IT Governance

IT-Governance, Risk & Compliance Management

Die Erwartungen an eine gute, transparente Unternehmensführung sind durch die Stakeholder, aber auch durch neue Vorschriften, Regeln und Standards gestiegen. Unternehmen haben daher in den vergangenen Jahren ihre IT-Risiko-Management-, IT-Compliance- und IT-Governance-Systeme entsprechend anpassen müssen und stehen vor neuen Herausforderungen. Im Rahmen unseres IT-Governance-, IT-Risiko- und IT-Compliance-Managements unterstützen Sie unsere Berater, damit Sie die Vorschriften dauerhaft effizient erfüllen können und so entscheidende Wettbewerbsvorteile erzielen.

IT-Governance-, IT-Risiko- und IT-Compliance-Management

IT-Governance-, IT-Risiko- und IT-Compliance-Management (IT-GRCM) sind drei wichtige Handlungsfelder eines Unternehmens, die sehr eng miteinander verbunden sind. Jedes Unternehmen sollte „seine" Risiken genau kennen und geeignete Antworten auf diese definieren. Dabei sind die Risiken eines Unternehmens so vielfältig und heterogen, wie es auch die möglichen Geschäftsmodelle sind. Ein methodisch sauberer und dabei aber pragmatisch handhabbarer Umgang mit diesen Risiken stellt viele Firmen noch immer vor große Herausforderungen. Hierbei sind externe und interne Regularien sowie die Grundlagen der Compliance der unverrückbare Rahmen jeden Handelns des Unternehmens. Diese Regularien fordern ein aktives und nachvollziehbares Risikomanagement und lassen dennoch auch neue Gefahren in der Compliance entstehen.

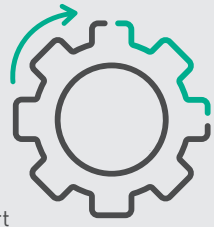
Alle Verantwortungsträger müssen jederzeit die geltenden Regularien kennen und ihre Einhaltung muss nachvollziehbar gewährleistet sein.

Das erfordert eine klare Vorgabe der Unternehmensführung, auch im Sinne der Unternehmenskultur, der operativen Ziele und internen Richtlinien – kurz: eine gute Governance. Diese darf aber keinesfalls losgelöst von dem täglichen Handeln und Entscheiden gelebt werden. Sie muss sich in ihrer Existenz und Bedeutung in jedem Teil der unternehmerischen Tätigkeit transparent und umfassend darstellen.

Wer einen dieser drei Bereiche vernachlässigt, setzt sich und sein Unternehmen zusätzlichen Risiken sowie existenzbedrohenden Situationen aus.

IT-Compliance

beschreibt die Einhaltung der gesetzlichen und vertraglichen Regelungen, denen ein Unternehmen unterliegt. Hierfür müssen geeignete Verfahren zur Definition, Umsetzung und Kontrolle integriert werden, die es externen Prüfern ermöglichen, die Effektivität der getroffenen Maßnahmen zu untersuchen.



IT-Governance

beinhaltet die verantwortungsvolle, kennzahlentreue, ethische und gesetzeskonforme Leitung und Steuerung des Unternehmens. Wichtigstes Ziel ist dabei die Erlangung einer langfristigen Wertschöpfung und Steigerung des Unternehmenswertes.

IT-Risiko-Management

analysiert, bewertet und kompensiert Risiken unter Berücksichtigung von Unternehmenszielen. Das Risikomanagement umfasst die Identifikation und Dokumentation von Risiken, die Risikoanalyse, die Bewertung der Risiken sowie die kontinuierliche Überwachung der Maßnahmen.

Abb. 1: Zusammenspiel zwischen IT-Governance, IT-Risiko-Management und IT-Compliance

Die unterschiedlichen Vorschriften und Regularien, wie die 8. EU-Richtlinie, das Kreditwesengesetz, ISO 14971, ISO 27000 und ISO 31000, SOX, Corporate Governance Kodex, verlangen ausdrücklich ein System für das Risikomanagement und das „Interne Kontrollsystem" (IKS), am besten integriert in ein ganzheitliches Managementsystem.

Umsetzung von IT-GRCM im betrieblichen Alltag

Diese vielfältigen Regularien der IT oder der Infrastruktur, ergänzt um andere Initiativen zum Schutz vor unerwünschten Ereignissen in den geschäftlichen Tätigkeiten und Abläufen, führen derzeit oft ein isoliertes Eigenleben und sind nicht auf einer stabilen sowie strukturierten Informationsplattform aufgebaut. Denn es fehlt eine operative Unterstützung, die sehr unterschiedliche Anforderungen erfüllen muss:

- Erfüllung diverser methodischer Anforderungen
- Berücksichtigung der organisatorischen Verteilung der Aufgaben
- Es muss eine stabile, performante, sichere und den modernen Ansprüchen an ein Managementsystem entsprechende Infrastruktur vorhanden sein.

Prozesse als Bindeglied

Dabei ist die Bewertung von Risiken und Regularien immer vor dem Hintergrund der betrieblichen Tätigkeit sowie Strategie zu bewerten. Regularien, Risiken, Kontrollen und Maßnahmen sind Teil des IT-GRCM-Prozesses. Sie lösen ihrerseits Prozesse aus und wirken direkt sowie indirekt auf die Geschäftsprozesse und die Organisation des Unternehmens, inklusive dessen Ressourcen und Ziele. Daher ist eine Betrachtung dieser Elemente ohne eine Prozessperspektive nicht zielführend. Die Überwachung und Steuerung der Risiken, Ereignisse sowie Kontrollen müssen die Geschäftsprozesse berücksichtigen, auf die sie wirken und in denen sie stattfinden. Für ein erfolgreiches und effektives IT-GRCM wird daher eine integrierte, prozessbasierte und operative Lösung benötigt.

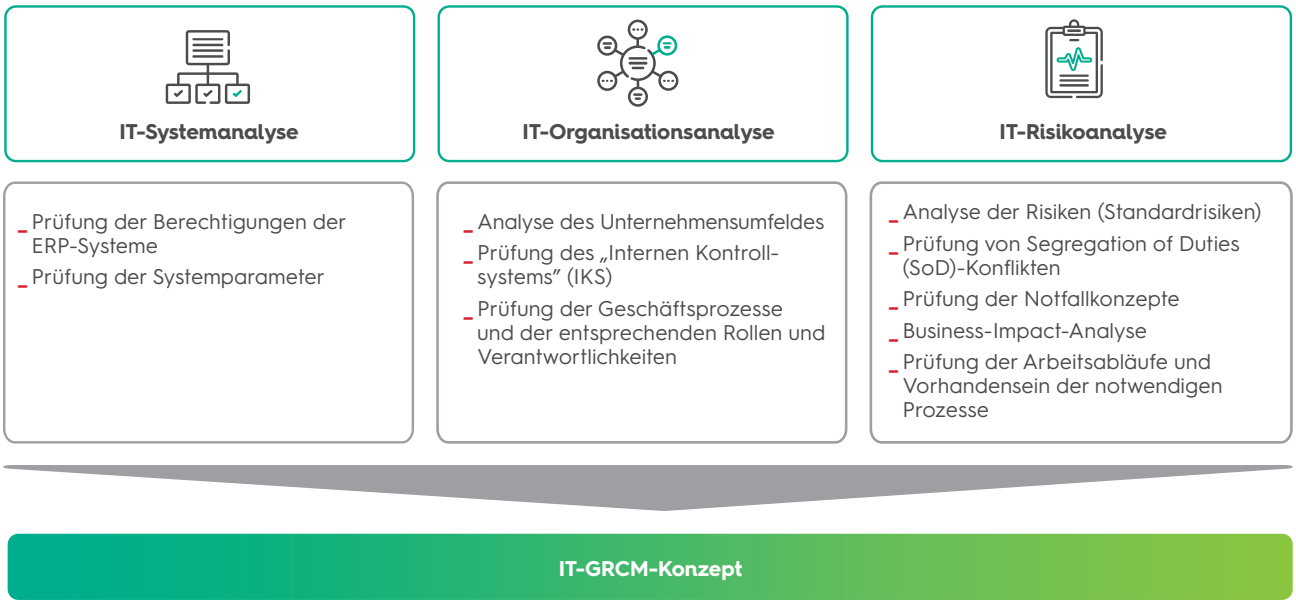


Abb. 2: Analyseschwerpunkte auf dem Weg zu einem unternehmensspezifischen IT-GRCM-Konzept

Unser Leistungs- und Serviceportfolio bietet ein einheitliches sowie integriertes Konzept für die Gestaltung von IT-GRCM

Wir bieten unseren Kunden ein breites IT-GRCM-Leistungs- und Serviceportfolio, um bestehende Schwachstellen zu identifizieren, Optimierungspotenziale aufzuzeigen sowie bereits bekannte Defizite zu korrigieren. Hauptmerkmale dabei sind:

IT-GRCM-Reifegradanalyse

Zur Bestimmung des aktuellen Status quo hinsichtlich externer und interner Einflussfaktoren (Unternehmensumfeld, IT-Risiken, IT-GRCM-Tools, Aufbau- und Ablauforganisation) haben wir eine Reifegradanalyse entwickelt, die eine Einschätzung hinsichtlich der Güte der IT-GRCM-Aktivitäten verschiedener Unternehmensebenen durch die Abbildung unternehmensinterner Stärken sowie Verbesserungspotenziale von IT-GRCM liefert. Aus IT-GRCM-fachlicher Sicht sind insbesondere die Themen Kultur, Integration, Transparenz/Kommunikation, Prozesse, Organisation und IT/Automatisierung beurteilungsrelevant. Das Ergebnis dieser Analyse ermöglicht die Messung der IT-GRCM-Reife der IT-Organisation und bietet einen optimalen Startpunkt für die Bestimmung von Maßnahmen, die wir in einem umfassenden Handlungskonzept aufbereiten.

IT-GRCM Consulting Services

Ein besonderes Augenmerk richtet sich hierbei auf die Geschäftsprozesse eines Unternehmens. Diese sind als Einstieg in die IT-GRCM-Thematik besonders für Analysen im Hinblick auf Risiken und Compliance geeignet. Schwerpunkte dieses Leistungspaketes sind u. a.:

- Einführung von definierten Prozessen für ein IT-Governance-Rahmenwerk
- Aufbau, Einführung und Review des IKS, basierend auf Best Practices (COSO II oder andere Normen) zur effizienten Ausgestaltung des Systems
- Risikoanalyse und Erstellung des Risikoportfolios
- Verankerung kontinuierlicher Kontrollprozesse
- Zielgerichtetes Berichtswesen und Nachweis der Compliance
- Monitoring
- Aufbau und Einführung von IKS/Risiko-Management-Portalen
- Evaluierung von IT-GRCM-Lösungen inkl. Tool-Evaluierung

IT-GRCM Audit Services

Ein weiterer wichtiger Baustein unseres Leistungs- und Serviceportfolios ist der Audit Service, u. a. mit folgenden Schwerpunkten:

- Unterstützung und Beratung bei internen Audits sowie Beseitigung der aufgetretenen Mängel
- Prüfung und Bewertung von Prozess-Compliance-Themen

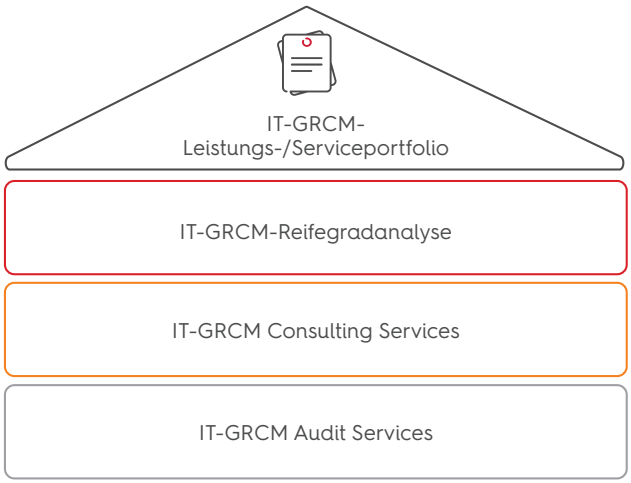


Abb. 3: Leistungsportfolio der Sopra Steria im Bereich IT-GRCM

Was bedeutet unser IT-GRCM?

- Klar definierte IT-Governance-Prozesse
- Umfassende Kontrollmechanismen
- Realtime Monitoring
- Einhaltung der Prozess-Compliance
- Sicherstellung der Nachhaltigkeit durch kontinuierliche Verankerung von Kontrollprozessen
- End-to-End-Analyse

Ihr Nutzen

- Einsatz von Best Practices und anerkannten Rahmenwerken
- Kostenreduktion durch optimierte und automatisierte Strukturen sowie Prozesse
- Verbesserte Geschäftsentwicklung durch eine verantwortungsvolle, zielgetreue und gesetzeskonforme Leitung sowie Steuerung
- Erhöhung der Effektivität durch Steigerung der Kommunikation und Transparenz

Unsere Leistungen

Die Beratung und Unterstützung von IT-GRCM-Projekten bedarf langjähriger Erfahrung auf dem Gebiet der Managementberatung. Wir bieten durch die ausgezeichnete Expertise unserer qualifizierten Berater und ein bewährtes Vorgehensmodell in diesem Bereich eine hervorragende Grundlage zur Optimierung Ihrer IT-GRCM-Fragestellungen.

Kontaktieren Sie uns!

Gerne beraten wir Sie und stellen Ihnen unsere IT-GRCM Consulting Services vor. Wir freuen uns auf Ihre Anfrage!

Über Sopra Steria

Als ein führender europäischer Management- und Technologieberater unterstützt Sopra Steria mit 46.000 Mitarbeiterinnen und Mitarbeitern in 25 Ländern seine Kunden dabei, die digitale Transformation voranzutreiben und konkrete und nachhaltige Ergebnisse zu erzielen. Sopra Steria bietet mit Beratung, Digitalisierung und Softwareentwicklung umfassende End-to-End-Lösungen, die große Unternehmen und Behörden wettbewerbs- und leistungsfähiger machen – und zwar auf Grundlage tiefgehender Branchenexpertise, innovativer Technologien und eines kollaborativen Ansatzes. Das Unternehmen stellt die Menschen in den Mittelpunkt seines Handelns mit dem Ziel, digitale Technologien optimal zu nutzen und eine positive Zukunft für seine Kunden zu gestalten.

The world is how we shape it

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
info.de@soprasteria.com
www.soprasteria.de

40183