Wertpapierhäusern, Zahlungsinstituten und IT-Dienstleistern wie das deutsche Finanzsystem einem schweren Cyberangriff effektiv und abgestimmt begegnen und im Ernstfall schnell und vor allem koordiniert entscheiden könnte.[24] Aufsichtsrechtlich steckt der EU Digital Operational Resilience Act (DORA) den regulatorischen Rahmen ab, auf dessen Grundlage die BaFin dafür sorgt, dass die Finanzunternehmen in Deutschland zur Abwehr von Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie (IKT) künftig besser aufgestellt und widerstandsfähiger sind – ab 17. Januar 2025 wird die EU-Verordnung für mehr als 3 500 Unternehmen im deutschen Finanzsektor verbindlich.[25]

„Aufsichtsrechtlich steckt der DORA den regulatorischen Rahmen ab."

Die regulatorischen Schwerpunkte von DORA sind in Abbildung 2 dargestellt.

Neben den Anforderungen an die internen Unternehmensbereiche und -verfahren stehen vor allem die Risiken aus IT-Dienstleistungen Dritter im Fokus, denn Unzulänglichkeiten in den komplexen IT-Auslagerungsvereinbarungen bei zunehmender Abhängigkeit von externen Anbietern können zu neuen Konzentrationsrisiken führen – eine wesentliche Schwachstelle, die auch die EZB unter anderem mit der Analyse von Auslagerungsregistern zur Ermittlung von Verflechtungen zwischen beaufsichtigten Instituten und externen Anbietern sowie gezielten Überprüfungen von Auslagerungsvereinbarungen in Angriff nehmen wird.

Gerade was die Überwachung von kritischen Dienstleistern und den Einfluss auf große internationale Cloud-Anbieter angeht, erwartet die BaFin durch DORA jedenfalls eine deutliche Verbesserung: künftig dürften Verflechtungen und Marktkonzentrationen bei Dienstleistern viel besser erkannt und gemeinsam europäisch überwacht werden. Um eine vorausschauende und effektive Aufsicht sicherzustellen, sieht der Entwurf des Finanzmarktdigitalisierungsgesetzes vor, die Einhaltung der Vorschriften von DORA im Rahmen der Jahresabschlussprüfung zu prüfen. Offen ist aktuell noch, inwieweit es durch diese geplanten Gesetzesänderungen zu Überschneidungen in den Jahresabschlussprüfungen durch Prüfungshandlungen zur Einhaltung der Anforderungen aus BAIT, KAIT und ZAIT kommen wird.[26]

Die Institute werden die Zeit bis Januar 2025 auf jeden Fall gut nutzen müssen: Das gesamte IKT-Risikomanagement muss einer Reifegradprüfung unterzogen werden und gegebenenfalls auf ein neues Level gehoben werden, um die Vielzahl der (auch technischen Vorgaben) umzusetzen. Dies betrifft insbesondere die Dienstleistungen Dritter, denn auch dort müssen Risiken bekannt, analysiert und überwacht werden beziehungsweise darüber nachgedacht werden, wie Exit-Maßnahmen und -Strategien aussehen können. Nicht zu vergessen, dass hier noch umfangreiche Level-2-Dokumente der EBA in Form von RTS, Leitlinien und Empfehlungen ausstehen. Dabei ist der Weg zur digitalen operationellen Resilienz nicht nur Aufgabe der IT, sondern auch des Risikomanagements – und damit Chefsache.[27]

Krisenmanagement für den Ernstfall

Mit überarbeiteten Rundschreiben und Konsultationen geht die BaFin die Verbesserung der Abwicklungsfähigkeit der Institute an.[28] Dabei werden die bereits auf europäischer Ebene für Institute unter Zuständigkeit des Single Resolution Board (SRB) überarbeiteten EBA/GL/2023/05 (anwendbar ab dem 1. Januar 2024) berücksichtigt. Die Institute sind dazu aufgefordert – basierend auf den vorab festgelegten Abwicklungsstrategien – ihre Abwicklungsfähigkeit herzustellen oder zu verbessern. Dabei erhöht sich der Umfang und Detaillierungsgrad der aufsichtlichen Anforderungen und macht eine intensive Auseinandersetzung mit den unterschiedlichen Dimensionen der Abwicklungsfähigkeit unerlässlich.

Die BaFin erwartet von den Instituten, dass sie ihre Abwicklungsfähigkeiten testen und wird ebenfalls Tests mit den Instituten durchführen, die später in ein mehrjähriges Testprogramm der Abwicklungsplanung überführt werden. Mögliche (auch kombinierbare) Testmethoden sind dabei: Selbsteinschätzung, Walkthrough, Prüfung durch die Interne Revision, Dry Run (Testlauf), Bestätigung durch einen unabhängigen Dritten, Vor-Ort-Besuch oder Krisenübung.

Abwicklung erleichtern

Die Abwicklung von kleineren und mittelgroßen Banken in Schieflage zu erleichtern, steht im Fokus eines Vorschlags der EU-Kommission zur Anpassung und Stärkung des bestehenden EU-Rahmens für das Krisenmanagement im Bankensektor.[29] Gerade mittelgroße und kleinere Banken würden bei Ausfall häufig nicht abgewickelt, sondern andere Lösungen zulasten der Steuerzahler zum Einsatz kommen.

„Die BaFin erwartet von den Instituten, dass sie ihre Abwicklungsfähigkeiten testen."

Der Kommissionsvorschlag soll die Behörden in die Lage versetzen, ausfallende Banken unabhängig von ihrer Größe und ihrem Geschäftsmodell in einen geordneten Marktaustritt zu führen, und gibt ihnen diesbezüglich eine breite Palette von