Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Stellungnahme

Öffentliche Konsultation des Rundschreibens „Bankaufsichtliche Anforderungen an die IT" (BAIT)

Konsultation 13/2020 vom 26.10.2020

Kontakt:
Berit Schimm
Telefon: +49 30 2021- 2111
Telefax: +49 30 2021-19 - 2100
E-Mail: b.schimm@bvr.de

Berlin, 23.11.2020

Federführer:
Bundesverband der Deutschen Volksbanken
und Raiffeisenbanken e. V.
Schellingstraße 4 | 10785 Berlin
Telefon: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Allgemeine Anmerkungen

Die BAIT-Novelle, die insbesondere auch die Anforderungen der EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken (EBA/GL/2019/04) sowie Klarstellungen aufgrund von Prüfungsfeststellungen berücksichtigt, wird für die Umsetzung bankaufsichtlicher Anforderungen in den Instituten einen wesentlichen Orientierungsrahmen bilden.

Die BAIT-Novelle enthält insbesondere neue Anforderungen an die operative Informationssicherheit und das IT-Notfallmanagement. Auch wenn entsprechende Rahmenbedingungen grundsätzlich durch die EBA-Leitlinien vorgegeben ist, liegen die konkreten nationalen Vorgaben mit der Veröffentlichung der BAIT-Novelle dann erstmalig vor. Den Instituten sollte für die Umsetzung der neuen BAIT-Anforderungen deshalb unbedingt eine angemessene Übergangsfrist von einem Jahr ab Veröffentlichung der BAIT-Novelle eingeräumt werden. Wir verweisen in diesem Zusammenhang auf die DK-Stellungnahme vom 23.3.2020 „Vorschläge zu unmittelbaren Handlungen von Bankenaufsicht, Gesetzgeber und Förderinstituten angesichts der Herausforderungen der Corona-Krise", Unmittelbarer Handlungsbedarf der Aufsicht, 2. o).

Bei den neuen bzw. erweiterten Anforderungen der BAIT-Novelle ist ein teilweise deutlich höherer Detaillierungsgrad zu erkennen, der in Folge auch höhere Dokumentationsaufwände nach sich zieht. Wie bisher sollte eine risikoorientierte Vorgehensweise gewählt werden. Wir bitten grundsätzlich darum, die Detailtiefe der Anforderungen zu prüfen und nach besten Möglichkeiten zu reduzieren, um weiterhin einen prinzipienorientierten Ansatz und eine Umsetzung unter Proportionalitätsgesichtspunkten zu ermöglichen sowie den Dokumentationsaufwand der Institute nicht unverhältnismäßig zu erhöhen.

Einige Verständnisfragen zu neuen Anforderungen der BAIT-Novelle wurden im Fachgremium Informationstechnologie (Fachgremium IT) der Aufsicht bereits mit Banken und Vertretern der Verbände erörtert. Um Verständnisfragen der anwendenden Institute zu reduzieren, schlagen wir vor, die Erläuterungen der Aufsicht transparent zu machen (vgl. Abschnitt Verständnisfragen zu den jeweiligen Kapiteln). Mögliche Alternativen sind die Ergänzung der Erläuterungsspalte oder die Veröffentlichung der Protokolle des Fachgremiums Informationstechnologie auf der Homepage der BaFin.

Spezielle Anmerkungen zu den einzelnen Kapiteln

1. IT-Strategie / 2. IT-Governance

Zu 1.2 a) sowie 2.4 IT-Aufbau- und IT-Ablauforganisation

Die Formulierung "IT-Aufbau- und IT-Ablauforganisation" sollte mit Blick auf agile Vorgehensweisen und interdisziplinäre Teams überprüft werden. Eine „getrennte" IT-Aufbauorganisation schränkt organisatorische und ggf. prozessuale Gestaltungsmöglichkeiten ein. Wir gehen davon aus, dass die in den BAIT verankerten Prinzipien analog auch für agile Vorgehensweisen angewandt werden können, dies sollte jedoch auch durch die Begriffswahl in den BAIT deutlich werden.

Formulierungsvorschlag:
„~~IT-~~Aufbau- und ~~IT-~~Ablauforganisation zur Erstellung und Betrieb von IT-Systemen" sowie Ergänzung in der Erläuterungsspalte: Die Anforderungen sind prinzipienorientiert auf agile Vorgehensweisen zu übertragen.".

3. Informationsrisikomanagement

3.4 im Zusammenhang mit 3.2 Eigentümer der Informationen

Gemäß Tz. 3.4 hat die Ermittlung des Schutzbedarfes für die Bestandteile des Informationsverbundes zu erfolgen. Zu den Bestandteilen zählen u.a. geschäftsrelevante Informationen und Geschäfts- und Unterstützungsprozesse. Gemäß der Ergänzung in 3.4 i. V. mit 3.2 verantwortet jedoch der Fachbereich, der Eigentümer der Information ist, (alleinig) die Ermittlung des Schutzbedarfes.

Da eine Information innerhalb eines Informationsverbundes an verschiedenen Stellen vorhanden sein kann, ergibt sich der Schutzbedarf aus dem Zusammenspiel von Schutzbedarf der Information und des Geschäftsprozesses. Beispielsweise kann ein Geschäftsprozess einen hohen Schutzbedarf mit Blick auf die Verfügbarkeit haben, die im Geschäftsprozess genutzte Information eines anderen Fachbereichs benötigt jedoch aus Sicht des Informationseigentümers nur einen mittleren Schutzbedarf.

Formulierungsvorschlag:

Tz. 3.2 Zu den maßgeblichen Stellen gehören auch die Fachbereiche, die verantwortlich für die Geschäftsprozesse und/ oder Eigentümer der Informationen ~~oder der Informationsrisiken~~ sind.

Tz. 3.4 Die Fachbereiche, die verantwortlich für die Geschäftsprozesse und / oder Eigentümer der Informationen sind, verantworteten die Ermittlung des Schutzbedarfes.

Verständnisfragen zu Kapitel 3

3.5 und 3.9 Informationsrisikomanagement

In der Textziffer wird dem Informationsrisikomanagement die Aufgabe zur Überprüfung der Schutzbedarfsfeststellung und der Koordination und Überwachung der Risikoanalyse zugewiesen. In der Praxis wird die Schutzbedarfsfeststellung sowie die IT-Risikoanalyse häufig vom Informationssicherheitsmanagement koordiniert, die Risiken dann an das Risikomanagement (OpRisk) übergeben. Der genaue Schnitt kann sich dabei von Institut zu Institut unterscheiden. Wir gehen davon aus, dass dies im Einklang mit den aufsichtlichen Anforderungen steht.

Bei der Überprüfung der Schutzbedarfsfeststellung sowie der zugehörigen Dokumentation durch das Informationsrisikomanagement geht die DK auf Basis der Erläuterungen im Fachgremium IT davon aus,

dass hiermit eine übergreifende Plausibilisierung gemeint ist. Eine nachgelagerte Überprüfung aller einzelnen Klassifizierungen ist qualifiziert nicht durchführbar, dies obliegt den Fachabteilungen.

Für diese Frage sowie für die weiteren Verständnisfragen in den nachfolgenden Kapiteln: Wir bitten die Aufsicht, wie in den allgemeinen Anmerkungen angeregt, entsprechende Erläuterungen zu ergänzen bzw. öffentlich zu machen.

4. Informationssicherheitsmanagement

Verständnisfragen zu Kapitel 4

4.2 Auftragnehmer

In dieser Textziffer/ Erläuterungsspalte wird der Begriff „Auftragnehmer" anstelle dem an anderen Stellen gängigen Begriff „IT-Dienstleister" gewählt und damit breiter gefasst. Die DK bittet um eine erläuternde Klarstellung.

4.5 Organisatorische und prozessuale Unabhängigkeit des Informationssicherheits-beauftragten

Die Streichung des Wortes „aufbauorganisatorisch" im Satz „Die Funktion des Informationssicherheitsbeauftragten wird von den Bereichen getrennt, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind." ist sachgerecht. Wie im Fachgremium IT erläutert, wird somit eine zu strikte Auslegung im Sinne einer Trennung der Berichtslinien von IT-Organisation und ISB bis auf Vorstandsebene vermieden.

Wir bitten um Erläuterung zur Kombination aus Datenschutzbeauftragtem und Informations-sicherheitsbeauftragtem aus Sicht der BaFin, da es hierzu zahlreiche Rückfragen aus den Instituten gibt.

4.8 Richtlinie über das Testen und Überprüfen der Maßnahmen

Aus der Anforderung geht nicht eindeutig hervor, welche Tests und Überprüfungen durch diese Richtlinie abgedeckt werden sollen. Auf Basis der Erläuterungen aus dem Fachgremium IT schließt die DK, dass hier Vorgaben für die Überprüfungen gemeint sind, die in der Textziffer 5.6 aufgeführt werden, nicht jedoch der Vergleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen gemäß Tz. 3.7 oder die Audits der internen Revision.

4.9 Erfolgsprüfung Sensibilisierungs-und Schulungsmaßnahmen

Sensibilisierungs-und Schulungsmaßnahmen sollten nach unserem Verständnis auf Erfolg ausgelegt sein, dazu gehören auch Erfolgskontrollen. Da die EBA-Leitlinien keine ausdrückliche Erfolgskontrolle vorsieht, gehen wir davon aus, dass Institute die Art und die Tiefe einer Erfolgskontrolle selbst wählen können.

5. Operative Informationssicherheit

5.3 – 5.5 Auswertung sicherheitsrelevanter Informationen

Die Anforderung einer zentralen Auswertung sicherheitsrelevanter Informationen mit einem Portfolio an Regeln in 5.3 - 5.5 ist nicht prinzipienorientiert. Zum Vergleich: Die EBA-Leitlinien fordern Regelungen und Verfahren, um ungewöhnliche Aktivitäten zu identifizieren, welche die Informationssicherheit der Finanzinstitute beeinflussen könnten, und um auf diese Ereignisse auf angemessene Weise reagieren zu können. Die Art und Weise der Umsetzung solcher Regelungen und Verfahren wird in den EBA-Leitlinien nicht detailliert.

Die gewählten Formulierungen „angemessen zeitnah", „erfordert in der Regel" sowie „kann eine ständig besetzte Stelle" lassen eine gewisse Proportionalität erkennen. Es ist jedoch unklar, ob sich das Wort „angemessen" auch auf die Attribute „regelbasierte, zentrale Auswertung" bezieht. Je nach Auslegung des Begriffs „regelbasierte, zentrale Auswertung" in 5.3 kann dies faktisch doch zum zwingenden Einsatz automatisierter IT-Systeme führen. Bei

Auslagerung von IT-Systemen an IT-Dienstleister wird die Auswertung sicherheitsrelevanter Ereignisse häufig im Auftrag des Instituts durch den Dienstleister – hier i.d.R. automatisiert vorgenommen. Für die im Institut verbleibende IT-Systeme nimmt das Institut ggf. selbst Auswertungen vor, bei geringem Umfang ggf. nicht automatisiert und getrennt von den Auswertungen des Dienstleisters. Eine zentrale Auswertung aller Ereignisse unabhängig vom Betreiber, würde einen erheblichen Aufwand bei den Instituten verursachen.
Der Begriff „regelbasiert" in 5.3 kann zudem entfallen, da die Aussage ein angemessenes Portfolio an Regeln zu verwenden in 5.4 aufgegriffen wird und dort präziser gefasst ist.

Formulierungsvorschlag zu 5.3:

Gefährdungen des Informationsverbundes sind möglichst frühzeitig zu identifizieren. Potentiell sicherheitsrelevante Informationen sind angemessen zeitnah~~, regelbasiert und zentral~~ auszuwerten. Diese Informationen müssen bei Transport und Speicherung geschützt werden und für eine angemessene Zeit zur späteren Auswertung zur Verfügung stehen.

Sowie in der Erläuterungsspalte:

Die ~~regelbasierte~~ Auswertung ~~(z. B. über Parameter, Korrelationen von Informationen, Abweichungen oder Muster)~~ großer Datenmengen erfolgt ~~erfordert~~ in der Regel zentral unterstützt durch den Einsatz automatisierter IT-Systeme.

Ergänzung der Erläuterungsspalte 5.4

Regeln basieren z. B. auf Parameter, Korrelationen von Informationen, Abweichungen oder Muster.

Verständnisfragen zu Kapitel 5

Zu 5.6 Überprüfung der Sicherheit von IT-Systemen

Die Überprüfung der Sicherheit von IT-Systemen kann aus Sicht der DK auch durch den IT-Dienstleister erfolgen, wenn dieser unter Vermeidung von Interessenskonflikten eine Überprüfung der Sicherheit der IT-Systeme sicherstellt. Aus Sicht der DK, die im Fachgremium IT grundsätzlich geteilt wurde, muss das Institut in diesem Fall keine eigenen Überprüfungen vornehmen, sofern geeignete vertragliche Vereinbarungen mit dem Dienstleister getroffen wurden und das Institut eine angemessene Steuerung und Überwachung des Dienstleisters vornimmt (Erfüllung der Vorgaben des AT 9 MaRisk).

6. Identitäts- und Rechtemanagement

Verständnisfragen zu Kapitel 6

Zu 6.2 Ausweitung auf Zutritte

Grundsätzlich tragen Zutrittsrechte ebenso wie Zugangs- und Zugriffsrechte zur Informationssicherheit bei, jedoch geschieht dies bei der physischen Zutrittssteuerung weniger granular als bei Zugangsrechten zu IT-Systemen. Die DK geht auf Basis der Erläuterungen im Fachgremium IT davon aus, dass die üblichen Zonenkonzepte für Gebäudeteile unter Berücksichtigung besonderer Schutzmaßnahmen für privilegierte Zutrittsrechte (6.7) ausreichend sind.

Zu 6.3 Nicht personalisierte Aktivitäten

Die Passage "auch bei nicht personalisierten Aktivitäten" ist missverständlich.

Formulierungsvorschlag: Zugriffe und Zugänge müssen auch bei der nicht personalisierten Nutzung jederzeit zweifelsfrei einer handelnden bzw. verantwortlichen Person (möglichst automatisiert) zuzuordnen sein.

Zu 6.7 Privilegierte Benutzer- und Zutrittsrechte

Wir bitten um nähere Erläuterung der Abgrenzung von privilegierten Benutzer- und Zutrittsrechten. Die DK geht auf Basis der Erläuterungen im Fachgremium IT davon aus, dass der Begriff nicht nur kritische

Administrationsrechte meint, sondern z. B. auch Zutrittsrechte zu Rechenzentren oder Vorstandsräumen sowie Zugriffsrechte auf besonders zu schützende Informationen mit abdecken soll.

7. IT-Projekte, Anwendungsentwicklung

Vorgehensweise und Begriffe in diesem Kapitel orientieren sich stark an klassischen Vorgehensmodellen von IT-Projekten und wenig an agilen Arbeitsmethoden. Heute findet vermehrt ein Wechsel von projekt- zu einer produktbezogenen Organisation bei Veränderungen an IT-Systemen in Instituten statt. Planungszyklen mit nacheinander abzuschließenden Phasen nach der Wasserfallmethode entfallen zunehmend. Merkmal für agile Methoden sind schnelle Entwürfe mit vielen Feedbackschleifen, die sich nicht abstrakt auf einer Konzeptebene abspielen.

Verständnisfragen zu Kapitel 7

Zu 7.2 Projektunabhängige Qualitätssicherungsmaßnahmen

Wir bitten um Erläuterung, was unter „projektunabhängige Qualitätssicherungsmaßnahmen" zu verstehen ist. Die DK geht auf Basis der Erläuterungen im Fachgremium IT davon aus, dass Qualitätssicherungsmaßnahmen auch außerhalb des jeweiligen Projektes angesiedelt werden sollten, jedoch Handlungsspielraum besteht, ob diese der 1st oder 2nd Line of Defense zugeordnet werden.

Zu 7.6 IDV

Grundsätzlich sind aus Sicht der DK unterschiedliche Prozessausgestaltungen für IDV und reguläre Anwendungsentwicklung möglich und sinnvoll, auch wenn grundsätzlich die gleichen Anforderungen gelten.

Zu 7.11 Penetrationstests

Die DK geht auf Basis der Erläuterungen im Fachgremium IT davon aus, dass hier Penetrationstests zur Überprüfung der IT-Sicherheit vor Einführung der Anwendung gemeint sind, sofern dies aufgrund der potentiellen Angriffsfläche notwendig ist. Diese Anforderung steht im Zusammenhang mit den Tz. 4.8 und 5.6.

10. IT-Notfallmanagement

Zu 10.4 Wirksamkeit der IT-Notfallpläne

Tz. 10.4 fordert, dass alle IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, durch jährliche IT-Notfalltests vollständig abgedeckt werden müssen. Die EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken fordern zwar generell die jährliche Prüfung für kritische Geschäftsfunktionen, Unterstützungsprozesse und IT-Assets über angemessene plausible Szenarien, ohne jedoch den Abdeckungsgrad in der Tiefe zu detaillieren, wie dies zukünftig mit den BAIT i.V.m. den MaRisk AT 7.3 erfolgen soll. Derzeit erfolgt eine Streckung auf einen mehrjährigen, risikoorientierten Testplan. Eine jährliche Prüfung unter Einbeziehung aller IT-Systeme stellt einen hohen Mehraufwand in den Instituten oder bei den IT-Dienstleistern dar. Wir schlagen deshalb vor, dass bei den zeitkritischen Aktivitäten und Prozessen zwischen solchen, die kritische Geschäftsfunktionen unterstützen und eine sehr hohe Verfügbarkeit benötigen und anderen zeitkritischen Aktivitäten und Prozessen unterschieden wird, um eine stärkere risikoorientierte Vorgehensweise zu ermöglichen. Für IT-Systeme, die kritische Geschäftsfunktionen mit sehr hoher Verfügbarkeit unterstützen, könnte ein mindestens jährlicher IT-Notfalltest vorgesehen

werden. Für IT-Notfalltests anderer IT-Systeme, die zeitkritische Aktivitäten und Prozesse unterstützen, wäre ein mehrjähriger Turnus weiterhin möglich.

Formulierungsvorschlag zu 10.4:

Die Wirksamkeit der IT-Notfallpläne ist durch regelmäßige ~~mindestens jährliche~~ IT-Notfalltests zu überprüfen. Die Tests müssen alle IT-Systeme, die zeitkritische Aktivitäten und Prozesse unterstützen, vollständig abdecken. Für kritische Geschäftsfunktionen, die eine sehr hohe Verfügbarkeit erfordern, sind diese Tests mindestens jährlich durchzuführen.

Verständnisfragen zu Kapitel 10

Zu 10.5 Szenario Ausfall eines Rechenzentrums

Ein solcher Test kann erhebliche Risiken bergen, deshalb sollten risikoreduzierende Maßnahmen von der Aufsicht auf jeden Fall akzeptiert werden. Während des Tests sollte das andere Rechenzentrum nicht abgeschaltet oder Herunterfahren werden müssen und die Datenspiegelung aufrechterhalten werden dürfen.

Wir bitten um Ergänzung der Erläuterungen zu dieser Anforderung, insbesondere zu Umfang und Häufigkeit des Nachweises, so wie diese im Fachgremium IT diskutiert wurde.

Formulierungsvorschlag zur Erläuterungsspalte:

Der Test des Ausfalls eines Rechenzentrums soll sowohl die Kapazität als auch die Unabhängigkeit des anderen Rechenzentrums über realistische Szenarien adressieren. Da ein solcher Test erhebliche Risiken in sich bergen kann, werden auch risikoreduzierende Maßnahmen, bspw. die Aufrechterhaltung der Datenspiegelung, akzeptiert.