CORE®

BANKAUFSICHTLICHE ANFORDERUNGEN AN DIE IT (BAIT) DER BAFIN MIT VERÖFFENT-LICHUNG IN KRAFT GETRETEN

Christian Everts
Holger Friedrich
Dr. Waldemar Grudzien

November 2017
COREtechmonitor | Blogpost

Key Facts

- BAIT am 6. November 2017 in Kraft getreten, geringe Änderungen gegenüber Konsultationsstand Juni 2017
- Prinzipienorientierung und Proportionalitätsprinzip analog MaRisk, MaComp und MaSan
- Flexibilität für mögliche Änderungen durch modularen Aufbau
- Stärkung der Funktion des Informationssicherheitsbeauftragten
- Prüfung der Integration eines Moduls KRITIS in BAIT durch BSI und BaFin laufend, BAIT mit hoher Wahrscheinlichkeit Muster für Erarbeitung VAIT

Report

Übersicht BAIT

Wie die Mindestanforderungen an das Risikomanagement der Banken (MaRisk), deren neueste Fassung die BaFin Ende Oktober veröffentlicht hat, interpretieren auch die BAIT die gesetzlichen Anforderungen des § 25a Absatz 1 Satz 3 Nr. 4 und 5 Kreditwesengesetz (KWG). Die BAIT dient als aufsichtsrechtliche Erläuterung einer angemessenen technisch-organisatorischen Ausstattung der IT-Systeme unter besonderer Berücksichtigung der Anforderungen an die Informationssicherheit sowie an ein angemessenes Notfallkonzept. In Bezug auf den wachsenden Anteil von IT-Dienstleistungen Dritter, insbesondere im Rahmen von fachlichen Auslagerungen, dient die BAIT zudem der Konkretisierung der Anforderungen aus § 25b KWG.

Durch die BAIT macht die BaFin ihre Erwartungshaltung an gute Aufsicht den Instituten transparent. Zur Wahrung des Proportionalitätsprinzips – Rücksicht auf die unterschiedlichen Risikosituationen von Banken durch z.B. Größe, Geschäftsmodell und Risikoappetit – sind die Anforderungen prinzipienorientiert formuliert. Somit wird auch weiterhin Technologieneutralität gewahrt (das Ziel wird vorgegeben, nicht der Weg): Institute müssen „gängige Standards“ beachten und den Stand der Technik „berücksichtigen“.

Durch die modulare Struktur der BAIT wird die notwendige Flexibilität für künftig erforderliche Anpassungen oder Ergänzungen der Anforderungen sichergestellt; ein IT-Regelungsrahmen ist per se nicht abschließender Natur. Derzeit werden beispielsweise Anpassungen in Hinblick auf die Umsetzung der „G7 - Fundamental Elements of Cybersecurity“ geprüft. Des Weiteren wird in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gegenwärtig eruiert, ein spezielles Modul „Kritische Infrastrukturen“ (KRITIS) zu erarbeiten und in die BAIT zu überführen. Dieses Modul soll ausschließlich für die KRITIS-Betreiber des Sektors Finanz- und Versicherungswesen im Sinne des § 2 Abs. 10 BSI-Gesetz die notwendigen Anforderungen beinhalten, um den einschlägigen Vorgaben des BSI-Gesetzes nachzukommen.

Abbildung 1: BAIT verfügt über 8 Module

Einzelthemen

Stärkung der Funktion des Informationssicherheitsbeauftragten

Mit der BAIT erfolgt eine deutliche Stärkung der Funktion des Informationssicherheitsbeauftragten, der nunmehr endgültig auf eine Ebene mit den Risikofunktionen der 2nd Line gestellt wird.

Entsprechend konkretisiert die BaFin auch die Anforderungen an eine Auslagerung des Informationssicherheitsbeauftragen, der zukünftig nur in speziellen Gruppen- oder Verbandsstrukturen bzw. bei kleinen Instituten ohne wesentliche eigene IT-Infrastruktur auslagerungsfähig ist, wobei für diese Fälle innerhalb des Instituts immer ein zuständiger Ansprechpartner zu benennen ist.

Bewertung Integration eines KRITIS-Moduls

Aus Sicht der Autoren enthält die BAIT alle wesentlichen IT-Sicherheitsanforderungen an Banken und bietet durch Proportionalitätsprinzip, Prinzipienorientierung und nicht zuletzt den modularen Aufbau die notwendige strukturelle Flexibilität für zukünftige Anpassungen. Es bedarf unseres Erachtens keiner weiteren Anforderungen eines KRITIS-Moduls, das neben der Konkretisierung der Anforderungen aus der MaRisk auch das IT-Sicherheitsgesetz (IT-SiG) in die BAIT überführt.

Zudem würde sich die Zusammenführung aufgrund der Differenzen schwierig gestalten. Das IT-SiG stellt zwei zentrale Forderungen: Erreichen eines Mindestsicherheitsstan-

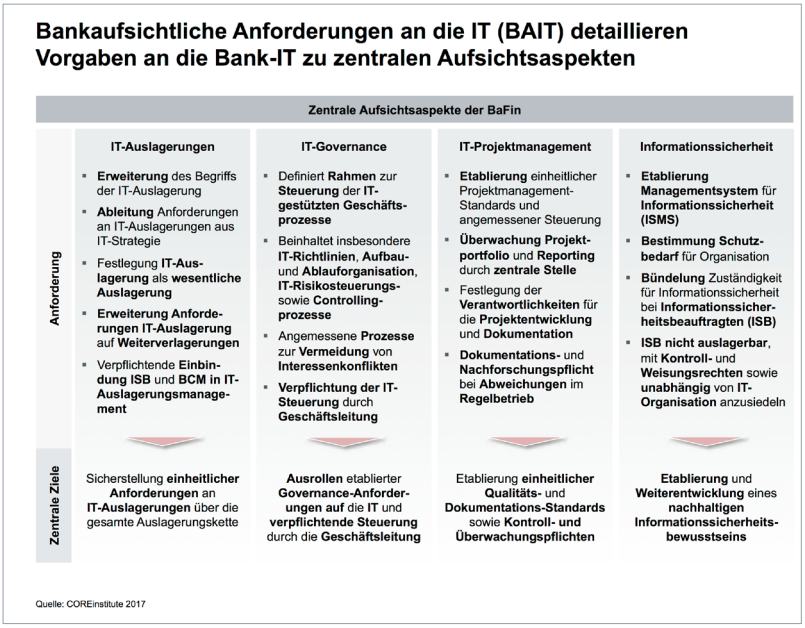

Abbildung 2: Zentrale Aufsichtsaspekte der BAIT

dards und Meldung schwerwiegender IT-Sicherheitsvorfälle. Es adressiert allgemein Betreiber kritischer Infrastrukturen, d.h. eine größere Gruppe als Finanzinstitute, und definiert starre Schwellwerte: Betreiber, die diese Schwellwerte überschreiten, fallen unter das Gesetz. Dagegen schreibt die BAIT durch die 8 Module und die allgemeine Berücksichtigung des Stands der Technik einen Mindestsicherheitsstandard vor; zudem beinhaltet sie kein Meldewesen, da dieses im Bankwesen bereits durch MaSI und die sie ablösende PSD II geregelt wird.

Da die BAIT für Banken gilt, das IT-SiG aber Betreiber von als kritisch identifizierten Infrastrukturen betrifft, stellt sich die Frage, wie diese beiden Regulierungskonzepte in einem KRITIS-Modul der BAIT vereinigt werden sollen und wie die praktische Ausgestaltung aussehen soll. Gerät gar eine im Sinne des IT-SiG nicht kritische Bank im Sinne der für alle Banken gültigen BAIT in den Genuss der Regulierung im Geiste des IT-SiG durch die BAIT-Hintertür?

Wie werden die unterschiedlichen Schwellenregime nach BAIT (Proportionalität) und KRITIS-Verordnung (starre Schwellwerte) kombiniert? Bedenkt man die siebenjährige Entwicklung des IT-SiG inklusive eines branchenspezifischen Sicherheitsstandards (B3S), dann kann bereits mit diesen ersten Fragen ermessen werden, wie lange sich eine Entwicklung und Implementierung des KRITIS-Moduls hinziehen könnte. Für alle Marktakteure sind zwei stabile Regulierungsrahmen in Form der BAIT und des IT-SiG besser als der Versuch einer Vereinigung beider Regulierungskonzepte in einem BAIT-Modul.

Hier ist eine starke politische Einflussnahme der beteiligten Stakeholder BMI (für BSI) und BMF (für BaFin) zu vermuten. Fachlichkeit und Technikbewertung treten zurück, politische Regulierungskosten steigen.

Einschätzung zum Modellcharakter der BAIT für die VAIT

Die BaFin hat in Q4/2017 – ebenfalls im bewährten Format eines Fachgremiums – mit der Entwicklung der VAIT (Versicherungsaufsichtliche Anforderungen an die IT) begonnen.

Schon im Sinne einer Gleichbehandlung muss die BaFin die Anforderungen an Banken auf Versicherungsunternehmen übertragen. Zudem beruht das Geschäftsmodell beider auf der Erfassung und Verarbeitung sensibler Daten, die demzufolge durch Banken wie Versicherungsunternehmen sicher gehandhabt werden müssen. Vor dem Hintergrund der Banken-Regulierungskette aus KWG (§25a) – MaRisk – BAIT ergibt sich für Versicherungssäule die Regulierungskette VAG (§23 Abs. 1) – MaGo – VAIT. Berücksichtigt man zudem, dass die MaGo (Aufsichtsrechtliche Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen) das Thema IT deutlich weniger behandeln als die MaRisk, kann umgekehrt geschlossen werden, dass die VAIT (noch) mehr als die BAIT Aussagen zu IT enthalten dürfte. Mit dem Fragebogen „Fragen zum Umgang mit Cyberrisiken“, den alle Versicherungsunternehmen bis zum 3. November beantworten mussten, verschafft sich die BaFin einerseits einen Überblick über Ausstattung und Fähigkeiten der Versicherungs-IT zur Informationssicherheit; andererseits schließt sie damit das Delta zwischen MaGo und MaRisk.

Insofern kann erstens davon ausgegangen werden, dass die VAIT die Struktur der BAIT bestehend aus acht Anforderungsmodulen übernehmen wird, und zweitens, dass sie gegenüber der BAIT deutlich mehr IT-Inhalt umfassen wird. Die Übertragung des hohen Aufsichtsstandards der Banken-IT auf die IT der Versicherungsunternehmen ist mithin bereits initiiert. Damit wird auch die Bedeutung der Versicherungsindustrie als auf IT basierender Branche und der damit einhergehenden Relevanz der Versicherungsunternehmen als Wirtschaftsfaktor gewürdigt.

FAZIT

Die Konsultation der BAIT hat wie die Konsultation der MaRisk-Novelle etwa anderthalb Jahre gedauert. Dieses Maß spiegelt den mittlerweile hohen Komplexitätsgrad der Regulierung wider und scheint sich als „Standardwert“ guter Regulierung zu etablieren. Immerhin kann so ein ausgereiftes und im Markt belastbares Regulierungswerk unterstellt werden.

Die final veröffentlichte Fassung der BAIT ist uneingeschränkt zu begrüßen. Zwar wäre eine Konkretisierung der regulatorischen Vorgaben hinsichtlich Cloud-Services wünschenswert gewesen; und auch die gemeinsame Prüfung von BSI und BaFin zur Integration eines KRITIS-Moduls in die BAIT sollte unseres Erachtens beendet werden, da die Redundanz und Vermengung unterschiedlicher Regelungsregime nicht zu einer besseren Regulierung und Aufsicht führen werden. Aber dies schmälert nicht die Güte der Struktur – und der strukturellen Offenheit – sowie der Inhalte. So hat der Regulator mit der BAIT zugleich ein Muster für die VAIT geschaffen und darüber hinaus für sämtliche Aufsichtssparten und -objekte der BaFin.

Quellen

INTERNET:

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1710_BAIT_anschreiben.html

VORAUSGEHENDE POSTS DER SERIE

COREinstitute 2016/2017

https://www.coretechmonitor.com/de/marisk-novelle-der-bafin-final-veroeffentlicht/

https://www.coretechmonitor.com/de/schwerpunkte-der-aufsicht-und-pruefung-der-bank-it-informationsveranstaltung-it-aufsicht-der-bafin/

https://www.coretechmonitor.com/de/it-sicherheitsgesetz-neue-anforderungen-an-kritische-betreiber/

ZEITUNG:

BÖRSEN-ZEITUNG 28.09.2017 „“REGTECH“ BESCHÄFTIGT AUFSICHT“

Autoren

Christian Everts

Christian Everts ist Transformation Manager bei CORE und bringt insbesondere seine Erfahrungen im Bereich Regulatorik bei CORE ein. Vor seiner Tätigkeit bei CORE war Christian bei verschiedenen Banken als Compliance Manager tätig, wo er vorrangig regulatorische Anforderungen in deutschen und internationalen Investment- und Universalbanken implementierte.

Mail: christian.everts@core.se

Holger Friedrich

Holger Friedrich verantwortet seit 2010 die Beratungseinheit von CORE. Er ist seit über 25 Jahren in der Softwareindustrie tätig. Vor der Gründung von CORE hat er ein Technologieunternehmen aufgebaut, wirkte in leitender Position bei marktführenden Technologieanbietern und war u.a. Partner in einer führenden internationalen Strategieberatung.

Mail: holger.friedrich@core.se

Dr. Waldemar Grudzien

Dr. Waldemar Grudzien setzt sich als Transformation Engineer mit den aktuellen regulatorischen Anforderungen und deren technischer Realisierung auseinander. Als promovierter Elektrotechniker war er als Leiter in einem nationalen Bankenverband für die Bereiche Retailbanking und Banktechnologien zuständig.

Mail: waldemar.grudzien@core.se

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae