Warum professionelles GRC-Management heute wichtiger ist denn je

Corporate Governance, Risk & Compliance

Die Anforderungen von Aufsichtsbehörden an Sicherheit und Qualität von Geschäftsprozessen, Produkten und Services steigen – ebenso wie Anzahl und Komplexität der Risiken. Unternehmen müssen Nachweise darüber erbringen, dass sie die Standards, Normen, regulatorischen Auflagen und Vorschriften einhalten. Wolfgang Surrey, Experte für GRC-Lösungen bei TÜV Rheinland, erläutert in der dreiteiligen Serie zum Thema Governance, Risk & Compliance (GRC) Erfolgsfaktoren für die Implementierung. Teil 1 der Artikelserie geht auf die hohe Bedeutung von professionellem GRC-Management ein.

Professionelles GRC-Management ermöglicht eine ganzheitliche Sicht auf das Unternehmen.

Bild: © Artystarty/photodune.net

Trotz stetig wachsender Bedeutung und Komplexität regulatorischer Anforderungen verpassen viele Unternehmen die Chance, sich durch Professionalisierung ihrer Risikomanagement- und Compliance-Prozesse Wettbewerbsvorteile zu sichern. Mitunter definieren sie IT-Risiken nicht, und wenn doch, dann verwalten sie sie per Lose-Blatt-Sammlung oder Excel. Einen zentral Verantwortlichen, der Daten aus Risikomanagement, Business Continuity oder auch Netzwerk-Logdaten regelmäßig nachhält, konsolidiert und daraus die richtigen Schlüsse für den Bereich Informationssicherheit und IT-Compliance zieht, gibt es bisher nur selten. Und wenn doch, dann erfolgt die Analyse von Kennzahlen nicht mit integrierten Softwarelösungen. Eine vernetzte und unternehmensweite Analyse und ein zentrales Reporting finden nicht statt. Daraus resultiert eine erhöhte Verwundbarkeit gegenüber Cyber-Angriffen. Sicherheitsvorfälle werden ad hoc bearbeitet, wenn sie denn auffallen. Lösungen, die Cyber-Angriffe erkennen, sind aber nicht implementiert oder liefern unzureichende Informationen über die eigentliche Geschäftskritikalität des Vorfalles. Dieses punktuelle Management von nicht oder nur unzureichend integrierten GRC-Prozessen bedeutet einen erheblichen Mehraufwand durch redundante Tätigkeiten und sich teils widersprechenden Aussagen im Management Reporting. Die fehlende Übersicht und der mangelnde Bezug zum Unternehmenskontext machen es für das Management unmöglich, angemessene Entscheidungen abzuleiten und die richtigen Prioritäten zur Steuerung von Unternehmensrisiken zu setzen. Als potentielle Konsequenz drohen nicht nur empfindliche Strafen. Nicht erkannte oder falsch eingeschätzte Risiken aus Cyber-Angriffen oder die Nichteinhaltung von Service Level Agreements (SLA) ziehen mitunter schwerwiegende Folgen wie einen Betriebsausfall bis hin zur Gefährdung der kompletten Existenz des Unternehmens nach sich.

IT-Sicherheitsgesetz, MaRisk, EU-DGSVO

Unternehmen sind schon immer gehalten, sich mit verantwortungsvoller Unternehmensführung und dem Management von Risiken auseinanderzusetzen. Auf europäischer Ebene greift bis Mitte 2018 die EU-Datenschutzgrundverordnung (EU-DGSVO), mit der sich unterschiedliche Unternehmen 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. Die neuen Richtlinien und Novellen beinhalten Pflichten, die Einfluss auf die Steuerung der Cyber-Sicherheit haben. Hinzu kommen industrie- und branchenspezifische Standards, Regularien und Vorschriften. Professionelles GRC-Management ermöglicht eine integrierte Herangehensweise, um die Komplexität zu beherrschen: Es erlaubt die ganzheitliche Sicht auf das Unternehmen. 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 nachzukommen. Teil 2 der Artikelserie in Ausgabe 1+2/2017 des SPS-MAGAZINs beschäftigt sich mit der Frage: Tool-Unterstützung: ja oder nein? ■

Autor: ***Wolfgang Surrey,***
Management Security Consultant und GRC-Experte,
TÜV Rheinland i-sec
www.tuv.com/grc

Auszug aus dem SPS-MAGAZIN, Fachzeitschrift für Automatisierungstechnik, Ausgabe 4/2016.