Sparkasse Managermagazin

12. Februar 2018 - 07:00 | Bait

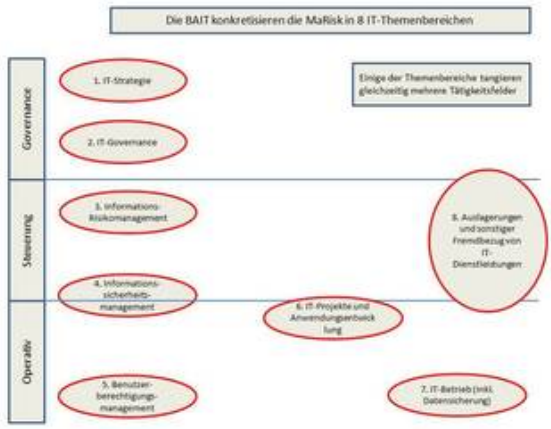
Neues Regelwerk dokumentiert die Aufsichtspraxis

Andreas Brugger, SIZ

Mit der Veröffentlichung der Bankaufsichtlichen Anforderungen an die IT (Bait) hat die Bafin im November 2017 die Mindestanforderungen an das Risikomanagement von Banken (MaRisk) hinsichtlich der Informationstechnologie konkretisiert.

Banken müssen sich auf Notfälle in ihren EDV-Systemen vorbereiten. Entsprechende Vorgaben sind Teil der Bankaufsichtlichen Anforderungen an die IT, die die Bafin im November 2017 in Kraft gesetzt hat. *(dpa)*

Wie die im Oktober 2017 veröffentlichten MaRisk interpretieren die Bait die Anforderungen aus dem Paragrafen 25a Absatz 1 des Kreditwesengesetzes (KWG). Die Bait regeln die Anforderungen an die Informationssicherheit, die technisch-organisatorische Ausstattung sowie an das Notfallmanagement von Banken. Da ein Großteil der Institute IT-Dienstleistungen von Dritten bezieht, konkretisieren sie darüber hinaus auch den Paragrafen 25b KWG, die in den MaRisk enthaltenen Anforderungen bleiben dabei unberührt. Nach Aussagen der Bafin adressieren die Bait darüber hinaus gehäuft aufgetretene Prüfungsfeststellungen. Die Anforderungen der Bait sind nach Regelungstiefe und -umfang nicht abschließend.



(SIZ)

Die Bait sind prinzipienorientiert formuliert, womit die Neutralität hinsichtlich der eingesetzten Technik ebenso gewahrt bleibt wie die Einhaltung des Proportionalitätsprinzips. Die Institute müssen entsprechend den Bait "den Stand der Technik berücksichtigen" sowie "gängige Standards" zur Informationssicherheit beachten, also sogenannte Best-Practice-Anforderungen berücksichtigen. Inhaltlich umfassen die Bait acht Kapitel beziehungsweise Themenbereiche. Die meisten der Themen sind in den gängigen Standards der Informationssicherheit bereits enthalten und auch aus dem bei allen Sparkassen eingesetzten Produkt Sicherer IT-Betrieb (SITB) des SIZ bekannt. Kurz zusammengefasst enthalten die in der Grafik dargestellten Kapitel folgende Anforderungen:

- **IT-Strategie:**
  Von der Geschäftsleitung wird eine nachhaltige IT-Strategie festgelegt, in der die Ziele sowie die Maßnahmen zu deren Erreichung dargestellt werden.
- **IT-Governance:**
  IT-Governance ist die Struktur zur Steuerung sowie Überwachung des Betriebs und der Weiterentwicklung der IT-Systeme einschließlich der zugehörigen IT-Prozesse auf Basis der IT-Strategie. Bei Änderungen von Aktivitäten und Prozessen sind die IT-Aufbau- und die IT-Ablauforganisation zeitnah anzupassen. Ebenso ist eine angemessene personelle Ausstattung erforderlich.
- **Informationsrisikomanagement:**
  Umfang und Qualität der Informationsverarbeitung ist insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie an der Risikosituation zu orientieren. Die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität der Daten sind sicherzustellen sowie angemessene Überwachungs- und Steuerungsprozesse einzurichten und diesbezügliche Berichtspflichten zu definieren Der SITB und andere gängige Standards subsummieren den Begriff Authentizität unter Integrität.
- **Informationssicherheitsmanagement (ISMS):**
  Durch das ISMS werden Vorgaben zur Informationssicherheit gemacht, Prozesse definiert und deren Umsetzung gesteuert. Darüber hinaus gibt es Berichtspflichten des InformationssicherheitsbBeauftragten an die Geschäftsleitung sowie einen festgelegten Turnus der Berichterstattung.
- **Benutzerberechtigungsmanagement:**
  Mittels des Benutzerberechtigungsmanagements wird sichergestellt, dass die eingerichteten Berechtigungen den organisatorischen und fachlichen Vorgaben des Instituts entsprechen.
- **IT-Projekte, Anwendungsentwicklung einschließlich Entwicklung in den Fachbereichen (IDV):**

Wesentliche Veränderungen in den IT-Systemen im Rahmen von IT-Projekten, deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse sind im Rahmen einer Auswirkungsanalyse zu bewerten.

- **IT-Betrieb einschließlich der Datensicherung:**
  Vom IT-Betrieb sind die Anforderungen aus der Geschäftsstrategie sowie aus den durch IT unterstützten Geschäftsprozessen umzusetzen.
- **Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen:**
  Bei Auslagerungen wie auch beim sonstigen Fremdbezug von IT-Dienstleistungen sind von den Instituten die allgemeinen Anforderungen an die Ordnungsmäßigkeit der Geschäftsorganisation zu beachten Bei jedem Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten.

Die Institute der Sparkassen-Finanzgruppe nutzen für ihr Informationssicherheitsmanagement den SITB. In der voraussichtlich ab März 2018 auch für die Sparkassen über die Finanz Informatik verfügbaren Version 16.0 sind die Anforderungen aus den Bait vollständig berücksichtigt. Bereits in der Version 15.0 wurde der SITB dahingehend umstrukturiert, dass Anforderungen an die Informationssicherheit und beschreibender Text deutlich voneinander getrennt wurden. In diesem Arbeitsschritt wurden mehr als 900 einzelne Anforderungen adressiert. Mit der Integration der Anforderungen aus den Bait in die Version 16.0 wurden 35 dieser Anforderungen präzisiert und fünf Anforderungen neu aufgenommen. Die Quote von weniger als einem Prozent der Anforderungen, die im Kontext Bait neu aufgenommen wurden, spricht für die Vollständigkeit und Qualität des SITB.

Im Kontext Informationssicherheit neu hinzugekommen sind folgende Anforderungen:

- Erstmals explizit in einem Dokument der Bafin wird die Bestellung eines Informationssicherheitsbeauftragten gefordert. Dieser muss zur Vermeidung von Interessenskonflikten organisatorisch und prozessual unabhängig ausgestaltet, also aufbauorganisatorisch von der IT und auch der Revision getrennt sein (Kap. II.4 Tz. 19 Bait).
- Die Funktion des Informationssicherheitsbeauftragten muss grundsätzlich im eigenen Haus vorgehalten werden (Kap. II.4 Tz. 20 Bait).
- Für bankfachliche oder rechnungslegungsrelevante IDV-Anwendungen muss ein zentrales Register geführt werden (Kap. II.6 Tz. 44 Bait). Darin sind unter anderem Name und Zweck der Anwendung, Versionierung, Datumsangabe etc. zu nennen. Im Kontext SITB bedeutet diese Anforderung, dass auch IDV-Anwendungen mit mindestens mittlerem Schutzbedarf in der Strukturanalyse als Anwendungen zu pflegen sind.
- Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung müssen definiert werden. Dabei sollte der Stand der Technik berücksichtigt werden (Kap. II.4 Tz. 17 Bait).
- IT-Projekte, deren Auswirkung auf die IT-Aufbau- und IT-Ablauforganisation sowie die dazugehörigen IT-Prozesse müssen angemessen gesteuert und die Projektrisiken im Risikomanagement berücksichtigt werden (Kap. II.6 Tz. 33, 34, 35 Bait). Dies betrifft auch Portfoliorisiken, also Risiken aufgrund von Abhängigkeiten verschiedener Projekte voneinander. Wesentliche IT-Projekte und IT-Projektrisiken müssen der Geschäftsleitung regelmäßig und anlassbezogen berichtet werden.
  Es ist zu beachten, dass mittelgroße und kleine Sparkassen kaum Projekte in dieser Größenordnung umsetzen und Häuser mit einem entsprechend großen Projektportfolio dies bereits auch in der Vergangenheit mit einem passenden Projektmanagement gesteuert haben. Daher ist diese Anforderung als neu im Kontext Informationssicherheit zu betrachten, sollte aber an anderer Stelle bereits implementiert sein.

Institute, die für ihr ISMS den Anforderungen des SITB bereits wirksam nachgekommen sind, sollten keine inhaltlichen Schwierigkeiten haben, das aus den Bait resultierende Delta zu schließen, wobei mit einem gewissen Umsetzungsaufwand zu rechnen ist. Gleiches gilt für die Themenbereiche IT-Steuerung und IT-Governance, die in der Regel außerhalb des ISMS angesiedelt sind.

Daneben haben sich einige bereits bestehende Anforderungen konkretisiert oder aber auch erweitert, das sind beispielsweise:

- Die Übersicht der für das ISM relevanten Unternehmenswerte muss enthalten: Geschäftsrelevante Informationen, Prozesse, Anwendungen, IT-Systeme, Vertragspartner/Verträge, Netzwerke/Kommunikationsverbindungen und Räume (Kap. II.3 Tz. 10 Bait). Hier sind die Prozesse neu hinzugekommen, das bedeutet, dass der der Reiter "Prozesse" in der Strukturanalyse ist erstmalig verpflichtend auszufüllen ist.
- Die Unternehmensführung muss gemäß BT 3.2 Tz. 6, 7 MaRisk mindestens jährlich, gemäß Kap. II.4 Tz. 22 Bait mindestens vierteljährlich und bei Bedarf über den Status und Tendenzen in der Informationssicherheit sowie gemäß Kap. II.3 Tz. 14 Bait über die Risikosituation informiert werden. An dieser Stelle ist vor allem die quartalsweise Berichterstattung neu hinzugekommen.

Die Bait präzisieren und dokumentieren damit an vielen Stellen die bisherige Aufsichtspraxis und unterstützen bei der Benennung der von den Instituten umzusetzenden Maßnahmen. Aus Sicht der Bafin enthalten die Bait keine neuen Anforderungen. Aus diesem Grund gibt es keine Übergangsfristen, die Bait traten mit Veröffentlichung sofort in Kraft.

Für Nutzer des SITB stellen die Bait inhaltlich keine große Herausforderung dar, nur die wenigsten Anforderungen sind neu. Derzeit finden Abstimmungen mit Instituten, Verbänden und der SIZ statt, um eine einheitliche, dem Risiko angemessene und ressourcenschonende Umsetzung der neuen Anforderungen in den Instituten zu ermöglichen. Anwendern, die sich hinsichtlich des Umsetzungsgrades der Bait in Ihrem Institut unsicher sind, stellt die SIZ ab dem ersten Quartal 2018 den "Bait-Checkup" zur Verfügung, um sich eine detailliertere Übersicht über deren Umsetzungsstand verschaffen zu können.

Scannen Sie diesen Code mit Ihrem Smartphone und lesen Sie diesen und weitere Beiträge online