RC&A Risk, Compliance & Audit
ISSN 1867-8122

Mehrwert durch GRC-Software statt Overhead durch Excel

Stephan Haupt und Hans-Joachim Müncheberg

RMA Frankfurt School Verlag bank-verlag medien Praxis, Methoden & Dialog

Mehrwert durch GRC-Software statt Overhead durch Excel

Sicherheit bei der Auswahl von GRC-Software

Durch die zunehmende Vielzahl und Komplexität regulatorischer, normativer und interner Anforderungen ist Excel als System für die Herausforderungen in den Bereichen „Governance, Risk & Compliance" (GRC) am Ende seines Lebenszyklus angelangt. Nur mit dem Einsatz geeigneter, datenbankbasierter GRC-Software können Unternehmen den vollen Mehrwert eines methodisch integrierten GRC-Managementansatzes realisieren. Für eine erfolgreiche GRC-Softwareauswahl sind aus diesem Managementansatz die Anforderungen strukturiert abzuleiten und die Beschaffung auf die wirklich zusätzlich benötigten Software-Komponenten zu fokussieren. Zu diesem Zweck ist „nur" noch Licht ins Dunkel des relativ jungen und virulenten Softwaremarktes für GRC-Lösungen zu bringen. Basierend auf einer systematischen Vorgehensweise und anhand des GRC-Software-Monitors wird im Folgenden ein praxisbewährter Weg zum sicheren Projekterfolg aufgezeigt.

1 Definitionen

Zur Entwirrung der GRC-Begrifflichkeiten sollen zunächst die wesentlichen der im Folgenden verwendeten Begriffe bestimmt und gegeneinander abgegrenzt werden:

- **Managementsysteme** unterstützen die zielorientierte Führung des Unternehmens und der Kerngeschäftsprozesse bei der Erfüllung spezifischer Anforderungen – mit eigener Führungstruktur, Methodik, Prozessen, Kontrollen und Berichtserfordernissen. In aller Regel handelt es sich bei den betrachteten Aktivitäten um Querschnittsprozesse. In diesem Sinne sind das Risikomanagement und das interne Kontroll-System von Unternehmen genauso als Managementsystem zu begreifen wie das IT-Risikomanagement oder das IT-Security-Monitoring, aber auch umfassendere Gebiete wie das Umweltmanagement, das Qualitätsmanagement u. v. m.
- **Integrierte Managementsysteme** verbinden ursprünglich getrennte Managementsysteme (wie beispielsweise einige der zuvor genannten) in methodischer und prozeduraler Hinsicht.
- **GRC-Management** ist das integrierte Managementsystem im Hinblick auf die Governance (Management der Führungs- und Kontrollstrukturen), die Risiken (Management der Zielerreichung) und die Compliance (Management der Konformität mit internen und externen Anforderungen). Auch das GRC-Management kann mit weiteren Managementsystemen verbunden werden.

2 Notwendigkeit des Einsatzes einer GRC-Software

Zur Sicherstellung höchstmöglicher Konformität wird heute in den meisten Unternehmen jede regulative, normative und interne Anforderung noch getrennt voneinander durch jeweils eigenständige Managementsysteme umgesetzt. Vor dem Hintergrund der Charakterisierung von GRC-Abläufen als Querschnittsprozesse wirken sich diese Managementsysteme durch die fehlende Vereinheitlichung und Vereinfachung dann oft kontraproduktiv (d. h. als Overhead) auf die Bemühungen um möglichst schlanke Kerngeschäftsprozesse aus.

Die markführende IKS- und RMS-Software Microsoft Excel wird meist zur Administration eingesetzt. Je komplexer oder weit verzweigter die Unternehmensorganisation aber ist, desto komplizierter wird es, Licht in das Dunkel der Risiken und der Erfüllung der Anforderungen zu bringen. Den Benchmark in diesem Bereich erreicht ein Unternehmen schon dann, wenn es ihm gelingt, dass unzählige „Excel-Tapeten" inhaltlich auf den gleichen Definitionen beruhen und diese widerspruchsfrei konsolidiert werden können. Die Kür besteht dann darin, die Ergebnisse ansprechend aufzubereiten und darzustellen. Insgesamt ergibt dies den perfekten Overhead – und all das für vergangenheitsbezogene Daten.

Um wirklich Mehrwert durch Managementsysteme zu schaffen, müssen die (in aller Regel ja mit hohem Aufwand erhobenen) Informationen das Management bei Entscheidungen unterstützen bzw. als Instrument der strategischen Unternehmenssteuerung dienen können. Zu diesem Zweck müssen die Informationen relevant, konsistent, verläßlich und aktuell

sein. Aufgrund dieser Anforderung ist der Einsatz einer datenbankbasierten Software für ein integriertes GRC-Management unerlässlich.

3 Vorgehensweise bei der GRC-Softwareauswahl

Aufgrund umfangreicher Praxiserfahrungen haben sich im Hinblick auf eine geeignete Vorgehensweise bei der Auswahl einer konkreten GRC-Softwarelösung die folgenden sieben nacheinander durchzuführenden Schritte als erfolgskritisch herauskristallisiert:

- **Projektdefinition**
  Schon an der unzureichenden Projektdefinition scheitern viele GRC-Initiativen. In vielen Fällen tauchen die Verantwortlichen mit großem Aufwand direkt in die Tiefen sehr spezifischer Fragestellungen ab, die eigentlich erst sehr viel später zu klären sind, wie beispielsweise „Welche Software ist die Geeignete?“ oder „Wie können die Strukturen und Inhalten der heutigen Excel-Tabellen erhalten werden?“. In den meisten Projekten wird das Fehlen klar definierter und von allen Beteiligten getragener Projektziele, -umfang, -organisation, -vorgehen, etc. erst zu spät transparent: Nämlich dann, wenn die Unterstützung der Sponsoren ausbleibt oder die Beschaffung oder die IT entscheidungsrelevante Fragen stellt, die das Team nicht ausreichend beantworten kann.
  Wichtig ist, schon im Schritt der Projektdefinition eine erste Idee für den Lösungsansatz und den Projektumfang zu skizzieren, um feststellen (und gegenüber anderen Beteiligten auch darstellen) zu können, ob und wie der Business Case trägt, bzw. das Projekt einen meßbaren Beitrag für das Unternehmen liefern kann. Hierzu ist viel Erfahrung notwendig. Auch der Umfang der sinnvollerweise und unter Wirtschaftlichkeitsüberlegungen vertretbar neben dem Risiko- und Compliance-Management einzubindenden Managementsysteme, wie IT-Risikomanagement, IT-Sicherheitsmanagement, Krisenmanagement, Revision, etc. ist vorab zu identifizieren.
  Diese erweiterte Projektdefinition ermöglicht aus Sicht der Autoren erst einen meßbaren Projekterfolg und erleichtert die nachhaltige Rückendeckung durch die Unternehmensführung, die Sicherstellung erforderlicher Ressourcen und die Führbarkeit des Projektes wesentlich.

- **GRC-Methodik**
  Für die einzubindenden Managementsysteme ist der unternehmensübergreifende, geschlossene methodische Rahmen für das GRC-Vorgehen im Detail festzulegen. Dies dient unter anderem der Ableitung der wesentlichen funktionalen Anforderungen. Außerdem setzen die Softwarehäuser bei der Implementierung darauf auf, d. h. sie setzen deren Existenz voraus! So ermöglicht eine spezifische GRC-Methodik erst die sinnvolle Nutzung einer GRC-Software.

- **GRC-Metadatenmodell**
  Des Weiteren ist ein unternehmensspezifisches Metadatenmodell abzustimmen, das die Schlüsselentitäten (Ziele, Risiken, Kontrollen, Mitarbeiter etc.) und deren erforderliche Beziehungen beschreibt – abgeleitet aus dem Vorgehensmodell und den Soll-Prozessen. Das der GRC-Software zugrundeliegende Datenbanksystem muss die aktuellen und zukünftig erforderlichen Beziehungen zwischen den Schlüsselentitäten abbilden können. Dies ist erfahrungsgemäß ein wesentlich wichtigeres Auswahlkriterium als die meisten funktionalen Aspekte. So können viele GRC-Softwarepakete gar nicht oder nur mit Hilfe von „Krücken“ (beispielsweise in Form eines reinen Textfelds) die Beziehung zwischen Risiken und Zielen darstellen. Das kann dann wesentliche funktionale Einschränkungen gegenüber der GRC-Methodik zur Folge haben und sich negativ auf die Wirtschaftlichkeitsrechnung auswirken.

- **GRC-IT-Architektur**
  Solange der Marktführer Excel eingesetzt wird, kann dies in der Regel ohne aktive Einbindung der IT-Abteilung vorgenommen werden. Eine datenbankbasierte GRC-Software hingegen ist nicht länger unabhängig und ohne Mitwirkung der IT einzuführen und zu betreiben, da sie wesentliche Schichten (konkret: Die unteren fünf in Abbildung 1) der existierenden Unternehmens-IT-Architektur tangiert. Vor diesem Hintergrund ist eine GRC-IT-Ziel-Architektur zur Identifikation und Eingrenzung von funktionalen und technischen Anforderungen an die zu beschaffende GRC-Software abzustimmen. Hierzu ist ein Grundverständnis der Softwarearchitektur erforderlich. Das in Abbildung 1 dargestellte GRC-Schichtenmodell kann dabei helfen. Die relevanten Schichten sind hierbei

  - **BI (Business Intelligence)**: Multidemensionale, frei definierbare Auswertungs- und Darstellungsmöglichkeiten über das gesamte Metamodell bzw. die Datenbanken aller tangierten Systeme.
  - **GRC-Management** (GRC-Software im engsten Sinne): Integrierte und wirksame Verfolgung aller Risiken (qualitative, quantitative) und Kontrollen (einmalige vs. regelmäßig, automatisiert vs. manuell) über diver-

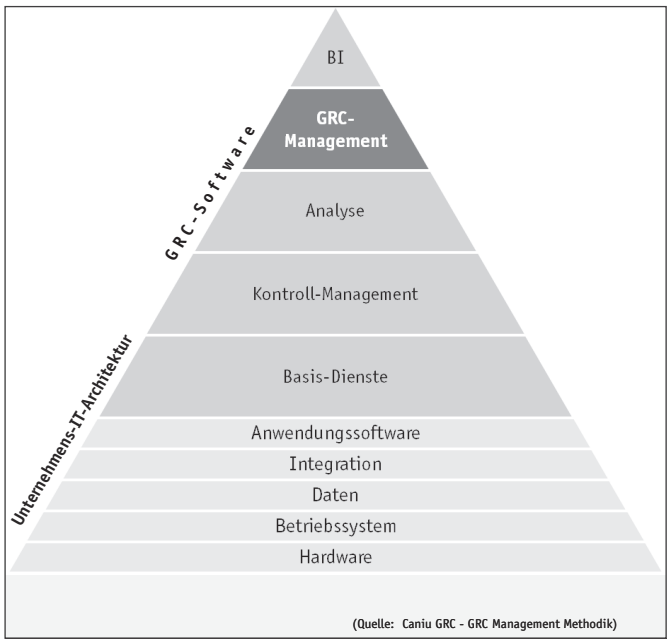

Abbildung 1: GRC-IT-Schichtenmodell

se (GRC-) Quellsysteme des gesamten Unternehmens zur Sicherstellung der Wirksamkeit des GRC-Managements.

- **Analyse:** Unterstützende Programme bei qualitativen Risikoeinschätzungen, aber auch zur quantitative Bestimmung oder Prognose von Risikokennziffern mit stochastisch mathematischen Modellen, beispielsweise eine Monte-Carlo Simulation.
- **Kontroll-Management**: Dedizierte Programme zur Überwachung oder Prüfung automatisierter (d. h. mit Schnittstellen zur Anwendungssoftware des Unternehmens, wie etwa SAP) und manueller Einmal-, Regel- oder Permanent-Kontrollen, beispielsweise für bestimmte Prozesse oder IT-Komponenten.
- **Basis-Dienste**: Wiederverwendbare Programme, die sich die GRC-Software mit anderen Systemen teilen kann bzw. die an dieser Stelle Wiederverwendung finden können, beispielsweise Dokumentenmanagement, Workflowmanagement, Aufgaben-/Projektmanagement, u. v. m.

Die oben detaillierten Schichten stellen die Definition der GRC-Software im weitesten Sinne dar. Die anderen Schichten sind die üblichen, die sich in praktisch jeder Unternehmens-IT-Architektur wieder finden.

Zur Vermeidung von Redundanzen, zusätzlichen Kosten und Non-Compliance mit der IT-Strategie, sollten zumindest grundsätzliche Abstimmungen über die Nutzung eventuell vorhandener, wiederverwendbarer oder zu integrierender Programme sowie zur Nutzung bereits vorhandener, automatisierter Kontrollen der Anwendungssoftware erfolgen. So stellt die Definition der Einbettung in die bestehende IT-Landschaft eine erfolgskritische Projektaufgabe dar.

- **GRC-Anforderungen**
  Auf der Basis der Ergebnisse der vorangegangenen Schritte fällt es im Anschluss leicht, die relevanten funktionalen und technischen Anforderungen abzuleiten.
  Wichtig ist bei diesem Schritt die Differenzierung und Gewichtung der Anforderungen (gemäß den Kriterien funktionale, technische, kaufmännische, Service, Anbieter) sowie deren Artikulation in der sehr eigenen Sprache der Softwarebranche.

- **GRC-Softwareauswahl**
  Um die Projektlaufzeit in engen Grenzen zu halten und damit die Aufmerksamkeitspanne der Projektsponsoren nicht zu sehr zu strapazieren, ist ein schneller und pragmatischer Auswahlprozess angezeigt. Bewährt hat sich eine Software-Auswahl in zwei Iterationen
  - Vorauswahl auf der Basis identifizierter K.o.- bzw. Schlüssel-Kriterien (funktional, technisch, Metamodell, Kosten, Investitionsschutzerfordernisse, Lieferantenrisiko), wobei maximal zehn bis fünfzehn Kriterien zur Selektion von drei bis fünf alternativen Anbietern verwendet werden sollten.
  - Endauswahl (zwischen zwei bis drei Finalisten) auf der Basis präzise definierter und gewichteter Anforderungen sowie einer Online-Software-Präsentation durch die vorgesehene Projektleitung des Anbieters. Hierbei sollte jedoch nicht die Standardpräsentation des Anbieters verwendet werden, sondern eine Präsentation repräsentativer Anwendungsfälle des betreffenden Unternehmens, die von Seiten des Projektteams vorgegeben werden.

- **Vertragsabschluss**
  Neben einem strukturierten Vorgehen (das selbstverständlich auch mit den jeweiligen Einkaufs- und IT-Richtlinien konform sein muss) sind in diesem Schritt vor allem die folgenden Punkte wichtig:
  - Eng getaktete Ausschreibungsmeilensteine und Termine, die damit auch die Leistungsfähigkeit des Supports des Lieferanten auf den Prüfstand stellen,
  - Abgestimmte Gewichtung aller Entscheidungskriterien vor der Anbieterpräsentation,
  - Entscheidung auf der Basis der „Total Cost of Ownership“ statt der ausschließlichen Betrachtung der Lizenzkosten sowie

- Tiefgreifende Erfahrungen in der Vertragsgestalltung mit Softwarelieferanten

4 Klassifikation von GRC-Software

Der Gattungsbegriff GRC-Software – vergleichbar zu ERP, CRM, PLM, u. v. a. – etabliert sich zunehmend. Der GRC-Softwaremarkt ist jung und sehr virulent. Derzeit dürften global weit über 100 Softwareanbieter (inkl. GRC-Teilsystemanbieter) in diesem Segment aktiv sein. So ist es selbst für einen sorgfältigen Marktbeobachter schwer, immer den Überblick zu behalten – geschweige denn für einen künftigen Anwender, der sich nur zur Software-Auswahl einmalig mit diesem „neuen Markt" beschäftigt.

Globaler und deutscher Marktführer in diesem Bereich ist immer noch Microsoft Excel – Die Tabellenkalkulation ist allerdings keine GRC-Software im eigentlichen Sinne, sondern wird als Werkzeug zur Arbeitserleichterung verwendet – unter anderem bei der strukturierten Risiko-, Kontroll- und Wirksamkeitserfassung und -bewertung.

Datenbankbasierte GRC-Software im weiteren Sinne umfasst im Kern das Risikomanagement (RMS) und Kontrollmanagement (IKS), oft auch das Umfragemanagement, das Maßnahmenmanagement, das Schadensmanagement und das übergreifende Berichtswesen. Es kann aber auch das Auditmanagement, Anforderungs/Policymanagement, IT-Sicherheitsmanagement, IT-Risikomanagement, Notfallmanagement beinhalten, nur um einige typische Module (bzw. Managementsysteme) zu nennen.

Aufgrund der meist unzureichenden Würdigung der für den deutschen Markt relevanten Anbieter in Softwarevergleichen internationaler IT-Analysten wie Forrester, Gartner, etc. haben sich die Autoren des vorliegenden Beitrags bereits im Jahr 2006 entschlossen, den Markt mit Hilfe eines eigenen GRC-Software-Monitors (siehe Abbildung 2) zu verfolgen. Hauptkriterien für die Klassifikation der unterschiedlichen Produkte sind die Firmenstärke (Finanzkraft, Liefer- und Supportfähigkeit) und Produktstärke (Funktionsbreite und -tiefe, Integrationsgrad). Beim Auftragen der GRC-Anbieter/Softwarepakete lassen sich aus aktueller Sicht die Abbildung 2 genannten wesentliche Cluster identifizieren, wobei von GRC-Management-Lösungen im engeren Sinne nur in den beiden oberen Matrixfeldern gesprochen werden kann. In diesem Zusammenhang ist anzumerken, dass die im Folgenden erwähnten Unternehmens- und Produktbeispiele rein exemplarisch für das jeweilige Cluster zu verstehen sind. Die Nennung impliziert somit keinerlei Wertung oder Ranking bestimmter Lösungen. Ohnehin helfen pauschale Bewertungen von Anbietern und deren Produkte nicht weiter, da die unternehmensspezifischen Anforderungen sehr unterschiedlich sein können.

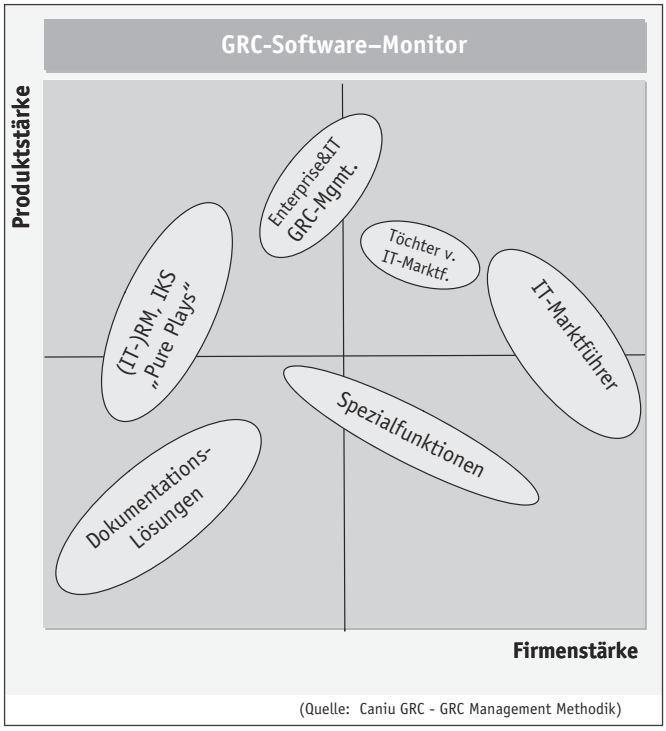

Abbildung 2: GRC-Software Monitor

Dokumentationslösungen: Diesem Cluster sind zum einen Excel-basierte Lösungen zuzuordnen, die zum Teil komplexere Makros enthalten oder sich in Access-Lösungen auswachsen. Zum anderen umfasst diese Kategorie Web-/Contentmanagement-basierte IKS-Dokumentationslösungen. In vielen Fällen wurden derartige Lösungen von Prüfern/Beratern einiger Wirtschaftsprüfungs- oder Steuerberatungskanzleien ursprünglich Kundenspezifisch entwickelt. Den Lösungen ist gemein, dass sie ursprünglich nicht von professionellen IT-Unternehmen und nicht für Anforderungen des kommerziellen Vertriebs entwickelt wurden.

Spezialfunktionen-Anbieter: Diese Ansätze fokussieren auf Teillösungen für spezifische, funktionale Anforderungen (beispielsweise Monte-Carlo-Simulationen), spezifische regulatorische Anforderungen (etwa der FDA, PCI) oder spezifische automatisierte Kontrollen. Als typischer Vertreter kann ACL genannt werden.

IT-Marktführer: Diese Kategorie beinhaltet zum einen marktführende IT-Dienstleister, die eigene GRC-Software-Teillösungen in ihr nicht strategisches Produktportfolio mit aufnehmen (typischer Vertreter: SAP). Zum anderen finden sich diverse, nicht integrierte Funktionalitäten der strategi-

schen Softwareprodukte des jeweiligen Anbieters, die marketingtechnisch unter dem Begriff GRC subsummiert werden, beispielsweise mehrere IT-Sicherheitsfunktionen und automatisierte Kontrollen eines umfassenden Datenbankmanagementsystems (typischer Vertreter: Oracle).

Töchter von IT-Marktführern: Bei dieser Gruppe handelt es sich um (meist zugekaufte) GRC-Software-Anbieter, die von großen Anbietern als separate Business Unit mit höheren Freiheitsgraden (da nicht zum strategischen Softwareproduktportfolio gehörend) weitergeführt werden. Ein typischer Vertreter dieser Gruppe ist unter anderem Openpages/IBM.

Pure Plays: Nur wenige Anbieter („Pure Plays"), haben sich exklusiv dem Thema Risiko- und Compliancemanagement verschrieben. In der Regel ist ihre datenbankbasierte GRC-Software als Erweiterung bestehender strategischer Produkte (etwa in den Bereichen Prozessmanagement, Qualitätsmanagement, Datenbankmanagement oder IT-(Kontroll-)Management) entstanden. Die einzelnen Module sind allerdings noch nicht zu einer gesamthaften GRC-Sofware-Lösung basierend auf einem Datenmodell und einer Datenbank integriert worden. Einen typischen Vertreter dieser Gruppe stellt Schleupen dar.

Enterprise & IT GRC-Management: Als Trend ist zu beobachten, dass neben dem Enterprise-(Unternehmens)-GRC-Management und dem heute meist noch getrennten IT-GRC-Management (mit den oben genannten Modulen) insbesondere folgende weitere funktionale Teilmärkte zu umfassenden GRC-Management-Lösungen und größeren Anbietern zusammenwachsen: Automatisiertes Kontrollmanagement, Enterprise Architekturmanagement, Prozessmanagement, IT-Planung und Management, Qualitätsmanagement sowie Anwendungen für Basis-Dienste, wie Zugriffsmanagement, Workflowmanagement, Dokumentenmanagement, Projektmanagement und Business Intelligence. Als typischer Vertreter für diesen Ansatz kann BWise genannt werden.

Über alle Cluster hinweg betrachtet lassen sich aktuell folgende Entwicklungen feststellen:

- Es sind nur wenige wirklich global lieferfähige Anbieter auszumachen.
- Eine geringe Anzahl von Anbietern kommt ursprünglich aus Deutschland. Viele sind erst dabei, den deutschsprachigen Raum zu erschließen.
- Die Mehrzahl der Anbieter ist den Clustern Dokumentations- und Teillösungen zuzurechnen.
- Gemein ist allen Anbietern der oberen beiden Matrixfelder, dass sie für gesamthafte GRC-Software-Lösungen meist sehr wenige (maximal drei) relevante Referenzen aufzuweisen haben. Bei Lösungen der Anbieter der beiden unteren Matrixfelder stellt sich dies grundlegend anders dar.
- Viele Anbieter verfügen nur über schwache Finanzkraft.
- Kritisch zu hinterfragen ist in jedem Fall die Installationsunterstützung durch den Anbieter oder Dritte. Hier sieht es erfahrungsgemäß jenseits der standardmäßigen Basisimplementierung problematisch aus. Aufgrund der geringen Installationszahlen und der geringen Installationsaufwände lohnt sich die Etablierung dedizierter Installationsteams schlichtweg nicht – weder für Software-Anbieter noch für dritte Dienstleister.

5 Aufwand für die Einführung

Die Investitionen für die Einführung einer GRC-Software lassen sich im Vergleich zu ERP, CRM, PLM in engen Grenzen halten und fallen insbesondere in folgenden Bereichen an:

- Die Projektausführung erfolgt durch teilzeit-dedizierte Mitarbeiter der betroffenen Abteilungen – als Teil ihrer Zeit, die sie ohnehin für die kontinuierliche Weiterentwicklung verwenden.
- Es erfolgt eine Expertenunterstützung durch prüfer- und softwareanbieter-unabhängige Berater (dies erscheint erforderlich im Sinne der Konformität mit den Anforderungen zur Trennung der Verantwortlichkeiten „Seggregation of duties") bei der Positionierung, Projektdefinition, GRC-Methodik, Softwareauswahl und dem Management der Softwareimplementierung. In der Regel kann dies im Rahmen eines workshop-orientierten Coachingmodus durchgeführt werden, d. h. insgesamt wird hierfür weniger als ein Vollzeit-Akquivalent für die durchschnittliche Projektlaufzeit von drei bis vier Monaten benötigt.
- Die Lizenzkosten für eine GRC-Software beginnen für eine mittelständische Lösung (die aber vielfach schon ausreichende zehn gleichzeitige Nutzer aufweist) im unteren fünfstelligen Eurobereich. Für Konzernlösungen liegen sie in der Regel bei mittleren sechstelligen Summen. Zusätzlich fallen die jährliche Wartungs- und Supportgebühren in der für Softwareanbieter allgemein üblichen Höhe an.
- Die Implementierungsaufwände für die Software-Installation, für die Basisimplementierung und die Parametrisierung auf der Basis der definierten GRC-Methodik belaufen sich meist auf einen Umfang von rund dreißig Softwareberatertagen. Zudem entstehen Integrationsaufwände für die IT (denen durch die Wiederverwendung vorhandener Basisdienste aber i. d. R. geringere Lizenzkosten gegenüberstehen). Eine Individualprogrammierung ist i. d. R. nicht notwendig.

- Schließlich sind Administrationsaufwände zu berücksichtigen, die zum großen Teil durch die jeweils verantwortliche Abteilungen im Rahmen ihrer operativen Aufgaben durchgeführt werden sollten sowie typischerweise geringe Aufwände der IT-Abteilung im Rahmen des Supportkonzeptes.

Die tatsächlich erforderlichen Investitionen und laufenden Kosten liegen bei derartigen Projekten in aller Regel weit unter den typischen Erwartungen, die sich eher an den teuren ERP-Lösungen orientieren. Vor dem Hintergrund der wirtschaftlichen und organisatorischen Vorteile und der positiven Innen- und Außenwirkung rechnet sich für viele Unternehmen daher die Einführung einer GRC-Software.

6 Fazit

Viele Unternehmen schrecken vor den (tatsächlich allerdings relativ moderaten) Aufwänden und dem Veränderungsprozess einer GRC-Softwareeinführung zurück, vergessen aber die Gesamtkosten ihrer heutigen Excel-basierten-Lösungen zu reflektieren. Im Total-Cost-of-Ownership-Vergleich schneidet eine GRC-Software in der Regel signifikant besser ab. Zusätzlich bietet eine GRC-Software noch wesentliche qualitative Vorteile und die Möglichkeit der schrittweisen Integration weiterer Managementsysteme. Als Alleinstellung gegenüber den vergangenheitsorientierten Dokumentationswerkzeugen (wie Excel) können Unternehmen wesentlichen Mehrwert durch den Einsatz einer umfassenden GRC-Software-Lösung als zukunftsorientiertes, strategisches Steuerungsinstrument erzielen – vorausgesetzt, es existiert eine „smarte“ und firmenspezifische GRC-Methodik. Dokumentationslösungen zementieren dagegen nur die Bürokratie und den Blick nach hinten.

Als kritische Erfolgsfaktoren eines GRC(-Software-Auswahl)-Projektes sind erfahrungsgemäß die folgenden Punkte zu nennen:

- Die Qualität, einer umfassenden und von allen Betroffenen getragenen Projektdefinition,
- die gesamthafte Wirtschaftlichkeitsbetrachtung,
- das strukturierte, erfahrungsbasierte Projekt- und Softwareauswahlvorgehen,
- die auf dem Zielumfang einzubeziehender Managementsysteme basierende unternehmensspezifische und ausformulierte GRC-Methodik,
- die Definition der Ziel-GRC-IT-Architektur und der damit verbundenen Anforderungen,
- die Kenntnis des Softwaremarktes (Produkte und Implementierungen) sowie
- die schrittweise Einführung.

Auch Rom wurde nicht an einem Tag erschaffen. Einer schrittweisen Umsetzung sollte allerdings eine gute Konzeption zugrunde liegen, um erfolgreich zu werden. Erfahrungsgemäß macht sich dies am langen Ende sehr bezahlt.

Autoren:

Stephan Haupt *und* ***Hans-Joachim Müncheberg*** *sind Geschäftsführer des auf die Integration von Managementsystemen fokussierten Beratungsunternehmens Caniu GRC (www.caniu.com).*