



White Paper  
Governance, Risikomanagement und Compliance:  
Nachhaltigkeit und Integration unterstützt durch Technologie

# White Paper

## Governance, Risikomanagement und Compliance: Nachhaltigkeit und Integration unterstützt durch Technologie

Herausgegeben von  
PricewaterhouseCoopers AG, Frankfurt am Main

Von  
Christof Menzies  
Alan Martin  
Michael Koch  
Carsten Trebuth  
Steffen Esche  
Thomas Heinze  
Christiane Roth  
Christoph Schellhas  
Philipp Stähle

## Executive Summary

Aufgrund der zunehmenden und komplexer werdenden Anforderungen der Stakeholder gewinnen die Themen Governance, Risikomanagement und Compliance (GRC) immer mehr an Bedeutung.

Der strategische und ganzheitliche Umgang mit GRC schafft Wettbewerbsvorteile und generiert einen signifikanten Mehrwert. Ziel ist es, GRC-Initiativen in das operative Tagesgeschäft einzubetten und soweit möglich zu integrieren, um Synergiepotenziale zu nutzen.

Der Einsatz von Technologie ist ein wesentlicher Erfolgsfaktor eines ganzheitlichen GRC-Managements. Technologie trägt dazu bei, unmittelbar Nutzen und Mehrwert für das Unternehmen zu generieren.

Mehr als je zuvor werden Unternehmen mit komplexen Regularien und weit reichenden Stakeholder-Anforderungen konfrontiert und stehen im Licht der Öffentlichkeit. In diesem Umfeld globale Chancen zu nutzen, bedeutet umso mehr, auch Verantwortung für globale Corporate Governance zu übernehmen. Kapitalmärkte, Geschäftspartner, Mitarbeiter und öffentliche Einrichtungen sind nur Beispiele für Stakeholdergruppen, die von Unternehmen fordern, dieser Verantwortung gerecht zu werden. Für Unternehmen bedeutet das, die Definition und Umsetzung ihrer unternehmensweiten Strategien entsprechend auszurichten. Als Folge haben die Themen Governance, Risikomanagement und Compliance (GRC) einen neuen, noch nicht dagewesenen Stellenwert auf der Ebene der Unternehmensführung erlangt.

Unternehmen, die nachhaltig erfolgreich sind, haben ein klar erkennbares Brand Image und werden dem Corporate Citizenship-Anspruch und den Erwartungen der Stakeholder gerecht. Dies bedeutet jedoch auch, die notwendigen Maßnahmen dauerhaft in die Struktur des gesamten Unternehmens einzubetten. Diese Einbettung wird erst erreicht, wenn Unternehmen den Compliance-Anforderungen nicht mehr überwiegend reaktiv und mit isolierten Maßnahmen begegnen. Erst über einen strategischen und ganzheitlichen Umgang mit Governance, Risikomanagement und Compliance wird es möglich, Wettbewerbsvorteile zu erzielen und einen signifikanten Mehrwert zu generieren.

Dieses White Paper zeigt die Vision eines ganzheitlichen GRC-Ansatzes und beschreibt einen Weg, wie Unternehmen ihre Governance-, Risikomanagement- und Compliance-Initiativen integrieren und in das operative Tagesgeschäft einbetten können. Das Ziel besteht darin, die GRC-Aktivitäten von einem reinen Kostenfaktor in ein strategisches Werkzeug der Unternehmensführung zu überführen. Gelingt die Überführung, wird ein flexibler und effektiver Umgang mit sich verändernden Stakeholder-Anforderungen ermöglicht und eine Basis für den langfristigen Unternehmenserfolg geschaffen.

Der Einsatz von Technologie nimmt bei der Umsetzung dieser Vision eine Schlüssel-funktion ein. Am Beispiel existierender Softwarelösungen der SAP AG wird dargestellt, wie die Technologie ein Unternehmen auf dem Weg zu einem ganzheitlichen GRC-Management unterstützen kann. Es wird gezeigt, wie deren Einsatz sowohl beim Management der GRC-Aktivitäten als auch auf der Ebene der Geschäftsprozesse unmittelbar dazu beiträgt, einen zusätzlichen Nutzen zu generieren. Ein Beispiel ist die Information des Managements über den Fortschritt verschiedener GRC-Initiativen mit Hilfe einer integrierten Reporting-Funktionalität. Auch die Einbettung von Compliance-Anforderungen in die Workflows des ERP-Systems oder die technologische Unterstützung beim Aufbau eines effektiven und effizienten Berechtigungsmanagements helfen, Nutzen und Mehrwert zu generieren.

Die Technologie nimmt auch in strategischer Hinsicht eine wesentliche Rolle ein – beispielsweise durch die Bereitstellung einer integrierten Plattform für GRC-relevante Informationen. Über diese Plattform kann der Zusammenhang zwischen den Stakeholder-Anforderungen, den relevanten Risiken, den Richtlinien, den unternehmensinternen Abläufen und dem internen Kontrollsystem abgebildet werden. Die so entstehende Transparenz ermöglicht es, Synergiepotenziale verschiedener GRC-Initiativen zu erkennen. Mit Hilfe dieser Transparenz können redundante GRC-Aktivitäten über einen ganzheitlichen GRC-Ansatz beseitigt und die Performance-Ziele des Unternehmens direkt unterstützt werden.

## Inhaltsverzeichnis

Executive Summary .....	3
Abbildungsverzeichnis .....	5
A Steigender Handlungsbedarf .....	6
B Ganzheitliches GRC-Management.....	10
1 Nutzen eines ganzheitlichen GRC-Managements .....	10
2 Nachhaltigkeit von GRC-Initiativen .....	11
3 Integration von GRC-Initiativen .....	15
C Technologie als entscheidender Erfolgsfaktor am Beispiel von SAP-Lösungen .....	19
1 IT-Unterstützung der Governance-Prozesse .....	20
2 IT-Unterstützung der Risikomanagement- und Compliance-Prozesse .....	22
3 IT-Unterstützung von Compliance innerhalb der Geschäftsprozesse .....	24
4 IT-Unterstützung von Compliance innerhalb der Berechtigungs- und IT-Prozesse .....	27
D Umsetzung eines ganzheitlichen GRC-Managements .....	30
E Fazit .....	35
F Quellen- und Literaturverzeichnis .....	36
Ansprechpartner.....	37

## Abbildungsverzeichnis

Abb. 1	Erweitertes Compliance-Verständnis .....	6
Abb. 2	Isolierte und fragmentierte Betrachtung von Governance, Risikomanagement und Compliance .....	7
Abb. 3	Integrierte Betrachtung von Governance, Risikomanagement und Compliance .....	11
Abb. 4	Sustainability-Elemente .....	12
Abb. 5	Ebenen der Integration .....	16
Abb. 6	Technologieeinsatz im Rahmen eines ganzheitlichen GRC- Managements .....	20
Abb. 7	Klassifizierung interner Kontrollen .....	25
Abb. 8	Transformationsprozess für ein nachhaltiges GRC-Management .....	31
Abb. 9	Schematische Darstellung einer Rule Base .....	33

## A Steigender Handlungsbedarf

Die gestiegene Anzahl und die Komplexität der regulatorischen Anforderungen, die hohen Erwartungen der Stakeholder sowie der wachsende Druck der Finanzmärkte sind nur einige Beispiele dafür, dass die Themen Corporate Governance, Risikomanagement und Compliance (GRC) zunehmend in den Mittelpunkt rücken. In der Regel werden diese Themen von vielen Unternehmen überwiegend losgelöst, operativ und nicht strategisch betrachtet. Die daraus abgeleiteten Maßnahmen sind eher kurzfristig gestaltet. Langfristig den größtmöglichen Nutzen zu erzielen erfordert jedoch, dass Unternehmen ihren bisherigen GRC-Ansatz überdenken und diesen strategisch und proaktiv ausrichten.

90 Prozent der Führungskräfte messen dem Thema Compliance eine hohe Bedeutung bei.<sup>1</sup>

Der strategische und proaktive Umgang mit Governance, Risikomanagement und Compliance trägt dabei nicht nur zur effektiven und effizienten Erfüllung von aktuell relevanten Compliance-Anforderungen bei, sondern ist auch mit einem zusätzlichen Nutzen verbunden. Ein Unternehmen kann beispielsweise flexibler auf neue und veränderte Anforderungen reagieren, seine öffentliche Reputation sowohl durch die Erfüllung von gesetzlichen als auch freiwilligen Anforderungen bewusst steigern, dabei einen nachhaltig profitablen Geschäftsbetrieb sicherstellen und letztendlich GRC als Wettbewerbsvorteil nutzen.

### Definition Governance, Risikomanagement und Compliance

**Governance** wird als Ordnungsrahmen für die zielgetreue, verantwortungsvolle, ethische und gesetzeskonforme sowie auf langfristige Wertschöpfung und Steigerung des Unternehmenswerts ausgerichtete Leitung und kontrollierende Steuerung eines Unternehmens beschrieben.<sup>2</sup> Im Mittelpunkt der Governance-Prozesse stehen dabei die Festlegung und Überwachung der übergeordneten Strategien und Ziele, die Definition relevanter organisatorischer Strukturen, die Steuerung des Unternehmens durch die Definition von unternehmensweiten Regeln und Richtlinien, die Messung und Überwachung der Leistung sowie die Kommunikation und Publikation relevanter Informationen.

Mit Hilfe eines effektiven **Risikomanagements** wird eine optimale Berücksichtigung und Kompensation von Risiken gewährleistet, welche das Erreichen der Unternehmensziele mittel- und langfristig gefährden können.<sup>3</sup> Ein effektiver Risikomanagementprozess umfasst neben der Risikoidentifikation und -dokumentation auch die Risikoanalyse, die Definition und Durchführung von Maßnahmen zum Management der identifizierten Risiken sowie eine kontinuierliche Überwachung der Maßnahmen.

Unter **Compliance** wird die Einhaltung sämtlicher Regeln und Standards verstanden, von denen ein Unternehmen betroffen ist.<sup>4</sup> Nach einer erweiterten Definition kann unter diesem Begriff die Einhaltung sowohl interner und externer Standards, Vorgaben und Regularien als auch freiwilliger Verpflichtungen und Vereinbarungen verstanden werden. Die Compliance-Prozesse im Unternehmen stellen sicher, dass die Stakeholder-Anforderungen und daraus abgeleitete Maßnahmen identifiziert und priorisiert, die Effektivität der Maßnahmen zur Erfüllung der Anforderungen getestet, identifizierte Schwachstellen behoben und sämtliche Compliance-Aktivitäten kontinuierlich überwacht werden. Abb. 1 stellt das zugrunde gelegte Compliance-Verständnis dar.

### Effektive Überwachung und Management von Risiken durch Compliance mit



Abb. 1 Erweitertes Compliance-Verständnis

Unternehmen werden mit einem zunehmend höheren Non-Compliance-Risiko und wachsenden Compliance-Kosten konfrontiert. Ein Anstieg von Risiko und Kosten folgt aus dem stetig steigenden Umfang und der Komplexität von sich verändernden Stakeholder-

<sup>1</sup> Vgl. Universität Hamburg: Umfrageergebnisse (2006).

<sup>2</sup> Vgl. PwC/BDI (2005), S. 7 und PwC/BDI (2002) S. 6.

<sup>3</sup> Vgl. COSO (2004) S.13 ff.

<sup>4</sup> Vgl. PwC (2004) S. 9 ff. und Menzies (2006), S. 2 ff.

Erwartungen. Dies zeigen beispielsweise die regulatorischen Anforderungen, die auf den Sarbanes-Oxley Act, Basel II oder den Foreign Corrupt Practices Act (FCPA) zurückzuführen sind. Die Projekte der vergangenen Jahre verdeutlichen, dass selbst die Erfüllung einer einzelnen Compliance-Anforderung eine große Herausforderung für Unternehmen darstellt und mit einem hohen Aufwand verbunden sein kann. Zudem ist ihre erstmalige Erfüllung keineswegs ein Garant für die nachhaltige Umsetzung einer Compliance-Initiative und die Vermeidung von Non-Compliance.

In der Praxis werden Compliance-Anforderungen oft isoliert und losgelöst von existierenden Strukturen und Abläufen umgesetzt.

In der Vergangenheit erfolgte oftmals eine krisengetriebene Umsetzung von Compliance-Anforderungen meist innerhalb sehr kurzer Zeiträume und unter einem hohen Termindruck. Aufgrund des hohen Zeitdrucks konnten Unternehmen bei der Umsetzung der Compliance-Projekte oft nur sehr begrenzt Überlegungen hinsichtlich einer nachhaltigen Gestaltung von Prozessen, Organisationsstrukturen und Technologien berücksichtigen. Eine hinreichende Einbettung der Compliance-Aktivitäten in die existierenden Unternehmensprozesse stand bei der Projektumsetzung nicht unmittelbar im Fokus. Viele Compliance-Anforderungen werden daher in der Praxis isoliert und weitgehend losgelöst von Strukturen und Abläufen umgesetzt, die im Unternehmen bereits für andere Anforderungen etabliert wurden. Ein derartiges Umsetzungsvorgehen führt auch dazu, dass die Compliance-Initiative<sup>5</sup> mit der erstmaligen Erfüllung nicht gleichzeitig in den nachhaltigen Regelbetrieb überführt wird. Bleibt diese Situation unverändert, sind ein hoher, regelmäßig wiederkehrender Aufwand zur Einhaltung der Compliance-Anforderung, eine hohe Ressourcenbindung und eine geringe Einbindung der Prozessverantwortlichen und -beteiligten hinsichtlich der Compliance-relevanten Themen die Folge.

Neben der isolierten Umsetzung der verschiedenen Compliance-Initiativen werden auch die Themen Governance, Risikomanagement und Compliance derzeit in vielen Unternehmen losgelöst voneinander betrachtet.

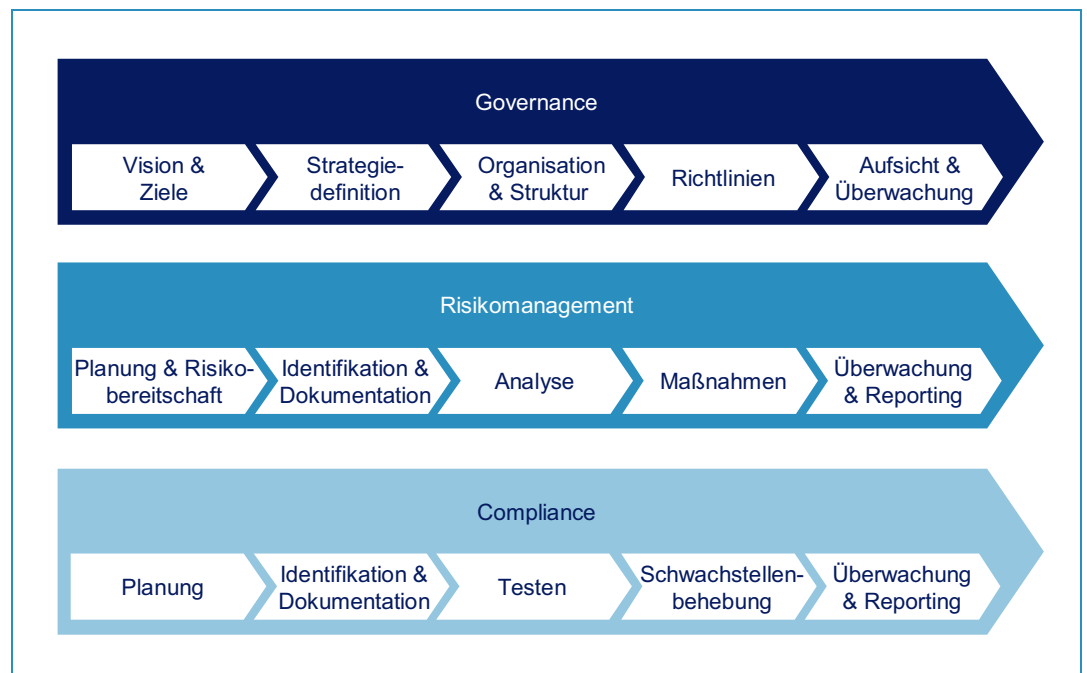


Abb. 2 Isolierte und fragmentierte Betrachtung von Governance, Risikomanagement und Compliance

Anforderungsübergreifend werden die Themen Governance, Risikomanagement und Compliance derzeit in vielen Unternehmen noch getrennt voneinander betrachtet (vgl. Abb. 2). Diese isolierte Betrachtung hat zur Folge, dass beispielsweise das Thema Governance oft auf formale Vorgaben reduziert wird, das Risikomanagement vorwiegend auf operative Risiken fokussiert und das Thema Compliance in erster Linie auf gesetzliche Regelungen und Standards bezogen wird. Mit dem Begriff Compliance sollte allerdings nicht nur die Einhaltung von gesetzlichen Regelungen und Standards verbunden werden, sondern auch die Einhaltung von freiwilligen Verpflichtungen und Vereinbarungen. Eine adäquate Verknüpfung des Risikomanagements als Frühwarnsystem mit den Compliance-

<sup>5</sup> Der Begriff „Compliance-Initiative“ bezieht sich auf ein Programm zur Einhaltung einzelner Stakeholder-Anforderungen, welches häufig von Governance- und Risikomanagement-relevanten Aspekten losgelöst umgesetzt wird. Der im Folgenden verwendete Begriff „GRC-Initiative“ bezieht sich hingegen auf Programme, welche auch die Aspekte Governance und Risikomanagement angemessen in Betracht ziehen.

Initiativen und der Corporate Governance bzw. der daraus resultierenden GRC-Aktivitäten<sup>6</sup> ist oftmals nicht gegeben. Außerdem wird den Abhängigkeiten zwischen den verschiedenen Compliance-Initiativen und den sich daraus ergebenden Synergiepotenzialen meist nicht die notwendige Aufmerksamkeit beigemessen. Bei der Umsetzung der verschiedenen Compliance-Initiativen kommen oft unterschiedliche Ansätze und Vorgehensweisen zum Einsatz, obwohl beispielsweise einheitliche Dokumentationsstandards oder Tools genutzt werden könnten.

58 Prozent der befragten Unternehmen halten ihre eigene Vorgehensweise bei der Umsetzung von Compliance-Anforderungen für ineffizient.<sup>7</sup>

Als Folge daraus entstehen zahlreiche Insellösungen sowohl in prozessualer, organisatorischer als auch technologischer Hinsicht. Diese Insellösungen führen zum Beispiel zu

- einer erhöhten Schnittstellenkomplexität zwischen den einzelnen Risikomanagement- und Compliance-Initiativen bzw. GRC-Aktivitäten sowie den entsprechenden Geschäftsprozessen,
- einer unzureichend integrierten Technologieunterstützung und damit zu einer heterogenen GRC-IT-Landschaft,
- heterogenen Berichtsstrukturen aufgrund von unterschiedlichen Berichtsperioden, Datenbanken oder Reporting-Tools und
- einem fehlenden integrierten Überblick über den gesamten GRC-Status des Unternehmens.

#### Beispiel : Heterogene Berichtsstrukturen bei isolierter Betrachtung von Initiativen

Eine Konsequenz der isolierten Betrachtung verschiedener Risikomanagement- und Compliance-Initiativen ist das Entstehen heterogener Berichtsstrukturen. Aufgrund der heterogenen Strukturen ist ein umfangreicher Überblick über die wesentlichen Compliance- und Risiko-Indikatoren und damit über den ganzheitlichen Compliance- und Risiko-Status des Unternehmens in der Regel nicht möglich. Dies ist insbesondere für das Senior Management eines Unternehmens von großer Bedeutung, denn durch ein unzureichendes GRC-Monitoring und -Reporting wird das Risiko erhöht, die Anforderungen einer bestimmten Compliance-Initiative nicht zu erfüllen bzw. mit Risiken nicht effektiv und effizient umgehen zu können.

Die heterogenen Berichtsstrukturen sind neben der oftmals fehlenden organisatorischen Integration auch auf den Einsatz unterschiedlicher IT-Applikationen innerhalb der verschiedenen Risikomanagement- und Compliance-Initiativen zurückzuführen. Diese Applikationen besitzen oftmals keine Schnittstellen, so dass zahlreiche Aktivitäten manuell durchgeführt werden müssen. Dies führt wiederum zu einer erhöhten Fehleranfälligkeit des Reportings als auch zu erhöhten Kosten. Heterogene Systeme führen somit zu aufwendigen Reportingaktivitäten, die mit Hilfe der verschiedenen Applikationen durchgeführt werden. Gleichzeitig ermöglichen die verschiedenen eingesetzten Applikationen in der Regel nicht, dass vergleichbare Kriterien, Standards oder Methoden bei der Analyse von Risiken bzw. Compliance-relevanten Informationen unternehmensweit eingesetzt werden. In der Konsequenz gestalten sich die effektive und effiziente Aggregation von Compliance- und Risiko-relevanten Informationen und das strukturierte Reporting dieser Informationen an das Management als problematisch und sehr komplex.

Die vorangegangenen Ausführungen verdeutlichen den Handlungsbedarf, der für viele Unternehmen aktuell besteht, um in Zukunft eine effektive und effiziente Umsetzung der relevanten Stakeholder-Anforderungen zu realisieren. Der Weg, um diese Herausforderungen zu bewältigen, besteht in einem ganzheitlichen GRC-Management. Erforderlich ist eine übergreifende, strategische Betrachtung von Governance, Risikomanagement und Compliance sowie des damit verbundenen dauerhaften und stabilen Regelbetriebs mit den folgenden übergeordneten Zielen:

- die Stakeholder-Anforderungen in dem komplexen und dynamischen Umfeld möglichst optimal zu erfüllen und damit das Non-Compliance-Risiko zu minimieren,
- die Effektivität von GRC-Initiativen langfristig sicherzustellen und die Kosten für GRC durch eine Steigerung der Effizienz zu senken,
- Synergieeffekte zur Vermeidung von Redundanzen zu nutzen und
- die GRC-Ziele und -Aktivitäten mit den Unternehmenszielen in Einklang zu bringen, so dass Compliance und Risikomanagement als integrale und Wert bringende Bestandteile des Unternehmens wirken können.

<sup>6</sup> Im Folgenden werden alle Aktivitäten, die in Zusammenhang mit Governance, Risikomanagement und Compliance stehen, als GRC-Aktivitäten bezeichnet.

<sup>7</sup> Vgl. Universität Hamburg: Umfrageergebnisse (2006).

Im folgenden Kapitel wird die unternehmensspezifische Gestaltung eines nachhaltigen GRC-Managements näher betrachtet, welches als strategisches Werkzeug im Unternehmen eingesetzt werden kann und langfristig den Nutzen aus der gezielten Erfüllung der Stakeholder- bzw. Compliance-Anforderungen maximiert.

*As individual issues, governance, risk management, and compliance have always been fundamental concerns of business and its leaders. What is new is an emerging perception of GRC as an integrated set of concepts that, when applied holistically within an organisation, can add significant value and provide competitive advantage.*  
Samuel DiPiazza Jr., CEO PricewaterhouseCoopers<sup>8</sup>

---

<sup>8</sup> Vgl. PwC (2005).

## B Ganzheitliches GRC-Management

Ein ganzheitliches GRC-Management beinhaltet

- die Nachhaltigkeit einzelner, im Unternehmen umgesetzter GRC-Initiativen und
- die Integration von GRC-Initiativen.

Ganzheitliches GRC-Management umfasst die nachhaltige Gestaltung der im Unternehmen relevanten GRC-Initiativen sowie deren methodische und inhaltliche Integration.

**Nachhaltigkeit** bedeutet in diesem Zusammenhang eine enge Verknüpfung der Elemente Governance, Risikomanagement und Compliance sowie eine unter Kosten- und Nutzen Gesichtspunkten optimale Einbettung von GRC-Initiativen in die existierenden Unternehmensstrukturen und -abläufe. GRC-Aktivitäten sollten nicht parallel zum aktuellen Tagesgeschäft verlaufen, sondern so weit wie möglich in die operativen Prozesse eingebettet sein.

Unter **Integration** als Teil des ganzheitlichen GRC-Managements wird die methodische und inhaltliche Zusammenführung verschiedener GRC-Initiativen verstanden. Die Notwendigkeit eines ganzheitlichen GRC-Managements wird aus den Umfrageergebnissen der von PricewaterhouseCoopers durchgeführten 10<sup>th</sup> Annual Global CEO Survey ersichtlich.<sup>9</sup> Darin sehen 40 Prozent der an der Umfrage teilnehmenden CEO in der Überregulierung ein wesentliches Geschäftsrisiko; 33 Prozent zeigen sich diesbezüglich sogar sehr besorgt. Ein ganzheitliches GRC-Management trägt dazu bei, diesem Risiko durch einen effektiven und effizienten Umgang mit aktuellen bzw. zukünftigen Anforderungen entgegen zu wirken.

Um ein ganzheitliches GRC-Management umzusetzen, ist es erforderlich, den im Unternehmen existierenden Compliance-Ansatz schrittweise über die unternehmensweite und integrative Betrachtung von Governance, Risikomanagement und Compliance zu einem ganzheitlichen Ansatz weiter zu entwickeln. In den folgenden Abschnitten wird zunächst der Nutzen erläutert, den Unternehmen durch ein ganzheitliches GRC-Management erzielen können. Anschließend wird auf die Nachhaltigkeit und Integration von GRC-Initiativen eingegangen.

### 1 Nutzen eines ganzheitlichen GRC-Managements

89 Prozent der befragten CEO sind der Meinung, dass der effektive Umgang mit GRC einen positiven Einfluss auf die Reputation bzw. die Marke des Unternehmens hat.<sup>10</sup>

Bereits die nachhaltige Gestaltung einzelner GRC-Initiativen ist mit zahlreichen kurz- und mittelfristigen Nutzenpotenzialen, wie zum Beispiel der gesteigerten Effizienz innerhalb der Prozesse, verbunden. Um jedoch den größtmöglichen Nutzen im Umgang mit Governance, Risikomanagement und Compliance zu erzielen, umfasst ein ganzheitliches GRC-Management neben der nachhaltigen Gestaltung der Initiativen auch deren Integration. Zum Nutzen eines ganzheitlichen GRC-Managements, der je nach Ausgangssituation des Unternehmens kurz-, mittel- und langfristig erreicht werden kann, zählen folgende Aspekte:

- die Schaffung flexibler und nachhaltiger Strukturen und Abläufe sowie einer angemessenen technologischen Unterstützung im Unternehmen, um die Erfüllung aktueller Stakeholder-Anforderungen effektiv und effizient zu gewährleisten und die Umsetzung von neuen bzw. veränderten Anforderungen durch die gestiegene Flexibilität zu ermöglichen,
- die Reduzierung der unternehmensweiten Kosten im Zusammenhang mit Governance-, Risikomanagement-, Compliance-Initiativen und dem internen Kontrollsystem,
- die Etablierung eines risikobasierten Entscheidungsprozesses,
- die Reduzierung des Non-Compliance-Risikos und damit die Sicherung und langfristige Steigerung des Unternehmenswertes sowie die Vermeidung von Strafen und Reputationsverlusten durch die adäquate Erfüllung relevanter Anforderungen,
- das Generieren zusätzlicher Werte für das Unternehmen und seine Stakeholder durch die Realisierung und Nutzung von Chancen und Synergiepotenzialen, die sich aus den Stakeholder-Anforderungen ergeben,
- die Verankerung ethischer Werte in der Unternehmenskultur (Corporate Culture) und die Schaffung einer Chancen- und Risikokultur im Unternehmen.

<sup>9</sup> Vgl. PwC (2007) S.11.

<sup>10</sup> Vgl. PwC (2005) S.23.

Ein ganzheitliches GRC-Management kann somit als strategisches Werkzeug des Top-Managements zum Erlangen von Wettbewerbsvorteilen und als Differenzierungsmerkmal gegenüber Mitbewerbern genutzt werden.

## 2 Nachhaltigkeit von GRC-Initiativen

Die langfristige Einbettung der Compliance-Initiativen in die bestehenden Organisationsstrukturen, Geschäftsprozesse und Systeme sowie die enge Verknüpfung von Governance, Risikomanagement und Compliance sind Voraussetzung für die Nachhaltigkeit einer GRC-Initiative.

Die nachhaltige Gestaltung der GRC-Initiativen erfordert deren Einbettung in die bereits bestehenden Organisationsstrukturen, Prozesse und Systeme eines Unternehmens. Das Ziel hierbei ist, langfristig die Effektivität und Effizienz der Initiativen unter Berücksichtigung der Unternehmensziele bei einem möglichst optimalen Kosten-/Nutzenverhältnis sicherzustellen und kontinuierlich zu verbessern. Durch die Einbettung werden neben der Steigerung der Effektivität und Effizienz auch eine zunehmende Transparenz und ein gesteigertes Verantwortungsbewusstsein in den relevanten Geschäftsprozessen geschaffen.

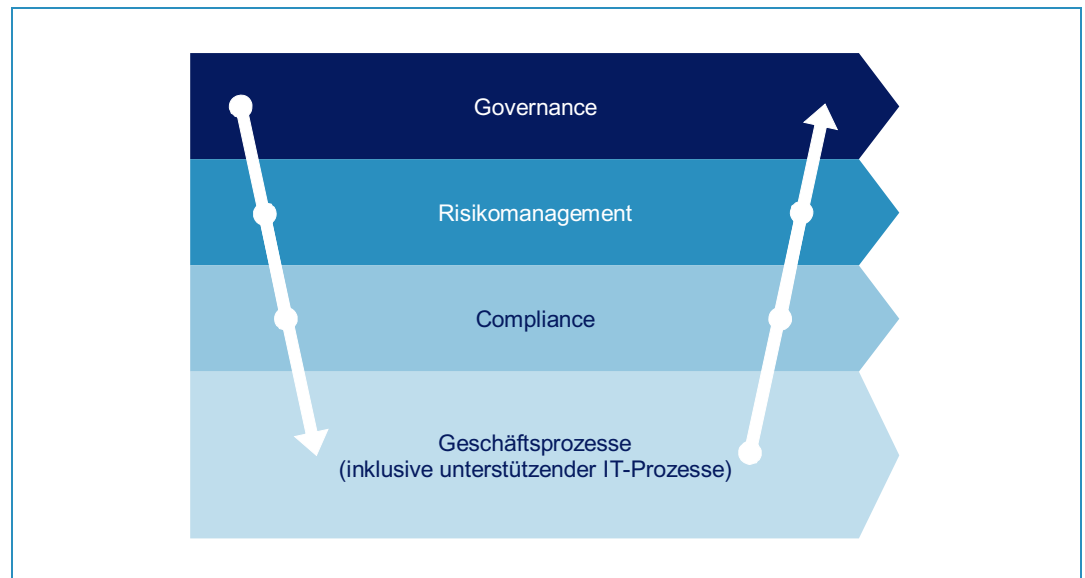


Abb. 3 Integrierte Betrachtung von Governance, Risikomanagement und Compliance

Die Governance des Unternehmens gibt den Ordnungsrahmen, bestehend aus Prozessen und Strukturen, für die Leitung und kontrollierende Steuerung des Unternehmens vor. Sie legt somit auch die aufbau- und ablauforganisatorische Gestaltung der für das Management und dessen Überwachung relevanten Funktionen und Verantwortlichkeiten sowie deren Beziehung zueinander fest. Eine effektive Governance berücksichtigt neben der übergeordneten Unternehmensstrategie und den Zielen auch die Anforderungen der relevanten Stakeholder sowie die individuelle Risikobereitschaft des Unternehmens.

Governance legt somit die Rahmenbedingungen für das unternehmensweite Risikomanagement fest. Das Ziel des Risikomanagements besteht in der Minimierung von Risiken, die eine Umsetzung der festgelegten Unternehmensstrategie und das Erreichen der Unternehmensziele gefährden können. Ein wesentliches Risiko besteht dabei in der Nichterfüllung von Stakeholder- bzw. den daraus abgeleiteten Compliance-Anforderungen (Non-Compliance-Risiko). Der Umgang mit den identifizierten Risiken wird durch die Risikobereitschaft des Unternehmens beeinflusst. Die Risikobereitschaft hinsichtlich der Einhaltung wesentlicher regulatorischer Anforderungen ist beispielsweise eher gering, da die Einhaltung eine Grundlage für den Geschäftsbetrieb darstellt. Die Risikobereitschaft hinsichtlich anderer Risiken wie z. B. bei Markt- und Währungsrisiken kann hingegen höher festgelegt sein. Unternehmen haben in diesem Zusammenhang verschiedene Möglichkeiten mit den identifizierten Risiken umzugehen.

Dazu zählen

- die Risikoakzeptanz,
- die Risikoabwälzung (bspw. durch Versicherungen),
- die Risikoeliminierung und
- die Risikoreduktion.

Zur Risikoeliminierung und zur Risikoreduktion setzen Unternehmen Compliance-Initiativen um. Diese Initiativen stellen auf der Compliance-Ebene sicher, dass sowohl interne und externe Standards, Vorgaben und Regularien als auch freiwillige Verpflichtungen und Vereinbarungen eingehalten werden und das Non-Compliance-Risiko reduziert wird, um letztendlich das Erreichen der Unternehmensziele zu unterstützen.

Governance, Risikomanagement und Compliance stehen in engem Zusammenhang zu den Geschäftsprozessen des Unternehmens. Die jeweiligen Anforderungen müssen in den Prozessen operationalisiert werden und üben folglich einen erheblichen Einfluss auf die Gestaltung und den Ablauf der Geschäftsprozesse aus. Demnach sind eine nachhaltige Einbettung der GRC-Initiativen und eine enge Verknüpfung von Governance, Risikomanagement und Compliance die Basis für die nachhaltige Gestaltung und Umsetzung der Initiativen.

Beispiel: Nachhaltigkeit von GRC-Initiativen

Die SAP AG hat in den vergangenen Jahren eine Reihe von Maßnahmen getroffen, um eine nachhaltige Umsetzung der Anforderungen des Sarbanes-Oxley Act (SOX) im Unternehmen sicherzustellen. Das Ziel bestand darin, das seit mehreren Jahren laufende Projekt zur Erfüllung der Anforderungen des Sarbanes-Oxley Act in einen fortlaufenden, langfristig angelegten Prozess zu überführen. Dabei wurde begonnen, den SOX 404-Prozess in das Enterprise Risk Management von SAP zu integrieren. Um dieses Ziel zu erreichen, werden die Dokumentations- und Bewertungsprozesse des SOX-Projekts in das einheitliche und integrierte Enterprise-Risk-Management-System eingebettet.

Die Sustainability-Elemente geben einen möglichen Rahmen für die Analyse der Nachhaltigkeit von GRC-Initiativen vor.

Die nachhaltige Gestaltung und Umsetzung von GRC-Initiativen lassen sich anhand der **Sustainability-Elemente** analysieren (vgl. Abb. 4). Diese Elemente spiegeln auf der Ebene einer einzelnen Anforderung deren Umsetzung und Einbettung in die Geschäftsprozesse sowie die Verknüpfung von Governance, Risikomanagement und Compliance wider. Die Elemente dienen somit als Rahmen für die Analyse der Nachhaltigkeit von GRC-Initiativen. Das Ergebnis einer Analyse zeigt häufig nicht nur Verbesserungspotenziale im Hinblick auf eine einzelne Initiative, sondern liefert darüber hinaus auch Ansatzpunkte für die methodische oder inhaltliche Zusammenführung verschiedener Initiativen.

Im Folgenden werden zunächst Zielsetzung und Inhalt der in Abb. 4 dargestellten Sustainability-Elemente erläutert. Eine Untersuchung von Möglichkeiten der Zusammenführung erfolgt in Abschnitt 3.

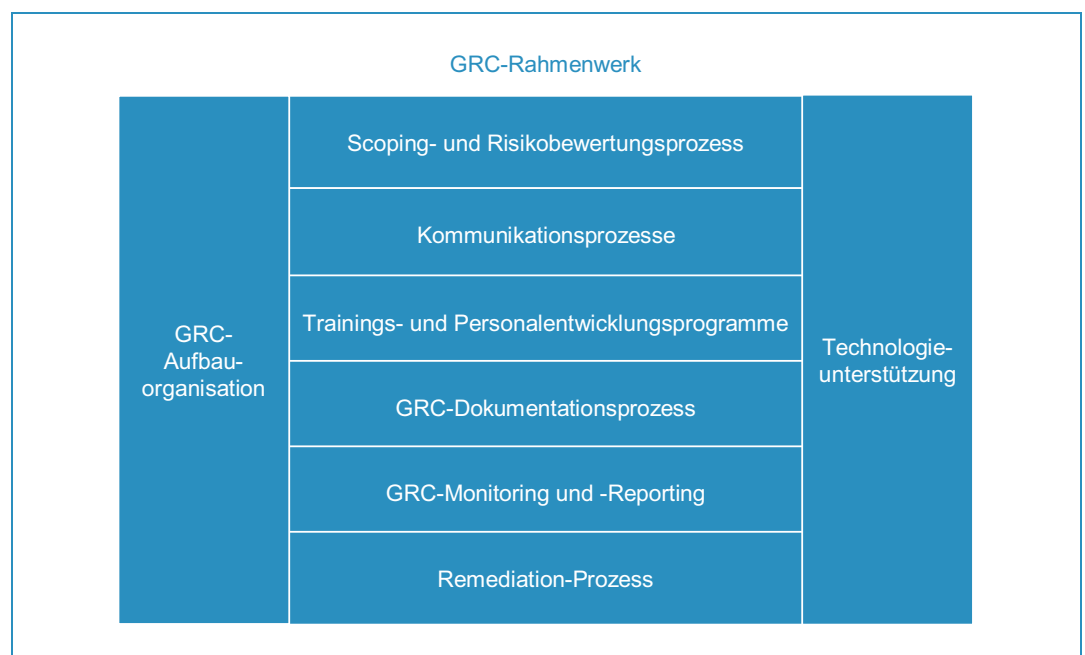


Abb. 4 Sustainability-Elemente

### 1. GRC-Rahmenwerk

Das GRC-Rahmenwerk schafft eine unternehmensweit einheitliche Vorgabe hinsichtlich Inhalt und Umsetzung unterschiedlicher GRC-Initiativen. Das Rahmenwerk ist daher die Basis für eine Definition von detaillierten Richtlinien und Arbeitsanweisungen – beispielsweise zur Dokumentation von Prozessen und internen Kontrollen – und dient der Ableitung von Maßnahmen. Zu den Inhalten eines GRC-Rahmenwerks zählen beispielsweise die GRC-Vision, -Strategie und -Zielsetzung des Unternehmens. Das Rahmenwerk greift typischerweise auch den Inhalt der Stakeholder-Anforderungen (z. B. in Form einer Rule Base<sup>11</sup>) auf und beschreibt zentrale aufbau- und ablauforganisatorische Vorgaben, die sich auf die Einhaltung der Anforderungen beziehen.

### 2. GRC-Aufbauorganisation

Eine nachhaltige GRC-Aufbauorganisation ist durch einen aufbauorganisatorischen Rahmen und eine Verantwortlichkeitsstruktur für die weitergehende Definition von Rollen und Verantwortlichkeiten charakterisiert. Daneben kennzeichnen Aktivitäten zur Einbettung des organisatorischen Rahmens und der Verantwortlichkeitsstrukturen im Unternehmen die GRC-Aufbauorganisation. Im Mittelpunkt des aufbauorganisatorischen Rahmens steht eine Organisationseinheit, welche die GRC-Aktivitäten unternehmensweit steuert und überwacht. Die Verantwortlichkeitsstruktur legt nicht nur Rollen und Verantwortlichkeiten für diese Organisationseinheit auf oberster Ebene, sondern auch für die operative Umsetzung in den einzelnen Unternehmensbereichen und -prozessen fest. Der Rahmen und die definierte Verantwortlichkeitsstruktur können dann beispielsweise durch Trainings- und Personalentwicklungsmaßnahmen, Stellenbeschreibungen oder Zielvereinbarungen kommuniziert und weiter in das Unternehmen integriert werden.

### 3. Scoping- und Risikobewertungsprozess

Der Anwendungsbereich einer GRC-Initiative auf das Unternehmen als Ganzes und auf dessen Organisationseinheiten und Geschäftsprozesse wird in der Regel durch einen strukturierten und institutionalisierten Scoping- und Risikobewertungsprozess festgelegt. Die periodische Überprüfung des Anwendungsbereichs stellt insbesondere sicher, dass interne wie externe Veränderungen (z. B. bei Gesetzesänderungen, Weiterentwicklungen von Standards oder Vertragsänderungen mit Geschäftspartnern) analysiert und entsprechend berücksichtigt werden. Damit trägt dieses Sustainability-Element wesentlich zur Effektivität und Effizienz einer nachhaltigen GRC-Initiative im Regelbetrieb bei. Empfehlenswert ist, dass der Scoping- und Risikobewertungsprozess in die strategischen und operativen Risikomanagementprozesse integriert werden.

### 4. Technologieunterstützung

Die eingesetzte Technologie hat große Auswirkungen auf die Effektivität und Effizienz der gesamten GRC-Initiative und fördert damit die Umsetzung der anderen Sustainability-Elemente. Potenziale einer Technologieunterstützung liegen beispielsweise in einer Automatisierung und einer möglichen Workflow-Unterstützung von GRC-Aktivitäten, einer effektiven Berechtigungsverwaltung oder auch in der Unterstützung von Kommunikations- und Berichtswegen. Eine adäquate Technologieunterstützung sollte in die vorhandene IT-Infrastruktur integrierbar und mit der Unternehmens- und IT-Strategie abgestimmt sein. Die Möglichkeiten der Technologieunterstützung werden in Abschnitt C am Beispiel von SAP-Lösungen nochmals detaillierter betrachtet.

### 5. Kommunikationsprozesse

Strukturierte, standardisierte und ggf. technologieunterstützte Kommunikationsprozesse schaffen zusätzliche Transparenz und erhöhen die Effektivität und Effizienz einer GRC-Initiative. Durch die Integration der GRC-bezogenen Kommunikation in die bisher etablierten Kommunikationsprozesse im Unternehmen können Synergien genutzt werden. Die Gestaltung der Kommunikationsprozesse sollte sicherstellen, dass relevante Informationen auf den Informationsbedarf des Empfängers angepasst sind und zeitnah den richtigen Ansprechpartnern zur Verfügung gestellt werden. Einen wesentlichen Beitrag zur Schaffung angemessener Kommunikationsstrukturen leistet der 'Tone at the

---

<sup>11</sup> Die Definition und Bedeutung der Rule Base werden in Abschnitt D vorgestellt.

Top' als die Art und Weise, wie die Unternehmensführung die angestrebten Unternehmenswerte vorlebt.

#### 6. Trainings- und Personalentwicklungsprogramme

Der Erfolg einer GRC-Initiative hängt in einem großen Maße von der Bereitschaft und den Fachkenntnissen der involvierten Mitarbeiter ab. Die Entwicklung und Durchführung geeigneter Trainings- und Personalentwicklungsprogramme trägt diesem Aspekt Rechnung und berücksichtigt unter anderem die in der GRC-Aufbauorganisation festgelegten Rollen und Verantwortlichkeiten sowie die daraus abgeleiteten Aufgaben. Die Ausbildungsbedarfe der Mitarbeiter sollten optimal berücksichtigt und eine Integration der Qualifizierungsmaßnahmen in die regulären Personalentwicklungs- und Ausbildungsprogramme des Unternehmens sichergestellt werden. Darüber hinaus ist die Evaluierung des Erfolgs von Trainings- und Personalentwicklungsmaßnahmen z. B. durch Tests oder im Rahmen eines Zielvereinbarungsprozesses von großer Bedeutung.

#### 7. GRC-Dokumentationsprozesse

Umfang und Bedeutung von Dokumentationsprozessen besitzen, abhängig von den Anforderungen aus einer GRC-Initiative, einen unterschiedlichen Stellenwert. Das Ziel ist es in erster Linie, die adäquate Abbildung von Richtlinien, Handlungsanweisungen, Geschäftsprozessen und Vorgehensweisen sicherzustellen und nachzuweisen. Die Wiederverwendbarkeit und Konsistenz der Dokumentation sind hierbei wichtige Kriterien. Effektivität und Effizienz der Prozesse werden zusätzlich durch Dokumentationsstandards und -richtlinien, Veränderungsüberwachungs- und Qualitätssicherungsprozesse beeinflusst. Eine geeignete Technologieunterstützung kann dazu beitragen, die Umsetzung der gestellten Anforderungen zu unterstützen.

#### 8. GRC-Monitoring und -Reporting

Die nachhaltige Erfüllung einer GRC-Initiative im Regelbetrieb erfordert, dass geeignete Steuerungs- und Überwachungsinstrumente definiert und in die operativen Prozesse und bestehenden Strukturen integriert werden. Ein adäquates GRC-Monitoring und -Reporting unterstützt so beispielsweise die kontinuierliche Identifikation von Schwachstellen und Abweichungen von Anforderungen, das Erkennen von Zeitverzug und Aufwandsüberschreitungen sowie eine zeitnahe Bestimmung von Risiken, die eine Einhaltung von GRC-Anforderungen gefährden können. Hierzu können u. a. Kennzahlen definiert und überwacht, Informationen mittels Statusreports ausgewertet oder Verfahren und Ergebnisse durch Audits überprüft werden. Ein wesentlicher Bestandteil eines effektiven GRC Monitorings und Reportings besteht in der Definition und Implementierung geeigneter Eskalationsprozesse für kritische Sachverhalte wie z. B. wesentliche Compliance-Verstöße oder Risiken.

#### 9. Remediation-Prozess

Nicht nur im Rahmen des GRC-Monitorings und -Reportings, sondern auch im täglichen Geschäftsbetrieb kann die Nichteinhaltung von Stakeholder-Anforderungen (Non-Compliance) identifiziert werden. Der daraufhin angestoßene Remediation-Prozess dient zur Beseitigung der erkannten Schwachstelle. Er ermöglicht neben der zeitnahen Initiierung von Maßnahmen ein schnelles, konsistentes und nachhaltiges Eingreifen und Steuern. Die Behebung der Schwachstelle wird im Rahmen des Remediation-Prozesses in einer anschließenden Feedbackschleife überwacht.

Die angemessene Gestaltung und Umsetzung der Sustainability-Elemente schafft die Grundlage für eine langfristige und nachhaltige Erfüllung von GRC-Initiativen. Dabei kommt der technologischen Unterstützung der verschiedenen Elemente eine besonders hohe Bedeutung zu. Die Gestaltung und Umsetzung der Elemente stellt jedoch keinen einmaligen Prozess dar. Um den Nutzen zu erhöhen, ist zusätzlich eine kontinuierliche Analyse und Optimierung der Sustainability-Elemente erforderlich.

Neben der nachhaltigen Erfüllung einer einzelnen Initiative ist die Nutzung von Synergien, die sich aus der Integration mehrerer Initiativen ergeben können, ein weiterer wichtiger Bestandteil eines ganzheitlichen GRC-Managements. Im folgenden Abschnitt wird daher auf die Integration mehrerer GRC-Initiativen eingegangen.

*Bei der Erfüllung gesetzlicher Auflagen und der Umsetzung interner Kontrollmechanismen setzen wir auf einen ganzheitlichen Ansatz, um über alle Bereiche und Anwendungen hinweg größtmögliche Transparenz und Sicherheit zu gewährleisten.*

Dr. Werner Brandt, CFO, Mitglied des Vorstands, SAP AG

### 3 Integration von GRC-Initiativen

Unternehmen befassen sich mit einer Vielzahl unterschiedlicher Stakeholder-Anforderungen. Komplexe und strategisch wichtige Anforderungen werden mit Hilfe von GRC-Initiativen im Unternehmen umgesetzt. Auch wenn einzelne Initiativen bereits (z. B. anhand der zuvor beschriebenen Sustainability-Elemente) als nachhaltig bezeichnet werden können, sind die erforderlichen Maßnahmen meist isoliert definiert und unabhängig von bereits bestehenden GRC-Strukturen umgesetzt worden. Die isolierte und fragmentierte Umsetzung verschiedener GRC-Initiativen führt häufig dazu, dass Überschneidungen zwischen den Initiativen nicht ausreichend berücksichtigt werden. Zu den Ausprägungen und Folgen einer isolierten Umsetzung zählen daher beispielsweise:

- die Bildung ineffizienter Parallelstrukturen und einer heterogenen GRC-IT-Landschaft,
- ein damit verbundener erhöhter Kosten- und Ressourcenaufwand und eine zunehmende Unzufriedenheit der Mitarbeiter aufgrund von Mehrfachbelastungen,
- eine fehlende Übersicht des Managements hinsichtlich eines ganzheitlichen GRC-Status des Unternehmens und damit auch
- ein erhöhtes Non-Compliance-Risiko.

Ein ganzheitliches GRC-Management stellt neben der Nachhaltigkeit von GRC-Initiativen auch die Nutzung von Synergieeffekten sicher, die sich aus der Integration verschiedener Initiativen ergeben.

Anhand der genannten Punkte zeigt sich, dass ein isoliertes und fragmentiertes Vorgehen zahlreiche Potenziale ungenutzt lässt. Daher spielt neben der Nachhaltigkeit einzelner Initiativen auch die integrative Sichtweise über verschiedene Initiativen hinweg eine entscheidende Rolle für ein ganzheitliches GRC-Management. Eine derartige Sichtweise bedeutet für Unternehmen, dass – aufbauend auf dem in Abschnitt B.2 beschriebenen Ansatz zum Erreichen der Nachhaltigkeit – GRC-Initiativen auch soweit wie möglich unter Abwägung von Kosten- und Nutzenaspekten zusammengeführt werden sollten. Dadurch können Synergieeffekte genutzt und gleichzeitig flexible Strukturen und Abläufe geschaffen werden, um auch zukünftige Anforderungen mit möglichst geringem Aufwand und Ressourceneinsatz zu erfüllen. Synergieeffekte lassen sich beispielsweise durch die Nutzung eines gemeinsamen IT-Systems oder durch die Durchführung eines einheitlichen Prozesses zur Erfüllung unterschiedlicher Stakeholder-Anforderungen realisieren.

Die zuvor beschriebenen Sustainability-Elemente stellen die Basis für die Identifizierung der Integrationspotenziale dar. Die standardisierte Umsetzung der Elemente in den verschiedenen GRC-Initiativen verschafft Transparenz und ermöglicht einen strukturierten und systematischen Vergleich der verschiedenen Initiativen. Die Vergleichbarkeit stellt eine Basis für die Identifizierung und Umsetzung der Integrationspotenziale dar, die sich aus einer besseren Verknüpfung verschiedener GRC-Initiativen ergeben können.

Die Integration von GRC-Initiativen sollte auf Grund der hohen Komplexität auf unterschiedlichen Ebenen betrachtet werden.

Eine ganzheitliche Integration kann in der Regel allerdings nicht vollumfänglich über alle betrachteten Initiativen hinweg erreicht werden. Diese Einschränkung ist insbesondere auf die inhaltlichen Unterschiede der einzelnen GRC-Initiativen zurückzuführen. Aufgrund der hohen Komplexität bei der Integration verschiedener Initiativen sollten die Integrationspotenziale daher auf unterschiedlichen Ebenen betrachtet und identifiziert werden. Dabei kann einerseits zwischen der **methodischen** und **inhaltlichen** Integration unterschieden werden. Andererseits kann die Integration auf der Ebene der **GRC-Steuerungsprozesse**<sup>12</sup> erfolgen und auf die Ebene der **Geschäftsprozesse** ausgedehnt werden. Im Vergleich zur methodischen und inhaltlichen Integration auf der Ebene der GRC-Steuerungsprozesse wird bei einer Integration auf der Ebene der Geschäftsprozesse eine höhere Integrationstiefe erreicht. (vgl. Abb. 5).

<sup>12</sup> Diese Ebene umfasst alle übergeordneten Prozesse, die parallel bzw. zusätzlich zu den Geschäftsprozessen durchgeführt werden, nicht unmittelbar Bestandteil der Geschäftsprozesse sind und die Einhaltung der GRC-Anforderungen sicherstellen.

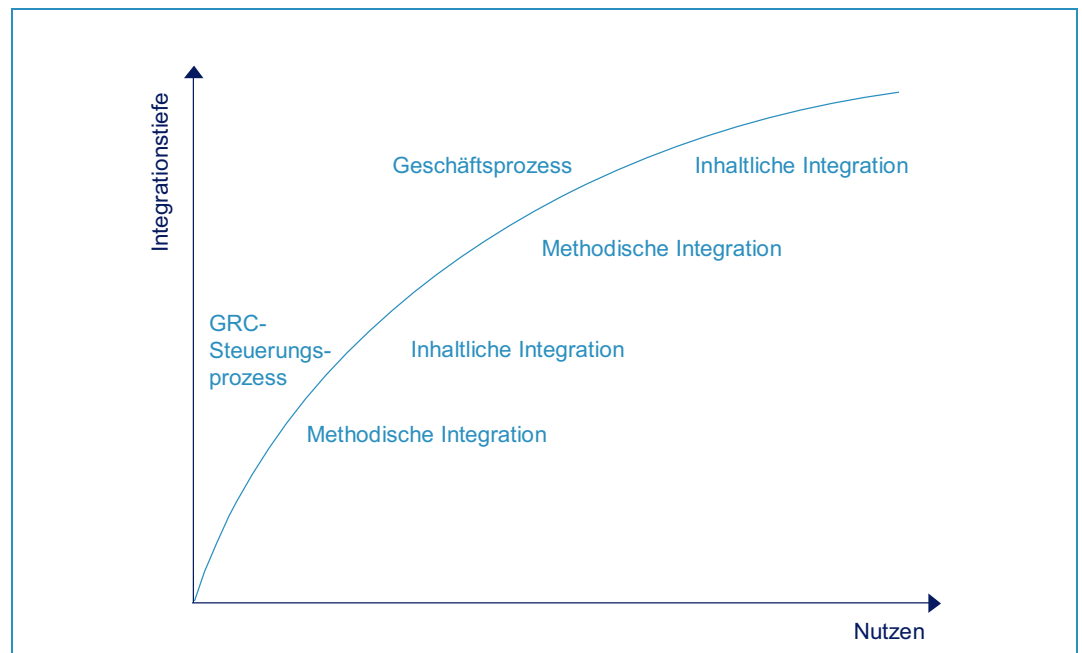


Abb. 5 Ebenen der Integration

Das Ziel der methodischen Integration ist in erster Linie eine Standardisierung der Sustainability-Elemente über die verschiedenen GRC-Initiativen hinweg. Die Nutzung eines integrierten GRC-Tools zur Unterstützung mehrerer Initiativen ist ein Beispiel für eine methodische Integration auf der Ebene der GRC-Steuerungsprozesse. Auch das Vorgehen hinsichtlich der erforderlichen Trainings- und Qualifizierungsmaßnahmen oder die einheitliche Gestaltung von GRC-Rahmenwerken lassen sich möglicherweise in methodischer Hinsicht angleichen bzw. zusammenfassen.

#### Beispiel: Methodische Integration über das Reporting

Bei der Analyse der GRC-Monitoring und -Reporting-Prozesse fällt in vielen Unternehmen auf, dass sich die einzelnen Adressaten – vor allem auf der Ebene des Vorstandes – mit sehr unterschiedlichen Berichtsformaten auseinandersetzen müssen. Dadurch wird es schwierig oder unmöglich, ein ganzheitliches Bild über den Compliance-Status sowie über wesentliche Chancen und Risiken zu erhalten. Diese Berichte sind nicht nur unterschiedlich strukturiert, sondern basieren auch auf uneinheitlichen Begriffsdefinitionen und werden oft in unterschiedlichen Frequenzen erstellt. Hinzu kommen verschiedene, nicht integrierte und häufig auch nicht ausreichend formalisierte Eskalationsprozesse für kritische Sachverhalte. Aufgrund der unterschiedlichen Reportingprozesse besteht außerdem die Unsicherheit, ob bei der Meldung von Risiken oder Compliance-Verstößen ein bestimmter Sachverhalt aus verschiedenen Perspektiven mehrfach denselben Adressaten gemeldet wurde, oder ob es sich bei der Meldung um unterschiedliche und unabhängige Sachverhalte handelt. Vereinfacht ausgedrückt: Existiert ein einzelnes Problem oder sind es zehn Probleme und was bedeutet dies für das Unternehmen als Ganzes? Die Schwierigkeiten, die aus einem nicht integrierten Monitoring und Reporting resultieren, sind offensichtlich. Die Integration der Monitoring- und Reportingprozesse kann als Startpunkt auf dem Weg zu einer stärkeren Integration unterschiedlicher Risikomanagement- und Compliance-Themen dienen. Auf diesem Weg sollten die folgenden Punkte berücksichtigt werden:

- Klare Festlegung des Scopes,
- Erarbeitung von einheitlichen Begriffsdefinitionen,
- Identifizierung der GRC-Monitoring und -Reporting-Adressaten,
- Analyse der Informationsbedürfnisse und -vorlieben hinsichtlich einer effizienten Nutzung von GRC-bezogenen Informationen,
- Festlegung der benötigten Informationen, Definition des Detaillierungsgrads, der Aufbereitung und Darstellung von Informationen sowie die Bestimmung von Reportingfrequenzen,
- Definition des GRC Monitoring- und Reportingprozesses sowie die Definition eines Eskalationsprozesses,
- Implementierung einer geeigneten Technologieunterstützung (z. B. auf Basis von SAP xApp Analytics/SAP NetWeaver BI),
- Konzeption und Implementierung eines Berechtigungsmanagements um sicherzustellen, dass nur berechtigte Personen Zugriff auf vertrauliche GRC-Informationen erhalten.

Die über eine methodische Integration erreichte Standardisierung schafft Transparenz und kann als Basis für eine inhaltliche Integration auf der Ebene der GRC-Steuerungsprozesse genutzt werden. Sie trägt dazu bei, inhaltliche Überschneidungen und damit potenzielle Synergien zwischen den betrachteten Initiativen zu identifizieren. Voraussetzung für das

Erkennen dieser Synergien ist, dass die betrachteten Initiativen tatsächlich inhaltliche Gemeinsamkeiten bzw. Schnittstellen aufweisen. Ein Beispiel für eine inhaltliche Integration auf der GRC-Steuerungsprozess-Ebene ist das einheitliche und gemeinsame Testen von Kontrollen mit Relevanz für verschiedene GRC-Initiativen.

Neben den aufgezeigten Integrationsarten auf der GRC-Steuerungsprozess-Ebene kann des Weiteren eine methodische und inhaltliche Integration auf der Geschäftsprozess-Ebene erfolgen. Ein Beispiel für eine inhaltliche Integration auf dieser Ebene ist das Ersetzen von zwei redundanten Kontrollhandlungen, die auf jeweils zwei unterschiedliche GRC-Initiativen zurückgeführt und unabhängig von einander durchgeführt werden, durch eine gemeinsame Kontrollhandlung, die beide Initiativen gleichzeitig abdeckt.

Beispiel: Integration von GRC-Initiativen am Beispiel des Sarbanes-Oxley und des Foreign Corrupt Practices Act

Das Potenzial einer inhaltlichen Integration von Compliance-Initiativen wird bei einer genauen Betrachtung der Compliance-Anforderungen erkennbar, die auf den **Sarbanes-Oxley Act (SOX)** und den **Foreign Corrupt Practices Act (FCPA)** zurückzuführen sind. Beide Gesetze gelten für Unternehmen, die an einer US-Börse gelistet sind und damit der Aufsicht der SEC unterliegen. Die aus den Gesetzen abgeleiteten Compliance-Initiativen stellen zum Teil vergleichbare Anforderungen an die Steuerung und Überwachung der Geschäftsprozesse. Dennoch werden beide Initiativen in vielen Unternehmen isoliert betrachtet und entsprechend losgelöst voneinander umgesetzt. Im Gegensatz zu einer ganzheitlichen Betrachtung kann dies zu einem erhöhten Non-Compliance-Risiko führen.

Die verschiedenen Anforderungen an die externe Berichterstattung einer SOX- und einer FCPA-Initiative haben dazu geführt, dass viele Unternehmen den beiden Initiativen unterschiedliche Aufmerksamkeit zuwenden. Section 404 des Sarbanes-Oxley Act verpflichtet Unternehmen, die Wirksamkeit des internen Kontrollsystems regelmäßig und explizit zu bestätigen. Der Bericht über die Wirksamkeit interner Kontrollen muss darüber hinaus vom Abschlussprüfer gesondert testiert werden. Im Gegensatz dazu wird ein Bericht über die Einhaltung der FCPA-Anforderungen erst dann öffentlich, sofern eine mögliche Gesetzesverletzung und eine daraus resultierende Non-Compliance vermutet werden. In Folge dessen kann es vorkommen, dass Unternehmen zum Teil unzureichende präventive Kontrollen in Bezug auf die Einhaltung der FCPA-Anforderungen implementiert haben. Daraus resultiert ein erhöhtes Non-Compliance-Risiko für die Unternehmen.

Ein integrativer Ansatz bei der Umsetzung beider GRC-Initiativen trägt dazu bei, die Risiken einer isolierten Betrachtung zu reduzieren. So kann ein Unternehmen einen zusätzlichen Nutzen aus dem in eine SOX - Initiative investierten Aufwand ziehen, indem beispielsweise bereits bei der Umsetzung der SOX-Initiative gewährleistet wird, dass auch ausreichende präventive Maßnahmen zur Einhaltung der FCPA-Compliance implementiert werden.

**Integration sowohl auf der GRC-Steuerungsprozess- als auch auf der Geschäftsprozess-Ebene**

Da die SOX- und FCPA-Anforderungen zum Teil die gleichen operativen Prozesse betreffen, ist es empfehlenswert, die Integrationspotenziale sowohl auf der GRC-Steuerungsprozess-Ebene als auch auf der Geschäftsprozess-Ebene zu betrachten. Ein integrativer Ansatz beginnt bei der Identifikation und der Analyse gemeinsamer Compliance-Risiken, gefolgt von der gemeinsamen bzw. abgestimmten Definition von Maßnahmen zur Reduzierung der identifizierten Risiken. Des Weiteren kann die Nutzung von Standardisierungs- und Synergieeffekten durch die Vereinheitlichung bzw. Nutzung identischer interner Kontrollen in den operativen Prozessen ein Bestandteil des integrativen Ansatzes sein. Folgende Integrationspotenziale lassen sich bei der Betrachtung einer SOX- und FCPA-Initiative auf den beiden unterschiedlichen Prozess-Ebenen erkennen.

**Phase 1: Integration auf der GRC-Steuerungsprozess-Ebene:**

- Definition der GRC-Anforderungen und ihre Auswirkungen auf die Prozesse des Unternehmens,
- Entwicklung eines einheitlichen Risk Assessments und Compliance-Scoping-Ansatzes (z. B. zur Identifizierung relevanter Unternehmenseinheiten, Geschäftsbereiche und Prozesse, die von beiden Compliance-Anforderungen beeinflusst werden),
- Entwicklung eines einheitlichen, risikoorientierten Top-Down-Ansatzes zur Dokumentation, Analyse und Berichterstattung über das interne Kontrollsystem insbesondere im Hinblick auf die Company-Level-Controls und Softer COSO-Komponenten (z. B. Code of Conduct, HR-relevante Prozesse, Tone at the Top), die Prozesskontrollen (z. B. Erweiterung der standardisierten SOX-Risiko- und Kontrollvorlagen, um auch FCPA-relevante Themen mit abzudecken) und die Compliance-Technologieunterstützung (z. B. Nutzung einer gemeinsamen technologischen Plattform wie SAP GRC Process Control).

**Phase 2: Integration auf der Geschäftsprozess-Ebene:**

- Abstimmung und Integration relevanter Richtlinien, Arbeitsanweisungen und operativer Kontrollen in Bezug auf die Finanzberichterstattung und die Einhaltung ethischer Grundwerte,
- Definition von Rollen und Verantwortlichkeiten mit Bezug auf die SOX- und FCPA-Initiativen sowie die Sicherstellung, dass die Rollen und Verantwortlichkeiten angemessen in den Recruiting-Richtlinien reflektiert und in die Leistungsbeurteilung der Mitarbeiter einbezogen werden,
- Einbeziehung von Compliance-Risiken beider Themen in das unternehmensweite Risikomanagement, um eine konsistente Risikobewertung, Risikoüberwachung und Berichterstattung über alle Unternehmenseinheiten und Prozesse hinweg zu gewährleisten,
- Integration der Trainings- und Kommunikationsmaßnahmen mit Bezug auf die SOX- und FCPA-Initiativen,
- Integration von Kontrollaktivitäten, um gleichzeitig sowohl SOX-relevante als auch FCPA-relevante Risiken abzudecken – insbesondere im Hinblick auf den Einkauf (z. B. Bezahlung von Vertriebsvermittlern), den Vertrieb (Festlegung von Preisen und Rabatten, Abschluss von Verträgen) und das Cash Management,
- Optimierung des Einsatzes automatischer Kontrollen und Zugriffsberechtigungen auf IT-Systeme, um eine adäquate Abdeckung der SOX- und FCPA-Risiken zu gewährleisten (z. B. durch Unterstützung mit der Anwendung SAP GRC Access Control).

## C Technologie als entscheidender Erfolgsfaktor am Beispiel von SAP-Lösungen

Wie zuvor beschrieben, adressieren Unternehmen neue oder veränderte Compliance-Anforderungen aufgrund des Zeitdrucks und der Komplexität häufig durch einen Ad-hoc-Ansatz und weitgehend isoliert. Ein solches Vorgehen führt dazu, dass auch im Bereich der Technologie die erforderlichen Maßnahmen nicht in vollem Umfang integriert und nachhaltig gestaltet werden können. Erfahrungsgemäß werden in vielen Unternehmen vielmehr verschiedenste Insellösungen parallel zu existierenden Systemen und Applikationen implementiert. Diese Lösungen führen zu einer zunehmend heterogenen und komplexer werdenden GRC-IT-Landschaft. Aus der wachsenden Komplexität der so entstehenden Strukturen resultiert ein höherer Aufwand zur Steuerung und Überwachung von Compliance.

Eine adäquate Technologieunterstützung trägt zur nachhaltigen Gestaltung von GRC-Initiativen und zur Nutzung von Synergiepotenzialen durch die Integration der Initiativen bei.

Der Einsatz geeigneter Technologien ist daher ein entscheidender Erfolgsfaktor bei der Umsetzung eines ganzheitlichen GRC-Managements. Eine adäquate Technologieunterstützung trägt dabei nicht nur zur nachhaltigen Gestaltung der GRC-Initiativen im Unternehmen bei. Sie ermöglicht auch die Nutzung von Synergiepotenzialen, die sich aus der Integration der verschiedenen Initiativen ergeben. Die eingesetzte GRC-Technologie sollte die nachhaltige Gestaltung der in Abschnitt B.3 dargestellten Sustainability-Elemente unterstützen. Ebenfalls von Vorteil ist, wenn die GRC-Systeme bzw. -Applikationen eng mit den ERP-Systemen verknüpft und weitestgehend integriert arbeiten. Letzteres ermöglicht beispielsweise ein ganzheitliches, unternehmensweites, verlässliches sowie aussagekräftiges GRC-Monitoring und -Reporting.

Im weiteren Verlauf wird am Beispiel der SAP-Lösungen für GRC dargestellt, in welchem Umfang die im Unternehmen existierenden GRC-Aktivitäten durch Technologieeinsatz unterstützt werden können und hierbei mit den ERP- und Fremdsystemen interagieren. Abbildung 6 zeigt, welche Anwendungen innerhalb des SAP-Lösungsportfolios derzeit vorhanden sind bzw. bald verfügbar sein werden. Die einzelnen Funktionalitäten dieser Anwendungen sind darauf ausgerichtet, die Governance-, Risikomanagement-, Compliance- und die Geschäftsprozesse durch einen möglichst hohen Automatisierungsgrad umfassend zu unterstützen. Die Anwendungen unterstützen die jeweiligen GRC-Aktivitäten innerhalb der Prozesse und nutzen die Daten aus dem SAP GRC Repository.

Die Anwendung SAP GRC Risk Management stellt ein globales Rahmenwerk von Risikomanagement-Methoden für Prozesse aller Geschäftsbereiche zur Verfügung. Die Risiken, die durch ein effektives und effizientes internes Kontrollsystem reduziert werden sollen, sind innerhalb der SAP-Lösung für Risikomanagement erfasst, und können auf der ausführenden Kontroll- und Prozessebene in SAP GRC Process Control dokumentiert und überwacht werden.

Die Lösungen SAP GRC Global Trade Services (SAP GRC GTS) und SAP Environment, Health & Safety (SAP EH&S) stellen spezielle Prozesse und Abläufe für die Anforderungen im Außenhandel sowie zum Umwelt-, Gesundheits- und Arbeitsschutz zur Verfügung. Durch den Einsatz dieser Module werden bereits umfangreiche Kontrollen in die jeweiligen Geschäftsprozess eingebettet, um die Einhaltung spezifischer Compliance-Anforderungen sicherzustellen.

Änderungs- und Genehmigungsprozesse im Hinblick auf die Zugriffskontrolle für ERP-Systeme werden von SAP GRC Access Control unterstützt. Die Anwendung enthält Prozesse und Kontrollen, um Funktionstrennungs- und Systemberechtigungsrisiken zu minimieren und diesen vorzubeugen.

SAP GRC Corporate Sustainability Management ermöglicht als weitere Anwendung der GRC-Lösungen ein Reporting über alle Governance-relevanten Aktivitäten. So können beispielsweise ökonomische, ökologische und soziale Kennzahlen definiert, gemessen und ausgewertet werden.

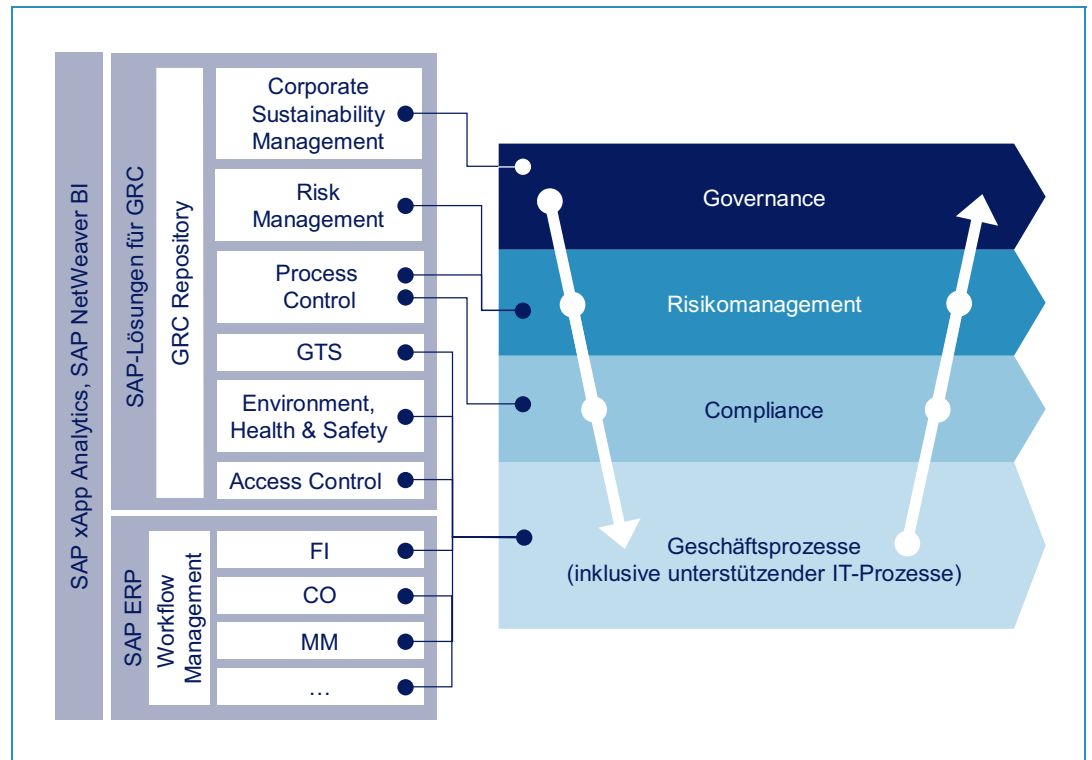


Abb. 6 Technologieeinsatz im Rahmen eines ganzheitlichen GRC-Managements

Alle Anwendungen der SAP-GRC-Lösungen verfügen über integrierte Reporting-Funktionalitäten und eine Business-Intelligence-Schnittstelle (BI-Schnittstelle), um GRC-relevante Informationen konsolidiert und aggregiert verfügbar zu machen.

In den folgenden Abschnitten werden die Einsatzmöglichkeiten und die Funktionalitäten der einzelnen Lösungen untersucht. Diese Untersuchung erfolgt aus der Perspektive der GRC-Steuerungsprozesse und der Geschäftsprozesse (inklusive der unterstützenden IT-Prozesse). Zur besseren Verständlichkeit der technologischen Unterstützungsmöglichkeiten werden im Folgenden die Governance-, Risikomanagement- und Compliance-Prozesse sowie die Geschäfts-, Berechtigungs- und IT-Prozesse nacheinander betrachtet.

#### Ausblick: SAP GRC Technology Foundation

Die SAP GRC Technology Foundation kann in Zukunft als zentrale Integrationsplattform für alle GRC-Applikationen dienen. Sie ist offen für die Anbindung von 3rd-Party-Lösungen, die spezielle GRC-Themen adressieren. Die Foundation besteht aus dem SAP GRC Repository, das eine konsistente Speicherung aller GRC-Daten ermöglicht, sowie aus Tools und Bausteinen für das Design von unternehmensspezifischen GRC-Lösungen. Das GRC Repository wird somit zur „single source of truth“ für alle GRC-Daten. Auf dieser Basis setzt ein integriertes GRC-Monitoring und -Reporting auf. Das Repository ermöglicht ebenfalls die Einbindung von externen Daten wie z. B. Best Practices oder Benchmarking-Informationen, die durch Content Provider angeboten werden. Weitere wesentliche Funktionen der Foundation sind das zentrale Berechtigungsmanagement sowie ein Prozessmodellierungs-Tool zum Erstellen von GRC-Workflows.

## 1 IT-Unterstützung der Governance-Prozesse

Die IT-Unterstützung der Governance-Prozesse zielt vor allem auf die zentrale Datenspeicherung der GRC-relevanten Informationen (single source of truth) sowie die Überwachung und Auswertung dieser Informationen durch ein geeignetes GRC-Monitoring und -Reporting ab. Eine Herausforderung innerhalb der Governance-Prozesse entsteht beispielsweise dadurch, dass relevante Informationen häufig nicht auswertbar sind bzw. nicht erhoben werden, da die Kommunikation der zugrunde liegenden Richtlinien und Arbeitsanweisungen und die Überwachung ihrer Einhaltung in den meisten Fällen nicht nachhaltig geregelt sind. Um dies zu gewährleisten, sollte bei der Gestaltung und

Umsetzung der Governance-Prozesse sichergestellt werden, dass alle Informationen, die Indikatoren für die Einhaltung der Richtlinien und Arbeitsanweisungen liefern, erhoben und gespeichert werden. Dies ermöglicht es dem Unternehmen, GRC-relevante Informationen ganzheitlich zu betrachten und somit ein unternehmensspezifisches Monitoring und Reporting zu gewährleisten.

Zur technischen Umsetzung eines zentralen Datenspeichers verfügt das GRC-Lösungsportfolio von SAP über das GRC Repository. Darüber hinaus ermöglicht das Modul SAP GRC Corporate Sustainability Management die Auswertung der Einhaltung von Richtlinien und Arbeitsanweisungen. Durch den Einsatz von SAP NetWeaver Business Intelligence (SAP NetWeaver BI) und SAP xApp Analytics steht, aufbauend auf den SAP-GRC-Applikationen, eine nachhaltige Unterstützung der GRC-Monitoring und -Reporting-Aktivitäten zur Verfügung.

### SAP GRC Repository

Das SAP GRC Repository wird dazu beitragen, die Transparenz über die GRC-Aktivitäten und -Informationen zu erhöhen und wird so eine angemessene Übersicht bei wachsenden Stakeholder-Anforderungen ermöglichen. Über das Repository werden strategische Zielsetzungen, das Risikomanagement und die Compliance-Aktivitäten aufeinander abgestimmt und ganzheitlich technisch unterstützt. Dies geschieht vor allem durch die Verwendung einer konsistenten Begriffsdefinition (konsistente Semantik) sowie durch die Speicherung von GRC-Daten in einer einheitlichen Datenstruktur. Alle vorhandenen Informationen und Dokumente, wie Richtlinien, Arbeitsanweisungen, Geschäftsprozessabläufe, Risiko- und Kontrollbibliotheken, Testpläne und Nachweise über die Einhaltung von Richtlinien können zentral vorgehalten werden. Das SAP GRC Repository wird hierdurch zukünftig eine integrative Funktion innerhalb der SAP-Lösungen für GRC übernehmen.<sup>13</sup> Diese Funktion wird dazu beitragen, die GRC-Aktivitäten zu überwachen und gezielt Risiken zu analysieren.

### SAP GRC Corporate Sustainability Management

Diese Anwendung dient dazu, die Einhaltung von Richtlinien und Arbeitsanweisungen durch geeignete Kennzahlen messbar zu machen und über das Reporting auszuwerten. SAP GRC Corporate Sustainability Management ermöglicht den direkten Datenzugriff auf die anderen Anwendungen des SAP-GRC-Lösungsportfolios, auf ERP- und andere 3rd-Party-Systeme sowie eine manuelle Erfassung von GRC-relevanten Informationen. Die Erfassung erfolgt über einen Standardprozess, mit dem das Sammeln, Validieren, Konsolidieren und Auswerten relevanter Daten und Informationen ermöglicht wird. Zur Berichterstellung besteht die Möglichkeit, Reporting Units zu definieren und somit individuelle Auswertungen zu ermöglichen. Reporting Units können beispielsweise Länder, Regionen, Organisationseinheiten oder Divisionen sein.

### SAP NetWeaver Business Intelligence (SAP NetWeaver BI) und SAP xApp Analytics

Jede Anwendung der GRC-Lösungen von SAP verfügt über eigene Reporting-Funktionalitäten. Darüber hinaus stellen die Module Schnittstellen zur SAP-NetWeaver-BI-Integration zur Verfügung. Dies ermöglicht den Einsatz dieser SAP-Komponente für das GRC-Monitoring und -Reporting. So können direkt über SAP NetWeaver BI oder in Kombination mit SAP xApp Analytics Management-Dashboards erstellt werden, um GRC-relevante Informationen unternehmensspezifisch auszuwerten und die Aktivitäten entsprechend zu überwachen. Mit dieser Funktion erhalten GRC-Verantwortliche wie beispielsweise der CEO, CFO oder der Compliance Officer zeitnah einen Überblick über den GRC-Status der Bereiche bzw. des gesamten Unternehmens. Die Management-Dashboards können adressatenspezifisch erstellt werden und verfügen über Drill-Down-Funktionalitäten. Ein Drill-Down ermöglicht es, alle relevanten Informationen auf unterschiedlichen Aggregationsstufen anzuzeigen.

Einheitlicher GRC-Status:  
Durch ein integriertes GRC-  
Monitoring und -Reporting  
wird die ganzheitliche  
Überwachung der GRC-  
Aktivitäten ermöglicht.

<sup>13</sup> Das SAP GRC Repository soll im Zuge der GRC Technology Foundation durch eine noch stärkere Integration weiter an Bedeutung gewinnen.

## 2 IT-Unterstützung der Risikomanagement- und Compliance-Prozesse

Risikomanagement- und Compliance-Prozesse tragen unmittelbar dazu bei, die Anforderungen der Stakeholder zu erfüllen und dem Non-Compliance-Risiko frühzeitig entgegenzuwirken. Die Prozesse stehen daher in direktem Zusammenhang mit einem nachhaltigen GRC-Management. Risikomanagement und Compliance sollten eng miteinander verzahnt sein, um relevante Risiken gezielt und frühzeitig zu erkennen, zu überwachen und ihnen mit geeigneten Compliance-Aktivitäten zu begegnen. Die verfügbaren Informationen können so ganzheitlich bei der strategischen und operativen Planung berücksichtigt werden.

Die Nutzung der Potenziale eines ganzheitlichen Ansatzes erfordert in der Regel, dass die Funktion des Risikomanagements eine proaktive Rolle im Unternehmen einnimmt. In vielen Unternehmen erfolgt der Umgang mit Risikomanagement und Compliance jedoch reaktiv. Im Rahmen der Risikomanagement-Prozesse werden Risiken meist nur periodisch erhoben. Bei der Umsetzung eines proaktiven Risikomanagements stehen Unternehmen vor der Herausforderung, Risiken kontinuierlich identifizieren zu können und nach einheitlichen und objektiven Kriterien zu bewerten.

Compliance-Prozesse dienen dazu, den identifizierten Risiken mit geeigneten Maßnahmen zur Risikoeliminierung bzw. zur Risikoreduktion und damit einer Non-Compliance entgegenzuwirken.<sup>14</sup> Die Unterstützung der Compliance-Prozesse durch Technologie wird von vielen Unternehmen sehr unterschiedlich gehandhabt. Auch innerhalb eines Unternehmens sind häufig Unterschiede zwischen den einzelnen GRC-Initiativen zu beobachten. Hinsichtlich des Einsatzes von Technologie im Zusammenhang mit Compliance-Prozessen sind beispielsweise folgende Herausforderungen erkennbar:

- Initiativen-übergreifend sollte ein einheitliches Verständnis von Compliance bestehen sowie einheitliche Begriffe und Vorgehensweisen für gleiche Sachverhalte verwendet werden.
- Bei der Umsetzung einzelner GRC-Initiativen sollte möglichst schon zu Beginn eine technologische Unterstützung der Dokumentation berücksichtigt werden, um den manuellen Arbeitsaufwand gering zu halten.
- Kontrollüberwachungen, Kontrolltests und Management-Selbsteinschätzungen sollten automatisiert eingeplant und ausreichend technologisch unterstützt werden.
- Die Auswertung des Compliance-Status durch ein angemessenes GRC-Monitoring und -Reporting erfordert, dass die relevanten Compliance-Informationen zentral und in elektronischer Form vorliegen.

Ein angemessener Einsatz von Technologie trägt dazu bei, diesen Herausforderungen gerecht zu werden und die Effektivität und Effizienz der Prozesse zu steigern. Eine ganzheitliche technologische Unterstützung der Risiko- und Compliance-Prozesse ermöglicht beispielsweise die Umsetzung eines Risikofrühwarnsystems in Echtzeit. Dieses Frühwarnsystem senkt das Non-Compliance-Risiko und kann als strategisches Werkzeug vielseitig im Unternehmen eingesetzt werden. Darüber hinaus unterstützt Technologie die Integration der Risikomanagement- und Compliance-Prozesse sowie das Setzen und Einhalten von einheitlichen Standards. Dadurch werden eine Messbarkeit der Einhaltung von Standards sowie eine stärkere Automatisierung der Kontrollen und Abläufe, z. B. von Genehmigungsverfahren, ermöglicht.

Zur technologischen und integrierten Unterstützung der Risikomanagement- und Compliance-Prozesse beinhalten die SAP-Lösungen für GRC die Anwendungen GRC Risk Management und GRC Process Control. Diese werden im Zuge der SAP-GRC-Foundation-Entwicklung zunehmend weiter integriert.<sup>15</sup>

---

<sup>14</sup> Vgl. Abschnitt B.1.

<sup>15</sup> Vgl. Ausblick: SAP GRC Technology Foundation, Seite 20.

**Ganzheitliches Risiko-  
management:** Risiken  
werden identifiziert und  
bewertet, um Maßnahmen  
zu deren Vermeidung oder  
Reduzierung abzuleiten.

### SAP GRC Risk Management

Die Applikation für Risikomanagement unterstützt ein Unternehmen bei der Etablierung eines unternehmensweiten und proaktiven Risikomanagements. Hierdurch können dem Risikomanager wichtige Informationen, beispielsweise über spezifische Dashboards und Berichte sowie in Form von personalisierten Scorecards, zeitnah zur Verfügung gestellt werden. Diese Informationen ermöglichen es, dass Risikokennzahlen analysiert und erforderliche Maßnahmen gezielt eingeleitet werden können. Zu den weiteren Funktionalitäten von SAP GRC Risk Management zählen beispielsweise die folgenden Punkte:

- Rahmenkonzept mit Best Practices und ein vordefinierter Risikomanagement-Prozess, der die Risikoplanung, die Risikoidentifizierung, die Risikoanalyse, sowie das Ableiten von Maßnahmen zur Risikokompensation und der Risikoüberwachung beinhaltet,
- Zugriff auf Daten und Informationen aus anderen SAP-GRC-Anwendungen und Fremdsystemen,
- Unterstützung der Analyse von Risiken im Hinblick auf Risikograd und Eintrittswahrscheinlichkeit sowohl aus monetären als auch aus qualitativen Gesichtspunkten,
- Überwachung des gesamten Risiko-Portfolios mittels weltweit einheitlicher Risikoprofile auf operativer und strategischer Unternehmensebene.

Die Verknüpfung zu ERP-Systemen trägt dazu bei, das Risikomanagement in die Geschäftsprozesse einzubetten. Für Kundenaufträge können beispielsweise Risiken mit Schwellenwerten hinterlegt werden. Sobald in SAP CRM ein Kundenauftrag angelegt wird, der diesen Schwellenwert überschreitet, bekommt der Verkaufsmitarbeiter einen Hinweis, dass eine Risikoanalyse notwendig ist. Der Mitarbeiter wird automatisch per E-Mail über das identifizierte Risiko informiert. Er kann weitere Risiken ergänzen und zusätzliche Personen per Workflow über das identifizierte Risiko informieren. Außerdem wird durch die Workflow-Funktionalität ein Risikomanager oder ein Risikoverantwortlicher zur Bewertung und Überwachung des Risikos in den Prozess eingebunden.

### SAP GRC Process Control

GRC Process Control stellt eine Lösung zur technologischen Unterstützung der Compliance-Prozesse dar. Die Unterstützung erstreckt sich von der Dokumentation der Kontrollen für die identifizierten Risiken innerhalb der Geschäftsprozesse über das Bewerten und Testen der Kontrollen bis hin zur Steuerung und Überwachung der Behebung von Kontrollschwächen. Die Anwendung trägt dazu bei, ein ganzheitliches Bild über die Compliance-Initiativen und deren Status zu erhalten.

**Stärkere Automatisierung  
des internen Kontroll-  
systems:** Durch die Nutzung  
von SAP GRC Process  
Control wird eine höhere  
Automatisierung des  
gesamten internen Kontroll-  
systems ermöglicht und die  
Notwendigkeit von kosten-  
intensiven manuellen  
Kontrollen verringert.

Durch die Implementierung von automatisierten Kontrollen in den Geschäftsprozessen<sup>16</sup> kann der Anteil von meist aufwendigeren, manuellen Kontrollaktivitäten reduziert werden. SAP GRC Process Control unterstützt Unternehmen dabei, Kontrollaktivitäten und damit verbundene Workflows stärker zu automatisieren. Zu den Funktionalitäten zählen beispielsweise:

- die Bereitstellung von detaillierten Anleitungen und genehmigten Vorlagen, nach denen Tester manuelle Prüfungsaufgaben ausführen können,
- die Durchführung von Selbsteinschätzungen für Kontrollen oder anderer Compliance-Indikatoren auf verschiedenen Unternehmensebenen und Managementzertifizierungen,
- eine flexible Survey-Funktionalität zur Erstellung von Compliance- und Risikofragebögen,
- die Überwachung von Konfigurationen und Transaktionen in Prozessen wie Beschaffung, Auftragsabwicklung und Rechnungslegung durch automatisierte Kontrolltests zur Verringerung des Überwachungsaufwands für Kontrollen (Monitoring Controls),
- die Weiterleitung der manuellen Kontrolltests an die zuständigen Mitarbeiter als automatische Workflow-Unterstützung,
- die Integration mit SAP GRC Access Control zur automatischen Kontrolle der Einhaltung der Funktionstrennung,

<sup>16</sup> Automatische Kontrollen in Geschäftsprozessen werden in Abschnitt C.3 beschrieben.

- die Durchführung eines elektronischen Sign-off-Prozesses (bottom-up) über alle relevanten Ebenen,
- das Aufzeigen von Verstößen gegen die Kontrollvorschriften und Priorisierung der Korrekturmaßnahmen durch eine globale Heatmap,
- ein integriertes Reporting zur Überwachung des Compliance-Status für die relevanten Compliance-Initiativen (inklusive einer Schnittstelle zur BI-Integration).

Mit Hilfe der Monitoring Controls innerhalb der Anwendung SAP GRC Process Control wird eine stärkere Automatisierung detektiver Kontrollen ermöglicht. Dazu können Konfigurationen und Transaktionen in ERP-Systemen in definierten Frequenzen überwacht werden. Bei Überschreitung von Schwellenwerten können automatisch zuvor definierte Verantwortliche informiert werden. Im Anschluss wird der Workflow bis zur Klärung des Sachverhaltes technisch unterstützt und dokumentiert.

Durch den gezielten Einsatz der SAP-Lösungen für Risikomanagement und Geschäftsprozesskontrollen sowie die Anpassung der Anwendungen an die GRC-Initiativen können Unternehmen beispielsweise folgende Nutzenpotenziale erzielen:

- Durch ein ganzheitliches Risikomanagement können Risiken frühzeitig identifiziert und bewertet werden, um geeignete Maßnahmen zu deren Vermeidung oder Reduzierung abzuleiten.
- Durch eine Erhöhung der Transparenz von Risikomanagement- und Compliance-Prozessen werden die Steigerung der Unternehmensleistung und die Verbesserung von Prognosen ermöglicht, da Risikoprognosen und notwendige Analysewerkzeuge zur Verfügung stehen.
- Eine stärkere Automatisierung sowie die Analyse und Überwachung von Risiken tragen zur Nachhaltigkeit bei und verringern den manuellen Aufwand sowie die Kosten.
- Ein proaktives Vorgehen ermöglicht ein effektives Management operativer Risiken und wirkt sich positiv auf zahlreiche immaterielle Werte wie den Markenwert und die Reputation des Unternehmens aus. Es trägt dazu bei, dass Reputationsverluste rechtzeitig vermieden werden können.
- Die technologische Unterstützung der Risikomanagement- und Compliance-Prozesse ist eine wesentliche Voraussetzung für ein nachhaltiges GRC-Monitoring und -Reporting.
- Durch die Möglichkeit, Kontrollen in ERP-Systemen automatisch zu überwachen, kann in Kombination mit dem Risikomanagement ein Frühwarnsystem aufgebaut werden.
- Durch die Survey-Funktionalität von SAP GRC Process Control können Compliance- und Risiko-Indikatoren durch einen Fragebogen erhoben werden. Die Ergebnisse können als Wirksamkeitsnachweise automatisch weiterverwendet werden und tragen somit zur Darstellung des ganzheitlichen GRC-Status bei.

### 3 IT-Unterstützung von Compliance innerhalb der Geschäftsprozesse

Nahezu alle Geschäftsprozesse in einem Unternehmen werden durch ERP-Systeme wie SAP ERP unterstützt. Bei der Optimierung der ERP-Systeme stehen in der Regel Performance-relevante Aspekte wie beispielsweise die Reduzierung der Prozess-durchlaufzeiten oder der Prozesskosten im Mittelpunkt. Die Möglichkeiten der Systeme zur Unterstützung von Compliance werden allerdings oftmals nicht vollständig ausgeschöpft. So werden zum Beispiel manuelle Kontrollen implementiert, obwohl das ERP-System bereits Möglichkeiten für den Einsatz automatisierter Kontrollen bietet. Die Einsatzmöglichkeiten und Vorteile automatisierter Kontrollen werden in den nachfolgenden Abschnitten untersucht, wobei auch eine grundsätzliche Unterscheidung von präventiven und detektiven Kontrollen von Bedeutung ist.

Detektive Kontrollen dienen dazu, bereits aufgetretene Fehler bzw. Verletzungen von Compliance-Anforderungen zu erkennen. Über entsprechend eingeleitete Maßnahmen sollen die Auswirkungen des Verstoßes korrigiert werden. Hierbei besteht jedoch die Gefahr, dass sich – abhängig vom Zeitpunkt des Erkennens und der Art des Verstoßes – nicht alle Auswirkungen nachträglich vollständig beseitigen lassen.

Präventive Kontrollen helfen hingegen Fehlern oder Verletzungen und deren negativen Auswirkungen vorzubeugen und diese nicht entstehen zu lassen. Der verstärkte Einsatz von präventiven Kontrollen kann somit zu einer Steigerung der Effektivität des Internen Kontrollsystems (IKS) beitragen. Darüber hinaus ergeben sich häufig auch Effizienzvorteile, z. B. durch den Wegfall von aufwendigen Maßnahmen zur Behebung eines erkannten Verstoßes.

Des Weiteren sind Kontrollen durch einen unterschiedlichen Automatisierungsgrad charakterisiert, der von manuell über semi-automatisch bis hin zu voll-automatisch reicht (vgl. Abb. 7). Wie die weiteren Ausführungen zeigen, ist diese Charakterisierung insbesondere im Zusammenhang mit der Effektivität und Effizienz präventiver Kontrollen von großer Bedeutung.

		manuell	semi-automatisch		voll-automatisch
			gering automatisiert	hoch automatisiert	
präventiv	SAP ERP		✓	✓	✓
	SAP-Lösungen für GRC		✓	✓	✓
detektiv	SAP ERP		✓	✓	
	SAP-Lösungen für GRC		✓	✓	

Abb. 7 Klassifizierung interner Kontrollen

Eine Automatisierung von Kontrollen bedeutet, dass deren Ausführung zumindest teilweise technisch unterstützt erfolgt. Semi-automatische Kontrollen können dabei sowohl präventiv als auch detektiv arbeiten, während voll-automatische Kontrollen grundsätzlich präventiv ausgelegt sind.<sup>17</sup> Letztere blockieren den weiteren Ablauf eines Prozesses bis zur erfolgreichen Durchführung der Kontrolle und stellen dadurch Compliance sicher.

Für eine effektive und effiziente Einhaltung von Compliance-Anforderungen besitzen sowohl die Automatisierung als auch die zuvor beschriebene präventive Ausprägung der Kontrollen eine wesentliche Relevanz. Signifikante Effekte – bezogen auf die Nachhaltigkeit und die Effizienz des IKS – können erzielt werden, indem der Grad der technischen Unterstützung von Kontrollen und die Anzahl präventiver Kontrollen erhöht werden. Die Automatisierung von präventiven Kontrollen ist typischerweise mit einer Reihe von Nutzenpotenzialen verbunden:

- Reduzierung des Ressourceneinsatzes für die Kontrolldurchführung,
- Erhöhung der Prozess-Durchlaufzeit durch die Beschleunigung der Kontrolldurchführung,
- Erhöhung der Kontrollwirksamkeit (Kontrolleffektivität),
- Effizientere Verwaltung der Kontrollnachweise (Control Evidence),
- Reduzierung des Testaufwands durch Senkung des geforderten Stichprobenumfangs und
- ggf. automatisiertes Testen der Kontrollen.

<sup>17</sup> Auf die stärkere Automatisierung von detektiven Kontrollen wird in Abschnitt C.2 eingegangen.

Durch eine Automatisierung präventiver Kontrollen lassen sich beispielsweise Genehmigungsprozesse durch einen systemseitig abgebildeten Workflow verbessern. Des Weiteren werden, als Folge der Automatisierung, verschiedene Informationen insbesondere zur Gestaltung und zur Durchführung von Kontrollen in IT-Systemen nachvollziehbar gespeichert. Die gespeicherten Informationen können wiederum das Testen der Kontrollwirksamkeit erleichtern, die Transparenz bzgl. des Status einer Genehmigung erhöhen und den Aufwand für die Kontrollausführung reduzieren. Die Workflow-Nutzung stellt in diesem Beispiel jedoch eine geringe Automatisierung dar, da Berichte zwar automatisch generiert werden können, deren Auswertung und Weiterverarbeitung jedoch weitestgehend manuell abläuft.

Das ERP-System von SAP bietet bereits eine Vielzahl von automatischen Kontrollen an, die bei entsprechender Konfiguration des ERP-Systems zur Einhaltung von Compliance-Anforderungen genutzt werden können. Diese Kontrollen sind in den Geschäftsprozess eingebettet und haben neben einer erhöhten Effizienz als Folge der Automatisierung den weiteren Vorteil, dass sie in der Regel präventiv ausgeführt werden. Diese Kontrollen sollten bestmöglich genutzt werden, um die Effizienz aller GRC-Aktivitäten innerhalb der Geschäftsprozesse zu steigern bzw. den erforderlichen Aufwand zu reduzieren.

Neben den automatischen Kontrollen in SAP ERP werden mit den SAP-Lösungen für GRC weitere Anwendungen für spezifische Geschäftsprozesse zur Verfügung gestellt.<sup>18</sup> Diese unterstützen Unternehmen bei der Einhaltung spezieller Compliance-Anforderungen durch automatische Kontrollen innerhalb der Geschäftsprozesse für Außenhandel sowie Umwelt, Gesundheit und Arbeitsschutz. Im Folgenden werden zwei ausgewählte Module im Detail dargestellt.

#### SAP GRC Global Trade Services (SAP GRC GTS)

Durch die Globalisierung und den damit verbundenen grenzüberschreitenden Warenverkehr haben sich die Komplexität der Geschäftsvorfälle und die damit verbundenen Risiken erheblich erhöht. Hierzu tragen insbesondere die zahlreichen und vielfältigen Außenhandelsabkommen, -gesetze und -vorschriften als auch die stärkere Interaktion mit verschiedenen Zollbehörden bei. Unternehmen müssen auf die entsprechenden Anforderungen und deren Veränderung zeitnah und flexibel reagieren, um den nachhaltigen Geschäftserfolg und die Einhaltung der länderspezifischen Handelsbeschränkungen sicherzustellen. Damit können die erhöhten Risiken bezüglich eines Gesetzesverstößes und eines Zahlungsausfalls minimiert werden. SAP GRC GTS unterstützt Unternehmen dabei, diese Herausforderungen im Bereich des Außenhandels nachhaltig durch eine integrierte Lösung zu bewältigen.

Folgende Nutzenpotenziale können durch den Einsatz von SAP GRC GTS erschlossen werden:

- Standardisierung, Automatisierung und Optimierung von Außenhandelsprozessen und Sicherstellung der Compliance durch Integration der präventiven Kontrollen in die Prozesse, u. a. durch Einhaltung von internationalen Handelsbeschränkungen durch eine automatische Embargo- und Boykottlistenprüfung,
- Erleichterung der Interaktion mit den zuständigen Zollbehörden durch Unterstützung bei der Tarif- und Zollwertermittlung, der Erstellung von Außenhandelsdokumenten sowie bei der Kommunikation mit den jeweiligen Zollbehörden (z. B. NCTS, ATLAS), welche in Zukunft zwingender Bestandteil des Außenhandelsverkehrs sein wird,
- Beschleunigung des Kundenabrechnungsprozesses durch grenzüberschreitende, effiziente Waren- und Informationsbewegungen und damit Verbesserung der Forderungsalterstruktur,
- Automatisierung und Beschleunigung von Rückerstattungen durch effiziente Unterstützung bei Export-Rückzahlungen sowie Präferenzabwicklung und -kalkulation.

<sup>18</sup> Diese gehörten bisher zur SAP Business Suite.

### SAP Environment, Health and Safety (SAP EH&S)

Besonders international operierende Unternehmen müssen unterschiedlichste Anforderungen in den Bereichen Umwelt- und Arbeitsschutz berücksichtigen und einer Verletzung entsprechender (Sicherheits-)bestimmungen vorbeugen. Auch die Anforderungen in den Gebieten Umwelt, Gesundheit und Sicherheit unterliegen einer stetigen Veränderung, was zu einer zusätzlichen Herausforderung führt.

Als integraler Bestandteil der SAP Business Suite und wichtige Anwendung der GRC-Lösungen unterstützt SAP EH&S daher die Sicherstellung von Compliance, indem gesetzlichen Anforderungen effizient in die Geschäftsprozesse integriert werden. Hierbei werden die Anforderungen hinsichtlich der Restriction of Hazardous Substances (ROHS) und der Waste Electrical and Electronic Equipment (WEEE) Directive genauso berücksichtigt wie die des Health and Safety at Work Acts. So kann in SAP EH&S beispielsweise festgelegt werden, dass gefährliche Substanzen nur auf speziell hierfür vorgesehenen Lagerplätzen zu lagern sind. Bei Zuwiderhandlung kann eine Einlagerung oder eine Bestellung direkt im Beschaffungsprozess blockiert werden. Das SAP EH&S unterstützt des Weiteren das Gefahrstoff-, Gefahrgut- und Abfallmanagement sowie den Arbeitsschutz und die Arbeitsmedizin und ein effizientes Umwelt und Sicherheitsmanagement.

Folgende Nutzenpotenziale lassen sich durch den Einsatz von SAP EH&S herausstellen:

- Produktsicherheit von Gefahrgütern über eine zentrale Verwaltung aller Produktdaten und Bereitstellung der Informationen genau an der benötigten Stelle in den Prozessen,
- Flexibles und schnelles Reagieren auf veränderte Regularien und Vorschriften in den Gebieten der Produkt- und Arbeitssicherheit,
- Optimierung durch Standardisierung von Prozessabläufen, Dokumentationen und der Kommunikation durch Integration der Prozesse des Gefahrstoff-, Claim- und Unfallmanagements in die Beschaffungs-, Lagerungs-, Arbeitsschutz- und Sicherheitsprozesse,
- Verbesserung von Entscheidungsprozessen, indem die benötigten Informationen durch Aggregation und Auswertung von Daten zeitnah und qualitativ hochwertig bereitgestellt werden können.

Der Einsatz von präventiven und möglichst automatisierten Kontrollen trägt zur nachhaltigen Unterstützung von Compliance bei. Dies wird beispielsweise durch die angemessene Nutzung der SAP-ERP-Module, SAP GRC GTS und SAP EH&S ermöglicht. Detektive und vorwiegend manuelle Kontrollen können durch die verfügbaren SAP-Lösungen für GRC stärker automatisiert werden. Hierbei sind die Monitoring Controls der SAP-GRC-Process-Control-Anwendung von wesentlicher Bedeutung.

## 4 IT-Unterstützung von Compliance innerhalb der Berechtigungs- und IT-Prozesse

Die zunehmend komplexer werdenden IT- und Berechtigungsstrukturen erschweren es den Unternehmen, einen angemessenen Überblick zu bewahren. Fehlende Auswertungsmöglichkeiten über existierende Berechtigungsstrukturen verstärken dieses Problem. Darüber hinaus führt die wachsende Komplexität dazu, dass sich der Aufwand zur Sicherstellung der Compliance-Anforderungen erhöht. Unternehmen stehen beispielsweise vor der Herausforderung, standardisierte Kommunikationsprozesse zwischen den Fachabteilungen und der IT-Abteilung sicherzustellen, um ein effektives Management der Zugriffsberechtigungen zu gewährleisten. Zur Bewältigung dieser Herausforderung tragen automatisierte Abläufe und Prävention bei. Eine entsprechende Umsetzung erweist sich in der Praxis jedoch häufig als schwierig.

Ein wichtiger Bestandteil eines effektiven und nachhaltigen internen Kontrollsystems ist die Umsetzung und Überwachung der Funktionstrennungen (Segregation of Duties, SoD) und die eingeschränkte Verwendung von sensiblen und daher kritischen Einzelberechtigungen für alle operativen und administrativen Bereiche. Diese Berechtigungen müssen überwacht und restriktiv vergeben werden. Darüber hinaus sollte eine nachhaltige Umsetzung der Funktionstrennung durch die Einbettung in die Prozesse und Kontrollumgebung sichergestellt werden. Zudem sollten zukünftige Änderungen im

organisatorischen Aufbau, beispielsweise resultierend aus Veränderungen im Markt-  
umfeld, ständig berücksichtigt und aktualisiert werden können.

In diesem Zusammenhang stehen Unternehmen vor folgenden Herausforderungen:

- Identifizierung der relevanten Funktionstrennungsrisiken und Erstellung eines einheitlichen Regelwerkes zur Funktionentrennung,
- Analyse der Risiken in den Systemen und Auswertung der Ergebnisse,
- Bewältigung der Konflikte und Verstöße in den Fachbereichen und Erarbeitung von Lösungen,
- Sicherstellung der nachhaltigen Überwachung dieser Risiken und ständige Erweiterung sowie Verbesserungen des Regelwerkes resultierend aus einem dynamischen Umfeld und
- Einbettung der Funktionstrennung in den Regelbetrieb und in die Kontrollstrukturen.

Unternehmensweite Zugriffs- und Berechtigungskontrolle: Die SAP-Software unterstützt die Prüfung, Kontrolle und Organisation des unternehmensweiten Rollen- und Berechtigungswesens und beugt somit Funktionstrennungsrisiken vor. Unberechtigte Zugriffe und Missbrauch von Berechtigungen werden verhindert.

Zur Bewältigung dieser Herausforderungen kann der Einsatz von SAP GRC Access Control beitragen. Diese Anwendung unterstützt die Geschäftsprozessverantwortlichen, Dateneigner und IT-Manager während des gesamten Ablaufs in den jeweiligen Aufgabebereichen. SAP GRC Access Control besteht aus den folgenden vier Anwendungen:

#### Virsa Compliance Calibrator

Der Compliance Calibrator unterstützt die Identifizierung, Überwachung und Reduzierung von Funktionstrennungsrisiken sowie kritischer Einzelberechtigungen. Das integrierte Funktionstrennungsregelwerk ist die Grundlage für die automatisierte Risikoanalyse im System und ermöglicht eine kontinuierliche Überwachung der Risiken. Auf Basis dieses Regelwerkes (SoD-Risiko-Matrix) können buchhaltungs-, finanz- und berichterstattungsrelevante Systeme automatisch untersucht und überprüft werden. Konflikte können dadurch zeitnah entdeckt und über klar definierte Verantwortlichkeiten und Prozesse proaktiv gelöst werden. Über eine Risikoklassifizierung werden auftretende Konflikte beurteilt und priorisiert. Ausnahmefälle führen zu einer sofortigen Benachrichtigung der zuvor definierten Verantwortlichen.

#### Virsa Access Enforcer

Das Berechtigungsvergabemanagement wird über den Access Enforcer automatisiert. Durch Einbettung des Access Enforcers in die IT-Management-Prozesse sowie die integrierte SoD-Risikoanalyse wird die präventive Steuerung über die gesamten Berechtigungen und deren Veränderung in den operativen Systemen maximiert.

#### Virsa Role Expert

Der Role Expert unterstützt ein effizientes und präventives Rollenmanagement durch integrierte SoD-Risikoanalysen sowie die Bereitstellung einer standardisierten und zentralen Rollendefinition und -verwaltung. Rollenkonflikte werden vor einer Zuweisung in den Systemen blockiert und müssen bearbeitet werden. Dies wird prüfungssicher dokumentiert und verwaltet.

#### Virsa FireFighter for SAP

Über diese Anwendung können Systemzugänge von sogenannten Super-Usern mit umfangreichen Berechtigungen (z. B. für Notfälle oder für Support-Situationen) gesteuert und überwacht werden. Die prüfungssichere Protokollierung trägt zur Nachvollziehbarkeit und Transparenz aller durchgeführten Aktivitäten bei.

SAP GRC Access Control ermöglicht den Aufbau einer geschlossenen und lückenlosen Überwachung im Bereich des Berechtigungsmanagements. Die Risiken sind eindeutig Geschäftsprozessen zugeordnet. Dies definiert klare Verantwortlichkeiten, integriert die SAP GRC Access Control bestmöglich in die Organisation und stellt eine nachhaltige Umsetzung sicher. Der Einsatz von SAP GRC Access Control trägt dazu bei, Richtlinien, die durch das Compliance-Rahmenwerk definiert sind und sich auf den Bereich des Berechtigungsmanagements beziehen, effektiv und effizient im Unternehmen zu operationalisieren.

Folgende Nutzenpotenziale können erschlossen werden:

- Signifikante Reduzierung von Aufwand und Kosten bei der Erfüllung regulatorischer Anforderungen im Hinblick auf die Funktionstrennung bei gesteigerter Qualität zur Sicherstellung und Einhaltung der Anforderungen,
- Optimierung des internen Kontrollsystems durch Automatisierung, Prävention und Identifizierung von organisatorischen Prozessschwachstellen,
- Erhöhte Standardisierung durch ein zentral definiertes Regelwerk und die Einbettung von SAP GRC Access Control in bestehende Kontrollprozesse,
- Erhöhte Transparenz über die IT- und Berechtigungsstrukturen sowie den Status der Compliance-Aktivitäten aus Sicht der Geschäftsprozessverantwortlichen,
- Höhere Effektivität bei der Zusammenarbeit zwischen Fach- und IT-Abteilung über eine einheitliche und übersichtliche Plattform, abgestimmt auf die individuellen Bedürfnisse der jeweiligen Benutzergruppe,
- Gestiegene Prozesssicherheit und Absicherung gegen dolose und wirtschaftskriminelle Handlungen über die Systeme durch Minimierung der Betrugsrisiken,
- Nachhaltige Unterstützung der Internen Revision sowie des Jahresabschlussprozesses.

#### Beispiel: Erfahrungen aus Implementierungsprojekten von SAP GRC Access Control

PricewaterhouseCoopers (PwC) unterstützte einen führenden Hersteller von Hochleistungskeramikprodukten mit weltweit insgesamt 13 Werken bei der Einführung der SAP-GRC-Access-Control-Anwendungen Virsa Compliance Calibrator und Virsa FireFighter for SAP. Der Kunde unterliegt den regulatorischen Anforderungen des Sarbanes-Oxley Act. PwC hatte den Auftrag, im Bereich der Funktionstrennungen (SoD) sowie im Bereich sensibler und kritischer Systemzugriffe (SAT) bei der Einführung von SAP GRC Access Control zu unterstützen und das Kontrollsystem in diesem Bereich zu optimieren. Primäres Projektziel war es, die SoD-Risikoüberwachung sicherzustellen sowie effektive Kontrollen und effiziente Abläufe einzuführen. Dabei sollte eine größtmögliche Automatisierung der Kontrollen und die Sicherstellung der Nachhaltigkeit gewährleistet werden.

Nachfolgende Projekterfolge konnten abschließend erzielt werden:

- SoD-Risiken konnten mit der Einführung von SAP GRC Access Control automatisiert überwacht werden. Dies bedeutet eine zunehmende Sicherheit in den Prozessen.
- Über die Diskussion mehrerer Funktionstrennungskonflikte im Zahlungsprozess des Unternehmens wurde eine organisatorische Schwachstelle identifiziert. Statt der Einführung einer komplexen und aufwendigen, wiederkehrenden Kontrolle erfolgte eine organisatorische Umstrukturierung des Geschäftsbereichs. Die Umstrukturierung reduzierte nicht nur die aufgedeckten Funktionstrennungsrisiken, sondern erhöhte zudem auch die Prozessqualität durch klar definierte Aufgaben und Verantwortlichkeiten und reduzierte den ursprünglich notwendigen Ressourceneinsatz.
- Der Kontrollaufwand zur Bearbeitung der SoD-Konflikte aus den regelmäßigen Risikoanalysen konnte durch nachhaltige und präventive Maßnahmen erheblich reduziert werden.
- Im Bereich der SAT und Notfallbenutzerzugriffe konnten durch den Einsatz des Virsa FireFighters for SAP mehrere notwendige, zumeist manuelle Kontrollen, eingespart werden. Der Kontrollaufwand konnte in diesem Zusammenhang nach Einschätzung des Unternehmens um ein Fünffaches reduziert werden.
- Die durch den Sarbanes-Oxley Act notwendigen Tests des Abschlussprüfers in diesem Bereich wurden auf Basis der SAP-GRC-Access-Control-Ergebnisse durchgeführt. Dies bedeutete eine Reduzierung des Aufwands bei einer gesteigerten Qualität und Sicherheit.

#### Ausblick: SAP-Lösungen für GRC

Die Planung der SAP sieht vor, dass im vierten Quartal 2007 eine Anwendung zum „Governance & Policy Development Management“, SAP Analytics Dashboards und eine SEM-Integration für die strategische Planung zur Verfügung stehen werden. Darüber hinaus werden die SAP-Lösungen für GRC in Zukunft weiter ausgebaut und um neue Funktionalitäten erweitert.

Als Teil der SAP GRC Technology Foundation können die einzelnen Anwendungen zukünftig als „Out-of-the-Box“-Lösungen angeboten werden. Darüber hinaus ist auf Basis dieser Anwendungen geplant, branchenspezifische Lösungen anzubieten. Das Ziel besteht somit darin, die SAP-Lösungen für GRC zu einer integrierten Lösung zu entwickeln, die eine technische Unterstützung bei der Umsetzung zahlreicher GRC-Anforderungen im Unternehmen sicherstellt.

## D Umsetzung eines ganzheitlichen GRC-Managements

Wie in Abschnitt B beschrieben, besteht das Ziel eines nachhaltigen GRC-Managements einerseits darin, die Nachhaltigkeit einzelner GRC-Initiativen sicherzustellen. Darüber hinaus sollen Synergieeffekte, die sich aus der methodischen und inhaltlichen Integration der verschiedenen GRC-Initiativen ergeben, genutzt werden. Der Weg von einer losgelösten und fragmentierten Umsetzung von GRC-Initiativen hin zu einem nachhaltigen GRC-Management lässt sich anhand eines Transformationsprozesses beschreiben. Für ein Unternehmen stellt sich in diesem Zusammenhang die Frage, wie ein nachhaltiges GRC-Management konkret umgesetzt werden kann.

Die GRC-Strategie bildet das Fundament einer nachhaltigen, risiko- und wertorientierten, ethischen und regelkonformen Unternehmensführung.

Voraussetzung für eine erfolgreiche Umsetzung eines nachhaltigen GRC-Managements ist die Definition einer angemessenen unternehmensweiten **GRC-Strategie**. Die GRC-Strategie schafft die Grundlage zur Erfüllung der Stakeholder-Anforderungen im Unternehmen und damit auch für das Erreichen der Unternehmensziele. Sowohl die Unternehmensvision und die Unternehmensziele als auch die Unternehmenswerte und die wesentlichen Stakeholder-Anforderungen sind wichtige Faktoren, die eine unternehmensweite GRC-Strategie beeinflussen. Weitere Faktoren, die bei der Festlegung einer geeigneten Strategie berücksichtigt werden sollten, sind:

- die Unternehmensgröße und -struktur,
- die Rechtsform des Unternehmens,
- die Internationalität des Unternehmens,
- der Ort der Börsennotierung,
- die Zugehörigkeit zu bestimmten Branchen und Industrien,
- die Komplexität der Compliance-Anforderungen,
- die Risikobereitschaft des Unternehmens,
- die Positionierung innerhalb des Marktes (besondere Anforderungen werden an Marktführer oder Unternehmen mit besonderer Marktposition gestellt) und auch
- die Notwendigkeit der Einhaltung von Compliance-Anforderungen der Vertriebspartner (z. B. Einhaltung von Anti-Korruptionsgesetzen) und Lieferanten (z. B. Einhaltung von Umwelt-, Arbeits- oder sozialen Standards).

Die GRC-Strategie bildet das Fundament einer nachhaltigen, risiko- und wertorientierten, ethischen und regelkonformen Unternehmensführung unter Beachtung der langfristigen Unternehmensziele und der wesentlichen Stakeholder-Anforderungen. Sie bestimmt somit den Fokus und Umfang der Risikomanagement- und Compliance-Aktivitäten. Eine Veränderung in der GRC-Strategie führt in der Regel auch zur Veränderung bzw. Neugestaltung der relevanten Prozesse, Organisationsstrukturen sowie der Technologieunterstützung.

Die Rule Base kann als Instrument zur Bestimmung der unternehmensweiten GRC-Strategie eingesetzt werden. Ihr Einsatz trägt zur transparenten Darstellung der relevanten Stakeholder-Anforderungen bei.

Für eine ganzheitliche Betrachtung von Governance, Risikomanagement und Compliance und damit auch für die Festlegung einer GRC-Strategie ist eine zielgerichtete Berücksichtigung aller relevanten Stakeholder-Anforderungen notwendig. Durch eine Analyse sollten diese Anforderungen nicht nur identifiziert, sondern auch hinsichtlich ihrer Bedeutung für das Unternehmen und die Unternehmensziele bewertet und priorisiert werden. Bei der Analyse und Bewertung als zentrale Sammlung der verschiedenen Anforderungen besitzt die sogenannte **Rule Base** eine besondere Bedeutung.<sup>19</sup>

Die Rule Base ist ein Instrument zur Aufnahme, Analyse und Überwachung aller externen und internen Vorschriften, Standards und Vereinbarungen, die aufgrund von Wesentlichkeits- und Risikogesichtspunkten für ein Unternehmen als relevant erachtet werden. Aufbau und Umfang einer Rule Base können von einer einfachen Auflistung der Anforderungen (z. B. als Tabelle) bis hin zu einer komplexen Datenbank bzw. eines Repositories reichen. Letzteres ermöglicht es, detaillierte Informationen zu den identifizierten Anforderungen darzustellen und beispielsweise deren Auswirkungen auf das Unternehmen und die Prozesse auszuwerten. Der Einsatz einer Rule Base trägt somit zu einer effektiven und transparenten Unternehmenssteuerung unter Berücksichtigung von Governance-, Risikomanagement- und Compliance-Aspekten bei. Dabei reflektieren die

<sup>19</sup> Vgl. Menzies (2006) S. 351 ff. zu den Ausführungen zur Rule Base.

Inhalte der Rule Base sowohl die Unternehmensstrategie und -ziele als auch die Risikobereitschaft des Unternehmens.

Auf Basis der definierten GRC-Strategie und der identifizierten und analysierten, relevanten Stakeholder-Anforderungen kann ein unternehmensspezifisches, nachhaltiges GRC-Management mit Hilfe des im Folgenden beschriebenen Transformationsprozesses im Unternehmen umgesetzt werden. Im Rahmen des Transformationsprozesses werden das existierende GRC-Umfeld analysiert und Maßnahmen zur Sicherung der Nachhaltigkeit der GRC-Initiativen sowie zur Nutzung von Integrationspotenzialen abgeleitet und umgesetzt. Der Transformationsprozess unterteilt sich, wie in folgender Abbildung dargestellt, in insgesamt sechs Schritte.

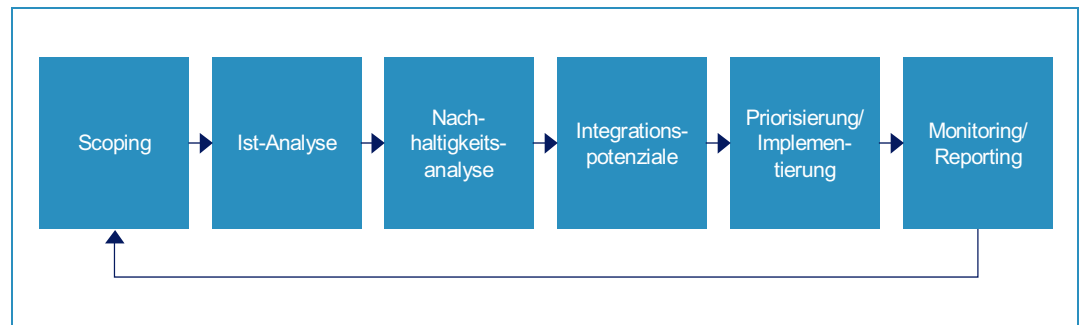


Abb. 8 Transformationsprozess für ein nachhaltiges GRC-Management

### Scoping

Zu Beginn des Transformationsprozesses sollte ein Scoping durchgeführt werden. Dabei wird bestimmt, in welchen Bereichen die größten Handlungsbedarfe liegen, um die GRC-Strategie umzusetzen und ein ganzheitliches GRC-Management im Unternehmen zu ermöglichen. Im weiteren Verlauf des Transformationsprozesses kann das Scoping auf Basis der gewonnenen Informationen zunehmend detailliert, überprüft und ggf. angepasst werden.

Das Ergebnis des Scopings stellen GRC-bezogene Themen bzw. daraus abgeleitete GRC-Initiativen als Ausgangspunkt für ein zukünftiges Optimierungsprojekt dar. Über die Umsetzung des Optimierungsprojekts sollen einerseits die Nachhaltigkeit der relevanten Initiativen gesichert und andererseits die Synergieeffekte, die sich aus der Integration verschiedener GRC-Initiativen ergeben, genutzt werden. Die Auswahl der für ein Optimierungsprojekt relevanten GRC-Initiativen erfolgt in der Regel auf Basis unterschiedlicher Kriterien. Dazu zählen beispielsweise:

- Einschätzung des Non-Compliance-Risikos,
- Höhe der laufenden Compliance-Kosten (Cost of Compliance Operations),
- Bewertung der Wichtigkeit von GRC-Initiativen durch das Management, z. B. im Hinblick auf das Erreichen der Unternehmensziele,
- zeitliche Restriktionen, Interdependenzen mit anderen Projekten, die Verfügbarkeit von Ressourcen oder
- mögliche Einschränkungen, inwiefern Organisationsstrukturen, Prozesse und Technologien innerhalb des Unternehmens grundsätzlich verändert werden können.

### Ist-Analyse

Nachdem der Scope der zu betrachtenden GRC-Initiativen definiert wurde, schließt sich als nächster Schritt eine detaillierte Aufnahme des relevanten unternehmensspezifischen GRC-Umfelds an. Das Ziel der Ist-Analyse besteht darin, eine grundsätzliche Einschätzung bezüglich der bereits im Unternehmen vorhandenen und GRC-relevanten Organisationsstrukturen, Prozesse und Technologien zu erlangen. Das Vorgehen bei der Analyse sollte daher zwar am festgelegten Scope ausgerichtet, jedoch nicht ausschließlich auf die darin enthaltenen GRC-Initiativen beschränkt sein. Die Ergebnisse der Ist-Analyse liefern, zusammen mit den Resultaten der Nachhaltigkeitsanalyse für einzelne GRC-Initiativen, die Basis für die Priorisierung und Umsetzung der erforderlichen Maßnahmen.

Aufgrund der unterschiedlichen Ausgangssituationen, in denen sich ein Unternehmen prinzipiell befinden kann, ist es von großer Bedeutung im Rahmen dieser Phase:

- die Unternehmensstrategie und -ziele,
- die bestehenden Governance- und Risikomanagement-Strukturen und -Abläufe,
- die existierenden Compliance-Strukturen und -Initiativen sowie
- die Aufbauorganisation, die relevanten Prozesse und die eingesetzte Technologieunterstützung der im Scope befindlichen Themen zu analysieren.

#### Nachhaltigkeitsanalyse

Im Anschluss an die Ist-Analyse erfolgt die Nachhaltigkeitsanalyse der einzelnen GRC-Initiativen im Scope. Sie dient vor allem der Beurteilung, wie nachhaltig die betrachteten GRC-Initiativen im Unternehmen umgesetzt werden. Die Nachhaltigkeitsanalyse sollte daher Antwort darauf geben,

- ob und vor allem wie die Elemente Governance, Risikomanagement und Compliance angemessen verknüpft sind,
- in welchem Maße die GRC-Aktivitäten der verschiedenen Initiativen effektiv und effizient in den operativen Geschäftsbetrieb eingebettet sind und
- wie flexibel das Unternehmen auf Änderungen des GRC-Umfelds reagieren kann (Change Readiness und Change Ability).

Die Nachhaltigkeitsanalyse sollte sich an den in Abschnitt B vorgestellten Sustainability-Elementen orientieren. Dadurch wird sichergestellt, dass die verschiedenen GRC-Initiativen strukturiert analysiert und Optimierungspotenziale identifiziert werden können.

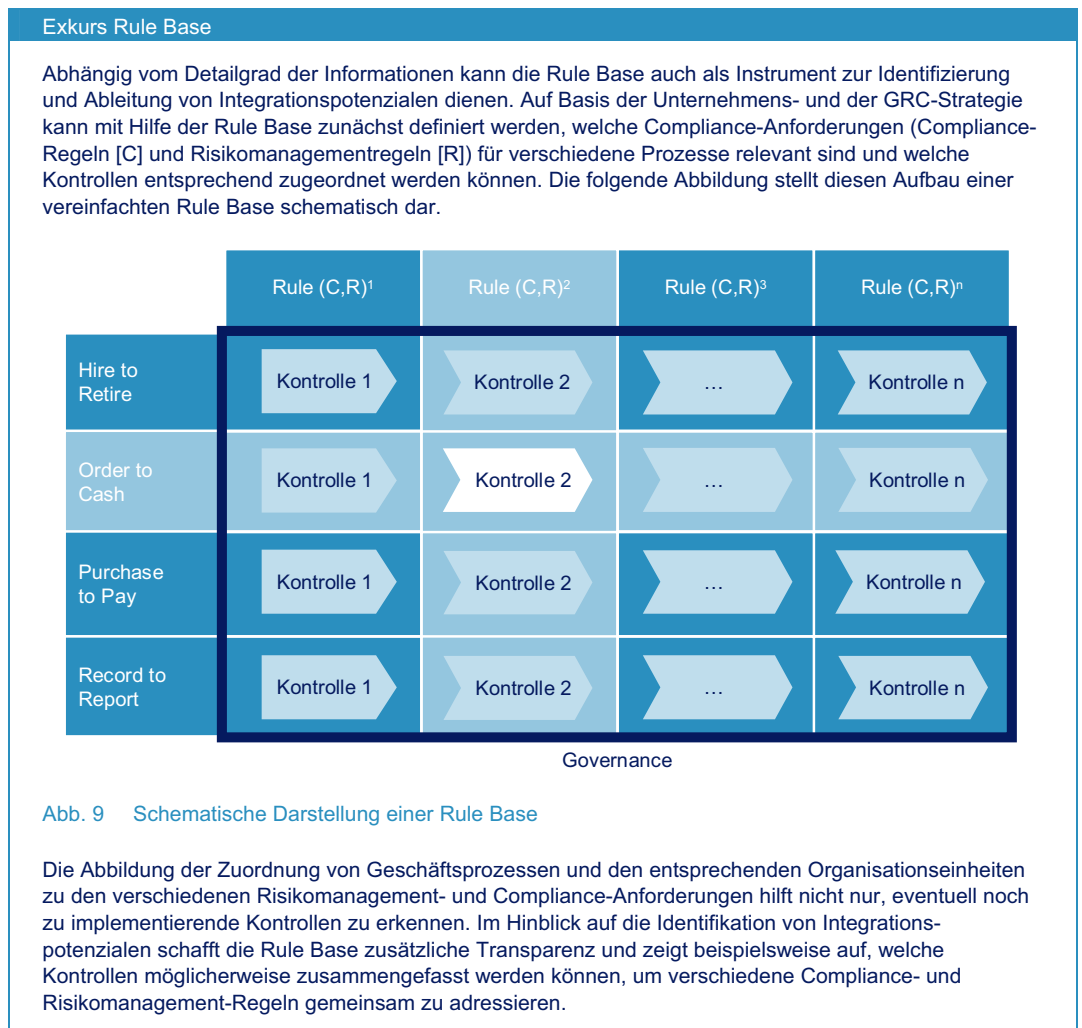
Zur Durchführung der Ist- und der Nachhaltigkeitsanalyse eignen sich beispielweise themenspezifische Workshops und Interviews mit dem Management, dem Compliance Officer sowie den Internal-Control-Verantwortlichen. Auch Fragebögen oder Benchmarking-Studien stellen geeignete Hilfsmittel für eine Analyse dar.

#### Ableitung von Integrationspotenzialen

Auf Basis der Ist- und der Nachhaltigkeitsanalyse können mit Hilfe der Sustainability-Elemente Optimierungspotenziale hinsichtlich der nachhaltigen Umsetzung von einzelnen GRC-Initiativen identifiziert werden. Die Analyse der verschiedenen GRC-Initiativen dient allerdings auch dazu, methodische und inhaltliche Integrationspotenziale zu identifizieren. Diese Potenziale können durch das strukturierte Vorgehen bei der Analyse vergleichbar gemacht werden.<sup>20</sup> Das Erkennen von methodischen Integrationspotenzialen verfolgt das Ziel, die Sustainability-Elemente über verschiedene Initiativen hinweg zu standardisieren. Inhaltliche Integrationspotenziale beziehen sich hingegen auf eine ganzheitliche Umsetzung verschiedener GRC-Initiativen.<sup>21</sup>

<sup>20</sup> Vgl. Abschnitt B.2 zu den methodischen und inhaltlichen Integrationspotenzialen.

<sup>21</sup> Vgl. Abschnitt B.2 für ein Beispiel zur Integration einer SOX- und FCPA-Compliance-Initiative.



### Priorisierung/Implementierung

Basierend auf den Ergebnissen der Ist- und der Nachhaltigkeitsanalyse sowie mit Hilfe der ermittelten Integrationspotenziale lassen sich die Maßnahmen definieren, die zur Umsetzung der GRC-Strategie und zur Etablierung eines nachhaltigen GRC-Managements des Unternehmens beitragen. Bei der Ableitung der verschiedenen Maßnahmen sollte darauf geachtet werden, dass der Nutzenbeitrag (Benefit) jeder einzelnen Maßnahme zum Erreichen eines nachhaltigen GRC-Managements erkenn- und messbar ist.

Unternehmen können sich in verschiedenen Ausgangssituationen befinden und unterschiedliche Ziele in Bezug auf GRC verfolgen. Für die erfolgreiche Umsetzung des Transformationsprozesses ist es daher von großer Bedeutung, den für das Unternehmen unter Kosten- und Nutzenabwägungen anzustrebenden GRC-Zielzustand zu definieren und die abgeleiteten Maßnahmen entsprechen zu priorisieren. Dabei ist zu beachten, dass der beschriebene Transformationsprozess nicht statisch zu betrachten ist. Die einzelnen Phasen bauen sukzessive aufeinander auf und stehen in enger Wechselwirkung zueinander. Beispielsweise können die Erkenntnisse aus der Ist-Analyse den zuvor definierten Scope eines Projekts beeinflussen. Außerdem kann der Transformationsprozess in Form von verschiedenen Implementierungswellen mehrmals durchlaufen werden, um den anzustrebenden, unternehmensspezifischen Sollzustand zu erreichen.

Aufgrund der hohen Komplexität des Themas erfolgt in der Praxis häufig eine sukzessive Umsetzung der identifizierten Potenziale. Dabei ist es empfehlenswert, sich zunächst auf die GRC-Initiativen mit den größten Synergiepotenzialen zu konzentrieren.

Die Implementierung der Maßnahmen kann durch zahlreiche Faktoren beeinflusst werden. Dazu zählen beispielsweise:

- die zeitliche Koordination der Implementierung,
- das Vorhandensein ausreichender Ressourcen,

- die Interdependenzen zwischen bestehenden Unternehmensstrukturen und -prozessen,
- die Auswirkungen von Veränderungen, die mit der Implementierung verbunden sind sowie
- der Erfolg eines kontinuierlichen Change Managements.

#### Monitoring/Optimierung

Im Rahmen der letzten Phase „Monitoring/Optimierung“ wird die Zielerreichung der umgesetzten Maßnahmen durch eine kontinuierliche Überwachung sichergestellt. Hierzu bedarf es eines geeigneten Projektmanagements und der Überwachung bereits zuvor definierter Kennzahlen. Durch die Überwachung sollen nicht nur der Erfolg der umgesetzten Maßnahmen sichergestellt, sondern ggf. auch zusätzliche Optimierungspotenziale bei der Implementierung identifiziert werden.

Bei einer erkannten Abweichung zum gewünschten Sollzustand können zusätzliche Maßnahmen eingeleitet und umgesetzt werden. In diesem Zusammenhang ist das nochmalige Durchlaufen vorgelagerter Schritte des Transformationsprozesses denkbar. Auch eine positive Zielerreichung kann den Anstoß für das erneute Durchlaufen des Transformationsprozesses geben – beispielsweise um den ursprünglich definierten Scope durch weitere Compliance-Initiativen zu erweitern.

## E Fazit

Unternehmerischen Erfolg im Zeitalter der Globalisierung zu sichern und Chancen aus globalem Wachstum zu realisieren, erfordert ein ganzheitliches GRC-Management. Die angemessene Gestaltung und Umsetzung der einzelnen GRC-Initiativen im Unternehmen, ihre Einbettung in das operative Tagesgeschäft und ihre Integration schaffen hierfür die Voraussetzung. Die Unterstützung durch Technologie nimmt hierbei eine Schlüssel-funktion ein. Sie ermöglicht nicht nur die effektive und effiziente Durchführung von GRC-Aktivitäten auf der Prozessebene. Als integrierte Plattform schafft sie die Basis für eine ganzheitliche Steuerung und Überwachung aller unternehmensweiten GRC-Aktivitäten. Die Technologieunterstützung trägt damit wesentlich dazu bei, dass GRC-relevante Informationen als fester Bestandteil bei der Definition und Umsetzung der obersten Unternehmensziele zur Verfügung stehen und hilft so, den unternehmerischen Erfolg langfristig zu sichern.

## F Quellen- und Literaturverzeichnis

### COSO (2004)

Enterprise Risk Management – Integrated Framework, Executive Summary Framework, Hrsg.: COSO - Committee of Sponsoring Organization of the Treadway Commission, o.O., 2004

### Menzies (2006)

Menzies, C. et al.: Sarbanes-Oxley und Corporate Compliance – Nachhaltigkeit, Optimierung, Integration, Hrsg.: Schäffer-Poeschel Verlag, 1. Auflage, Stuttgart, 2006

### PwC/BDI (2002)

Wolfram, J.: Corporate Governance in Deutschland, Hrsg.: PricewaterhouseCoopers AG und Bundesverband der Deutschen Industrie e.V., Frankfurt, 2002, [http://www.bdi-online.de/BDIONLINE\\_INEAASP/iFILE/X2FAFDEBD7B2542CD9A7822F2924E0109/2F252102116711D5A9C0009027D62C80/PDF/Corp%20Gov%20gesamt.PDF](http://www.bdi-online.de/BDIONLINE_INEAASP/iFILE/X2FAFDEBD7B2542CD9A7822F2924E0109/2F252102116711D5A9C0009027D62C80/PDF/Corp%20Gov%20gesamt.PDF), Abruf am 20.02.2007

### PwC (2004)

Integrity-Driven Performance: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management, A White Paper, Hrsg.: PricewaterhouseCoopers, 2004, <http://www.pwc.com/extweb/service.nsf/docid/c8753369ed2d193e85256e1b001c03d6>, Abruf am 20.02.2007

### PwC/BDI (2005)

Hönisch, H. et al.: Corporate Governance in Deutschland – Entwicklungen und Trends vor internationalem Hintergrund, Hrsg.: PricewaterhouseCoopers AG und Bundesverband der Deutschen Industrie e.V., Berlin – Frankfurt, 2005, [http://www.bdi-online.de/Dokumente/Recht-Wettbewerb-Versicherungen/BDI\\_PwC\\_Studie.pdf](http://www.bdi-online.de/Dokumente/Recht-Wettbewerb-Versicherungen/BDI_PwC_Studie.pdf), Abruf am 20.02.2007

### PwC (2005)

8th Annual Global CEO Survey – Bold Ambitions, Careful Choices, Hrsg.: PricewaterhouseCoopers LLP, o.O., 2005, [http://www.pwc.com/gx/eng/pubs/ceosurvey/2007/8th\\_ceo\\_survey.pdf](http://www.pwc.com/gx/eng/pubs/ceosurvey/2007/8th_ceo_survey.pdf), Abruf am 20.02.2007

### PwC (2007)

10th Annual Global CEO Survey, Hrsg.: PricewaterhouseCoopers LLP, o.O., 2007, [http://www.pwc.com/gx/eng/pubs/ceosurvey/2007/10th\\_ceo\\_survey.pdf](http://www.pwc.com/gx/eng/pubs/ceosurvey/2007/10th_ceo_survey.pdf), Abruf am 20.02.2007

### Universität Hamburg: Umfrageergebnisse (2006)

Compliance kann Mehrwert für Unternehmen schaffen, Hrsg.: Universität Hamburg, Hamburg, 2006, <http://www.verwaltung.uni-hamburg.de/pr/2/21/pm/2006/pm25.html>, Abruf am 20.02.2007

## Ansprechpartner

### Christof Menzies

Marie-Curie-Straße 24-28  
60439 Frankfurt am Main  
Tel.: 069 9585-1122  
E-Mail: christof.menzies@de.pwc.com

### Alan Martin

Marie-Curie-Straße 24-28  
60439 Frankfurt am Main  
Tel.: 069 9585-1188  
E-Mail: alan.r.martin@de.pwc.com

### Michael Koch

Marie-Curie-Straße 24-28  
60439 Frankfurt am Main  
Tel.: 069 9585-5919  
E-Mail: michael.koch@de.pwc.com

### Carsten Trebuth

Friedrichstraße 14  
70174 Stuttgart  
Tel.: 0711 25034-3576  
E-Mail: carsten.trebuth@de.pwc.com

PricewaterhouseCoopers ist weltweit eines der führenden Netzwerke von Wirtschaftsprüfungs- und Beratungsgesellschaften und kann auf die Ressourcen von insgesamt 142.000 Mitarbeitern in 149 Ländern zugreifen. In Deutschland erwirtschaften mehr als 8.100 Mitarbeiter in den Bereichen Wirtschaftsprüfung und prüfungsnahe Dienstleistungen (Assurance), Steuerberatung (Tax) sowie in den Bereichen Transaktions-, Prozess- und Krisenberatung (Advisory) an 28 Standorten einen Umsatz von 1,2 Milliarden Euro.

PricewaterhouseCoopers wird mit seinen Spezialisten sowohl in Deutschland als auch weltweit als „Trusted Advisor“ in den Themengebieten Governance, Risikomanagement und Compliance anerkannt und unterstützt Unternehmen bei der Optimierung ihres GRC-Managements. Dabei bietet PricewaterhouseCoopers einen pragmatischen und integrierten Ansatz, um die in Zusammenhang mit Governance, Risikomanagement und Compliance entstehenden Kosten zu senken sowie den damit verbundenen Nutzen zu steigern und eine nachhaltige, risiko- und wertorientierte, ethische und regelkonforme Unternehmensführung sicherzustellen.

