Effektives IT-RisikoManagement schafft echten Mehrwert in der Informationstechnologie

IT-Risikomanagement ist deutlich mehr als reine Compliance-Erfüllung

Risiken in der IT und die damit verbundenen Risiken im Geschäftsablauf von Unternehmen wachsen durch die zunehmende Komplexität der IT stetig an. Sie gewinnen nicht zuletzt durch die steigenden Anforderungen zur Erfüllung von Compliance-Vorgaben (SOX, FDA, MaRisk, Solvency etc.) an Bedeutung. Während die meisten Unternehmen die klassischen Risikobereiche wie Finanz- oder Marktrisiken bereits umfangreich adressieren oder aufgrund regulatorischer Anforderungen regelmäßigen Informationspflichten unterliegen, besteht in der IT häufig Nachholbedarf bei der Erkennung und dem Management von Chancen und Risiken.

Ziel des IT-Risikomanagements ist es, nicht nur technische und prozessuale Risiken direkt in der IT zu betrachten, sondern den Wertbeitrag der IT zum Unternehmenserfolg zu steuern und langfristig zu sichern. Dazu müssen Risiken in der IT sowie resultierende Effekte auf den Geschäftsablauf im Unternehmen systematisch und übergreifend erkannt, bewertet und verfolgt werden.

Nicht nur die Minimierung von Risiken bzw. die Vermeidung von Schäden steht im Mittelpunkt, sondern auch eine enge Verknüpfung mit der IT-Steuerung. Nur dann können zusätzliche Wertbeiträge aus der Risikobetrachtung identifiziert und im Rahmen der Portfoliosteuerung realisiert werden.

Eine optimierte ökonomische Planung und Steuerung der IT erfolgt idealerweise auf Basis systematischer Analysen anhand der IT- und Geschäftsarchitektur sowie der kontinuierlichen Bewertung und Nutzung von identifizierten Chancen und Risiken. Im Ergebnis leistet das IT-Risikomanagement so einen aktiven Beitrag zu einer wertorientierten und erfolgreichen Unternehmensführung und führt nicht nur zu einer Verbesserung von Verfügbarkeiten und Datensicherheit in der IT.

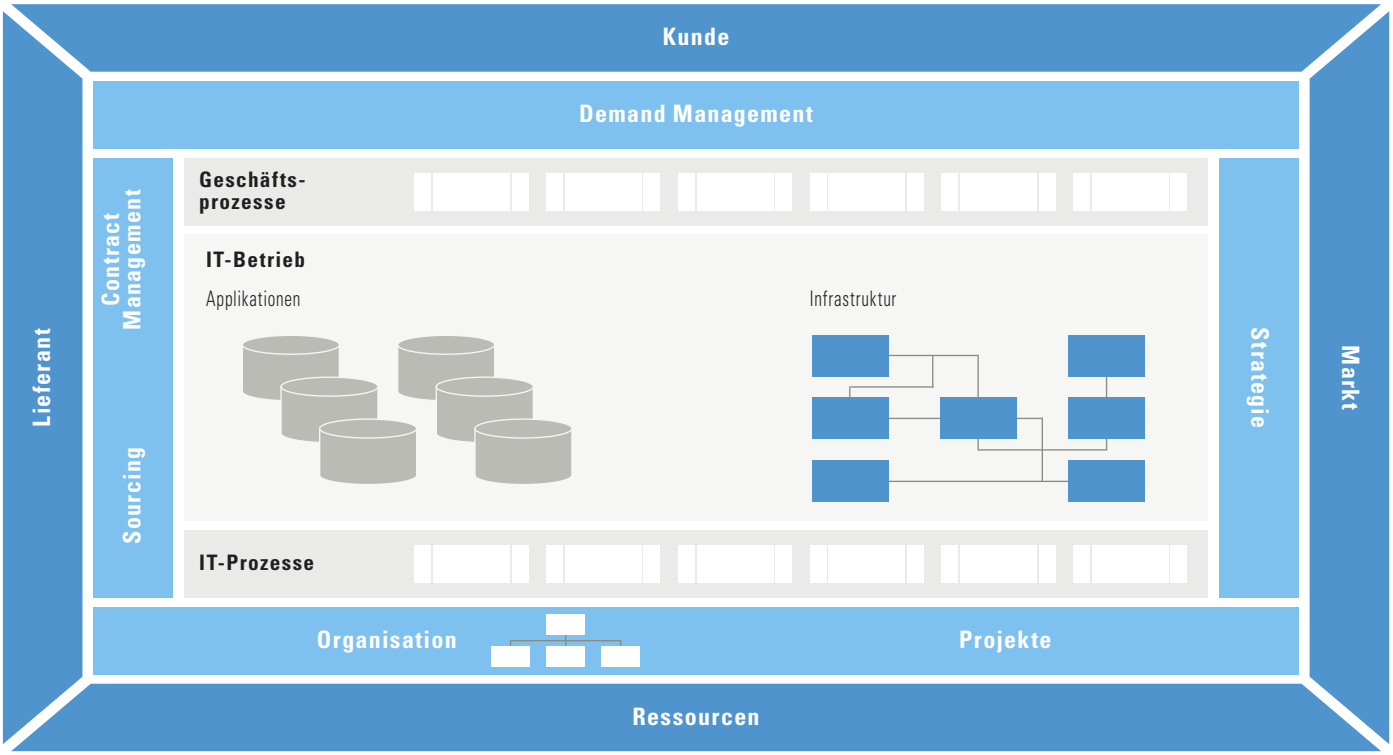

Abbildung 1. Risikolandkarte: Die IT aktiv steuern – durch Identifikation und Bewertung relevanter Risikoelemente und -faktoren auf allen Ebenen

Lösungsweg:

Basis eines effektiven IT-Risikomanagements sind Transparenz und belastbare Risikobewertungen. Die Etablierung des IT-Risikomanagements erfolgt zunächst in enger Abstimmung mit den Geschäftsbereichen aus der übergeordneten Risikostrategie des Unternehmens heraus. Dabei werden anhand einer Checkliste die potenziellen Chancen und Risiken pro Risikofeld identifiziert.
Das Ergebnis wird in einer Risikolandkarte (siehe Abb. 1) abgebildet, die mögliche Risiken und Chancen anhand ihres Einflusses auf die (IT-)Wertschöpfung des Unternehmens darstellt und bewertet. So deckt z. B. eine Know-how-Analyse das Betriebs- und Entwicklungsrisiko aufgrund nicht mehr vorhandenen Know-hows bei älteren Applikationen auf und beeinflusst darüber die Kapazitätsentwicklung und -steuerung oder aber die Neuinvestition. Je nachdem, welche Wichtigkeit die Applikation für den Geschäftsablauf hat und welche Veränderungsdynamik zu erwarten ist.
Damit bilden Risikoidentifizierung und -bewertung der einzelnen Bausteine und Prozesse der IT-Landschaft die Grundlage für eine optimale Investitionssteuerung. Investitionen werden so zielgerichteter eingesetzt. Als Ergebnis der Analyse liegt ein Katalog vor, der die Gesamtheit der identifizierten Risiken in Risikofelder einordnet sowie Abhängigkeiten und die potenzielle Schadenshöhe darstellt.
Je nach Eintrittswahrscheinlichkeit und Risikotypus wird dann die jeweils adäquate Maßnahme zur Risikobewältigung vor dem Hintergrund einer Wirtschaftlichkeitsbetrachtung definiert.
Die Bandbreite erstreckt sich dabei von der Risikovermeidung und -verminderung über das Auslagern von Risiken an Dritte, bis hin zu dem Entschluss, das (Rest-)Risiko bewusst in voller Höhe zu tragen. Etablierte Standards können bei der Umsetzung der Risikomaßnahmen helfen, sind jedoch meist um die Besonderheiten im Unternehmen zu ergänzen. In dieser Phase werden die kontroll- bzw. risikobezogenen Informationen in einen Monitoring- und Reportingzyklus integriert, der kontinuierlich Risikostatusänderungen identifiziert, bewertet und an das Management berichtet. Bei Veränderungen bzw. in einem periodischen Review wird das Risk Assessment jeweils erneut auf den Prüfstand gestellt.
Diese kontinuierliche Steuerung der IT-Risiken aus Unternehmenssicht ist essentielle Managementaufgabe und damit zwingender Bestandteil der Unternehmenssteuerung (siehe Abb. 2).

Der Erfolg bei der Vermeidung und Steuerung von IT-Risiken lässt sich an vier wesentlichen Säulen festmachen:

_ Identifikation der IT-Risiken in den Geschäftsprozessen sowie Berücksichtigung in der ökonomischen Planung
_ Definition unternehmensspezifischer Bewertungskriterien zur Identifikation der eigenen substanziellen Risiken
_ Etablierung und Verankerung des IT-Risikomanagements als kontinuierlicher und integrierter Prozess auf Management- und Arbeitsebene
_ Nutzung der Chancenpotenziale statt reiner Compliance-Erfüllung

4C Beratungsansatz:

Die 4C Methode für ein effektives IT-Risikomanagement enthält aber auch die klassischen Maßnahmen zur Erfüllung von Compliance-Vorgaben und integriert diese ebenfalls in die Steuerung der IT. Dabei wird auf Basis der 4C Checkliste „Risk Assessment" auf verschiedenen Ebenen angesetzt: Auf Managementebene wird eine IT-Risikostrategie und -kultur etabliert. Auch Organisation und Prozesse werden im Hinblick auf mögliche Chancen und Risiken auf den Prüfstand gestellt. Dazu wird die IT-Landschaft als Fundament der Geschäftsprozesse auf ihre Stabilität und Zukunftstauglichkeit hin geprüft und in enger Abstimmung mit den Geschäftsbereichen in Bezug auf die Erfüllung geschäftlicher Anforderungen und Entwicklungen bewertet. Auch die Leistungsbereitstellung in Form von IT-Betrieb und Service Level Agreements wird unter die Lupe genommen.

Es gilt dabei, die Risiken zu identifizieren, die tatsächlich durch das Unternehmen steuerbar und in ihrer Hebelwirkung signifikant sind. Die Bewertung erfolgt grundsätzlich in allen relevanten Dimensionen mit dem Ziel, eine umfassende Risikolandkarte zu generieren: Die quantitative Bewertung der potenziellen Risiken, wie z. B. die Zahl der Schnittstellen von Applikationen, wird dabei ergänzt durch qualitative Aspekte, wie z. B. Effekte zukünftiger Technologien, verfügbares IT-Know-how etc.
Anhand der Gesamtbewertung wird ein unternehmensindividueller Maßnahmenkatalog entwickelt, der Umsetzungsverantwortliche benennt sowie die Messkriterien zur Zielerreichung festlegt und den identifizierten Risiken begegnet.
Die identifizierten Chancen und Risiken nehmen ebenfalls Einfluss auf das IT-Budget und auch auf die Auswahl der zu berücksichtigenden Maßnahmen (z. B. Investitionen). IT-Investitionen fließen so an die richtige Stelle und das IT-Portfolio wird optimal gesteuert.

Das IT-Risikomanagement agiert insofern als weiterer Steuerungshebel einer optimalen IT-Investitionsplanung.
Die Schaffung einer einheitlichen Datenbasis als Grundlage für das IT-Risikomanagement ist somit essentiell für die rechtzeitige Erkennung neuer Chancen und Risiken sowie die Erfüllung der regulativen Anforderungen. Es gilt darüber hinaus, die Entwicklung der Risiken kontinuierlich zu beobachten. Dazu sind die Aktivitäten zur Risikobewältigung in vorhandene Steuerungsprozesse zu integrieren und nicht isoliert zu führen. Regelmäßige Berichte über Status und Entwicklung der Aktivitäten halten schließlich das Management auf dem Laufenden. Im Ergebnis ist eine kontinuierliche, aktive Steuerung der IT-Risiken im Unternehmen etabliert (siehe Abb. 3).

Nutzen und Ergebnisse:

Die Implementierung eines aktiven IT-Risiko-Managements ermöglicht eine effektive und effiziente Risikosteuerung und deckt neue Chancenpotenziale auf. Daraus resultiert folgender Mehrwert:
_ Gestaltung des Wertbeitrags der IT zum Unternehmenserfolg bei gleichzeitiger Erfüllung von Compliance-Anforderungen durch das IT-Risikomanagement
_ Verbesserte Entscheidungsbasis durch frühzeitige Erkennung von Risiken und Chancen
_ Zielgerichtete Steuerung der Investitionen anhand der Risikolandkarte
_ Senkung des Risk Exposure (Operational Risk)
_ Reduktion von Schäden

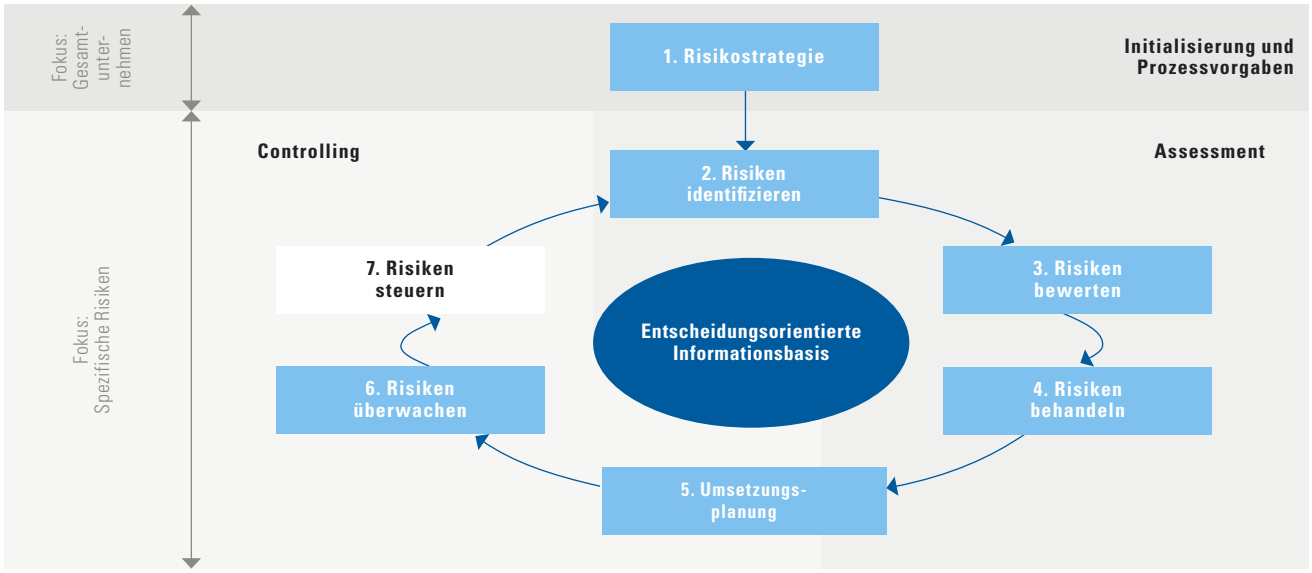

Abbildung 2. Etablierung des IT-Risikomanagements im Unternehmen als „gemanagter" Prozess

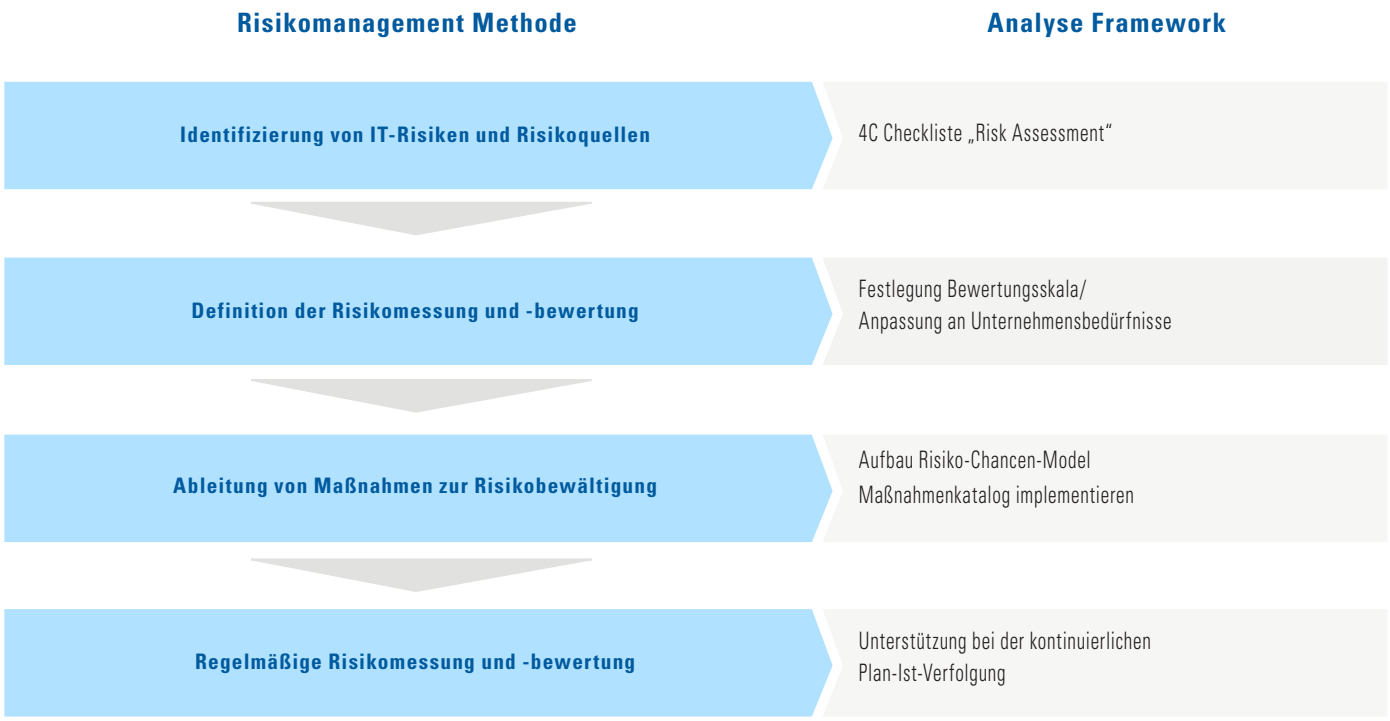

Abbildung 3. Ein effizientes IT-Risikomanagement identifiziert und steuert Chancenpotenziale sowie Maßnahmen zur Risikobewältigung

Ihre Experten für IT-Risikomanagement

Gerne unterstützen wir Sie zum Thema IT-Risikomanagement

Jörg Bassen
Vorstand und Senior Partner

Mobil +49 173 346 58 14
joerg.bassen@4cgroup.com

Focke Meyer
Senior Partner

Mobil +49 173 346 58 34
focke.meyer@4cgroup.com

4C GROUP AG

OFFICE MÜNCHEN
Elsenheimerstraße 55a
D-80687 München
Telefon +49 89 599 882-0

OFFICE BERLIN
Französische Straße 8
D-10117 Berlin
Telefon +49 30 747 82 98-0

OFFICE FRANKFURT
MesseTurm
D-60308 Frankfurt
Telefon +49 69 269 249-0

OFFICE DÜSSELDORF
Neuer Zollhof 2
D-40221 Düsseldorf