

GRC *aktuell*

Governance – Risiko – Compliance – Management
Fachzeitschrift für nachhaltige Unternehmensführung

Markus Fally | Markus Hölzl | Eva Maria Schrittwieser | Dieter Stangl-Krieger

Governance

„One-GRC“ für mehr Performance, Resilienz und Vertrauen
Governance im Finanzsektor
High Reliability Organizations

Risiko

Psychologie im Sicherheits- und Risikomanagement
Risikotraditionalisten vs Risikostrategen
Wenn Vertrauen zum Risiko wird

Compliance

Informationsfreiheitsgesetz: Überblick & Erfahrungen
Compliance als Wettbewerbsvorteil

Case Study

Hinschauen als Governance-Leistung

Interview

Rita Niedermayr, Österreichisches Controller-Institut

Service

GRC-Update – Überblick für die Praxis

„One-GRC“: Zusammenführung von GRC für mehr Performance, Resilienz und Vertrauen

Elias Polak / Peter Schentler



Elias Polak ist Managing Consultant für Risk & Compliance Excellence bei Horváth Österreich.



Dr. Peter Schentler ist Partner bei Horváth Österreich.

GRC-Funktionen sind häufig organisatorisch getrennt und historisch gewachsen. Dadurch entstehen Ineffizienzen, inkonsistente Chancen- und Risikoassessungen und Informationsverluste, die zu schlechter Entscheidungsqualität führen. „One-GRC“ konsolidiert, harmonisiert und integriert GRC-Funktionen entlang der sechs Dimensionen Governance & Organisation, Strategie, Prozesse, Methodik & Taxonomie, Kultur & Know-how und Daten & Technologie. Das schafft ein belastbares Gesamtbild über Chancen und Risiken, reduziert Aufwände und stärkt somit Performance, Resilienz und Vertrauen.

1. Ausgangslage: Warum GRC-Funktionen häufig zersplittert sind

Fragmentierte GRC-Funktionen sind keine Seltenheit. Viele Unternehmen managen ihre Risiken und damit einhergehende Chancen in thematisch abgesonderten Teilbereichen, die zu wenig miteinander kommunizieren bzw. interagieren. Folglich sind sie mit Ineffizienz, die Mehrkosten verursacht, und Ineffektivität konfrontiert, die zu Verlust an Informationsgehalt führt. Dies kann zu schlechteren Geschäftsentscheidungen führen, beispielsweise wenn die Entscheidung getroffen wird, einen Eintritt in einen neuen Markt nicht zu vollziehen, weil die Compliance die rechtlichen und politischen Gefahren als zu gravierend eingestuft hat, obwohl das Risikomanagement das ganzheitliche Risiko-Ertrags-Profil (inkl. rechtlichen und politischen Gefahren) des Markteintritts als positiv bewertet und folglich eine Durchführung empfohlen hätte.

Ein anonymisiertes Beispiel für eine fragmentierte GRC-Governance und -Organisation aus der Praxis stellt sich folgendermaßen dar: Ein international tätiges Industrieunternehmen mit rund 4.000 Mitarbeitenden betreibt sechs GRC-Funktionen. Das **Enterprise Risk Management (ERM)** bewertet Risiken in einer „5x5-Matrix“ mit Netto-Betrachtung und berichtet halbjährlich an den Vorstand. Die **Informationssicherheit** arbeitet mit Schutzbedarfsklassen nach ISO 27001 und einem eigenen Maßnahmenregister. Der **Datenschutz** dokumentiert Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzungen in einem separaten Tool und berichtet quartalsweise an die Informationssicherheit. Das **IKS** pflegt eine COSO-orientierte Kontrollmatrix in Excel und berichtet jährlich an die Compliance. Die **Compliance** führt ein jährliches Compliance-Risk-Assessment im Legal-System durch und berichtet an den CFO. Die **ESG-Funktion** hat im Rahmen der doppelten Wesentlichkeitsanalyse eine gänzlich eigene Risiko- und Auswirkungsbewertung aufgebaut und berichtet halbjährlich an den Head of Investor Relations. Verpflichtungen aus der CER-Richtlinie¹ (in Österreich RKEG²) werden durch eine Stabstelle beim CEO umgesetzt.

Sieben GRC-Mandate, sechs GRC-Funktionen, fünf Bewertungslogiken, vier Berichtslinien, drei Tools. Auf die Frage des Vorstands und des Aufsichtsrats nach den zehn wesentlichen Risiken des Unternehmens existieren unterschiedliche Antworten – abhängig davon, wer gefragt wird.

Solche ineffizienten Systeme werden in Unternehmen nicht bewusst geschaffen, sondern entstehen in der Regel aus drei unterschiedlichen Gründen:

- 1. Historisch gewachsene Silos, insbesondere durch steigende regulatorische Dichte:** Viele Funktionen wurden ad-hoc als Antwort auf einen konkreten Anlass etabliert – eine Prüfungsfeststellung, ein Vorfall, eine neue EU-Richtlinie bzw. ein neues Gesetz. Der jeweilige Aufbau war sachlich richtig, eine Abstimmung mit den bereits bestehenden Funktionen erfolgte selten. DSGVO, NIS2, DORA, CRA, CSRD bzw. ESG-Berichtspflichten, RKEG etc. erzeugen jeweils neue Pflichten mit eigenen Fristen. Unter dem Zeitdruck, diese einzuhalten, entstehen für neue rechtliche Vorgaben oft unabgestimmt neue Rollen, Prozesse und Tools je Vorgabe. Dadurch wachsen die internen GRC-Strukturen mit der Regulatorik mit, jedoch ohne ausreichende Koordination bzw. Zusammenführung.
- 2. Veraltetes GRC-Paradigma:** Die nach wie vor weitverbreitete Wahrnehmung von GRC als „Ausbremsen“, „regulatorisches Laster“, „Showstopper“ usw. ohne tangiblen Mehrwert für den Unternehmenserfolg sorgt dafür, dass bei Konzeption und Umsetzung von GRC-Systemen und -Strukturen Kosten und Mühen gespart werden. Man macht „das, was regulatorisch notwendig ist“. Wo GRC oder einzelne Funktionen davon – vermehrt zB IKS oder Compliance – primär als

¹ EU Critical Entities Resilience Directive.

² Resilienz kritischer Einrichtungen-Gesetz.

Kontrollinstanz wahrgenommen werden, ist die Bereitschaft zum Teilen von Informationen und damit auch zu Integration begrenzt.

3. **Trennende Governance und Organisation:** Unterschiedliche oder gar konkurrierende Berichtslinien (CEO, CFO, CIO, Legal etc), starre, rigide Bereichsgrenzen und Incentivierungssysteme, die Zusammenarbeit nicht belohnen, und ein latenter Wettbewerb um Ressourcen und Aufmerksamkeit erschweren die Zusammenarbeit.

Die notwendigen Anstrengungen für Konsolidierung, Harmonisierung und Integration werden daher häufig auf unbestimmte Zeit vertagt oder gänzlich unterlassen.

Der Beitrag zeigt, warum eine Zusammenführung fragmentierter GRC-Funktionen wirtschaftlich und organisatorisch sinnvoll ist: Kapitel 2 beleuchtet die negativen Konsequenzen der Fragmentierung sowie den Nutzen eines „One-GRC“-Ansatzes. Kapitel 3 zeigt, warum eine Zusammenführung in der Praxis möglich ist. Kapitel 4 beschreibt das Zielbild und die zentralen Gestaltungsdimensionen von „One-GRC“, bevor Kapitel 5 eine pragmatische Roadmap zur Umsetzung skizziert. Kapitel 6 fasst die zentralen Erkenntnisse zusammen und leitet konkrete Empfehlungen ab.

2. Die Konsequenzen einer fragmentierten GRC-Landschaft

Die Konsequenzen einer zersplitterten GRC-Landschaft treten selten als eigene Kostenposition in einer Ergebnisrechnung in Erscheinung, wirken aber in Summe erheblich. Es gibt drei übergeordnete negative Konsequenzen:

1. **Schwächere Performance:** Risiken und Chancen sind immer Querschnittsthemen und eng miteinander vernetzt. Ein Ausfall eines IT-Dienstleisters ist gleichzeitig ein Auslagerungs-, Informationssicherheits-, Kontinuitäts- und Reputationsrisiko. Werden Risiken nicht integriert beleuchtet und behandelt, gehen relevante Informationen verloren und Interdependenzen, Kumulationseffekte und mit Risiken einhergehende Chancen bleiben unerkannt. Nicht notwendige Redundanzen und Inkonsistenzen (unübersichtliche Toollandschaft, unterschiedliche Identifikations- und Bewertungslogiken etc), Reibung (zB konkurrierende Berichtslinien und unabgestimmte Prozesskalender etc) und Compliance-Lücken verursachen materielle und immaterielle Kosten.
2. **Fragilität:** Durch die Ineffizienz, Ineffektivität, den Informationsverlust und die Rigidität von stark fragmentierten Systemen und Strukturen können weniger Gefahren verhindert und bei eintretenden Schadensvorfällen und Krisen inadäquater reagiert werden. Der Unternehmenserfolg und -fortbestand sind schlechter abgesichert.
3. **Misstrauen:** Die durch fragmentiertes GRC verursachte schwächere Performance und Fragilität sorgt für langsam erodierendes Vertrauen aufgrund von häufiger auftretenden Problemen, unterschiedlichen Chancen- und Risikoassessungen, uneinheitlichen Prioritäten und widersprüchlichen Maßnahmenplänen. Kunden nehmen Compliance-Verstöße oder leichtsinnige Entscheidungen wahr. Für Eigentümer entsteht Unsicherheit, ob Managemententscheidungen auf einem vollständigen und belastbaren Chancen- und Risikobild beruhen. Partner hinterfragen, ob das Unternehmen verlässlich, resilient und anschlussfähig agieren kann. Regulatoren wiederum sehen in inkonsistenten Bewertungen, dezentralen Nachweisen und unklaren Verantwortlichkeiten Hinweise auf Steuerungs- und Kontrollschwächen. Das Unternehmen wirkt weniger transparent, steuerungsfähig und verlässlich.

3. Die Vorteile von „One-GRC“: Warum GRC-Funktionen zusammengeführt werden können und warum es sich lohnt

Überschneidungen und Zusammenhänge zwischen den GRC-Funktionen werden in der Praxis häufig übersehen, zum Großteil bedingt durch andere Prioritäten im operativen Alltagsgeschäft. Doch GRC-Funktionen besitzen mehr Ähnlichkeiten als auf den ersten Blick erkenntlich ist und eindeutig mehr als viele fragmentierte Organisationsstrukturen suggerieren:

- ▶ Jede GRC-Funktion verfolgt im Grunde dasselbe Ziel: Transparenz herstellen, Risiken des Themenfokus (ESG, Compliance etc) steuern und Chancen ergreifbar machen.
- ▶ Jede GRC-Funktion folgt einem Risiko- und Chancen-Prozess: Identifikation, Bewertung, Steuerung, Monitoring, Reporting. Unterschiedlich sind lediglich Anzahl/Namen der Prozessschritte, der Betrachtungsgegenstand/Themenfokus und die Granularität – nicht die Kernlogik.
- ▶ Jede GRC-Funktion benötigt ähnliche Daten: Schadenshöhen, Wahrscheinlichkeiten und Risikobewertungen, Prozesse und deren Kritikalität, Assets und Systeme, Dienstleister, Kontrollen, Maßnahmen, Schadenseintritte/Vorfälle etc.

Wo es ähnliche Ziele, Prozesse und Datengrundlagen gibt, liegt hohes Zusammenführungspotenzial vor. Skepsis entspringt oft dem fehlenden Glauben daran, dass das vorhin erwähnte veraltete GRC-Paradigma nicht verändert und eine trennende Unternehmenskultur und Organisationsstruktur nicht überwunden werden kann. Viele Transformationserfolge inner- und außerhalb des GRC-Bereichs

reichs zeigen jedoch, dass Wandel möglich ist. Zudem fehlt es oft an einem klaren Verständnis der Vorteile einer Zusammenführung. Der folgende Abschnitt erläutert diese klar und verständlich, um das Verständnis zu schärfen und deren Kommunikation zu ermöglichen.

Eine Zusammenführung durch den „One-GRC“-Ansatz transformiert die in Kapitel 2 beschriebenen negativen Konsequenzen in drei zentrale Wettbewerbsvorteile.

1. Von schwächerer zu stärkerer Performance:

Umsatzsteigerung: Der Informationsgehalt über die Unternehmenssituation, mit denen Entscheidungsträger arbeiten, steigt mit einem konsistent aggregierten Risiko- und Chancenbild; Interdependenzen und Kumulationseffekte werden in Betracht gezogen. Durch einen einheitlichen Überblick und erhöhten Informationsgehalt können bessere Entscheidungen getroffen werden, wodurch Chancen besser ergriffen werden können und die Risiko-Ertragsposition optimiert werden kann.

Kostensenkung: Redundanzen durch Doppelarbeit, uneinheitlichen Tooleinsatz, parallele Kommunikationswege etc werden reduziert und nur erhalten, wo es für Robustheit nötig ist. Die erste Verteidigungslinie wird deutlich entlastet und Zusatzaufwände sowie Bußgelder durch Compliance-Lücken vermieden.

2. Von Fragilität zu Resilienz:

Durch den erhöhten synergiebasierten Informationsgehalt und die damit möglichen besseren Entscheidungen kann nicht nur die allgemeine Performance verbessert werden. Gefahren können effektiver antizipiert, vermieden und mitigiert werden und in Krisen kann durch flexiblere Systeme und Strukturen adäquater reagiert werden, sodass die operative Handlungsfähigkeit aufrechterhalten werden kann und Schäden auf ein Minimum reduziert werden können.

3. Von Misstrauen zu Vertrauen:

Von „One-GRC“ gestärkte Performance und erhöhte Resilienz sorgen für mehr Vertrauen bei Kunden, Eigentümern, Partnern und Regulatoren. Geschäftsbeziehungen werden nachhaltig gestützt: Für Kunden wird das Unternehmen verlässlicher, weil Compliance-Verstöße, operative Brüche und leichtfertige Entscheidungen seltener auftreten bzw professioneller gesteuert werden. Eigentümer und Aufsichtsrat erhalten mehr Sicherheit, dass Managemententscheidungen auf einer vollständigen, belastbaren und funktionsübergreifend abgestimmten Informationsbasis beruhen. Partner können sich stärker auf schnittstellenfähige Prozesse, klare Ansprechpartner und stabile Leistungsfähigkeit verlassen. Regulatoren und Auditoren erkennen in konsistenten Bewertungen, zentral verfügbaren Nachweisen und eindeutigen Verantwortlichkeiten ein höheres Maß an Steuerungs- und Kontrollfähigkeit. Vertrauen entsteht damit nicht durch Kommunikation allein, sondern durch wiederholt beobachtbare Verlässlichkeit im Entscheiden, Handeln und Nachweisen.

4. Wie eine Zusammenführung aussieht – das Zielbild „One-GRC“

„One-GRC“ vereint drei Stoßrichtungen der Zusammenführung: Konsolidierung, Harmonisierung und Integration.

1. **Konsolidierung (Bündelung)** beinhaltet das organisatorische, kulturelle und technologische Zusammenlegen bzw Zentralisieren: Gebündelte Mandate, abgestimmte Berichtslinien, zentrale Vision und Ziele, kompakte Toollandschaft und Datenspeicherorte mit einem einheitlichen Datenmodell.
2. **Harmonisierung (Angleichung)** beinhaltet die Vereinheitlichung und Standardisierung von Wissen und Methodik: eindeutige Nomenklaturen und Taxonomien, einheitliches Risikoverständnis, sowie abgestimmte Visualisierungen.

Konsolidierung macht aus zwei Elementen ein neues gebündeltes Element. Harmonisierung gleicht die zwei Elemente dort aneinander an, wo Überschneidungen bzw Ähnlichkeiten bestehen, beide Elemente bleiben in abgestimmter Form parallel bestehen.

3. **Integration (Verzahnung)** beinhaltet die prozessuale, methodische und technologische Verzahnung bzw Schnittstellenbildung: Anbindungen zwischen Tools, zusammenhängende Risikoregister sowie gemeinsame Risikoidentifikationen und -bewertungen.

Es geht nicht darum, alles zu homogenisieren bzw zu generalisieren. Fachliche Spezialisierung bleibt notwendig – ein Datenschutzbeauftragter ist nicht durch einen strategischen Risikomanager ersetzbar. Ebenso bleibt die Funktionstrennung nach dem Vorbild des „Three-Lines-Modells“ nach dem Institute of Internal Auditors (IAA)³ erhalten: Die Interne Revision wird nicht Teil des „One-GRC-Office“, gesetzlich verankerte Unabhängigkeiten bleiben unberührt.

Die drei erläuterten Stoßrichtungen werden auf das „One-GRC-Framework“ angewendet. Dieses teilt die für „One-GRC“ weiterzuentwickelnden Bereiche in sechs Dimensionen mit jeweils drei

³ The Institute of Internal Auditors (IIA), The IIA's Three Lines Model. An Update of the Three Lines of Defense. Lake Mary (FL): IIA (2020).

Subteilen ein, um klar abgrenzbare, aber ineinandergreifende Arbeitsbereiche zu schaffen: Governance & Organisation, Strategie, Prozess, Methodik & Taxonomie, Kultur & Know-how, Daten & Technologie. Diese sind in Abbildung 1 dargestellt.



Abb 1: One-GRC-Framework.

- **Governance & Organisation:** Ein übergelagertes „One-GRC-Office“ fungiert als Business Partner für den Vorstand und Kontakt für Prüfer und Revision. Es ist dafür verantwortlich, die GRC-Funktionen zu koordinieren und Stringenz sowie Zusammenarbeit sicherzustellen. Das ERM fungiert als Dachfunktion, in der die (Risiko- und Chancen-) Fäden zusammenlaufen und in der aggregiert wird. Es ist dafür zuständig, alle Risiken und Chancen der anderen GRC-Funktionen zu bündeln, ein Gesamtrisiko aufzustellen und eine übergreifende Chancenlandschaft herauszuarbeiten. Aufgaben werden überschneidungsfrei zusammengeführt, Kommunikationslinien und Gremien definiert und abgestimmt:

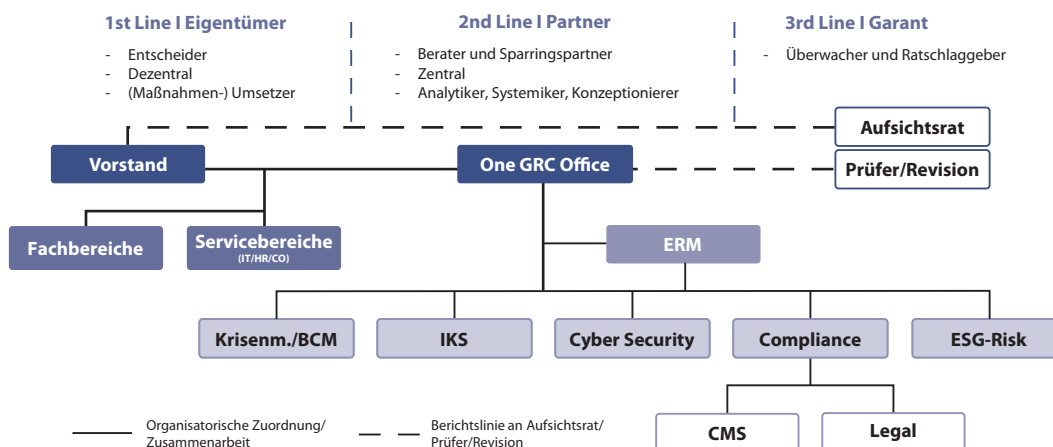


Abb 2: One-GRC-Governance & -Organisation.

Konkrete Rollen und Verantwortlichkeiten werden eindeutig festgelegt. Darüber hinaus unterstützt ein unternehmensweites risikoorientiertes Incentivierungssystem die proaktive Inanspruchnahme von und Beteiligung an „One-GRC“. Alles wird in einer zugänglichen schriftlichen Ordnung/Dokumentation festgehalten, um ein verlässliches „One-GRC“-Nachschlagewerk zu gewährleisten.

- **Strategie:** Eine Risikostrategie, die die Schnittstelle zur Geschäftsstrategie bildet und allen GRC-Funktionen eine gemeinsame, stringente Richtung vorgibt. Dafür werden sechs Kernfragen beantwortet:
1. Ist unsere Geschäftsstrategie im Einklang mit unserer Mission und unseren Werten?
 2. Welche Risiken und Chancen impliziert unsere Geschäftsstrategie?
 3. Was bedroht unsere Geschäftsstrategie – gibt es bessere Alternativen?
 4. Wie viel Risiko können wir uns maximal leisten?
 5. Wie viel Risiko wollen wir uns leisten?
 6. Wie wollen wir mit Risiko präferiert umgehen?

Die Antworten auf diese Fragen bilden die Leitplanken für alle GRC-Funktionen.

- **Prozess:** Ein Risikozyklus, der Überschneidungen der einzelnen Prozessschritte durch Konsolidierung, Harmonisierung und Integration nutzbar macht – gemeinsame einander ergänzende Risikoidentifikationen, abgestimmte Bewertungsprozesse, zusammengeführte Risikosteuerung (mithilfe zentraler Maßnahmenkataloge und den Leitplanken der Risikostrategie), verbundenes Monitoring und aufeinander abgestimmte Berichtsinhalte und -zyklen.
- **Methodik & Taxonomie:** Eine einheitliche Risikosprache als Fundament, gemeinsame Risikokategorien, akkordierte Granularitätsstufen, abgestimmte Zeithorizonte, harmonisierte Bewertungsskalen und eine zusammenhängende Aggregationslogik sowie die Definition einer Einflusstransitionslogik zur Unternehmensstrategie und -performance (z.B. Ergebnisrechnungsüberleitung). Diese legt fest, wie GRC methodisch mit Strategie, Finance und Controlling verzahnt wird.
- **Kultur & Know-how:** Ein gemeinsames Zielbild und Risikoverständnis, das im gesamten Unternehmen gelebt wird. GRC wird von der „Performance einschränkende Kontrollinstanz“ zum „Performance steigernden Business Partner“. Risiken werden von „etwas Schlechtem“ zur „Notwendigkeit für Geschäftserfolg und Ertrag“ und zur „Möglichkeit für Chancen“. Funktionsübergreifende Fortbildungen, gemeinsame Formate zum fachlichen Austausch und Rotation zwischen den Funktionen erhöhen das gegenseitige Verständnis und die Sprachfähigkeit gegenüber dem Management, den Fachabteilungen bzw dem Business.
- **Daten & Technologie:** Ein zentrales GRC-Toolset mit einem gemeinsamen Datenmodell als „Single Source of Truth“, ergänzt um Schnittstellen zu ERP-, HR- und sonstigen internen und externen Systemen, statt Insellösungen. Auf dieser Basis wird auch der Einsatz von KI ermöglicht bzw zumindest vereinfacht – etwa für das Mapping regulatorischer Anforderungen auf bestehende Kontrollen, für die Auswertung von Vorfalldaten, die Inklusion von Informationen in natürlicher Sprache in Risikosimulationen und -bewertungen, oder für die Erstellung von Berichtsentwürfen.

5. Roadmap zu „One-GRC“

Die Roadmap zu „One-GRC“ bietet ein Phasenmodell mit fünf Abschnitten, um „One-GRC“ ambitionsgerecht und wirtschaftlich zu verwirklichen: Bestandsaufnahme & Ambitionsniveau, Zielbildkonzeption, Implementierungsplanung, Umsetzung, Erfolgssicherstellung. Eine Übersicht findet sich in Abbildung 3.

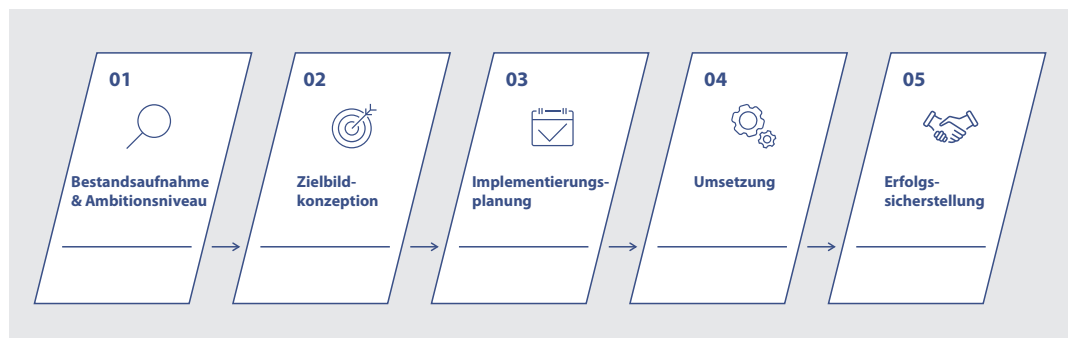


Abb 3: One-GRC-Roadmap.

„Phase 1 – Bestandsaufnahme & Ambitionsniveau“ umfasst die Erstellung einer GRC-Landkarte, die den aktuellen Status aus der Perspektive der sechs Dimensionen beleuchtet – daraufhin wird diese Ist-Aufnahme in ein Reifegradmodell eingeordnet. Zudem wird ein klares Ambitionsniveau festgelegt – dimensionsübergreifend und dimensionsspezifisch: Welcher Reifegrad wird angestrebt?

„Phase 2 – Zielbild“ enthält die Konzeption des Zielbilds entlang der sechs Dimensionen. Das Zielbild definiert den zukünftigen Soll-Zustand pro Dimension in Form von Fachkonzepten und Maßnahmen. Die konkrete Ausgestaltung berücksichtigt das festgelegte Ambitionsniveau, Machbarkeit und Wirtschaftlichkeit. Bei der Schaffung des Zielbilds ist zudem auf die Verzahnung mit bereits laufenden GRC- und/oder Regulatorikprojekten zu achten – beispielsweise zu NIS2, RKEG oder CRA.

„Phase 3 – Implementierungsplanung“ beinhaltet die Überleitung von Konzept zu Umsetzung mithilfe eines Fahrplans mit klaren Meilensteinen zur Implementierung der Fachkonzepte und Maßnahmen einschließlich der Berücksichtigung von Ressourcen, Verfügbarkeiten und Stakeholder-Interessen. Nutzen und Aufwand werden dabei mitgedacht. So werden zum Beispiel Quick Wins, wie eine gemeinsame Taxonomie oder ein abgestimmter Reportingkalender, vorgezogen und Tool-Konsolidierungen mittelfristig geplant.

„Phase 4 – Umsetzung“ umfasst die sukzessive Umsetzung der Implementierungsplanung. Neue Governance-Strukturen gehen live, neue Prozesse durchlaufen die ersten Piloten, Methodiken & Taxonomie finden Anwendung, Kultur & Know-how werden ua durch Veranstaltungen, Schulungen und Workshops geprägt und gefördert und neue Daten- & Technologie-Architekturen technisch verwirklicht.

„Phase 5 – Erfolgssicherstellung“ enthält die Erhebung und Sicherung der Wirksamkeit des neuen GRC entlang der drei Nutzenkategorien „stärkere Performance“, „Resilienz“ und „mehr Vertrauen“ anhand von Wertschöpfungsleitfragen, daraus abgeleiteten KPIs und darauf basierender Korrekturmaßnahmen.

6. Fazit & Empfehlungen

Fragmentierte GRC-Funktionen verursachen Ineffizienz und Ineffektivität. Folglich fallen nicht notwendige Aufwände an und Informationsgehalt geht verloren, der in Anbetracht steigender Unsicherheiten essenziell für fundierte Geschäftsentscheidungen ist. „One-GRC“ schafft Abhilfe, indem es die GRC-Funktionen konsolidiert, harmonisiert und integriert. Das Resultat ist bessere Performance, erhöhte Resilienz und gestärktes Vertrauen. Wir schlagen drei Schritte vor, um die Reise zu „One-GRC“ zu starten:

1. Kommunizieren Sie den Mehrwert von GRC klar, konsistent und verständlich – einschließlich der zugrunde liegenden Narrative, Einstellungen und Grundverständnisse.
2. Priorisieren und fokussieren Sie Quick Wins bei der Zusammenführung, wenn es um das Erlangen und Verwenden erster Ressourcen geht.
3. Nutzen Sie regulatorische Anlässe wie NIS2 und RKEG als Aufhänger und Treiber für „One-GRC“, also als Ansporn bzw Anlass, GRC neu zu denken und zum Business Partner zu transformieren.

Auf den Punkt gebracht

Ausgangslage: GRC-Funktionen sind in vielen Organisationen historisch getrennt gewachsen. Das erzeugt Redundanzen, inkonsistente Chancen- und Risikoaussagen, unübersichtliche Toolandschaften, Informationsverlust und Compliance-Lücken.

Machbarkeit: Alle GRC-Funktionen verfolgen dieselben Kernziele, folgen einem ähnlichen Risikomitigationszyklus und benötigen ähnliche Daten – darin liegt das Zusammenführungspotenzial.

Zielbild: Der „One-GRC“-Ansatz führt organisatorisch und kulturell zusammen und verzahnt Prozesse, Methodik und Daten – entlang von sechs Dimensionen und ohne die Funktionstrennung des Three-Lines-Modells aufzugeben.

Nutzen: Konsolidierung und Integration senken Kosten, entlasten die erste Verteidigungslinie und liefern der Geschäftsführung ein konsistentes Gesamtchancen und -risikobild. Performance, Resilienz und Vertrauen werden gestärkt.

Vorgehen: Bestandsaufnahme und Ambitionssetzung, Zielbild, Roadmap, Umsetzung, Erfolgs-sicherstellung – iterativ und verzahnt mit laufenden Regulatorikprojekten.

GRC-Update II

Überblick für die Praxis

Victoria Typpelt

Verlautbarungen II

Die *Europäische Kommission* hat die überarbeiteten European Sustainability Reporting Standards (ESRS) am 3. 7. 2026 als delegierte Verordnung erlassen, um eine Vereinfachung der Nachhaltigkeitsberichterstattung und eine Verringerung des Berichtsaufwands zu erzielen (<https://tinyurl.com/xrnyvnt3>).

Die *Europäische Kommission* hat einen delegierten Rechtsakt für einen freiwilligen EU-Nachhaltigkeitsstandard verabschiedet, der KMU eine praxistaugliche Berichterstattung ermöglichen soll (<https://tinyurl.com/mr44mtz3>).

Das *International Accounting Standards Board (IASB)* hat den neuen Standard IFRS 20 „Regulatorische Vermögenswerte und regulatorische Schulden“ herausgegeben, welcher für eine bessere Vergleichbarkeit die Bilanzierung von preisregulierten Geschäftsvorfällen regelt und für Geschäftsjahre ab dem 1. 1. 2029 in Kraft tritt (<https://tinyurl.com/2jn64a9u>).

Das *International Accounting Standards Board (IASB)* hat die Änderung „Fair Value Option for Investments in Associates and Joint Ventures (Amendments to IAS 28)“ veröffentlicht, welche die Anwendungsberechtigung der Fair-Value-Option präzisiert (<https://tinyurl.com/2mhahky>).