IT (BAIT).

Allgemeine Schwerpunkte bei der Beurteilung von IT-Risiken in Banken sind:

- Die IT-Systeme und das Personal des Instituts stellen die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von Daten entsprechend ihres Schutzbedarfs sicher.
- Die IT-Systeme sind angemessen, um den operativen Anforderungen, den Geschäftsanforderungen und dem Risikoappetit des Instituts gerecht zu werden.
- Die IT unterstützt das Geschäft, das Risikomanagement und die Entscheidungen der Geschäftsleitung angemessen.
- Die IT sichert ein angemessenes Niveau von Datenqualität.

5. Spezielle Prüffelder im einheitlichen Bankaufsichtsmechanismus

Im allgemeinen Bankenaufsichtsmechanismus gibt es derzeit folgende spezielle Prüffelder:

- Ablauforganisation, Dokumentation, Strategie und Systemarchitektur
- Aufbauorganisation und Auslagerungen
- Informationsrisikomanagement und IT-Sicherheitsmanagement
- IT-Betrieb
- Softwareeinkauf, Anwendungsentwicklung und Projektmanagement
- Datenqualitätsmanagement
- Individuelle Datenverarbeitung (IDV)
- IT-Notfallmanagement
- IT-Berichtswesen
- IT-Revision

6. Fazit

Auch wenn die konkreten Details der BAIT noch nicht vorliegen, ist eine Tendenz zu formaleren und strengeren Anforderungen erkennbar.

Handlungsbedarf

- Prüfung, inwieweit die IT-Sicherheit die bekannten Risiken bereits steuert
- Analyse, ob ein Standard zur Ausgestaltung der IT-Systeme definiert wurde und ob dieser umgesetzt ist (AT 7.2 MaRisk)
- Prüfung der Beauftragung eines geplanten Cyber-Angriffs auf das Institut („Notfalltest“)
- Analyse, ob das eigene Institut in den speziellen Prüffeldern gut aufgestellt ist und gegebenenfalls Erstellung einer GAP-Analyse mit Ableitung von Maßnahmen

Individuelle Datenverarbeitung - ein Prozessrisiko

Empfängerkreis

- Vorstände, Führungskräfte IT und Risikocontrolling

Hintergrund

Die in der Bankenpraxis vielfältige Nutzung von eigenentwickelten Anwendungen (Individuelle Datenverarbeitung, IDV) ist aufsichtsrechtlich grundsätzlich zulässig, die Anforderungen an ihre Nutzung werden aber weiterhin der intensiven Überwachung und Prüfung der Aufsicht unterliegen und zudem in der Zukunft klarstellend konkretisiert (z. B. in den MaRisk 6.0).

Aufgrund ihres „schnellen Entwicklungsprozesses“ und der einfachen Handhabung wird die Nutzung von IDV als hoch flexibel und kostengünstig empfunden und ist daher beliebt. Typischerweise werden IDV-Anwendungen vom Endanwender selber programmiert und es fehlt häufig an der vollständigen fachlichen und technischen Dokumentation. In der Praxis ist eine Fehlererkennung bei IDV schwierig, und es liegt aufgrund der meist fehlenden standardisierten Entwicklungsprozesse (inklusive Test– und Releasemanagement), nicht vorhandener Dokumentation (Fach– und DV-Konzepte, Anwenderhandbücher), fehlender oder mangelhafter Berechtigungskonzepte und nicht wirksamer Kontrollsysteme ein erhebliches Risiko vor.

Die MaRisk fordern bereits heute, dass IT-Systeme und die zugehörigen IT-Prozesse die Integrität, Verfügbarkeit, Authentizität sowie die Vertraulichkeit der Daten sicherstellen. Dies soll durch die Ausgestaltung auf Basis gängiger Standards erfolgen. Speziell Excel-Anwendungen als typische Form von IDV können trotz eigener Schutzmaßnahmen (Schreib– und Blattschutz) die Anforderungen an Integrität, Authentizität und Vertraulichkeit der Daten nicht immer wirksam sicherstellen und lediglich vor ungewollten Änderungen schützen.

Aus Sicht der Institute empfiehlt es sich, eine IDV-Richtlinie zu erstellen, in welcher eine Klassifizierung von Kritikalität, Vorgaben für Entwicklung, Betrieb, Qualitätssicherung und Dokumentation definiert werden. Eine Übersicht über die vorhandene Gesamtheit der IDV (einschließlich als unkritisch klassifizierter Anwendungen) in Form einer Anwendungsliste sollte erstellt und um Festlegungen von Zuständigkeiten ergänzt werden. IT-Fachpersonal sollte in den Prozess der Anwendungsentwicklung (analog IT-Anwendungen) einbezogen werden und vor erstmaliger Inbetriebnahme und nach wesentlichen Änderungen Tests und Abnahmen durchführen. Produktionsumgebung und Testumgebung sind zwingend voneinander zu trennen, anschließend kann eine Freigabe und Implementierung erfolgen.

Fazit

Unter Verwendung standardisierter, formaler Verfahren zur Entwicklung und Pflege sowie der Implementierung von Kontrollprozessen können regulatorische Vorgaben eingehalten und muss auf die Nutzung von IDV nicht grundsätzlich verzichtet werden.

Handlungsbedarf

- Sicherstellung, dass IDV-Richtlinie (Definition von Standards) vorhanden ist, gegebenenfalls Erstellung
- Führen eines IDV-Registers inklusive Schutzbedarfsklassifizierung und Verantwortlichkeiten
- Qualitätssicherung der Anwendungen (u. a. Sicherstellung Funktionstrennung)
- Einhaltung von Programmierstandards (technische Standards, Trennung von Test– und Produktionsumgebung, Dokumentation, Anwenderhandbuch)
- Verwendung von Schutzmaßnahmen (z. B. Schreibschutz) und Einschränkung der Benutzerrechte (Einbindung von IDV in das Berechtigungsmanagement)

Einlagensicherung — das neue Gesetz ist in Kraft getreten

Empfängerkreis

- CRR-Kreditinstitute

Hintergrund

Mit dem am 3. Juli 2015 in Kraft getretenen Einlagensicherungsgesetz (EinSiG) wird die Einlagensicherungsrichtlinie (Richtlinie 2014/49/EU) in nationales Recht umgesetzt. Ziel ist es, die Einleger in Europa besser zu schützen und im Entschädigungsfall die Institute als Risikoträger so einzubinden, dass staatliche Beihilfen vermieden werden. Das zuvor geltende Einlagensicherungs- und Anlegerentschädigungsgesetz (EAEG) bleibt als Anlegerentschädigungsgesetz (AnlEntG) erhalten. Die Regelungen stehen in engem Zusammenhang , nsbesondere mit der Regulierung zur Sanierung und Abwicklung von Banken.

Entschädigungsfähige Einlagen

Die Definition der entschädigungsfähigen Einlagen (grundsätzlich bis zu 100 TEUR) schließt – anders als bisher – auch Konten ein, die auf die Währung eines Staats außerhalb des Europäischen Wirtschaftsraums lauten, z. B. US-Dollar. Zudem besteht dieser Rechtsanspruch auch für größere Unternehmen (Einlagen von Kapitalgesellschaften). Ebenso sind auch Kunden von Sparkassen, Landesbanken, Landesbausparkassen sowie Volks- und Raiffeisenbanken anspruchsberechtigt. In besonderen Fällen ist für sechs Monate ab Gutschrift ein Betrag von bis zu 500 TEUR geschützt, wenn die Einzahlung mit bestimmten Lebensereignissen zusammenhing – etwa dem Verkauf einer Privatimmobilie, einer Heirat, Renteneintritt, Ruhestand oder Kündigung. Aufrechnungsrechte oder Zurückbehaltungsrechte des CRR-Kreditinstituts werden künftig nicht mehr berücksichtigt.

Kundeninformationen

Einlagenkreditinstitute müssen ihre Kunden unter Verwendung eines gesetzlich vorgegebenen Musters schriftlich – und zwar sowohl bei der Kontoeröffnung als auch regelmäßig einmal jährlich — über ihre Rechte aufklären.

Entschädigungsmasse und Beiträge

Die gesetzlichen Einlagensicherungssysteme und die anerkannten Institutssicherungssysteme haben bis 2024 mindestens ein Vermögen in Höhe von 0,8 Prozent der zu sichernden Einlagen—und damit mehr Mittel als zuvor—anzusparen. Hieran wird sich die Erhebung der risikoorientierten Beiträge orientieren. Reichen die vorhandenen finanziellen Mittel im Entschädigungsfall nicht aus, um alle Einleger zu entschädigen, können neben den jährlichen Beiträgen unmittelbar Sonderbeiträge erhoben oder bei Bedarf Kredite aufgenommen werden. In zwei derzeit entwickelten EBA-Leitlinien soll die Beitragserhebung konkretisiert werden. Sich daraus gegebenenfalls. ergebende Änderungen des derzeitigen Beitragsverfahrens bleiben abzuwarten.

Entschädigungsverfahren

Ab 1. Juni 2016 müssen Einleger innerhalb von sieben (derzeit: 20) Arbeitstagen entschädigt werden. Die Kontaktaufnahme hat dann durch das Einlagensicherungssystem zu erfolgen (keine Antragspflicht des Einlegers). Eine Darlegungspflicht für den Einleger besteht nur, wenn er mehr als 100.000 EUR geltend machen will. Die Einlagenkreditinstitute sind daher verpflichtet, ihre entschädigungsfähigen Einlagen so zu kennzeichnen, dass sie für jeden Einleger sofort ermittelt werden können.

Meldepflicht

Hinsichtlich der gedeckten Einlagen, die sich aus den entschädigungsfähigen Einlagen errechnen, bestehen Meldepflichten. Gemäß der EU-Verordnung Nr. 2015/63 war die erste Meldung über die Höhe der gedeckten Einlagen mit Stand zum 31. Juli 2015 am 1. September 2015 abzugeben.

Handlungsbedarf

- Prüfung, inwiefern die bestehende bankinterne Systematik zur Erhebung der entschädigungsfähigen sowie der gedeckten Einlagen eine ordnungsgemäße Meldung sicherstellt
- Anpassung der Informationen gegenüber Einlegern und Einrichtung einer jährlichen Information
- Beobachtung von möglichen Veränderungen der Beitragshöhe auch vor dem Hintergrund zu bildender Rückstellungen

Neuer EU-weiter Standard für Produktinformationen für Verbraucher

Empfängerkreis

- Emittenten und Anbieter von Anlageprodukten

Hintergrund

Mit der EU-Verordnung 1286/2014 vom 26. November 2014 werden EU-weit einheitliche Basisinformationsblätter (Key Information Dokuments—KID) für bestimmte Anlageprodukte (PRIIP Packaged Retail and Insurance-based Investment Products, verpackte Anlageprodukte für Kleinanleger und Versicherungsanlageprodukte, die einem Anlagerisiko unterliegen) eingeführt. Demzufolge müssen die Anforderungen ab dem 1. Januar 2017 eingehalten werden und die Basisinformationsblätter für die relevanten Anlageprodukte vorhanden sein.

Bis zum 31. März 2016 sollen Entwürfe für Technische Regulierungsstandards (RTS) vorgelegt werden, die im Einzelnen regeln, wie die Basisinformationen (z. B. die Indikatoren und Szenarien) zu berechnen und in den KIDs darzustellen sind. Mitte Juni 2015 wurde dazu ein Technisches Diskussionspapier zur Konsultation gestellt. Zwar gibt es in Deutschland bereits Regelungen zu Informationspflichten (z. B. in § 31 Abs. 3a WpHG), jedoch enthält die PRIIP-Verordnung höhere Anforderungen zur Darstellung der Risiken und Kosten. Eine umschreibende Darstellung dieser Informationen ist dann nicht mehr möglich. Vielmehr sollen diese anhand von Indikatoren dargestellt werden.

Verpackte Anlageprodukte (PRIIP)

PRIIP sind Anlagen in verpackter Form, hinter denen sich ein Anlagerisiko verbirgt. Die Definition wird nur über eine Negativaufzählung eingeschränkt und ist bewusst weit gefasst, um der Heterogenität der Anlageprodukte in der EU gerecht zu werden und um eine Umgehung der Verordnung durch eine bewusste Wahl von Rechtformen, Bezeichnungen oder Zweckbestimmungen zu vermeiden. Zu den PRIIPS zählen z. B. strukturierte Finanzprodukte, Derivate oder geschlossene und offene Investmentfonds.

Basisinformationsblätter

Verantwortlich für die Erstellung ist der Hersteller des jeweiligen Anlageproduktes. Anforderungen sind z. B.

- Leicht verständliche Sprache, Begrenzung der Seitenanzahl auf drei DIN-A4 Seiten
- Angaben zu Risiken des Anlageprodukts (u. a. Beschreibung und Angabe eines Gesamtrisikoindikators)
- Renditemöglichkeiten und maximal möglicher Verlust
- Unterschiedliche Performance-Szenarien
- Direkte, indirekte, einmalige und laufende Kosten in einem Gesamtkostenindikator
- Hinweis auf weitere Vertriebskosten
- Warnhinweis für besonders komplexe PRIIP: „Sie sind im Begriff ein Produkt zu erwerben, das nicht einfach strukturiert ist und schwer zu verstehen sein kann.“

Einzelheiten, z. B. zur Berechnung der Indikatoren und zu Performance-Szenarien, sollen sich in den RTS finden und werden derzeit im Diskussionspapier zur Konsultation gestellt.

Handlungsbedarf

Es ist davon auszugehen, dass der Gesetzgeber die Landschaft der gesetzlichen Produktinformationsblätter neu ordnen wird, so dass pro Produkt nur ein Informationsblatt an den Verbraucher gegeben wird.

- Stellen Sie als Hersteller rechtzeitig sicher, dass Ihre Basisinformationsblätter den Anforderungen entsprechen.
- Stellen Sie rechtzeitig sicher, dass Ihnen alle erforderlichen Basisinformationsblätter für den Vertrieb vorliegen, damit keine Rechtsrisiken entstehen.

Neues zur Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen

Empfängerkreis

- CRR-Kreditinstitute und CRR-Wertpapierfirmen

Rechtsgrundlagen

Die Pflicht zur Erstellung von Sanierungsplänen wurde von ursprünglich nur potenziell systemgefährdeten Instituten auf alle CRR-Kreditinstitute und CRR-Wertpapierfirmen ausgedehnt. In Deutschland wurde dazu zum 1. Januar 2015 das Sanierungs- und Abwicklungsgesetz (SAG) in Kraft gesetzt.

Aktuell ist das Abwicklungsmechanismusgesetz (AbwMechG) im Gesetzgebungsverfahren. Hiermit erfolgen weitere Anpassungen am SAG und am KWG. Insbesondere werden Regelungen zur Haftungskaskade formuliert. Es ist vorgesehen, dass das Gesetz am 1. Januar 2016 in Kraft tritt.

Was passiert mit den bisherigen MaSan (Mindestanforderungen an die Ausgestaltung von Sanierungsplänen)?

Die MaSan beziehen sich noch auf die alten Regelungen im KWG. Bisher wurden die MaSan durch die BaFin nicht widerrufen. Es gibt Überlegungen, die MaSan wie auch die MaRisk in eine Verordnung zu überführen. Diesbezüglich gibt es noch keine endgültige Entscheidung.

Sanierungs– und Abwicklungspläne

Der Zeitpunkt für die erstmalige Fertigstellung und der Umfang des institutsspezifischen Sanierungskonzepts richtet sich nach Größe und Systemrelevanz des jeweiligen Instituts. Ein genauer Zeitplan, wann welche Institute einen Sanierungsplan fertiggestellt haben müssen, ist noch nicht verfügbar.

Die Verpflichtung zur Erstellung eines **Sanierungsplans** besteht erst ab Aufforderung durch die BaFin.

Besondere Ausnahmen gelten für Institute, die einem institutsbezogenen Sicherungssystem angehören. Diese Ausnahmen gelten insbesondere für Sparkassen und Volks- und Raiffeisenbanken.

Die Sanierungspläne sind regelmäßig, mindestens jährlich, zu aktualisieren. Zusätzlich sind anlassbezogene Aktualisierungen vorzunehmen.

Die Erstellung von **Abwicklungsplänen** erfolgt durch die Abwicklungsbehörde (FMSA, Bundesanstalt für Finanzmarktstabilisierung), gegebenenfalls unter Mitwirkung des Instituts. Die genauen Inhalte und Anforderungen an Sanierungs- und Abwicklungspläne sind im SAG festgehalten.

Durch die Erstellung von **Sanierungs- und Abwicklungsplänen** soll die Sicherheit des Finanzsystems gestärkt werden. Wenn ein Institut in Schieflage gerät, soll somit sichergestellt werden, dass eine Sanierung oder gegebenenfalls Abwicklung schnell und ohne großen Schaden für weitere Markteilnehmer und Kunden erfolgen kann. Die Erstellung und regelmäßige Aktualisierung der Sanierungskonzepts stellt teilweise einen erheblichen Mehraufwand für die Institute dar.

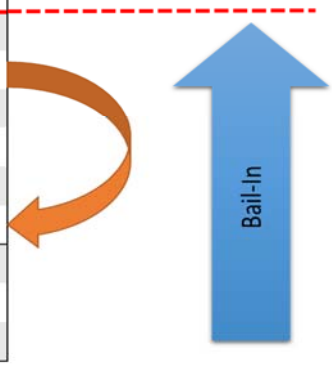
Haftungskaskade

Das SAG sieht die Beteiligung der Gläubiger und Anteilseigner an der Sanierung oder einer späteren Abwicklung vor. Ausnahmen hiervon bilden die besicherten Einlagen bis 100.000 EUR pro Kunde sowie besicherte Verbindlichkeiten (z. B. Pfandbriefe). Anleihen fallen nach dem AbwMechG vom 3. auf den 4. Insolvenzrang. Das bedeutet, dass sie mit als Erste zur Sanierung des Emittenten herangezogen werden.

Die Definition der Haftungskaskade wird so vom Gesetzgeber vorgenommen und nicht der Abwicklungsbehörde überlassen.

Die Abbildung zeigt die Reihenfolge bei einem Bail-In. Hier ist die Umgliederung von Anleihen ersichtlich.

Insolvenzrangfolge		
Besicherte Verbindlichkeiten	0	Pfandbriefe
Unbesicherte Verbindlichkeiten	1	Besicherte Einlagen <= 100 TEUR
	2	Einlagen > 100 TEUR (Private, KMU)
	3	Anleihen (aktuelles Insolvenzrecht)
	3	Interbank Einlagen >= 7 Tage
	3	Strukturierte Verbindlichkeiten/ Derivate
	3	Weitere
	4	Anleihen (AbwMechG)
Eigenkapital & Nachrangkapital		Ergänzungskapital
		Zusätzliches Kernkapital (AT 1)
		Hartes Kernkapital (CET 1)



Fazit:

Deutschland ist mit den Regelungen des SAG und den Anpassungen durch das AbwMechG einer der Vorreiter in der Sanierung und Abwicklung von Banken und Wertpapierfirmen.

Sanierungspläne sind nach und nach von allen deutschen Instituten und Wertpapierfirmen zu erstellen. Anleihen werden nach dem AbwMechG in Deutschland im Falle einer Sanierung/Abwicklung schneller an einem Bail-In beteiligt.

Die weitere Gesetzgebung im Bereich der MaRisk und der MaSan bleibt abzuwarten.

Handlungsbedarf

- Nach Aufforderung durch die BaFin zeitnahe Aufstellung und regelmäßige Aktualisierung eines Sanierungskonzepts
- Erarbeitung einer internen wie externen Kommunikationsstrategie für den Sanierungsplan
- Beachtung der Möglichkeiten zum Bail-In von Anleihen
- Verfolgung der Gesetzgebung zu den MaRisk & MaSan

EBA veröffentlicht work programm

Die European Banking Authority (EBA) hat im Oktober 2015 ihr Arbeitsprogramm veröffentlicht.

Es beschreibt die Hauptziele und Ergebnisse der EBA für die nächsten Jahre. Für 2016 ist das Arbeitsprogramm in acht strategische Felder und insgesamt 34 Aktivitäten aufgeteilt und beinhaltet eine Beschreibung der Ziele, der erwarteten Ergebnisse und der geplanten Outputs.

Im Aufgabenfeld für 2016 zeigen sich zum einen die Auswirkungen aus dem unterjährig angepassten Arbeitsprogramm 2015, in dem u. a. die Erarbeitung einiger RTS und ITS verschoben wurde, und zum anderen eine Schwerpunktsetzung der EBA auf die Weiterentwicklung des Single Rulebook.

„Zahlungskontenrichtlinie“ - Sind Ihre Prozesse zur Kontenwechselhilfe schnell genug?

Empfängerkreis

- Verantwortliche für die Kontoführung, Verantwortliche für Prozessmanagement

Hintergrund

Die Richtlinie 2014/92/EU über die Vergleichbarkeit von Zahlungskontoentgelten, den Wechsel von Zahlungskonten und den Zugang zu Zahlungskonten mit grundlegenden Funktionen („Zahlungskontenrichtlinie“) ist am 17. September 2014 ist in Kraft getreten. Sie ist bis zum 18. September 2016 ins deutsche Recht umzusetzen. Das Inkrafttreten des künftigen Zahlungskontengesetzes ist für Anfang 2016 geplant, der Referentenentwurf wurde bereits veröffentlicht. Zielsetzung des Gesetzes ist, jedem Verbraucher den Zugang zu einem Zahlungskonto mit grundlegenden Funktionen zu geben.

Weiterhin soll Verbrauchern EU-weit der Wechsel ihrer Zahlungskonten erleichtert werden. In diesem Zusammenhang ist eine Kontenwechselhilfe auf Basis einer Ermächtigung des Verbrauchers/Konteninhabers vorgesehen.

Kontenwechselhilfe

Für die Ermächtigung zur Kontenwechselhilfe werden Musterformulare zur Verfügung gestellt.

Der ermächtigte (neue) Zahlungsdienstleister hat dann innerhalb von zwei Geschäftstagen nach Erhalt der Ermächtigung den übertragenden Zahlungsdienstleister aufzufordern, Informationen zur Verfügung zu stellen, u. a.:

- Liste bestehender Daueraufträge und verfügbare Informationen zu Lastschriftmandaten
- Informationen über wiederkehrende eingehende Überweisungen und vom Zahlungsempfänger veranlasste Lastschrifteinzüge der vorangegangenen 13 Monate

Der übertragende Zahlungsdienstleister hat die Informationen innerhalb von fünf Geschäftstagen dem ermächtigten Zahlungsverkehrsdienstleister zur Verfügung zu stellen.

Nach Erhalt der Informationen hat der ermächtigte Zahlungsdienstleister u. a. innerhalb von fünf Geschäftstagen:

- die gewünschten Daueraufträge einzurichten und alles Notwendige für die Akzeptanz der Lastschriften vorzubereiten
- den Auftraggebern wiederkehrender, eingehender Überweisungen die Angaben zur neuen Zahlungskontoverbindung mitzuteilen
- Lastschrift-Zahlungsempfängern die Angaben zur neuen Zahlungskontoverbindung mitzuteilen

Liegen dem neuen Zahlungsdienstleiter nicht alle erforderlichen Informationen vor, die er für die zuvor genannten Mitteilungen benötigt, hat er den Verbraucher oder den übertragenden Zahlungsdienstleister aufzufordern, ihm die fehlenden Informationen mitzuteilen.

Der empfangende (neue) und der übertragende (alte) Zahlungsdienstleister haften gegenüber dem Verbraucher für Schäden aus einer Verletzung ihrer Pflichten.

Handlungsbedarf

- Prüfen Sie, ob Ihre Prozesse zum Kontenwechsel auf die neuen Anforderungen ausgelegt sind und passen Sie diese rechtzeitig an (ggf. auch im Hinblick auf IT-Lösungen oder Personalkapazitäten).
- Prüfen Sie, ob die festgelegten Fristen eingehalten können.

Lageberichterstattung nach DRS 20 - Update

Empfängerkreis

- Primär: Mutterunternehmen, die einen Konzernlagebericht gemäß § 315 HGB verpflichtend oder freiwillig aufstellen
- Empfehlung: Alle Unternehmen, die einen Lagebericht gemäß § 289 HGB verpflichtend oder freiwillig aufstellen

In 2012 hat das Deutsche Rechnungslegungs-Standards Committee e.V. (DRSC) einen neuen Standard zur Konzernlageberichterstattung verabschiedet. Dieser ist seit dem 1. Januar 2013 für alle deutschen Unternehmen, die zur Konzernlageberichterstattung verpflichtet sind oder eine Aufstellung auf freiwilliger Basis vornehmen, anzuwenden.

Das Thema „Lageberichterstattung“ war auch in 2015 wieder einer der Prüfungsschwerpunkte der Deutschen Prüfstelle für Rechnungslegung (DPR). Unter anderem wird eine „konsistente und transparente Berichterstattung finanzieller und nicht finanzieller Leistungsindikatoren“ auch gemäß DRS 20 überprüft. Die DPR-Prüfungen der gleichen Anforderung in 2014 haben gezeigt, dass hier noch viele Mängel, z. B. bezüglich einer Darstellungskonsistenz bestehen. Erforderlich ist, dass sämtliche Lageberichtsabschnitte eine kongruente Abbildung von relevanten Leistungsindikatoren gewährleisten müssen, d. h. die gleichen bedeutsamen Indikatoren sollen sowohl bei dem internen Steuerungssystem, Vergütungssystem als auch bei der Prognoseberichterstattung verwendet werden, damit die erforderliche Transparenz sichergestellt werden kann.

Bei den Angaben zum Vergütungssystem ist auch die Institutsvergütungsverordnung in ihrer gültigen Fassung entsprechend zu beachten. Dies bedeutet, dass z. B. die Vergütungsstruktur entsprechend den erfolgs– und anreizabhängigen Leistungsparametern unter Beachtung des internen Steuerungssystems transparent auszurichten ist.

Schlussfolgernd ist hervorzuheben, dass bei der Erstellung des Lageberichts insbesondere auf Transparenz, Einheitlichkeit und Wesentlichkeit zu achten ist.

Handlungsbedarf

Überprüfen Sie nochmals die Konformität Ihrer Lageberichtsangaben mit den Anforderungen nach DRS 20. Beachten Sie dabei insbesondere die folgenden Punkte:

- Sind alle Lageberichtsbestandteile schlüssig?
- Erfolgt die Kategorisierung der wichtigsten Leistungsindikatoren in finanzielle und nicht finanzielle einheitlich?
- Werden die wichtigsten Leistungsindikatoren (finanzielle und nicht finanzielle) konsequent in allen Bestandteilen des Lageberichts (z. B. Internes Steuerungssystem, Prognosebericht, Wirtschaftsbericht etc.) berücksichtigt?
- Werden beim Vergütungssystem die gleichen bedeutsamen Leistungsindikatoren wie beim internen Steuerungssystem erfasst?
- Werden alle bedeutsamen Indikatoren (finanzielle und nicht finanzielle) des Steuerungssystems berücksichtigt? Werden die Berechnungsansätze dargelegt, soweit erforderlich?
- Erfolgt eine deutliche Differenzierung zwischen Annahmen und Prognosen? Werden Prognosen über sämtliche bedeutsamen Leistungsindikatoren erstellt?
- Wird auf die Prognosegenauigkeit bei allen relevanten Leistungsindikatoren geachtet?
- Erfolgt der Vergleich der relevanten Leistungsindikatoren des aktuellen Geschäftsjahres mit den im Lagebericht des Vorjahres abgegebenen Prognosen?

Vor dem Stresstest ist nach dem Stresstest—Was kommt 2016?

Empfängerkreis

- Vorstände, verantwortliche Führungskräfte Stresstest

Hintergrund

Der Stresstest im Zusammenhang mit dem Asset Quality Review (AQR) in 2014 bedeutete für die teilnehmenden Institute großen und in weiten Teilen insbesondere manuellen Aufwand. Die erforderlichen Zulieferungen und Bereitstellungen von Daten machte Instituten deutlich, an welchen Stellen Daten noch nicht „auf Knopfdruck“ geliefert werden konnten und zeigte damit Optimierungspotenzial auf. Es wurde daher empfohlen, aus dem ersten Stresstest „lessons learned“ zu generieren und einen Stresstest als „Regelprozess“ zumindest zu konzipieren, um den „Stress“ im Zusammenhang mit künftigen Stresstests für die beteiligten Mitarbeiter im Unternehmen zu minimieren.

Mit Beschluss vom 2. März 2015 teilte die EBA mit, dass in 2015 kein EU-weiter Stresstest geplant ist, aber die Vorbereitungen für einen Stresstest in 2016 beginnen.

Stresstest 2016

Im Juli 2015 veröffentlichte die EBA weitere Informationen zur Transparenzübung 2015 und zum Stresstest 2016.

Die an der Transparenzübung 2015 teilnehmenden Kreditinstitute sind bekannt. Darunter sind 20 deutsche Institute.

Für 2016 ist ein erneuter EU-weiter Stresstest vorgesehen. Dieser soll viele Aspekte des Stresstests 2014 aufgreifen u. a. den Bottom-Up-Ansatz einschließlich eines statischen Bilanzansatzes und eine weitgreifende Berücksichtigung von Risiken zur Beurteilung der Solvabilität der EU Banken. Als Lehre aus dem Stresstest in 2014 ist in 2016 eine engere Verzahnung mit dem SREP-Prozess geplant, um sicherzustellen, dass die Ergebnisse des Stresstest in den SREP integriert werden können.

Die Methodik und die Templates wurden als Entwurf am 5. November 2015 veröffentlicht und zur Diskussion gestellt. Es ist geplant, die finalen Templates und die Methodik Ende Februar 2016 zu veröffentlichen und die Ergebnisse im 3. Quartal 2016 zu publizieren.

Da bereits Templates im Entwurf veröffentlicht wurden (siehe http://www.eba.europa.eu/-/eba-announces-details-of-2016-eu-wide-stress-test), kann jedoch schon jetzt damit begonnen werden zu prüfen, inwieweit die hierin enthaltenen Daten so vorgehalten werden, dass diese auch in einem Stresstest 2016 entsprechend zur Verfügung gestellt werden können.

Handlungsbedarf

Sofern Sie zum Kreis der Institute mit Optimierungspotenzial gehören, tragen Sie die Erfahrungen aus dem letzten Stresstest und AQR zusammen, bewerten und dokumentieren sie diese:

- Was lief gut? – Was lief weniger gut?
- Welches Optimierungspotenzial wurde bereits erkannt? – Was wurde bereits umgesetzt? – Wo besteht noch Handlungsbedarf?
- Vergleichen Sie die gemäß Entwurf der Templates (Link s. o.) geforderten Daten mit den zur Verfügung stehenden Daten.—Konzipieren und planen Sie die Umsetzung des Handlungsbedarfs rechtzeitig.

Beratungsangebote und weitere Dienstleistungen (Auszug)

- Umsetzung BCBS 239 Risikoreporting
- SREP Quick Scan
- Simulation und Change Management einer Sonderprüfung nach § 44 KWG
- Umsetzung Asset Encumbrance
- Optimierungsprozesse im Rahmen von aufsichtsrechtlichen Umsetzungsprojekten
- Rechtliche Gestaltungsberatung (CASIS Rechtsanwaltsgesellschaft)
- Marken– und Lizenzanmeldungen (CASIS Rechtsanwaltsgesellschaft)

Aus unserem Seminar- und Workshop-Angebot (Auszug)

- Aufsichtsenglisch für nationale/lokale Banken
- § 44 KWG reloaded—SREP, AQR, Challenger Modell 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
  - Mitarbeiter in Marktfolgebereichen (Marktfolgen Passiv/Aktiv, Zahlungsverkehr)
- MaRisk 6.0
- IT-Prüfung
- Aktuelle Hinweise für die Gesamtprüfungsplanung der Internen Revision 2016

V. Impressum

Herausgeber dieser Ausgabe sind:

CASIS Heimann Buchholz Espinoza
Partnerschaft
Wirtschaftsprüfungsgesellschaft

Esplanade 41
20354 Hamburg
T: +49 40 80 80 110 20
F: +49 40 80 80 110 29
E-Mail: info@casis-wp.de

CASIS
Rechtsanwaltsgesellschaft mbH

Esplanade 41
20354 Hamburg
T: +49 40 80 80 110 24
F: +49 40 80 80 110 29
E-Mail: s.beiersdorfer@casis-wp.de

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

Carolin Riekel
c.riekel@casis-wp.de

Redaktionsschluss: 30.10.2015

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