

Offener Umgang mit Risiken

Statt über Governance zu sprechen, sollten Unternehmen IT Risk Management betreiben. Dieses darf aber nicht zum Verhinderer werden. Rahmenwerke helfen bei der Umsetzung.

Deregulierung, weltweite Kommunikation, ökonomische und politische Integration beschleunigen die Globalisierung. Neue Technologien und das Internet schaffen neue Märkte und verbinden Menschen sowie Unternehmen schneller und effizienter denn je. Sie scheinen Zeit und Raum gleichsam zu komprimieren. Gleichzeitig eskaliert für viele Unternehmungen der Wettbewerbsdruck aufgrund einer erhöhten Anzahl von Konkurrenzunternehmen. Sie werden mit einer noch nie da gewesenen Vielfalt von Geschäftsrisiken, im Sinne von Chancen und Bedrohungen, konfrontiert. Unternehmerische Entscheidungsprozesse sind deshalb durch folgende Herausforderungen geprägt:

► **Neue Geschäftsmodelle:** Manager wie auch Investoren erkennen, dass nicht nur das materielle Vermögen, sondern zunehmend auch die immateriellen Werte – wie Mitarbeiter, Wissen, geistiges Eigentum und Beziehungen mit Anspruchsgruppen – aktiv bewirtschaftet werden müssen. Sie bestimmen heute den Unternehmenswert (Corporate Value) wesentlich mit. Wir sehen dies in neuen Strategien und Geschäftsmodellen aufstrebender Unternehmen, welche Elemente der Old und New Economy erfolgreich kombinieren. Zudem verkürzen sich die Zeithorizonte für die Umsetzungsmöglichkeit von Strategien und Geschäftsmodellen extrem. Beispiele sind Firmen wie eBay, Amazon oder Geschäftsfelder wie das Internetbanking und web-basierte Handelssysteme.

► **Neue Risiken:** Neue, komplexere Geschäftsmodelle schaffen neue Risiken, welche die Grenzen traditioneller Überwachungs- und Kontrollsysteme aufzeigen. Das herausragendste Beispiele der letzten Jahren ist der Fall von Enron (Derivatgeschäft).

► **Neue Prozesse und Instrumente:** Trotz wachsender Bedeutung immaterieller Werte haben die meisten Unternehmungen keine fle-

xiblen beziehungsweise einfach und klar beschriebenen Prozesse und Systeme, um alle Vermögensobjekte zu bewirtschaften und die daraus entstehenden Risiken zu steuern.

► **Neue Informationsbedürfnisse:** Unternehmen brauchen in diesem Umfeld Informationsmanagement-Modelle, die transparent und benutzergesteuert sind. Sie sollten den Stakeholdern unmittelbaren Informationszugang erlauben (real-time). Unternehmen müssen deshalb alle ihre wertgenerierenden Unternehmensobjekte messen, einschließlich der nur schwierig quantifizierbaren immateriellen Werte.

Zwischen Führung und Sicherheit

Das Erwirtschaften von risikolosen Gewinnen über einen längeren Zeitraum ist unter den oben beschriebenen Umständen unmöglich. Ein wesentlicher Teil der Risiken entsteht in der IT. Es stellt sich darum für Unternehmen die Frage: «Wer macht IT Risk Management?» Diese Frage mündet schnell in einer etwas philosophischen Diskussion rund um das Votum «Jeder macht Risiko Management». Nur ist damit noch nicht die Frage nach der Verantwortung geklärt. Kaum damit konfrontiert, werden schnell die heute besetzten Rollen wie Linienverantwortliche, Stabsstellenleiter, IT-Security-Verantwortliche und interne Revision zur Diskussion gestellt. Obwohl bereits viele Firmen diesen Prozess durchlaufen haben, lässt sich die aufbauorganisatorische Frage des IT-Risikomanagements noch nicht auf Basis von «Good Practice»-Vorgaben beantworten. Dies rührt zum einen daher, dass sich IT Risk Management nicht von den im Unternehmen eingeführten Kernprozessen loslösen lässt und zum anderen, weil häufig nicht ein fachtechnischer Erfahrungsschatz im Vordergrund steht. IT Risk Management repräsentiert also in keiner Weise eine Spezialisten-Wissenschaft, sondern fordert vielmehr ein hohes Mass an Sozialkompe-

tenz: In der Rolle als Motivator, um bestehende Denkstrukturen aufzubrechen, als Durchsetzer von Veränderungsprozessen und als Vermittler bei internen Konfliktsituationen. Diese unscharfe Rollenbeschreibung ist zwangsläufig sehr konfliktgeladen, zumal in der Regel alle vorgenannten Funktionen für sich in Anspruch nehmen, das entsprechende Profil mitzubringen.

Vor allem bei der Abgrenzung zwischen IT Security Management und IT Risk Management tun sich viele Unternehmen schwer. In diesen Fällen kommt der Informatikleiter nicht um die Frage herum, ob sich der IT-Risk-Manager als «Macher» oder als «Polizist» profilieren soll. In der erstgenannten Rolle wird er im Anschluss an die Risikoidentifikationsphase wohl auch das Veränderungsprojekt leiten, respektive sich dafür verantwortlich zeigen wollen, dass die notwendigen technischen und organisatorischen Kontrollen adäquat umgesetzt werden. Ein späterer Follow-up der Initial-IT-Risikoanalyse muss in einer solchen Konstellation jedoch von extern, sprich von der Revisionsseite durchgeführt werden, um die Unabhängigkeit zu gewährleisten. Diese Abhängigkeit zum Revisorat motiviert deshalb auch viele CIO's, ihre IT-Risk-Manager eher als «Polizisten» zu posi-

tionieren, um das IT-Risikomanagement unter eigener Kontrolle zu halten und gleichzeitig auch die Unabhängigkeit dieser Verantwortlichkeit gewährleisten zu können.

Methoden und Frameworks

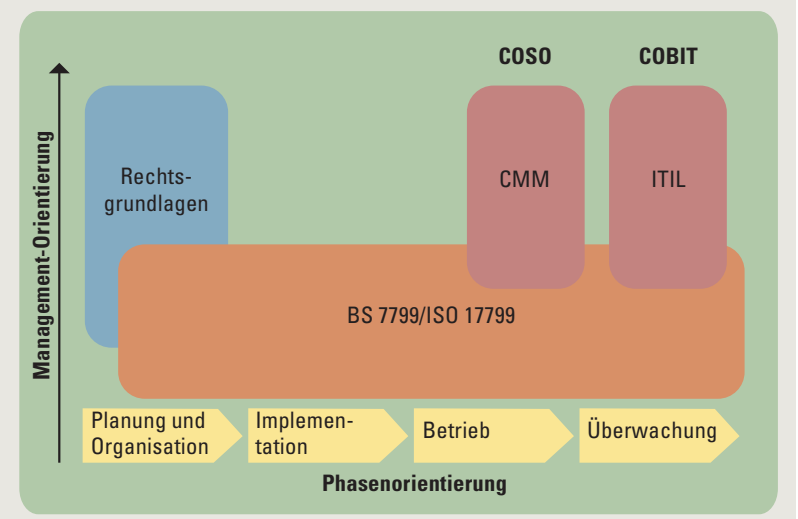
Methoden, Tools und Frameworks für das IT Risk Management sind zuerst in ein unternehmensweites (Risk-)Managementsystem einzubetten. Da wir heute eine Vielzahl von Anforderungen und Herausforderungen wie Sicherheit, operationelle Risiken und Qualitätslücken für Unternehmen vorfinden ist ein zentrales Managementsystem, das unterschiedlichste Ausprägungen (z.B. Qualitäts-, Umwelt-, Risiko-, Kontrollsystem) hat, anzustreben.

Bewährt hat sich, die Wertschöpfung durch die IT als Prozessmodell darzustellen. Wir unterscheiden dabei Planung und Organisation, Implementierung (Projekte), Betrieb (Service-Erbringung) und Überwachung.

Von der Bedeutung her ist COBIT das zentrale Werkzeug, um ein Kontrollsystem mit Kontrollzielen als Kern des IT-Risk Management zu realisieren. Der Vorteil von COBIT liegt auch an der zugrundeliegenden Prozessstruktur, die sich für jede Art und Ausprägung einer IT-Organisation anpassen lässt.

Hilfsmittel des IT Risk Management

Die einzelnen Rahmenwerke und Hilfsmittel für das IT-Risikomanagement kommen an unterschiedlichen Stellen des IT-Prozessmodells zum Einsatz.



Wenn wir das Projektgeschäft innerhalb der IT näher betrachten, so zeigt sich, dass die Risiken in diesem Bereich einerseits durch besser Prozessqualität (Prozessreife) und andererseits durch aktives Risikomanagement in den Projekten erreicht werden kann.

Die Prozessreife wird heute durch Assessments nach dem Reifegradmodell CMM des SEI (Software Engineering Institute) oder der ähnlichen Normen bewertet und anschliessend verbessert. Viele Unternehmen streben in diesem Bereich den Level 3 («der definierte Prozess») an, oder müssen ihn als Vorgabe erreichen (als Zulieferer in der Automobilindustrie oder als Auftragnehmer bei IT-Ausschreibungen).

Noch näher an den Kernprozessen der Informatik sind Hilfsmittel wie ISO 17799 oder ITIL zu positionieren. Unternehmen, welche ein umfassendes Informationssicherheitsmanagementsystem zur Zertifizierungsreife entwickeln wollen, basieren meist auf der ISO-Norm, während dessen ITIL einen Good-Practice-Werkzeugkasten für Informatik-Prozesse darstellt.

Unternehmerische Chancen fokussieren

Risiken treten erfahrungsgemäss besonders dann auf, wenn Neuland betreten wird, sprich Projekte in Arbeit sind, zu welchen die Unternehmen noch keine Erfahrung mitbringen. Eine banale Strategie, um solche Risiken zu vermeiden, wäre natürlich, auf die Projekte gänzlich zu verzichten. Auf Basis der «Lessons Learned» aus dem E-Business-Hype darf heute auch durchaus zu recht hinterfragt werden, ob die Investitionen in ein Projekt gerechtfertigt sind. Andererseits darf das

IT Risk Management auf keinen Fall zu einem «Verhinderer» werden. Risiko- und Chancen-Management sind Unternehmensprozesse, welche nicht voneinander abgekoppelt werden können. Die Konsequenz für Unternehmen, welche das Chancen-Management mit Hilfe eines Projektportfoliomanagements und gleichzeitig auch das Risikomanagement nachhaltig betreiben wollen, müssen entscheiden, welcher dieser Prozesse einen übergeordneten und welcher einen untergeordneten Charakter hat.

Kein Geschäftsleitungsmitglied hat in der Regel Verständnis dafür, für dieselben Fragestellungen – einmal als Chance und einmal als Risiko formuliert – seine Zeit zu opfern. Ob nun der IT-Portfolio oder der IT-Risk-Manager in den «Driver Seat» gehoben werden soll, ist unerheblich. Wiederum ist dieser Entscheid durch die jeweiligen Persönlichkeiten getrieben. Beim Verbesserungsprozess geht es schliesslich darum, die folgenden Fragestellungen (in eben dieser Reihenfolge) zu adressieren:

- ▶ Welche unternehmerischen Chancen lassen wir heute ungenutzt, und welche Opportunitätskosten sind damit verbunden? Kennen wir diese bereits? Falls nein, über welche Motivations- und Kreativ-Hilfsmittel sind diese zu identifizieren?
- ▶ Welche IT-Risiken bedingen Rückstellungen. Durch welche Massnahmen können die Risiken und die entsprechenden Rückstellungen reduziert werden? Welche dieser Massnahmen können mit einem Business Case untermauert und somit als äquivalente Unternehmens-Chance im Projektportfolio festgehalten werden?
- ▶ Welche Ressourcen (finanzielle

und personelle) stellen wir frei, um die identifizierten Chancen zu nutzen?

- ▶ Welche der genannten Chancen fliessen in ein formelles Projektportfolio?
- ▶ Welche Projektrisiken beeinflussen die Priorisierung der Projekte?
- ▶ Werden die Security-Anforderungen in den Projekten ordnungsgemäss umgesetzt. Welche neuen Sicherheitsrisiken entstehen im gegenwärtigen Projektportfolio?
- ▶ Last but not least: Mit welchen Controlling-Hilfsmittel stellen wir sicher, dass die Umsetzung der Projekte effizient und effektiv geschieht?

Basierend auf diesen Fragestellungen gelangt man zum Fazit, dass IT Risk Management einen ganz wesentlichen Führungsprozess repräsentiert, oder einfacher ausgedrückt: IT Risk Management ist Chefsache.

Stiefkind Projektmanagement

Jedes Projekt verfügt über Unsicherheiten und Gefahren, die in Schwierigkeiten und Problemen bei der Durchführung enden können. Um diese Unsicherheiten und Gefahren (Risiken) kontrollieren zu können, bedient man sich des Managements von Projektrisiken. Heute ist Risikomanagement eine integrierte Teildisziplin des Projektmanagements.

Projektmanagement erfolgt einerseits kontinuierlich über die Projektdauer und andererseits energetisch in den Projektmanagementprozessen. Mit Hilfe des Risikomanagements in Projekten werden die Unsicherheiten und Gefahren identifiziert, um sie bewerten und dann umgehen, oder bei ihrem Eintreten auf sie reagieren zu können. Wir wollen hier auf den Guide des Project Management Institute (PMI) verweisen, der international allgemeine Anerkennung erlangt hat und auch die Grundlage für die Zertifizierung von Projektleitern darstellt. Das besondere Interesse des PMI gilt der Schaffung von internationalen Standards. Mit dem Project Management Body of Knowledge (PMBOK™) wurde die Basis dafür gelegt. Seit 1984 gilt die Prüfung zum Project Management Professional (PMP) als anerkannter Nachweis des Wissens über Projektmanagement.

Ein weiteres Hilfsmittel auf Pro-

jektenebene sind der Continuous Riskmanagement-Ansatz (CRM) des SEI und die damit verfügbaren Checklisten und Trainingsangebote. Es handelt sich dabei um einen Teil-Prozess des Projektmanagements, der vom Projektleiter bereits sehr früh zum Zeitpunkt der Offerte und/oder des Projektantrags zu laufen beginnt und bis zu Projektabschluss betrieben wird. Dies bedeutet, dass je nach Phase in regelmässigen Zeitabständen Risikobewertungen des Projekts durchgeführt werden, eine Risikoliste geführt wird und die Risikobehandlungsmassnahmen etabliert und verfolgt werden. Mit diesen einfachen Massnahmen lassen sich Projektkatastrophen vermeiden und auch bei kleineren Projekten eine Menge Geld einsparen.

Fazit: Ausschau nach neuen Chancen halten

Mit den Firmenzusammenbrüchen der letzten Jahre wurde der Ruf nach «Corporate Governance» laut. Dies ist gut so; nur wurde mit diesem Begriff ein neues Schlagwort kreiert, das in erster Instanz nicht verstanden wurde und später den Vorwurf ausgelöst hat «alter Wein in neuen Schläuchen» zu präsentieren. Diese Kritik ist auch gerechtfertigt, denn eine Firma vor dem Untergang zu bewahren hat immer die oberste Führungspriorität. Um diesem Anspruch gerecht zu werden, genügt es heute immer weniger, die unternehmerischen Prioritäten nach Intuition zu lenken. Denn strukturiertes und nachhaltiges Leben von Risikomanagementprozessen heisst nichts anderes als sämtlichen Mitarbeitern die Augen zu öffnen, um Ausschau nach neuen Chancen zu halten.

Rahmenwerke für das IT-Risikomanagement

- **CMM (Capability Maturity Model):** Prozessreifegrad-Modell, ursprünglich mit starkem Fokus auf die Softwareentwicklung, heute aber breiter angewandt, z.B. für «Supplier Sourcing» u.a.
- **COBIT (Control Objectives for Information and related Technology):** Hilfsmittel zur Identifikation von IT-Risiken, das sehr stark von Informatikrevisoren eingesetzt wird.
- **COSO (Committee of Sponsoring Organizations of the Tradeway Commission):** Rahmenwerk, das den Aufbau von unternehmensweiten Risikomanagementsystemen unterstützt.
- **ITIL (IT Infrastructure Library):** Prozessmodell für die Informatik im Sinne von Good-Practice-Ansätzen
- **ISO 17799:** Informationssicherheitsnorm, die sich aus dem IT Security Management herausgebildet hat.

Die Autoren

Dr. Ernest Wallmüller ist Geschäftsführer von Qualität & Informatik, Ralf Ploner leitet bei KPMG den Bereich Projektrisikomanagement. Ernest Wallmüller hat kürzlich das Buch «Risikomanagement für IT- und Software-Projekte» (Hanser Verlag, ISBN 3446224300) herausgegeben.