Wolfgang Surrey

Corporate Governance, Risk & Compliance: Auf Nummer sicher gehen!

Ob Datenschutz oder Datensicherheit, IT-Risikomanagement, Audit Management oder der Umgang mit Lieferanten: Die Anforderungen von Aufsichtsbehörden und anderen interessierten Parteien an Sicherheit und Qualität von Geschäftsprozessen, Produkten und Services steigen – ebenso wie Anzahl und Komplexität der Risiken. Kein Wunder also, dass Unternehmen häufig Nachweise darüber erbringen müssen, dass sie die Standards, Normen und regulatorischen Auflagen sowie Vorschriften unter anderem im Bereich Informationssicherheit einhalten. Wie lassen sich Governance, Risk & Compliance, – kurz: GRC – professionell umsetzen?

Unternehmen müssen sich seit jeher mit verantwortungsvoller Unternehmensführung und dem Management von Risiken auseinandersetzen. Was früher mit den „Grundsätzen des ehrbaren Kaufmanns" umschrieben wurde und heute mit dem Akronym GRC (Governance, Risk & Compliance, siehe Kasten) besetzt ist, gestaltet sich inzwischen deutlich komplexer. Auf europäischer Ebene greift bis Mitte 2018 die EU-Datenschutzgrundverordnung (EU-DGSVO), mit denen sich Unternehmen unterschiedlichster Branchen konfrontiert sehen. Bei den Betreibern kritischer Infrastrukturen, z. B. in den Bereichen Energie- und Wasserversorgung oder Telekommunikation, ist es heute schon das IT-Sicherheitsgesetz, das auch für das Banken- und Finanzwesen gilt. Diese Branche ist außerdem von der Ende 2016 anstehenden Novelle der Mindestanforderungen an das Risikomanagement, kurz MaRisk, betroffen.

All diese neuen Richtlinien und Novellen bergen Pflichten, die einen erheblichen Einfluss auf die Steuerung der Cyber-Sicherheit haben werden. Hinzu kommen weitere industrie- und branchenspezifische Standards, Regularien und Vorschriften.

Ein professionelles GRC-Management ermöglicht eine integrierte Herangehensweise, um diese Komplexität zu beherrschen: Es erlaubt eine ganzheitliche Sicht auf das Unternehmen, die alle Managementsysteme und Maßnahmen im Fokus hat. Das Ergebnis ist eine verbesserte Steuerung von Informationssicherheitsmanagement, IT-Risikomanagement sowie IT-Compliance, um die unterschiedlichen Anforderungen an das aktive Risikomanagement und den geforderten Reportings bzw. Berichtspflichten effizient nachkommen zu können.

➜ Tool-Unterstützung: ja oder nein?

Was macht professionelles GRC-Management aus? Es basiert auf einer objektiven Analyse der Unternehmenssituation. Die Umsetzung erfolgt auf strategischer, taktischer und operativer Ebene, die Prozesslandschaft ist belastbar und stimmig. Eine Unterstützung durch eine darauf spezialisierte Management-Softwarelösung ist nicht zwingend, ab einer gewissen Größenordnung oder Geschäftsmodell des Unternehmens nahezu unverzichtbar. Möglicherweise fällt die Entscheidung dafür nach einer Wirtschaftsprüfung, bei der die Revisionssicherheit des Risikomanagements angezweifelt wird, z. B. weil Inkonsistenzen im Berichtswesen bestehen, die sich nicht kurzfristig konsolidieren lassen. Auch die Ausweitung der Geschäftsaktivitäten in die USA hinein, wo etwaige Compliance-Verstöße teils drastisch geahndet werden, kann ein wichtiger Grund sein, sich weiter zu professionalisieren.

Mit GRC-Software lassen sich manuelle Prozesse effizienter gestalten, Informationen aus verschiedenen Quellen sinnvoll zusammenführen und mit dem eigentlichen Unternehmenskontext in Verbindung bringen. Das bedeutet: Im Rahmen eines risikozentrierten Ansatzes lassen sich die einzelnen Informationen nur dann sinnvoll auf ihre Kritikalität für das Unternehmen beurteilen, wenn sie sich im Zusammenhang mit für das Unternehmen wesentlichen Geschäftsprozessen, damit verbundenen Produkten oder Services, Anwendungen, Standorten etc. betrachten lassen.

Allerdings sollte man nicht dem Irrtum erliegen, verantwortliche Unternehmensführung und unternehmensweites Risikomanagement ließen sich so per Knopfdruck erledigen. Das Unternehmen muss im Vorfeld definieren, welchen internen und externen Vorschriften es unterliegt und welche Workflows am besten in die Abläufe des Unternehmens passen. Mit einem toolgestützten Ansatz verbessern sich Nachvollziehbarkeit und Auswertbarkeit von Informationen erheblich – und damit auch die Steuerungsmöglichkeiten innerhalb des Risikomanagements, selbst wenn Compliance-Anforderungen einem schnellen Wandel unterliegen.

➜ Technologiemanagement: die Auswahl der GRC-Software

Wer sich einen ersten Überblick verschaffen will, wirft am besten einen Blick in die Produktübersichten von Analysten wie Forrester und Gartner. In Rahmen eines Ausschreibungsverfahrens sollten Unternehmen ihre funktionalen und technischen Anforderungen an die Managementsoftware-Lösung definieren. Dabei kommt es darauf an, dass die Technologie nicht nur in der Lage ist, die aktuelle Situation abzubilden, sondern „mitzuwachsen", um auch künftigen Anforderungen gerecht zu werden. Darüber hinaus liefern die Analysten auch wertvolle Informationen über die Stärken und Schwächen der hinter der Software-Lösung stehenden Anbieter und deren Strategien, um den Kunden langfristig und mit ausreichender „Manpower" mit notwendigen Services rund um die gewählte GRC-Lösung lokal zu betreuen. Genau anschauen sollte man sich, ob es ein funktionierendes Partnernetzwerk oder eine regionale Präsenz gibt, die über das Vorhandensein eines Vertriebsansprechpartners hinausgeht.

Die Einführung eines nachhaltigen GRC-Managements

GRC-Management: Sechs Tipps für die Praxis

1. *Das Unternehmen sollte schrittweise vorgehen und sich nicht zu viel vornehmen, sondern zunächst einmal nach Quick Wins streben und zwar anhand von ein bis zwei Fragestellungen hoher Priorität, also zum Beispiel das Messen der Lieferantenperformance anhand einheitlicher Metriken oder das zentrale Nachverfolgen von Feststellungen. Stellen sich hier schnell Erfolgserlebnisse ein, ist der Projektsponsor auch eher geneigt, weitere Budgets freizugeben. Startet das Projekt mit einer zu hohen Komplexität, droht sich das Team schnell zu verzetteln, der Fortgang des Projekts kann gefährdet sein.*
2. *Es ist wichtig von Beginn an abzuwägen, wie viele Abteilungen direkt involviert sind. Die Integration von zu vielen Abteilungen bedeutet eine entsprechende Multiplikation von Individualanforderungen, die unter Umständen schwer miteinander zu harmonisieren sind, insbesondere, wenn die Gesamthoheit über die fachliche Projektsteuerung nicht geklärt und in der Organisation verankert wurde.*
3. *Von hoher Bedeutung ist die Vorbereitung der prozessualen Seite: Wie sieht der Implementierungsprozess aus? Wer ist verantwortlich? Welche Vorarbeiten muss das Unternehmen leisten, z. B. mit der Definition branchenrelevanter Use Cases.*
4. *Zentral sind personelle Fragen, die das Unternehmen kritisch und ehrlich beantworten sollte: Wer ist der Lösungseigentümer, eine einzelne Person, eine Abteilung oder Gruppe, und müsste diese ggf. organisatorisch eingebettet werden, um über die notwendige Weisungsbefugnis zu verfügen? Wie geht es nach der Implementierung weiter, sind wir intern in der Lage, den Support zu leisten? Verfügen wir heute und zukünftig über die technische Expertise, um die Lösung gemäß unseren Anforderungen weiterzuentwickeln? Der oder die Lösungseigentümer sollten in ausreichendem Maße einen Teil ihrer Arbeitszeit der Pflege und Weiterentwicklung der GRC-Softwarelösung widmen können und ein Mindestmaß an „Tool-Affinität" aufweisen. Dies beinhaltet auch weniger fachliche Aufgaben wie die Einrichtung von User-Accounts über Rollen- und Berechtigungsvergaben bis hin zur Prüfung der Berichtsqualität und gegebenenfalls 1st Level Support für Endbenutzeranfragen und Troubleshooting.*
5. *Wer dieses Personal nicht im Hause hat, oder organisatorisch nicht sicherstellen kann, dass das Wissen und die Kompetenz rund um die GRC-Lösung nachhaltig gesichert werden kann, sollte dies bereits bei der Wahl des Implementierungspartners berücksichtigen und darauf achten, dass diese Funktionen nach Bedarf an den Partner ausgelagert werden können. Sich allein auf den Helpdesk des Herstellers zu verlassen, ist riskant. Oft mangelt es diesen Support-Abteilungen am fachlichen Verständnis für die teilweise stark angepassten Kundenlösungen (nicht zu sprechen von erheblichen sprachlichen Barrieren internationaler Support-Organisationen), was zu erheblichem Aufwand bei der Fehlersuche und -beseitigung führt.*
6. *Sind mehrere Abteilungen involviert, ist es wichtig, sich methodisch auf eine gemeinsame Taxonomie zu einigen, um Sprachverwirrung zu vermeiden. Ist beispielsweise das „Issue" aus dem internen Kontrollsystem gleich der „Feststellung" der internen Revision? Abzustimmen sind bei der Integration mehrerer Abteilungen auch die methodischen Herangehensweisen an bestimmte Aufgaben oder der jeweils erforderliche Detailgrad an Informationen im Berichtswesen.*

Denn ein Tool ohne Experten, die die Anwendung fachmännisch und zweckmäßig einrichten können, ist nahezu wertlos. Experten müssen nicht nur „theoretisch" verfügbar sein, sondern praktisch für den Kunden da sein.

Die Implementierung – externes Know-how hinzuziehen?

Einführung und Betrieb eines GRC-Managements sollten Unternehmen nicht unterschätzen, geht es hier doch nicht nur um die Einführung und Anpassung einer Software, sondern auch um das Prozessdesign, das nicht selten mit einem Change-Management verbunden ist. Ist kein lösungsspezifisches Know-how vorhanden, lässt es sich mit dem richtigen Partner im Team relativ schnell aufbauen. Die frühzeitige Einbindung eines externen Partners kann auch dann zweckmäßig sein, wenn man sich die Möglichkeit offenhalten möchte, die fachliche und/oder technische Betriebsverantwortung für das GRC-System teilweise oder ganz auszulagern.

Doch wie findet sich ein geeigneter Partner für das GRC-Implementierungsprojekt? Entscheidend für die Partnerwahl sind im Wesentlichen die beiden Faktoren Beratungskompetenz und Verfügbarkeit. Dabei sollte die Beratungskompetenz eine gute Balance aufweisen zwischen fachlichem Verständnis und technischer Umsetzungserfahrung mit der bevorzugten GRC-Lösung. Der Faktor Verfügbarkeit beinhaltet sowohl die regionale Vorschriftenkenntnis des Partners sowie eine größere Flexibilität und Kompetenz durch ein im Bedarfsfalle internationales Team und die zeitliche Verfügbarkeit kompetenter Berater in erforderlichem Umfang. Solche Partner sind in der Lage, ein Implementierungsprojekt (kosten-)effizient und ausgerichtet an die Compliance-Anforderungen des Kunden abzuliefern. Nicht zuletzt sprechen sie die „Sprache des Kunden".

Der Autor

Wolfgang Surrey ist ausgewiesener Experte für die Implementierung von GRC-Management-Lösungen. Nach einer mehrjährigen Tätigkeit auf Herstellerseite ist er seit 2015 bei TÜV Rheinland als Management Security Consultant tätig und berät Unternehmen unterschiedlichster Größenordnung darin, wie sie Governance, Risk & Compliance professionell steuern.

✉ *surrey@wissensmanagement.net*