MaRisk-Compliance

BAIT 2.0 – Umsetzung ohne Übergangsfrist

Wie die MaRisk-Novelle ist auch die neue Fassung der BAIT am 16. August 2021 in Kraft getreten. Da aus Sicht der BaFin lediglich bestehende Vorgaben konkretisiert werden, gibt es keine Übergangsfristen.

Die Konkretisierungen in den neuen Bankaufsichtlichen Anforderungen an die IT (BAIT) beziehen sich auf bestehende Vorgaben gemäß § 25a Abs. 1 und § 25b des KWG.

Im November 2017 wurden die BAIT erstmalig veröffentlicht. Die Entwicklung der letzten Jahre begründet jedoch einen erheblichen Bedeutungszuwachs der Informationssicherheit und damit auch der BAIT.

Die Novellierung ist unter anderem auch als Reaktion auf die Anpassung bzw. Digitalisierung von Arbeitsabläufen in der Pandemie zu sehen. Aus der Not heraus geboren, haben sich zwischenzeitlich eine Reihe von digitalisierten Prozessen bewährt. Es ist davon auszugehen, dass sich diese Entwicklung fortsetzen wird. Allerdings wird auch deutlich, dass es im operativen Umgang – sowohl mit der Informationssicherheit als auch mit den technischen Verfahren – einen Anpassungsbedarf gibt: Erklärtes Ziel ist, die Schere zwischen technischem Nutzen und technischen Risiken nicht auseinanderdriften zu lassen.

IT-Sicherheit

In diesem Zusammenhang stellt die BaFin klar, dass die fortlaufende Beachtung der Informationssicherheit und deren Einhaltung auf Basis angemessener und wirksamer Sicherungsmaßnahmen künftig deutlicher von der Aufgabe der Identifikation und Steuerung der mit den digitalen Prozessen einhergehenden Informationssicherheitsrisiken abzugrenzen ist. Dies mündet darin, dass in den BAIT ein völlig neues Kapitel zur operativen IT-Sicherheit aufgenommen wurde. Aus Sicht der Behörde mag dies nur eine Konkretisierung bestehender Vorgaben sein. Operativ bedeutet dies allerdings die Notwendigkeit, sich mit allen Verfahren und Prozessen innerhalb des Hauses auseinanderzusetzen und dabei auch potenzielle Interessenkonflikte im Auge zu behalten.

Die Häuser müssen sich zwangsläufig mit den Fragen beschäftigen, inwieweit Leit- und Richtlinien zum Informationsrisikomanagement und zur Informationssicherheit, aber auch der Umgang mit IT-Projekten und den Anwendungsentwicklungen den überarbeiteten Anforderungen der BAIT gerecht werden. Insbesondere ist zu prüfen, inwieweit die verantwortlichen Mitarbeiter*innen und Strukturen der Häuser hierfür operativ angemessen ausgestattet bzw. ausgelegt sind. Das beginnt bei der Prüfung und Anpassung bestehender Arbeitsanweisungen, setzt sich fort in der Prüfung aktueller Rollen, Verantwortlichkeiten und Dokumentationen und endet in der Aktualisierung des SOIT. Dabei kann der erforderliche Anpassungsbedarf in den Häusern je nach aktueller Organisationslage durchaus unterschiedlich ausfallen.

In der Summe lässt sich aber jetzt schon sagen, dass im Rahmen eines Analyseprozesses der Vorstand, diverse Fachabteilungen, die IT-Organisation, der Notfallbeauftragte und der Informationssicherheitsbeauftragte gefordert sein werden. Diese breite Auffächerung verdeutlicht ein wesentliches operatives Ziel der Novelle:

Die Wahrung der Informationssicherheit ist nicht und kann nie die Aufgabe von einzelnen Mitarbeiter*innen oder Beauftragten sein. Informationssicherheit impliziert vielmehr

- Leitplanken und Vorgaben (Vorstand),
- die Bereitstellung angemessener Mittel und Ressourcen (Vorstand),
- klare Arbeitsanweisungen (Orga),
- eindeutige Verantwortlichkeiten (Vorstand und Orga),
- Umsetzung und Beachtung in den operativen Einheiten sowie
- die fortlaufende Analyse, Steuerung und Beratung der jeweiligen Facheinheiten durch den Informationssicherheitsbeauftragten (ISB).

>

AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter
Geschäftsführung,
E-Mail: andreas.marbeiter@dz-cp.de

Operative Informationssicherheit

Damit unterstreicht die Aufsicht einmal mehr ihr Verständnis der drei Verteidigungslinien. Die operativen Einheiten stehen als „first line of defense" nun mal an vorderster Front und „verantworten" damit die meisten Einfallstore zur Gefährdung der Informationssicherheit.

In diesem Zusammenhang ist auch die Hervorhebung der Bedeutung der Informationseigentümer zu sehen, die sich aus dem neu geschaffenen Kapitel 3 der BAIT – operative Informationssicherheit – ergibt. Die interessenkonfliktfreie Trennung von operativem Handeln einerseits und unterstützender Beratung, Risikoanalyse und -steuerung andererseits verdeutlicht die Erfordernis eines Zusammenwirkens von Fachabteilungen und den dortigen Informationseigentümern mit dem Informationssicherheitsbeauftragten als verantwortlichem Kollegen der „second line of defense". Klare Schnittstellendefinitionen vereinfachen dabei nicht nur die Allokation durchzuführender Tätigkeiten. Sie ermöglichen dem Vorstand darüber hinaus einen transparenten Überblick über erforderliche Ressourcen und Kosten, die den jeweiligen Rollenprofilen innewohnen.

IT-Governance

Ein weiterer wichtiger, operativer Aspekt ist die Rolle der internen Kontrollsysteme (IKS) aus Kapitel 2 der BAIT – IT-Governance. Die Einbindung der ordnungsgemäßen Aufgabenwahrnehmung in das IKS der Bank ist auch hier der wesentliche Faktor.

Wir haben dieser Entwicklung bereits Rechnung getragen und stellen unseren Auslagerungsmandaten seit letztem Jahr zur Bestätigung unserer ordnungsgemäßen Aufgabenwahrnehmung ein Testat nach IDW PS 951 Typ II zur Verfügung. Dieses kann ohne weiteren eigenen Aufwand in die Kontrolldokumentation des eigenen Hauses übernommen und dem Prüfer zur Verfügung gestellt werden.

Schlussendlich thematisieren die neuen BAIT das (IT-)Notfallmanagement. Unserer Einschätzung zufolge gibt es nicht unerhebliche Synergien mit den im Informationssicherheitsprozess definierten Sicherungsmaßnahmen. Insbesondere die Einschätzungen zu Verfügbarkeitsbedarf und Zeitkritikalität können als Basis genutzt werden. Dennoch wird es auch in diesem Segment nicht ohne detaillierte Analyse und ggf. Anpassung bestehender Systeme und Prozesse gehen.

Detaillierte Informationen auf unserer Homepage

Auf unserer Homepage unter www.dz-cp.de/bait können Sie auszugsweise einige wesentliche Änderungen und daraus resultierende Handlungserfordernisse für Ihr Haus in tabellarischer Form herunterladen. Die detaillierten Analysen und Maßnahmenempfehlungen sprechen wir mit unseren Auslagerungsmandaten in den nächsten Wochen systematisch durch.

Auch wenn die BAIT viel enthalten, was in den Häusern bereits heute so durchgeführt wird, haben sich neue Schwerpunkte – insbesondere im Bereich der Einbindung der Informationseigentümer in der Bank, der operativen Informationssicherheit sowie des IT-Notfallmanagements – ergeben. ▬

Einen ersten, tabellarischen Überblick der wesentlichen Änderungen und daraus resultierenden Handlungsempfehlungen finden Sie unter www.dz-cp.de/bait