Governance, Risk und Compliance

Welche Unterstützung bieten GRC-Tools?

Im Auftrag vom Netzwerk Risikomanagement untersuchte die Studentin Nicole Greter in ihrer Bachelorarbeit an der Hochschule Luzern – Wirtschaft Werkzeuge, welche die Funktionen von Governance, Risk und Compliance (GRC) abbilden. Nebst diesem Tool-Vergleich hat sie anhand einer Umfrage analysiert, welche Anforderungen seitens der Wirtschaft an die Werkzeuge effektiv gestellt werden.

Bettina Hübscher

Das Modell der «3-lines-of-defense» wird seit einigen Jahren auch aus regulatorischer Sicht explizit als Ansatz zur Einbettung der Risiko- und Kontrollfunktionen in ein ganzheitliches Governance-System propagiert. Zur Unterstützung der operativen Umsetzung gibt es diverse Tools auf dem Markt. Allerdings: Erbringen die Tools den Unternehmen einen effektiven Mehrwert? Welcher Ansatz funktioniert wie, und welche Punkte sind bei der Implementierung eines GRC-Werkzeugs zu beachten?

GRC-Ansatz

GRC beschreibt den funktionsübergreifenden Ansatz, bestehend aus Governance, Risk und Compliance. Eine mögliche, allerdings nicht allgemeine Definition lautet: «Governance, Risk & Compliance bezeichnet die kontinuierliche gesamthafte Betrachtung aller Funktionen einer Organisation, um rechtliche, finanzielle und Reputationsrisiken effektiv und effizient zu steuern».

Ein Beispiel einer Abbildung, welche die Verhältnisse zwischen den einzelnen Disziplinen aufzeigt, ist das «House of Governance». Dabei umfasst der GRC-Ansatz zusätzlich zu den titelgebenden Bereichen das interne Kontrollsystem und die interne Revision.

Durch das Konzept sollen Synergien der Bereiche genutzt und Ressourcen geschont werden. Die Integration kann sowohl horizontal als auch vertikal erfolgen. Bei der horizontalen Integration sollen die Bereiche Governance, Risk und Compliance vermehrt Synergien untereinander nutzen. Die vertikale Integration hingegen soll den GRC-Ansatz in bestehende Geschäftsprozesse einbinden. Welche Hilfestellung kann hier nun ein Tool bieten?

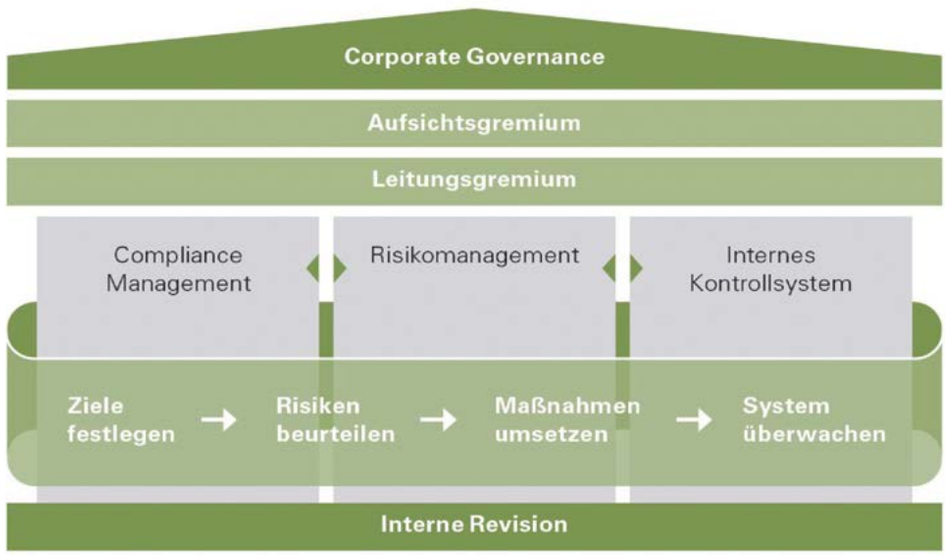
Eine GRC-Softwarelösung kann dabei unterstützend eingesetzt werden, um beispielsweise Meldungen zu erfassen sowie Analysen und Risikobewertungen (teil-)automatisiert durchzuführen. Dabei kann sie die Effizienz steigern und das Management unterstützen, die Beziehung zwischen Risiko- und Compliance-Management besser zu verstehen. Ausserdem kann sie helfen, die bestehende Komplexität zu verringern, indem Transparenz geschaffen wird sowie Mängel in den bestehenden Prozessen identifiziert und beseitigt werden.

Verbreitung und Anforderungen bei Schweizer Unternehmen

Eine Umfrage bei 60 Schweizer Unternehmen hat gezeigt, dass GRC-Tools inzwischen vor allem in Unternehmen mit mehr als 250 Mitarbeitenden weit verbreitet sind. So haben bereits 51,7 Prozent der Umfrageteilnehmenden eine Lösung im Einsatz und 20 Prozent eine Einführung geplant. Es bleibt hier zu vermerken, dass aufgrund der Corona-Pandemie nur 60 Unternehmen an der Umfrage teilgenommen haben und die Zahlen somit nur bedingt aussagekräftig sind.

Dabei zeigt sich bei der Nutzung der Tools ein Trend hin zu lokalen, deutschsprachigen Anbietern, obwohl internationale Anbieter einen höheren Bekanntheitsgrad aufweisen.

Die Anforderungen aus der Praxis an ein GRC-Tool sind vor allem die Grunddisziplinen von GRC: die Risikoidentifikation und Beurteilung, das interne Kontrollsystem (IKS) und das Compliance-Management. Als weitere Muss-Kriterien sollen verständliche und konsolidierte Reports erstellt werden können und das Tool eine hohe Benutzerfreundlichkeit aufweisen. Zudem muss der Anbieter einen effizienten Support leisten und, wenn gewünscht, benutzerdefinierte Anpassungsmöglichkeiten umsetzen können. Weitere ergänzende Funktionen wie Simulationen, Vertrags- oder Auditmanagement wurden in der Umfrage eher tief gewichtet.



Quelle: House of Governance, KPMG

Verwendung Tool nach Unternehmensgrösse

Anzahl

		Unternehmensgrösse				
		< 10 Mitarbeitende	10 - 100 Mitarbeitende	101 - 250 Mitarbeitende	> 250 Mitarbeitende	Gesamt
Verwendung Tool	Ja	3	4	2	22	31
	Nein, allerdings ist eine Einführung geplant	0	0	3	9	12
	Nein, eine Einführung ist auch nicht geplant	1	3	0	13	17
Gesamt		4	7	5	44	60

Quelle: Nicole Greter

Analyse von aktuellen GRC-Tools

Die Analyse von neun ausgewählten Tools hat ergeben, dass sämtliche analysierten Lösungen die vorgängig erwähnten Muss-Kriterien erfüllen. So kann mit jeder Lösung das interne Kontrollsystem abgebildet sowie eine Risikoidentifizierung vorgenommen werden. Zudem ist es möglich, benutzerdefinierte Berechtigungen zu vergeben. Bei den ergänzenden Funktionen gibt es allerdings grosse Unterschiede. Die kleineren Tools konzentrieren sich häufig auf die Kernfunktionen, während grössere Lösungen zusätzlich vertiefende Funktionen anbieten, welche sehr unterschiedlich und umfassend ausfallen können. Als Beispiele können hier Monte-Carlo-Simulationen, Vertragsmanagement oder auch die Hinterlegung von Standards wie ISO 9001 genannt werden. Automatisierte Workflows und Verknüpfungen zwischen den einzelnen Funktionen werden ebenfalls in sehr unterschiedlichem Umfang angeboten. Der Umfang hat jedoch einen Einfluss auf die Komplexität der Lösungen.

Ausserdem unterscheiden sich die Möglichkeiten der benutzerdefinierten Anpassungen stark. Grössere Ergänzungen und Anpassungen benötigen meistens vertiefte Kenntnisse oder IT-Unterstützung. Der Support durch die Anbieter wird sowohl in diesem Zusammenhang als auch allgemein als gut beschrieben und war bei den meisten Anwenderinnen und Anwendern ein wichtiges Auswahlkriterium. Dabei war den meisten Unternehmen ein regionaler und deutschsprachiger Support wichtig.

Bemängelt werden häufig die Standardberichte, welche gerade für die Erstellung von Reports zuhanden des Verwaltungsrates oder der Geschäftsleitung als unzureichend beschrieben werden. Alle interviewten Personen gaben hierbei an, entweder manuelle Anpassungen an den Berichten vorzunehmen oder eigene Vorlagen erstellt zu haben.

Tipps für die Einführung

Die Einführung eines GRC-Tools ist, wie jedes Projekt, ausführlich zu planen und erfolgt am besten schrittweise. Die gewünschten und auch in Zukunft benötigten Funktionen müssen im Voraus klar definiert werden. So soll festgelegt werden, ob zusätzliche Funktionen notwendig sind oder ob zugunsten der Einfachheit darauf verzichtet werden kann. Eine entscheidende Frage ist ausserdem, ob die entsprechenden IT-Ressourcen intern vorhanden sind oder ob man den Support des Anbieters in Anspruch nehmen muss. Dies hat wiederum einen Einfluss auf die Kosten. Auch benötigen grössere Tools hier aufgrund ihrer Komplexität mehr Ressourcen im Unternehmen.

Es gilt, alle Betroffenen zu Beteiligten im Auswahl- und Einführungsprozess zu machen, um so alle Bedürfnisse abzuholen und eine Unterstützung durch die Linie sicherzustellen. Es hat sich zudem gezeigt, dass es schwierig ist, eine Lösung abteilungsübergreifend einzuführen, wenn diese nicht organisatorisch zusammengefasst sind. Der GRC-Ansatz ist in der Folge zuerst in der Organisation umzusetzen, bevor das Tool eingeführt wird. Viele Unternehmen verwenden trotzdem eine GRC-Lösung, welche in der Folge nur von einer Abteilung (meist dem Risikomanagement) verwendet wird. Bei der Evaluierung sollten zuerst Softwarelösungen in anderen Abteilungen betrachtet werden. Viele Lösungen sind beispielsweise auch im Prozess- beziehungsweise Unternehmensmodellierungsmanagement einsetzbar und besonders für eine Verknüpfung innerhalb des Unternehmens geeignet. So können Ressourcen eingespart und Synergien genutzt werden.

«Bemängelt werden häufig die Standardberichte.»

Das Tool soll für die Mitarbeitenden einfach zu pflegen sein. Häufig wird ein GRC-Tool von vielen Risiko- und Kontrolleignerinnen benutzt, welche alle entsprechend instruiert werden müssen. So sollten die einzelnen Formulare zur Erfassung nicht überladen sein. Dafür muss im Vorhinein definiert werden, welche Informationen im Tool hinterlegt werden sollen und auf welche verzichtet werden kann. Dadurch kann auch sichergestellt werden, dass das Reporting einfach und kompakt daherkommt und damit die Transparenz und Effizienz bis zum Controlling hin gewährleistet ist. ■

Dieser Fachartikel erscheint in einer MQ-Serie, die von Expertinnen und Experten des «Netzwerk Risikomanagement» beigesteuert wird:

www.netzwerk-risikomanagement.ch

Literaturhinweis

Haupt, S. & Müncheberg, H.-J. (2012). Mehrwert durch GRC-Software statt Overhead durch Excel – Sicherheit bei der Auswahl von GRC-Software. Risk, Compliance & Audit 2012 (3), 17-23.

Otremba, S., & Wieland, J. (2016). GRC-Management als interdisziplinäre Corporate Governance: die Integration von Revision, Risiko- und Compliance-Management in Unternehmen. Wiesbaden: Springer Gabler.

Standke, F. (2010). Unternehmensweiter Ansatz einer Governance-, Risk und Compliance-Lösung. In Keuper, F. & Neumann, F. (Hrsg.). Corporate Governance, Risk Management und Compliance. Innovative Konzepte und Strategien (S. 269–290). Wiesbaden: Gabler Verlag.