



Governance, Risk & Compliance (GRC) Lösungen

Operationelle Risiken systematisch bewältigen und die digitale Transformation unterstützen

Dynamische Veränderungen im regulatorischen Umfeld sowie neue Geschäftsmodelle und Technologien eröffnen Unternehmen bedeutende Chancen zur Weiterentwicklung und Innovation. Eine Governance Risk Compliance (GRC)-Plattform ermöglicht eine funktionsübergreifende Risiko-Governance, sorgt für Transparenz und beschleunigt die Entscheidungsfindung. Deloitte unterstützt Sie bei der Auswahl, Anpassung, Implementierung und Umsetzung eines passenden GRC-Tools für Ihr Unternehmen.

GRC auf einen Blick

Warum GRC-Lösungen besonders jetzt wichtig sind? Dies hat mehrere Gründe, darunter das Verlangen von Stakeholdern nach starken Ergebnissen mit hoher Transparenz und die Verringerung der operationellen Risikokosten. Des Weiteren steigen Lieferkettenrisiken, Inflation sowie die Marktvolatilität und drängen so den Fokus von Unternehmen in Richtung Krisenmanagement, operativer Resilienz und Notfallplanung.

Die Abhängigkeit der Unternehmen von Geschäftsbeziehungen mit Drittparteien, insbesondere mit IKT-Anbietern, birgt ebenfalls Risiken und stellt eine Herausforderung für das Risikomanagement dar.

Ein GRC-Tool ermöglicht eine agile Sichtweise auf nicht-finanzielle Risiken in Ihrem Unternehmen. Die Integration von Risiko-, Compliance-, IT-, Sicherheits-, Geschäftskontinuitäts- und Lieferantenmanagementdaten auf einer gemeinsamen Plattform hilft, Ressourcen zu optimieren sowie redundante Prozessschritte zu reduzieren. Letztendlich verbessert es den Entscheidungsprozess und unterstützt die sofortige Reaktion auf Bedrohungen und Vorfälle. Die automatisierten Prozesse und Arbeitsabläufe

ermöglichen eine kontinuierliche Überwachung von Risiken und Kontrollen in Echtzeit. Eine gemeinsame Sicht auf Vorfälle, Risiken, kritische Geschäftsprozesse und die Leistung von Drittanbietern erhöht die Transparenz und hilft, das Risiko innerhalb der strategischen Grenzen zu verwalten.

Die Verwaltung von Risiko- und Compliance-Daten auf einer einzigen Plattform unterstützt die Grundprinzipien einer effektiven Risikodatenaggregation und Risikoberichterstattung und ermöglicht einen umfassenden Überblick über die Risiko- und Regulierungsagenda.

Governance: Etablierung interner Rahmenbedingungen für interne Kontrollmechanismen und das Risikomanagement.

Risk: Risikoidentifikation und -bewertung, Früherkennung, Zusammenführung und Monitoring von Risiken mittels Technologie.

Compliance: Einhaltung von gesetzlichen und internen Vorschriften mithilfe von Tools.



Operationelle Resilienz im Fokus für Finanzunternehmen und deren IKT-Anbieter

Die aufsichtsbehördlichen Anforderungen nach operationeller Resilienz werden immer deutlicher. Im Jahr 2020 legte die Europäische Kommission ein neues Paket für digitale Finanzen vor, um die Innovation und den Wettbewerb im digitalen Finanzwesen zu unterstützen und gleichzeitig den Verbraucherschutz zu gewährleisten, Risiken zu mindern und die Finanzstabilität zu erhöhen.

Als Teil dieses Pakets trat am 16. Januar 2023 der neue EU Digital Operational Resilience Act (DORA) in Kraft, der für Finanzunternehmen und IKT-Drittanbieter gilt, um die digitale Betriebs- und Cyber-Resilienz im Finanzsektor zu verbessern. Operationelle Resilienz konzentriert sich auf die Festlegung von Ausfallsicherheitsstandards für kritische Operationen und Kerngeschäftsbereiche, deren Unterbrechung für den weiteren Betrieb von wesentlicher Bedeutung wäre. Der Schwerpunkt liegt auf dem Management von IKT-Risiken, IKT-Vorfällen, Geschäftskontinuität und dem Management Dritter und führt einen einheitlichen Aufsichts- und Governance-Rahmen ein. GRC-Tools können Sie bei der Adaptierung der neuen DORA-Anforderungen unterstützen und die verschiedenen Risikodomänen verbinden.

GRC-Modul

Eine erfolgreiche Implementierung von GRC in Ihr Unternehmen bedeutet nicht die Erarbeitung von neuen Strukturen, sondern viel mehr die Entwicklung eines Ansatzes, mit dem sichergestellt wird, dass Arbeitskräfte und andere Stakeholder mit übereinstimmenden Informationen, Zielen, Maßnahmen und Kontrollen zusammenwirken, um mit Integrität zu handeln. Ausgewählte GRC-Module können an Ihre Geschäftsanforderungen angepasst werden.



Regulatorische Compliance

Überwachung regulatorischer Aktualisierungen, Entwicklung und Umsetzung von Kontrollen und Prozessen, um die Einhaltung von Änderungen der Rechtsvorschriften zu gewährleisten. Auditplanung und -durchführung



Operationelles Risiko & Internes Kontrollsystem

Betrachtung unternehmensweiter operationeller Risiken. Das in die Kernprozesse integrierte interne Kontrollsystem trägt dazu bei, das ordnungsgemäße Funktionieren der Geschäftsabläufe zu überwachen



BCM & Operationelle Resilienz

Business-Impact-Analyse, Business-Continuity-Planung und Krisenmanagement. GRC-Tools helfen bei Risikobewertungen, Notfallübungsplanung, Wiederherstellungsmanagement und Krisenkommunikation



IKT & Cyber Risk

Identifizierung potenzieller Schwachstellen, Steuerung möglicher IKT-Vorfälle, Durchführung von IKT-Kontrollen sowie Third-Party Risk Management von IKT-Dienstleistern



Third-Party Risikomanagement

Steuerung der Geschäftsbeziehungen mit Drittparteien. Third-Party Engagement Management und Monitoring der Performance und Risiken in einem Lieferanten Portal



ESG-Management

Management strategischer ESG-Ziele und Übergang zu einer grünen Wirtschaft, Analyse von ESG-Faktoren, Unterstützung bei der GHG Berechnung, ESG-Berichterstattung und -Offenlegungen

Deloitte GRC Transformation Services

Deloitte unterstützt Sie bei der Auswahl eines für Ihr Unternehmen passenden Tools und hilft Ihnen, dieses zu personalisieren und auf Ihr Unternehmen auszurollen. Unsere Expert:innen begleiten Sie und Ihr Unternehmen durch den gesamten Prozess einer erfolgreichen GRC-Implementierung.

- **Analyse**
Evaluierung und Assessment von aktuellen Risikomanagement-Lösungen
- **Risk Process Transformation**
Proposal eines optimierten Integrated Risk Management Konzepts sowie Erstellung einer Vision und Strategie für die Plattform
- **Auswahl des GRC-Tools**
Unterstützung bei der strategischen Entscheidung über die Auswahl eines passenden GRC-Tools basierend auf unserer Expertise
- **Implementierung**
Unterstützung bei Design und Erstellung sowie Integration des neuen GRC-Tools in die IT-Umgebung
- **Engagement Ihres Teams**
Entwickeln Sie Teamfähigkeiten, um führende GRC-Innovatoren zu werden
- **Fortlaufende Unterstützung**
Laufender technischer und methodologischer Support

Ihre Ansprechpersonen

Christa Janhsen

Partnerin

+43 1 537 00-4843
cjanhsen@deloitte.at

David Pewal

Senior Manager

+43 1 537 00-4817
dpewal@deloitte.at

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk von Mitgliedsunternehmen und deren verbundene Unternehmen innerhalb der „Deloitte Organisation“. DTTL („Deloitte Global“), jedes ihrer Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen. DTTL erbringt keine Dienstleistungen für Kundinnen und Kunden. Weitere Informationen finden Sie unter www.deloitte.com/about.

Deloitte Legal bezieht sich auf die ständige Kooperation mit Jank Weiler Operenyi, der österreichischen Rechtsanwaltskanzlei im internationalen Deloitte Legal-Netzwerk.