Prof. Dr. Andreas Igl
TH Deggendorf

Synergien und Schnittstellen zwischen DORA und MaRisk im Kontext des IKT-Drittparteien- und Auslagerungsmanagements

Deggendorfer Notiz 2025/04 | April 2025

Einleitung

Die fortschreitende Digitalisierung und Modularisierung der Wertschöpfungsketten im Finanzsektor führt zu einer zunehmenden Abhängigkeit von externen Dienstleistern, insbesondere im Bereich der Informations- und Kommunikationstechnologie (IKT). Deutsche Kreditinstitute und Sparkassen stehen vor der Herausforderung, in dieser Hinsicht zwei regulatorische Rahmenwerke zu vereinen: die Verwaltungsvorschrift **Mindestanforderungen an das Risikomanagement (MaRisk)**, insbesondere AT 9 zum Auslagerungsmanagement, und die **Verordnung (EU) 2022/2554 über die digitale operationelle Resilienz (DORA)**, die seit dem 17. Januar 2025 ein spezifisches IKT-Drittparteienmanagement vorschreibt. Beide Regelwerke verfolgen das Ziel, Risiken im Zusammenhang mit externen Dienstleistern zu steuern, überschneiden sich jedoch in zahlreichen Anforderungen. Dies führt bei den verpflichteten Instituten zu Unsicherheiten und einem erheblichen Doppelaufwand. Die vorliegende Notiz analysiert die Überschneidungen und Unterschiede zwischen MaRisk und DORA, identifiziert Synergien und schlägt einen proaktiven Ansatz vor, um Doppelarbeiten zu minimieren. Sie richtet sich an Kreditinstitute, Sparkassen sowie prüfende Betriebswirte wie interne Revisoren, Verbandsprüfer und Wirtschaftsprüfer und beleuchtet, wie ein einheitlicher Umgang mit Drittparteien die regulatorische Effizienz steigern kann.

Überschneidungen zwischen MaRisk und DORA

Die MaRisk regeln in AT 9 das Auslagerungsmanagement umfassend, indem sie Anforderungen an die Übertragung von Aktivitäten oder Funktionen an Dritte, die Risikoanalyse, die Überwachung, die Auslagerungsverträge, das Risikomanagement, Kontrollverfahren, die Berichterstattung, Prüfungsrechte, das Proportionalitätsprinzip, die Notfallplanung sowie das Auslagerungsregister stellen. DORA hingegen fokussiert auf IKT-Drittparteien und legt detaillierte Vorgaben für das Risiko- und Vertragsmanagement, die Überwachung, die Notfallplanung und ein IKT-Drittparteienregister fest. Beide Regelwerke teilen

das Ziel, die Stabilität und Kontinuität der Finanzinstitute sicherzustellen, unterscheiden sich jedoch in ihrem Anwendungsbereich und ihrer Granularität.

Ein zentraler Überschneidungsbereich ist die **Risikoanalyse**. MaRisk fordert eine Bewertung der mit einer Auslagerung verbundenen Risiken, einschließlich operativer, rechtlicher und strategischer Risiken. DORA spezifiziert diese Anforderung für IKT-Dienstleister, indem es eine Bewertung von Konzentrationsrisiken, Abhängigkeiten und potenziellen Systemausfällen vorschreibt. Beide Ansätze erfordern eine strukturierte Identifikation und Bewertung von Risiken, unterscheiden sich jedoch in der Tiefe der IKT-spezifischen Analyse unter DORA.

Ein weiterer Bereich ist der **Auslagerungsvertrag**. MaRisk verlangt eine schriftliche Vereinbarung, die die Rechte und Pflichten der Parteien, einschließlich Prüfungsrechten und Notfallmaßnahmen, klar definiert. DORA geht darüber hinaus und legt detaillierte Mindestanforderungen an IKT-Verträge fest, etwa zu Kündigungsrechten, Datenschutz und Unterauftragsvergabe. Während MaRisk allgemeiner bleibt, sind die Vorgaben von DORA spezifischer und technisch detaillierter, was bei IKT-Auslagerungen zu einer erhöhten Dokumentationslast führt.

Die **Überwachung** ausgelagerter Aktivitäten ist ein weiteres gemeinsames Element. MaRisk schreibt eine kontinuierliche Kontrolle der Dienstleisterleistung und -risiken vor, während DORA zusätzlich spezifische Überwachungsmechanismen für IKT-Dienstleister verlangt, etwa regelmäßige Berichte und Audits. Diese Überschneidung führt häufig dazu, dass Institute ähnliche Kontrollprozesse doppelt implementieren, obwohl eine Integration möglich wäre.

Das **Risikomanagement** ist ebenfalls ein Kernbereich beider Regelwerke. MaRisk fordert Prozesse zur Identifikation, Steuerung und Minderung von Auslagerungsrisiken, während DORA ein umfassendes IKT-Risikomanagement mit Fokus auf Cyberrisiken, Abhängigkeiten und Konzentrationsrisiken vorschreibt. Die DORA-Vorgaben sind hier präziser, bauen jedoch auf ähnlichen Prinzipien wie MaRisk auf, was eine Harmonisierung erleichtert.

Kontrollverfahren sind ein weiterer Überschneidungspunkt. MaRisk verlangt interne Mechanismen zur Sicherstellung der Einhaltung regulatorischer Anforderungen, während DORA spezifische Kontrollen für IKT-Dienstleister vorschreibt, etwa zur Sicherstellung der Datensicherheit und Resilienz. Die zugrunde liegenden Prinzipien sind vergleichbar, doch die technische Ausgestaltung unter DORA erfordert zusätzliche Ressourcen.

Die **Berichterstattung** ist ebenfalls ein gemeinsames Thema. MaRisk fordert regelmäßige Berichte über den Status und die Risiken von Auslagerungen, während DORA detaillierte Berichtspflichten für IKT-Dienstleister einführt, etwa zu Zwischenfällen und Vertragsänderungen. Die parallele Berichterstattung führt zu einem erhöhten administrativen Aufwand, der durch einheitliche Berichtsformate reduziert werden könnte.

Prüfungsrechte sind ein weiterer Bereich der Überschneidung. MaRisk gewährt Instituten das Recht, Audits beim Dienstleister durchzuführen, während DORA dies für IKT-Dienstleister konkretisiert und erweitert, etwa durch Regelungen zur grenzüberschreitenden Prüfung. Beide Regelwerke zielen auf eine wirksame Kontrolle ab, doch die DORA-Anforderungen sind spezifischer.

Die **Notfallplanung** ist ein weiteres Beispiel. MaRisk fordert Maßnahmen zur Sicherstellung der Kontinuität bei Störungen, während DORA detaillierte Vorgaben für IKT-Notfallpläne macht, etwa zu Wiederherstellungszeiten und Backup-Systemen. Die Zielsetzung ist identisch, doch die DORA-Regelungen sind technisch detaillierter.

Das **Informationsregister** bzw. **Auslagerungsregister** ist ein zentraler Punkt der Doppelregulierung. MaRisk verlangt ein Register aller Auslagerungen, während DORA ein spezifisches Register für IKT-Dienstleister vorschreibt, das zusätzliche Details wie Vertragslaufzeiten und Risikokategorien enthält. Die parallele Führung beider Register führt zu einem erheblichen administrativen Aufwand.

Synergien und proaktiver Ansatz

Die genannten Überschneidungen verdeutlichen, dass MaRisk und DORA in vielen Bereichen ähnliche Ziele verfolgen, jedoch unterschiedliche Schwerpunkte setzen. Um den Doppelaufwand zu minimieren, empfiehlt sich ein proaktiver Ansatz, der Schnittstellen nutzt und Synergien schafft. Ein erster Schritt besteht darin, Drittparteien grundsätzlich einheitlich zu betrachten, bevor eine Differenzierung zwischen IKT- und Nicht-IKT-Dienstleistern erfolgt. Dieser Ansatz ermöglicht eine einheitliche Governance-Struktur, die sowohl MaRisk- als auch DORA-Anforderungen abdeckt.

Für IKT-Dienstleister bietet DORA präzisere Vorgaben, die auch für wesentliche Auslagerungen unter MaRisk relevant sind. Beispielsweise können die detaillierten Vertragsanforderungen von DORA als Blaupause für alle Auslagerungsverträge dienen, wodurch einheitliche Standards geschaffen werden. Ebenso kann das IKT-Risikomanagement nach DORA als Grundlage für ein umfassendes Auslagerungsrisikomanagement genutzt werden, das auch Nicht-IKT-Dienstleister abdeckt. Die Überwachungsmechanismen von DORA, etwa regelmäßige Audits und Berichte, lassen sich auf andere Dienstleister übertragen, um ein konsistentes Kontrollsystem zu etablieren.

Ein weiterer Ansatz ist die Integration der Register. Statt separate Register für MaRisk und DORA zu führen, können Institute ein einheitliches Drittparteienregister entwickeln, das alle relevanten Informationen konsolidiert. Dies erfordert eine initiale Investition in Datenmanagement, reduziert jedoch langfristig den Aufwand. Zudem kann das

Proportionalitätsprinzip, das beide Regelwerke berücksichtigen, genutzt werden, um Anforderungen an die Größe und Komplexität des Instituts anzupassen und Überregulierung zu vermeiden.

Die Notfallplanung bietet ebenfalls Synergiepotenzial. Die detaillierten Vorgaben von DORA zu Wiederherstellungszeiten und Backup-Systemen können als Standard für alle Dienstleister dienen, wodurch die Kontinuität über alle Auslagerungen hinweg gesichert wird. Ähnlich lassen sich die Prüfungsrechte unter DORA als Vorbild für einheitliche Auditprozesse nutzen, die sowohl IKT- als auch Nicht-IKT-Dienstleister abdecken.

Herausforderungen und Übergangsphase

Trotz der Synergiepotenziale bleibt die parallele Anwendung von MaRisk und DORA eine Herausforderung. Die BaFin hat im Rahmen eines Workshops am 6. März 2025 darauf hingewiesen, dass die EBA-Guidelines on Outsourcing Arrangements derzeit überarbeitet werden, um Doppelregulierungen zu vermeiden. EIOPA und ESMA prüfen ebenfalls Schritte in diese Richtung, und eine Anpassung nationaler Rundschreiben wird erwartet. Bis diese Harmonisierung abgeschlossen ist, stehen Institute vor einem unbefriedigenden Zustand, der zusätzliche Ressourcen bindet.

Für prüfende Betriebswirte wie interne Revisoren, Verbandsprüfer und Wirtschaftsprüfer stellt die Übergangsphase ein „moving target“ dar. Angesichts der sich überschneidenden Anforderungen empfiehlt sich ein risikobasierter Prüfansatz, der auf Stichproben basiert und weniger prüfend als beratend agiert. Dies ermöglicht es, Schwachstellen zu identifizieren, ohne Institute mit übermäßigen Anforderungen zu belasten.

Empfehlungen für Kreditinstitute und Verbände

Kreditinstitute und Sparkassen sollten das Thema Drittparteien strategisch angehen und aus beiden Regelwerken – MaRisk und DORA – „das Beste“ nutzen. Ein breiteres Verständnis von Dienstleistern, das über IKT hinausgeht, erleichtert die Entwicklung einheitlicher Prozesse. Konkret sollten Institute Kompetenzen und Kapazitäten im Drittparteienmanagement aufbauen, da die Bedeutung externer Anbieter in einer modularisierten Wertschöpfungskette weiter zunimmt. Eine hohe DORA-Compliance fördert zudem die Erfüllung der MaRisk-Anforderungen, da viele DORA-Vorgaben die MaRisk-Regeln spezifizieren und ergänzen.

Empfehlenswert ist die Einrichtung eines zentralen Drittparteienmanagements, das sowohl IKT- als auch Nicht-IKT-Dienstleister abdeckt. Dies umfasst ein konsolidiertes Register, standardisierte Verträge, einheitliche Risikoanalysen und integrierte Überwachungsprozesse. Durch Investitionen in Automatisierung, etwa durch Governance-, Risk- und Compliance-Tools, lässt sich der administrative Aufwand weiter reduzieren. Zudem sollten Institute aktiv an Konsultationen der EBA und BaFin teilnehmen, um die Harmonisierung der Regelwerke mitzugestalten.

Empfehlungen für prüfende Betriebswirte

Für Revisoren, Verbandsprüfer und Wirtschaftsprüfer ist Flexibilität entscheidend. Ein risikobasierter Ansatz, der auf Stichproben und wesentlichen Risiken fokussiert, ist in der Übergangsphase zielführend. Statt strikter Prüfungen sollten Prüfer „beratend“ tätig werden und Institute bei der Integration von MaRisk- und DORA-Anforderungen unterstützen. Dies schließt die Bewertung von Synergiepotenzialen, die Überprüfung von Registern und die Analyse von Notfallplänen ein. Langfristig wird die Harmonisierung der Regelwerke die Prüfprozesse vereinfachen, doch bis dahin ist eine pragmatische Herangehensweise erforderlich.

Fazit

Die parallele Anwendung von MaRisk und DORA stellt Kreditinstitute, Sparkassen und prüfende Betriebswirte vor Herausforderungen, bietet jedoch auch Chancen. Durch die Identifikation von Synergien, etwa in der Risikoanalyse, der Vertragsgestaltung, der Überwachung und der Notfallplanung, lässt sich der Doppelaufwand reduzieren. Ein einheitlicher Ansatz im Drittparteienmanagement, der IKT- und Nicht-IKT-Dienstleister integriert, schafft langfristige Effizienz. Institute sollten Kompetenzen aufbauen, standardisierte Prozesse etablieren und aktiv an der Harmonisierung der Regelwerke mitwirken. Prüfer sollten risikobasiert und beratend agieren, um Institute in der Übergangsphase zu unterstützen. Eine hohe DORA-Compliance stärkt nicht nur die digitale Resilienz, sondern erleichtert auch die Erfüllung der MaRisk-Anforderungen, wodurch Institute ihre regulatorische Robustheit nachhaltig steigern können.

Prof. Dr. Andreas Igl
BDO-Stiftungsprofessor an der TH Deggendorf
Lehrbeauftragter an der Hochschule der Deutschen Bundesbank

andreas.igl@th-deg.de
(Mobil): 0151 2301 8610
(LinkedIn): Link