Coporate Governance, Risk- and Compliance Management in der Beschaffung

Lothar Goll / Stephan Haupt

1. Einleitung

Die zweite Industrielle Revolution führte zu einer Verringerung der Fertigungstiefe, die dritte zu einer Verminderung der Leistungstiefe. Beide Entwicklungen mündeten in eine fortschreitende Virtualisierung der Wertschöpfungsprozesse über Unternehmensgrenzen hinweg – Revolution der Wertschöpfung –, die den Unternehmensbereich Einkauf nachhaltig aus seinem historischen Dornröschenschlaf riss. Denn die Verantwortung der Beschaffung nahm im Rahmen der immer komplexer werdenden Führungsstrukturen und Unternehmensverfassungen dramatisch zu, ebenso wie das verantwortete Beschaffungsvolumen. So hat die Beschaffung heute einen maßgeblichen Anteil am Erfolg eines Unternehmens, seinem Ergebnis sowie seinem Wert insgesamt.

Die immer noch fortschreitende Revolution der Wertschöpfung bringt zugleich einen Verlust an Transparenz mit sich, dessen Auswirkungen als „Enron"-, „Volkswagen"- oder „Siemens-Skandal" bekannt wurden. Dies rief die Gesetzgeber insbesondere in den Wirtschaftsländern der ersten Welt und einige ethisch motivierte Wirtschaftslenker auf den Plan: Die von ihnen initiierten Regeln und Richtlinien greifen inzwischen tief in die Freiheiten des Unternehmens- und Fachbereichsmanagements ein. Mehr noch: Vordergründig bremsen die neuen Vorschriften das Tempo der Unternehmensentwicklung sogar unnötig, indem sie einen überflüssigen Overhead schaffen.

Trotzdem: Mit einer neuen Sicht und einem methodischen, werteorientierten Ansatz können Unternehmen ihre Ziele ohne Umschweife erreichen!

Dieser Beitrag zeigt anhand von Projekterfahrungen, wie sich insbesondere die Beschaffung unter Beachtung aller Anforderungen an zeitgemäßes Corporate Governance sowie Risiko- und Compliance Management (GRC) auf die Unternehmensziele hin ausrichten lässt, um allen Widrigkeiten zum Trotz zusätzlichen und nachweisbaren Mehrwert für das Unterneh-

men zu generieren. Ferner wird erläutert, wie erste Schritte eines erfolgreichen „GRC-Management“ aussehen sollten. Dabei wird deutlich, wie sich mit einer ganzheitlichen Betrachtung aus der Beschaffung heraus der Beitrag zur Sicherung und Erhöhung des Unternehmenswertes nachweisbar steigern lässt.

2. Herausforderungen

Die Bedeutung der Beschaffung für den Unternehmenserfolg nahm in den vergangenen Jahren dramatisch zu: Inzwischen erreicht das Beschaffungsvolumen in den meisten Industrien mehr als 60 Prozent des Umsatzes. Nun lag insbesondere in den gerade überstandenen Krisenjahren der Fokus der Unternehmen ohnehin deutlich auf der Kostenseite. Doch selbst in wirtschaftlich prosperierenden Zeiten hängt das Unternehmensergebnis immer stärker von der Kompetenz der Beschaffung ab. Um erfolgreich agieren zu können, ist ein aktives Corporate Governance, Risko und Compliance Management nötig.

2.1 GRC-Management

GRC-Management erfordert grundsätzlich die umfassende, unternehmensweit einheitliche Ausrichtung des Managements und aller eingesetzten Ressourcen auf das eine Ziel, Mehrwert für das gesamte Unternehmen zu schaffen.

Zum GRC-Management gehören:

- **Corporate Governance:** Rahmenwerk von Regeln und Richtlinien, nach denen ein Unternehmen geführt und kontrolliert werden soll
- **Risk Management:** strukturierter Prozess des einheitlichen und pro-aktiven Umgangs mit Risiken und Chancen
- **Compliance Management:** effektive und effiziente Erfüllung sämtlicher verbindlichen Richtlinien und Vorgaben.

Werden die Faktoren erfolgreich in Form konkreter Ziele (siehe Abbildung 1) umgesetzt, entsteht daraus eine Wertsteigerung für das Unternehmen. Dies schließt jede einzelne Unternehmensfunktion ein, also auch die Beschaffung.

Corporate Governance	Unternehmensstrategie	
Unternehmenswert	Compliance	Verlässlichkeit der Rechnungslegung
Optimierung des unternehmensweiten Risiko-Chancenportfolios unter Beachtung der Unternehmens- und Risikostrategie sowie der gesetzlichen Anforderungen an Risiko-Management- bzw. Risikofrüherkennungs-systeme	Erreichen der Unternehmensziele: • unter Einhaltung aller relevanten internen und externen gesetzlichen und freiwilligen Anforderungen • durch Sicherung der Wirksamkeit und Wirtschaftlichkeit der Geschäftsführung • durch Vermögensschutz einschließlich der Aufdeckung und Verhinderung von Vermögensschädigungen	Rechnungslegung gemäß allen steuerlichen, handelsrechtlichen und börslichen Anforderungen

Quelle: Caniu GRC – GRC Management Methodik
Abbildung 1 : Ziele des GRC-Managements

2.2 Externe und interne Anforderungen

Die Beschaffung bekommt immer mehr Verantwortung zugesprochen. Damit verbunden sind allerdings auch wachsende gesetzliche Anforderungen und Qualitätskriterien, mit denen Unternehmen heute konfrontiert sind. Dies betrifft insbesondere das Risiko- und Compliance Management. Die globale Vernetzung der Wertschöpfungskette zieht eine Flut von Vorgaben und Richtlinien nach sich, die vom Einkauf bislang so nicht direkt zu beachten waren. Zudem sind die Unternehmen oft auch vor der internen „Regelungswut“ nicht gefeit. Obendrein stimulierten prominente „Skandale“ (Enron, Opel, VW, Siemens) die Regelungs- und Durchsetzungswut des Gesetzgebers, anstatt wie oft gefordert Gesetze zu verschlanken und die freie Wirtschaft nicht über Gebühr zu behindern.

2.2.1 Gesetzliche Vorschriften

Zu den Anforderungen der lokalen und internationalen Gesetze gehören:

- **Aufbau eines Chancen- und Risikomanagements**
  Der Aufbau eines Risikomanagementsystems wird gefordert im *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich* (KonTraG), § 91, 2 AktG, §§ 289, 315 HGB. Weiteren Druck auf Vorstand/Geschäftsführung übt das *Transparenzrichtlinie-Umsetzungsgesetz*

(TUG) aus: Es fordert den Bilanzeid und droht erstmals in Deutschland direkt Geld- und/oder Gefängnisstrafen an. Dies bedeutet für die Beschaffung, die Chancen- und Risikosituation im Lagebericht darzustellen und effektiv zu bewerten. Ferner müssen die identifizierten Chancen und Risiken im Rahmen standardisierter Abläufe und Methoden gesteuert werden.

- **Internes Kontrollsystem**
  Interne Kontrollen sind nicht nur ein Erfordernis der Eigentümer oder Manager, sondern werden auch von externen Stellen, wie Gesetzgeber, EU, Rechnungshöfen, Wirtschaftsprüfern, Versicherungen und Banken, verlangt. Gesetzliche Grundlage dafür sind in Deutschland vor allem § 317 Abs. 4 HGB-Gesetz und § 91 Abs. 2 AktG. Die Änderungen der Anforderungen der 4., 7. und 8. EU-Richtlinie üben zusätzlichen Druck zur Verbesserung und Effizienzsteigerung des internen Kontrollsystems über die Abschlussprüfung aus.

  Daraus ergeben sich umfassende Anforderungen an die Organisation und den Prozess der Beschaffung:

  - Sicherstellung der gesetzlich geforderten Ordnungsmäßigkeit der Buchführung und der DV-gestützten Anwendungssysteme
  - Schutz von Vermögenswerten
  - Einhaltung der Geschäftspolitik bzw. der Strategie
  - Wirtschaftlichkeit und Transparenz der Arbeitsabläufe
  - Erhöhung der Informationsqualität durch genaue, aussagefähige, zeitnahe Aufzeichnungen
  - Fehlerprävention und Fehleraufdeckung
  - Verhinderung doloser Handlungen und Rechnungslegungsdelikte

- **SOX (Sarbanes-Oxley-Act)**
  Die multinationale Vernetzung der Wertschöpfungskette und Best Practices machen zunehmend die SOX-Zertifizierung der Lieferanten von SOX-pflichtigen Unternehmen erforderlich – zunächst als Best Practice.

- **Basel II:**
  Schärfere Finanzierungskriterien fordern von der Beschaffung:

  - alternative Finanzierungsoptionen beim Kauf zu validieren (Kapitalstruktur), z.B. Miete, Operate Leasing (IFRS-neutral) oder Full Service Leasing für Fahrzeuge, Maschinen, Computer etc.
  - aktiven Beitrag zur Optimierung des Chancen-/Risikoprofils im Hinblick auf die Wahrscheinlichkeit, dass unvorhergesehene Umstände die Kapitaldecke aufzehren könnten und dies zur Zahlungsunfähigkeit führt.

- **Boykottlisten**
  Die Konformität mit Außenwirtschaftsgesetz (AWG) und US-Recht verlangt von der Beschaffung, dass sogenannte Boykottlisten mit den aktuellen EU-Listen sowie den verschiedenen US-Listen (Denied Persons List/DPL), Entity List, Specially/ELS) und Designated Nationals List/SDN) zeitnah abgeglichen und zur Prüfung herangezogen werden.

Weitere relevante Rechtsetzungen können unter anderem sein:

- OWiG (Gesetz über Ordnungswidrigkeiten)
- Int/EuBestG (Internationales/EU-Bestechungsgesetz)
- Rahmenbeschluss zur Korruptionsbekämpfung des Rates der EU von 2003
- GefStoffV (Gefahrstoffverordnung)
- MaRisk (Mindestanforderungen für Risikomanagement – Fokus Banken)
- VHB (für die öffentliche Hand), BDSG (Bundesdatenschutzgesetz)

Mit diesen komplexen Anforderungen wird es immer schwerer, ohne Transparenz schaffende Systeme Aussagen zu Compliance und Sicherheit zu treffen.

2.2.2 Deutscher Corporate Governance Kodex (DCGK) und Corporate Compliance-Programme

Der Deutsche Corporate Governance Kodex (DCGK), Verhaltensstandard zur Unternehmensführung und -überwachung, soll die entsprechenden hierzulande geltenden Regeln für nationale und internationale Unternehmen transparent machen. Die meisten Bestimmungen des DCGK haben sich in den zurückliegenden fünf Jahren als Kernbestand der Standards guter Corporate Governance in der deutschen Wirtschaft etabliert. Sie zwingen viele Unternehmen, umfangreiche Regelungen einzuführen, die sie so bislang nicht praktizierten. Zu deren Umsetzung hat sich in Unternehmen als „Good Practice“ die Einführung von Corporate Compliance-Programmen etabliert.

Für die Beschaffung stellt sich die Anforderung, dieses Compliance-Programm nachhaltig in das operative Tagesgeschäft umzusetzen. Dies geschieht durch die Etablierung konkreter Verfahrensanweisungen, etwa Prozesshandbücher mit Zeichnungsautorisierungen, und die Vorgabe von Normen.

2.3 Herausforderungen durch Innovationswellen der Beschaffung

Die Beschaffung hat in den vergangenen Jahren in Wellen eindrucksvoll den Wandel vollzogen von einer sogenannten Bestellschreiberfunktion zu ihrer aktuellen Rolle als Organisationseinheit, die maßgeblich Unternehmenswert schafft. Als Konsequenz dessen müssen sich die Beschaffungsleiter nun wachsenden gesetzlichen Anforderungen (Haftung bei Nicht-Erfüllung von Sorgfaltspflichten) und Qualitätskriterien stellen.

2.3.1 Automatisierungswelle

Lange Jahre war die Beschaffung eher ein Stiefkind der Softwarelieferanten. Dann jedoch dynamisierten wesentliche Innovationen aus diesem Bereich die Beschaffungswelt:

- Produktionsplangetriebene Bestellschreibung (PPS/ERP)
- Lieferantenmanagementsysteme
- Katalogsysteme
- Automatisierung von Teilprozessen der strategischen Beschaffung
- Beschaffungsanalyse-Systeme
- „Deep Linking“ mit Geschäftspartnersystemen,

Positiv wirkt sich der Einsatz dieser Systeme aus, weil ihre Durchgängigkeit ermöglicht, beachtliche Nutzenpotenziale zu heben, etwa im Bereich der Bearbeitungszeiten und der Fehlerkosten. Ferner lassen sich so zahlreiche Risiken minimieren, wie Fehleingaben, Doppelbestellungen, Liegezeiten oder nicht autorisiertes Handeln. Andererseits resultieren aus diesen Systemen neue Komplexitäten und Risiken, die von der Beschaffung professionell gemanagt werden müssen.

2.3.2 Beschaffungskategorienwelle

Die Wellen der IT-Innovationen ermöglichten es, die Produktivität der Beschaffung maßgeblich zu steigern. Dadurch ließ sich die Beschaffungs-Compliance signifikant erhöhen, sodass zunehmend mehr Beschaffungskategorien abgedeckt wurden. Im Zuge dessen bekam die Beschaffung das Spend-Volumen des Unternehmens und die Preise zunehmend in den Griff. Zugleich tat sich aber auch hier eine bislang unbekannte Vielfalt an Risiken und Compliance-Anforderungen auf.

2.3.3 Verringerung der Leistungstiefe (Industrialisierungswellen)

Nach der signifikanten Verminderung der Wertschöpfungstiefe in der Produktion (beim SMART auf 20 Prozent) reduziert sich auch im Verwaltungsbereich, zu dem die Beschaffung gehört, zunehmend die „Leistungstiefe“. Diese Entwicklung ist geprägt durch …

- unternehmens-externe Prozessunterstützung für Teilaufgaben der strategischen und operativen Beschaffung
- Beschaffungskooperationen
- Einsatz von externen Beschaffungsdienstleistern für einzelne Beschaffungskategorien

- Übernahme des gesamten „Procure to Pay“-Prozesses
- Outsourcing der strategischen Beschaffung von nicht strategischen Materialien.

Je komplexer diese Geschäftsprozesse und -modelle werden, desto mehr Relevanz erhalten die zentralen Aspekte des GRC-Managements.

2.3.4 Welle der multinationalen Vernetzung

Die Beschaffungsorganisationen sind heute Länder übergreifend vernetzt und virtualisiert. Dafür sorgen die Öffnung der Märkte, die Reduktion von Handelsbarrieren und das globale Wachstum, die Exportorientierung der Wirtschaft sowie das globale Preisgefüge bzw. -gefälle. Zudem ermöglicht das durchgängige World Wide Web immer größere Transparenz, mehr Informationsgewinnung und schnelleren Informationsaustausch. Gemeinsam mit den vorgenannten Entwicklungslinien ergeben sich dadurch für die Beschaffung jedoch auch Anforderungen, die durch ihre Kombination noch schwieriger professionell und industriell zu beherrschen sind.

Betrachten wir einige Auslöser und ihre Folgen:

- *Die Verringerung der Wertschöpfungstiefe ...*
  führt zu einer laufenden Erhöhung der Beschaffungsvolumina und damit der Kritikalität beschaffter Komponenten für das Unternehmensergebnis; die kontinuierliche Make-Or-Buy Entscheidung wird zum operativen Tagesgeschäft.
- *Die Verringerung der Leistungstiefe ...*
  erfordert das Management von Beschaffungsdienstleistern (Outsourcern) als externe, aber integrale Bestandteile der Führungsorganisation der Beschaffung.
- *Das Global Sourcing, die Beschaffung für mehr als nur die lokale Produktion, ...*
  schafft eine neue Qualität von Länder- und Lieferantenrisiken (Rechtssysteme, Kulturen etc.); diese ziehen zum Teil weit reichende Eingriffe in das Management der eigenen und die Wertschöpfung der Lieferanten nach sich, um die Lieferqualität und Genauigkeit sicherzustellen.
- *Die unternehmensübergreifende Beschaffung im Wege von Co-Sourcing, Einkaufskooperation, Konsortien etc. ...*
  macht eine unternehmensexterne Standardisierung von Waren und Dienstleistungen erforderlich, um Skaleneffekte und die Reduktion der Prozesskosten zu ermöglichen.

2.3.5 Handlungsbedarf für die Beschaffung

Angesichts der dynamischen Veränderungen der Rahmenbedingungen wird deutlich: Die zunehmenden Herausforderungen an die Beschaffung machen ein pro-aktives GRC-Management nicht nur notwendig, sondern vielmehr unerlässlich!

Herausforderungen	Risiken / Chancen	Compliance	Rechnungslegung	Handlungsansätze in der Beschaffung
Gesetzliche Vorschriften	0 / --	--	-	Risikomanager, Compliancemanager,...
Normen, Kodices, …	0 / --	--	-	"Whistelblower"
Firmenspezifische Richtlinien	-- / --	--	-	Mitarbeiter-Qualifikation, Monitoring, …
Automatisierungs-Welle	-- (Risiken der IT, Sicherheit der IT, Betrug)	++	++	Management der IT, Mitarbeiter-Qualifikation, IT-Sicherheit, …
Beschaffungs-kategorie-Welle	-- /++	++	0	Mitarbeiter-Qualifikation, Standards, interdisziplinäre Zusammenarbeit, Monitoring
Industrialisierungs-Welle (Verringerung der Leistungstiefe)	-- / ++	++	+	SLAs Aufgabenteilung; strukturiertere Arbeit, Verlagerung und Hohe Anforderungen an Koop-Mgmt
Welle der multinationalen Vernetzung	-- / ++	--	--	Lieferantenmonitoring, und Support, Kultur, …

(-- hoher Handlungsbedarf bis ++ Chancen resultieren)

Quelle: Caniu GRC – Handlungsbedarf in der Beschaffung
Abbildung 2: *Evaluationsmatrix neuer GRC-Herausforderungen*

Dabei sollten die Herausforderungen und ihre Auswirkungen grundsätzlich nicht isoliert voneinander betrachtet werden, da sie hohe Interdependenzen und oft gegensätzliche Wirkungsrichtungen zeigen (siehe Abbildung 2). Die Vorhersehbarkeit des Großteils dieser Auswirkungen verlangt jedoch geradezu danach, ihnen nicht nur präventive, sondern auch bei ihrem Eintreten sofort aktivierbare Notfallpläne entgegen zu setzen. Vor diesem Hintergrund ist es notwendig, eine GRC-spezifische Kompetenz aufzubauen, die Mitarbeiter, Organisation, Abläufe und Systeme einschließt.

2.4 Status Quo des GRC-Management

GRC-Management als Begriff etabliert sich erst. Insofern sind definitionsgemäße, flächendeckende, strukturierte und integrierte Ansätze eines GRC-Managements für die Beschaffung noch in Planung. Derzeit sind folgende Einzelkomponenten des GRC anzutreffen:

- manuelles Risiko- und Frühwarnsystem, um dem KonTraG zu genügen; Interpretation nicht als IT- sondern als Verfahrenanforderung; meist nur jährliche Fortschreibung
- reaktives, aus dem Finanzbereich getriebenes Risiko-Management, das gesetzlichen Minimalanforderungen genügen soll; einzelne Pflichtenkreise (Haftung und Sorgfaltspflichten) werden an die Beschaffung delegiert, oft mit unzureichender Kommunikation und Qualifizierung der Mitarbeiter
- in Ausnahmefällen und oft nach Schadenseintritt wiederholte Betrachtung der Lieferantenbewertung sowie nachträgliche Reflektionen über Notfallpläne zur Krisenbewältigung
- isolierte Verfahren und Betrachtung von Gesetzen/Anforderungen und Einzelrisiken, aber auch Währungsrisiken, Lieferantenrisiken und Gesetzlichkeiten
- Risiko-Management als Standard bei der Beschaffung von Rohstoffen
- heterogene, punktuell unterstützende Verfahren und Systeme, wie Hedging, Lieferantenauditierung etc.
- Risiko- und Compliance-Management als Bestandteil des strategischen Sourcings, in eher eingeschränkter Form von Lieferantenqualifizierung, Lieferantenzertifizierung, Lieferantenauditierung
- Risiko-Management abhängig von der gefühlten Risikoaversität des Beschaffers, nicht von unternehmensstrategischen Überlegungen.

Festzuhalten bleibt eine große Interpretationsbandbreite externer und interner Richtlinien, die der jeweiligen Unternehmenskultur entsprechend durchgesetzt werden. Dies erfolgt oft mit minimal möglichem Aufwand – wohl eher weil über das Mehrwertpotenzial nicht ausreichend nachgedacht wird.

3. Folgen unzureichenden GRC-Managements

Mit welchen negativen Auswirkungen muss die Beschaffung rechnen, wenn sie sich nicht pro-aktiv den Anforderungen eines integrierten GRC-Managements stellt?

Sicher sind zumindest diese Folgen:

- **erhöhte Kosten**, z. B. Einstandspreise, Versicherungsprämien, Prozesskosten
- **erhöhtes Risiko**, z. B. nicht systematisch erkannte und gesteuerte Risiken
- **geringere Compliance**, z. B. Haftung aus Verletzung von Sorgfaltspflichten
- **eingeschränkte Fähigkeit zur Krisenbewältigung**, z.B. Produktqualitätsprobleme
- **Reputationsprobleme**, z. B. Sourcing bei nicht konformen Unternehmen (etwa Kinderarbeit)

Ein „weiter so wie bisher"-Verhalten kann auch noch weitere Konsequenzen haben.

3.1 Global Sourcing

Global Sourcing bringt ineffiziente Governance-Strukturen und ein unzureichendes Risiko-Management besonders deutlich ans Licht. Denn durch die meist mehrstufigen Lieferantenbeziehungen ergeben sich Gefahren, etwa Vorteilsnahmen oder weitere spezifischen Niedrig-Lohn-Land-Risiken. *Wertvernichter sind:*

- hohe Vorlaufkosten vor der ersten Lieferung bzw. ersten Ergebnissen
- hoher Abstimmaufwand und lange Abstimmzeiten im Gesamtprozess
- hohe Kommunikationskosten bei eingeschränkter Erreichbarkeit und eingeschränktem gegenseitigem Verständnis
- unzureichende Gewährleistung der Qualitätssicherung, die nach den Regeln des Auftraggebers vor dem Versand der Ware erfolgen sollte
- Marken- und Kopierschutz
- unzureichenden Länderbewertungen nach Chancen und Risiken
- hohe Korruptionsrisiken und Vermögensschädigungen (Niedrig-Lohn-Land-Risiken).

Hierbei handelt es sich jedoch auch um Mehrwert-Potenziale, die sich durch ein professionelles GRC-Management heben lassen.

3.2 Mengen- und Preisrisiken

Zur Absicherung von Mengen- und Preisrisiken bietet sich für börslich notierte Grundstoffe das Hedging an. Dieses Instrument wird jedoch, wie die meisten anderen seiner Art, eher isoliert angewandt und selten gebündelt, etwa in Form von „Baskets“. Dadurch werden zum einen Einsparpotenziale nicht genutzt. Zum anderen ist diese Form der Risikoabwehr selten in der Verantwortung der Beschaffung, obwohl dort meist die beste Produkt- und Marktkenntnis zur Verfügung steht.

3.3 Laufendes Risiko-Management und Notfallpläne

Der Stillstand des Kernkraftwerks Biblis (RWE) aufgrund fehlerhafter Verankerungstechnik (Dübel) löste bei den Mitbewerbern offenbar keine Überprüfung ihrer Vorsorgemaßnahmen gegen derartige Risiken aus. Wie anders lässt es sich erklären, dass das gleiche Problem ein halbes Jahr später bei Vattenfall auftreten konnte? Für letzteres Unternehmen kam dieser Störfall wohl so überraschend, dass er bei seinem Eintreten auch über keine voraus geplante Kommunikationsstrategie verfügte, die automatisch hätte anlaufen können.

Im Nachhinein drängt sich die Überlegung auf, um wie viel kleiner ein intaktes Risiko-Management, wie es in der Luftfahrtindustrie nach Flugzeugabstürzen anläuft, die Schädigung des Unternehmenswertes hätte halten können.

3.4 Insolvenzen von Lieferanten

Für die Beschaffung bleibt die Entwicklung der Unternehmensinsolvenzen kritisch, weil damit ebenfalls das Risiko steigt, an begrenzt solvente Lieferanten zu geraten. Will die Beschaffung vor diesem Hintergrund Mehrwert generieren und Schädigungen des Unternehmenswertes vermeiden, sollte sie sensibel jede Veränderung in der Gesellschafter- und Finanzierungsstruktur des Lieferanten oder der Partner (die mit zunehmendem Einbezug im Rahmen des Outsourcings von Beschaffungsdienstleistungen an Bedeutung gewinnen) im Blick haben. Zum anderen muss die Beschaffung bei Bedarf Notfallpläne für den Ausfall eines Lieferanten exekutierbar aus der Schublade holen können, mit denen sich z. B. wesentliche Teile der betroffenen Produktreihen alternativ beschaffen lassen.

3.5 Notwendigkeit des proaktiven GRC-Managements

Schon diese wenigen Beispiele lassen erkennen: Die „Costs of doing nothing“ durch ein fehlendes aktives und integriertes GRC-Management können erheblich sein. Zudem sind der Umsetzung von Best Practices Grenzen gesetzt, da es immer aufwändiger wird, hiermit Mehrwert zu generieren. Unsere Analysen in der Beschaffung von Industrie-, Handels- und Logistikunternehmen bestätigen, dass mit einer neuen Sicht bislang verborgene Synergien gehoben werden können:

- Nach Projekt-Erfahrungen zeichnen sich Investitionen in ein integriertes GRC-Management nicht nur generell durch einen schnellen „Pay-Back“ aus. Vielmehr sind so meist auch die betreffenden GRC-Problematiken zügig in den Griff, d. h. Risiken und Richtlinien-Compliance unter Kontrolle zu bekommen – soweit das Management hinter diesem Vorhaben steht.
- Außerdem winkt derzeit noch der Imagegewinn eines Vorreiters, der in die Beschaffung Best Practices einführt, die im Finanzbereich aufgrund gesetzlicher Vorgaben schon teilweise realisiert sind, aber bislang noch nicht integriert gehandhabt werden.

4. Erfolgreiches GRC-Management

„Cut out the risk for the biggest rewards“ – unter diesem Titel beschäftigte sich die Financial Times am 10. Mai 2007 mit dem Zusammenhang von Risiko und Gewinn. Dazu zitiert die Zeitung eine zentrale Aussage des Beraters und „Wachstumspropheten“ Adrian Slywotzky, der in seinem neuen Buch feststellt:

> *„THE LEADERS OF TODAY’S SUCCESSFUL COMPANIES ARE RISK SHAPERS RATHER THAN RISK TAKERS!“*

Anders formuliert bedeutet das: Aktives Mehrwert-Management basiert auf einer optimalen Balance zwischen unternehmerischem Handeln und der Abwehr von Risiken. Zu Letzterer zählt im Übrigen auch die Einhaltung der immer umfangreicheren Gesetze und Richtlinien. Um dies zu gewährleisten, bedarf es einer strategischen Zielsetzung des Unternehmens und einer daraus abgeleiteten Positionierung zu den jeweils relevanten GRC-Themen.

4.1 Definition

Eine umfassende Definition von GRC-Management könnte lauten:

> **GRC-Management …**
> ist die effiziente und effektive unternehmensweite Ausrichtung der drei Elemente Corporate Governance, Risiko-Management und Compliance auf die Sicherung bzw. Erhöhung des heutigen und zukünftigen Unternehmenswertes. GRC-Management stellt die Einhaltung aller unternehmensinternen und -externen Richtlinien sowie einer guten Corporate Citizenship sicher.

Die Bestandteile eines GRC-Managements, wie in Kapitel 2.1 erläutert, sind:

- Corporate Governance
- Risiko-Management
- Compliance-Management

Eine derart umfassende Definition bedingt folgerichtig eine integrierte Sichtweise und Umsetzung der Themenbereiche Risiko-Management und Compliance Management. Häufig werden diese jedoch in den Unternehmen isoliert betrachtet, zumal sie auch in unterschiedlichen Organisationseinheiten (Interne Revision, Versicherungsmanagement, Risikomanagement, etc.) sowie in verschiedenen Unternehmensbereichen/Niederlassungen angesiedelt sind. Meist gibt es ebenfalls unterschiedliche Beauftragte in und außerhalb des Unternehmens bei (Anzeigestellen, Korruptionsbeauftragte, ComplianceBeauftragte etc.). Tatsächlich setzen diese verschiedenen Bereiche in der Praxis jedoch oft auf identische Organisationsstrukturen und Geschäftsprozesse auf. Auf diese Weise lassen sich zwar Einzelziele erreichen, doch mögliche Synergieeffekte und Effizienz-Potenziale sind so nicht zu heben. Vielmehr bleiben wichtige Chancen zur Erhöhung des Unternehmenswertes ungenutzt.

4.2 Die wichtigsten Erfolgsfaktoren eines umfassenden GRC-Managements

Die erfolgreiche Umsetzung eines integrierten GRC-Managements im Unternehmen oder für einen Geschäfts-/Funktionsbereich ist an folgenden sechs Erfolgsfaktoren fest zu machen:

4.2.1 Strategische Ausrichtung

Die GRC-Positionierung und -Ziele eines Unternehmens müssen an seinen Corporate Governance-Leitlinien und seiner Unternehmensstrategie ausgerichtet sein (siehe auch Abbildung 1). So werden ein hoher Wirkungsgrad der GRC-Steuerungsmaßnahmen und ein nachhaltiger

Effekt auf den Unternehmenswert gewährleistet. Nachteilig wirkt sich eine isolierte und gegebenenfalls sogar funktionsspezifische, primär an Revisionsanforderungen orientierte Behandlung von Risiko- und Compliance-Fragestellungen aus.

Wie lassen sich GRC-Ziele operationalisieren?

Im ersten Schritt müssen die Anforderungen analysiert werden, die aufgrund der rechtlichen Struktur und des Aufbaus des Unternehmens gegeben sind. Den Rahmen dafür geben die nationalen und internationalen Gesetze und Richtlinien vor. Gleiches gilt für die Identifikation der materiellen bzw. immateriellen Werttreiber (siehe Abbildung 3), die für den aktuellen und den zukünftigen Unternehmenswert relevant sind. Auf dieser Basis werden die Ausgangs- und die Aufsetzpunkte für die Positionierung eines integrierten GRC-Managements im Unternehmen definiert.

Unsere auf die Werte fokussierte Methodik ermöglicht mit GRC Management MehrWert zu identifizieren, wahren und entwickeln

Werte - Anforderungen

Beispiel Beschaffung

	Leistung der Administration	Finanzielle Stärke	Lieferanten	Logistik	Personal	Technologie & Infrastruktur
Materiell	• Kosteneffizienz • Service-Level • Prozess-Standardisierung • Nachhaltigkeit erzielter Einsparungen • Compliance • …	• Kapital-produktivität • Cash-Flow • Forderungen • Liquidität • Investitionen • Gebäude, Maschinen und Ausrüstung • …	• Effizientes Vergabe-Management • Lieferantenpflege -aufwand • Erschlossener Lieferanten-Markt • Vertrags-management • …	• Nachfrage-Mgmt • Transport-Mgmt • Logistikabläufe • Bestandshöhe • Bestandswert • Working Capital • …	• Mitarbeiter-Fluktuation • “Diversity” • Management-Verträge • Dokumentierte, direkte verfügbare Fähigkeitsprofile • …	• Automatisierungs-und Integrationsgrad z.B. SRM-Systeme • Zentralisierung/ Standardisierung von Systemen und Daten • Betriebskosten-Effizienz
Immateriell	• Image der Beschaffung im Ug. • Risiko-transparenz • Compliance mit übergeordneten Regelungen SOX etc. • Ausmaß interner Kontrollen	• Lieferanten-Kredit- Ratings • Investor Relations • …	• Lieferanten-Abhängigkeit • Lieferanten-Präferenzen • Lieferanten-zusammenarbeit • …	• Nachfrage-Flexibilität in der Logistikkette • Logistik-Leistungsfähigkeit • Zugriffs-Rechte • Bestands-Qualität • …	• Führungs-kompetenz • Mitarbeiter-Loyalität • Mitarbeiter-Qualität • Problem-Lösungsfähigkeit • …	• Supply-Chain Transparenz • Daten-Integrität und Sicherheit • IT-Kunden und Lieferanten Service • …

(Quelle: Caniu GRC – GRC Management Methodik)
Abbildung 3: *Beispiel: Im- und materielle Werttreiber der Beschaffung*

Hinsichtlich der rechtlichen Anforderungen gibt es in der Regel keine Toleranzen. Allerdings bestehen derzeit noch erhebliche Interpretationsspielräume. Diese grenzen die Gerichte jedoch zunehmend ein. Damit erzwingen sie eine stringentere Umsetzung und engere Auslegung der Gesetze.

Dagegen verlangt die Operationalisierung der GRC-Ziele auf der Ebene der im/materiellen Werttreiber einen differenzierteren Ansatz (siehe Abb. 3). Um Transparenz, Vergleichbarkeit und klare Verantwortlichkeiten sicherzustellen, sollten mit der gebotenen Vertiefung je nach funktionalem Bereich messbare Ziele, akzeptierte Toleranzen und Steuerungsvorgaben (für identifizierte Handlungsbedarfe) vorgegeben werden.

Für Unternehmen, die ihr operatives Geschäft von verschiedenen internationalen Standorten aus betreiben, empfiehlt es sich, über nationale Gesetze und Richtlinien (wie etwa das KonTraG) hinaus eigene Compliance-Standards sowie Beschaffungsrichtlinien zu setzen. Diese müssen die jeweiligen nationalen Anforderungen der Länder, in denen man aktiv ist, hinreichend berücksichtigen und abdecken. Für die Beschaffung sind dabei auch die Vorgaben der Geschäftspartner zu betrachten.

4.2.2 Wertorientierung

GRC-Management ist Wertmanagement. Wichtiger als die ausschließliche Fokussierung auf Gesetze und Richtlinien ist, dass GRC-Management zur langfristigen Steigerung des Unternehmenswertes messbar beiträgt. Dies schließt auch das kritische Hinterfragen von Risiken und Kontrollen auf Ihre „materiality“ hin ein – sprich die Fokussierung auf das, was zur Schaffung von Mehrwert wesentlich ist.

Der Erfolg eines integrierten GRC-Managements ist an den (diesbezüglichen) spezifischen Messgrößen abzugreifen, die sowohl als Entscheidungskriterium wie auch zur Kontrolle der Steuerungsmaßnahmen aller Unternehmenseinheiten genutzt werden können:

- Economic Value Added (EVA)
  - Reduktion der Personal- und Sachkosten für Risiko- und Compliance Management
  - effiziente Risikosteuerung mit Maßnahmenportfolio
  - Reduktion von Vermögensschädigungen
  - Reduktion der Kontrollen und Prüfungen
- Enterprise Value (EV)
  - effiziente Unternehmensleitung
  - Wahrung der Kapitalgeberinteressen
  - transparenter Umgang mit Chancen und Risiken

4.2.3 Performance-Management

Für die Integration der GRC-Thematik in das Performance-Management eines Unternehmens ist es entscheidend, dass GRC zu einem elementaren Bestandteil des strategischen und operativen Planungs-, Steuerungs- und Controllingzyklus wird. Die aktive Einbeziehung der GRC-Fragestellungen muss im Rahmen des Performance Managements über das Linienmanagement der einzelnen funktionalen Bereiche (Beschaffung) erfolgen.

Die GRC-Inhalte sollten als gleichwertig mit anderen Zielgrößen (Total Cost of Ownership-Einsparungen, Prozesskostenkostensenkung, schnellere Markteinführung neuer bzw. veränderter Produkte und Services) anerkannt werden. Zudem stellen die GRC-Themen einen wichtigen Bestandteil für die Bewertung der Leistung einzelner Mitarbeiter dar.

4.2.4 Standardisierung

Eckpfeiler eines effektiven und effizienten GRC-Managements im Unternehmen ist eine einheitliche und umfassend integrierte Vorgehensweise. Sie sollte sich auf folgende Elemente stützen:

- schlanke GRC-Support-Organisation, die die verantwortlichen operativen Funktionsträger pro-aktiv unterstützt
- einheitliche GRC-Methoden und -Prozesse, basierend auf der COSO ERM-Methodik (Committee of Sponsoring Organizations of the Treadway Commission)
- integrierte GRC-Software-Standardlösung auf einheitlicher Datenbasis mit den Komponenten „Internes Kontrollsystem“, „Risiko-Managementsystem“, „Performance Management/Reporting“ und „Prozessmanagement“
- enge Vernetzung mit internen Applikationen und externen Informationsquellen.

Das bedeutet für die Beschaffung: gemeinsame Nutzung einer Softwarelösung, die die Belange des integrierten GRC-Managements abdeckt.

4.2.5 Kultur

Die Effektivität und Effizienz des GRC-Managements wird nicht nur durch die Governance, also die Führungsstruktur bestimmt, sondern insbesondere durch die Führungskultur. Die weitere Definition von Governance umfasst diesen Aspekt auch. Eine einheitliche und konsistente Umsetzung einer eigenen GRC-Kultur fördert ausgewogenes unternehmerisches Handeln unter Beachtung der Chancen und Risiken sowie der internen und externen Anforderungen.

Konkret sollte eine eigene, unternehmensspezifische und beschaffungsspezifische GRC-Kultur folgende Ansätze aufweisen:

- Führung und Strategie
  - Die Unternehmensführung ist sich ihrer Vorbildfunktion bewusst.
  - Klare Botschaften vom Topmanagement bekräftigen die GRC-Philosophie und deren strategische Vorteile.
  - Das Bewusstsein wächst, dass Risikokultur von der gesamten Organisation gelebt wird.
  - Das GRC-Management ist nicht alleinige Aufgabe eines GRC-Managers oder einer bestimmten Organisation.

- GRC-Management und Infrastruktur
  - Das operative GRC-Management und die Infrastruktur bilden ein System mit klar definierten Rollen und Prozessen.
  - Das GRC-Management hat keine reine Stabsfunktion; vielmehr ermöglicht es den Mitarbeitern, die Risiken bzw. Chancen und die Compliance ständig im Tagesgeschäft zu erleben.
- Mitarbeiter und Kommunikation
  - Alle Mitglieder der Organisation sind involviert; Kommunikationsplattformen fördern ein kontinuierliches Risiken-Chancen-Bewusstsein.
  - Alle Mitarbeiter tragen Verantwortung; sie kennen ihre Freiheiten und Kompetenzen bezüglich Risiken und Compliance-Anforderungen.
  - Trainings und Coachings verbessern den Einsatzwillen in risiko- bzw. compliancerelevanten Problemsituationen; die Bereitschaft zu kontinuierlicher Fortbildung wächst.

4.2.6 Anforderungsmanagement

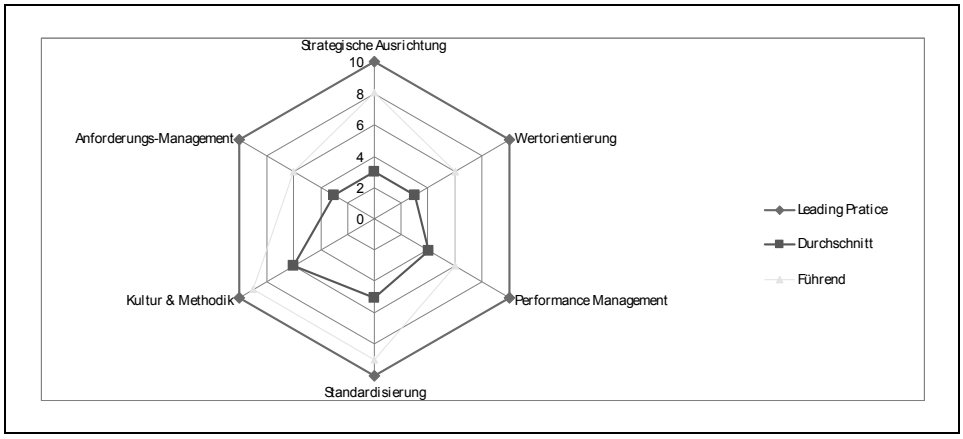
Das GRC-Management muss sowohl bekannte als auch unerwartete interne und externe Entwicklungen dahingehend bewerten, ob und wie sie sich diese positiv oder negativ auswirken können. Kriterien dabei sind die identifizierten im-/materiellen Werttreiber, aber auch das Erreichen der Unternehmensziele bzw. der Bestand des Unternehmens. Im Ergebnis lassen sich so zeitnah Handlungs- und Steuerungsbedarfe aufzeigen. So werden der Wirkungsgrad des GRC-Managements erhöht und die Kosten für die Steuerungsmaßnahmen nachhaltig gesenkt.

Ein effektives Anforderungs-Management umfasst folgende Bestandteile:

- Früherkennungssystem mit den Komponenten
  - operative Kontrolle (t, t+1) in Form von Frühwarn-, Frühindikatoren- und Frühaufklärungssystemen
  - Prognosesysteme (t+2, n) in Form etwa der Delphi-Methode und der Szenariotechnik
  - Umfassende Schadensdatenbank, die zeitnah aus internen und externen Quellen aktualisiert wird; sie beinhaltet tatsächliche, durch Zufall vermiedene sowie potenzielle unbeabsichtigte und beabsichtigte Vermögensschäden
  - Bewertung der laufenden Änderungen relevanter Gesetze, Richtlinien und Standards
  - Etablierung einer einheitlichen GRC-Systematisierung als Referenzsystem.

4.3 Bewertung des individuellen Handlungsbedarfs

Die Kompetenz der derzeitigen Beschaffungsorganisationen offenbart in Bezug auf ein GRC-Management in den meisten Bereichen noch kritische Defizite (siehe Abbildung 4).



Quelle: Caniu GRC – GRC Management Methodik
Abbildung 4: *GRC-Positionierungs-Profil*

Die Mehrzahl der Beschaffungsorganisationen weist in Bezug auf das GRC-Management ein durchschnittliches Profil auf. Stärken finden sich bei …

- der Einsicht in die Notwendigkeit interner Kontrollen und eines Risiko-Managements
- der Übernahme der vom Finanzbereich im Rahmen des übergreifenden Risiko- und Compliance Managements deligierten Pflichten
- der Lieferantenqualifzierung.

Synergie-Potenziale ergeben sich durch …

- Erweiterung des Risikobegriffs und gleichzeitige Fokussierung auf die Chancen in der strategischen Ausrichtung des Unternehmens
- Definition und Verankerung der GRC-Ziele in den Zielvereinbarungen („what you get is what you measure“) sowie die Erweiterung der oft eindimensionalen Performance-Messung,
- Qualifizierung der Mitarbeiter mit den erforderlichen GRC-Kompetenzen.

Die bislang verbreiteten (Best) Practices in der Beschaffung entheben nicht der Notwendigkeit eines integrierten GRC-Managements. Vielmehr offenbaren die meisten Unternehmen in

dieser Hinsicht einen erheblichen Handlungsbedarf, der in der Regel ein strukturiertes, abgestimmtes Vorgehen erforderlich macht. Wer sich dem pro-aktiv stellt, eröffnet sich in jedem Fall größere Zeitfenster als durch ein re-aktives, fristgerechtes Handeln nach internen und externen Prüfungen – oder gar Korruptions- und Betrugsfällen im eigenen Beschaffungsbereich.

5. Kritische Schritte der Umsetzung

Die erfolgreiche Etablierung eines effektiven und effizienten GRC-Managements ist ein komplexes und oft mit weit reichenden Veränderungen verbundenes Vorhaben. Hierbei sind vorrangig weniger technische als vielmehr organisatorische und kulturelle Aspekte zu beachten. Aus der Erfahrung von Einführungsprojekten und der operativen Erfahrung haben sich dafür folgende Schritte als äußerst effektiv erwiesen:

- frühe Etablierung konkreter GRC-Ziele
- GRC-Positionierung und projektbasiertes Umsetzungsprogramm
- klare Verantwortlichkeiten für GRC bezogene Aufgaben
- praxisnahes Training und Support
- kontinuierliche Verbesserung und „Learning from Experience“.

6. Fazit

Der Zuwachs an Verantwortung konfrontiert die Beschaffung zunehmend mit immer neuen und strengeren gesetzlichen Anforderungen und Richtlinien. Zugleich werden die bislang eher lasch gehandhabte Durchsetzung dieser Pflichten und ihre Prüfung zunehmend stringenter.

Vor diesem Hintergrund greifen ein punktuelles Management von Einzelrisiken und Compliance zu kurz. Denn so entstehen meist nur Overhead und wenig Wert.

Mit einem integrierten und auf die Steigerung des Unternehmenswertes fokussierten GRC-Management-Ansatz hingegen lassen sich, wie erste Beispiele zeigen, bislang verborgene Potenziale identifizieren und realisieren.

Dazu sollte immer in einem ersten Schritt der Handlungsbedarf unter den Aspekten Unternehmensstrategie und Wirtschaftlichkeit bewertet werden.

Der Erfolg der Umsetzung des GRC-Managements hängt dann, wie so oft, wesentlich von dem Buy-In der Geschäftsleitung und den Möglichkeiten der Governance und der Unternehmenskultur ab.

Fest steht: Nachdem die naheliegenden Best Practices umgesetzt sind, wird es für die meisten Beschaffungsorganisationen deutlich schwieriger, ihren erweiterten Verantwortungsbereich und die damit zusammenhängenden Komplexitäten zu beherrschen, als auch neue, zusätzliche Potenziale zur Erhöhung des Unternehmenswerts zu realisieren.

Dabei kann nur ein neuer integrierter Ansatz helfen.

Die Autoren

Lothar Goll

Direktor Einkauf und Materialwirtschaft

DPD GeoPost Deutschland GmbH & Co. KG
Wailandtstraße 1
63741 Aschaffenburg

Stephan Haupt

Gesellschafter

Caniu GRC Manangement GmbH
Rodenbacher Chaussee 7
63457 Hanau