Dabei bringt die Nachhaltigkeitsberichterstattung viele neue Anforderungen: Die Daten müssen rechtzeitig erhoben und auf Wesentlichkeit analysiert werden, Reporting-Strategien und Systeme der Finanzberichterstattung werden sich nur bedingt auf die Nachhaltigkeitsberichterstattung übertragen lassen.[21)] Die Geschäftsführung wird auch die Nachhaltigkeitsberichterstattung überwachen und mit Blick auf den Anwendungszeitpunkt vorantreiben müssen, denn die BaFin prüft künftig die Nachhaltigkeitsberichterstattung als Teil des Lageberichts von kapitalmarktorientierten Unternehmen im Rahmen der Bilanzkontrolle.

Schwachstelle operative Resilienz

Die operative Widerstandsfähigkeit der Institute bei fortschreitender Digitalisierung des Geschäftsbetriebs und ihres Leistungsangebots ist für 2024 ein weiteres Fokusthema. Die EZB testet seit dem 2. Januar 2024 im Rahmen eines Stresstests zur Cyberresilienz, inwieweit die Institute in der Lage sind, auf einen erfolgreichen Cyberangriff, der Störungen im Tagesgeschäft verursacht, zu reagieren und sich davon zu erholen.[22)] In diesen qualitativen Test sind 109 direkt beaufsichtigte Institute einbezogen, 28 davon werden im Testverlauf eingehender geprüft. Rund 500 Fragen müssen von allen betroffenen Instituten beantwortet werden: Es geht um das Security-Incident-Response-Verfahren, also um die Meldung eines simulierten Cybervorfalls, die Nachweisbarkeit der Reaktionsfähigkeit im Rahmen der internen Richtlinien, Wiederherstellungsprozesse und Notfallpläne. Darüber hinaus werden auch potenzielle Auswirkungen und quantitative Bewertungen der Risiken im operationellen Bereich gefragt.

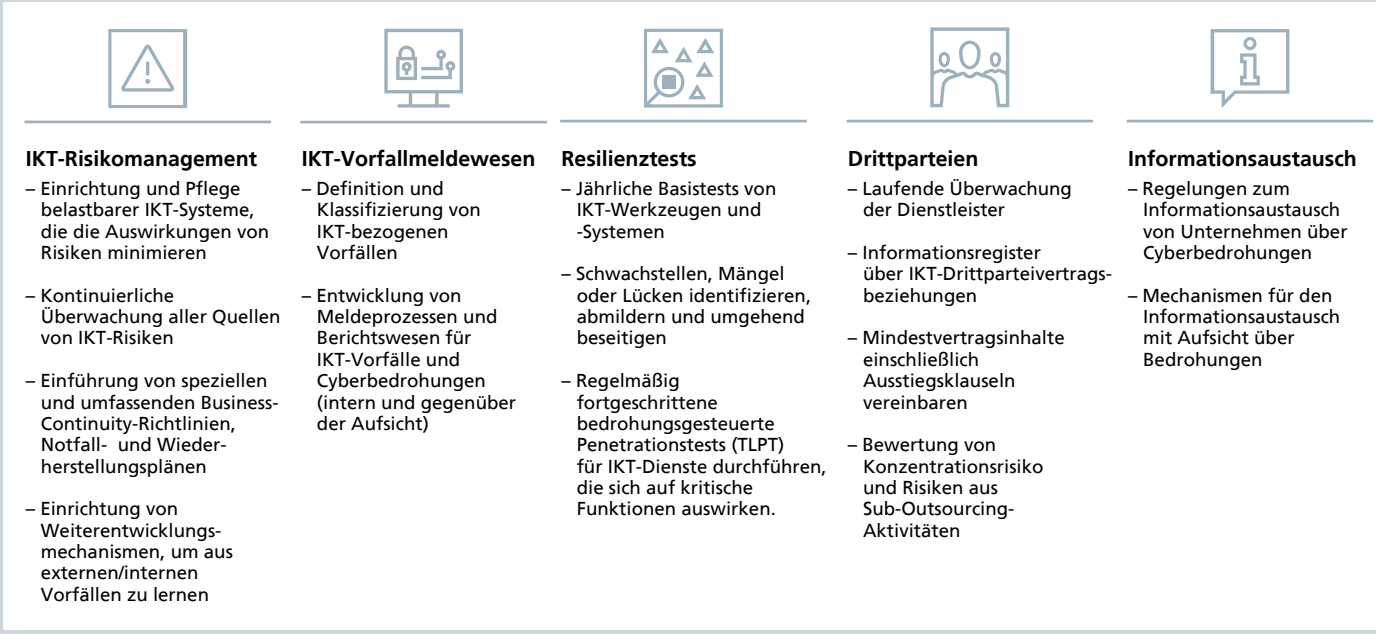
Beide Themenkomplexe erfordern eine detaillierte, umfangreiche und vollständige Dokumentation aller Verfahren, Methoden und Verantwortlichkeiten. Bis zum 29. Februar 2024 haben die Institute Zeit, den Fragenkatalog zu beantworten. Für die 28 Institute im vertieften Testverfahren geht es weiter: Sie müssen einen umfassenden IT-Recovery-Test durchführen. In beiden Testläufen müssen sich Institute auf Nachfragen, Validierungen und vor allem Nachbesprechungen mit der Aufsicht einstellen, denn die gewonnen Erkenntnisse sollen 2024 in die allgemeine aufsichtliche Beurteilung des SREP einfließen und die Ergebnisse beziehungsweise die daraus gezogenen Lehren mit den einzelnen Banken besprochen werden.

Nicht nur eine rein regulatorische Aufgabe

Letztlich sollten die Institute also die Chance nutzen, den Cyberresilienztest nicht nur als rein regulatorische Übung zu sehen, sondern ihre Widerstandsfähigkeit tatsächlich auf ein neues Level zu heben, zumal im aktuellen geopolitischen Umfeld die Zahl der gemeldeten Cyberangriffe zuletzt sprunghaft angestiegen ist.[23)] Darüber hinaus dürften alle Anstrengungen, die über Standardverfahren zur Quantifizierung von operationellen Risiken hinausgehen, ein lohnendes Investment für zukünftige regulatorische Anforderungen und aufsichtliche Erwartungen sein, die in diesem Bereich eher steigen werden.

Institute, die nicht unter EZB-Aufsicht stehen, dürfen sich beim Thema Cyberresilienz kaum entspannt zurücklehnen, denn auch die deutsche Aufsicht läuft sich schon mal warm für kommende Aufgaben: Im Rahmen einer Cyberkrisenübung probten BaFin zusammen mit Behörden und Banken, Versicherern,

Abbildung 2: Regulatorische Schwerpunkte von DORA



Quelle: PwC