

Compliance am Wendepunkt: Warum das klassische Modell an seine Grenzen stößt

Einleitung

Die regulatorischen Anforderungen an Unternehmen nehmen kontinuierlich zu. Neue Vorgaben müssen identifiziert, bewertet, umgesetzt und nachvollziehbar belegt werden. Viele Organisationen arbeiten dabei noch mit einem manuellen Compliance-Modell. Je komplexer die regulatorischen Anforderungen werden, desto deutlicher treten die Schwächen dieses Ansatzes zutage: Der Aufwand steigt, Transparenz geht verloren und die Nachweisführung wird zunehmend anspruchsvoll.

Unternehmen benötigen neue Ansätze, um gesetzliche Vorgaben effizient, nachvollziehbar und skalierbar zu steuern. Künstliche Intelligenz und Konzepte wie Regulatory Intelligence können dabei unterstützen, regulatorische Entwicklungen frühzeitig zu erkennen, Auswirkungen systematisch zu bewerten und fundierte Entscheidungen vorzubereiten.

Gleichzeitig wirft der Einsatz von KI neue Fragen nach Governance, Nachvollziehbarkeit und Verantwortung auf. Dieses Paper zeigt, warum klassische Compliance-Modelle angesichts wachsender regulatorischer Komplexität zunehmend an ihre Grenzen stoßen, welche Herausforderungen daraus entstehen und wie sich Organisationen für die Zukunft aufstellen können.

forvis mazars

1. Die strukturellen Herausforderungen heutiger Compliance

Hoher Aufwand bei begrenzter Skalierbarkeit

Jede neue oder geänderte Vorgabe löst mehrere Arbeitsschritte aus. Unternehmen müssen

- die Anforderung erfassen,
- ihre Relevanz prüfen,
- die eigene Betroffenheit bestimmen,
- Auswirkungen untersuchen,
- Maßnahmen ableiten,
- deren Umsetzung festhalten und,
- adressatengerecht an die internen und externen Stakeholder kommunizieren.

Wenn diese Schritte überwiegend manuell erfolgen, steigt der Ressourcenbedarf. Gleichzeitig müssen immer größere Informationsmengen und mehr regulatorische Zusammenhänge berücksichtigt werden. Zusätzliche Anforderungen lassen sich in diesem Modell häufig nur durch weitere personelle Ressourcen bewältigen. Da diese Kapazitäten nicht unbegrenzt verfügbar sind, stößt der Ansatz zunehmend an seine Skalierungsgrenzen und erreicht mit wachsender Regulierungsdichte ein Plateau.

Datensilos begrenzen Transparenz und Geschwindigkeit

Relevante Informationen sind häufig über verschiedene Tools, Dokumente, Systeme und Teams verteilt. Das heißt:

- Regulatorische Anforderungen,
- interne Vorgaben,
- Verträge,
- Nachweise und
- Prüfergebnisse bilden keine gemeinsame Informationsgrundlage.

Vor einer belastbaren Bewertung müssen Unternehmensverantwortliche daher die benötigten Inhalte suchen, zusammenführen und abgleichen. Dadurch bleibt oft unklar, welche Vorgaben bereits berücksichtigt wurden, wo Lücken bestehen und welche Anpassungen Priorität haben. Das führt zu drei zentralen Problemen:

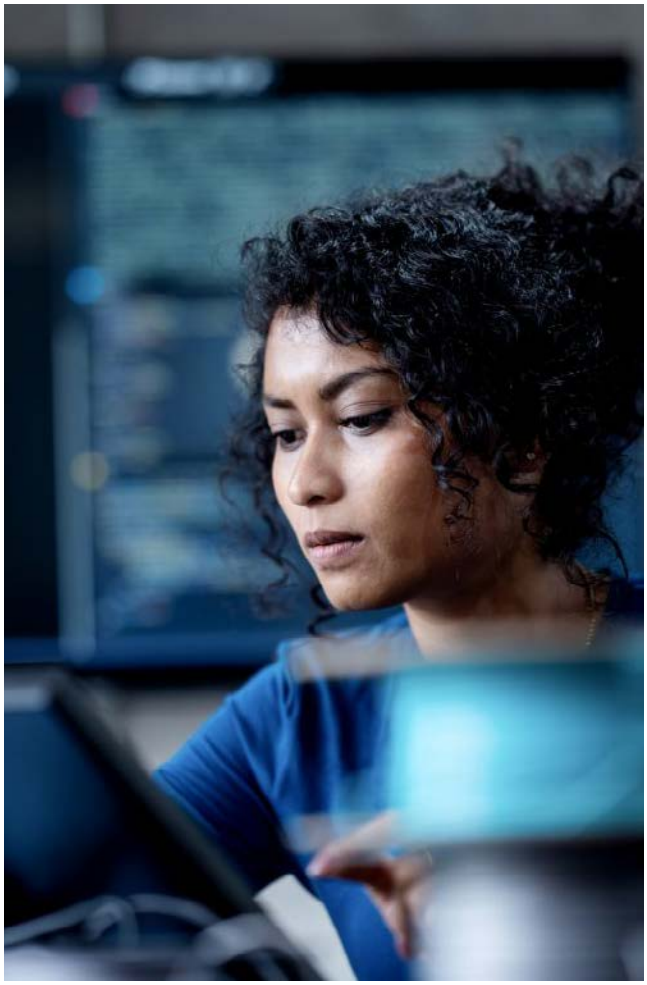
- sehr hoher operativer Aufwand,
- begrenzte Transparenz und
- eingeschränkte Auditierbarkeit

Wechselwirkungen erschweren die Steuerung

Regulatorische Anforderungen stehen selten für sich allein – vielmehr gibt es häufig inhaltliche Überschneidungen und Wechselwirkungen zwischen einzelnen Vorgaben. Sie betreffen dieselben Unternehmensbereiche, greifen auf gemeinsame Prozesse und Kontrollen zu oder stellen vergleichbare Anforderungen an bestehende Governance-Strukturen. Mit zunehmender Regulierungsdichte wächst damit auch die Zahl dieser regulatorischen Abhängigkeiten. Dies erschwert die Bewertung von Auswirkungen, die Priorisierung von Maßnahmen und die konsistente Steuerung regulatorischer Anforderungen.

Nachweis- und Auditrisiken steigen

Unternehmen müssen belegen können, wie sie zu ihren Bewertungen gelangt sind und welche Maßnahmen daraus folgten. Liegen die relevanten Informationen in unterschiedlichen Systemen, Dokumenten und Arbeitsständen vor, muss die Audit-Spur nachträglich zusammengesetzt werden. Mit wachsender Regulierungsdichte steigen der Ressourcenbedarf und das Risiko unvollständiger oder nicht ausreichend belastbarer Nachweise.



2. Regulatory Intelligence übersetzt Anforderungen in konkrete Handlungen

Die beschriebenen Herausforderungen zeigen, dass viele Unternehmen regulatorische Änderungen zwar identifizieren können, die Ableitung konkreter Maßnahmen jedoch häufig aufwendig bleibt. Zwischen einer neuen Vorgabe und ihrer Umsetzung liegen zahlreiche Bewertungs-, Abstimmungs- und Dokumentationsschritte. Genau hier setzt Regulatory Intelligence an.

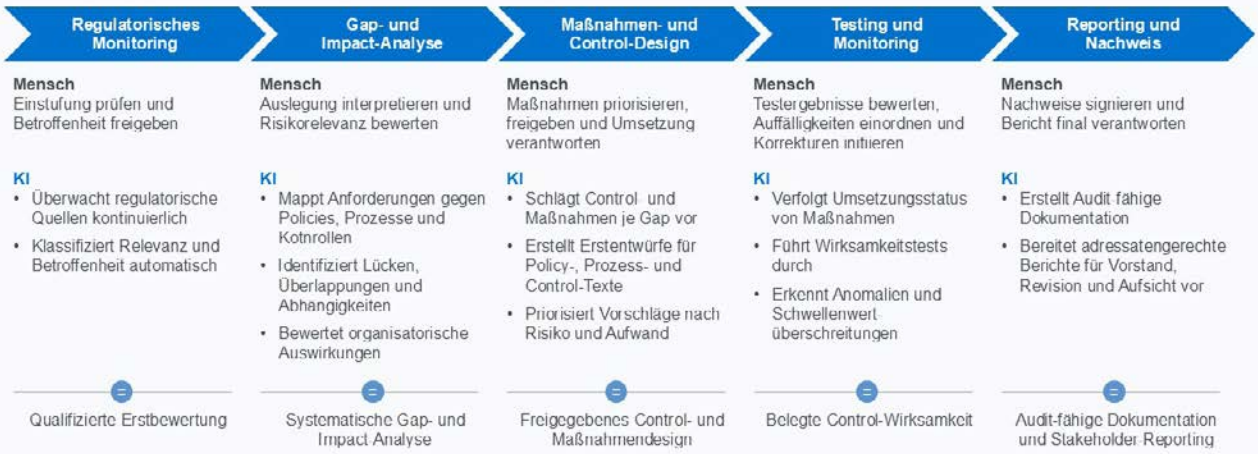
Der Mehrwert liegt nicht allein in der schnelleren Analyse regulatorischer Informationen. KI verknüpft neue Anforderungen mit bestehenden Richtlinien, Prozessen und Kontrollen und macht dadurch Betroffenheiten, Abhängigkeiten und Überschneidungen sichtbar. Das reduziert Doppelarbeiten, erleichtert die Priorisierung und schafft eine belastbarere Grundlage für Entscheidungen.

Regulatory Intelligence unterstützt u. a. bei drei zentralen Aufgaben:

- **Regulatorische Änderungen erkennen:** Neue und geänderte Anforderungen werden kontinuierlich erfasst und hinsichtlich ihrer potenziellen Relevanz eingeordnet.
- **Auswirkungen bewerten:** Die Anforderungen werden mit bestehenden Vorgaben, Prozessen und Kontrollen abgeglichen, um Betroffenheiten, Abhängigkeiten und mögliche Lücken sichtbar zu machen.
- **Konkrete Maßnahmen ableiten und priorisieren:** Die Ergebnisse fließen in eine priorisierte Handlungsagenda für regulatorische Anpassungen ein.

So wird aus einer regulatorischen Änderung eine belastbare Entscheidungsgrundlage für die weitere Steuerung. Die fachliche Bewertung und Entscheidung verbleiben dabei jederzeit bei den zuständigen Expert*innen, also dem „Human in the Loop“.

KI-Anwendungsfälle entlang der Compliance-Wertschöpfungskette



3. Phasen der Compliance-Wertschöpfungskette

Der Nutzen von Regulatory Intelligence endet jedoch nicht bei der Identifikation regulatorischer Änderungen und sich daraus ergebenden Maßnahmen. Die gewonnenen Erkenntnisse wirken entlang der gesamten Compliance-Wertschöpfungskette: von der Beobachtung regulatorischer Entwicklungen über die Analyse von Auswirkungen bis hin zu Umsetzung, Überwachung und Nachweisführung.

Damit diese Prozessschritte nicht isoliert nebeneinanderstehen, sondern auf derselben Informationsgrundlage aufbauen, benötigen Unternehmen eine integrierte technologische Basis. Eine mögliche technische Umsetzung hierfür ist z. B. die von Forvis Mazars entwickelte KI-native Plattform für Governance, Risk und Compliance (GRC). Diese verbindet Daten, Prozesse, Governance und KI-Funktionen in einer gemeinsamen Architektur.

Konkret ergeben sich folgende Phasen entlang der Compliance-Wertschöpfungskette:

1. Regulatorisches Monitoring

Die KI überwacht regulatorische Quellen kontinuierlich und identifiziert neue oder geänderte Anforderungen. Anschließend klassifiziert sie deren potenzielle Relevanz und die mögliche Betroffenheit des Unternehmens.

2. Gap- und Impact-Analyse

Anschließend ordnet die KI regulatorische Anforderungen bestehenden Richtlinien, Prozessen und Kontrollen zu, identifiziert Lücken, Überschneidungen und Abhängigkeiten und bewertet organisatorische Auswirkungen.

3. Maßnahmen- und Control-Design

Auf Basis der identifizierten Lücken erstellt die smarte Software Vorschläge für Maßnahmen und Kontrollen. Zudem kann sie erste Entwürfe für Richtlinien, Prozessbeschreibungen und Kontrolltexte vorbereiten.

4. Testing und Monitoring

Nach der Umsetzung verfolgt die KI den Status der Maßnahmen und unterstützt bei Wirksamkeitstests. Sie erkennt Anomalien und Schwellenwertüberschreitungen, die auf Abweichungen oder weiteren Anpassungsbedarf hinweisen können. Dadurch lässt sich belegen, ob die vorgesehenen Kontrollen tatsächlich funktionieren.

5. Reporting und Nachweis

Im letzten Schritt erstellt die KI auditfähige Unterlagen und bereitet Informationen adressatengerecht für Vorstand, Revision und Aufsicht auf. Anforderungen, Bewertungen, Maßnahmen, Kontrollen und Testergebnisse werden in einer nachvollziehbaren Audit-Spur zusammengeführt. Das Ergebnis sind prüfungsfähige Unterlagen und belastbare Berichte für unterschiedliche Adressaten.



4. Anwendungsfall: Gap-Analyse

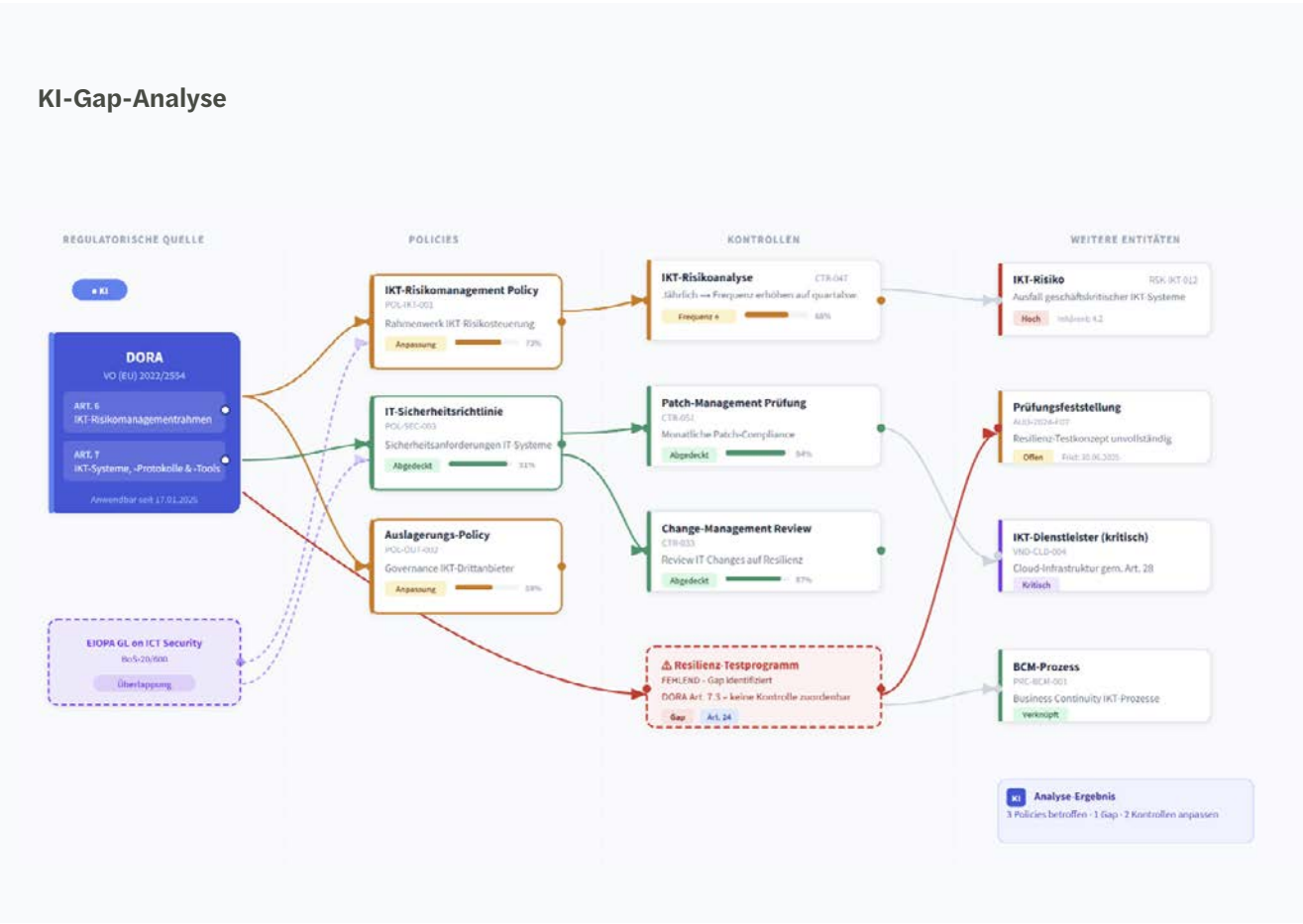
Die Gap-Analyse gehört zu den ressourcenintensivsten Aufgaben im Compliance-Management.
Neue regulatorische Anforderungen müssen systematisch mit bestehenden Richtlinien, Prozessen und Kontrollen abgeglichen werden, um Handlungsbedarf frühzeitig zu identifizieren. KI kann diesen Analyseprozess erheblich beschleunigen und strukturieren.

Ausgangspunkt ist ein qualitätsgesicherter regulatorischer Anforderungskatalog, der von Compliance-Expert*innen validiert wird. Die KI analysiert anschließend die Anforderungen im Abgleich mit bestehenden Policies, Kontrollen und weiteren Governance-Dokumenten. Ausgehend von einem qualitätsgesicherten regulatorischen Anforderungskatalog, der von Compliance-Expert*innen validiert wird, analysiert die KI die Anforderungen im Vergleich zu vorhandenen Dokumenten und Regelwerken.

Um die Anforderungen des Digital Operational Resilience Act (DORA) zu erfüllen (s. Grafik), müssen Unternehmen beispielsweise ihre bestehenden Policies, Kontrollen und Governance-Strukturen systematisch mit den regulatorischen Vorgaben abgleichen und mögliche Umsetzungslücken identifizieren. Dabei bewertet sie den Abdeckungsgrad vorhandener Regelungen, identifiziert potenzielle Lücken und zeigt auf, in welchen Bereichen Anpassungsbedarf besteht. Gleichzeitig werden Überschneidungen mit anderen regulatorischen Vorgaben transparent gemacht, sodass Synergien genutzt und Doppelarbeiten vermieden werden können.

Das Ergebnis ist eine strukturierte Bewertung der Compliance-Landschaft mit einer nachvollziehbaren Priorisierung identifizierter Handlungsfelder. Auf dieser Grundlage können Compliance-Verantwortliche gezielt Maßnahmen ableiten, Ressourcen effizient einsetzen und die Umsetzung regulatorischer Anforderungen risikoorientiert steuern.

KI-Gap-Analyse



5. KI skaliert nicht nur Chancen, sondern auch Risiken

Mit wachsendem Umfang der KI-Unterstützung können sich auch Fehlentscheidungen schneller und in größerem Umfang auswirken als in einem manuellen Prozess. Unternehmen müssen technische Leistungsfähigkeit deshalb mit Nachvollziehbarkeit, Kontrolle und klarer Verantwortlichkeit verbinden.

Ein möglicher Ansatz ist **„Compliance by Design“**. Dabei werden Gesetze, regulatorische Vorgaben und Richtlinien in eine nachvollziehbare, maschinell ausführbare Logik überführt, die drei Voraussetzungen erfüllen muss:

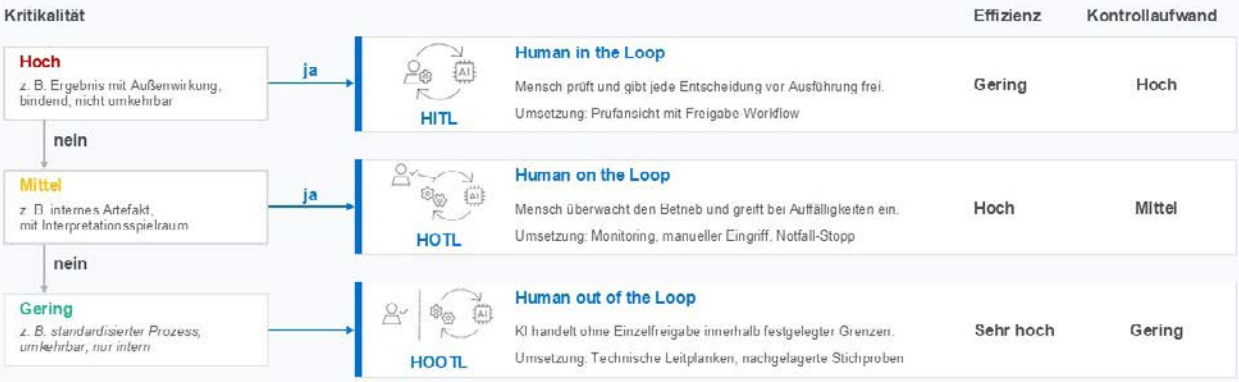
- **Richtig:** Die angewandte Logik bildet die fachlich freigegebene regulatorische Auslegung ab.
- **Reproduzierbar:** Vergleichbare Sachverhalte werden nach denselben Regeln bewertet und führen zu konsistenten Ergebnissen.
- **Belegbar:** Bewertungen, Verarbeitungsschritte und Freigaben hinterlassen eine nachvollziehbare Audit-Spur.

Das bedeutet: Die fachliche Verantwortung verbleibt bei den zuständigen Expert*innen. Sie legen fest, welche Aufgaben die KI übernehmen darf und an welchen Stellen eine menschliche Beurteilung erforderlich ist. Außerdem prüfen sie Vorschläge, interpretieren Ergebnisse, erteilen Freigaben und verantworten die abschließende Entscheidung.

Governance wird damit zum festen Bestandteil des Compliance-Systems. Sie definiert die zulässigen Einsatzbereiche, menschliche Eingriffspunkte und Verantwortlichkeiten. Zudem stellt sie sicher, dass die zugrunde liegende Logik kontrolliert wird und jede Bewertung nachvollziehbar bleibt. Der Nutzen reicht über reine Effizienzgewinne hinaus. Richtig gestaltete Entscheidungslogiken ermöglichen prüffeste und reproduzierbare Ergebnisse. Die Audit-Spur entsteht während der Verarbeitung, und der Weg von der regulatorischen Anforderung zur belastbaren Entscheidung verkürzt sich.

Interventionsmechanismen im Überblick

Einstufung je KI-Anwendungsfall – Kriterium ist die Auswirkung eines Fehlers



6. Was bedeutet das für Entscheider*innen?

Die beschriebenen Entwicklungen zeigen:
Die Herausforderungen vieler Compliance-Modelle sind kein Ressourcen-, sondern ein Skalierungsproblem. Ansätze wie Regulatory Intelligence eröffnen neue Möglichkeiten, regulatorische Anforderungen effizienter und transparenter zu steuern.
Daraus ergeben sich vier zentrale Handlungsfelder für Geschäftsführungen, Vorstände und Compliance-Verantwortliche.

1. Skalierbarkeit statt reinen Personalaufbau verfolgen

Mehr Personal schließt die strukturelle Lücke von klassischen Compliance-Modellen nicht. Entscheider*innen sollten analysieren, welche wiederkehrenden Arbeitsschritte KI strukturiert unterstützen kann und an welchen Stellen standardisierte Abläufe erforderlich sind. Das Ziel ist ein Compliance-System, das zusätzliche regulatorische Anforderungen verarbeiten kann, ohne Ressourcenbedarf, Kosten und Nachweisrisiken zu erhöhen.

2. Datensilos auflösen und Zusammenhänge sichtbar machen

Viele Herausforderungen entstehen, weil Informationen zu regulatorischen Anforderungen, Bewertungen, Maßnahmen und Nachweisen nicht ausreichend miteinander verknüpft sind. Entscheider*innen sollten deshalb die Voraussetzungen für eine gemeinsame Informationsgrundlage schaffen, die Zusammenhänge transparent macht und konsistente Entscheidungen unterstützt.

3. Von der Informationsflut zur belastbaren Entscheidung

Der größte Mehrwert entsteht dort, wo große Informationsmengen analysiert, strukturiert und in konkrete Handlungsempfehlungen übersetzt werden müssen. Regulatory Intelligence unterstützt dabei, Zusammenhänge sichtbar zu machen und Entscheidungen vorzubereiten. Im Mittelpunkt sollte deshalb nicht die möglichst weitgehende Automatisierung stehen, sondern die Frage, wo KI die Qualität, Geschwindigkeit und Nachvollziehbarkeit menschlicher Entscheidungen verbessern kann.

4. Governance zur Voraussetzung für KI machen

Bereits bei der Auswahl und Gestaltung eines Anwendungsfalls muss feststehen, welche Aufgaben automatisiert werden dürfen, wie die zugrunde liegende Logik geprüft wird, welche Freigaben erforderlich sind und wie eine lückenlose Audit-Spur entsteht.

Fazit

Die steigende regulatorische Komplexität verlangt mehr als zusätzliche Ressourcen. Unternehmen benötigen ein Compliance-System, das neue Anforderungen frühzeitig erkennt, mit relevanten Informationen verbindet und in konkrete Handlungen übersetzt. Regulatory Intelligence, KI-gestützte Anwendungen entlang der Compliance-Wertschöpfungskette und eine integrierte GRC-Plattform zeigen, wie diese Weiterentwicklung aussehen kann. Entscheidend ist ein durchgängiger Ansatz: Informationen müssen verknüpft, Abläufe aufeinander abgestimmt und Governance-Anforderungen von Beginn an berücksichtigt werden.

So kann Compliance schneller von einer neuen Anforderung zu einer belastbaren Entscheidung gelangen, ohne Nachvollziehbarkeit und Prüfbarkeit einzubüßen. Ob Unternehmen dieses Potenzial erschließen, entscheidet sich daher nicht allein an der eingesetzten Technologie. Ausschlaggebend ist die Fähigkeit, Komplexität beherrschbar zu machen und regulatorische Entscheidungen transparent und belastbar zu steuern.

Ihre Ansprechpartner



Marco Ehlert
Partner, Consulting
Tel: +49 30 208 88 1771
+49 172 286 56 73
Marco.Ehlert@forvismazars.com



Tobias Schuster
Senior Manager, Consulting
Tel: +49 211 83 99 219
+49 170 375 44 68
tobias.schuster@forvismazars.com



Fadi Ramadan
Partner, Tax & Accounting
Tel: +49 40 288 01 3553
+49 151 61 71 93 89
Fadi.Ramadan@forvismazars.com