IT-Governance

# Praxisnah und qualitätsgesichert

Aufgrund der Entwicklung der Digitalisierung und der Vernetzung steigt die Bedeutung und die Komplexität von Informationssicherheitsfragen stetig an. Der Druck der Aufsicht – auch im Kontext der Nachverfolgung von §44er-Findings – wird seit einiger Zeit für die Banken und deren Dienstleister spürbarer. Die ZAM wurde deshalb von der genossenschaftlichen FinanzGruppe beauftragt, ein Verfahren zur methodischen Unterstützung der IT-Regulatorik aufzubauen.

**Andreas Kötter**

Mit den ständig erweiterten Anforderungen aus den MaRisk, den BAIT, dem Zahlungsdiensteaufsichtsgesetz (ZAG) und DORA wird deren Umsetzung stetig komplexer und herausfordernder.

Nicht zuletzt wird die Nachverfolgung der aktuellen Umsetzungen für alle Genossenschaftsbanken durch Abfragen mittels Fragebögen zur Bewertung der ICT-Risiken (Information and Communication Technologies) im Rahmen des aufsichtlichen SREP-Prozesses flächendeckend vorgenommen.

*Andreas Kötter ist Spezialist Verfahrenslieferant bei der ZAM eG.*
*E-Mail: andreas.koetter@zam-eg.de*

Derzeit gibt es keine zentrale Unterstützung der Banken bei der Operationalisierung der regulatorischen Anforderungen. Einzelne Anforderungen müssen aktuell noch von den Instituten selbst oder mit Unterstützung der Regionalverbände erarbeitet werden.

### *Zielbild des Verfahrens*

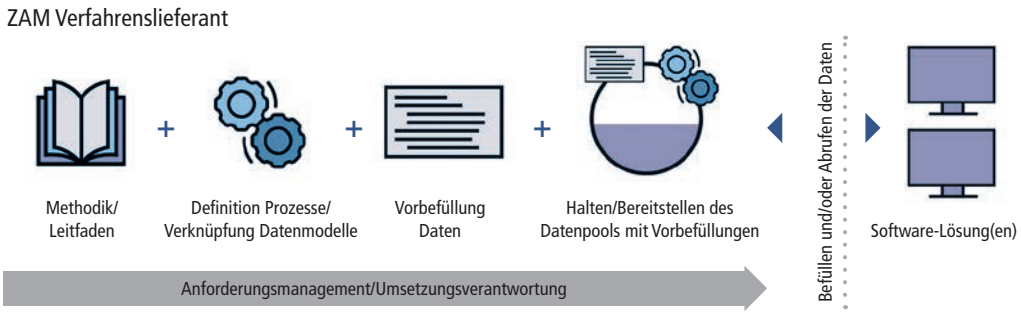
Mit dem zentralen Verfahren plant die ZAM, den Banken eine durchgängige Abbildung der methodischen Unterstützung – unter Berücksichtigung des BVR-Leitfadens „Methodische Grundlagen zur IT-Regulatorik" – in Form von vereinheitlichten Prozessen und Modellen als Vorschläge zur Verfügung zu stellen.

Dabei richtet sie das Verfahren an den regulatorischen Anforderungen MaRisk, BAIT, DORA und weiteren sowie an gängigen Standards, wie etwa ISO/IEC 27001:2022, ISO/IEC 27002:2022 und BSI 200-4, aus. Die Umsetzung erfolgt in einer detaillierten Darstellung aller IT-regulatorischen Prozesse mit Zuordnung der verantwortlichen Funktionsbereiche inklusive ausführlicher Beschreibungen.

Darüber hinaus wird ein zentraler Datenpool bereitgestellt, in dem alle relevanten Informationen eines Informationssicherheits-, Informationsrisiko- sowie Notfallmanagements zur Verfügung gestellt und gespeichert werden. Der Zugriff auf den Datenpool ist für alle Genossenschaftsbanken über die aktuell eingesetzten Softwarelösungen geplant.

### *Informationssicherheits-management*

Zur Unterstützung der Banken ist eine Vorbefüllung von Vorschlägen, wie etwa Informationsklassen, Prozesse aus der einheitlichen BVR-Prozesslandkarte und bereitgestellte IT-Assets (wie etwa An-




wendungen), der durch die ZAM gesteuerten Dienstleister geplant.

Ergänzend wird ein zentraler Sollmaßnahmenkatalog auf Basis der Standards ISO/IEC 27001:2022 sowie ISO/IEC 27002:2022 mit Ergänzungen der Anforderungen aus den BAIT, den MaRisk und der DORA etc. angeboten. Dieser wird mit allen im Datenpool zentral gepflegten IT-Asset-Vorschlägen für Unternehmen der genossenschaftlichen FinanzGruppe im Rahmen von Soll-/Soll- und Soll-/Ist-Abgleichen zentral abgeglichen und kann ergänzend für selbstgepflegte Assets ebenfalls angewendet werden. Für die aus den Vorschlägen ermittelten Abweichungen werden Risikovorschläge generiert und zudem eine vorbewertete Risikoeinwertung aufgrund von Expertenschätzungen empfohlen.

### *Informationsrisikomanagement*

Im Informationsrisikomanagement können unter anderem Risiken aus Soll-/Soll- und Soll-/Ist-Abgleichen sowie gemeldete oder erkannte Schwachstellen, Ergebnisse aus Penetrationstests, Audits, SIEM-Meldungen und Sicherheitsvorfällen erfasst und bearbeitet werden.

Auch hier wird die ZAM zentrale Vorschläge für alle IT-Assets der von ihr gesteuerten Verbundpartner machen und diese im Rahmen der Leistungsüberwachung nachverfolgen. Durch eine bankindividuelle Parametrisierung des Verfahrens werden die vorgeschlagenen Risiken den bankindividuellen OpRisk-Ausprägungen bezüglich Eintrittswahrscheinlichkeiten und Schadensausmaßen weitestgehend entsprechen. Somit ist eine effiziente Weiterverarbeitung aller erfasster Informationsrisiken durch das Risikomanagement der Bank durch Export dieser Daten gewährleistet.

### *Notfallmanagement*

In Bezug auf das Notfallmanagement kann ein vollständiges Notfallkonzept im Verfahren dargestellt werden. Business-Impact-Analysen, daraus abgeleitete Notfallszenarien und Risikoanalysen werden den Banken aus den erfassten Geschäftsprozessen und den damit verknüpften Ressourcen in einem einheitlichen Modell im Datenpool strukturiert und mit Vorschlägen ergänzt zur Verfügung gestellt. Daraus abzuleitende Notfallpläne für zeitkritische Prozesse und Ressourcen sowie durchzuführende Notfallübungen werden umfassend nachgehalten und durch Beispiele unterstützt.

Das Verfahren orientiert sich praxisnah an den regulatorischen Vorgaben unter Berücksichtigung des vom BVR veröffentlichten Leitfadens „Methodische Grundlagen zur IT-Regulatorik“. Sieben Pilotbanken aus ganz Deutschland – repräsentativ für alle Größen von Genossenschaftsbanken und alle Gebiete der Regionalverbände – begleiten von Anfang an die Entwicklung des Verfahrens, bringen eigenes Know-how ein und verproben die Ergebnisse. Zusätzlich finden Austausche mit den Verbundunternehmen statt.

Dies hat den Vorteil, dass möglichst viele Synergien und Erfahrungen gebündelt werden. Die Entwicklung des Verfahrens wird von den Regionalverbänden und dem BVR begleitet.

Mit der Veröffentlichung des Verfahrens am Ende des ersten Halbjahrs 2024 gibt die ZAM allen Volksbanken und Raiffeisenbanken regulatorische Sicherheit. Unter Berücksichtigung und Aktualisierung aller Vorgaben und Standards etabliert sie eine einheitliche IT-Governance für alle Genossenschaftsbanken der genossenschaftlichen FinanzGruppe.

Das umfassende Angebot von Vorschlägen und die Bereitstellung im zentralen Datenpool gewährleisten eine einheitliche Steuerung der Dienstleister hinsichtlich Informationssicherheitsmanagement, Informationsrisiko- und Notfallmanagement. Durch Einbindung der Pilotbanken erfolgt eine praxisnahe Umsetzung der Anforderungen an den Bedürfnissen aller Genossenschaftsbanken und schafft somit eine Entlastung ihrer Ressourcen. BI