WHITE PAPER

DRITTPARTEIENRISIKOMANAGEMENT UNTER DORA

HERAUSFORDERUNGEN UND LÖSUNGEN

Foto: Getty Images

protiviti®
Global Business Consulting

RELEVANZ VON DORA UND DRITTPARTEIENRISIKO-MANAGEMENT

Die digitale Abhängigkeit von Drittparteien hat in den letzten Jahren stark zugenommen. Cloud-Anbieter, FinTech-Partner und spezialisierte IKT-Dienstleister sind aus dem Finanzsektor nicht mehr wegzudenken – doch sie stellen auch potenzielle Schwachstellen dar. Dies hat der europäische Gesetzgeber erkannt und mit dem **Digital Operational Resilience Act (DORA)** einen einheitlichen Rechtsrahmen geschaffen, der seit dem 17. Januar 2025 in der gesamten EU gilt. DORA verpflichtet nahezu alle Finanzinstitute – von Banken über Versicherungen bis hin zu Zahlungsdienstleistern – dazu, ihre digitale operative Resilienz zu stärken und **insbesondere das Risiko aus Drittparteien aktiv zu managen**.

Warum drängt DORA gerade jetzt? Zum einen endete die Übergangszeit: Finanzunternehmen müssen **seit 17. Januar 2025 die Anforderungen aus DORA erfüllen**, was einen erheblichen Umsetzungsdruck erzeugt. Zum anderen haben Aufsichtsbehörden ihre Erwartungen klar formuliert. Beispielsweise forderte die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) von allen Instituten, bis April 2025 ein **umfassendes Register aller Verträge mit IT-Drittparteien** vorzulegen – ein deutlicher Hinweis, dass Regulierer schnell Transparenz über Drittparteirisiken erwarten.

Warum ist gerade das Drittparteienrisikomanagement eine besonders große Herausforderung? Weil hier **praxisnahe, operative Maßnahmen** gefragt sind: Institute müssen hunderte Dienstleister identifizieren, bewerten, Verträge anpassen und laufend überwachen – ein arbeitsintensiver Prozess, der mehrere Fachbereiche (Auslagerungsmanagement, IT, Einkauf, Compliance, Informationssicherheit, Risikomanagement) involviert. Viele Finanzhäuser stellen fest, dass Drittparteienrisikomanagement kein neues Thema ist, aber DORA einen umfassenderen Rahmen dafür vorgibt. Häufig liegen die Tücken im Detail: Alte Verträge erfüllen die neuen Vorgaben nicht, interne Prozesse sind lückenhaft, und die schiere Menge an Dienstleistern überfordert bestehende Strukturen. **DORA macht dieses Thema jetzt zur Chefsache**, denn Mängel können nicht nur zu Compliance-Verstößen, sondern auch zu echten betrieblichen Risiken führen.

PRAXISPERSPEKTIVE: ERKENNTNISSE AUS BERATUNGSPROJEKTEN

Als spezialisierte **Beratungsgesellschaft im Finanzsektor** haben wir in den vergangenen Jahren zahlreiche Projekte zur operativen Resilienz begleitet – häufig mit Fokus auf **IKT-Dienstleister und ausgelagerte Prozesse**. Dabei zeigte sich immer wieder, dass das Drittparteienrisikomanagement in der Praxis an sich ähnelnden Hürden scheitert. Aus unseren Erfahrungen in Zusammenarbeit mit Banken und Finanzdienstleistern in Deutschland haben sich **drei zentrale Umsetzungsprobleme** herauskristallisiert:

1. **Intransparenz im Dienstleister-Portfolio:** Vielen Instituten fehlt **der vollständige Überblick** über alle IKT-Drittanbieter und eine klare Einstufung der **Kritikalität** einzelner Services.

2. **Vertragliche Lücken und fehlende Exit-Strategien:** Bestehende Verträge mit IKT-Dienstleistern enthalten oft **nicht die erforderlichen Klauseln** (z. B. zu Ausstiegsplänen, Audit-Rechten, Informationspflichten), die DORA verlangt.

3. **Unzureichendes Monitoring und Testing:** Nach Vertragsabschluss gibt es häufig kein konsequentes und kontinuierliches Risikomanagement – regelmäßige Überprüfungen, Berichte und Resilienztests unter Einbezug der Dienstleister fehlen.

Im Folgenden beleuchten wir jede dieser Herausforderungen genauer. Wir zeigen typische Schwachstellen, die uns in der Praxis begegnet sind – **inklusive anonymisierter Fallbeispiele** – und skizzieren praxisorientierte Lösungsansätze. Ziel ist es, ein Verständnis dafür zu vermitteln, **wo die operativen Knackpunkte** bei DORA liegen und wie man ihnen begegnen kann.

> »„In unseren Projekten sehen wir: Drittparteienmanagement ist kein reines Compliance-Thema mehr – es ist ein strategischer Hebel für Resilienz."«
>
> ANDREJ GREINDL, MANAGING DIRECTOR

HERAUSFORDERUNG 1: FEHLENDE ÜBERSICHT UND KRITIKALITÄTSBEWERTUNG VON DRITTANBIETERN

Problemstellung

Viele Finanzinstitute haben nur eine **fragmentierte Übersicht** über ihre IKT-Dienstleister. Die Verträge und Informationen liegen verteilt in verschiedenen Abteilungen – etwa im Einkauf, in IT-Fachbereichen oder beim Auslagerungsmanagement. Es fehlt ein zentrales Register, das alle **IKT-Drittparteien** und deren **Risikoeinstufung** umfasst. Genau dieses fordert jedoch DORA ein: Jedes Institut muss ein vollständiges **Verzeichnis aller IKT-Drittanbieter** führen, inklusive der vereinbarten Leistungen und der Einschätzung, welche davon **kritisch oder wichtig** für das Geschäftsmodell sind. Ohne solche Transparenz können die weiteren Schritte – von Risikoanalysen bis zur Überwachung – kaum wirksam umgesetzt werden.

Typische Symptome

In einem aktuellen Projekt mit einer großen Bank zeigte sich, dass die initial gemeldete Liste der IKT-Dienstleister unvollständig war. Erst durch bereichsübergreifende Workshops kam ans Licht, dass rund 30 % **mehr externe IKT-Dienstleister** genutzt wurden als ursprünglich angenommen. Diese „blinden Flecken" entstehen oft, weil Fachabteilungen eigenständig Verträge schließen (Stichwort: Shadow IT oder dezentrale Beschaffung) oder weil historische Vertragslisten nicht gepflegt wurden. Ein anderes Beispiel: Ein mittelständisches Finanzinstitut fand heraus, dass es **keine Kriterien definiert hatte, um kritische von unkritischen Anbietern zu unterscheiden**. Dadurch wurden **alle Lieferanten gleichbehandelt**, und wichtige Dienstleister erhielten nicht die nötige Aufmerksamkeit, während man sich an unwichtigen gleichermaßen abarbeitete. Die Konsequenz solcher Intransparenz ist zweierlei: Zum einen besteht **das Risiko der Nichteinhaltung regulatorischer Anforderungen**, da Artikel 28 der DORA ein solches Register verlangt und Aufseher dieses einsehen oder anfordern können. Zum anderen gehen **operative Risiken** unter – z. B. könnte ein kleiner, aber für einen kritisch oder wichtigen Geschäftsprozess zentraler Softwareanbieter übersehen werden, bis es zu spät ist.

Lösungsansatz

Der erste Schritt ist der Aufbau eines **zentralen Drittanbieter-Registers**. Dieses sollte idealerweise digital geführt werden und **alle bestehenden IKT-**

Dienstleister-Verträge mit den wichtigsten und durch die DORA geforderten Parametern erfassen (Leistungsbeschreibung, zuständige interne Besitzer, Laufzeit, etc.). Wichtig ist, gleich **Kritikalitätskriterien** zu hinterlegen: Zum Beispiel kann man fragen, ob der Service einen **kritischen oder wichtigen Geschäftsprozess** unterstützt oder ob es schwierig wäre, den Anbieter kurzfristig zu ersetzen. Auf Basis solcher Kriterien lässt sich jeder Dienstleister als **„kritisch/wichtig" oder „normal"** einstufen. DORA selbst spricht von **„kritischen oder wichtigen Funktionen"**, für die besondere Sorgfalt gilt. Praktisch empfehlen wir:

- **Bereichsübergreifende Datensammlung:** Alle Fachbereiche sollten eingebunden werden, um wirklich alle externen IT-Bezüge zu identifizieren (inklusive kleiner Nischenanbieter und indirekter IT-Leistungen). Hier kann ein standardisierter Fragebogen helfen.
- **Klare Verantwortlichkeiten:** Legen Sie fest, wer das Register pflegt und aktualisiert (oft das Auslagerungsmanagement). Neue Verträge sollten nur geschlossen werden, wenn die Daten im Register erfasst sind – so bleibt es aktuell.
- **Kritikalität bewerten:** Entwickeln Sie ein Scoring-Modell, um die Bedeutung eines Dienstleisters zu bewerten (z. B. anhand Geschäftsimpact, regulatorischer Anforderungen, Datensensibilität, Datenvolumen). Priorisieren Sie dann die kritischen Anbieter für weitere Maßnahmen.
- **Review-Prozess etablieren:** Das Register ist kein Einmal-Projekt – mindestens jährlich sollte ein Abgleich mit den tatsächlichen Dienstleisterbeziehungen erfolgen. Veränderungen (neue oder gekündigte Verträge, geänderte Bewertungen) müssen nachgepflegt werden.

Durch eine solche strukturierte Vorgehensweise erhält das Institut eine belastbare **Gesamtübersicht**. Diese bildet die Grundlage, um **DORA-konform** Drittparteirisiken zu steuern. Zudem schafft das Bewusstsein über kritische Abhängigkeiten oft intern schon **Dringlichkeit** für weitere Schritte: Wenn Entscheidungsträger schwarz auf weiß sehen, welche externen Partner für die Betriebsfähigkeit unverzichtbar sind, wächst die Bereitschaft, in das Management dieser Risiken zu investieren.

> »„Besonders herausfordernd ist das Vertragsmanagement – nicht nur wegen der Masse an Dienstleistern, sondern weil viele Verträge grundlegende DORA-Klauseln schlicht nicht enthalten. Ohne strukturierte Nachverhandlung droht hier ein regulatorisches Risiko."«
>
> CHRISTOPHER CHASSÉE, DIRECTOR

HERAUSFORDERUNG 2: VERTRAGLICHE LÜCKEN – FEHLENDE KLAUSELN UND EXIT-STRATEGIEN

Problemstellung

Ein zentrales Element des Drittparteienrisikomanagements sind die **Vertragsbedingungen** mit den IT-Dienstleistern. DORA schreibt explizit vor, dass Finanzinstitute gewisse **Schlüsselklauseln** in Verträgen mit IKT-Dienstleistern verankern müssen. Dazu gehören z. B. **Kündigungsrechte, Mindestkündigungsfristen, Unterstützung bei IKT-Vorfällen, Datenzugriff und -rückgabe, Audit- und Zugriffsrechte sowie Kooperationspflichten mit Aufsichtsbehörden**. Die Realität: Viele bestehende Verträge – vor allem ältere oder mit geringerer strategischer Bedeutung – erfüllen diese Anforderungen nicht. Häufig wurden IT-Services ohne **spezifische Resilienz- oder Compliance-Klauseln**

eingekauft, und eine systematische Vertragsüberarbeitung fand noch nicht statt.

Typische Symptome

„Ein Kunde mit über 100 aktiven IKT-Dienstleistern hatte in über 75% aller Fälle keinerlei Vertragsklauseln zu Exit-Strategien verankert." Dieses Zitat aus einem unserer Projekte verdeutlicht ein verbreitetes Problem: In einer Vielzahl der Verträge dieser Bank war nicht geregelt, **wie ein geordneter Ausstieg** im Ernstfall erfolgen soll – z. B. was passiert, wenn der Dienstleister insolvent wird oder gravierende Sicherheitsmängel zeigt. Auch **Audit-Rechte** oder Verpflichtungen der Dienstleister, bei Sicherheitsvorfällen **Informationen zu liefern**, fehlten weitgehend. Solche Lücken sind riskant: Ohne **Exit-Plan** steht das Institut im Krisenfall unter Zeitdruck da und muss improvisieren. Ein anderes Beispiel aus der Praxis: In einem Projekt stellte sich heraus, dass Unterauftragnehmer der IKT-Dienstleister im Regelfall nicht vertraglich genehmigungspflichtig waren – das Finanzinstitut wusste in diesen Fällen also gar nicht, welche Drittparteien im Hintergrund noch beteiligt sind. DORA verlangt jedoch, dass auch **Unterauftragnehmer** kontrolliert werden, insbesondere wenn kritische Funktionen betroffen sind. Die Aufsichtsbehörden erwarten, dass Verträge entsprechend nachgebessert werden. DORA gibt hier klare Leitplanken vor und ermuntert Institute, **Verträge nachzuverhandeln** und mit den Anforderungen in Einklang zu bringen.

Lösungsansatz

Ein systematisches **Vertrags-Audit** aller relevanten IKT-Dienstleisterverträge ist der erste Schritt. Dabei wird überprüft, welche der geforderten Klauseln bereits vorhanden sind und wo **Nachbesserungsbedarf** besteht. Erfahrungsgemäß betrifft dies vor allem folgende Punkte:

- **Kündigungsrechte und Exit:** Jeder Vertrag sollte das Recht beinhalten, die Dienstleistung bei Bedarf (z. B. bei schweren Verstößen oder strategischer Neuausrichtung) kündigen zu können, sowie eine vereinbarte **Exit-Strategie**. Letztere umfasst Regelungen, wie der Dienstleister im Falle der Vertragsbeendigung unterstützen muss (z. B. Datenübertragung an den Nachfolger, Weiterbetrieb für eine Übergangsfrist, Wissenstransfer).

- **Unterstützung bei IKT-Vorfällen:** Verträge sollten festhalten, dass der Dienstleister bei **IKT-Vorfällen** proaktiv informiert und unterstützt. So muss er Sicherheitsvorfälle **unverzüglich melden** und bei der Aufklärung/Behebung mitwirken – idealerweise ohne **Zusatzkosten**, wie DORA es für kritische Dienstleistungen erwartet.

- **Regulatorischer Zugriff und Audit:** Es sollten **Prüfungs- und Zugriffsrechte** vereinbart sein – sowohl für das Finanzinstitut (bzw. beauftragte Dritte) als auch für Aufsichtsbehörden. Die BaFin bzw. europäische Aufseher müssen im Zweifelsfall Einblick nehmen dürfen, um die Einhaltung von Vorgaben zu überwachen. Fehlen solche Klauseln, droht im Ernstfall Rechtsunsicherheit, ob z. B. ein Cloud-Anbieter Prüfungen zulässt.

- **Subunternehmer & Standort:** Vertragsklauseln sollten den **Einsatz von Subdienstleistern** nur mit Zustimmung erlauben, insbesondere bei kritischen Services. Auch Transparenz über die **Standorte der Datenverarbeitung** ist nötig (Stichwort: Cloud und Drittstaatenrisiken).

- **Service Levels und Sicherheit:** Präzise **Service Level Agreements (SLAs)** mit Messgrößen gehören in Verträge zu kritischen IT-Leistungen (Verfügbarkeit, Reaktionszeiten, etc.). Zudem sollten **Mindeststandards zur Informationssicherheit** festgeschrieben sein (z. B. Zertifizierungen, Verschlüsselungsanforderungen, Patch-Management).

In der Praxis empfiehlt es sich, **Standardvertragsklauseln** oder Musterergänzungen zu entwickeln, die all diese Punkte abdecken. Diese können dann bei Neuabschlüssen direkt verwendet und bei bestehenden Verträgen im Rahmen von **Nachverhandlungen** eingebracht werden. Natürlich ist die Nachverhandlung mit Aufwand verbunden: Bei hunderten Dienstleistern muss priorisiert werden. Ein pragmatischer Weg ist es, **zunächst die Top 10–20 kritischsten Anbieter** ins Visier zu nehmen und dort rasch vertragliche Klarheit zu schaffen. Parallel kann man für die restlichen Dienstleister einen gestuften Plan aufsetzen. Viele große Anbieter (z. B. Cloud-Konzerne) kennen die DORA-Anforderungen bereits und haben ggf. eigene Vertragsanhänge vorbereitet – hier lohnt es sich nachzufragen.

Wichtig ist, die **Balance** zu halten: Verträge sollten nicht unnötig „aufgebläht" werden, aber **alle nötigen Schutzmechanismen** enthalten. Letztlich profitieren beide Seiten von klaren Regelungen: Das Finanzinstitut erhält Rechte und Unterstützung zugesichert, der Dienstleister weiß genau, welche Pflichten er erfüllen muss (und kann diese

einkalkulieren). Durch robuste Verträge wird das **Risiko im Vorfeld** eingehegt, sodass man im Krisenfall handlungsfähig bleibt. DORA setzt hier den Rahmen – die Institute müssen ihn nun mit Leben füllen.

HERAUSFORDERUNG 3: KONTINUIERLICHES MONITORING UND FEHLENDE RESILIENZTESTS

Problemstellung

Drittparteienrisikomanagement ist keine einmalige Aufgabe beim Onboarding eines IKT-Dienstleisters, sondern muss **laufend betrieben** werden. DORA verlangt, dass Finanzinstitute das Risiko von IKT-Dienstleistern **kontinuierlich überwachen und steuern**. Dazu gehört z. B., die **Leistung und Sicherheit** der Dienstleister regelmäßig zu beurteilen, sich über **Änderungen oder Vorfälle** informieren zu lassen und notfalls einzugreifen. Außerdem müssen Institute ihre **operative Resilienz** testen – inklusive Szenarien, in denen ein kritischer Dienstleister ausfällt. In der Praxis fehlt es hier oft an etablierten Prozessen. Viele Institute haben zwar bei Vertragsschluss eine erste Risikoanalyse gemacht, lassen aber im laufenden Betrieb nach: **Berichte der Dienstleister werden nicht eingefordert, Kennzahlen nicht ausgewertet, Notfallübungen** mit Dienstleistern finden gar nicht statt. So können schleichende Verschlechterungen oder neue Risiken unbemerkt bleiben.

Typische Symptome

In einem Projekt beobachteten wir, dass ein Finanzdienstleister die Leistungsbewertungen seiner Outsourcing-Partner **nur auf dem Papier** definiert hatte – es gab Service-Level-Vorgaben, aber keine regelmäßigen Service Review Meetings, um Abweichungen zu besprechen. Erst als ein wichtiger Dienstleister wiederholt Ausfallzeiten hatte und interne Beschwerden laut wurden, begann man damit, systematisch Reports anzufordern. Ein anderes Beispiel: Ein Institut hatte zwar Notfallpläne für eigene IT-Systeme, aber **keinen Plan B für den Ausfall eines kritischen Cloud-Anbieters**. Man vertraute darauf, dass der Dienstleister schon irgendwie liefern würde. Diese Fälle sind typisch für die **Lücke zwischen Theorie und Praxis**: Risiken aus Drittpartien werden initial erkannt, aber es mangelt an **kontinuierlicher Risikobeobachtung**. DORA fordert indes explizit, dass Institute die Kontrolle über alle Entwicklungen auf Drittanbieterebene behalten müssen. Dazu zählt, dass Dienstleister wichtige Änderungen oder Vorfälle **melden müssen** und dass das Institut **frühzeitig reagieren kann** – sei es durch Notfallmaßnahmen oder Anpassung der Strategie.

Lösungsansatz

Effektives **Monitoring** und **Testen der Resilienz** mit IKT-Dienstleistern lässt sich organisatorisch und technisch untermauern. Wichtige Elemente dabei sind:

- **Regelmäßige Risiko- und Performance-Reviews:** Etablieren Sie einen festen Rhythmus (z. B. quartalsweise) für Meetings oder Reports mit jedem **kritischen IKT-Dienstleister**. In diesen Service Reviews sollten KPIs wie Verfügbarkeit, Zwischenfälle, Sicherheitsmetriken und Vertragspflichten durchgegangen werden. Dokumentieren Sie Abweichungen und vereinbaren Sie Verbesserungsmaßnahmen.

- **Frühwarnindikatoren:** Richten Sie **Kennzahlen und Schwellenwerte** ein, die Alarm schlagen, wenn sich ein Dienstleister-Risiko zuspitzt – z. B. wiederholte SLA-Verletzungen, negative Finanznachrichten über den Anbieter, hohe Mitarbeiterfluktuation beim Provider oder Verzögerungen in der Lieferkette. Solche Indikatoren können teils auch automatisiert, bspw. durch Nachrichtenfeeds, überwacht werden.

- **IKT-Vorfallsmanagement einbinden:** Stellen Sie sicher, dass **Sicherheitsvorfälle oder IT-Störungen** beim Dienstleister umgehend in das **interne Incident- und Krisenmanagement** Ihres Instituts einfließen. Dazu braucht es klare Meldewege: Wer informiert wen, wenn z. B. der Cloud-Provider einen Cyberangriff erleidet? Idealerweise übt man diese Abläufe vorab in **Simulationsübungen**.

- **Gemeinsame Notfalltests:** Integrieren Sie kritische Dienstleister in Ihre **Business Continuity- und Disaster Recovery-Tests**. Beispielsweise kann man jährlich einen Test durchführen, bei dem angenommen wird, der Dienstleister ist nicht verfügbar – wie gut funktioniert der vorbereitete **Exit- bzw. Backup-Plan**? Oder man bittet den Dienstleister, eigene Notfallprozeduren vorzustellen und nachzuweisen (Stichwort: **Business Continuity-Tests** und ggf. Teilnahme an institutseigenen Threat Led Penetration Tests

(TLPT) – soweit relevant). Solche Tests decken Lücken auf, bevor ein echter Ausfall eintritt.

- **Zentrale Steuerung und Tools:** Viele Institute richten eine **dedizierte Stelle oder Task-Force** für Drittparteisteuerung ein (z. B. **Drittparteirisikomanager**). Diese koordiniert effektiv die genannten Maßnahmen. Eine klare Governance stellt sicher, dass die Erkenntnisse aus dem Monitoring auch **Entscheidungen auslösen** – z. B. Eskalation an das Management, wenn Risiken nicht abnehmen.

DORA schreibt zudem vor, dass bedeutende **IKT-Vorfälle an die Aufsicht gemeldet** werden müssen. Dies schließt natürlich Vorfälle ein, die von einem IKT-Dienstleister ausgehen und das eigene Geschäft beeinträchtigen. Das interne Monitoring muss also so aufgestellt sein, dass solche Vorfälle **rasch erkannt und gemeldet** werden können.

In Summe geht es darum, vom **reaktiven** zum **proaktiven Drittparteienmanagement** zu gelangen. Institute sollten jederzeit den „Gesundheitszustand" ihrer wichtigsten Dienstleister kennen und vorbereitet sein, falls etwas schiefläuft. Das erfordert zwar initial Aufwand und neue Routinen, zahlt sich aber aus: Probleme können früher adressiert werden, die **operative Stabilität** erhöht sich und letztlich erfüllt man die DORA-Vorgaben nachweislich.

»„In der Praxis fehlt es oft an einem vollständigen Überblick über alle IKT-Dienstleister. Sobald wir gemeinsam ein zentrales Register aufbauen, zeigen sich schnell kritische Abhängigkeiten, die vorher keiner auf dem Schirm hatte."«

TIMO RUPPRECHT, MANAGER

FAZIT UND AUSBLICK

Die Einführung von DORA hat das **Drittparteienrisikomanagement** endgültig ins Rampenlicht gerückt. Unsere Beispiele haben gezeigt, dass viele Institute zwar das „Was" – also die Anforderungen – verstanden haben, aber beim „Wie" – der praktischen Umsetzung – auf typische Hürden stoßen. **Intransparenz im Dienstleisterportfolio, unzureichende Vertragsklauseln und fehlendes Monitoring** sind dabei die Kernprobleme, die angegangen werden müssen. Die gute Nachricht: All diese Herausforderungen lassen sich mit einem **strukturierten, praxisnahen Ansatz** bewältigen. Es bedarf bereichsübergreifender Anstrengungen, klarer Methoden und mitunter externer Unterstützung, aber die **operativen Knackpunkte** sind lösbar.

Für Finanzinstitute bietet die konsequente Umsetzung gleich **mehrfachen Mehrwert**: Zum einen wird die Compliance mit DORA sichergestellt – ein Muss, um Prüfungen durch Aufseher ohne Beanstandungen zu überstehen. Zum anderen erhöht ein robustes Drittparteienmanagement die **tatsächliche operative Resilienz** des Instituts. Man kennt seine Schwachstellen und kann im Krisenfall schneller reagieren. Nicht zuletzt entsteht **internes Bewusstsein**: Führungskräfte und Fachverantwortliche sehen, welche Abhängigkeiten bestehen, und treffen informiertere Entscheidungen (z. B. zu neuen Auslagerungen oder Investitionen in Backup-Lösungen).

Als umsetzungsstarke Beratungsgesellschaft haben wir in den skizzierten Bereichen **erprobte Vorgehensweisen** entwickelt – von der Bestandsaufnahme zur Umsetzung von Kontrollmechanismen bis hin zur Beistellung von helfenden Händen bei der Durchführung von Vertragsprüfungen und der operativen Implementierung von Anforderungen der DORA. Gern teilen wir unser Know-how: **Kontaktieren Sie uns für einen unverbindlichen Austausch.**

ÜBER PROTIVITI

Protiviti *(www.protiviti.com)* ist ein weltweit tätiges Beratungsunternehmen, das fundiertes Fachwissen, objektive Erkenntnisse, einen maßgeschneiderten Ansatz und beispiellose Zusammenarbeit bietet, um Führungskräfte selbstbewusst in die Zukunft blicken zu lassen. Protiviti und seine unabhängigen und regional ansässigen Mitgliedsfirmen unterstützen Kunden mit Beratungsleistungen und Managed Solutions in Bezug auf Finanzen, Technologien, Operatives, Digitales, HR, Risiko und Interne Revision – mithilfe eines Netzwerkes von mehr als 90 Niederlassungen in über 25 Ländern. Protiviti wurde zum zehnten Mal in Folge in die Liste der **Fortune 100 Best Companies to Work For®** aufgenommen und hat mehr als 80 Prozent der Fortune-100- und fast 80 Prozent der Fortune-500-Unternehmen betreut. Protiviti arbeitet ebenfalls mit Regierungsbehörden sowie kleineren und wachsenden Unternehmen zusammen, einschließlich solchen, die den Börsengang planen. Protiviti ist darüber hinaus eine hundertprozentige Tochter der **Robert Half Inc.** (NYSE: RHI).

KONTAKT

ANDREJ GREINDL
Managing Director
+49 172 698 30 53
andrej.greindl@protiviti.de

CHRISTOPHER CHASSÉE
Director
+49 172 621 73 01
christopher.chassee@protiviti.de

TIMO RUPPRECHT
Manager
+49 160 550 59 27
timo.rupprecht@protiviti.de

www.protiviti.de