# GRC
# Governance, Risk Management & Compliance

**von Dr. Ulrich Kampffmeyer**
Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH

## Vorwort

Kürzel wie GRC (Governance, Risk Management und Compliance) rufen beim deutschsprachigen Leser zunächst eine Reihe von Fragezeichen auf die Stirn. Einzeln besehen hat fast jeder die Begriffe einmal gehört: Governance im Zusammenhang mit Corporate Governance oder IT-Governance, Risk Management als Risikomanagement und auch den seit Jahren eingeführten Begriff Compliance. Neu ist die ganzheitliche Betrachtungsweise. Alle drei Begriffe stellen Komponenten einer grundsätzlichen Strategie dar, um größtmögliche Rechtssicherheit im geschäftlichen Handeln zu erreichen. Die Strategie beginnt auf der Geschäftsführungs- oder Vorstandsebene mit den Richtlinien zur Geschäftstätigkeit, dem Verhalten als ordentlicher Kaufmann. Sie erstreckt sich über die Erhebung und Bewertung von Risiken, die aus der Geschäftstätigkeit entstehen. Die Erfüllung der rechtlichen und regulativen Vorgaben stellt die operative Umsetzung der grundsätzlichen Strategie dar. Sie erstreckt sich von der Geschäftsleitung bis hinunter zum Sachbearbeiter, schließt Organisation und technische Systeme ein.

Das vorliegende Whitepaper soll einen Einstieg in diesen neuen Ansatz für Anwender in Deutschland, Österreich und der Schweiz bieten. Es kann keine erschöpfende Auskunft geben, da in jedem Unternehmen der Umgang mit Governance, Risk Management und Compliance unterschiedlich ist. Dies wird bereits durch die Geschäftstätigkeit, die Organisationsform, Aufstellung, unterschiedliche Märkte und relevante zu berücksichtigende Vorschriften bedingt. Es obliegt jedem Unternehmen, hier selbst sich seine Regularien zu setzen und geeignete Verfahren zur Erfüllung der Vorgaben umzusetzen. Dies ist keine einmalige Tätigkeit sondern ein ständiger Prozess. Mit geeigneter Software kann dieser Prozess unterstützt und nachvollziehbarer gemacht werden.

IBM ist international einer der führenden Anbieter von Lösungen für GRC Governance, Risk Management und Compliance. IBM-Lösungen unterstützen bereits seit Jahren Anwender auf allen Kontinenten, unterschiedlicher Größe und Geschäftstätigkeit, bei der Umsetzung von GRC-Strategien. Unser Unternehmen kann dabei für seine Erfahrungen auf drei Quellen zurückgreifen:

1) Durch zahlreiche Projekte in allen Branchen wurden organisatorische und technische Lösungen realisiert. Dabei wurden die rechtlichen Anforderungen nahezu aller Staaten weltweit berücksichtigt. Diese Projekte beinhalteten nicht

nur die Einführung von Archiv-, Dokumenten-Management- und Records-Management-Systeme zur Erfüllung von Compliance, sondern auch Datawarehouse-, Business-Intelligence-, IT-Governance- und Management-Informationssysteme, um den ganzheitlichen Ansatz von GRC umzusetzen. Diese Erfahrungen haben sich auch in den kontinuierlich weiterentwickelten Standardprodukten von IBM niedergeschlagen.

2) Für die Umsetzung von Lösungen bietet IBM ein weitgefasstes Produktportfolio. Diese Produkte sind für nahezu alle Betriebssystemumgebungen verfügbar und integrieren sich als Infrastruktur in die Informationslandschaft der Anwender. Hierzu gehören nicht nur die klassischen ECM Enterprise-Content-Management-Komponenten sondern auch Produkte für E-Discovery, Audit Trails, E-Mail-Management und Betriebssteuerung. IBM ist hier das einzige Unternehmen, das geeignete Software und Hardware kombiniert mit professionellen Dienstleistungen weltweit anbieten kann. Das Ziel von IBM ist hier, einfach einzusetzende Lösungskomponenten anzubieten, die Informationsinseln im Unternehmen vermeiden und die Transparenz des Informationsmanagements fördern.

3) IBM selbst unterliegt als international aufgestelltes IT- und Dienstleistungsunternehmen zahllosen Regularien unterschiedlicher Länder und Wirtschaftsräume. Diese reichen von grundsätzlichen GRC-Themen bis in die speziellen Bereiche der Produkthaftung, des Patentrechts usw. Die Angebote von IBM reflektieren daher nicht nur auf theoretischer oder Projekt-Basis das Thema GRC – IBM selbst lebt GRC. Dies ist eine weitere Motivation und Erfahrungsquelle, die IBM ihren Kunden zugänglich macht. GRC ist daher für IBM nicht irgendein neues „Hype-Thema“, das wieder vom Markt verschwindet, sondern GRC ist langfristig in Strategie und Produkten verankert.

Weltweit gibt es über 20.000 unterschiedliche Gesetze und Regularien, die die Dokumentation der Geschäftstätigkeit erforderlich machen. Je nach Standort und Tätigkeit wird jedoch jedes Unternehmen nur von einem Teil dieser Anforderungen direkt oder auch indirekt betroffen sein. Ziel von IBM ist es, Lösungen anzubieten, die generisch und konfigurierbar möglichst viele der Anforderungen zu erfüllen. Rechtliche Anforderungen ändern sich und ständig kommen neue hinzu. Die Welt des Rechts und der Rechtsprechung orientiert sich immer mehr an den Gegebenheiten der elektronischen Kommunikation und Informationsverarbeitung. Elektronische Informationen werden zur führenden Information, Ausdrucke auf Papier sind häufig nur noch eine Kopie eines elektronischen Originals. Mit diesen Veränderungen muss die Organisation der Unternehmen und die Aufbereitung von Informationen Schritt halten. Angesichts des exponentiellen Wachstums von elektronischer Information kommt der Verwaltung und Erschließung von Daten, Dokumenten, Content, Transaktionen, Prozessen und anderen Formen von Informationsobjekten eine existenzentscheidende Bedeutung zu. Softwaresysteme zur Unterstützung von GRC Governance, Risk Management und Compliance sind

ein wesentlicher Baustein solcher Lösungen. Auch wenn der wirtschaftliche Einsatz und die Steigerung der Effizienz im Unternehmen beim Einsatz von Systemen im Vordergrund steht, müssen diese Lösungen auch auf die Erfüllung der gesetzlichen wie unternehmensinternen Vorgaben ausgelegt sein. Die Strategie von IBM ist hier, Produkte anzubieten, die beide Aspekte unterstützen und die Dokumentation der Geschäftstätigkeit quasi nebenbei mit erledigen.

Software und Systeme werden so zu einer wichtigen Säule von GRC-Strategien, die durch automatisierte Verfahren menschliche Fehler vermeiden helfen und die Nachvollziehbarkeit der Geschäftstätigkeit sicherstellen. Am Anfang steht jedoch die GRC-Strategie, die jedes Unternehmen für sich entwickeln und umsetzen muss. Unser Whitepaper soll hierfür Anregung und Rahmen sein. Gern unterstützt Sie IBM bei Ihrer individuellen Umsetzung von GRC Governance, Risk Management und Compliance in Ihrem Unternehmen.

Stefan Pfeiffer
Market Manager Lotus EMEA

### GRC – Eine Einführung

Die Governance-, Compliance- und Risikomanagement-Landschaft unterliegt einem ständigen Wandel: Zunehmend mehr Gesetze und Richtlinien 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.

*Alle rechtlichen und gesetzlichen Vorgaben der Papierwelt gelten auch in der elektronischen Welt!*

*Die Anforderungen der IT-Welt sind jedoch häufig noch nicht oder nicht direkt enthalten und müssen daher adäquat abgeleitet werden.*

Unternehmen stehen 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 Umfanges führen dabei jedoch zu sehr verschiedenen Ansätzen.

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

## *Begriffsdefinitionen*

### Governance & Corporate Governance

Der Begriff Governance lässt sich zum Einen von dem französischen Begriff Gouvernance ableiten, der sich mit Herrschaft, Lenkung, Steuerung übersetzen lässt und zum Anderen von dem englischen Begriff für Regierung, Steuerung.

Für den Begriff Corporate Governance gibt es keine deutsche Direktübersetzung. Aus dem lateinischen Wortstamm lässt sich folgendes erkennen: "gubernator" bedeutet: Steuermann, "corporatio" bedeutet: Körperschaft. Wörtlich kann Corporate Governance also mit "körperschaftliche Steuerung" oder " Leitung einer Körperschaft bzw. einer Gesellschaft" übersetzt werden.

**Risk Management**

Risiko ist das italienische Wort für Wagnis, Gefahr. Risikomanagement umfasst also die Maßnahmen zur Erfassung, Bewertung und Steuerung der Risiken.

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 beziehungsweise dem Vorstand eines Unternehmens, die Verantwortung für den Umfang der Maßnahmen und deren Einhaltung zu übernehmen.

**Compliance**

Der Begriff Compliance kann aus dem Englischen mit Befolgung, Einhaltung oder Erfüllung bestimmter Anforderungen übersetzt werden.

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. Compliance bezieht sich dabei sowohl auf die Erfüllung externer rechtlicher Vorgaben als auch auf die Erfüllung interner regulativer Vorgaben.

## *GRC als ganzheitlicher Ansatz*

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 Arbeitsgebiete aufgefasst und auf verschiedene Bereiche und Rollen verteilt sowie in spezifischen Lösungen umgesetzt.


Unter diesen Gesichtspunkten betrachtet ist ein ganzheitlicher Blick auf das Unternehmen gefordert. Die separate Betrachtung von Governance, IT-Governance, Compliance und Information Management Compliance, Risk Management und Quality Management führt nicht zur geforderten Transparenz, Nachvollvollziehbarkeit und Durchgängigkeit. Für die Umsetzung in Prozessen und in der Organisation eines Unternehmens oder einer Verwaltung ist eine ganzheitliche Betrachtung erforderlich, bei der die Governance die Regeln und Richtlinien liefert, das Risiko Management diese bewertet und im Rahmen von Compliance die praktische, operative Umsetzung sichergestellt werden muss.

*GRC vereinigt die Disziplinen Corporate Governance, Risikomanagement und Compliance als durchgängiges Vorgehensmodell.*

Abgesehen von den Anforderungen aus Dokumentationssicht 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.

## Corporate 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. Konkret wurde aber der Begriff in England als verbindliche Richtlinie eingeführt. Der Cadbury Report mit dem Titel "Financial Aspects of Corporate Governance" ist der Bericht eines von Adrian Cadbury geleiteten Komitees, das Empfehlungen für die Gestaltung der Board-Besetzung und der Rechnungssysteme erarbeitet hat. Beides soll die Gefahren schlechter Corporate Governance abschwächen. Der Bericht wurde 1992 veröffentlicht und wurde in verschiedenem Ausmaß von der Europäischen Union, den Vereinigten Staaten, der Weltbank und anderen Institutionen bei der Gestaltung eigener Regelwerke übernommen.

*Der Begriff Governance bezeichnet Standards beziehungsweise spezielle Rahmenbedingungen für Strukturen und Prozesse der Führung, Verwaltung und Überwachung börsennotierter Unternehmen.*

Corporate Governance ist dabei sehr vielschichtig und umfasst sowohl obligatorische als auch freiwillige Maßnahmen für die verantwortungsvolle Unternehmensführung: Compliance mit Gesetzen und Regelwerken, 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. Für die Umsetzung 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.

## Corporate Governance International

Corporate Governance Vorgaben gibt es auf verschiedenen Ebenen. 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.

Jedes Land verfolgt eine etwas andere Strategie. In England liegen die Corporate Governance-Vorgaben als „Reports“ vor (Cadbury Report, 1992; Greenbury Report, 1995; Hampel Report, 1998; Turnbull Report, 2005). In Frankreich ist dagegen Corporate Governance direkt im LSF Loi de Sécurité Financière (2003) verankert. Die Bandbreite schwankt also von expliziten Gesetzen bis hin zu mehr oder weniger unverbindlichen Codes of Best Practice als Selbstverpflichtung. Auch in Deutschland, Österreich und der Schweiz existieren entsprechende Kodizes.

### Corporate Governance in Deutschland

2002 hat das Bundesministerium der Justiz den Corporate-Governance-Kodex veröffentlicht. Dieser Kodex wurde am 14.06. 2007 aktualisiert. Ihm liegen verschiedene Unternehmensgesetze und Verordnungen wie KonTraG und UMAG aber auch Handels- und Steuerrecht und Verbraucherschutz zu Grunde.

Der Kodex stellt wesentliche gesetzliche Vorschriften zur Leitung und Überwachung deutscher börsennotierter Gesellschaften dar und enthält international und national anerkannte Standards guter und verantwortungsvoller Unternehmensführung. Der Governance-Kodex soll das deutsche Corporate Governance System transparent und nachvollziehbar machen. Er will das Vertrauen der internationalen und nationalen Anleger, der Kunden, der Mitarbeiter und der Öffentlichkeit in die Leitung und Überwachung deutscher börsennotierter Gesellschaften fördern.

Der Kodex wird in der Regel einmal jährlich vor dem Hintergrund nationaler und internationaler Entwicklungen überprüft und bei Bedarf angepasst.

### Corporate Governance in Österreich

Der Österreichische Corporate Governance Kodex (ÖCGK) ist ein Regelwerk für die verantwortungsvolle Führung und Kontrolle von Unternehmen, das den internationalen Standards entspricht. Es richtet sich vor allem an österreichische, börsennotierte Aktiengesellschaften.

Der ÖCGK wurde am 1. Oktober 2002 der Öffentlichkeit präsentiert und erlangte dadurch seine Gültigkeit. Änderungen erfolgten im Februar 2005 und Januar 2006.

Der Österreichische Corporate Governance Kodex stellt einen wichtigen Baustein für die weitere Entwicklung und Belebung des österreichischen Kapitalmarktes dar. Durch die freiwilligen Selbstregulierungsmaßnahmen wird das Vertrauen der Aktionäre unter anderem durch mehr Transparenz und eine Qualitätsverbesserung im Zusammenwirken zwischen Aufsichtsrat, Vorstand und Aktionären gefördert.

### Corporate Governance in der Schweiz

Der Swiss Code of Best Practice (kurz Swiss Code) ist eine Empfehlung aus dem Jahre 2002 des Wirtschafts-Dachverbandes Economiesuisse der Schweiz an alle Aktiengesellschaften bezüglich Corporate Governance. Der Swiss Code of Best Practice richtet sich hauptsächlich an die Unternehmen, die an der Swiss Exchange notiert sind.

Der "Swiss Code" gibt Vorgaben vor allem zu folgenden Bereichen zu Verwaltungsrat und Geschäftsleitung: Aufgaben und Zusammensetzung des Verwaltungsrates, Arbeitsweise und Vorsitz des Verwaltungsrates, Umgang mit Interessenkonflikten und Wissensvorsprüngen, Personalunionen und Doppelsitze, Internes Kontrollsystem, Ausschüsse des Verwaltungsrates, etc.

## Risk Management

Entsprechend Corporate Governance und Unternehmensgesetzen ist das 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.

*Risk Management ist die systematische Erfassung, Bewertung und Steuerung der unterschiedlichsten Risiken im Unternehmen.*

## Risiko Management in Deutschland

Risiko Management ist die systematische Erfassung, Bewertung und Steuerung der unterschiedlichsten Risiken. Das Risk Management wird direkt aus der Corporate Governance und verschiedenen Gesetzen abgeleitet. Es ist ein systematisches Verfahren, das in verschiedensten Bereichen Anwendung findet, zum Beispiel bei Unternehmensrisiken, Kreditrisiken, Finanzanlagerisiken, Umweltrisiken, Versicherungstechnischen Risiken, Technische Risiken etc.

Potenzielle Risiken, die die Vermögens-, Finanz- und Ertragslage eines Unternehmens mittel- und langfristig gefährden könnten, werden zunächst mit Hilfe des proaktiven Risk Managements identifiziert, analysiert und bewertet. Das Ziel besteht in der Sicherung des Fortbestandes eines Unternehmens, der Absicherung der Unternehmensziele gegen störende Ereignisse und in der Steigerung des Unternehmenswertes. Für verschiedene Branchen gelten besondere Risikomanagement-Vorgaben.

## Risiko Management in Österreich

In Österreich existieren eine Reihe von Risiko-Management-Vorgaben für die öffentliche Verwaltung und die Privatwirtschaft. Das Österreichische Normungsinstitut (ON) empfiehlt in den im Jahr 2004 veröffentlichten ON-Regeln "Risikomanagement" die Integration des Risikomanagements in ein ganzheitliches Managementsystem. Außerdem ist im österreichischen Corporate Governance Kodex im Abschnitt VI Transparenz und Prüfung entsprechende Vorgaben für das Risikomanagement enthalten.

## Risiko Management in der Schweiz

In der Schweiz werden seit dem 01. Januar 2008 mit der Vorschrift des Art. 663b Ziff. 12 im revidierten Obligationenrecht von allen Unternehmen, die einen Anhang zur Jahresrechnung erstellen, Angaben über eine Risikobeurteilung verlangt. Der Verwaltungsrat ist ausdrücklich verpflichtet, eine Risikobeurteilung seiner Unternehmung durchzuführen und diese zu dokumentieren. Bei größeren Gesellschaften ist das Interne Kontrollsystem (IKS) zu dokumentieren.

### Compliance

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. Auch in Europa gab es entsprechende Skandale, ohne dass sich dies in ähnlich rigiden Maßnahmen wie den USA niedergeschlagen hätte.

In der Vergangenheit gab es schon immer eine Reihe von rechtlichen Anforderungen; so musste beispielsweise 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.

## *Compliance ist schwer ins Deutsche übersetzbar*

*Compliance ist die Übereinstimmung mit und die Erfüllung von gesetzlichen und regulativen Vorgaben.*

Betrachtet man die einzelnen Begriffe der deutschen Übertragung der Definition von Compliance „Übereinstimmung mit und Erfüllung von gesetzlichen und regulativen Vorgaben“, dann werden unterschiedliche Aspekte von Compliance-Anforderungen deutlich.

### „Übereinstimmung“

Zur Erreichung der „Übereinstimmung“ wird vorausgesetzt, dass es nachlesbare, definierte, offizielle Vorgaben gibt, die die Regeln enthalten, was zu tun ist. Hier ist „Übereinstimmung“ gefordert, ohne das die Regeln meistens eine technische Vorgabe enthalten, wie die Anforderung umzusetzen ist. Dies ist auch sinnvoll, da sich solche Vorgaben nicht an einer Technologie festmachen sollten, die in ein paar Jahren schon wieder obsolet ist. Die Übereinstimmung ist der „statische Aspekt“ von Compliance.

### „Erfüllung“

Der Begriff „Erfüllung“ impliziert zweierlei: Einmal, dass die Anforderungen in einer Lösung umgesetzt werden müssen, und zum Zweiten, dass dies ein Prozess ist, keine einmalige Aktion. Das Unternehmen oder die Organisation muss kontinuierlich für die Einhaltung der Vorgaben Sorge tragen. „Erfüllung“ geht dabei meistens über eine rein technische Lösung hinaus und beinhaltet auch organisatorische und Management-Aspekte. Die kontinuierliche Erfüllung ist der „dynamische Aspekt“ von Compliance.

**„Gesetzliche Vorgaben“**

Hierbei handelt es sich um Gesetze oder behördliche Verordnungen, die bestimmte Unternehmen, Organisationen oder Personen verpflichten, die jeweils aufgeführten Regelungen einzuhalten. Hier kann man sich auch nicht um die Erfüllung „drücken“, lediglich in Hinblick auf Auslegung, Umfang und Umsetzungsweise besteht Handlungsspielraum.

**„Regulative Vorgaben“**

Man unterschiedet zwischen „rechtlich“ und „regulativ“, da es eine Reihe von Vorgaben, die nicht direkt auf Gesetzen basieren wie z.B. Normen, Standards, Codes of Best Practice oder andere Vorgaben. Vielfach ergeben sich aus gesetzlichen Vorgaben für einen Anwendungsfall auch Auswirkungen und implizite Anforderungen für andere Fälle. Diese werden als „regulative Vorgaben“ abgegrenzt.

## *Unterschiedliche Auswirkungen*

Grundsätzlich gelten alle gesetzlichen, rechtlichen und regulativen Vorgaben auch in der elektronischen Welt. Häufig sind die Anforderungen der IT-Welt jedoch noch nicht oder nicht direkt enthalten und müssen daher adäquat abgeleitet werden.

**„Direkte Betroffenheit“**

Dies betrifft besonders Gesetze und gesetzesgleiche Verordnungen, die in jedem Fall eingehalten werden müssen. Hier kann man lediglich den Umfang und die Ausprägung interpretieren. Neben generell gültigen Vorgaben treten besondere, die auf die Branche oder Geschäftstätigkeit bezogen sind.

**„Indirekte Betroffenheit“**

Hier beginnt die große Grauzone, wo es darum geht, zunächst die für das Unternehmen oder die Organisation zutreffenden Regelungen zu ermitteln und zu bewerten. So betrifft beispielsweise Basel II nicht nur die Banken, sondern jedes kreditnehmende Unternehmen, da die Dokumentations- und Transparenzauflagen an die Kunden weitergegeben werden.

Für direkte und indirekte Auswirkungen gibt es zahlreiche Compliance-Regeln, die sowohl die herkömmliche Papierdokumentation wie auch die eingesetzte EDV betreffen.

Der bindende Charakter einer Vorgabe kann also sehr unterschiedlich sein. Nicht zuletzt Steckdosen, Lebensmittel, Flugzeuge, elektrische Geräte, Medikamente, Kindergärten, Bildschirme usw. müssen auch bestimmte Compliance-Anforderungen erfüllen, die sich beispielsweise in Prüfsiegeln niederschlagen.

## *Information Management Compliance*

Ein Abgleich der unterschiedlichen Anforderungen und Ausprägungen mit dem, was heute unter dem Schlagwort „Compliance“ bei informationstechnologischen Lösungen verstanden wird, zeigt aber große Unterschiede. Daher wird im Folgenden konkreter im Sinne von „IMC“, „Information Management Compliance“, gesprochen.

Information Management Compliance ist die Übertragung des Compliance-Begriffes auf die Handhabung von Informationen. Sie spielt eine besondere Bedeutung bei der Nutzung von Informationssystemen, die Compliance-Anforderungen unterliegen. Dies beschränkt sich nicht auf Dokumentenmanagement- und Archivsysteme sondern umfasst alle Informationssysteme im Unternehmen.

*Information Management Compliance darf nicht isoliert betrachtet werden.*

*Compliance muss Bestandteil der Corporate Governance des Unternehmens und ständiger Begleiter aller Prozesse werden.*

### Compliance-Vorgaben

Beim Thema Compliance geht es direkt um die Umsetzung von Anforderungen in Organisation und Technik. 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.

*Die Verantwortung für die Einhaltung von Compliance-Vorgaben liegt bei Vorständen, Aufsichtsräten und Geschäftsführern.*

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. Direktive 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.

## *Ausgewählte internationale Vorgaben*

### Basel II

Als gutes Beispiel für direkte und indirekte Auswirkungen der Gesetzgebung kann Basel II angeführt werden. Mit Basel II wird die Neugestaltung der Eigenkapitalvorschriften der Kreditinstitute bezeichnet. Finanzdienstleister müssen umso mehr Eigenkapital vorhalten, je höher das Risiko des Kreditnehmers ist. Auch wenn man in Bezug auf die Kreditvergabe und die Dokumentationspflichten hier zunächst nur an die Banken denkt, hat Basel II auch erhebliche Auswirkungen auf alle Unternehmen.

Ziel von Basel II ist es, die Stabilität des internationalen Finanzsystems zu erhöhen. Dazu sollen die Risiken im Kreditgeschäft besser erfasst und die Eigenkapitalvorsorge der Kreditinstitute risikogerechter ausgestaltet werden.

Basel II hat eine Vielzahl von Auflagen für die Dokumentation nach sich gezogen, die in einer elektronischen Welt nur mit Informationsmanagementlösungen vollzogen werden können.

## *Ausgewählte europäische Vorgaben*

Auf europäischer Ebene werden durch die Europäische Kommission zahlreiche Richtlinien entwickelt, die von den Mitgliedstaaten in nationales Recht überführt werden müssen. Bereits durch die Richtlinien zum E-Commerce und zur elektronischen Signatur ist eine Reihe von Anforderungen für Compliance entstanden. Der elektronische Geschäftsverkehr und die Umstellung der öffentlichen Verwaltung auf elektronisch unterstützte Verfahren werden weitere Compliance-Anforderungen nach sich ziehen.

Beispiele für europäische Richtlinien mit Gesetzescharakter, die Bedeutung für die Rechtskraft elektronischer Dokumente besitzen und Dokumentationspflichten nach sich ziehen, sind z.B.:

„E-Commerce“
E-Commerce-Richtlinie, die genau festlegt, was im elektronischen Geschäftsverkehr erlaubt und verboten ist. Hierzu gehören auch Nachweis- und Dokumentationspflichten.

„E-Signatur“

Basis für die Signaturgesetzgebung in der EU ist die EG-Richtlinie 1999/93/EG

Sie definiert die Vorgaben für die Regelungen elektronischer Signaturen, die durch die Mitgliedstaaten und die anderen Staaten des europäischen Wirtschaftsraumes in nationalen Gesetzen umgesetzt werden. Der Einsatz der elektronischen Signatur ersetzt unter bestimmten Voraussetzungen das Papier. Die elektronische Signatur ist daher Bestandteil zahlreicher Compliance-Regelungen.

Zahlreiche andere Richtlinien der Europäischen Kommission haben ebenfalls Compliance- und Dokumentationspflichten nach sich gezogen. Hierzu gehört auch Solvency II. Die größte Wirkung entwickeln jedoch zurzeit die sogenannte 8. Direktive und die europäische Dienstleistungsrichtlinie.

**Solvency II**

Solvency II ist ein Projekt der EU-Kommission zu einer grundlegenden Reform des Versicherungsaufsichtsrechts in Europa, vor allem der Solvabilitätsvorschriften für die Eigenmittelausstattung von Versicherungsunternehmen. Am 10. Juli 2007 hat die Europäische Kommission einen Vorschlag für eine Solvency II-Rahmenrichtlinie dem Europäischen Parlament und Rat vorgelegt. Eine Verabschiedung der Richtlinie ist für Ende 2008 geplant. Nach Erlass der entsprechenden Durchführungsbestimmungen wird Solvency II voraussichtlich von 2012 an national umgesetzt.

Wie bei Basel II wird ein 3-Säulen-Ansatz verfolgt, anders als bei der Bankenbranche stehen aber weniger die Einzelrisiken, als vielmehr ein ganzheitliches System zur Gesamtsolvabilität im Zentrum. Neben quantitativen (steht jederzeit ein ausreichendes Solvenzkapital zur Verfügung?) werden hier auch qualitative Aspekte (besteht ein adäquates Risikomanagementsystem im Unternehmen?) betrachtet.

### 8. Direktive

Die 8. Direktive (auch 8. EU-Richtlinie oder Euro-SOX genannt) ist in der europäischen Gemeinschaft bereits seit dem 29.06.2006 in Kraft und musste bis zum 29.06.2008 in nationales Recht umgesetzt werden. Sie enthält ausführliche Vorschriften über die Durchführung der Abschlussprüfung von Jahresabschlüssen sowie über damit verbundene Anforderungen an den beauftragten Abschlussprüfer. Die 8. Direktive verfolgt das Ziel, international einheitliche Regelungen für die Prüfung des Finanzabschlusses zu schaffen.

Die 8. Direktive betrifft in erster Linie also die Wirtschaftsprüfer sowie alle Unternehmen, die Finanzabschlüsse tätigen müssen. Aus ihr leiten sich eine Reihe von Offenlegungs- und Dokumentationsanforderungen ab. Die Nachvollziehbarkeit der Abschlüsse ist eine wesentliche Voraussetzung, die geordnete Ablagen mit vollständigen und inhaltlich richtigen Dokumentationen voraussetzt.

### Dienstleistungsrichtlinie

Die EU-Dienstleistungsrichtlinie, die bis Ende 2009 in nationale Gesetzgebung umzusetzen ist, soll die Zulassung von Dienstleistungserbringern in der EU vereinfachen. Die Dienstleistungsrichtlinie hat den Abbau von bürokratischen Hindernissen und zwischenstaatlichen Hemmnissen sowie die Förderung des grenzüberschreitenden Handels mit Dienstleistungen zum Ziel. Alle Verfahren und Formalitäten müssen zukünftig elektronisch durchgeführt werden können. Dementsprechend sind elektronische Informationsangebote, die Möglichkeit elektronischer Kommunikation zwischen Dienstleistern und Ansprechpartnern oder zuständigen Stellen gefordert, aber auch die ganzheitlich elektronische Abwicklung von kompletten Verwaltungsverfahren. Ein weiterer bedeutender Bestandteil der Forderungen der Richtlinie ist auch der Datenaustausch zwischen den Verwaltungen der europäischen Staaten.

Ausdrücklich hat die EU Kommission in dem zugehörigen Handbuch deutlich gemacht, dass die Richtlinie nicht mit einfachen Mitteln der elektronischen Kommunikation realisiert werden soll, wie z.B. über Internetportale oder E-Mail, vielmehr ist eine integrierte Entwicklung IT-gestützter Kommunikation zwischen den öffentlichen Verwaltungen und deren Zielgruppen gewünscht. Verwaltungsverfahren müssen also vollständig durch Online-Interaktionen oder gar -Transaktionen unterstützt werden und ausländischen wie auch einheimischen Dienstleistungsanbietern zugänglich sein. Erstmals ist also ein rechtlicher Zwang zur Realisierung von e-Government-Anwendungen gegeben. Als IT-Basisdienste wurden folgende Komponenten identifiziert: Elektronischer Zugang, Portale,

Wissensmanagement, Verwaltungsnetze, Elektronische Identifizierung, e-Signatur, Formularservice, Online-Zahlverfahren, Verschlüsselung, Dokumentenmanagement und Dokumentensafe. Vor dem Hintergrund der Behörden- und Länderübergreifenden Verwaltungsprozesse ist die Festlegung von nationalen und EU-weiten Standards eine der Kernvoraussetzungen.

## *Ausgewählte Vorgaben aus den USA*

In den USA gab es schon sehr lange Compliance-Anforderungen an Softwaresysteme und die Dokumentation von Geschäftsprozessen. Am bekanntesten und am engsten mit dem Begriff Compliance ist jedoch der Sarbanes-Oxley Act verknüpft.

### Sarbanes-Oxley Act

Durch die Skandale um ENRON, WorldCom und einige andere Unternehmen rückte das Thema Compliance in den Mittelpunkt des allgemeinen Interesses. Anlass waren „geschönte“ Prüfungen von Wirtschaftsprüfern und die Geschäftsberichte der Unternehmen. E-Mail wurde dabei als eine der möglichen Nachweisquellen für ungesetzliches Handeln entdeckt. Dies führte im Jahr 2002 zum Sarbanes-Oxley Act, allgemein SOA oder SOX abgekürzt. Typisch amerikanisch wurde es nach den beiden Leitern der Kommission benannt, die das Gesetz entworfen hat. Das Gesetz findet Anwendung für alle Unternehmen, die an der New York Stock Exchange gelistet sind.

SOX hat die Aufgabe, die Transparenz und Nachvollziehbarkeit in den Unternehmen bei Prüfungen durch die SEC, Securities und Exchange Commission, zu verbessern.

Unternehmen werden verpflichtet, u. a. ein internes Kontrollsystem für die Rechnungslegung zu unterhalten, die Wirksamkeit der Systeme zu beurteilen und die Richtigkeit der Jahres- und Quartalsberichte beglaubigen zu lassen.

SOX hat in den USA besonders auf Grund von Abschnitt 802 Bedeutung erlangt, weil hier empfindliche Strafen in der Strafgesetzgebung verankert worden sind. Die Zerstörung oder Veränderung von aufbewahrungspflichtigen Unterlagen kann mit bis zu 20 Jahren Gefängnis bestraft werden.

Besonders die Wirtschaftsprüfer legen in ihrer Beratung nunmehr sehr viel Wert auf Compliance, da im Rahmen der Skandale große, namhafte Wirtschaftsberatungsfirmen wie Arthur Andersen vom Markt verschwanden.

### e-Discovery

Die in den USA am 1. Dezember 2006 in Kraft getretenen Änderungen der FRCP Federal Rules of Civil Procedure können als signifikanter Wendepunkt von den herkömmlichen papierbasierten hin zu elektronischen Beweisführungsregeln

gesehen werden. Die wachsende Bedeutung von elektronisch gespeicherten Daten wurde somit auch durch den obersten Gerichtshof unterstrichen.

Electronic discovery, auch e-discovery oder eDiscovery, bezieht sich dabei auf jeden Prozess bei dem elektronische Daten abgefragt, gefunden, gesichert und gesucht werden, mit dem Ziel, sie bei einem Gerichtsverfahren zu verwenden. Dabei können sämtliche Daten, wie z.B. Texte, Bilder, Datenbanken, Audio-Dateien, Animationen, Webseiten und Programme als Beweis dienen. Die wertvollsten Quellen für strafrechtliche oder zivile Gerichtsverfahren stellen aber oft E-Mails dar.

Nachdem mit Sarbanes-Oxley bereits die elektronische Information vor Gericht aufgewertet worden war schafft eDiscovery nun die rechtliche Grundlage für die Anerkennung elektronsicher Informationen in Gerichtsverfahren. Alle Formen von elektronischen Informationen, nicht nur als Record definierte Dokumente, können als Beweismittel vorgebracht werden. Anders als in Europa und besonders in Deutschland spielt die elektronische Signatur dabei keine Rolle. Bei der Ermittlung gilt das als gültig, was von den ermittelnden Behörden vorgefunden wurde. Bei der Beweissicherung galten bisher nur Papierdokumente als sicherer Nachweis. Durch die Möglichkeiten der elektronischen Recherche ändert sich dies.

eDiscovery wird nicht nur die sichere, unveränderbare Speicherung von Informationen fördern sondern mehr noch den Schutz des Zugriffs und andere Sicherheitsaspekte. Policies zur kontrollierten Entsorgung von Information werden dabei zunehmend wichtiger.

Es sind aber nicht allein SOX und FRCP, die den Druck in bezug auf umfassende Dokumentationsanforderungen im Umfeld der Steuerprüfung und Steuerfahndung erhöht haben.

Viele dieser Regelwerke beziehen sich auf die neu gefassten FSG, Federal Sentencing Guidelines, von 2002, so dass Verstöße mit erheblichen Strafen belegt werden können.

Gesetze und Regularien in den USA haben auch Auswirkungen auf Unternehmen im Ausland, wenn sie Tochtergesellschaften oder Muttergesellschaften amerikanischer Unternehmen sind, oder bestimmte Geschäfte in den USA abwickeln.

**SEC**

Die United States Securities and Exchange Commission (SEC) sind für die Kontrolle des Wertpapierhandels in den Vereinigten Staaten zuständig. Die SEC wurde als Reaktion auf den Börsenkrach von 1929 im Jahre 1934 durch den Securities Exchange Act gegründet, um eine staatliche Aufsicht über die bis dato unkontrolliert ablaufenden Wertpapiergeschäfte zu schaffen. Ihre Aufgaben sind die Überprüfung des Handels auf Recht- und Ordnungsmäßigkeit und der Einhaltung börsenrechtlicher Anordnungen. Zur Erfüllung dieser Aufgaben wurden ihr umfangreiche legislative, exekutive sowie judikative Kompetenzen eingeräumt, so

dass sie manchmal auch als "Vierte Gewalt" bezeichnet wird. Alle Unternehmen, die den amerikanischen Kapitalmarkt nutzen möchten, müssen sich bei der SEC registrieren lassen. Nur wenn die SEC ihr Einverständnis gibt, kann ein Unternehmen sich an der New York Stock Exchange listen lassen. Die SEC stellt sicher, dass die Unternehmen Informationen, die für die Anleger wichtig sein könnten, wie zum Beispiel Informationen über die finanzielle Situation des Unternehmens, veröffentlichen.

## *Ausgewählte Vorgaben aus Deutschland*

In Deutschland wird der Begriff „Compliance“ zwar noch selten verwendet, doch die Anforderungen gibt es schon längst. 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. Auch in Deutschland werden die Gesetze, wie BGB, ZPO oder HGB, immer mehr den Anforderungen der Informationsgesellschaft angepasst sowie Richtlinien der Europäischen Kommission in nationales Recht übertragen. In diesem Umfeld kommt der elektronischen Signatur eine besondere Bedeutung zu.

### Elektronische Signatur

Der Einsatz der elektronischen Signatur findet sich inzwischen in nahezu allen jüngeren Gesetzen. So z.B. auch bei der elektronischen Rechnung. Zum Vorsteuerabzug berechtigen den Empfänger nach § 14 Abs. 4 Satz 2 UStG nur elektronisch signierte Rechnungen. Da die elektronische Rechnung das Original darstellt, ist es auch elektronisch aufzubewahren. Hier greifen die verschiedenen neuen Gesetze und Regelungen ineinander. Das Signaturgesetz und die Änderungen von BGB Bürgerlichem Gesetzbuch und ZPO Zivilprozessordnung zur Verankerung der elektronischen Signatur finden ihren Widerhall in der Handels- und Steuergesetzgebung. Aktuelle Beispiele sind das EHUG und die Erweiterung des Anwendungsbereiches der GDPdU durch aktuelle Gerichtsurteile. In eine ähnliche Kerbe wie die GDPdU schlägt auch das Gesetz zu den Dokumentationspflichten bei Verrechnungspreisen die Gewinnabgrenzungsaufzeichnungsverordnung (GAUFZ).

### EHUG & E-Mails

Das bundesweite Elektronische Handels- und Genossenschaftsregister (EHUG), das am 1. Januar 2007 in Kraft getreten ist, stellt eine digitale Version des Handelsregisters dar. Kapitalgesellschaften sind verpflichtet, ihre Abschlüsse beim

elektronischen Bundesanzeiger einzureichen. Verstöße gegen die Offenlegungspflicht werden mit bis zu 25.000 Euro von den Verwaltungsbehörden, welche vom elektronischen Bundesanzeiger informiert werden, geahndet.

Das EHUG hat eine Reihe von Änderungen auch in anderen Gesetzen wie z.B. für GmbHs und AGs nach sich gezogen. Eine Regelung betrifft die Angabe der kompletten Firmierungs- und Verantwortungsangaben in der Signatur von E-Mails. Was längst schon galt wird hierdurch jetzt jedem deutlich gemacht: E-Mails sind Geschäftsbriefe und sind dementsprechend aufzubewahren.

Dabei wird häufig übersehen, dass E-Mails in einen Geschäftszusammenhang gehören und nicht isoliert archiviert werden sollten. Sie müssen zusammen mit anderen Dokumenten in Kunden-, Sach-, Projekt- oder anderen Akten gemeinsam verwaltet werden, damit die Vollständigkeit und Nachvollziehbarkeit des Geschäftsganges gewährleistet ist. Da jeder Mitarbeiter im Unternehmen Empfänger wie Versender von geschäftsrelevanten E-Mails sein kann, ist jedwede technische Lösung durch organisatorische Maßnahmen zu unterfüttern.

**GDPDU**

Nach den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) sind alle steuerlich relevanten Daten auswertbar über den Zeitraum der Aufbewahrungsfristen nach HGB auswertbar aufzubewahren und für Prüfungen zugänglich zu machen.

Die GDPdU sind eine Verordnung, die auf den Änderungen im Steueränderungsgesetz und HGB Abgabenordnung, §§ 146, 147 und 200, basiert. Sie stellen eine Richtlinie für das Vorgehen der Finanzbehörden bei Außenprüfungen dar. Die Unternehmen müssen sicherstellen, dass alle steuerrelevanten Daten identifiziert, unverändert und vollständig und über einen Zeitraum von 10 Jahren aufbewahrt werden. Die originalen Daten müssen vollständig, richtig und auswertbar entweder in den sie erzeugenden Systemen vorgehalten oder aber in elektronische Archive ausgelagert werden. Auch bei den GDPdU spielen inzwischen Dokumente und E-Mails neben den Daten aus ERP- und Buchhaltungssystemen eine zunehmend wichtigere Rolle.

Bereits in einer Reihe von Verfahren vor Finanzgerichten war die Auslegung der GDPdU ein Thema. Während frühere Urteile der Finanzgerichte Rheinland-Pfalz und Hamburg aus dem Jahr 2006 das Recht auf Datenzugriff noch an vielen Stellen eingeschränkt und damit den Steuerpflichtigen unterstützt haben, weisen die Urteile der Düsseldorfer Finanzrichter nun in eine andere Richtung. Beide Entscheidungen vom 5. Februar 2007 beschäftigen sich im Kern mit der Reichweite des Datenzugriffs, also mit dem Umfang, welcher einer digitalen Betriebsprüfung zu Grunde zu legen ist und interpretieren diesen in einer Art, welche über das bisherige Verständnis von Literatur und Verwaltung hinausgeht. Dazu haben die Richter

teilweise eigenständige Definition von GDPdU-Begrifflichkeiten vorgenommen und damit neue Diskussionspunkte eröffnet.

Die Finanzbehörde darf im Rahmen des steuerlichen Datenzugriffs auch auf solche Konten der handelsrechtlichen Finanzbuchhaltung zugreifen, auf denen steuerlich nicht abzugsfähige Betriebsausgaben verbucht werden. Auf der Grundlage des § 147 Abs. 1 i. V. m. Abs. 6 AO darf die Finanzverwaltung für Zwecke der steuerlichen Außenprüfung ausschließlich auf Daten zugreifen, die für die Besteuerung von Bedeutung sind. Die vom Datenzugriff betroffenen Unternehmen sind deshalb seit jeher darauf bedacht, das digitale Suchfeld des Betriebsprüfers auf solche Datenbestände zu begrenzen, die vom Sinn und Zweck des Rechts auf Datenzugriff gedeckt sind. Das Finanzgericht Düsseldorf gab der Auffassung des Finanzamts Recht und sah keine ernstlichen Zweifel an der Rechtmäßigkeit des Datenzugriffs auf die ursprünglich gesperrten Konten. Bei den fraglichen digitalen Kontoaufzeichnungen handele es sich um „Bücher“ i.S.d. § 147 Abs. 1 Nr. 1 AO, die – anknüpfend an das Handelsrecht – die Funktion erfüllen, für einen Kaufmann seine Handelsgeschäfte und die Lage seines Unternehmens zu dokumentieren. Die im Rahmen der GDPdU geforderte steuerliche Relevanz kann nicht mit der vom betroffenen Unternehmen angeführten steuerlichen Auswirkung gleichgesetzt werden. Dabei habe sich die eigentliche Steuerrelevanz stets auch daran zu orientieren, inwieweit die in Frage kommenden Unterlagen einen Bezug zur Buchführung aufwiesen und mithin zu deren Verständnis erforderlich seien.

Werden Eingangsbelege beim Steuerpflichtigen gescannt, gespeichert und die Originale anschließend vernichtet, so erstreckt sich das Zugriffsrecht im Rahmen der elektronischen Steuerprüfung auch auf derart erzeugte Datenbestände. Der Steuerpflichtige muss diese Datenbestände so organisieren, dass bei einer zulässigen Einsichtnahme keine geschützten Bereiche des Unternehmens tangiert werden. Der EDV-Zugriff der Finanzverwaltung bezieht sich grundsätzlich auf solche Datenbestände, die originär bereits in elektronischer Form vorliegen. Dies schließt eine Verpflichtung zum Einscannen oder Digitalisieren von Papierdokumenten aus. In Bezug auf den viel diskutierten Umfang einer digitalen Betriebsprüfung stellt sich jedoch vermehrt die Frage, inwieweit digitalisierte Eingangsbelege, deren Papieroriginal vernichtet wurde, dem Betriebsprüfer auch in digitaler Form zur Verfügung zu stellen sind. Das Finanzgericht Düsseldorf gestand dem Finanzamt das Recht zu, auf die fraglichen Belege aus dem System des Unternehmens heraus zuzugreifen und diese am Bildschirm einzusehen. Die Rechtsgrundlage hierfür ergibt sich nach Auffassung der Richter bereits aus § 147 Abs. 6 Satz 1 AO.

Während die bisherige Rechtsprechung eher in Richtung Unternehmensseite tendierte, verschaffen die beiden nun vorliegenden vorläufigen Entscheidungen aus Düsseldorf der Finanzverwaltung einen deutlichen Rückenwind. Die Unternehmen sollten insbesondere das Urteil betreffend die digitalisierten Originalbelege in ihre künftige GDPdU-Strategie einbeziehen und einen adäquaten Datenzugriff nebst Trennung in steuerlich relevante und irrelevante Unterlagen einplanen. Was man in diesem Zusammenhang nicht vergessen sollte, ist das derzeit häufig bemühte

Thema der Verfahrensdokumentation. In dem Maße, wie der Außenprüfer selbst solche Systeme für den Z1- und Z2-Zugriff benutzt, wird der Nachweis von ordnungsgemäßer Verarbeitung, Nutzung und Betrieb immer wichtiger.

Mit dem Jahressteuergesetz 2009 erhielten die GDPdU ein „Preisschild“; das Verzögerungsgeld. Kommt ein steuerpflichtiges Unternehmen der Bereitstellung der geforderten Daten und Informationen nicht zeitgerecht nach, können die Finanzbehörden eine Verzögerungsgeld zwischen mindestens 2.500 und 250.000 € verhängen. Damit wird die Bedeutung der GDPdU unterstrichen, die seit 2002 Gültigkeit hat. Die Schonfrist ist vorbei, wie auch die oben aufgeführten Urteile von Finanzgerichten zeigen.

### GoBS und GoBIT

In den GoBS, Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme, wird die Behandlung aufbewahrungspflichtiger Daten und Belege in elektronischen Buchführungssystemen sowie in revisionssicheren Dokumentenmanagement- und Archivsystemen geregelt. Die GoBS behandeln dabei auch Verfahrenstechniken wie Scannen und Datenübernahme. Ein wesentlicher Kernpunkt ist das so genannte Interne Kontrollsystem (IKS). Aus HGB, AO und GoBS leiten sich auch die grundsätzlichen Anforderungen an die Dokumentation und Aufbewahrung ab.

*Vorgaben für Compliance*

- *Ordnungsmäßigkeit*
- *Vollständigkeit*
- *Sicherheit des Gesamtverfahrens*
- *Schutz vor Veränderung und Verfälschung*
- *Sicherung vor Verlust*
- *Nutzung nur durch Berechtigte*
- *Einhaltung der Aufbewahrungsfristen*
- *Dokumentation des Verfahrens*
- *Nachvollziehbarkeit*
- *Prüfbarkeit*

Die Anforderungen an eine Verfahrensdokumentation sind ebenfalls in den GoBS niedergelegt. Sie stellen quasi eine Übertragung der Anforderungen, die ursprünglich für eine papiergebundene Dokumentation gedacht waren, in die elektronische Welt dar.

Dokumentationspflichten ergeben sich jedoch nicht nur für den handelsrechtlichen und steuerrechtlichen Bereich, sondern gelten auch alle anderen Anwendungsgebiete, die gesetzlich oder regulativ betroffen sind. Die oben

aufgeführten Grundsätze aus dem Handelsrecht gelten so im Prinzip für alle Compliance-relevanten Anforderungen.

Zukünftig sollen die GoBS, die bereits aus dem Jahr 1995 stammen, durch die GoBIT, Grundsätze ordnungsmäßiger Buchführung beim IT-Einsatz, abgelöst werden. In den GoBIT, mit denen im Jahr 2010 zu rechnen ist, werden auch Widersprüche aufgelöst, die sich durch jüngere Verordnungen und die technologische Weiterentwicklung ergeben haben. Entwickelt wurden die GoBIT von einer Arbeitsgruppe der AWV Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. in Zusammenarbeit mit Verwaltungsexperten, IT-Spezialisten, Wirtschaftsprüfern und Mitarbeitern der Finanzverwaltung.

## *Ausgewählte Vorgaben aus Österreich*

In Österreich sieht die Situation nicht viel anders aus als in Deutschland. Die Unterschiede liegen nur im Detail. Dies ist darauf zurückzuführen, dass die wesentlichen Compliance-Anforderungen auf den europäischen Richtlinien basieren. Auch in Österreich ist analog zum BGB in Deutschland die elektronische Signatur verankert, auch Österreich kennt im Handelsrecht und in der Abgabenordnung ähnliche Bestimmungen wie in Deutschland. Dies gilt z.B. für die Aufbewahrung von elektronischen Informationen in Bezug auf Vollständigkeit, Inhaltsgleichheit, Geordnetheit und Urschriftstreue. Auch wenn die Bereithaltung von Daten zur steuerlichen Prüfung in Österreich in Listenform ausreichend erscheint, ist die Forderung der Auswertbarkeit die Gleiche. Zur Vermeidung des Umsatzsteuerbetruges finden sich natürlich auch die Regelungen zur elektronischen Rechnung wieder.

### Unternehmensgesetzbuch

Im Jahr 2007 wurde das UGB Unternehmensgesetzbuch in Kraft gesetzt, dass das bisherige österreichische HGB Handelsgesetzbuch ablöst. Aus dem neuen UGB ergeben sich zahlreiche Informations- und Dokumentationspflichten Unter der Überschrift „Geschäftspapiere und Bestellscheine“ werden die Mindestangaben festgelegt, die für Geschäftsbriefe und ähnliche Dokumente gelten. Es müssen die Firma, die Rechtsform und der Sitz sowie auch Firmenbuchnummer und Gerichtsstand angegeben werden. Die neuen Bestimmungen gelten nicht mehr nur für Geschäftspapiere und Bestellscheine, sondern in Ergänzung zu den Bestimmungen des MedG Mediengesetzes auch für E-Mails und Webseiten.

### Grundsätze ordnungsmäßiger Compliance

Seit Ende 2007 gibt es in Österreich die GoC „Grundsätze ordnungsmäßiger Compliance“, die vom Arbeitskreis Compliance der Bundessparte Banken und Versicherungen bei der Wirtschaftskammer Österreich erarbeitet wurden. Die Grundsätze richten sich an diejenigen österreichischen Kreditinstitute, die Geschäfte und Dienstleistungen im Zusammenhang mit Finanzinstrumenten durchführen. Sie

wurden u.a. mit dem Ziel entwickelt, aufgrund der großen Anzahl von gesetzlichen Regelungen eine Klarstellung der Verhaltenspflichten zu verfassen und somit auch dem Schutz der Mitarbeiter zu dienen. Die in zehn Kapitel unterteilten Grundsätze behandeln zunächst die Definition, Zwecksetzung sowie die Zielsetzung von Compliance. Gemäß den Grundsätzen ist Compliance ein „Organisationskonzept, dessen Ziel es ist, ein von Fairness, Solidarität und Vertrauen getragenes Verhältnis der Informationssymmetrie zwischen den Kunden, dem Kreditinstitut und den Mitarbeitern zu erreichen, Interessenkonflikte zu bewältigen und die Einhaltung geltender Gesetze und sonstiger (z.B. bankinterner) Regelungen sicherzustellen“. Anschließend werden noch die Punkte Managementverantwortung, Unabhängigkeit, Stellung im Unternehmen, Ausstattung/Ressourcen, Aufgabenbereiche, Konzept der Vertraulichkeitsbereiche und das Outsourcing von Geschäftsfeldern behandelt.

## *Ausgewählte Vorgaben aus der Schweiz*

Selbst die Schweiz hat als nicht EU-Mitglied inzwischen die wesentlichen Gesetze und Verordnungen an die europäischen Vorgaben schrittweise angeglichen. Dies zeigt sich z.B. im Obligationenrecht in den Bestimmungen über die Buchführung OR Art. 957ff, die die Aufbewahrung von Geschäftskorrespondenz, der Bücher und der Buchungsbelege in elektronischer Form regeln.

### GeBüV Geschäftsbücherverordnung

Ein wesentliches Dokument ist die GeBüV34), Geschäftsbücherverordnung bzw. die Verordnung über die Führung und Aufbewahrung der Geschäftsbücher. Die GeBüV legt fest, wie die Geschäftsunterlagen geführt und aufbewahrt werden müssen. Sie beinhaltet die Grundsätze der ordnungsgemäßen Buchführung sowie die Grundsätze der ordnungsgemäßen Datenverarbeitung bei elektronisch oder in vergleichbarer Weise geführten Büchern. Die GeBüV hält die Anforderungen an Integrität, zulässige unveränderbare Speichermedien und andere Spezifikationen mit Compliance-Relevanz fest.

Weitere Gesetze regeln sehr dediziert und mit Hinweisen auf geeignete Speichertechnologien und elektronische Signatur die Dokumentations- und Aufbewahrungspflichten auch außerhalb des Handelsrechtes.

## *Beispielhafte Branchenanforderungen*

Neben den Richtlinien, die für alle Unternehmen, Organisationen, Behörden und Personen gleichermaßen gelten, gibt es zahlreiche spezielle Regelungen für bestimmte Branchen, die öffentliche Verwaltung und Geschäftstätigkeitsgebiete. Hierbei gibt es internationale wie auch nationale Regelungen.

### Pharma

So ist die FDA Food and Drug Administration aus den USA, mit ihren bindenden Regularien für die Herstellung von Lebensmitteln, Pharmazeutika und Medikamenten auch über die Grenzen der Vereinigten Staaten zu beachten. Bei der Beantragung eines neuen Medikamentes, mit Vorlage von allen Testnachweisen und Produktionsverfahren, hat sich die Anschaffung eines Dokumentenmanagementsystems meistens bereits gelohnt. Die FDA-Kriterien sind abgekürzt unter FDA Part 11 bekannt. Um Herstellungsmethoden zu standardisieren hat die FDA ein Regelwerk mit der Bezeichnung CGMP herausgebracht. Eine grundsätzliche Forderung der FDA ist, dass elektronische Aufzeichnungen äquivalent zu Papieraufzeichnungen sind und elektronische Unterschriften die gleiche Aussagekraft und Eindeutigkeit wie handgeschriebene Unterschriften haben. Auf europäischer Ebene sind die entsprechenden Regularien als GxP mit den Teilen GSP und GMP39 einzuhalten. In diesem Umfeld spielen auch GAMP Good Automated Manufactoring Practice, PharmBetrV und Arzneimittelgesetz eine wichtige Rolle.

### Gesundheit

Den Gesundheitssektor in den USA reguliert HIPAA. Im Vordergrund steht die Reformierung der Gesundheitspflege-Industrie. Die Gesetzgebung strebt nach größerer Wirtschaftlichkeit, Verringerung von Schreibarbeiten und einfacher Identifizierung und Weiterverfolgung von Betrug durch die Auferlegung von unterschiedlichen Normen und Sicherheitsmaßnahmen gegen den Missbrauch von gesundheitsbezogenen Angaben des Bürgers. HIPAA beinhaltet so zahlreiche Dokumentations- und Vertraulichkeitsanforderungen, die auch auf Europa ausstrahlen.

### Finanz

Neben dem bereits erwähnten Basel II gibt es zahlreiche weitere Vorgaben für die Finanzdienstleistungsbranche, die sich angesichts der Finanzkrise im Jahr 2008 noch verschärfen werden.

Die grundsätzlichen Anforderungen an das Risikomanagement definiert das MaRisk. Die Bundesanstalt für Finanzdienstleistungsaufsicht BaFin hat am 30.10.2007 ihre neu gefassten Mindestanforderungen an das Risikomanagement veröffentlicht. Die MaRisk wurden dabei insbesondere um modernisierte Outsourcing-Standards ergänzt. Ab 1. November 2007 gelten die neuen MaRisk-Regeln für alle Kredit- und Finanzdienstleistungsinstitute.

Auf internationaler Ebene ist die MiFID Markets in Financial Instruments Directive, angesiedelt. MiFID ist die Umsetzung der europäischen Richtlinie 2004/39/EG über Märkte für Finanzinstrumente. Alle diese Richtlinien ziehen umfangreiche Dokumentationsanforderungen nach sich.

### Öffentliche Verwaltung

Ein Beispiel für einen detaillierten Standard für den Einsatz elektronischer Vorgangsbearbeitungssysteme in der öffentlichen Verwaltung ist das deutsche DOMEA-Konzept. DOMEA beschreibt die Anforderungen an das Dokumentenmanagement und elektronische Archivierung in der öffentlichen Verwaltung und ermöglicht auch die Prüfung und Zertifizierung von entsprechenden Produkten. DOMEA-Compliance ist bei vielen Ausschreibungen eine Anforderung. Wesentliches Ziel des DOMEA-Konzeptes ist die Einführung der elektronischen Akte. Da für diese die gleichen Gesetze, Geschäftsordnungen, Richtlinien und Vorschriften wie für Papierakten gelten, müssen behördliche Geschäftsprozesse, Vorgangsbearbeitung und Archivierung vollständig in konforme IT-Prozesse überführt werden. Das DOMEA-Konzept liefert dafür Richtlinien, ist aber trotz seiner weiten Verbreitung und der Möglichkeit der Zertifizierung kein genormter Standard. Durch die Zertifizierung von Softwareprodukten hat es aber einen normativen Charakter.

In Österreich wird das Thema Vorgangsbearbeitung in der öffentlichen Verwaltung im Rahmen von ELAK, „Elektronischer Akt“, adressiert. Dabei geht es längst nicht mehr nur um die Vereinfachung und Konsolidierung des Bundes-internen Aktenlaufes sondern auch um den Einsatz in Ländern und Kommunen sowie die Bereitstellung von E-Government-Services für den Bürger.

In der Schweiz werden die Aktivitäten unter dem Namen Geschäftsverwaltung (GEVER) gebündelt. GEVER unterscheidet die Anwendungsfelder Geschäftskontrolle, Prozessführung und Records Management. Unter Geschäftskontrolle ist dabei die Überwachung von Bearbeitungsstatus, Termin etc. gemeint. Die Zuweisung, Ausführung und Nachverfolgung von Vorgängen wird unter Prozessführung zusammengefasst.

### Vorgehen bei der Bewertung von Compliance-Vorgaben

Nicht jede Vorgabe betrifft jedes Unternehmen und auch der Umfang der Maßnahmen unterscheidet sich. Man darf sich nicht von der Vielzahl der Vorgaben verunsichern lassen sondern muss für jedes Unternehmen individuell die Vorgaben, ihre Auswirkungen und die notwendigen Umsetzungsmaßnamen bewerten.

Hierfür bietet es sich an, zunächst einen Katalog der möglicherweise zutreffenden Regularien zu erstellen und diesen nach folgenden Kriterien zu klassifizieren:

- **Worum handelt es sich bei der Vorgabe?**
  Hier ist zu unterscheiden, was wirklich ein Gesetz ist und was eine Art "Ausführungsvorgabe" darstellt. Hier würden Kriterien wie Gesetz, Verordnung, Code of Practice oder gesetzlich vorgeschriebene oder referenzierte Norm zum Tragen kommen. Es ist zu berücksichtigen, dass

natürlich alle Regeln der Papierwelt auch für die elektronische Welt gelten.

- **Gilt dies auch im Land oder Tätigkeitsumfeld meines Unternehmens?** Hier sind die unterschiedlichen Rechtsräume zu berücksichtigen, die des Firmenstandortes, des Vertriebsgebietes, der Niederlassungen usw. Nicht zu unterschätzen ist, dass manche Nationen wie die USA ihr Recht überall hin „mitnehmen“. Kriterien wären hier internationale Gültigkeit, europäische Gültigkeit, national „importierte“ Gültigkeit, Gültigkeit im Land des Standortes, Gültigkeit nach Herkunftslandprinzip usw.

- **Betrifft dies abhängig von der Rechts- und Gesellschaftsform meines Unternehmens?**
  Bei diesen Anwendbarkeitsbereichen ist die Form des Unternehmens, der Organisation oder der Verwaltung zu unterscheiden. Kriterien sind hier z.B.: Betrifft die Vorgabe nur die öffentliche Verwaltung, privatwirtschaftliche Unternehmen, Vereine, andere Organisationen (einschließlich supranationale), Einrichtungen, politische Gremien, Jurisprudenz oder aber auch Privatpersonen. Hierzu gehören auch die "Grauzonen" z.B. öffentlich-rechtliche Unternehmen, die sowohl den Vorgaben der öffentlichen Verwaltung sowie den Vorgaben für die freie Wirtschaft unterliegen sowie indirekt weitergereichte Verpflichtungen durch Beteiligungen, Lieferungen und Leistungen in andere oder aus anderen Rechtsräumen, usw.

- **Wie ist mein Unternehmen betroffen?**
  Bei den Kriterien ist zu betrachten, wie stark, wie direkt oder indirekt das Unternehmen durch eine Vorgabe betroffen ist. Es kann differenziert werden zwischen direkt betroffen, d.h. in jedem Fall umzusetzen, indirekt betroffen, d.h. gegebenenfalls umzusetzen (z.B. wenn in einer Supply Chain vom Abnehmer Anforderungen an die Lieferanten „durchgereicht" werden), möglicherweise zutreffend, d.h. gegebenenfalls umzusetzen (für bestimmte Arten von Tätigkeiten), betroffen durch Einbindung Dritter oder Erbringung von Dienstleistungen (z.B. Outsourcing), d.h. durch entsprechende Vorgaben, Verträge und Prüfungen umzusetzen, usw.

- **Wie sind die Anforderungen zu beurteilen?**
  Bei der Beurteilung geht es um die Bewertung und die Abwägung im Rahmen der rechtlichen Würdigung und des Risiko Managements. Kriterien können sein: unbedingt vollständig zu erfüllen, abwägbar im Rahmen der Grundsätze der Verhältnismäßigkeit, abwägbar im Rahmen des Risikomanagements und andere.

- **Wie geht man mit widersprüchlichen Anforderungen um?**
  Gesetze und Verordnungen können sich widersprechen, auf nationaler Ebene, in unterschiedlichen Rechtsbereichen (siehe z.B. die Frage des Datenschutzes im Verhältnis zu den Aufbewahrungspflichten des Handelsrechtes) und natürlich auch international. Kriterien können hier der

Datenschutz, konkurrierende Regelungen (hier nimmt man meistens die umfassendste), Offenlegungsverpflichtungen (z.B. Informationsfreiheitsgesetz) etc. sein.

- **In welchem Umfang sind die Regeln gültig?**
  Hat man ermittelt, welche Regularien überhaupt zutreffend sind, ist noch dem Umfang der Gültigkeit und damit auch der Umfang der notwendigen Maßnahmen zu definieren. Hierzu gehören Kriterien wie generelle Gültigkeit (z.B. Handelsgesetz für alle Unternehmen), teilweise Gültigkeit (z.B. nur für bestimmte Bereiche oder mit Einschränkungen), branchenspezifische Gültigkeit (z.B. nur für Pharma, Krankenhäuser, etc.), tätigkeitsspezifische Gültigkeit (z.B. Verbraucherschutz etc.), nachgeordnete Gültigkeit (z.B. durch interne Qualitäts-Richtlinien, Records-Management-Prinzipien) und weitere.

- **Welche internen Regelungen sind zusätzlich zu berücksichtigen?**
  Jedes Unternehmen setzt sich Ziele und befolgt interne Regelungen, wie diese Ziele im Rahmen der Geschäftstätigkeit umzusetzen sind. Auch diese internen Regelungen können unterschiedliche Qualität und Gültigkeit besitzen. Hier können Kriterien wie Bestandteil der Corporate Governance, Bestandteil der IT-Governance, Bestandteil des Qualitätsmanagementsystems, Arbeitsanweisung, Betriebsvereinbarung, Datenschutz & Datensicherheit, und andere notwendig werden. Vielfach leiten sich solche Vorgaben bereits aus rechtlichen oder regulativen Vorgaben ab.

An die Umsetzung von Compliance-Vorgaben sollte man erst schreiten, wenn diese Analyse und Bewertung vorgenommen wurde. Die Verantwortung hierfür liegt bei Geschäftsführern und Vorständen. In der Regel wird eine solche Bewertung (je nach Unternehmensgröße und –aufstellung) zusammen mit der Rechtsabteilung, der Revision, dem Controlling, Wirtschaftsprüfern, Anwälten oder Unternehmensberatern durchgeführt. Diese bewertete Aufstellung wird in der Governance-Richtlinie verankert und ist der Maßstab für das Risikomanagement und den Umfang der Compliance-Maßnahmen.

**Records Management als Methode zur Erfüllung von GRC-Anforderungen**

## *Records & Records Management*

### Definitionen

Unter einem Record wird ein beliebiger Content-Typ verstanden, der sich auf die Geschäftstätigkeit oder die Transaktion eines Unternehmens bezieht. Ein Record definiert sich durch Inhalt und Rechtscharakter, nicht durch seine physische oder elektronische Form. Beispiele sind E-Mails, Verträge, Geschäftsvereinbarungen, Kontoübersichten, Berichte sowie Video- und Audiodateien.

*Record:*

*Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.*

Die Begriff Record und Records Management sind durch ISO-Norm 15489, Teil 1, „Records Management“, bzw. im Deutschen „Schriftgutverwaltung“, international normiert. So lautet die deutsche Übersetzung der Definition von Record:

„Information, die erzeugt, empfangen und bewahrt wird, um als Nachweis einer Organisation oder Person bei rechtlichen Verpflichtungen oder zum Nachvollzug einer geschäftlichen Handlung zu dienen.“

*Records Management:*

*Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.*

Dem entsprechend lautet die deutsche Übersetzung von Records Management “Schriftgutverwaltung“ – und trifft dabei nicht den Kern des Begriffes:

„Als Führungsaufgabe wahrzunehmende effiziente und systematische Kontrolle und Durchführung der Erstellung, Entgegennahme, Aufbewahrung, Nutzung und Aussonderung von Schriftgut, einschließlich der Vorgänge zur Erfassung und Aufbewahrung von Nachweisen und Informationen über Geschäftsabläufe und Transaktionen in Form von Akten.“

Nur mit Mühe lässt sich dieser Begriff aus der Akten- und Papierorganisation auf das elektronische Records Management übertragen. Wesentlich ist dabei die

Herausstellung des Begriffes „Führungsaufgabe“, die wieder die Brücke zur Verantwortung der Geschäftsleitung und zu Corporate Governance schlägt.

**Funktionalität**

*Records Management wurde designt, um Compliance-Anforderungen umsetzen zu können.*

Records Management bezeichnet die Verwaltung von Aufzeichnungen unabhängig vom Medium. Die Verwaltung muss dabei geordnet, sicher und nachvollziehbar sein. Die Records müssen eindeutig identifizierbar, im Sachzusammenhang erschließbar, authentisch und originär, gegen unauthorisierte Benutzung geschützt und entsprechend den vorgesehenen Aufbewahrungs- und Vernichtungsfristen der Objekte verwaltet werden. Basis für Records Management sind strukturierte Ablagepläne, definierte Ordnungskriterien und geeignete, persistente Findmittel. Records Management wird heute als eine Komponente des übergreifenden Enterprise Content Management verstanden.

Für die Verwaltung von Records muss ein Records-Management-System nach den Vorgaben der amerikanischen Nationalen Records Verwaltung (NARA) folgende Bedingungen erfüllen:

*Anforderungen an das Records Management*

- *Zugreifbarkeit (Accessible)*
- *Lesbarkeit (readable)*
- *Reproduzierbarkeit (reproducable)*
- *Nachvollziehbarkeit (tracable)*
- *Unveränderbarkeit (unchanged, integrity, authenticity)*
- *Langfristige Bewahrbarkeit (preservable)*
- *Selbstbeschreibbarkeit der Records (self-documenting)*
- *Entsorgbarkeit (disposable)*
- *Rechtssicherheit (usable as evidence in regulatory and legal queries)*

Records Management geht dabei über den Ansatz der elektronischen Archivierung hinaus: Records-Management-Systeme verwalten über Referenzen auch Informationen auf Papier in Aktenordnern oder auf Mikrofilm. Dies ermöglicht die vollständige Kontrolle auch „gemischter“ Verfahren, in denen ein Parallelbetrieb mit unterschiedlichen Medien erforderlich ist. Records-Management-Systeme besitzen elektronische Ablagepläne und Thesauri, die eine strukturierte, geordnete, nachvollziehbare und eindeutige Zuordnung der Informationen sicherstellen. Hierbei werden Mehrfachzuordnungen nach unterschiedlichen Sachzusammenhängen und die Verwaltung unterschiedlicher Versions- und Historienstände der Ordnungssystematik unterstützt.

Records Management ist daher eine Basiskomponente für die Abbildung elektronischer, virtueller Akten und für die elektronische Vorgangsbearbeitung.

## *Internationale Standards im Records Management*

Das elektronische Records Management ist der Bereich der IT-Anwendungen, der weitreichend standardisiert ist. Neben zahlreichen nationalen Standards für Records Management existieren auch internationale und europäische Vorgaben. Auf die wichtigsten soll im Folgenden eingegangen werden.

### ISO 15489 Records Management

Die ISO-Norm Records Management stellt Management-Richtlinien zur Unternehmenspolitik und Vorgehensweisen für das Records Management des Unternehmens auf und dient als Anleitung zur Implementierung bei der unternehmensweiten Einführung von Records Management. ISO 15489 Teil 1 (2001) ist der Führer für die Leitungsebene von Unternehmen, Behörden und Verwaltungen. Er gibt als kurzes und prägnantes Dokument mit 17 Seiten Rat zum Festlegen, welche Dokumente erzeugt, welche Information in die Dokumente eingefügt werden müssen und welcher Genauigkeitsgrad erforderlich ist, zum Entscheiden, in welcher Form und Struktur Dokumente erzeugt und erfasst werden sollen, zum Festlegen der Anforderungen zum Retrieval und Gebrauch von Dokumenten und wie lange sie archiviert sein müssen, um diesen Anforderungen zu genügen und zum Festlegen, wie Dokumente zu organisieren sind, um die Anforderungen für den Gebrauch zu unterstützen. ISO 15489 Teil 2 legt die Vorgehensschritte fest: von der ersten Analyse, Identifizierung der Anforderungen bis zur Implementierung eines Records-Management-Systems.

### ISDF International Standard for Describing Functions

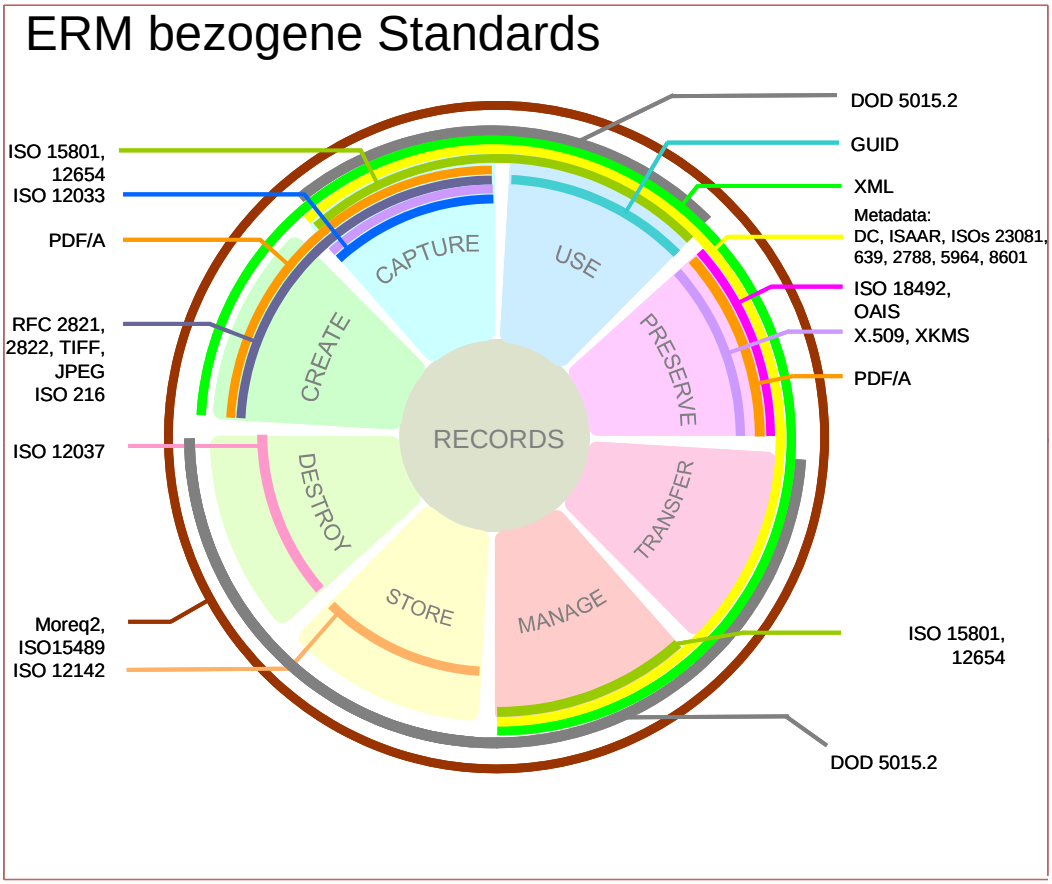
Der International Council on Archives, ICA hat mehrere Dokumente zur Standardisierung des Records Managements herausgegebenen. Der ISDF, International Standard for Describing Functions, erstellt vom Committee of Best Practices and Standards (CBPS), wurde auf dem ICA Kongress 2008 in Kuala Lumpur präsentiert. Dieser Records Management Standard besteht aus Informationselementen, wobei jedes aus folgenden Teilen besteht: dem Namen des Elementes; einer Erläuterung zum Zweck des Elementes; einer Erläuterung zu den Regeln und Daten-Restriktionen, die auf das Element anwendbar sind, und, wo möglich, Beispiele, die verdeutlichen, wie die Regel zu implementieren ist.

Ebenfalls wurden die “Principles and Functional Requirements for Records in Electronic Office Environments” vorgestellt. Das Ziel des Projekts ist es, global einheitliche Prinzipien und funktionelle Anforderungen an Software, die zum Erzeugen und Managen von elektronischen Records eingesetzt wird, zu definieren.

### MoReq Model Requirements for the Management of electronic Records

Die erste Version von MoReq, herausgegeben von der Europäischen Kommission und dem DLM Forum, wurde bereits im Jahr 2001 veröffentlicht. Diese Leitlinie umfasst eine „formelle Spezifikation für funktionale und nichtfunktionale Anforderungen an Systeme zur Verwaltung von elektronischen Archiven (ERMS, engl. Electronic Records Management System) und gilt gleichermaßen für Organisationen des öffentlichen und privaten Sektors“. MoReq1 wurde in 11 Sprachen übersetzt.

Im Februar 2008 wurde die vollständig überarbeitete Spezifikation MoReq2 veröffentlicht. Wesentliche Inhalte der Erweiterungen sind die Schaffung einer flexibleren Struktur, die Erweiterung des Basismoduls, die Schaffung neuer optionaler Module, die Entwicklung eines MoReq Compliance Tests für Softwareprodukte sowie die Ergänzung um eine länderspezifische Einleitung, das „Chapter 0“. MoReq2 setzt auf dem MoReq1 Standard auf und lehnt sich in Struktur und Format an diesen an. MoReq2 besteht aus einem „Requirements“-Dokument, dem eigentlichen Standard mit mehreren Anhängen, Datenmodell und funktionalen Anforderungen, einem dazugehörigen XML-Schema für Daten- und Entitäten-Modell, einem umfangreichen Testszenarien-Katalog und einem Zertifizierungsprogramm. Softwareproduktanbieter können ihre Produkte ähnlich wie bei DOMEA, DoD 5015.2 und anderen Standards prüfen lassen, wobei das Zertifikat europaweit gilt. Aber auch für Anwender in der öffentlichen Verwaltung und der Privatwirtschaft ist der Standard nützlich, um damit Ausschreibungen, Anforderungen und bereits vorhandene Installationen entsprechend dem State-of-the-Art überprüfen zu können.




Neben den „großen“, ganzheitlichen Standards für das Records Management wie ICA und ISO 15489 international, MoReq2 in Europa oder DoD 5015.2 in den USA gibt es zahlreiche weitere Normen und Standards, die Teilbereiche abdecken oder bestimmte Funktionalität. Hier sind z.B. Standards wie PDF/A (ISO 19005) für Archivformate, OAIS Open Archival Information System (ISO 17421) für die Architektur von Archivsystemen oder die ISO 23081 für Metadaten zum Records Management zu nennen. Am umfassendsten und aktuellsten ist der im Jahr 2008 herausgegebene Standard MoReq2, der seinerseits zahlreiche andere Standards inkorporiert.

Records Management deckt so heute alle Bereiche von der Erzeugung, Erfassung, Verwaltung, Archivierung, Verteilung, Bereitstellung und Zerstörung von elektronischen Aufzeichnungen ab.

### GRC: Lösungsansätze

Beim Thema GRC Governance, Risk Management und Compliance, geht es aber nicht nur um Records-, Dokumenten- und Archivmanagement.

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 Data-Warehouse-Lösungen, unstrukturierte Informationen in E-Mail-, Archiv-, Dokumentenmanagement-, Collaborations-, MultiMedia- oder GIS-Lösungen.

*GRC muss wirtschaftlich sein.*

*Im Vordergrund stehen Geschäftsprozesse, Wissenserschließung und durchgängiges Informationsmanagement – die Compliance-Anforderungen sind sozusagen als Selbstverständlichkeit nebenbei mitzuerfüllen.*

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 Enterprise-Content-Management-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. Records Management ist die Basisfunktionalität für eine geordnete Informationsverwaltung. 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 langzeitig unverändert und sicher aufbewahrt werden müssen.

Hierfür bieten Archivsysteme datenbankgestützten Zugriff auf archivierte Daten und Dokumente, unveränderbare „revisionssichere“ Speicherung aller Informationen, Audit Trails der Speicherung und Nutzung, Verwaltung sehr großer Informationsmengen auf sehr unterschiedlichen Speichern, Migrationskonzepte zur Verfügbarhaltung 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.

## Ausblick

Für das Thema GRC gibt es sehr unterschiedliche Lösungsansätze unterschiedlicher Hersteller. So bieten ERP-Anbieter häufig Daten-orientierte Module und Funktionen an, die Daten-Records und Referenzen auf dazugehörige Dokumente verwalten. 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 bis hin zu europäischen Firmen. 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.

Da im deutschsprachigen Raum, besonders in Deutschland, der Begriff Records Management noch kaum bekannt ist, und auch der Begriff Compliance für viele Anwender wenig Aussagekraft hat, stehen wir 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.

*GRC Governance, Risk Management und Compliance kann nicht mit Insellösungen erreicht werden – ein durchgängiger Ansatz ist gefordert.*

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.

## Herausgeber und Verfasser

### Herausgeber

IBM Deutschland GmbH
ECM Marketing
Wihelm-Fay-Str. 30 – 34
65936 Frankfurt

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
www.ibm.com

## Autor

Dr. Ulrich Kampffmeyer, Jahrgang 1952, ist Gründer und Geschäftsführer der PROJECT CONSULT Unternehmensberatung GmbH, Hamburg, eine der führenden produkt- und herstellerunabhängigen Beratungsgesellschaften für ECM Enterprise Content Management, BPM Business Process Management, Knowledge Management und andere DRT Document Related Technologies.

Er beriet namhafte Kunden aller Branchen im In- und Ausland bei der Konzeption und Einführung von ECM-Lösungen.

Als Gründer und langjähriger Vorstandsvorsitzender nationaler und internationaler Branchenverbände prägte er wesentlich den deutschen Markt für Dokumenten-Management. Er ist einer der Gründer und Geschäftsführer des DLM-Network EEIG. Dr. Kampffmeyer ist Mitglied in mehreren internationalen Standardisierungsgremien im Umfeld des Workflow-, Dokumenten- und Records-Management.

Dr. Kampffmeyer ist anerkannter Kongressleiter, Referent und Moderator zu Themen wie elektronische Archivierung, Records-Management, Dokumenten-Management, Workflow, Rechtsfragen, Business Re-Engineering, Wissensmanagement und Projektmanagement. Auf zahlreichen nationalen und internationalen Kongressen und Konferenzen wirkte er als Keynote-Sprecher mit.

**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