IT-Risk Management heute.

Ein „must have“ für die Geschäftsleitung und ein Benefit für die IT.

Der dramatische Anstieg an Cyber Crime, die Ausweitung auf die persönliche Haftung der Geschäftsleitung bei Delikten des Datenschutzgesetzes, sowie die steigenden Forderungen nach Risikobewertung und Risikovermeidung, im Rahmen des *Corporate Governance Kodex*, *Basel II Akkord* und dem Gesetz zur Kontrolle und Transparenz im Unternehmen – *KonTraG* in Deutschland, oder auch der in Österreich kürzlich verabschiedeten Informationssicherheitsverordnung, verlangen nach transparenten und nachvollziehbaren Managementprozessen.

Die Einführung solcher Prozesse verhilft der Informationstechnologie zu einem besonderen Vorteil. Erstmals kann mit bestimmten Methoden des Riskmanagements die Wertschöpfung ermittelt werden, die die IT dem Unternehmen beisteuert.

Anforderungen an ein zeitgemäßes IT-Riskmanagement

Vergleichbarkeit und Nachvollzierbarkeit

Die Herausforderung eines zeitgemäßen IT-Riskmanagements ist es, mit einer reproduzierbaren Methode, auf relevante Risiken im Unternehmen einzugehen, diese zu analysieren, zu bewerten und vergleichbar darzustellen. (zB nach dem Ratingkennzahlenmodell von Standard & Poors)

Einbindung der Unternehmensleitung - ganzheitliche Betrachtung

IT-Riskmanagement, sollte nicht als simple Maßnahme des Gebäudeschutzes, der Internet-Security, etc verstanden werden. IT-Riskmanagement bedarf einer ganzheitlichen Betrachtung des Unternehmens von Seiten der Strategie, der Organisation, der Technologie und des Rechts und nimmt die Geschäftsleitung als letztendlich verantwortliche Instanz in die Pflicht.

Softwareunterstützung für Administration, Controlling, Simulation und Reporting

Die Informationstechnologie ist in unterschiedlicher Abhängigkeit in allen Organisationseinheiten bzw. Prozessen des Unternehmens involviert. Die Einführung eines IT-Riskmanagementsystems mit derart komplexen Zusammenhängen, kann sinnvoll nur mit der Unterstützung eines Softwaretools implementiert und administriert werden. Der echte Mehrwert für das Management entsteht durch die Funktionen, wie Risikocontrolling, Reporting und Simulation von Risken und Maßnahmen.

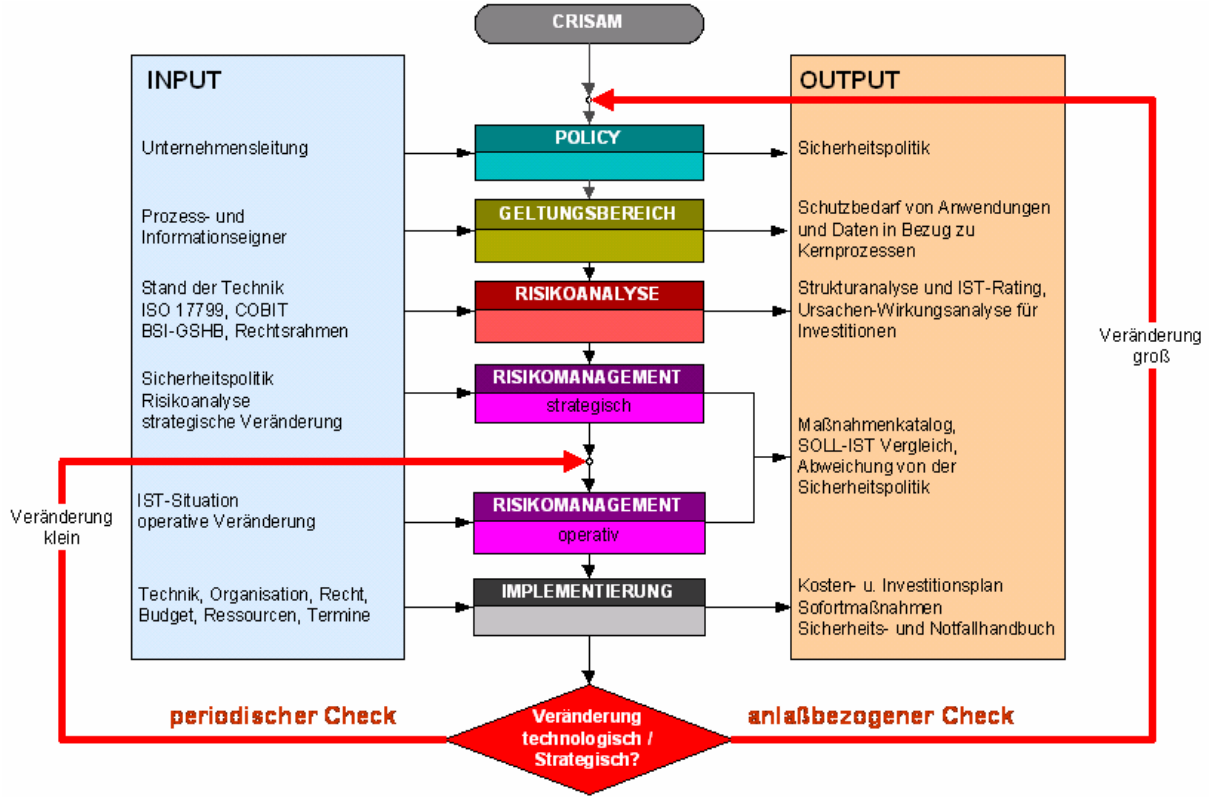
Kompatibilität mit gängigen Standards und Normen.

Die Entwicklungen im Bereich der Standardisierung von Risikomanagementsystemen sind noch in vollem Gange. Daher sollte bei der Auswahl darauf geachtet werden, dass eine neutrale Methode verwendet wird, die nicht nur auf Basis eines Standards beruht.

Beispiel eines Implementierungsprozesses nach der Methode CRISAM®: Sicherheitspolitik / Geltungsbereiche / Risikoanalyse / Risikomanagement / Implementierung / KVP

Die Unternehmensleitung erarbeitet, als Vorgabe für den weiteren Prozess, eine bindende Sicherheitspolicy. Nach den Randbedingungen dieser Policy werden die, in einem **Geltungsbereich** abgegrenzten und geschäftsprozesskritischen, IT-Anwendungen bzw. Datenstämme fixiert. Risikobeeinflussende Ressourcen und Abläufe werden in einer hierarchischen Struktur zueinander dargestellt und das resultierende Restrisiko mit einer transparenten und nachvollziehbaren **Risikoanalyse** nach einem, analog der im Finanzbereich angewendeten Ratingskala, bewertet. Die, aus dem Ergebnis dieser Analyse und dem Sollwert aus der Sicherheitspolitik resultierenden Abweichungen, ergeben im Rahmen des **Risikomanagements** die Grundlage für den zu erfolgenden Verbesserungsprozess. Somit ist ein bereits aus dem Qualitätsmanagement der ISO 9001 bekannter kontinuierlicher Verbesserungsprozess sichergestellt.

Im Rahmen der **Implementierung** werden die einzelnen Maßnahmen nach technologischer und organisatorischer Umsetzbarkeit bewertet und erforderliche Aktivitäten und Projekte initialisiert.



zum Unternehmen:

calpana business consulting gmbh

Als zertifizierter Auditor nach der Norm ISO 17799 versteht sich die calpana business consulting gmbh als kompetenter Businessberater an der Schnittstelle zwischen Technologie, Organisation, Recht und Finanzen. Schwerpunkte sind das Consulting, das Coaching, das Management auf Zeit, sowie die Aus- und Weiterbildung in den Bereichen Risikomanagement, IT & Recht, Datenschutz und Zertifizierungen.

CRISAM®, die Methode analysiert und bewertet Gefährdungen auf Geschäftsprozesse und potenzielle IT-relevante Bedrohungen. CRISAM®, das Tool unterstützt die Einführung und die Administration von Risikomanagementsystemen und ermöglicht Simulationen.
Das Resultat ist ein Maßnahmenpaket mit der Bewertung nach dem Standard & Poors Ratingmodell.

Dipl.-Ing. Dr. Manfred Stallinger, MBA
calpana business consulting gmbh
Europaplatz 6
4020 Linz
Tel.: +43 732 600 610 0
Fax: +43 732 600 610 9
Mail: manfred.stallinger@calpana.com
Internet: www.calpana.com