BAIT

INFORMATIONSSICHERHEIT
wird ab sofort großgeschrieben

Informationssicherheit rückt mit der MaRisk-Novelle und den BAIT in den aufsichtsrechtlichen Fokus. Banken müssen einen Informationssicherheitsbeauftragten benennen, der weitreichende Befugnisse hat, aber auch mit entsprechenden Kompetenzen und Ressourcen ausgestattet sein muss. Die Funktion ist grundsätzlich auslagerbar.

Die „Bankaufsichtlichen Anforderungen an die IT“ (BAIT vom 3. November 2017) konkretisieren die aufsichtsrechtlichen Erwartungen an die Informationssicherheit. Einleitend wird der Stellenwert der Informationssicherheit unterstrichen. Die Aufsicht setzt ihn mit der Kapitalausstattung der Institute gleich. Entsprechend hoch sind die Anforderungen an die Sorgfalt, Vollständigkeit, Transparenz und Nachvollziehbarkeit in diesem Bereich.

Die BAIT interpretieren unter besonderer Berücksichtigung der „Mindestanforderungen an das Risikomanagement“ (MaRisk vom 27. Oktober 2017) die Regelungen des § 25a S. 3 Nr. 4 u. 5 KWG. Sie sind ein Leitfaden für behördliches Handeln und bieten so eine verlässliche „Guideline“, wie die aufsichtsrechtliche Prüfungspraxis (künftig) gestaltet werden wird.

Die MaRisk („AT 7.2 Technisch-organisatorische Ausstattung“) haben die Tonalität bereits vorweggenommen: Zur Feststellung des Schutzbedarfes und Ableitung entsprechender Sicherheitsmaßnahmen sind entsprechende Risikosteuerungs- und Risikoüberwachungsprozesse einzurichten. Dies gilt sowohl für eigenentwickelte Software als auch für den Fremdbezug von Software. Insgesamt rückt das Informationssicherheitsmanagement damit näher an die anderen Beauftragtenthemen.

Auslagerbarkeit

Im Lichte des § 25b KWG räumt die Aufsicht in den BAIT regional tätigen, verbundangehörigen Instituten (z. B. Volksbanken Raiffeisenbanken) sowie kleinen, gruppenangehörigen Instituten (z. B. etwa kleine Privatbanken und kleine Auslandsbanken bei vergleichbarem Geschäftsmodell) weiterhin die Möglichkeit ein, den Informationssicherheitsbeauftragten auszulagern („… einen gemeinsamen Informationssicherheitsbeauftragten zu bestellen.“). Wichtig ist, dass in der Bank eine Steuerungskompetenz zur Wahrnehmung der Verantwortung verbleibt.

Dies ist sachgerecht, weil ohne die Auslagerungsoption die Komplexität der Materie in einer risikoorientierten Betrachtung zu unangemessen hohen Aufwänden in kleineren Häusern führen würde. Gleichzeitig kann dem Schutzzweck der Informationssicherheit unter dem Gesichtspunkt der Proportionalität durch die Vollauslagerung am besten Rechnung getragen werden. Die Auslagerungsoption sichert eine machbare, effektive und auch wirtschaftlich sinnvolle Alternative.

Sachgerecht ist aber auch der Verbleib der Verantwortung beim auslagernden Unternehmen: Weil es für die Banken heute entscheidend ist, jederzeit Transparenz über die ausgelagerten IT-Prozesse zu haben. Die BAIT-Anforderungen sind auch vor dem Hintergrund zu lesen, dass Banken zunehmend für ihre Geschäftstätigkeit wesentliche IT-Prozesse an Dienstleister beziehungsweise FinTech-Unternehmen auslagern. Um diese Auslagerungen zu steuern, erwartet die Aufsicht künftig ein zentrales Auslagerungsmanagement – auch und insbesondere mit Blick >

auf die IT. Es soll einen zeit- und ortsunabhängigen Überblick über ausgelagerte Prozesse vermitteln und die damit verbundenen Risiken einheitlich bewerten. Letztlich dient es der Wahrnehmung der unternehmerischen Verantwortung

Keine Umsetzungsfristen

Da die Aufsicht in den BAIT lediglich „Klarstellungen ohnehin schon vorhandener Anforderungen" sieht, gibt es keinerlei Umsetzungsfristen. Sie gelten ab sofort.

Durch die BAIT ergibt sich aber für einige Kreditinstitute ein nicht unerheblicher Anpassungsbedarf, der institutsspezifisch herauszuarbeiten ist. Insgesamt beschreibt die Aufsicht in acht Themenblöcken ihre Anforderungen: IT-Strategie, IT-Governance, Informationsrisikomanagement, Benutzerberechtigungsmanagement, IT-Projekte und Anwendungsentwicklung, IT-Betrieb sowie Auslagerungen (siehe auch nachfolgende Übersicht, S. 23).

Informationssicherheit

Erstmalig fordert die Aufsicht, die Funktion eines Informationssicherheitsbeauftragten einzurichten. Bislang leitete sich die Funktion nur indirekt, beispielsweise aus dem BSI-Grundschutzkatalog, ab. Der Informationssicherheitsbeauftragte arbeitet auf Grundlage einer Informationssicherheitsrichtlinie. Er ist mit entsprechenden Ressourcen auszustatten, wobei mögliche Interessenkonflikte zu vermeiden sind. Aufbauorganisatorisch ist er beispielsweise von IT-Betrieb oder IT-Weiterentwicklung zu trennen.

Sein Aufgabenkatalog ist umfassend. Zunächst berät er den Vorstand direkt in allen Belangen der Informationssicherheit (IT-Strategie). Er muss also Qualifikationen vorweisen können, die es ihm ermöglichen, Entscheidungen vorzubereiten. Den Kern seiner Tätigkeit bilden jedoch die IT-Governance und das Informationsrisikomanagement.

IT-Governance meint die Notwendigkeit, den IT-Betrieb und die Weiterentwicklung der IT-Systeme einschließlich

Abb. 1 CHECKLISTE ZUR UMSETZUNG DER BAIT

BAIT		MaRisk	Verantwortung in der Bank (Gesamtablauforga)	Umsetzungsschritt	Wer?	Anmerkungen
IT-Strategie	1.1	AT 4.2	Geschäftsverteilungsplan	Die IT-Strategie muss mit der Gesamtbankstrategie konsistent sein.		Sind Ziele sowie Maßnahmen zur Erreichung der Ziele zu definieren?
IT-Strategie	1.2.a	AT 4.2	Geschäftsverteilungsplan	Zu folgenden Punkten sollte in der IT-Strategie Position bezogen werden: Personaleinsatz und Budget, IT-Aufbau und IT-Ablauforganisation, strategische Einordnung der IT-Dienstleistung, Aussagen zu Auslagerungen.		Aussagen zur Auslagerung von IT-Dienstleistungen können sich in der Stellungnahme zur Auslagerung wiederfinden.

der dazugehörigen IT-Prozesse auf Basis der IT-Strategie zu steuern und zu überwachen – mit allem, was dazugehört. Das Informationsrisikomanagement referenziert dagegen auf die Daten- bzw. Informationsverarbeitung und Daten- bzw. Informationsweitergabe durch IT-Systeme. Hier muss die Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit der Daten sichergestellt werden. Haben Sie derzeit noch auf ein Informationssicherheitsteam gesetzt, so ist dies nunmehr in Richtung der Bennenung eines Informationssicherheitsbeauftragten weiter zu entwickeln.

Auf Prozess- bzw. Steuerungsebene rückt die Aufsicht die Informationssicherheit damit in die Nähe der anderen Beauftragtenthemen, wie der Betrugs- und Geldwäscheprävention oder auch der MaRisk- oder WpHG-Compliance. Der Gefährdungs- bzw. Schutzbedarfsanalyse folgen der Kontroll- bzw. Maßnahmenplan und die Umsetzung, begleitet von einem Monitoring, der Schulungs- und Sensibilisierungskampagnen sowie der Kommunikation der Arbeitsergebnisse.

Auf der operativen Ebene sind darüber hinaus das Benutzerberechtigungsmanagement, IT-Projekte und Anwendungsentwicklung sowie der IT-Betrieb inklusive Datensicherung gesetzt. Spannend ist insbesondere das Thema Fremdbezug von Software.

Fremdbezug von Software

Die MaRisk bemühen sich mit Blick auf den „Fremdbezug von Software“ um einen „pragmatischen“ Lösungsansatz und stellt klar, dass der Erwerb von Software an sich noch keine Auslagerung darstellt.

Aber: Alle Softwarelösungen, die

- zur Steuerung, Messung und Überwachung von Risiken eingesetzt werden sowie
- für die Wahrnehmung bankgeschäftlicher Aufgaben wesentlich sind,

fallen unter den Anwendungsbereich des AT 9, das heißt, sie sind wie wesentliche Auslagerungen zu behandeln. >

Wann?	Status	Bemerkung zur Regelung
	offen	
	offen	

Zusammenfassung Projektstatus/Aufgaben gesamt:	2
Anzahl nicht relevant:	0
Anzahl offen:	2
Anzahl begonnen:	0
Anzahl erledigt:	0

AUTOREN UND ANSPRECHPARTNER

Michael Switalla
Stv. Bereichsleiter IT-Sicherheit & Datenschutz,
E-Mail: michael.switalla@geno-tec.de

Sandra Sitter
Leiterin IT & Projekte
E-Mail: sandra.sitter@geno-tec.de

Was bedeutet dies für die genossenschaftlichen Institute?

Wichtig ist, dass bei Bezug der Software auf Lasten- und Pflichtenhefte geachtet wird und dass entsprechende Einführungsprojekte gestartet werden. Zudem sind die Regelungen zum IT-Betrieb, Patch- und Releasemanagement zu betrachten. Hier ist also nicht mehr nur die MaRisk AT 8.2 zu beachten, sondern auch der AT 9. Beim Fremdbezug von Software muss regelmäßig zumindest eine Risikobewertung anhand definierter Bewertungskriterien vorgenommen werden. Wenn der Fremdbezug eine wesentliche Auslagerung darstellt, muss diese darüber hinaus nach den Regeln, die für Auslagerungsmanagement gelten, bewertet und analysiert werden.

Bei den Produkten der Rechenzentralen ist die Bank in der Regel gut aufgestellt, wenn sie die Vorschläge des Standards für Ordnungsmäßigkeit der IT-Verfahren (SOIT) berücksichtigt. SOIT hat bereits viele der Anforderungen integriert. Er befasst sich sowohl mit den rechtlichen Rahmenbedingungen, der organisatorischen Gestaltung der IT und den verschiedenen Managementbereichen (Informationssicherheit, Risikomanagement, Auslagerungsmanagement, Notfallmanagement etc.) als auch mit anwendungsspezifischen Themen zum Kernbankenverfahren. Darüber hinaus integriert SOIT alle gängigen Standards.

Unterstützungsangebote

Mit Blick auf die GenoTec-Auslagerungsangebote Informationssicherheit und IT-Revision sind sämtliche Anforderungen aus den BAIT abgedeckt und in unsere Prozesse überführt. Als Bank bilden Sie die BAIT prüfungssicher und effizient ab. Im Rahmen unserer Auslagerungsdienstleistung überprüfen wir die BAIT-Konformität anhand einer Checkliste im Rahmen der jährlichen Prüfungsplanung kostenfrei. (Auf Wunsch kann die Überprüfung auch entgeltlich separat durchgeführt werden.)

Daneben bieten wir institutsindividuelle, punktuelle Unterstützungsleistungen an.

- Checkliste BAIT-Konformität: Diese Checkliste enthält alle Umsetzungsschritte aus der BAIT und fasst die Umsetzungsempfehlungen zusammen. Sie enthält eine Projektsteuerung und einen Vollständigkeitsabgleich. Damit erkennen Sie auf einen Blick Ihren Status quo in der Umsetzung der BAIT (siehe auch Abbildung 1).
- Unser Compliance-Management-System im Bereich der Informationssicherheit, ISI kompakt, ermöglicht schon heute eine MaRisk- und BAIT-konforme Umsetzung der Informationssicherheit. Alle Standards, so auch der SOIT, sind bereits vollumfänglich integriert. Das System unterstützt Sie in der Informationssicherheit: effektiv, transparent und sicher.
- Ergänzend stehen wir Ihnen gerne auch als Berater zur Verfügung: Sie haben den Zugriff auf unser Spezialistenwissen und die Erfahrungen aus über 120 Informationssicherheitsmandaten. ■

WICHTIGSTE UMSETZUNGSFELDER AUS DEN BAIT BZW. DEN MARISK

Thema/Zielsetzung	Handlungsempfehlung
IT-Strategie BAIT 1.1 – 1.2 MaRisk AT 4.2	– Mit der Gesamtbankstrategie konsistente IT-Strategie – Definition der Standards (BSI-Grundschutz, ISO, SOIT) – Beschreibung der Anwendungslandschaft insgesamt, des Notfallkonzepts etc.
IT-Governance BAIT 2.3 – 2.7 MaRisk AT 4.3.1, AT 4.3.2, AT 5, AT 7.1, AT 7.2	– Steuerung und Überwachung des IT-Betriebs sowie – Steuerung und Überwachung der IT-Weiterentwicklung auf Basis der IT-Strategie (Personalausstattung, technisch-organisatorische Ausstattung) – Ausstattung des Informationssicherheitsmanagements – Aufgabentrennung zwischen IT-Aufbau- und IT-Ablauforganisation – Festlegung quantitativer und qualitativer Steuerungs- und Überwachungskriterien etc.
Informationsrisikomanagement BAIT 3.8 – 3.14, 4.15 – 4.22 MaRisk AT 4.3.1, AT 7.2, BT 3.2	– Orientierung der IT-Systeme und IT-Prozesse an den Geschäftsaktivitäten und der Risikosituation – Sicherstellung von Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit – Einrichtung, Steuerung und Dokumentation eines kompetenzgerechten Risikomanagements – Dokumentation der geschäftsrelevanten Informationen, Geschäftsprozesse, IT-Systeme sowie der Netz- und Gebäudeinfrastruktur – Definition von Informationssicherheitsrichtlinien – Benennung eines Beauftragten, der u. a. Schutzbedarfe und Schutzziele dokumentiert, Informationssicherheitssvorfälle analysiert und regelmäßig an den Vorstand berichtet
Benutzerberechtigungsmanagement BAIT 5.23 – 5.30 MaRisk AT 4.3.1, AT 7.2, BTO TZ 9	– Kompetenz- und Berechtigungskonzept entsprechend den organisatorischen und fachlichen Vorgaben – Definition von Berechtigungsvergabeprozessen – Vermeidung von Interessenkonflikten – Einbeziehung von Kontrollinstanzen bei der Rezertifizierung – Nachvollziehbare Dokumentation
IT-Projekte, Anwendungsentwicklung BAIT 6.31 – 6.44 MaRisk AT 7.2, AT 8.2, AT 8.3	– Einbindung von Risikocontrolling, Compliance und Interne Revision sowie der involvierten Fachabteilungen – Durchführung von Auswirkungsanalysen und Tests – Organisationsanweisungen zur Behandlung von IT-Projekten inkl. Qualitätsmanagement – Anforderungsmanagement, Meilensteinplanungen, Projektmanagement – Regelmäßige Information des Vorstandes – Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten – Nachvollziehbare Dokumentation und regelmäßige Tests – Regelwerk für Eigenentwicklungen etc.
IT-Betrieb (inkl. Datensicherung) BAIT 7.45 – 7.51 MaRisk AT 7.2	– Regelmäßige Prüfung, ob IT-Betrieb mit den Anforderungen der IT-Strategie übereinstimmt – Administration und Aktualisierung der IT-Systeme – Risikoüberprüfung – Steuerung, Dokumentation, Bewertung von Prozessänderungen – Datensicherungskonzept etc.
Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen BAIT 8.52 – 8.56 MaRisk AT 9, AT 7.2	– Risikoanalysen, Änderungsbewertungen, Exit-Strategien, Dienstleisterüberwachung – Strategieabgleich etc.