Mathias Steinmann

Die Novelle der BAIT **nutzenorientiert umsetzen**

Mit der zweiten Novelle erfahren die Bankaufsichtlichen Anforderungen an die IT (BAIT) deutliche Anpassungen und Erweiterungen, die von den Kreditinstituten umgesetzt werden müssen. Die Schwerpunkte liegen auf Konkretisierungen im Auslagerungsmanagement, im IT-Risikomanagement und auf Neuanforderungen in der operativen Informationssicherheit sowie im Notfallmanagement. Doch die notwendigen Umsetzungsaktivitäten sind nicht nur regulatorische Pflicht, sie bieten auch die Chance für Effizienzgewinne.

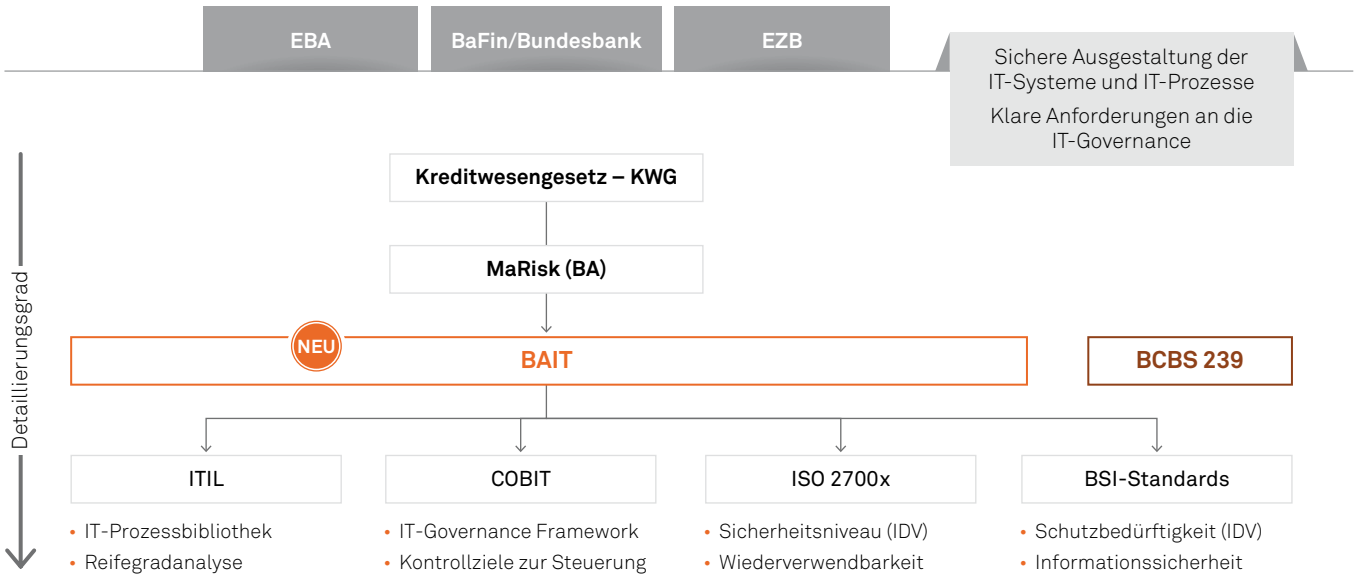

Abbildung 1: Einordnung der BAIT zwischen Regulatorik und IT-Standards

ÜBERBLICK UND EINORDNUNG IN DEN REGULATORISCHEN RAHMEN

Die erstmals 2017 veröffentlichten BAIT wurden im Jahr 2018 bislang einmal novelliert. Wie die Mindestanforderungen an das Risikomanagement der Institute (MaRisk) stellen sie eine Verwaltungsvorschrift zur Konkretisierung des § 25a des Kreditwesengesetzes (KWG) dar. Obwohl formal den MaRisk nicht untergeordnet, sind die BAIT dennoch als weitere Spezifikation des AT 7 (Ressourcen), insbesondere AT 7.2 (Technisch-organisatorische Ausstattung) und AT 7.3 (Notfallmanagement) sowie AT 9 (Auslagerung) der MaRisk zu verstehen. Im internationalen Kontext erfolgt regelmäßig die Umsetzung der EBA Guidelines unter anderem im Rahmen der BAIT.

Inhaltlich beruhen die BAIT auf in der IT gängigen Frameworks und Standards wie ITIL für das IT-Servicemanagement, COBIT für die IT-Governance, IT-Prozesse und Steuerungsvorgaben sowie ISO 2700x und den BSI-Standards für die Informationssicherheit.

Abbildung 1 veranschaulicht die Einordnung der BAIT in diesen Kontext.

FOKUS DER NOVELLE

Im Gegensatz zur ersten Novelle 2018, die lediglich in der Aufnahme des Bereichs der kritischen Infrastrukturen in die BAIT bestand, umfasst die zweite Novelle tiefer greifendere strukturelle Anpassungen und inhaltliche Ergänzungen.

Neu in Form eigenständiger Kapitel sind die Regelungsbereiche *5. Operative IT-Sicherheit* und *10. IT-Notfallmanagement*. Zwar waren entsprechende Regelungen schon bislang grundsätzlich in den BAIT enthalten. Aufgrund der neuen Struktur erfahren sie jedoch eine deutliche Aufwertung, während gleichzeitig die Anforderungen umfassender werden.

Die *operative IT-Sicherheit* setzt die Anforderungen des Informationssicherheitsmanagements um. Hierzu gehört insbesondere, dass die IT-Systeme, die zugehörigen IT-Prozesse und sonstige Bestandteile des Informationsverbunds die Schutzbedarfsziele Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit der Daten sicherstellen müssen. Dazu ist ein Verfahren zur frühzeitigen Erkennung von Gefährdungen des Informationsverbunds zu betreiben.

Im Rahmen des *IT-Notfallmanagements* müssen Kreditinstitute strategische Vorgaben zum Notfallmanagement definieren und hieraus abgeleitet einen Notfallmanagementprozess festlegen. Dazu gehört, dass

- für Notfälle in zeitkritischen Aktivitäten und Prozessen Vorsorge zu treffen ist (Notfallkonzept).
- das Notfallkonzept (Parameter und Abhängigkeiten) Geschäftsfortführungs- sowie Wiederanlaufpläne umfasst.

Komplett neu ist das Kapitel *11 Kundenbeziehungen mit Zahlungsdienstleistern*. Hier werden relevante Aspekte der PSD 2 aufgegriffen. Im Fokus stehen die Anforderungen an Zahlungsdienstleister, Prozesse zur Beratung und kommunikative Hilfestellungen für die Zahlungsdienstnutzer einzurichten, die das Bewusstsein der Zahlungsdienstnutzer für mögliche Gefahren und Sicherheitsrisiken stärken sollen.

Ferner wurden die bereits bestehenden Kapitel der BAIT in Detailfragen ergänzt und angepasst. An dieser Stelle sei hier lediglich auf die Notwendigkeit einer ganzheitlichen Umsetzung der Anforderungen an das Auslagerungsmanagement aus BAIT und MaRisk, die beide diesem Thema jeweils einen eigenständigen Regelungsbereich widmen, hingewiesen.

Abbildung 2 stellt die neue Struktur dar und ordnet die Kapitel nach Regelungen zu Governance, Steuerung und operativen Anforderungen.

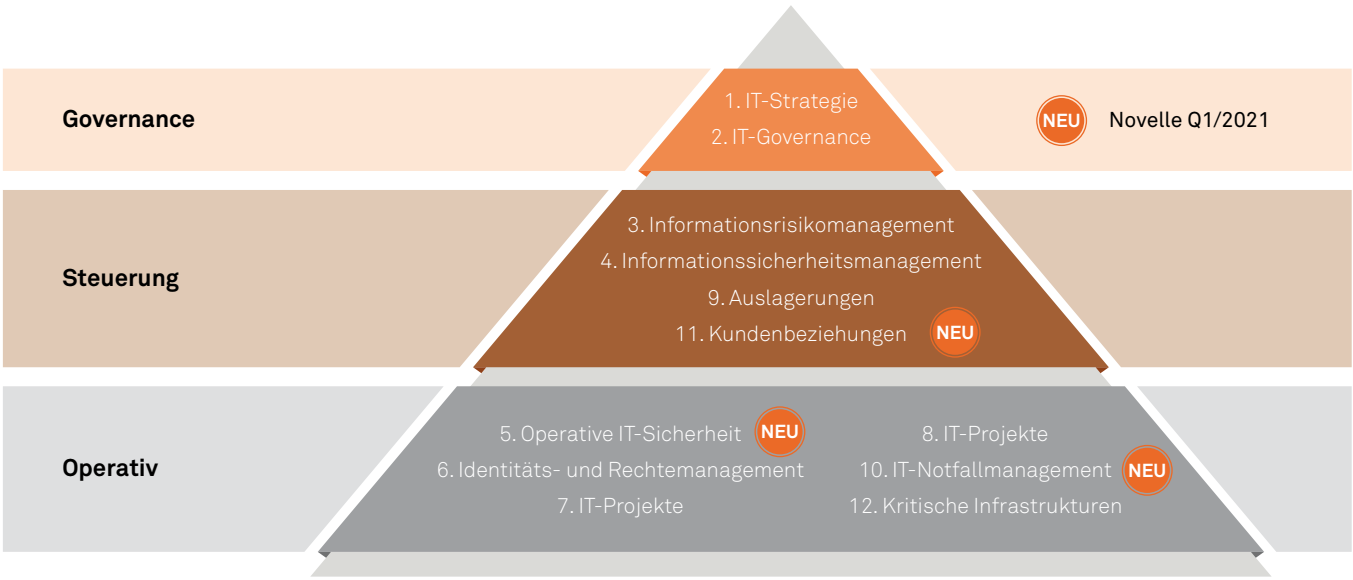

Abbildung 2: Struktureller Aufbau der BAIT

NUTZENORIENTIERTE UMSETZUNG

Das inhaltliche Fundament der oben genannten IT-Standards und Frameworks verleiht den BAIT einen hohen praktischen Nutzwert. Daher sollte die Umsetzung nicht als lästige regulatorische Pflicht gesehen werden.

Ein Aspekt, den die Aufsicht mit dem Papier BCBS 239 erstmals als expliziten Zweck regulatorischer Vorgaben genannt hat, ist die Steigerung des „Geschäftswerts" beziehungsweise Unternehmenswerts. Dahinter steckt die Idee, dass die Maßnahmen durch steigende Erträge und/oder sinkende Kosten in der Zukunft zu höheren Gewinnen führen, was natürlich den Unternehmenswert erhöht. Die Vorgaben aus BCBS 239 sollen dieses Ziel unterstützen, indem ihre Umsetzung den Reportingaufwand unter anderem in Risikoreporting, Meldewesen und weiterem internen Berichtswesen, etwa dem Vertriebsreporting, signifikant senkt, und zwar durch Vermeidung von System- und Datenredundanz, effektivere Prozesse, Senkung von Risikokosten (zum Beispiel operationelles Risiko und Modellrisiko) sowie Reduzierung von Entscheidungsunsicherheiten durch bessere Informationen.

Eine Argumentation, die sich auf die Umsetzung der BAIT übertragen lässt. Die Summe der IT-, Risiko- und Prozesskosten lässt sich durch Anwendung der entsprechenden Regelungen deutlich senken: durch eine zukunftsorientierte IT-Infrastruktur, verbesserte Prozessabläufe, die Optimierung von Informationssicherheit und somit Reduzierung entsprechender Risiken und der damit verbundenen Risikokosten. Abbildung 3 veranschaulicht diesen Zusammenhang.

DAS RICHTIGE HERANGEHEN

Auch wenn die Kreditinstitute einen Großteil der Regelungen bereits aus der vorherigen Fassung der BAIT umgesetzt haben, lohnt es sich – auch aufgrund der Dynamik in der IT und weil die BAIT sofort, ohne Umsetzungsfrist in Kraft treten –, die Novelle für eine gründliche Bestandsaufnahme zu nutzen, um so offene Flanken und erforderlichen Handlungsbedarf zu identifizieren.

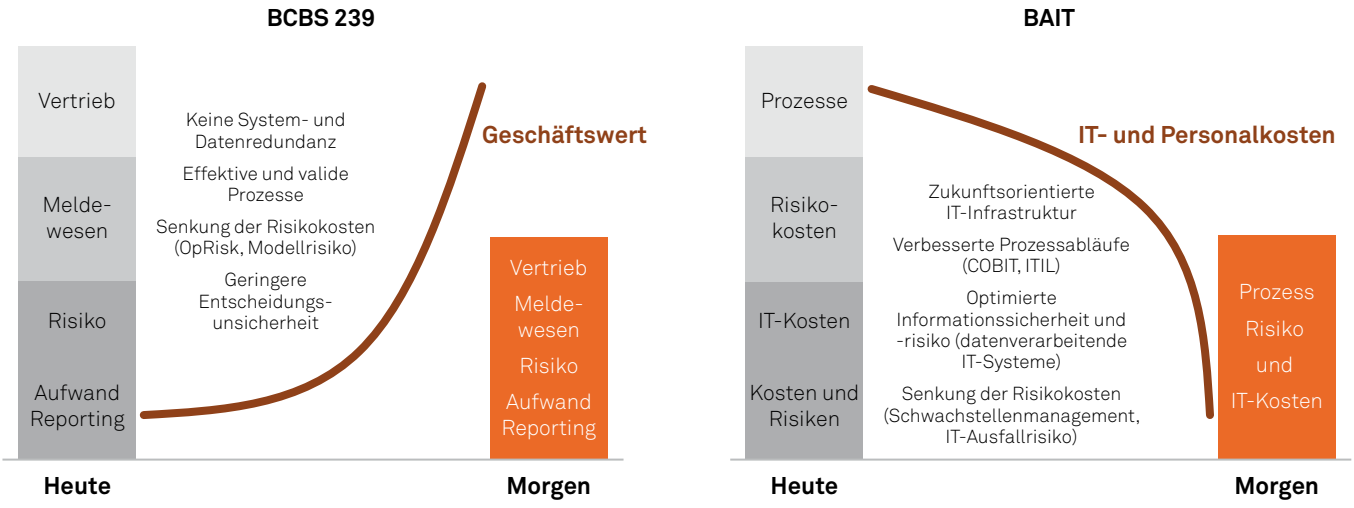

Abbildung 3: Betriebswirtschaftlicher Nutzen der BAIT-Umsetzung in Analogie zu BCBS 239

QUICK-CHECK BAIT VON msgGillardon

Der Quick-Check BAIT ermöglicht eine effiziente Bestandsaufnahme und vermittelt viel spezifisches Know-how zu allen inhaltlichen Teilbereichen der BAIT, das aufgrund der Vielzahl von Anforderungen unverzichtbar ist. Da es sich bei den BAIT um ein prinzipienorientiertes Werk handelt, kann so das Proportionalitätsprinzip genutzt werden, um ganzheitliche und individuelle praxisgerechte Lösungen für jedes Haus zu finden. Im Ergebnis erhält das Kreditinstitut eine umfassende Bestimmung des Reifegrads und der bestehenden Handlungsoptionen als Grundlage für die folgenden Umsetzungsaktivitäten.

Schlankes Assessment

- Ganzheitliche Betrachtung aller Anforderungen
- BAIT-Quick-Check zur Validierung des Reifegrades
- Analyse aller relevanten Anforderungen (Bestimmung Maturity Level)

Individuelle Positionsbestimmung

- Bankspezifisch designt
- Identifizierung von GAPs
- Individuelle Ableitung von Handlungsoptionen
- Begleitung von Audits (Vor- bis Nachbereitung)

Bewährtes Vorgehensmodell

- Standardisiertes Vorgehensmodell (auch toolgestützt)
- Spezielle Templates und Fragenkataloge
- Individuelle Quick-Checks, Workshops, Assessments

Optimierte Handlungsempfehlung

- Kostenschonende und zentrale Koordination der Experten
- Zugriff auf branchenübergreifende Erfahrung
- Konkrete Lösungsvorschläge bei Handlungsbedarf

Ansprechpartner

Mathias Steinmann
Partner
mathias.steinmann@msg-gillardon.de

Kurt Annen
Senior Manager
kurt.annen@msg-gillardon.de