Implementierung

Strenger, detaillierter, umfassender

DORA stellt eine erhebliche Erweiterung und Vertiefung der bisherigen regulatorischen Anforderungen hinsichtlich des IKT-Risikomanagements dar. Genossenschaftsbanken müssen ihre Strategien, Richtlinien, Prozesse und Strukturen erheblich anpassen und erweitern, um die operationale Resilienz zu erhöhen.

Gabriele Heiliger und Andreas Kötter

Mit den DORA-Artikeln 6, 7 sowie 13 und dem „RTS on ICT risk management tools, methods, processes and policies" in den Artikeln 3 und 28 erwartet die Aufsicht wesentliche Anpassungen im IKT-Risikomanagement der Bank. Darunter fallen etwa Anforderungen an die Strategie, den Governance- und Kontrollrahmen, eine neue IKT-Risikokontrollfunktion, erweiterte Anforderungen zur Analyse von IKT-Risiken, Schwachstellen, neuen Technologien, Altsystemen, Vorfällen und Tests, eine regelmäßige Überprüfung des IKT-Risikomanagementrahmens inklusive Berichtswesen und die strukturierte Überführung von IKT-Risiken ins OpRisk.

Daraus entsteht für Banken der Handlungsbedarf, die Methodik für das IKT-Risikomanagement zu überprüfen und um die neuen Aspekte aus DORA zu ergänzen. Die Bankenaufsicht erwartet einen einheitlichen IKT-Risikomanagementrahmen, der Teil des Gesamtrisikomanagementsystems ist und der es ermöglicht, IKT-Risiken inklusive der IKT-Drittbezugsrisiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten.

Der IKT-Risikomanagementrahmen ist jährlich und anlassbezogen zu überprüfen. Überprüfungsnotwendigkeiten ergeben sich aus dem Auftreten schwerwiegender IKT-bezogener Vorfälle, aus aufsichtsrechtlichen Anweisungen oder Feststellungen, Erkenntnissen aus Informationssicherheitstests und Feststellungen von Audits.

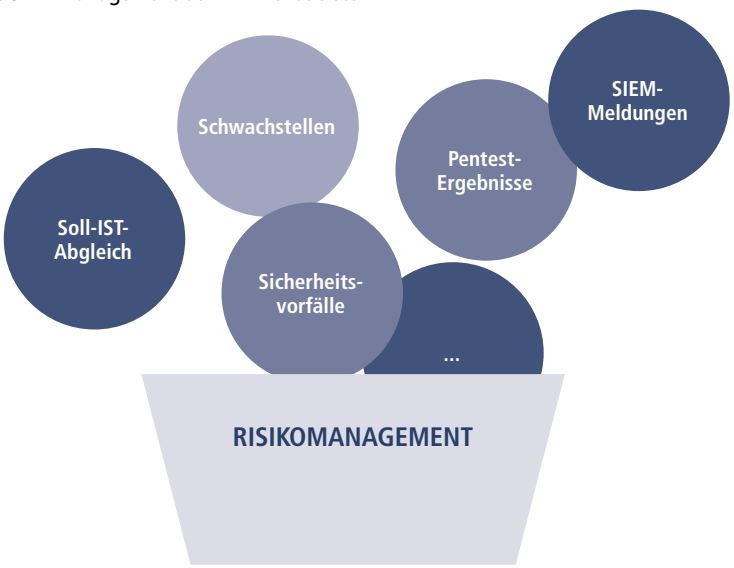
Zu den Ergebnissen der Überprüfung muss ein Bericht erstellt werden. Er muss vom Vorstand freigegeben und auf Anfrage der Bankenaufsicht zur Verfügung gestellt werden. Zusätzlich wird eine neue IKT-Risiko-Kontrollfunktion der Bank definiert. Diese verantwortet unter anderem folgende Aufgaben:

- Management und die Überwachung der IKT-Risiken sowie die Überwachung der einzelnen Phasen des IKT-Risikomanagementprozesses,
- Berichterstattung an den Vorstand sowie dessen Beratung,
- Festlegung der Ziele und der Risiko-Metriken inklusive der qualitativen und quantitativen Maßnahmen für ihre Erreichung sowie der wichtigsten Leistungsindikatoren,
- Überwachung der Einstufung der Bestandteile des Informationsverbunds,

Gabriele Heiliger ist Abteilungsleiterin Grundsatzmanagement bei der ZAM eG.
E-Mail: gabriele.heiliger@zam-eg.de

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

Abb. 1: Management der IKT-Dienstleister



- Überwachung der wirksamen Umsetzung von Programmen zur Sensibilisierung für die IKT-Sicherheit und Schulungen zur digitalen operativen Resilienz.

Die Aufgaben der IKT-Risiko-Kontrollfunktion können vom Informationssicherheitsbeauftragten in Personalunion wahrgenommen oder es kann eine zusätzliche IKT-Risiko-Kontrollfunktion geschaffen werden.

Unterstützung bei den Anpassungen und Ergänzungen des IKT-Risikomanagements erhalten die Genossenschaftsbanken zum einen durch die Aktualisierungen und Ergänzungen des BVR-Leitfadens „Methodische Umsetzung der IT-Regulatorik". Dieser wird zurzeit vom BVR in Kooperation mit den Regionalverbänden und der ZAM überarbeitet (siehe auch Artikel auf Seite 34).

Zum anderen erhalten die Banken mit dem Verfahrenslieferanten der ZAM die konkreten Unterstützungen in der strukturierten Umsetzung. Der IKT-Risikomanagementrahmen mit allen notwendigen Informationen wird dort zur Verfügung gestellt. Die IKT-Risiken leiten sich unter anderem aus erhobenen Schwachstellen, Abweichungen aus Sollmaßnahmenanforderungen, Testergebnissen, Audits und Sicherheitsvorfällen ab.

Alle Risiken werden in einer von der Bank zu definierenden Matrix (gemäß OpRisk-Riskmap) abgebildet. Die Überwachung, die Berichterstattung und Meldung der Risken an den Vorstand sowie eine Exportfunktion für OpRisk werden ebenfalls im Verfahren sichergestellt. Alle erfassten IKT-Risiken werden regelmäßig – gemäß DORA mindestens einmal jährlich – per Workflow dem Risiko-Owner zur Überprüfung vorgelegt.

Überarbeitung der schriftlich fixierten Ordnung

Zudem haben alle Institute die Notwendigkeit ihre IKT-Prozesse (inklusive Notfallmanagement und des Drittbezugsmanagements) sowie der Richtlinien, Arbeitsanweisungen und Stellenbeschreibungen anzupassen.

Dazu werden die Regionalverbände die Musterrichtlinien und -arbeitsanweisungen unter Berücksichtigung der Maßnahmen aus dem verbundweit einheitlichen Banken-Sollmaßnahmenkatalog der ZAM aktualisieren und veröffentlichen. Zusätzlich erhalten Banken aus dem Verfahren Musterbeschreibungen der notwendigen IKT-Prozesse sowie übergreifende Richtlinien nach Themenschwerpunkten (wie etwa IKT-Risikomanagement, Kryptografie) geclustert, die in den Musterdokumenten der Verbände vertieft werden.

Schulungsprogramme

DORA betont in den Artikeln 5.4, 13.6 sowie in den Artikeln 2.1(f), 11.2(k), 19 und 20 des „RTS on ICT risk magement tools, methods, processes and policies" die Schulungspflichten für das Leitungsorgan sowie Sensibilisierung von Mitarbeitern und Dienstleistern für die digitale operationale Resilienz. Dazu sind für den jeweiligen Aufgabenbereich angemessene Schulungen – auch für Vorstände – zu planen und zu implementieren.

Identifizierung

Die Verordnung fordert in dem Artikel 8 sowie ergänzend in den Artikeln 4 und 5 des „RTS on ICT risk management tools, methods, processes and policies" eine umfassende Identifizierung und Klassifizierung von Informations- und IKT-Assets sowie deren Abhängigkeiten von IKT-Diensten. Dies bedeutet in vielen Fällen eine Erweiterung des bestehenden Informationsverbunds.

Zusätzlich sind alle Prozesse gemäß den Definitionen aus Artikel

Mehr Infos

Weitere Informationen finden Sie im aktuellen Newsletter „DORA zielgerichtet umsetzen!". Dieser ist über die Anwendung ZAM-AR oder über das Atruvia Hub abrufbar..

3.22 bezüglich der „kritischen oder wichtigen Funktionen“ zu klassifizieren. Anschließend müssen die Abhängigkeiten der Prozesse von den einzelnen IKT-Assets und IKT-Dienstleistungen bewertet werden.

Um die Umsetzung der neuen Anforderungen so effizient wie möglich in allen Genossenschaftsbanken zu gestalten, wurde eine einheitliche, systematische Methode zur Identifizierung und Klassifizierung von kritischen oder wichtigen Funktionen entwickelt. Diese Methode basiert auf klaren Kriterien, die die Auswirkungen eines Ausfalls oder eine unterbrochene, fehlerhafte oder unterbliebene Leistung der jeweiligen Funktion auf die Gesamtbetrieblichkeit des Instituts und das Finanzsystem berücksichtigen.

Um Ressourcen in den Instituten zu optimieren, wurde die Klassifizierung von kritischen oder wichtigen Funktionen mit der Ermittlung der wesentlichen Prozesse nach MaRisk und den Anforderungen der Business-Impact-Analyse aus dem Notfallmanagement zusammengefasst und diese Klassifizierungen vereinheitlicht.

Jedes Institut kann so geschäftskritische Prozesse, die für den Erfolg maßgeblich notwendig sind oder diesen nachhaltig unterstützen, in einem Klassifizierungsprozess identifizieren, definieren und regelmäßig überprüfen.

Anpassung der Sicherheitsmaßnahmen

Viele Maßnahmen zum Schutz von Informationen und IKT-Assets sowie zur Prävention vor Bedrohungen wurden deutlich erweitert. Viele Themen, die bisher nur in den Erläuterungen der BAIT erwähnt wurden, werden in den technischen Regulierungsstandards über die Anforderungen der BAIT hinaus detailliert beschrieben. Banken sollten auf Basis der DORA-Anforderungen die bankeigenen Sollmaßnahmenkataloge und Konzepte bezüglich der neu geforderten Sicherheitsmaßnahmen aktualisieren, mit den Dienstleistern neu vereinbaren und für die bankindividuelle IT die Umsetzung selbst sicherstellen. Eine deutliche Erleichterung kann hier der neue verbundweit einheitliche Banken-Sollmaßnahmenkatalog (BaSo) der ZAM eG bieten, der die Anforderungen aus DORA berücksichtigt. Entsprechend dem IKT-Asset-Cluster und dem Schutzbedarf sind die Anforderungen in den Prozessen Soll-/Soll- und Soll-/Ist-Abgleich mit eigenen IKT-Assets bzw. mit den IKT-Dienstleistern abzugleichen. Die regelmäßig geforderten Rezertifizierungen der umgesetzten Maßnahmen finden ebenfalls im Verfahren statt.

IKT-Notfallmanagement

In den Artikeln 5.2, 11, 12, 14 der Verordnung sowie in den Artikeln 25 bis 27 im „RTS on ICT risk management tools, methods, processes and policies“ geht DORA auf das IKT-Notfallmanagement ein.

Eine (IKT-)Geschäftsfortführungsleitlinie muss verabschiedet und es müssen – ergänzend zu den herkömmlichen Notfallszenarien – weitere Szenarien aus den neuen Anforderungen gebührend in Betracht gezogen werden. Zusätzlich müssen anschließend die Reaktions- und Wiederherstellungspläne diesbezüglich aktualisiert und erweitert werden. Die IKT-Reaktions- und Wiederherstellungspläne werden unter Berücksichtigung der Ergebnisse der Business-Impact-Analyse und den entsprechenden Szenarien entwickelt. Zukünftige Tests und Notfallübungen müssen auf der Basis von realistischen Szenarien durchgeführt werden.

Mit ihrem Verfahren stellt die ZAM den Genossenschaftsbanken einen strukturierten Rahmen zur Erfassung der Notfallszenarien, des jeweiligen Business Impacts auf alle erfassten Prozesse sowie den jeweils damit verknüpften IKT-Assets bereit. Daraus abgeleitet können die Risiken für potenzielle Auswirkungen schwerwiegender Betriebsstörungen und Ausfälle anhand quantitativer und qualitativer Kriterien für die Bank ermittelt sowie Notfallpläne (in Form von Geschäftsfortführungs-, IKT-Reaktions- und Wiederherstellungsplänen) beschrieben werden.

Die notwendigen Tests und Ergebnisse können strukturiert nachgewiesen und mit den Sollvorgaben verglichen werden. Zudem werden Tätigkeiten vor und während Störungen dokumentiert. Die Berichterstattung und Meldung der Risken an das Leitungsorgan sowie eine Exportfunktion für OpRisk werden ebenfalls sichergestellt.

Klassifizierung und Meldung IKT-bezogener Vorfälle

DORA fordert in den Artikeln 11.10 sowie 17 bis 19 die Differenzierung von IKT-bezogenen Vorfällen in „schwerwiegende IKT-bezogene Vorfälle“ und andere. Die Klassifizierungskriterien werden durch DORA über den technischen Regulierungsstandard on incident response, RTS / ITS on major incident reporting vorgegeben. Die zukünftigen Meldungen schwerwiegender IKT-bezogener Vorfälle an die BaFin weiten die bisherigen Meldungen nach dem Zahlungsdiensteaufsichtsgesetz ZAG (PSD2-Meldungen) deutlich aus.

Nach einem IKT-Sicherheitsvorfall soll die Bank einen Lernprozess zur Verbesserung der Resilienz starten, um aus den Erkenntnissen des Vorfalls mögliche Maßnahmen abzuleiten. Die ZAM stellt

Zukunft sichern – Payment neu denken

Karten-Forum 2024

18.09.2024
Jetzt anmelden!

Innovation und Zukunftsfähigkeit stehen im Fokus des 19. Karten-Forums. Entdecken Sie, wie Ihr Karten- und Payment-Geschäft aktiv zur Zukunft der Genossenschaftsbanken beitragen kann. Sie erleben spannende Keynotes und mitreißende Diskussionsrunden mit Branchenkennern. Tauschen Sie Ideen aus und lassen Sie sich von den neuesten Trends und Entwicklungen inspirieren – eingebettet in einem abwechslungsreichen optionalen Rahmenprogramm zum Netzwerken und Staunen.

Seien Sie dabei, wenn wir gemeinsam Zukunft schreiben – auf dem Karten-Forum 2024 in Wiesbaden!

s.dg-nexolution.de/kartenforum2024

DG nexolution

Gemeinsam vorn.

im Verfahren einen Prozess für die Erfassung und Behandlung IKT-bezogener Vorfälle bereit.

Vorgehen und Umsetzung des Testprogramms

In den Artikeln 24 bis 27 der Verordnung sowie im Artikel 10 des RTS werden eine Reihe von Testarten über die in den BAIT hinaus genannten beschrieben. Das Test- und Überprüfungsprogramm beinhaltet angemessene Tests, wie etwa Schwachstellenscans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Gap-Analysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

Für die Genossenschaftsbanken bedeutet dies, die Planungen zur Durchführung von Tests – unter anderem durch Einholung von Angeboten bei Dienstleistern – zu erweitern.

Management von IKT-Drittparteienrisiken

Die Anforderungen an das Management für IKT-Drittparteienrisiken sind primär in den Artikeln 6.9, 28, 29 und 31 von DORA sowie in den „RTS on use of ICT services" sowie „RTS on subcontracting" beschrieben und fordern Erweiterungen der bestehenden Strategien und Richtlinien, umfassende Regelungen zur Unterauftragsvergabe und Ausweitungen der Ausstiegspläne. Die IKT-Drittparteienrisiken sind gemäß Artikel 28 als ein zentraler Bestandteil des neu zu definierendem IKT-Risikomanagementrahmens zu berücksichtigen.

Hierbei wichtig: DORA greift bei der Herleitung dieser Drittbezugsrisiken auf seine Definition der IKT-Dienstleistung zurück, die deutlich von der bisher geläufigen Definition der Auslagerung nach MaRisk abweicht. So umfasst laut DORA der Begriff IKT-Dienstleistung grundsätzlich alle „digitalen Dienste und Datendienste, die über IKT-Systeme …dauerhaft bereitgestellt werden".

Im Gegensatz zur Definition der Auslagerung gemäß der MaRisk steht bei der Betrachtung von Drittbezugsrisiken nach DORA demnach nicht nur der direkte fachliche Bezug der Dienstleistung zu Bankgeschäften oder Finanzdienstleistungen im Fokus. Maßgeblich für die Risikobetrachtung nach DORA ist vielmehr die Frage, ob eine identifizierte IKT-Dienstleistung eine kritische oder wichtige Funktion innerhalb der Bank unterstützt.

Der Umgang mit Drittbezugsrisiken erfordert weiterhin eine detaillierte Due-Diligence-Prüfung vor Vertragsvergabe und ein kontinuierliches Monitoring, um sicherzustellen, dass die erforderlichen Sicherheitsstandards und die vereinbarten Leistungen eingehalten werden. Diese Prüfungen müssen um die neuen Anforderungen ergänzt werden.

Der kontinuierliche Überwachungsprozess mit darauf aufbauendem Reportingsystem muss erweitert werden, um zu gewährleisten, dass Risiken oder Schlechtleistungen zeitnah erkannt und gemanagt werden können. Regelmäßige Audits und Berichte sind erforderlich, um die Wirksamkeit der Maßnahmen zu bewerten und laufende Anpassungen vorzunehmen.

Eine der größten Chancen, die DORA bietet, ist die Möglichkeit, eine möglichst vollständige Übersicht der Drittbezugsrisiken – über die bekannten Risiken aus Auslagerungen hinaus - zu erlangen. Durch die detaillierte Analyse und Dokumentation der Risiken, die mit Drittanbietern verbunden sind, können Genossenschaftsbanken potenzielle Sicherheitslücken aufdecken und Maßnahmen zur Risikoreduktion implementieren.

Risikoanalyse

Die Anforderungen an die Risikoanalysen werden mit den Artikeln 28 und 29 konkreter und detaillierter beschrieben, als dies in bisherigen Regulatorik gefordert wurde. Zudem weichen die Anforderungen zu den noch weiterhin gültigen Anforderungen der MaRisk ab, sodass alle Anforderungen an Auslagerungen nach MaRisk genauso wie alle Anforderungen aus DORA an IKT-Dienstleistungen zu erfüllen sind.

Dies führt dazu, dass zu Beginn der Risikoanalyse bereits ermittelt werden muss, ob es sich um eine Auslagerung und/oder um eine IKT-Dienstleistung handelt. Bei der Inventarisierung und Berichterstattung der Risiken im Risikomanagement darf es durch die erweiterten Analysen nicht zu Dopplungen der Risken kommen.

Informationsregister

Ein weiteres zentrales Element des Drittparteienmanagements ist das Informationsregister, das alle relevanten IKT-Dienstleistungsverträge nach einer von der Aufsicht aufgesetzten Vorlage beinhalten muss. Alle Institute sind verpflichtet, die identifizierten IKT-Dienstleistungen einschließlich Informationen über die unterstützenden Funktionen, die vertraglichen Vereinbarungen sowie der damit verbundenen Risiken zu führen. Die notwendige detaillierte Dokumentation fordert einen hohen Initialaufwand. Die dann folgende laufende Aktualisierung wird zusätzliche Ressourcen binden.

Nicht nur die Vorlage ist hochkomplex, sondern auch die dazugehörigen Antwortoptionen und Vorgaben stellen die Institute vor

große Herausforderungen. So sind beispielsweise die Konzernstrukturen von IKT-Dienstleistern abzubilden und jede IKT-Art mit aufzuführen, die nicht unbedingt der Definition eines IKT-Systems entspricht. Im Gegensatz zum Auslagerungsregister müssen auch die IKT-Dienstleistungen, die keine kritische oder wichtige Funktion unterstützen, erfasst werden. Das neue Register bietet die Möglichkeit einer umfassenderen Übersicht über die Dienstleistungen bezüglich der IT-Landschaft des Instituts.

Die Erstellung und Pflege des Informationsregisters erfordert eine enge Zusammenarbeit zwischen den Fachbereichen und den Führungskräften der Genossenschaftsbanken. Darüber hinaus sind IKT-Dienstleister regelmäßig abzufragen, um sicherzustellen, dass das Register vollständig und aktuell ist (siehe Abbildung 2). Die Abbildung des Informationsregisters erfolgt im Laufe des Jahres nach Veröffentlichungen aller Anforderungen in ZAM-AR.

Vertragsanpassungen

Eine weitere sehr aufwändige Herausforderung ist die Anpassung der Verträge mit den IKT-Dienstleistern. Die Verträge mit IKT-Dienstleistern müssen alle regulatorischen Anforderungen und -verpflichtungen aus dem Artikel 30 der Verordnung, Artikel 9 und 11 des „RTS Policy on the use of ICT-Services“ und Artikel 7 des „RTS on subcontracting“ enthalten. Diese umfassen sowohl technische als auch organisatorische Maßnahmen sowie regelmäßige Audits und Berichte.

Zusätzlich zu generellen Anforderungen an die Verträge von IKT-Dienstleistungen gibt es verschärfende und detailliertere Mindestvertragsinhalte für IKT-Dienstleistungen, die eine kritische oder wichtige Funktion unterstützen.

DORA betont die Schulungspflichten für das Leitungsorgan sowie Sensibilisierung von Mitarbeitern und Dienstleistern für die digitale operationale Resilienz

Die Mindestvertragsinhalte sollen die Institute in die Lage versetzen, IKT-Drittbezugsrisiken schneller zu erkennen, etwa über die Angaben von Standorten der Datenverarbeitung, -speicherung und -bereitstellung. Zusätzlich ist damit eine entsprechende Sensibilisierung von IKT-Dienstleistern in Bezug auf IKT-Sicherheit gewährleistet.

Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, gibt es weitreichendere Vorgaben zu Unterauftragsvergaben und zu Sicherheitsstandards, beispielsweise Ausstiegspläne, Berechtigungsmanagement bezüglich Zugängen zu Daten und Räumlichkeiten, weitreichenderes Testmanagement. Die Vorgaben dienen dazu, die operationale Resilienz der Institute – insbesondere bei kritischen oder wichtigen Funktionen – zu stärken und diese in bessere Position für die Steuerung und Überwachung der IKT-Dienstleister zu versetzen.

Übersicht und Kontrolle

Ausgehend von den DORA-Mustervertragsklauseln des BVR wird die ZAM für die ZAM-gesteuerten Dienstleister auf die Umsetzung in den Standardverträgen hinwirken.

Die neuen Anforderungen aus DORA stellen mit ihrem Umfang und der Detailtiefe Banken vor große Herausforderungen. Mit dem immer noch andauernden Gesetzgebungsverfahren besteht zusätzlich noch nicht Klarheit über alle Anforderungen.

Doch es ergeben sich auch Chancen: Durch die klare und deutliche Formulierung der Anforderungen können Institute potenzielle Sicherheitslücken aufdecken sowie beheben. Mit einer durchdachten Klassifizierung und anschließendem Fokus auf kritische und wichtige Funktionen können Genossenschaftsbanken gezielt Ressourcen einsetzen und steuern.

Die systematische Implementierung eines umfassenden IKT-Risikomanagementrahmens und die Pflege eines Informationsregisters ermöglichen eine bessere Übersicht und Kontrolle über die IT-Landschaft der Institute und tragen zur Erhöhung der operationalen Resilienz bei.

Die enge Zusammenarbeit in der Genossenschaftlichen FinanzGruppe trägt zur erfolgreichen Umsetzung von DORA bei und führt dazu, dass die Gruppe sicherer, effizienter und resilienter wir. BI