

GRC

Governance, Risk Management und Compliance

Dr. Ulrich Kampffmeyer

P R O J E C T C O N S U L T

Unternehmensberatung Dr. Ulrich Kampffmeyer GmbH

Hamburg November 2007



GRC

Governance, Risk Management und Compliance

Von Dr. Ulrich Kampffmeyer

Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH

Einleitung

Die Compliance- und Risikomanagement-Landschaft unterliegt einem ständigen Wandel: zunehmend mehr Gesetze und Richtlinien – sowohl auf nationaler Ebene als auch länderübergreifend – fordern von Unternehmen Transparenz im Umgang mit Daten sowie die Trennung, Überwachung und Dokumentation von Geschäftsprozessen. Gleichzeitig findet eine Ausweitung der noch für die Papierwelt geschriebenen Gesetze auf die elektronische Welt statt: Die Aufbewahrungs- und Dokumentationspflichten für elektronische Geschäftsunterlagen nehmen zu. Mit dieser Entwicklung geht die Zunahme der Risiken, denen Unternehmen ausgesetzt sind, einher. Unternehmen stehen damit vor der großen Herausforderung, ihr Geschäft in Einklang mit den bestehenden und zukünftigen Regularien zu bringen und ein effektives Risikomanagement zu betreiben. Die Zusammenführung von Governance, Risikomanagement und Compliance, kurz GRC, ist ein wichtiger Schritt in der Bewältigung dieser Herausforderung. GRC - die Buchstaben werden auch gern in anderer Reihenfolge kombiniert – bietet dabei einen ganzheitlichen Ansatz, der das Entstehen von Insellösungen verhindert. Die Führung von Unternehmen, die Einhaltung gesetzlicher Vorschriften und die Bewertung von Risiken gehen dabei zunehmend Hand-in-Hand. Die Abgrenzung der Aufgaben und der unterschiedlichen Auffassungen des Umfangs führen dabei jedoch zu sehr verschiedenen Ansätzen.

GRC: Definitionen

Um Klarheit in das Verhältnis der drei zugrundeliegenden Akronymbestandteile von GRC zu bringen, ist es erforderlich sie zunächst einzeln zu definieren.

Governance

Governance für privatwirtschaftliche Unternehmen wird als Corporate Governance bezeichnet.

Corporate Governance umfasst die rechtlichen und institutionellen Rahmenbedingungen, auf nationaler und internationaler Ebene, die mittelbar oder unmittelbar Einfluss auf die Führungsentscheidungen eines Unternehmens und somit auf den Unternehmenserfolg haben. Der Ursprung für Corporate Governance liegt bereits in den 30er Jahren, als man sich verstärkt Gedanken über die Rechte der Aktionäre machte.



Corporate Governance ist dabei sehr vielschichtig und umfasst sowohl obligatorische als auch freiwillige Maßnahmen für die verantwortungsvolle Unternehmensführung: Compliance mit Gesetzen und Regelwerken (siehe nächster Abschnitt.), das Befolgen anerkannter Standards und Empfehlungen sowie das Entwickeln und Befolgen eigener Unternehmensleitlinien. Ein weiterer Aspekt der Corporate Governance ist die Entwicklung und Einrichtung von Leitungs- und Kontrollstrukturen.

Eine wesentliche Komponente von Corporate Governance ist die IT-Governance, die auf die Transparenz und Beherrschbarkeit der eingesetzten IT- und Kommunikationsinfrastruktur zielt. Besonders bei der technischen Unterstützung der Governance-Anforderungen spielt die IT-Governance eine wichtige Rolle.

Compliance

Compliance umfasst die Gesamtheit aller zumutbaren Maßnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Organisationsmitglieder und seiner Mitarbeiter im Hinblick auf alle gesetzlichen Ge- und Verbote begründen.

Auch wenn es Compliance-Anforderungen schon immer, auch im Ursprungsland des Begriffes - den USA - gab, so haben sie nach den Skandalen um ENRON und WorldCom eine brisante Qualität erhalten: neue, strafbewehrte Anforderungen zur Aufbewahrung geschäftsrelevanter elektronischer Informationen. In der Vergangenheit gab es schon immer eine Reihe von rechtlichen Anforderungen; so mussten z.B. Finanzbuchhaltungssoftware schon immer Compliance-Standards erfüllen. Mit dem steigendem Aufkommen und der wachsenden Bedeutung von E-Mails und E-Commerce gewann die Notwendigkeit der Dokumentation und elektronischen Archivierung von Geschäftsvorgängen immer mehr Bedeutung.

Im Folgenden wird für den Begriff Compliance nachstehende Übertragung verwendet:

„Übereinstimmung mit und Erfüllung von gesetzlichen und regulativen Vorgaben“

Compliance umfasst sowohl direkte gesetzliche Vorgaben wie auch regulative Branchenvorgaben und interne Richtlinien, die aus der Governance abgeleitet werden.

Risiko-Management

Die Risiken müssen erhoben, aufbereitet und bewertet werden. Maßnahmen zur Vermeidung der Risiken und zur Einhaltung der relevanten Compliance-Anforderungen sind zu treffen. Dabei obliegt es der Geschäftsführung bzw. dem Vorstand eines Unternehmens, die Verantwortung für den Umfang der Maßnahmen und deren Einhaltung zu übernehmen. Entsprechend Corporate Governance und Unternehmensgesetzen ist dies auch genau die Aufgabe der für die Geschäftstätigkeit verantwortlichen Personen und Gremien. Diese Verantwortung schließt heute bei Aktiengesellschaften auch den Aufsichtsrat ein.

Risiko-Management bezieht sich jedoch nicht nur auf die Bewertung von Compliance-Anforderungen, sondern vielmehr auf den planvollen Umgang mit allen Risiken, die ein Unternehmen betreffen.



Wie aus den Definitionen bereits deutlich wird, können die Bereiche Governance, Risiko Management und Compliance nicht losgelöst von einander betrachtet werden: Compliance-Anforderungen beinhalten Verpflichtungen zu Risikomanagement und der Einhaltung von Governance-Richtlinien; Risikomanagement beinhaltet die Bewertung von Compliance-Anforderungen; und Corporate Governance umfasst sowohl Compliance als auch Risiko Management. Lange jedoch wurden diese Aufgabenkomplexe als einzelne Säulen aufgefasst und auf verschiedene Bereiche und Rollen verteilt sowie in spezifischen Lösungen umgesetzt. GRC fordert nun die ganzheitliche Betrachtung und Umsetzung der Anforderungen und damit auch eine technische Infrastruktur, die die Implementierung und Überwachung von Prozessen, die Definition und Kontrolle von Risiken, sowie die Dokumentation und Archivierung von Geschäftsvorfällen ermöglicht.

GRC: internationale Normen, Standards, Gesetze und Regularien

Für GRC kommen auf verschiedenen Ebenen sehr unterschiedliche Gesetze, Richtlinien und Standards zur Geltung.

Für die Corporate Governance gelten international die „Principles of Corporate Governance“ der OECD aus dem Jahr 1984, die in 2004 aktualisiert wurden. Auf europäischer Ebene gibt es bisher nur eine lose Organisation. Die Europäische Kommission hat im Jahr 2004 ein European Corporate Governance Forum als Beratungsgremium eingerichtet, ohne jedoch bisher eine verbindliche Richtlinie herauszugeben. So gelten in Europa sehr unterschiedliche Maßstäbe: in einigen Ländern regeln die Corporate Governance Gesetze, in anderen Codes of Best Practice oder Selbstverpflichtungserklärungen. In Deutschland hat das Bundesministerium der Justiz im Jahr 2002 den Corporate-Governance-Kodex veröffentlicht. Dieser hat Auswirkungen auf die Unternehmensgesetze KonTraG und UMAG sowie auf das Handels- und Steuerrecht und auf den Verbraucherschutz. In Österreich gibt es den ÖCGK Österreichischen Corporate Governance Kodex, der im Jahr 2002 veröffentlicht wurde und sich an den internationalen Vorgaben orientiert. In der Schweiz gibt es nur einen freiwilligen Swiss Code of Best Practice aus dem Jahr 2002.

Für die IT-Governance kommen immer mehr Verfahrensmodelle und Werkzeuge wie COBIT, ITIL und andere in Gebrauch, die Transparenz und Überprüfbarkeit der ITK-Landschaft im Unternehmen ermöglichen sollen. Verbände wie die ISACA schaffen hier ein international gültiges Rahmenwerk, das einheitliche Kriterien und Vergleichbarkeit umsetzt. Jedoch sind die Aufwände für die Umsetzung nicht zu unterschätzen. Letztlich geht es auch hier um die Dokumentation von Lösungen und Prozessen.

Beim Thema Compliance geht es direkt um die Umsetzung von Anforderungen in Organisation und Technik. Auch hier geht es um Lösungen und Prozesse. Allein die Anzahl der Gesetze und Verordnungen in Deutschland, die Auswirkungen auf die Ausgestaltung von GRC-Lösungen haben, sind schier endlos. Zwei Aspekte sind dabei generell von Bedeutung: zum einen der Rechtscharakter elektronischer Information und zweitens die Nachvollziehbarkeit der Entstehungs-, Nutzungs- und Speicherprozesse der Information. In Deutschland sind BGB und ZPO maßgebliche Gesetze, die sich allgemein mit dem Rechtscharakter von Information beschäftigen.



HGB, AO, GAufZ, GoBS und GDPdU beschäftigen sich dagegen sehr konkret mit den Anforderungen, wie Information bereitgehalten werden muss. Ebenso wie beim Thema E-Mail-Archivierung gibt es hier sehr konkrete Vorgaben, die direkt in technischen Lösungen münden. Grundlage sind aber auch hier Vorgaben der Governance im Unternehmen und Regelwerke, Policies im Englischen, die den Umgang mit Information verbindlich machen. Hier greifen Governance und Compliance direkt ineinander. Führungs-, Organisations- und Technik-Aspekte lassen sich hier nicht mehr trennen. Da immer mehr Information originär elektronisch entsteht und ein Ausdruck in Papier nur eine mögliche Form der Repräsentation des originär elektronischen Inhalts darstellt, muss sich die gesamte Organisation des Unternehmens auf die elektronische Welt einlassen und Informationssysteme bei allen Governance- und Compliance-Fragen berücksichtigen. Man sollte sich auch in diesem Umfeld auf verschärfte Vorgaben einrichten, wie sie zum Beispiel in den USA mit dem Sarbanes-Oxley-Act, e-Discovery oder dem Patriot Act bereits gang-und-gäbe sind. Mit der sogenannten 8. Richtlinie wurde bereits eine Richtlinie der Europäischen Kommission verbindlich, die ähnlich wie der Sarbanes-Oxley-Act die Prüfung der Unternehmen regelt und damit auch automatisch eine Brücke zwischen Compliance- und Governance-Fragen schlägt.

Würde man alle nur denkbaren und eine spezifische Situation betreffenden Compliance-Anforderungen im Unternehmen vollständig umsetzen und durch technische Systeme unterstützen wollen, käme die Geschäftstätigkeit zum Erliegen. Risiko-Management ist daher eine wichtige Ergänzung von Corporate Governance und Compliance. Auch für das Risikomanagement gibt es vermehrt Normen und Standards, die vereinheitlichte Bewertungs- und Vorgehensmodelle bieten sollen, so z.B. die ISO-Norm 14971. Das Risikomanagement liefert sozusagen die Messlatte für den Aufwand, der für Governance- und Compliance-Management in einem Unternehmen betrieben werden kann.

Unter diesen Gesichtspunkten betrachtet ist ein ganzheitlicher Blick auf das Unternehmen gefordert. Die separate Betrachtung von Governance, IT-Governance, Compliance, Risk Management und Quality Management führt nicht zur geforderten Transparenz, Nachvollziehbarkeit und Durchgängigkeit. Abgesehen von den Anforderungen aus Dokumentationsicht ist hier auch ein wirtschaftlicher Faktor zu berücksichtigen – Governance, Compliance und Risikomanagement ermöglichen durch die geschaffene Transparenz auch die Einsparung von Kosten und ein wirtschaftlicheres Arbeiten. So können z.B. auch die erheblichen Kosten für die Umsetzung von Governance- und Compliance-Anforderungen ins Positive gewendet werden und zum wirtschaftlichen Erfolg des Unternehmens beitragen.

GRC: Lösungsaspekte

Betrachtet man die Umsetzung von GRC mit Unterstützung von informationstechnischen Lösungen, so stellt man zunächst fest, dass die relevanten Daten und Dokumente heute noch auf zahlreiche unterschiedliche Systeme verteilt sind. Strukturierte Daten liegen in CRM-, ERP-, Produktionsmanagement- oder Datawarehouse-Lösungen, unstrukturierte Informationen in E-Mail-, Archiv-, Dokumentenmanagement-, Collaborations- oder GIS-Lösungen. Abgesehen davon, dass GRC vorrangig eine organisatorische Aufgabe ist, bieten Enterprise Content Management Lösungen alle notwendigen Komponenten, um Informationen aus



unterschiedlichen Systemen zusammenzuführen, die Prozesse nachvollziehbar zu machen und die Informationen sicher und langfristig zu speichern. Grundlage für die Einhaltung von Compliance-Anforderungen und den Nachweis dieser Regel-Konformität ist die Dokumentation der Geschäftsvorgänge und die langfristige, sichere Aufbewahrung von Dokumenten und Korrespondenz. ECM, Enterprise Content Management, ist daher eine wichtige Basislösung zur Umsetzung von GRC. Dementsprechend sind die folgenden Komponenten von ECM-Systemen als Teil einer GRC-Lösung zu betrachten.

Records Management

Records Management oder ERM Electronic Records Management bezieht sich auf die Strukturierungs-, Verwaltungs- und Organisationskomponente zur Handhabung von Aufzeichnungen. ERM ist nicht mit elektronischer Archivierung deutscher Prägung gleichzusetzen, obwohl viele Ansätze sich hier wiederfinden.

Zu Records Management gehören z.B. die Abbildung von Aktenplänen und anderen strukturierten Verzeichnissen zur geordneten Ablage von Informationen, Thesaurus- oder kontrollierte Wortschatz-gestützte eindeutige Indizierung von Informationen, Verwaltung von Aufbewahrungsfristen und Vernichtungsfristen, Schutz von Informationen entsprechend ihren Eigenschaften, z.T. bis auf einzelnen Inhaltskomponenten in Dokumenten, und Nutzung international, branchenspezifisch oder zumindest unternehmensweit standardisierter Meta-Daten zur eindeutigen Identifizierung und Beschreibung der gespeicherten Informationen.

Records Management dient zur Verwaltung beliebiger aufbewahrungspflichtiger Unterlagen unabhängig vom Medium, elektronische wie auch papiergebundene Vorgänge.

E-Mail-Management

E-Mails enthalten geschäftsrelevante Information und sind als Geschäftsbriefe zu bewerten. Dementsprechend ist ihre Verwaltung und Aufbewahrung im Rahmen unternehmensweiter Lösungen von großer Bedeutung. Dabei sollten E-Mails im Zusammenhang mit anderen geschäftsrelevanten Aufzeichnungen erschlossen und verwaltet werden. Die große Herausforderung ist dabei die Identifikation aufbewahrungspflichtiger und aufbewahrungswürdiger E-Mails, insbesondere wenn Unternehmen die private Nutzung von E-Mails zulassen. Unterschieden wird zwischen vollständiger und selektiver Archivierung, sowie der regelbasierten und manuellen Archivierung. Wichtig ist, E-Mails nicht in isolierten Repositories außerhalb des geschäftlichen Kontexts aufzubewahren. Es empfiehlt sich die Integration in ein ECM-System.

Business-Process-Management

Prozess Design und Dokumentation sind eine weitere wichtige Basis für die Erfüllung von Compliance-Anforderungen. Eine vollständige Dokumentation der Geschäftsprozesse erleichtert die Identifikation der Regelungen, die das Unternehmen betreffen; und nur das Einhalten der definierten Prozesse kann die Regel-Konformität sicherstellen. Business Process Management (BPM) strebt die vollständige



Integration aller betroffenen Anwendungen in einem Unternehmen mit Kontrolle der Prozesse und Zusammenführung aller benötigten Informationen an. BPM greift über bisherige Workflow-Funktionen hinaus und bietet z.B. Prozess- und Datenkontrolle auf Server-Ebene, die Geschäftsprozesse begleitende Protokolle und Auditdokumentationen, EAI Enterprise Application Integration zur Verbindung verschiedener Anwendungen bis hin zu BI Business Intelligence mit hinterlegten Regelwerken, Integration von Information Warehouses und den Anwender bei seiner fachlichen Tätigkeit unterstützenden Hilfsprogrammen.

Elektronische Archivierung

Elektronische Archivierung steht für die unveränderbare, langzeitige Aufbewahrung elektronischer Information. Für die elektronische Archivierung werden in der Regel spezielle Archivsysteme eingesetzt. Der Begriff Elektronische Archivierung fasst unterschiedliche Komponenten zusammen, die im angloamerikanischen Sprachgebrauch separat als „Records Management“, „Storage“ und „Preservation“ bezeichnet werden.

Zweck eines elektronischen Archivsystems ist es, unabhängig von Quelle, Erzeuger und späterer Nutzung Information sicher aufzubewahren und datenbankgestützt auf Anforderung wieder bereit zu stellen. Archivsysteme sind daher Dienste, die allen Anwendungen zur Verfügung stehen, die Informationen erzeugen, die langfristig unverändert und sicher aufbewahrt werden müssen.

Hierfür bieten Archivsysteme datenbankgestützten Zugriff auf archivierte Daten und Dokumente, unveränderbare „revisionssichere“ Speicherung aller Informationen, Audittrails der Speicherung und Nutzung, Verwaltung sehr großer Informationsmengen auf sehr unterschiedlichen Speichern, Migrationskonzepte zur Verfügbarmhaltung von Daten, Konverter zur Erzeugung von Anzeige- und Archivformaten und andere spezielle Funktionen. Zunehmend werden Archivsysteme auch um Information-Lifecycle-Management-Konzepte ergänzt oder sie werden als nachgeordnete Dienste selbst Bestandteil des Lebenszyklusmanagements von Daten, Informationen, Dokumenten, Records, Content und Wissen.

GRC: Lösungsangebote

Für das Thema GRC gibt es sehr unterschiedliche Lösungsansätze. So bietet SAP im Rahmen seiner ERP-Produktsuite GRC-Komponenten an, die die Kontrolle über die Informationen innerhalb der SAP-Umgebung sicherstellen aber auch auf Informationen außerhalb von SAP zugreifen sollen. Die ERP-Anbieter haben in der Vergangenheit selbst sehr viel in die Entwicklung von GRC-Werkzeugen investiert oder Firmen aufgekauft.

Aber auch im Bereich der klassischen ECM-Anbieter spielt das Thema GRC eine immer wichtigere Rolle. So hat z.B. IBM in seiner „Tango“-Strategie für die Zusammenführung der IBM- und der FileNet-Produktlinie oberhalb der ECM-Dienste eine komplette GRC-Schicht eingezogen. Längst speichern ECM-Lösungen neben unstrukturierten Dokumenten auch Daten aus den operativen Anwendungen und bieten mit „föderierten Repositories“ einen einheitlichen, kontrollierten Zugriff auf alle Informationen. Hier wird GRC als die verbindende Schicht gesehen, die von Anfang-



bis-Ende alle Informationen über die Geschäftsprozesse, die Geschäftsprozesse und ihre Daten und Dokumente sowie die verbundenen Transaktionen und Audittrails verwaltet. Waren in der Vergangenheit bei den mittelständischen Anbietern vorrangig Speziallösungen zur Handhabung von Einzelproblemen aus dem GRC-Umfeld im Angebot – z.B. Lösungen zur Archivierung von GDPdU-Daten, SAP- oder Exchange-Datenauslagerung, E-Mail-Archive usw. -, so setzt sich auch hier der integrierende Ansatz von Universalarchiven mit einer übergreifenden Verwaltung aller Informationen und der Ergänzung um Business-Process-Management-Lösungen durch. Beispiele finden sich mit internationalen Anbietern wie OpenText oder EMC bis hin zu europäischen Firmen wie ELO Office, Saperion, Docuware, SER Solutions, d.velop, COI, Windream und vielen anderen. Interessant ist auch, dass Firmen aus anderen Marktsegmenten sich immer mehr in den regulatorischen Bereich, besonders das Records Management orientieren. Dies betrifft einerseits den Bereich der technischen und der Qualitätsmanagement-Dokumentation, aber auch die Schriftgutverwaltung im öffentlichen Sektor, bei Banken, in Versicherungen, für Energieversorger, Industrie – nahezu alle Branchen.

Ausblick

Da in Deutschland der Begriff Records Management noch nicht so eingeführt ist, wie sonst international, und der Begriff Compliance für viele wenig Aussagekraft hat, stehen wir in Deutschland immer noch am Anfang ganzheitlicher GRC-Konzepte und -Lösungen. Um mit der Entwicklung im Markt, die durch die Globalisierung sowie die immer rasanter werdende technische Innovation eine ungeahnte Beschleunigung erfährt, Schritthalten zu können, müssen sich die Unternehmen auf ihre Informations- und Kommunikationslösungen verlassen können. Diese im Griff zu halten, erfordert ganzheitliche Konzepte, die auch den Einsatz von Enterprise-Content-Management-Lösungen als Grundlage für eine effektive GRC-Umsetzung berücksichtigen.



Anschrift des Autors

PROJECT CONSULT GmbH, Büro Hamburg
Breitenfelder Str. 17
D-20251 Hamburg
Tel.: 040 / 460 762 20
Fax: 040 / 460 762 29
E-Mail: Presse@PROJECT-CONSULT.com
Web: www.PROJECT-CONSULT.com

Autorenrecht und CopyRight

Autor: Dr. Ulrich Kampffmeyer
PROJECT CONSULT Unternehmensberatung GmbH
Breitenfelder Str. 17
D-20251 Hamburg
Tel.: 040 / 460 762 20
Fax: 040 / 460 762 29
E-Mail: Presse@PROJECT-CONSULT.com
Web: www.PROJECT-CONSULT.com

© PROJECT CONSULT Unternehmensberatung GmbH 2007/2008. Alle Rechte vorbehalten

Der gesamte Inhalt ist, sofern nicht gesondert zitiert, ein Originaltext des Autors. Jeglicher Abdruck, auch auszugsweise oder als Zitat in anderen Veröffentlichungen, ist durch den Autor vorab zu genehmigen. Die Verwendung von Texten, Textteilen, grafischen oder bildlichen Elementen ohne Kenntlichmachung der Autorenschaft ist ein Verstoß gegen geltendes Urheberrecht. Belegexemplare, auch bei auszugsweiser Veröffentlichung oder Zitierung, sind unaufgefordert einzureichen.