SOIT

Effizient umsetzen

Nur wer seine Prozesse und die eingesetzten IT-Systeme genau kennt, kann sie optimal auf die sich ständig verändernde Umwelt anpassen. Neben betriebswirtschaftlichen Aspekten sind daher auch aufsichtsrechtliche Anforderungen an das Risikomanagement (MaRisk) sowie künftig die „Bankaufsichtlichen Anforderungen an die IT" (BAIT) zu erfüllen.

Stefan Beck

Nach den MaRisk AT 7.2 ist eine angemessene technisch-organisatorische Ausstattung von IT-Systemen und den dazugehörigen IT-Prozessen notwendig. Dabei müssen die Schutzziele Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sichergestellt sein und bei der Ausgestaltung der IT-Systeme und der zugehörigen Prozesse gängige Standards eingehalten werden. Diese Anforderung gilt unabhängig davon, ob die IT-Systeme und -Prozesse von der Bank selbst betrieben werden, ob sie ausgelagert sind oder die Leistung von externer Stelle bezogen wird.

Jedes Institut ist daher verantwortlich, anhand eines solchen Standards regelmäßig zu überprüfen, ob ihre IT-Systeme und -Prozesse diese Anforderungen (noch) erfüllen oder ob sich bei Abweichungen vom Standard hieraus zusätzliche Risiken ergeben. Da diese Prüfung sowohl Bestandteil der internen als auch der externen Compliance-Prüfungen ist, sollte sie in Form eines Überwachungs- und Steuerungsprozesses so gestaltet werden, dass für einen sachverständiger Dritten dies leicht nachvollzogen werden kann.

Aufsicht fordert

Die gestiegene Bedeutung der IT-Risiken und die Notwendigkeit für diese, ein angemessenes Verfahren einzurichten, bringt die Aufsicht dadurch zum Ausdruck, dass in der aktuellen Konsultation der Novellierung der MaRisk 6.0 die Anforderungen des AT 7.2 „Technisch-organisatorische Ausstattung" diesbezüglich sogar um eine eigenständige Tz. 4 erweitert wurde. Dies konkretisiert sich auch weiter bereits im Konsultationsentwurf der bankaufsichtlichen Anforderungen an die IT (BAIT), in der ein Mindestniveau an ein Informationsrisikomanagement beschrieben wird.

Wörtlich heißt es in AT 7.2 Tz.4 künftig: „Für IT-Risiken sind angemessene Überwachungs- und Steuerungsprozesse einzurichten, die insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung entsprechender Maßnahmen zur Risikobehandlung und -minderung umfassen. Beim Bezug von Software sind die damit verbundenen Risiken angemessen zu bewerten".

Dadurch erwartet die Aufsicht künftig von allen Instituten, dass die IT-Risiken durch einen Regelprozess in ein Gesamtbild der operationellen Risiken überführt werden. Die Absicht dahinter ist es, nicht nur das Gesamtbild der operationellen (IT-)Risiken auf Ebene der Geschäftsleitung zu stärken und weiter in den Fokus zu rücken, sondern zusammen mit einer Risikostrategie diesen auch für eine direkte Mitarbeiteransprache zu nutzen. Eine transparente Risikodarstellung und -politik geben den Mitarbeitern eine Orientierung im Umgang mit der IT und deren Ri-

Stefan Beck ist Berater Kostenmanagement/ IT in der Beratung Genossenschaftsbanken Abteilung Prozesse beim BWGV.

E-Mail: stefan.beck@bwgv-info.de

siken. Informationen und Transparenz sind somit auch eine Chance zur Risikovermeidung und Sensibilisierung der Mitarbeiter.

Zur Umsetzung einer angemessenen technischen und organisatorischen Ausgestaltung der IT-Systeme nutzten Genossenschaftsbanken im ehemaligen Fiducia-Geschäftsgebiet bisher das Regelwerk „Handbuch für Ordnungs mäßigkeitsfragen der agree-Bankorganisation" (HB OF). Das HB OF bildete die Vorgaben der gängigen Standards ab und konkretisierte sie für das Umfeld der Bank. Dabei wurde das HB OF bei Prüfungen durch die Aufsicht als ein Standard im Sinne der AT 7.2 mit anforderungsspezifischer Sicht anerkannt.

Im Zuge der Verschmelzung beider Kernbankverfahren im genossenschaftlichen Bereich erfuhr das bisherige HB OF eine komplette Überarbeitung und wurde Ende des Jahres 2016 als „Standard für Ordnungsmäßigkeit der IT-Verfahren (SOIT) der Fiducia & GAD" veröffentlicht.

Dreiteiliger SOIT

Der SOIT ist in drei Teile aufgeteilt. Der erste Teil „Grundlagen" beschäftigt sich mit grundlegenden Themenstellungen und ist an alle Banken adressiert – unabhängig welches Bankverfahren eingesetzt wird. Zu diesen Themenbereichen gehören zum Beispiel der Aufbau eines Informationssicherheits- und Risikomanagements, Regelungen zum Umgang mit Auslagerungen und die Ausgestaltung eines Notfall-Managements. Dieser Teil trägt durch Umsetzung der dort beschriebenen technisch-organisatorischen Maßnahmen maßgeblich dazu bei, dass die Anforderung des MaRisk AT 7.2 und der BAIT erfüllt werden können. Der zweite Teil „agree21" richtet sich an die Anwender des Bankverfahrens agree21 und betrachtet das agree21-Portfolio. Die einzelnen Produkte werden kurz beschrieben, auf mögliche Risiken und Steuerungsmöglichkeiten wird eingegangen. Weiter werden mit dazugehörigen Fragestellungen Maßnahmen und Hinweise aufgeführt, die die Bank bei der individuellen Umsetzung unterstützen. Sowohl die Struktur als auch die Inhalte des zweiten Teils wurden aus dem ehemaligen HB OF übernommen. Es beinhaltet konkrete Maßnahmen und Fragestellungen zu den verschiedenen Produkten des agree21-Portfolios.

Der Teil drei „bank21" richtet sich an die Anwender des Bankverfahrens bank21 und betrachtet ausgewählte bank21-Komponenten. In Verbindung mit den bestehenden Anwenderdokumenta-

Die MaRisk fordern gängige Standards für die IT

tionen zu den einzelnen Produkten werden die Besonderheiten hervorgehoben. Fragestellungen zur Unterstützung beim Einsatz und der bankindividuellen Umsetzungen sind ebenfalls enthalten.

Der SOIT wird durch den Arbeitskreis „Ordnungsmäßigkeit und Revision" herausgegeben und regelmäßig aktualisiert. Er trägt die inhaltliche Verantwortung. Durch weitere Unterarbeitskreise wird durch die Kooperation zwischen Rechenzentrale, Vertretern der regionalen Prüfungsverbände und der Partnerbanken sichergestellt, dass sowohl die Anforderungen der täglichen Praxis als auch die Prüfungssicherheit berücksichtigt werden. Innovationen und aufsichtsrechtliche Neuerungen im sich ständig ändernden Umfeld werden im SOIT dadurch in praxisnahe Anforderungen formuliert.

Der SOIT interpretiert somit nun für alle Banken der genossenschaftlichen FinanzGruppe die Vorgaben gängiger Standards und konkretisiert diese auf das agree21- und bank21-Umfeld. Dadurch entsteht ein für die Genossenschaftsbanken einheitlicher Standard. Durch die Anwendung und Umsetzung der darin genannten Maßnahmen können die aufsichtsrechtlichen Anforderungen zur Ausgestaltung der IT-Systeme und der zugehörigen Prozesse anhand eines gängigen Standards erfüllt werden. Dies auch, weil die Beachtung des Inhalts aus dem SOIT ebenfalls Bestandteil des Rahmendienstleistungsvertrags zwischen der jeweiligen Genossenschaftsbank und der Fiducia & GAD ist.

Die Methoden, Vorgehensweisen, Maßnahmen (Fragestellungen) und Empfehlungen berücksichtigen gesetzliche und aufsichtsrechtliche Vorgaben sowie allgemeingültige Standards zur IT-Sicherheit. Hierdurch können die Ausführungen des SOIT auch für Anwendungen und IT-Systeme außerhalb der Fiducia & GAD adaptiert werden. Mit dem SOIT haben somit alle Banken in der genossenschaftlichen FinanzGruppe – unabhängig vom eingesetzten Bankverfahren – ein Werk, in dem sie die Themenstellungen rund um Ordnungsmäßigkeit und IT-Sicherheit nachschlagen und für ihre eigene Bankorganisation berücksichtigen und umsetzen können.

Dabei dient der SOIT auch als Arbeitshilfe zur Umsetzung der in der MaRisk geforderten Prüfung des internen Kontrollsystems. Zeitgleich werden die Anwender des SOIT für Themen der Ordnungsmäßigkeit und Sicherheit sensibilisiert, um damit die Einhaltung der Compliance-Anforderungen gewährleisten zu können.

Regelmäßige Überprüfung

Nach jeder Aktualisierung des SOIT über eine Ergänzungslieferung müssen bei sich ergebenden Veränderungen die bisherigen Regelungen der Bank zum aktualisierten Themenbereich auf den Prüfstand gestellt und entsprechend angepasst werden. Die Bearbeitung der Fragestellungen (Maßnahmen) ist entscheidend, da bei Abweichungen vom Standard bewusst Risiken eingegangen werden, die es gilt transparent zu machen und als operationelle Risiken in das Risikomanagement der Bank zu überführen.

Diese Aufgabe bindet oft viele Ressourcen, da Neuerungen und Anforderungen zuerst im Volltext des SOIT gefunden und anschließend entsprechend manuell zur Bewertung und Dokumentation ausgearbeitet werden müssen. Die Identifizierung von Abweichungen sollte jedoch möglichst schlank und effizient umgesetzt werden. Da es sich hierbei vorwiegend um die Verhinderung potenzieller Schäden dreht, ist eine Erfolgsmessung durch direkt messbare Größen nicht möglich. Entscheidend für einen wirtschaftlichen Erfolg ist es daher, sich neben der Umsetzung der aufsichtsrechtlichen Anforderung in der Auseinandersetzung mit den Geschäftsprozessen unter Ordnungsmäßigkeits- und Sicherheitsaspekten zugleich auch die Betrachtung und Anpassung von Prozessen unter Effizienzgesichtspunkten vorzunehmen.

Zur Unterstützung und effizienten Ausgestaltung dieser Anforderung hat der BWGV eine gleichnamige Notes-Datenbank entwickelt. Aufgrund der Einheitlichkeit des SOIT kann diese nun auch unabhängig der Verbandszugehörigkeit und in Abstimmung mit anderen Regionalverbänden erworben und verwendet werden. Dieses Hilfsmittel unterstützt das Institut dabei, die im SOIT enthaltenden Fragestellungen (Maßnahmen) praxis- und technikorientiert sowie nachvollziehbar zu bearbeiten und zu dokumentieren. Durch die Evaluierung des Inhalts des SOIT und insbesondere der darin eingeschlossenen Fragestellungen und Maßnahmen ist es möglich, ein effizientes internes Kontrollsystem unter Kosten-, Nutzen- und Risikoaspekten zu entwickeln.

Eine kapitelweise Darstellung der Fragestellungen innerhalb der Datenbank ermöglicht es, die thematischen Zusammenhänge beizubehalten. Durch die Bereitstellung von Updates unterstützt der BWGV die Abonnenten der Datenbank gezielt dabei, nur die Neuerungen zu bearbeiten und diese ressourcenschonend umzusetzen. Die Datenbank unterstützt zusätzlich, indem sie beispielsweise bei Standard unmittelbar einer Risikoanalyse unterzogen werden können.

Das Ergebnis dieser Umsetzungs- und Risikoanalyse wird innerhalb der Datenbank über diverse Ansichten übersichtlich dargestellt, um damit eine Übertragung in das übergreifende Risikocontrolling der Bank zu erleichtern. Dazu bietet der BWGV im Bundle mit der Notes-Datenbank „BWGV Risikomanagement" die Möglichkeit, diesen Schritt über eine integrierte Schnittstelle vollautomatisch in eine Übersicht auszuführen. Die Funktionen der Datenbanken können darüber hinaus für weitere Risikoanalysen, etwa für Anwendungen in wesentlichen Geschäftsprozessen und zur Dokumentation von regelmäßigen Kontrollhandlungen genutzt werden.

Durch diese effiziente Umsetzungsanalyse wird schnell und einfach Transparenz über die Abläufe geschaffen und damit das interne Kontrollsystem der Bank gestärkt. Durch die Zuweisung von Verantwortlichkeiten sowie ein integriertes Workflowsystem ist die revisionssichere Bearbeitung jederzeit gewährleistet. Darüber hinaus bieten die Datenbanken ein umfangreiches Wiedervorlagesystem, um der Anforderung der jährlichen regelmäßigen Überprüfung eben-

BAIT

Die Aufsicht bereitet auch ein Rundschreiben zu den bankaufsichtlichen Anforderungen an die IT (BAIT) vor, dass zurzeit noch konsultiert wird. Die BAIT knüpft dabei an die Verantwortung der Geschäftsleitung nach § 25a Absatz 1 Kreditwesengesetz (KWG) zur Einrichtung einer ordnungsgemäßen Geschäftsorganisation an. Mit den BAIT wollen Deutsche Bundesbank und BaFin nach eigener Aussage die Erwartungshaltung der Aufsicht an die Institute transparenter darstellen und die in den Mindestanforderungen an das Risikomanagement (MaRisk) enthaltenen Anforderungen in Bezug auf die IT konkretisieren sowie das Bewusstsein für IT-Risiken erhöhen. Mit der Veröffentlichung des finalen Rundschreibens ist Mitte des Jahres zu rechnen.

Die zielorientierte und effiziente Ausgestaltung des internen Kontrollsystems mit der Festlegung technisch-organisatorischer Maßnahmen zur Sicherstellung der Ordnungsmäßigkeit samt der Optimierung der Prozesse ist nicht nur eine Frage der Erfüllung aufsichtsrechtlicher Anforderungen, sondern auch eine Frage der bewussten Übernahme von Risiken und übergeordneten Managemententscheidungen, die in der besonderen Verantwortung von Vorstand und Führungskräften liegt. BI