plenum

bait – novellierung 2021

erweiterung der anforderungen an die it

historie und grundlagen der novellierung

Die BAIT wurde zuletzt im Jahr 2018 mit der Ergänzung des Kapitels Kritische Infrastrukturen aktualisiert. Nach Abschluss der Konsultation im vergangenen Jahr, wurde die novellierte BAIT nun am 16. August 2021, parallel zur 6. MaRisk-Novelle, veröffentlicht. Inhaltliche Basis bilden insbesondere die in 2020 in Kraft getretenen EBA-Leitlinien zu IKT- und Sicherheitsrisikomanagement, welche in der aktuellen MaRisk-Novelle aufgegriffen werden und in der BAIT-Novelle eine erweiternde Konkretisierung erfahren. Mit der finalen Veröffentlichung finden die ergänzten und geänderten Inhalte der BAIT sofort Anwendung. D.h. es gilt traditionell wieder die Wirksamkeit bzw. der Umsetzungszeitraum der Anforderungen „sofort“, da die o.g. inhaltliche Basis von der BaFin als bekannt vorausgesetzt wird.

die kapitel der novellierten bait

1. IT-Strategie
2. IT-Governance
3. Informationsrisiko-management
4. Informationssicherheits-management
5. Operative Informations-sicherheit NEU
6. Identitäts- und Rechte-management
7. IT-Projekte und Anwendungsentwicklung
8. IT-Betrieb
9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
10. IT-Notfallmanagement NEU
11. Management der Beziehungen mit Zahlungsdienstnutzern NEU
12. Kritische Infrastrukturen

Abb. 1: Die Kapitel der novellierten BAIT

gesamtbetrachtung der kapitel-änderungen

Die BAIT-Novelle umfasst die drei zusätzlichen Kapitel Operative Informationssicherheit, IT-Notfallmanagement und Management der Beziehungen mit Zahlungsdienstnutzern. Diese finden sich analog zum großen Teil auch in den EBA-Leitlinien wieder und stellen weitere Konkretisierungen der MaRisk dar (AT 7.2 und AT 7.3).

Das Kapitel Management der Beziehungen mit Zahlungsdienstnutzern entstammt dem neuen Rundschreiben „Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld Instituten“ (ZAIT). Die Inhalte sind auch für große Teile der BAIT-Zielgruppe relevant und sind daher in die nun veröffentlichte Fassung der BAIT-Novelle eingeflossen.

Sieben weitere, bereits bestehende Kapitel wurden inhaltlich geändert bzw. ergänzt. Basis der Änderungen/ Ergänzungen sind, neben den EBA-Leitlinien, insbesondere in Prüfungen der Aufsicht ermittelte Defizite (Prüfungsfeststellungen) sowie punktuell erforderliche, explizitere bzw. detailliertere Vorgaben.

Die Kapitel IT-Governance und Kritische Infrastrukturen sind unverändert geblieben.

strukturelle änderungen

Die BAIT wurde auch strukturell novelliert. Die drei neuen Kapitel wurden eingefügt, nicht angehängt, so dass sich eine neue Nummerierung in der Gesamtabfolge ergibt.

Die bisherigen, übergreifenden Textziffern wurden zugunsten eine Nummerierung innerhalb der Kapitel abgelöst, was eine Zuordnung auf einen Blick ermöglicht.

Die Benennung der Kapitel 6 und 7 wurde textuell angepasst, so dass sie deren Anforderungs-Inhalt bzw. -Intention besser widerspiegeln.

ausmaß und wesentliche inhalte der änderungen im überblick

erhebliche anpassunsbedarfe für die institute

Die Ergänzungen/ Änderungen der BAIT ziehen insgesamt einen erheblichen Handlungsbedarf in den Banken nach sich. Dieser Handlungsbedarf entspringt den neuen bzw. geänderten Kapiteln in unterschiedlichem Ausmaß und ist abhängig von der individuellen „Absprunghöhe“ des Hauses. Insbesondere für kleine und mittlere Institute ist die Beachtung bzw. Ausgestaltung der Proportionalität in der Erfüllung der Anforderungen ein zentrales Thema.

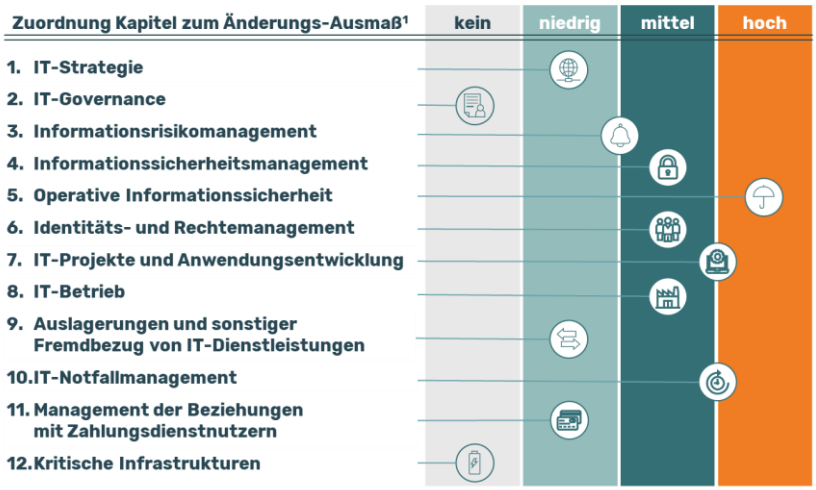

Abb. 2: Ausmaß der Änderungen im Überblick

die wichtigsten änderungen im überblick

it-strategie

Aussagen zu Zielen der Informationssicherheit sowie zu Schulungs- und Sensibilisierungsmaßnahmen zur Informationssicherheit

informationsrisikomanagement

Nachvollziehbarkeit SBA; Steuerbarkeit Informations-risiken in Verbindung zum OpRisk; Kompetenzge-rechte Genehmigung; Aktive Information über interne und externe Bedrohungen; Transparenz und Reichweite des Informationsverbundes

informationssicherheitsmanagement

Eingang physische Sicherheit in IS-Vorgaben; Operabilität von Ereignisdefinitionen; Vorgabe von Schutzmaßnahmentests; IS-Schulungen und Sensibilisierungsmaßnahmen

operative informationssicherheit

Zusammenhang mit den Kapiteln 3. „IRM“ und 4. „ISM“ (2nd LoD) - Abgrenzung der entsprechenden Aufgaben der 1st LoD; Identifikation und Bewertung sicherheitsrelevanter Ereignisse und Reaktion (SOC/ SIEM); Risikoorientierte Prüfung der Wirksamkeit von Sicherheitsmaßnahmen

identitäts- und rechtemanagement

Anwendungsübergreifende Vergabe und Überwachung von Berechtigungen auf jeder Systemebene; Besondere Aufmerksamkeit bei privilegierten Nutzern (PAM)

it-projekte & anwendungsentwicklung

Berücksichtigung der Informationssicherheit im gesamten Lebenszyklus aller Arten von Anwendungen und IT-Projekten; Testen der Maßnahmen zum Schutz der Informationen in der Entwicklung

it-betrieb

Etablierung Leistungs- und Kapazitätsmanagement; Erweiterung Bestandsangaben in einer CMDB um obligatorische Inhalte

auslagerungen & sonst. fremdbezug

Prüfung und Eingang von Vorgaben zum IT-Betrieb in Vereinbarungen/ Verträge zum sonstigen Fremdbezug von IT-Dienstleistungen (Risikoanalyse)

it-notfallmanagement

Verschärfung der Vorsorge; Planung/ Maßnahmen bei IT-Notfällen; Verzahnung mit BCM; Systematische Gewährleistung der Wiederherstellbarkeit (Tests etc.) Test und Nachweis Beherrschbarkeit RZ-Ausfall

mgt. beziehungen zahlungsdienstnutzer

Aktive Unterstützung und Beratung der Zahlungsdienstnutzer zu sicherheitsrelevanten Risiken bei Zahlungsdiensten; Maßnahmen und Kommunikationsprozesse

delta erkennen - zeit zu handeln

Mit der veröffentlichten, novellierten BAIT besteht die aufsichtliche Erwartung, daß die Vorgaben umgesetzt sind. Bei eventuellen Lücken ist die verbleibende Zeit für die Banken eng bemessen. Inwiefern Ihr Haus konkreten Handlungsbedarf aufweist, können Sie in einem ersten Schritt mit unseren BAIT Delta-Self Assessment ermitteln: Falls Sie eine der Fragen nicht eindeutig mit „Ja“ beantworten können, ist eine tiefergehende Analyse angeraten.

bait delta-self assessment – auszug aus dem anforderungskatalog

Ausgewählte Fragestellungen der BAIT	ja	tlw.	nein	?
1. IT-Strategie				
Ist die IT-Strategie auf die Ziele der Informationssicherheit ausgerichtet und führt sie sonstige wichtige Abhängigkeiten von Dritten auf? Enthält die IT-Strategie Aussagen zu Schulungs- und Sensibilisierungsmaßnahmen zur Informationssicherheit?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
3. Informationsrisikomanagement				
Sind die Schutzbedarfsfeststellungen nachvollziehbar dokumentiert und werden sie durch das IRM überprüft? Werden Risikoanalysen (Maßnahmen Soll-Ist) durchgeführt, die Ergebnisse kompetenzgerecht genehmigt und in OpRisk überführt?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
4. Informationssicherheitsmanagement				
Existieren Richtlinien zur physischen Sicherheit und zum Testen/ Überprüfen der Maßnahmen zum Schutz der Informationssicherheit? Ist ein kontinuierliches Sensibilisierungs- & Schulungsprogramm zur Informationssicherheit (inkl. Erfolgsüberprüfung) vorhanden?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
5. Operative Informationssicherheit				
Ist eine zentrale Speicherung potenziell sicherheitsrelevanter Informationen vorhanden? Existiert ein Verfahren zur zeitnahen regelbasierten Identifizierung und Bewertung von Bedrohungen mit zeitnaher Reaktion (SIEM/SOC)? Sind die operative IT-Sicherheit und das ISM gemäß dem 3 LoD Modell getrennt aufgestellt und die Verantwortlichkeiten klar definiert?	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
6. Identitäts- und Rechtemanagement				
Bestehen Berechtigungskonzepte auf allen Ebenen der IT-Systeme und sind SoD auch berechtigungskonzeptübergreifend gewährleistet? Sind Protokollierungs- & Überwachungsmaßnahmen der Berechtigungsverwendung, insbesondere für Aktivitäten mit privilegierten (besonders kritischen) Benutzer- und Zutrittsrechten, etabliert?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
7. IT-Projekte und Anwendungsentwicklung				
Sind Maßnahmen/ Vorgaben definiert, welche die Integrität der Anwendung (insbesondere des Quellcodes) angemessen sicherstellen? Werden die Maßnahmen zum Schutz der Informationen (z.B. via Penetrationstests) im Rahmen der Entwicklung systematisch getestet?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
8. IT-Betrieb				
Wird der aktuelle Leistungs- & Kapazitätsbedarf der IT-Systeme erhoben, zukünftiger abgeschätzt, geplant und überwacht? Sind die obligatorischen Bestandsangaben zu den Komponenten der IT-Systeme vollständig (und aktuell)?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen				
Wird geprüft, ob Vorgaben des IT-Betriebs in Vereinbarungen/ Verträge zum sonst. Fremdbezug von IT-Dienstleistungen eingehen müssen?	☐	☐	☐	☐
10. IT-Notfallmanagement				
Ist das IT-Notfallmanagement mit dem BCM (und auch IRM/ ISM) hinsichtlich der Ziele und Inhalte verzahnt? Sind Notfallpläne für alle IT-Systeme, welche zeitkritische Aktivitäten und Prozesse unterstützen, vorhanden, aktuell und werden sie regelmäßig auf Wirksamkeit überprüft (Notfalltests)? Ist die Bedienbarkeit zeitkritischer Aktivitäten und Prozesse bei Komplettausfall des Rechenzentrums nachweislich gegeben?	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐
11. Management der Beziehungen mit Zahlungsdienstnutzern				
Sind Prozesse eingerichtet, durch die das Bewußtsein der Zahlungsdienstnutzer zu sicherheitsrelevanten Risiken in Bezug auf die Zahlungsdienste verbessert werden können? Werden die Prozesse an die spezifische, aktuelle Risiko- und Bedrohungslage angepaßt?	☐ ☐	☐ ☐	☐ ☐	☐ ☐

Abb. 3: Ausgewählte Fragestellungen der BAIT

unser angebot - der bait delta-check

plenum führt seit vielen Jahren sehr erfolgreich regulatorische Projekte für die IT von Banken und Versicherungen durch. Die hier gewonnenen Erkenntnisse über die Prüfungspraxis der Aufsicht kombinieren wir für Sie zu einem „BAIT Delta-Check“, der Ihnen in kurzer Zeit Ihre individuellen Handlungsbedarfe aufzeigt. Als Partner der IT betrachten wir die IT und ihre Risiken hierbei „end-to-end“ entlang der Leistungsprozesse und gehen den Risikoursachen sorgfältig auf den Grund. Denn unser Auftrag endet nicht damit, die IT „durchzuprüfen”, sondern beginnt damit erst. Mit einem kompakten und ressourcenschonenden Vorgehen bieten wir Ihnen eine Standortbestimmung innerhalb weniger Wochen. Neben den Schwachstellen Ihrer IT aus Sicht der novellierten Teile der BAIT zeigen wir Ihnen hierin auf, mit welchen Sofortmaßnahmen Sie Ihre Compliance kurzfristig steigern können. Der wichtigste Mehrwert in unserem Vorgehen liegt jedoch darin, dass wir auf Basis unserer mehr als 25 Jahre Erfahrung mit Ihnen zukunftsorientierte Maßnahmen erarbeiten, die für eine angemessene & nachhaltige Compliance sorgen – damit Sie sich wieder voll auf Ihr Kerngeschäft konzentrieren können.

plenum AG
Management Consulting
THE SQUAIRE WEST 15 | Am Flughafen | D-60549 Frankfurt am Main
Telefon: +49 69 6435524-0 | Fax: +49 69 6435524-60 | Internet: www.plenum.de
Stand:
02.09.2021