GRC – von der Theorie zur Praxis

Prozesse für Governance, Risk & Compliance (GRC) umzusetzen bleibt für viele Unternehmen trotz Softwareunterstützung eine Herausforderung. Nachfolgend einige wichtige Ansatzpunkte, wie Sie dafür Ihr Internes Kontrollsystem (IKS) effizienter machen können.

Unternehmensskandale und Wirtschaftskrisen haben in vielen Ländern zu strengeren Vorgaben an interne Kontrollsysteme (IKS) geführt. Angelehnt an Referenzmodelle wie COSO oder COBIT etablierten viele Unternehmen im vorigen Jahrzehnt Compliance-Management-Abläufe, um den gesetzlichen Anforderungen an die Zuverlässigkeit der externen Finanzberichterstattung gerecht zu werden. Heute gehören die drei Buchstaben GRC (Governance, Risk & Compliance) zum Wortschatz der Top-Führungsetagen und finden sich auf jeder CFO-Agenda.

In der Praxis wurden IKS-Prozesse meist manuell gepflegt, was sich als ressourcenintensiv und teuer herausstellte. Daher wurde der Ruf nach einer Automatisierung immer lauter, was zunehmend die Softwareanbieter auf den Plan rief. Mittlerweile propagieren sie eine gesamtheitliche GRC-Automatisierung, die durch ihre Angebote möglich sein soll. Doch diese Idee bleibt leider für viele Unternehmen genauso verlockend wie abstrakt.

Nachfolgend daher die wichtigsten Punkte, wie und wo Sie die Automatisierung verstärken und eine höhere Effizienz Ihrer Abläufe erzielen können:

Am besten lässt sich das Konzept der GRC-Automatisierung erklären, wenn man zwei Sichtweisen darauf abstrahiert, die es in einer softwaregestützten Lösung zusammenzuführen gilt: inhaltliche Sicht (Content) und Prozesssicht.

Inhalte im IKS

Mit Inhalten sind alle Elemente eines IKS-Frameworks gemeint (zum Beispiel Prozesse, Risiken, Kontrollen oder Sachkonten), die oft in einer Risiko- und Kontrollmatrix zusammengefasst werden. Content zu automatisieren bedeutet in erster Linie, dass dank einer einheitlichen Struktur und dank wiederverwendbarer Elemente – zentralisierte Dokumentationsvorlagen, parallele Benutzung mehrerer IKS-Dimensionen, etwa für Compliance und operationelle Kontrollen, Abbildung von Shared Services – der Verwaltungsaufwand verringert werden kann. Und es gibt noch weitere Vorteile: Der Zugriff auf die einzelnen Elemente ist berechtigungsgesteuert, Änderungen an ihnen werden protokolliert und gehen in die Berichterstattung ein.

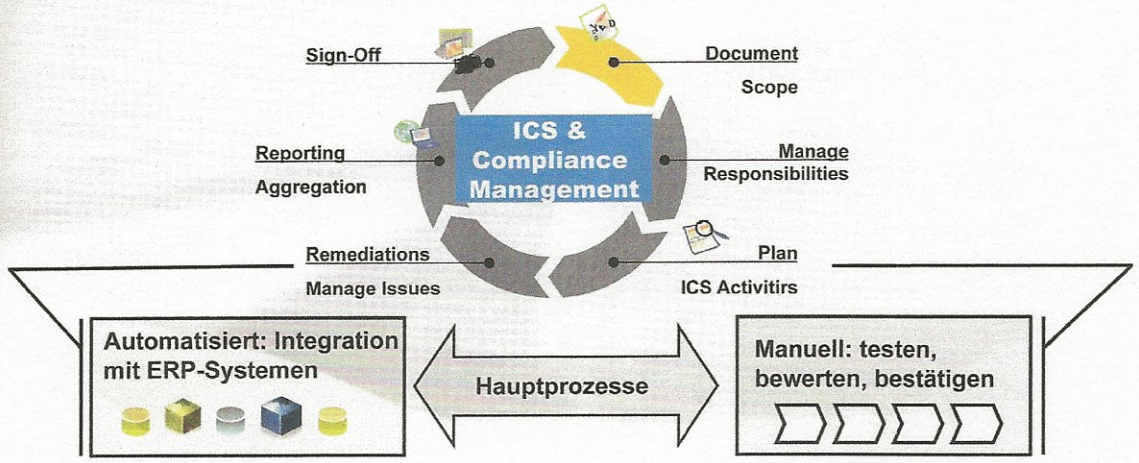
Prozesse im IKS

Aus Sicht der Prozesse geht es primär um diverse Aktivitäten, die auf einzelne Elemente eines IKS-Frameworks angewendet werden (Abb. 1).

Die Hauptaktivitäten bilden eine Vielzahl wiederkehrender, manueller IKS-Vorgänge wie die Bestätigung der Kontrolldurchführung, Designbewertung und Effektivitätstest. Die manuellen IKS-Vorgänge zu automatisieren bedeutet vor allem deren einfache und intuitive Handhabung, vorgegebene Abläufe sowie automatisierte Benachrichtigungen und Erinnerungen; ferner können die Vorgänge effizienter geplant werden. Bei automatisierten Prozessen lassen sich außerdem die Aktivitätsergebnisse elektronisch speichern, was die Berichterstattung beschleunigt

Zu den größten Effizienztreibern im IKS-Prozess gehören allerdings die automatisierten Test- und Überwachungsszenarien (auch als Continuous-Contro-Monitoring-Ansatz bezeichnet). Dabei identifiziert ein mit Business-Anwendungen integriertes GRC-System automatisch Abweichungen vom

Abb. 1: IKS-Prozess als Abfolge diverser Aktivitäten



Quelle: Chuprunov

Soll-Zustand, indem Stamm-, Bewegungs- und Steuerungsdaten sowie Änderungsprotokolle nach bestimmten Regeln ausgewertet werden.

Zusammengefasst lassen sich die Hauptmerkmale eines automatisierten IKS-Managements wie folgt darstellen:

Automatisiertes IKS-Management: Effizienztreiber	
Inhalt	*Wertanalyse*
1. Einsatz zentraler Referenzkataloge & Vorlagen für Framework-Elemente (Kontrollen, Risiken etc.)	1. Einfache & intuitive Handhabung (z.B. Workflow-basiert)
2. Mehrere Framework-Dimensionen (z.B. US-SOX-Compliance, Wirtschaftlichkeit, FDA-Compliance)	2. Continuous Compliance Monitoring (manuelle Auswertungen fallen weg)
3. Shared-Services-Konzept	3. Dokumentation wird online aufbewahrt („Supporting Evidence")
	4. Aktuelle Berichte auf Knopfdruck (kein Konsolidierungsaufwand)

Nachfolgend weitere Bausteine, mit denen Sie automatisierte IKS-Prozesse noch mehr in Richtung GRC ausbauen können:

A. Zugriffsberechtigungen

Auch wenn Kontrollen in Geschäftsprozessen und Zugriffsberechtigungen aus der IKS-Sicht ein einheitliches Gerüst bilden sollen, so stellen diese zwei Bereiche in der Praxis oft eigenständige Domänen dar. Der Grund ist vor allem organisatorischer Natur: Die Zugriffsberechtigungen werden üblicherweise in der IT verwaltet.

Die GRC-Automatisierung bei der Benutzer- und Berechtigungsverwaltung besteht deswegen vorwiegend darin, die operativen Prozesse IKS-konform zu gestalten und mit zusätzlichen IKS-relevanten Aktivitäten anzureichern. Dies sind zum Beispiel:

- die Analyse bestehender sowie Simulation potenzieller Funktionstrennungskonflikte (engl. Segregation of Duties – SOD);
- die Genehmigung der Vergabe von Berechtigungen.

In den meisten Fällen wird der Prozess der Zugriffsberechtigungen schneller und zuverlässiger.

Zusammenfassend lassen sich die folgenden wichtigsten Elemente bei der GRC-Integration von Benutzer- und Berechtigungsverwaltung hervorheben:

Benutzer- und Berechtigungsverwaltung als GRC-Bestandteil	
Inhalt	*Prozess*
1. IKS-Integriertes Datenmodell (berechtigungsspezifische Prozesse, Risiken & Kontrollen)	1. Integration der IKS-Aktivitäten in operative Prozesse (z.B. Antrags- und Genehmigungsverfahren, Risikoanalyse, Audit Trail)
2. Aktive Rolle von Kontrollen für Mitigationszwecke (Nutzung bestehender Kontrollen zum Minimieren der SoD-Risiken)	2. Intuitive Analyse der vergebenen Berechtigungen (z.B. mittels Workflows)
	3. Automatisierung des Notfallbenutzerkonzepts

B. Richtlinienverwaltung und Risikomanagement

Richtlinienverwaltung und Risikomanagement sind weitere Hauptelemente von GRC-Funktionen im Unternehmen. Die Richtlinienverwaltung ist ein eigenständiger Prozess, und seine Automatisierung bedeutet in erster Linie, den gesamten Lebenszyklus einer Richtlinie effizient zu gestalten. Aus IKS-Sicht können Richtlinien jedoch auch als wichtige Kontrollmechanismen angesehen werden, deswegen ist an dieser Stelle eine Integration mit dem IKS-Framework erforderlich. Außerdem sind Integrationsmöglichkeiten mit Risikomanagement interessant, wenn weitere GRC-Bausteine berücksichtigt werden. So tragen wirksame Richtlinien aktiv dazu bei, das Risiko zu minimieren.

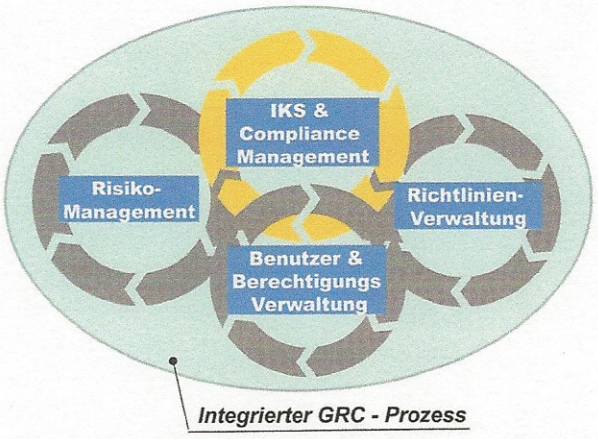
Richtlinienmanagement als GRC-Bestandteil	
Inhalt	*Prozess*
1. Zentrales Repository aller Richtlinien, einschließlich Versionsmanagement etc. 2. Integriertes Datenmodell (Verlinkung einzelner Richtlinien mit dem IKS-Framework) 3. Aktive Verwendung von Richtlinien im Risikomanagement (z.B. Risikoreduktion) und im Berechtigungswesen (Mitigation fehlender Funktionstrennung)	1. Workflow-gestützter Lebenszyklus (Entwurf, Review, Genehmigung, Veröffentlichung) 2. Verteilung der Richtlinien an Endanwender (u.a. formelle Kenntnisnahme festhalten, Einhaltung bestätigen)

C. Risikomanagement

Betrachtet man das Risikomanagement im Kontext integrierter GRC-Prozesse, so gibt es weitere Synergieeffekte: Einerseits spielen Risiken eine wichtige Rolle im IKS, andererseits werden sie je nach Ebene (strategisch versus operativ) direkt in diverse Abläufe im Rahmen des Risk-Management-Prozesses einbezogen. Aus der eingangs erwähnten Inhalts- und Prozessperspektive lassen sich die wichtigsten Integrationspunkte von Risiko- und IKS-Management wie folgt zusammenfassen:

Risikomanagement (RM) als GRC-Bestandteil	
Inhalt	*Prozess*
1. Integriertes Datenmodell (z.B. Möglichkeit, gleiche Risiken, Organisations- und Prozessstruktur in RM und IKS) 2. „Aktive" Rolle von Kontrollen und Richtlinien in RM, um Risiken zu minimieren.	1. Wiederverwendung der Ergebnisse RM-relevanter Aktivitäten aus IKS (z.B. Scoping und Kontrolltests) 2. Wiederverwendung relevanter RM-Ergebnisse an das IKS-Management (z.B. qualitative Risikobewertung)

Abb. 2: Elemente eines integrierten GRC-Prozesses



Quelle: Chuprunov

Die dargestellte Vorgehensweise für die GRC-Automatisierung, bei der vier wichtige Elemente in sich geschlossene Prozesse darstellen, aber auch genügend Integrationspunkte anbieten, um von einem gesamtheitlichen GRC-Ansatz sprechen zu können, ist keinesfalls reine Theorie mehr. So bietet beispielsweise SAP eine „GRC Suite" (v. 10) an, deren Aufbau der Darstellung oben entspricht (Abb. 2).

Anders als integrierte softwaregestützte GRC-Prozesse ist die Verbindung von GRC mit Themen wie Strategie- und Performance-Management noch Zukunftsmusik, doch wird auch daran bereits gearbeitet.

Maxim Chuprunov

ist Geschäftsführer der Schweizer RISCOMP GmbH. Zuvor war er viele Jahre bei KPMG und SAP. Vor Kurzem ist von ihm ein umfassendes Handbuch erschienen, das vom Konzept bis zur Automatisierung eines IKS sämtliche Fragestellungen adressiert:

SAP PRESS
672 S., 2011, geb.
ISBN 978-3-8362-1603-6