ppi

Expert Summary

Digital Operational Resilience Act

Legislativvorschläge zur Betriebsstabilität digitaler Systeme

Dr. Selvam Dhamotharan,
Tim Glenewinkel

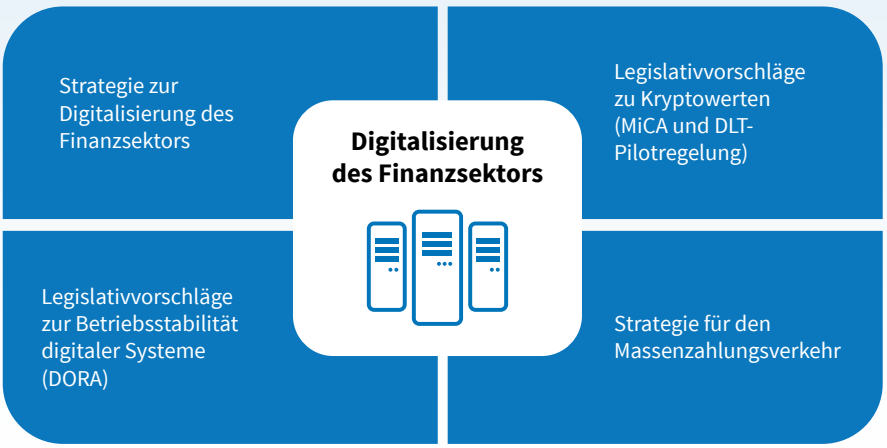
Die EU plant einheitliche, sektorübergreifende Regelungen für das Management und die Minderung der IT-Risiken in Finanzunternehmen. Dazu gehört der Digital Operational Resilience Act (DORA). Die Vorgaben sind dazu gedacht, das vorherrschende uneinheitliche Netz aus nationalen Regelungen zu konsolidieren. Hiervon betroffen sind zum einen traditionelle Marktakteure wie Banken, Versicherungen und Investmentgesellschaften. Zum anderen werden sich die Regelungen auch auf Fin- und BigTechs erstrecken, die beispielsweise Zahlungen, Versicherungen und IT-Dienstleistungen anbieten.

INHALT

Ausgangslage

Am 24. September 2020 hat die Europäische Kommission ein neues Paket zur Digitalisierung des Finanzsektors angenommen. Dieses besteht aus vier Bausteinen (siehe Grafik) und soll den Verbrauchern mehr Auswahl und Möglichkeiten bei Finanzdienstleistungen und modernen Zahlungsweisen bieten. Gleichzeitig gewährleistet es Verbraucherschutz und Finanzstabilität. Der Vorschlag der Kommission bedarf noch der Zustimmung der beiden gesetzgebenden EU-Organe, also des Europäischen Parlaments und des Rats.

EU-Paket zur Digitalisierung des Finanzsektors



Quelle: PPI AG

Die vier Bausteine des Pakets der Europäischen Kommission zur Digitalisierung des Finanzsektors.

Minderung der IT-Risiken durch strenge und gemeinsame Regeln

Ob digitale Transformation, gewachsene Prozesse in Großrechnerstrukturen oder neue Dienstleistungen durch FinTechs – so vielfältig die IT-Landschaft, -Ausgangslage und -Ziele, so vielfältig die Risiken. Die neue EU-Verordnung soll all diesen Strukturen gerecht werden und die digitale operative Resilienz stärken.

DORA soll den unterschiedlichen Risikoarten eines diversifizierten Marktes gerecht werden.

Der Entwurf fordert die Einführung:

- von speziellen Risikomanagementfähigkeiten hinsichtlich der Infomations- und Kommunikationstechnologie (IKT),
- der Meldung schwerwiegender IKT-bezogener Vorfälle,
- von Tests der Betriebsstabilität digitaler Systeme,
- eines Managements von IKT-Risiken Dritter durch Finanzunternehmen,
- der Aufsicht über Drittanbieter kritischer IKT-Dienstleistungen sowie
- eines Informationsaustauschs zwischen Finanzunternehmen.

Das Dokument betrifft ein breites Spektrum von Finanzunternehmen – von Kreditinstituten und Investmentfonds bis hin zu Anbietern von Kryptodienstleistungen. Damit ist im EU-Raum erstmals ein einheitliches und kohärentes Framework für den Umgang mit IKT-Risiken in der gesamten Finanzbranche vorgesehen.

Erstmals soll der Umgang mit IKT-Risiken in der EU nach einheitlichen Regeln erfolgen.

- Alle Finanzunternehmen unterliegen betrieblichen Belastbarkeitsanforderungen, um ein sicheres, sektorübergreifendes Finanzsystem zu gewährleisten.
- Es gibt eine regulatorische Aufsicht für kritische IKT-Drittanbieter wie Cloud-Computing-Dienste, um sicherzustellen, dass sie keine unangemessenen Betriebsrisiken für Finanzinstitute darstellen.
- Von traditionellen Marktakteuren – Banken, Versicherungen und Investmentgesellschaften – bis hin zu FinTechs und BigTechs, die Zahlungen, Sparpläne oder Versicherungen anbieten, ist jeder der Aufsicht unterstellt.
- Die Aufsichtsbehörden werden verstärkt in der Lage sein, Risiken im Finanzsystem zu vermeiden und somit die finanzielle Stabilität besser zu schützen.

Besondere Beachtung findet der Grundsatz „Gleiche Tätigkeit, gleiches Risiko, gleiche Regeln“. Dies dient dem Verbraucherschutz und stellt einheitliche Wettbewerbsbedingungen für bestehende Finanzinstitute und neue Marktteilnehmer sicher.

Es gilt der Grundsatz: Wer das Gleiche anbietet unterliegt auch den gleichen Vorschriften.

Digitalisierung des Finanzsektors – wachsende Angriffsfläche für Cyberattacken

Finanzunternehmen sind im Besitz umfangreicher und vielfältiger Bestände an personenbezogenen und Finanzdaten wie etwa Angaben über Bankkonten oder Anlagen sowie Versicherungsdaten. Die ständig steigende Abhängigkeit des Finanzsektors von Software und digitalen Prozessen bringt es mit sich, dass das Finanzwesen mit IKT-Risiken konfrontiert ist. Auf Finanzunternehmen werden gezielt Cyberangriffe unternommen, die schwerwiegende finanzielle und Reputationsschäden für die Unternehmen und deren Kunden zur Folge haben können. Allein während der Covid-19-Pandemie ist die Zahl von Cyberangriffen auf Finanzinstitute um 38 Prozent gestiegen. Daher stimmen die nationalen Finanzaufsichtsbehörden in der gesamten EU sowie die europäischen Aufsichtsbehörden darin überein, dass Finanzunternehmen mit ausgereiften und modernen Fähigkeiten ausgestattet sein müssen. Nur so können sie die Vorteile des digitalen Wandels in vollem Umfang nutzen und gleichzeitig die sich daraus ergebenden Risiken minimieren.

Während der Corona-Pandemie nahm die Zahl der Cyberangriffe auf Finanzinstitute um mehr als ein Drittel zu.

Der Einsatz von IKT hat dadurch in den vergangenen Jahrzehnten eine zentrale Rolle im Finanzwesen erlangt und nimmt heute eine entscheidende Position bei allen Finanzinstituten ein, wenn es um den Betrieb typischer Alltagsfunktionen geht. Der existierende Flickenteppich an nationalen Vorgaben und Standards in der EU macht es vor allem international agierenden Finanzunternehmen schwer, einheitliche, angemessene Prozesse zu etablieren. DORA, Teil des EU-Pakets zur Digitalisierung des Finanzsektors, fasst die Vielzahl an Bestimmungen zum ersten Mal in konsistenter Weise in einem einzigen Rechtsakt zusammen.

Vor allem Interntional tätige Finanzinstitute tun sich mit der Entwicklung einheitlicher Prozesse oft schwer – schuld ist das Sammelsurium nationaler Vorschriften.

Betriebsstabilität operativer Systeme

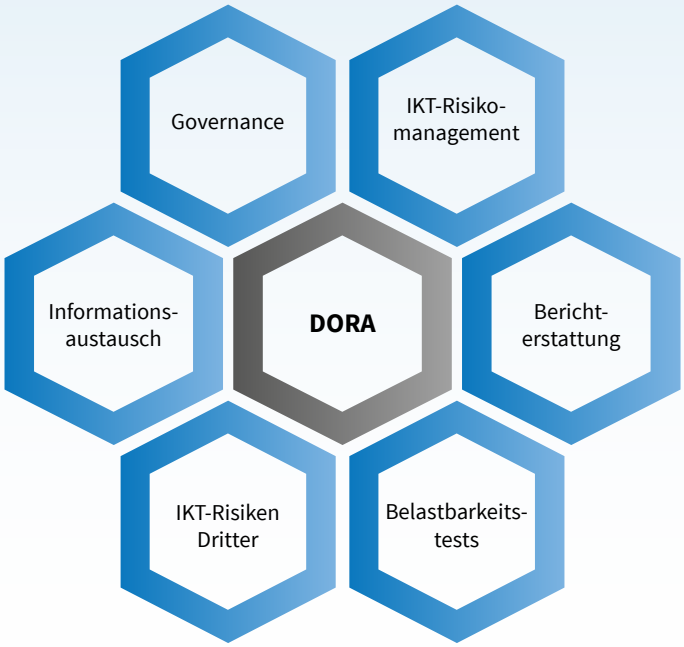
DORA wird mit dem Ziel eingeführt, die Betriebsstabilität operativer Systeme zu gewährleisten und zu verbessern. Damit ist die Fähigkeit von Unternehmen gemeint, allen Arten von Störungen und Bedrohungen im Zusammenhang mit Informations- und Kommunikationstechnologien zu widerstehen. Dem dienen die

Festlegung von Standards und eine optimierte Koordinierung der Regulierungs- und Aufsichtsarbeit. DORA unterstützt und stärkt das digitale Finanzwesen bei Innovation und Wettbewerb und hilft, die IKT-Risiken zu mindern.

Stärkung der digitalen operativen Resilienz

DORA ist für ein breites Spektrum der Finanzunternehmen – von Kreditinstituten, Versicherungen und Investmentfonds bis hin zu Anbietern von Kryptodienstleistungen – relevant. Die Ausgestaltung der Richtlinie lässt sich in sechs Bereiche einteilen.

Ausgestaltung der DORA-Richtlinie



Quelle: PPI AG

Die Richtlinie Digital Operational Resilience Act (DORA) fokussiert sechs betriebliche Arbeitsfelder.

Gewährleistung der Governance (Artikel 4)

Für das Leitungsorgan sieht DORA eine entscheidende, aktive Rolle bei der Lenkung und Steuerung des IKT-Risikomanagements vor. Seine Aufgabe ist es, die Einhaltung des Risikorahmens sicherzustellen und ein striktes Befolgen der Cybergovernance zu gewährleisten. Das Leitungsorgan ist gefordert, die Geschäftsstrategie an die Durchführung des IKT-Risikomanagements anzugleichen und Kohärenz herzustellen. Dazu zählt ein kontinuierliches Engagement bei dessen

Die Geschäftsleitung ist für die strikte Einhaltung der IKT-Richtlinien verantwortlich.

Kontrolle und Überwachung sowie eine klare Zuweisung von Rollen und Verantwortlichkeiten im Zusammenhang mit IKT-Funktionen. Weiterhin ist eine angemessene Bereitstellung von Geldern für Investitionen in die IKT-Sicherheit sowie Schulungsmaßnahmen für die Angestellten zu garantieren.

Für die Cybersicherheit müssen die notwendigen Mittel bereitgestellt werden.

Anforderungen an das IKT-Risikomanagement (Artikel 5 bis 14)

Die in DORA aufgeführten Anforderungen an das IKT-Risikomanagement beziehen sich auf spezifische Fähigkeiten und Funktionen, die Finanzunternehmen zukünftig erreichen beziehungsweise erfüllen müssen. Die Forderungen orientieren sich an internationalen, nationalen und branchenspezifischen Normen, Richtlinien und Empfehlungen. Dazu gehören etwa

- die Identifizierung von Bedrohungen,
- der Schutz vor Angriffen,
- die Angriffsprävention,
- die Aufdeckung von Schwachstellen,
- eine angemessene Reaktion auf Sicherheitsvorfälle,
- die Wiederherstellung der Geschäftstätigkeit,
- der Wissenserwerb über Bedrohungsszenarien,
- die Weiterentwicklung der Abwehrfähigkeit sowie
- die angemessene interne und externe Kommunikation über Vorfälle.

Pläne zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung der Geschäftstätigkeit sind erforderlich, um es den Finanzinstituten zu ermöglichen, IKT-Vorfälle umgehend zu lösen. Die genaue Ausgestaltung der IKT-Risikomanagementmodelle steht dabei den Instituten frei, sodass die Modelle auf die individuellen Bedürfnisse eines Instituts angepasst werden können.

Notfallpläne sind in jedem Fall aufzustellen und sollen dazu beitragen, IKT-Vorfälle schnell zu bereinigen.

Im Detail werden Finanzunternehmen zu den nachfolgenden Punkten verpflichtet:

- Etablierung und Unterhaltung von stabilen und widerstandsfähigen IKT-Systemen und -Instrumenten, wodurch IKT-Risiken zuverlässig minimiert werden
- Sicherstellung einer ausreichenden Kapazität, um mit den sich entwickelnden Cyberbedrohungen Schritt halten zu können
- Kontinuierliche Identifizierung von IKT-Risikoquellen und Einführung von Schutz- und Präventionsmaßnahmen
- Sicherstellung, dass anomale Aktivitäten zeitnah aufgedeckt werden
- Erarbeitung und Einführung von dedizierten und umfassenden Strategien zur Kontinuität des Geschäftsbetriebs
- Einführung von Notfallplänen als fester Bestandteil der einschlägigen operativen Strategie zur raschen Wiederherstellung nach IKT-bezogenen Vorfällen sowie Gewährleistung der Integrität, Sicherheit und Belastbarkeit physischer Infrastrukturen und Einrichtungen
- Verwendung europäischer und international anerkannter technischer Normen, zum Beispiel ISO, oder bewährter Praktiken der Industrie durch die Finanzinstitute – sofern deren Verwendung in vollem Einklang mit den spezifischen aufsichtsrechtlichen Anweisungen zur Verwendung und Übernahme internationaler Normen steht

Berichterstattung über IKT-bezogene Vorfälle (Artikel 15 bis 20)

Neben dem Aufbau eines wirkungsvollen Rahmens zum Management von IKT-Risiken wird in DORA die Meldung von IKT-bezogenen Vorfällen definiert. Finanzunternehmen müssen ein Managementverfahren zur Überwachung, Klassifizierung und Meldung schwerwiegender IKT-Vorfälle an die zuständigen Behörden einführen. Ziel ist, die Meldung für alle Finanzinstitute zu harmonisieren und größere Vorfälle mit IKT-Bezug durch aufsichtliches Feedback zu ergänzen. Empfänger der Meldungen sind die zuständigen nationalen Behörden. Sie müssen anderen Einrichtungen oder Ämtern – etwa den zentralen

DORA konkretisiert die Meldepflichten für IKT-Vorfälle und fordert ein entsprechendes Managementverfahren.

Anlaufstellen gemäß der Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie), der EZB oder den ESA (European Supervisory Authorities) – sachdienliche Einzelheiten und Angaben über IKT-bezogene Vorfälle übermitteln.

Die nationalen Behörden sind weiterhin verpflichtet, alle notwendigen Rückmeldungen oder Anleitungen an die Finanzinstitute zu geben und Orientierungshilfen zu bieten. Aufgabe der ESA ist es, anonymisierte Daten über Bedrohungen und Schwachstellen im Zusammenhang mit einem Vorfall weiterzugeben. So wird eine breitere kollektive Verteidigung unterstützt. Weiterhin ist geplant, die Berichterstattung über IKT-bezogene Vorfälle auf EU-Ebene zu zentralisieren. Finanzinstitute sind immer noch verpflichtet, Erst-, Zwischen- und Abschlussberichte einzureichen sowie Nutzer und Kunden zu informieren, falls der Vorfall Auswirkungen auf deren finanzielles Interesse haben könnte.

Digitale operationelle Belastbarkeitstests (Artikel 21 bis 24)

Ein wichtiger Aspekt zur erfolgreichen Umsetzung eines effektiven IKT-Risikomanagements ist der Test der implementierten Systeme, Prozesse und Strukturen. Darin wird überprüft, ob die Finanzinstitute in der Lage sind, Schwächen, Mängel oder Lücken zu erkennen und Probleme zu lösen. Dies ist die Voraussetzung, um eine im Einklang mit internationalen Standards robuste digitale operative Belastbarkeit zu erreichen.

IKT-Systeme müssen regelmäßig auf Präventions-, Erkennungs-, Reaktions- und Wiederherstellungsfähigkeiten getestet werden, um potenzielle IKT-Schwachstellen aufzudecken und zu beheben.

IKT-Systeme müssen regelmäßig Tests auf potenzielle Schwachstellen durchlaufen.

Entsprechend muss sich auch das zuständige Personal Tests unterziehen. Für diese Checks stehen Finanzinstituten eine Vielzahl von Instrumenten zur Verfügung. Diese reichen von der Beurteilung grundlegender Anforderungen wie

- Schwachstellenbewertungen und -scans,
- Open-Source-Analysen,
- Bewertungen der Netzsicherheit,
- Gap-Analysen,
- Überprüfungen der physischen Sicherheit,
- Fragebögen,
- Scan-Software,
- Quellcodeüberprüfungen,
- szenariobasierte Tests,
- Kompatibilitätstests,
- Leistungstests und
- End-to-End-Tests

bis hin zu fortgeschrittenen Überprüfungen, zum Beispiel bedrohungsgesteuerte Penetrationstests.

Die genaue Ausgestaltung der Belastbarkeitstests muss verhältnismäßig sein und ist von der Größe, dem Geschäfts- und dem Risikoprofil des Instituts abhängig. Besonders anspruchsvolle beziehungsweise ausführliche Checks sind für bedeutende Organisationen, zum Beispiel große Kreditinstitute, Börsen, zentrale Gegenparteien und zentrale Wertpapierverwahrstellen, vorgesehen. Dies gilt auch für Teilsektoren, die eine zentrale systemische Rolle im Zahlungsverkehr, im Bankenwesen, im Clearing und in der Abrechnung einnehmen. Für als signifikant eingestufte Finanzinstitute sind darüber hinaus bedrohungsgesteuerte Penetrationstests verpflichtend. Welche Institute als signifikant gelten, bestimmen die zuständigen nationalen Behörden auf Basis der in DORA festgelegten und von der ESA weiterentwickelten Kriterien. Die Ergebnisse der bedrohungsgesteuerten Penetrationstests sollen für Institute, die in mehreren Mitgliedsstaaten tätig sind, in der gesamten Europäischen Union anerkannt

Bedrohungsgesteuerte Penetrationstests sollen für als signifikant eingestufte Institute verpflichtend werden.

werden können. Außerdem werden in DORA Kriterien festgelegt, die (externe) Tester erfüllen müssen, um bedrohungsgesteuerte Penetrationstests im Sinne der Vorschrift durchführen zu dürfen.

IKT-Drittrisiko (Artikel 25 bis 39)

In der IKT-Strategie von Finanzunternehmen spielt die Auslagerung von digitalen Funktionen eine wichtige Rolle. Dadurch können diese sich auf ihre Kernkompetenzen konzentrieren. Auslagerungen reichen von der Bereitstellung von Speicherplatz oder Rechnerleistung (Infrastructure as a Service) über die Bereitstellung von Entwicklerplattformen (Plattform as a Service) bis hin zur Bereitstellung von Softwareapplikationen beziehungsweise Webanwendungen (Software as a Service). Bezüglich ihrer IKT-Dienstleistungen sind Finanzunternehmen zunehmend auf nichtfinanzielle Technologieunternehmen angewiesen. Funktionieren können Auslagerungen aber nur, wenn die Institute die Risiken weiterhin unter Kontrolle behalten. IKT-Drittanbieter offerieren häufig standardisierte Dienstleistungen für verschiedene Arten von Kunden. Entsprechende Verträge genügen nicht immer in angemessener Weise den individuellen oder spezifischen Bedürfnissen der Finanzindustrie. Weiterhin sehen viele Verträge keine ausreichenden Schutzmaßnahmen vor, die eine vollwertige Überwachung von Untervergabeprozessen ermöglichen. Im Ergebnis können Finanzinstitute dann die damit verbundenen Risiken nicht wirksam kontrollieren.

Auch bei der Auslagerung digitaler Funktionen müssen die Institute die Risiken genau unter Kontrolle halten können.

DORA hilft, prinzipienbasierte Regeln festzulegen, an denen sich Finanzinstitute bei der Überwachung von Risiken im Zusammenhang mit der Auslagerung von IKT-Dienstleistungen und der Abhängigkeit von IKT-Drittanbietern orientieren können. DORA harmonisiert Schlüsselelemente der Dienstleistung und der Beziehung zu IKT-Drittanbietern. Die Regelung gibt Mindestpakete vor, um eine vollständige Überwachung des IKT-Drittmarktrisikos durch das Finanzinstitut zu ermöglichen. Das gilt während des Vertragsabschlusses, der Durchführung, der Beendigung und der nachvertraglichen Phasen.

Die EU will die wichtigsten Elemente von Drittanbieterleistungen einheitlich regeln.

DORA ist so ausgestaltet, dass eine solide Überwachung der IKT-Risiken Dritter sichergestellt ist. Finanzinstitute sollen zu jeder Zeit und in vollem Umfang für die Einhaltung von Verpflichtungen, die sich aus den DORA-Bestimmungen ergeben, verantwortlich bleiben.

Drittanbieter kritischer IKT-Dienstleistungen

Zu den DORA-Vorgaben gehört außerdem, dass Drittanbieter kritischer IKT-Dienstleistungen einem Aufsichtsrahmen der Union unterliegen. Dies gewährleistet die aufsichtliche Konvergenz. Die ESA, die als federführende Aufsichtsbehörde für jeden kritischen IKT-Drittdienstleister bestimmt ist, erhält die Befugnis zur Überwachung. Diese Tätigkeit baut auf der bestehenden Architektur im Bereich der Finanzdienstleistungen auf. Dabei wird die ESA von einem Unterausschuss, einem Aufsichtsforum, bei ihrer Arbeit unterstützt.

Auch Drittanbieter von IKT-Leistungen für den Finanzsektor sollen künftig einer Aufsicht durch die EU unterliegen.

Informationsaustausch (Artikel 40)

Dem Informationsaustausch zwischen Finanzinstituten zu Cyberbedrohungen misst DORA eine gewichtige Bedeutung zu. Finanzinstitute erhalten die Erlaubnis, untereinander Vorkehrungen dafür zu treffen. Durch die immer komplexeren und ausgeklügelteren IKT-Bedrohungen hängen gute Erkennungs- und Präventionsmaßnahmen in hohem Maße vom regelmäßigen Austausch der Finanzinstitute über Bedrohungen und Schwachstellen ab. Ein Zögern bei der Informationsweitergabe oder ein Zurückhalten nützlicher Informationen führt zu geringerer operativer Resilienz im gesamten Finanzwesen. Institute können ihr individuelles Wissen und ihre praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam nutzen. Das Ziel: ihre Fähigkeiten zur angemessenen Bewertung, Überwachung und Abwehr von Cyberbedrohungen sowie zur angemessenen Reaktion darauf zu verbessern.

Finanzinstitute sollen sich in Zukunft über Cyberbedrohungen untereinander austauschen.

Handlungsbedarf

Bereits zum jetzigen Zeitpunkt sollten sich Finanzinstitute über erste Maßnahmen zur Umsetzung des Gesamtpaketes DORA Gedanken machen und entsprechend handeln.

Wir gehen davon aus, dass DORA in den nächsten 12 bis 18 Monaten von den EU-Institutionen ausgehandelt und danach die weitere sekundäre Gesetzgebung angestoßen wird. Auf Grundlage des vorliegenden Textes sind wir jedoch der Meinung, dass die Unternehmen die folgenden Maßnahmen in Betracht ziehen sollten:

- IKT-Third-Party-Provider (TPP) werden bewerten müssen, ob sie gemäß DORA als „kritisch" eingestuft werden. Diejenigen, die es werden, müssen eventuell neue Regulierungsteams einrichten und analysieren, wie sie am besten mit dem in Entwicklung befindlichen Aufsichtsrahmen übereinstimmen können.
- Für größere Firmen empfiehlt es sich, die ESAs genau zu beachten, wenn sie die Kriterien für die Durchführung von Threat Lead Penetration Testings (TLPTs) ausarbeiten. Diejenigen, die neu in den Bereich fallen, werden eine Strategie entwickeln müssen, um diese fortgeschrittenen Tests bestmöglich zu nutzen.
- Viele der IKT-Risikomanagement-Anforderungen in der DORA wenden große Unternehmen bereits an. Es bleibt die Prüfung, ob ihre Reaktions- und Wiederherstellungsstrategien und -pläne den erweiterten Regeln in diesen Bereichen angemessen entsprechen.
- Alle Firmen werden ihre Verfahren zur Meldung von Vorfällen in Übereinstimmung mit den neuen Regeln entwickeln oder ändern müssen. Sie sollten in Erwägung ziehen, diese an ihre internen Meldeprozesse anzupassen, um die Ressourcenzuweisung zu optimieren.

Die PPI AG

Die PPI AG ist seit über 30 Jahren als Beratungs- und Softwarehaus erfolgreich für Banken, Versicherungen und Finanzdienstleister tätig. Als stabil wachsende Aktiengesellschaft in Familienbesitz verknüpfen wir Fach- und Technologie-Know-how, um Projekte kompetent und unkompliziert umzusetzen. Mehr als 700 Mitarbeiter konzentrieren sich dabei ganz auf den Erfolg unserer Kunden.

Im Bereich Consulting Banken identifizieren wir gemeinsam mit ihnen die entscheidenden Handlungsfelder, um ihre Wertschöpfungsketten zukunftssicher zu machen. Unsere Experten besitzen tiefgehendes Know-how in den zentralen Bereichen des Bankgeschäfts, von der fachlichen Beratung bis hin zur technischen Umsetzung praxistauglicher Lösungen.

Versicherungsunternehmen bietet PPI fachlich wie methodisch exzellente Lösungen für alle Kernprozesse des Assekuranzgeschäfts. Wir unterstützen unsere Kunden dabei auf allen Ebenen, von Management- über Strategie- bis hin zu Prozess- und IT-Beratung.

Ansprechpartner

Consulting Banken
Andreas Bruckner
Senior Manager
+49 151 70335418
andreas.bruckner@ppi.de

Consulting Versicherungen
Tim Glenewinkel
Manager
+49 151 17601697
tim.glenewinkel@ppi.de

PPI AG
Moorfuhrtweg 13
22301 Hamburg
www.ppi.de