Informationssicherheit

BAIT und SOIT: 2 x 4 Buchstaben mit großer Wirkung

Die **Bankaufsichtlichen Anforderungen an die IT (BAIT)** konkretisieren die spezifischen Anforderungen mit Bezug zur IT (MaRisk AT 7.2 „Technisch-organisatorische Ausstattung"). Der Konsultationsentwurf wurde zwischenzeitlich veröffentlicht. Die finale Veröffentlichung wird im Laufe des Jahres 2017 erwartet.

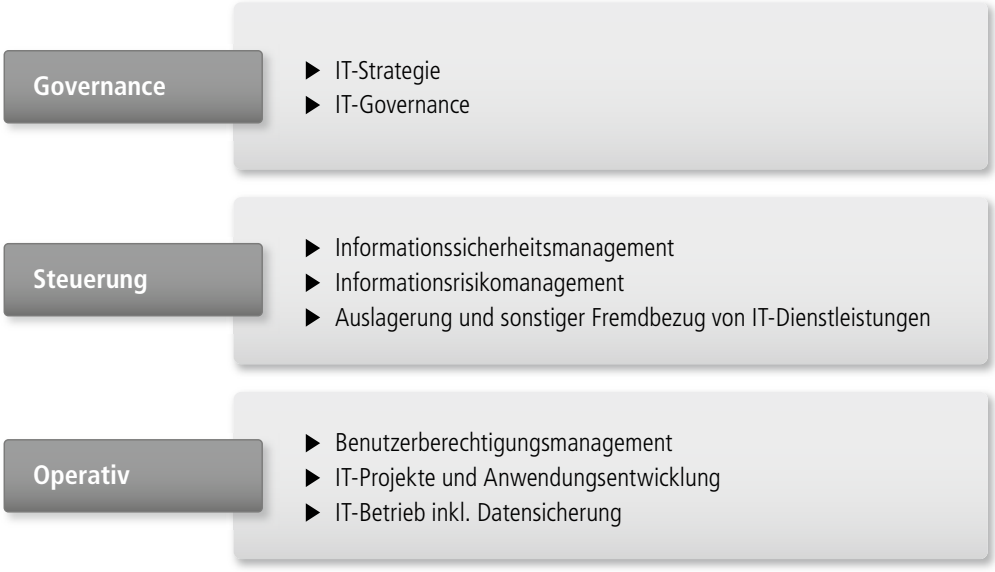
Schwerpunkte sind u. a. die IT-Strategie, das IT-Risikomanagement, das Informationssicherheitsmanagement und das Benutzerberechtigungsmanagement sowie IT-Dienstleistungen (siehe Abb. 1).

Die Hauptintention der BaFin ist es, die Risiken aus dem IT-Bereich stärker in den Mittelpunkt zu rücken. So liegt auch die Umsetzung der BAIT in der Verantwortung der Geschäftsleitung. Mit Risiken sind dabei nicht nur die Risiken aus der Vernetzung gemeint („Cyberrisiken"). Auch Mitarbeiter, Dienstleister oder ein technischer Ausfall von IT-Ketten können Auslöser von Störungen oder Unterbrechungen sein. Daraus ergibt sich auch der in der Abbildung 1 dargestellte Umfang der BAIT, der fast wie eine Checkliste aufgebaut ist.

Nahezu parallel löst der neue **Standard für Ordnungsmäßigkeit der IT-Verfahren (SOIT)** die bisherigen Handbücher in den Geschäftsgebieten der ehemaligen Fiducia IT AG (Handbuch Ordnungsmäßigkeitsfragen) und GAD eG (Ordnungsmäßigkeits-Handbuch GAD Bankverfahren) ab.

SOIT integriert wie seine Vorgänger viele gängige Standards. Er gliedert sich in drei Teile: Teil 1 befasst sich mit übergreifenden Themen von rechtlichen Rahmenbedingungen über organisatorische Gestaltung der IT-Organi-

Abb. 1 ÜBERSICHT BAIT NACH KONSULTATIONSENTWURF 02/2017



sation bis hin zu den verschiedenen Managementbereichen wie Informationssicherheit, Risikomanagement, Auslagerungsmanagement, Notfallmanagement und Kontrollsystemen. Die übrigen beiden Teile enthalten anwendungsspezifische Themen zu dem jeweiligen Kernbankenverfahren, wobei sich Teil 2 mit agree21 und Teil 3 mit bank21 auseinandersetzt.

Im Fiducia-Umfeld war der Vorgänger bereits Vertragsbestandteil zwischen Bank und IT-Dienstleister und somit verbindlich umzusetzen. Dies hat sich mit dem SOIT nicht geändert und gilt mit Migration von bank21 auf agree21 auch für die Banken aus dem Geschäftsgebiet der ehemaligen GAD eG.

Bei der Umsetzung des SOIT sind beide Hauptaspekte, Ordnungsmäßigkeit und Sicherheit, gleichermaßen zu beachten. Dies gilt insbesondere bei der Zuordnung von Verantwortlichkeiten. Der SOIT wird auch zur Beurteilung der Ordnungsmäßigkeit des Rechnungswesens sowie als Rahmenwerk für die Umsetzung der Aufgabenbereiche herangezogen. Das heißt, SOIT ist kein reines Informationssicherheitsthema, auch wenn dies eine gewichtige Rolle spielt. Entsprechend breit gefächert ist die Zielgruppe des SOIT: Sowohl der Vorstand und Führungskräfte als auch Mitarbeiter des Beauftragtenwesens, der Organisation, der Administration, des Rechnungswesens, des Risikomanagements und der IT-Revision nutzen den Standard.

Im Übrigen deuten aktuelle Erkenntnisse aus 44er-Prüfungen im IT-Bereich darauf hin, dass die Bankenaufsicht großen Wert auf die Einhaltung verbindlich vereinbarter Maßnahmen legt. Schließlich dienen die Maßnahmen als Nachweis für ein gemeinsames Sicherheitsniveau zwischen Bank und IT-Dienstleister.

Sie als Bank müssen sich sowohl mit dem neuen Standard – SOIT – als auch mit den neuen bankenaufsichtsrechtlichen Anforderungen – BAIT – auseinandersetzen. Der Aufwand ist dabei nicht zu unterschätzen.

Der Fragenkatalog in SOIT ist sehr umfangreich und bedarf der ständigen Überarbeitung bzw. Anpassung. Seitens des IT-Dienstleisters wird der SOIT inklusive des Fragenkatalogs als MS-Word-Dateien und als PDF-Dokumente zur Verfügung gestellt. Zur Bearbeitung der Fragen und Kontrolle des Umsetzungsstandes sind in der Regel zusätzliche administrative Aufwendungen erforderlich.

Diesen administrativen Aufwand können Sie mit Unterstützung der GenoTec einsparen. Der SOIT ist als Maßnahmenpaket in unsere Dienstleistung „Informationssicherheit kompakt“ integriert. Sie haben jederzeit und automatisch Zugriff auf die aktuellste Version.

Der SOIT ist durch unsere neue Lösung „Informationssicherheit kompakt“ optimal in das Informationssicherheitsmanagement eingebunden. Die Bank kann sich auf das Wesentliche konzentrieren, die Sicherheit und Ordnungsmäßigkeit sicherstellen und prüfungssicher dokumentieren.
Gleichzeitig sind selbstverständlich in unsere Lösungen – Auslagerung, dauerhafte Beratung, punktuelle Unterstützung – die neuen Anforderungen aus MaRisk bzw. BAIT vollumfänglich integriert. Sie als Bank sind in jeder Hinsicht (prüfungs) sicher und werden im hohen Maße von administrativen Tätigkeiten entlastet. ▬

Ansprechpartner: ***Michael Switalla,*** *Stv. Leiter IT-Sicherheit & Datenschutz, E-Mail: michael.switalla@geno-tec.de*
Marc Hübner, *Beauftragter IT-Sicherheit & Datenschutz, E-Mail: marc.huebner@geno-tec.de*