IT-Compliance – Management der Risiken in der IT

Aufbau eines Kontrollsystems zur Steuerung regulatorischer Anforderungen

Das kennen Sie?

- Das Management ist verpflichtet, ein System zu gestalten, einzuführen und aufrechtzuerhalten, welches operative Risiken und die Vielzahl regulatorischer Anforderungen durch geeignete Kontrollen abdeckt. Das gilt auch für die IT. Die Wirksamkeit eines solchen internen Kontrollsystems ist regelmäßig zu beurteilen.
- Compliance-Regeln in der IT allein sind keine Garantie für Sicherheit. Viele Unternehmen haben die Prozesse dokumentiert und nutzen Kennzahlen zur Steuerung der IT - sind sogar 27001- und BSI-zertifiziert; trotzdem bleibt der ‚Reality Check', ob die Maßnahmen wirksam sind und die Unternehmen sicherer werden, auf der Strecke.
- Die Herausforderung liegt darin, Compliance in der IT durch eine möglichst weitgehende Automatisierung der Kontrollen kosteneffizient zu managen und gleichzeitig den Nachweis zu erbringen, dass die Anforderungen der relevanten Kontrollorgane auch wirksam erfüllt werden.

Das bieten wir

- Der ictsourcing.de-Transformationsansatz entwickelt schrittweise das Verständnis für das Management von IT-Risiken
- Wir bewerten Ihr Risikomanagement-System und entwickeln es auf Basis von Standards und Best-Practices-Ansätzen (Enterprise Risk Management, COBIT5®, IDW PS 330, ISO 27001) weiter.
- Wir entwickeln gemeinsam mit Ihnen automatisierte, halbautomatisierte und manuelle Kontrollen zur Steuerung der IT und begleiten Sie bei der Umsetzung.
- Wir etablieren - abgestimmt auf Ihre IT-Organisation - Prozesse, Richtlinien und Arbeitsanweisungen, auf deren Basis
  - die Prozessverantwortlichen ihre Risiken identifizieren,
  - auf Auswirkungen hin bewerten und
  - nach ihrem Handlungsbedarf klassifizieren und gewichten können.
- Wir entwickeln gemeinsam mit Ihnen Management-Awareness-Programme.

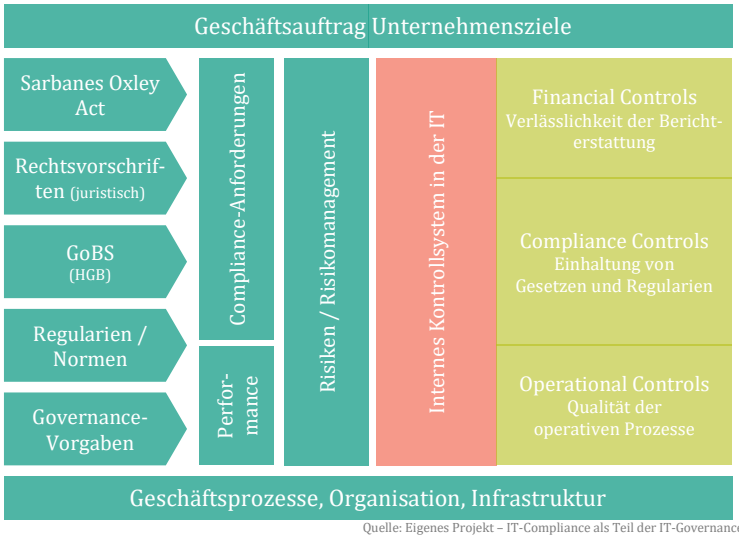
Benefits – Nutzeneffekte

- Durch ein wirksames Frühwarnsystem wird die Fähigkeit des Unternehmens verbessert, mögliche Risiken rechtzeitig zu erkennen und einhergehende Kosten zu verringern.
- Zuverlässigkeit der Berichterstattung sowie Einhaltung von Gesetzen und Vorschriften.
- Durchführung von IT-Audits für Unternehmen, Wirtschaftsprüfer, interne Revisionen.
- Regelmäßige Prüfung von IT-Organisationen anhand der Kriterien Vertraulichkeit, Integrität, Verfügbarkeit, Zuverlässigkeit, Einhaltung rechtlicher Erfordernisse.
- Vorbereitung auf Audits und Prüfungen durch externe Aufsichtsorgane.

Kernbestandteile und Ergebnisse

Der Transformationsansatz zum Aufbau eines internen Kontrollsystems in der IT umfasst vier Module, die einzeln beauftragt werden können. Wir nutzen dabei den internationalen Standard COBIT5® und dem Prüfstandard IDW PS 330 des Instituts der Wirtschaftsprüfer in Deutschland.

- Reifegradgutachten: Prüfung der Qualität vorhandener Steuerungssysteme der IT (Rollen, Prozesse, Richtlinien, Dokumente).
- Optimierung oder Neugestaltung eines wirksamen Kontrollsystems zur Steuerung der Risiken der IT: Risikoinventur, Rollen & Richtlinien, Anpassung van vorgegebene Standards, Wirksamkeit bewerten.
- Automatisierung der Kontrollen.
- Umsetzung: Erarbeitung und Einführung von Richtlinien, Policies und Arbeitsanweisungen.



Quelle: Eigenes Projekt – IT-Compliance als Teil der IT-Governance

Erfahrungen und Kompetenzen

Unsere Mitarbeiter waren u.a. an folgenden Projekten beteiligt:

- Standortbestimmung und Neupositionieren des Informationsmanagements der Konzern-IT: Stärken-/Schwächenanalyse; Entwickeln/Validieren innovativer Soll-Szenarien; Umsetzung
- Kompetenzen und Prozesse der IT-Organisation, die für eine erfolgreiche Abbildung von Business-Anforderungen in eine wirtschaftliche ERP-Lösung erforderlich sind; Fähigkeit zur Umsetzung der IT-Strategie in schlanke IT-Prozesse; Neuausrichtung der IT
- Aufbau IT-Governance-Organisation für den CIO eines internationalen Industriekonzerns – SAP-Assessment mit Provider; Kontrollsystem (SAP Controls); Compliance mit ISO, SOX
- Positionierung und Transformation der internen Bank-IT als IT-Provider am Markt – Erarbeitung von KPIs für Leistungen, SLAs, Konzept zur Steuerung mit Kennzahlen
- ITK Service Portfolio-Definition, Service Request- und Katalog-Management, Optimierung des Order-to-Cash Prozesses im Key Account eines internationalen Outsourcing-Providers
- IT-Management-System, Kennzahlen zur Steuerung der IT und Begleitung des Veränderungsprozesses für einen Schweizer Industriebetrieb und eine Münchner Versicherung.
- Near- & Offshore-Transition von Application Development und Application Maintenance in der internen IT eines internationalen Telekommunikations-Konzerns.

Ein Angebot der convio Leadership Consulting
Steingarten 5A | 22175 Hamburg | Tel: +49 40 1801 2101 | Fax: +49 40 1801 2102 | info@ictsourcing.de