11 Risiko-Management-Prozesse im Unternehmen

Im Teil B dieses Buches haben wir die Anforderungen an ein RM im Unternehmen aufgezeigt. Aus diesen Anforderungen ging hervor, dass das RM auf höchster Unternehmensebene zur Frühwarnung und Steuerung der Risiken im Gesamtunternehmen für eine gute Corporate Governance unerlässlich ist. Die Einblicke in das Führungssystem zeigten, dass das Risiko-Management Einfluss auf die Strategiefindung im Unternehmen haben muss. Um den Erfordernissen einer risikoabhängigen Strategiefindung bezüglich Strategien und Massnahmen gerecht zu werden, ist sogar die Integration des RM in den Führungs- und Strategieprozess des Unternehmens zu empfehlen.

Im Teil C wurden Modelle, Methoden und Verfahren für das Management der IT-Risiken beleuchtet.

In diesem Teil D des Buches wird veranschaulicht, wie der IT-RM-Prozess und auch andere RM-Prozesse mit dem Gesamt-RM-Prozess und dem Strategie-Prozess verzahnt werden können. Auch werden die aus der Sicherheits-Perspektive des Unternehmens wichtigen Prozesse der „Geschäftskontinuitäts-Planung", des „Outsourcing" und des „Vulnerability und Incident Management" aufgezeigt.

11.1 Verzahnung der RM-Prozesse im Unternehmen

Der Forderung eines Gesamt-RM-Prozesses wird nicht widersprochen, wenn in Teilbereichen eines Unternehmens, z.B. in einer Geschäftseinheit, in einem strategischen Geschäftsfeld, in einzelnen Gruppengesellschaften oder in einzelnen Organisationseinheiten spezifische RM-Prozesse durchgeführt werden.

Kompatibilität für Gesamt-RM-Prozess

Für einen sinnvollen Gesamt-RM-Prozess müssen jedoch die untergeordneten, nachgeordneten oder übergeordneten Risiko-Management-Prozesse zueinander kompatibel sein.

Mit anderen Worten, die Risiko-Informationen als Output des einen Prozesses müssen als Input bei einem anderen Prozess richtig interpretiert werden können.

Informationen über grösste Risiken

So erhält beispielsweise der übergeordnete Gesamt-RM-Prozess von einem IT-RM-Prozess die Analyse-Ergebnisse über die grössten IT-Risiken. Bestehen bereits Massnahmen, dann werden die Restrisiken und die für die Risiko-Bewältigung eingesetzten Massnahmen an den übergeordneten RM-Prozess „berichtet".

Neue Risiko-Bewertung

Das Mittel dazu kann der in Abschnitt 2.5.4 vorgestellte Risiko-Katalog sein. Aus der Sicht aller Unternehmens-Risiken und deren Vernetzungen untereinander müssen diese Risiken (resp. Restrisiken) allenfalls neu bewertet werden.

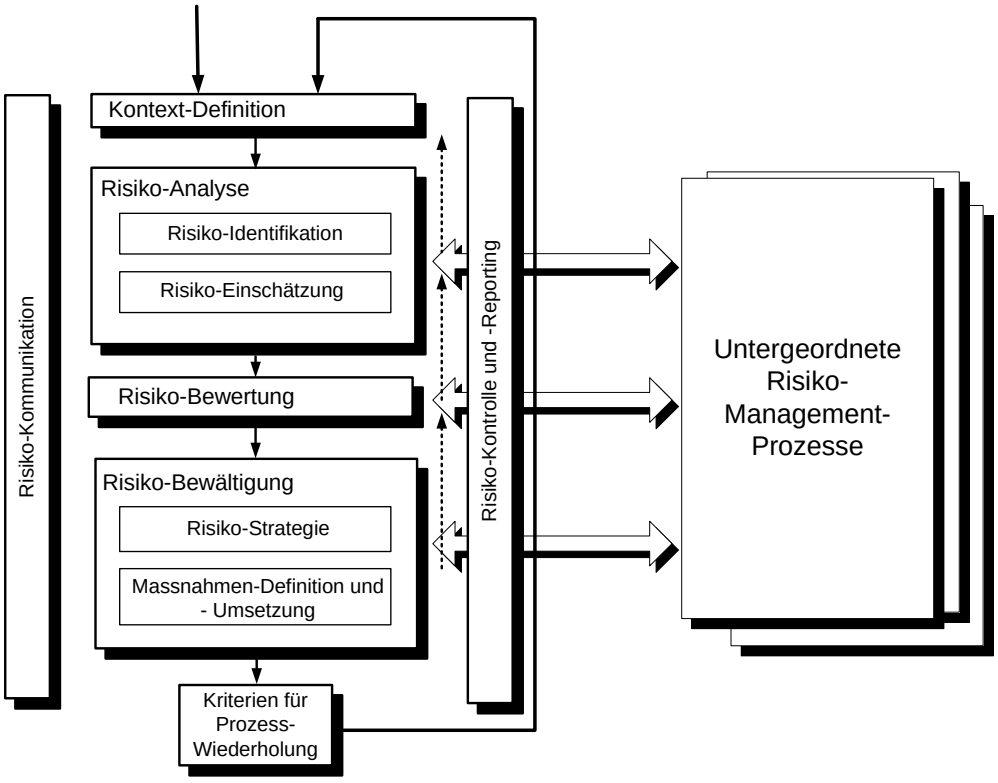
Entscheide über Risiko-Bewältigung

Von der Ebene des Gesamt-RM-Prozesses werden die Entscheide über die Risiko-Bewältigung (z.B. einzuschlagende Risiko-Strategie, Aktionspläne oder Budgets für Massnahmen) an die untergeordneten Risiko-Management-Prozesse zurückgegeben (Abbildung 11.1).

Betrachten wir einen IT-Risiko-Management-Prozess als einen dem Geschäfts-RM-Prozess nachgeordneten RM-Prozess, dann müssen der Geschäfts-RM-Prozess und der IT-RM-Prozess ebenfalls kompatibel zueinander sein, da die IT-Risiken innerhalb der Geschäftsrisiken meist eine wesentliche Rolle spielen. Diese Situation ergibt sich beispielsweise beim „Geschäftskontinuitäts-Plan", in welchem der nachgeordnete „IT-Notfall-Plan" entscheidend zur Geschäftskontinuität beiträgt.

Zeitlich aufeinander abgestimmte RM-Prozesse

Die untereinander kommunizierenden RM-Prozesse müssen auch zeitlich aufeinander abgestimmt sein. Besteht beispielsweise das strategische Ziel, einen bestimmten Geschäftsprozess oder Teile davon zu „outsourcen", dann sind die IT-Risiken und deren Konsequenzen vor dem Strategie-Beschluss durch die Fachstellen der IT-Sicherheit zu analysieren.



Abildung 11.1 RM-Prozess mit Sub-RM-Prozessen

11.1.1 Risiko-Konsolidierung

Zur Gewährleistung der Kompatibilität von untergeordneten mit nachgeordneten und übergeordneten Risiko-Management-Prozessen ist, ähnlich einer „Konzernrechnung“, die Konsolidierung der Risiken notwendig.

Risiken dürfen nicht addiert werden

Im Gegensatz zu den Rechnungslegungsinformationen sind die Risiken statistische Werte, die meist gewisse statistische Abhängigkeiten voneinander haben (Korrelationen). Die Werte dürfen deshalb nicht addiert, sondern müssen gemäss ihrer Korrelationen aggregiert werden. Gerade die grossen IT-Risiken lassen sich statistisch kaum sinnvoll fassen.

Ordnen der Risiken

Für eine Gesamt-RM-Betrachtung ist es daher sinnvoll, die Risiken nach ihrer Höhe unter Angabe ihrer Abhängigkeiten zu ordnen. Bei der Ordnung der Risiken für eine Gesamt-RM-Betrachtung spielt die Aktualität der Erhebung eine wichtige Rolle. Abbildung 11.2 zeigt die Parameter, die an den Schnittstellen der Risiko-Management-Prozesse kompatibel sein müssen.

Kompatible Parameter

- ❒ Schadens-Metrik (d.h. Zuordnung von kardinalen oder ordinalen Schweregraden zu bestimmten Schadenskategorien, s. Abbildung 2.3)
- ❒ Häufigkeits-Metrik (z.B. „selten = 1 mal in 10 Jahren, s. Abbildung 2.2)
- ❒ Risiko-Metrik (s. Abbildung 2.2)
- ❒ Massnahmenkosten-Metrik

Abbildung 11.2 Kompatibilität für verschiedene Risiko-Management-Prozesse

11.1.2 Subsidiäre RM-Prozesse

Risiken behandeln wo sie entstehen oder Schaden anrichten

Die Risiken müssen dort behandelt werden, wo sie entstehen und wo sie primären Schaden anrichten können. Die für die lokale Behandlung zuständigen Sub-Prozesse müssen über kompatible Schnittstellen den Gesamt-RM-Prozess alimentieren. Nur so kann die Unternehmensführung und Unternehmensaufsicht Einblick in die Unternehmens-Risken erhalten und ihrer Verantwortlichkeit bezüglich des Risikomanagements mit entsprechenden Entscheiden nachkommen. Auch ist es nur so möglich, Risikokosten und Massnahmenkosten in ausgewogener Weise den Risikobereichen zuzuordnen. Hier rufen wir die Balanced Scorecard in Erinnerung, welche die Ausgewogenheit der strategischen Zielsetzungen unter den vier Unternehmensperspektiven „Lernen und Entwickeln“, „Interne Geschäftsprozesse“, „Kunden“ und „Finanzen“ anstrebt und alle Aktivitäten im Unternehmen auf die Strategie fokussiert.

Bottom-up-Vorgehen

Im Abschnitt 2.6 haben wir das Top-Down-Vorgehen für das RM im Unternehmen diskutiert. Zu einer optimalen Gesamtsicht über die Risiken gehört aber auch das Bottom-up-Vorgehen. In den einzelnen Geschäftseinheiten, Organisationseinheiten und Prozessen werden beispielsweise projektspezifische, systemspezifische und prozessspezifische Risiko-Analysen durchgeführt.

Die im Abschnitt 10.1 gezeigte Erstellung von Sicherheitskonzepten in der Struktur eines Risiko-Management-Prozesses dient einem solchen Bottom-up Vorgehen. Die nach der Umsetzung des Sicherheitskonzepts verbleibenden *grossen* Restrisiken gehen in den übergeordneten Risiko-Management-Prozess ein.

Grosse Restrisiken in übergeordneten Risiko-Arten

Im übergeordneten Risiko-Management-Prozess werden diese Risiken allenfalls in übergeordnete Risiko-Arten zusammenfasst und konsolidiert.

Verschiedene System-Ausfall-Risiken innerhalb eines wichtigen Geschäftsprozesses werden beispielsweise auf der übergeordneten Ebene zu einem einzigen Ausfall-Risiko des gesamten Geschäftsprozesses aggregiert und konsolidiert.

Prinzip der Wesentlichkeit

Das Reporting und die Behandlung der Risiken müssen dem „Prinzip der Wesentlichkeit“ gehorchend innerhalb des Management-Systems stufengerecht erfolgen. So sollte die oberste Führungsstufe nur die grössten Risiken behandeln (Erfahrungswert: Twenty is plenty). Die kleineren Risiken werden lokal behandelt und an das zuständige Management respektive den Risiko-Owner des Bereichs berichtet. Auch dort gilt, dass im Bereich einer Linienverantwortung sinnvollerweise nicht mehr als 20 hauptsächliche Risiken bearbeitet werden sollten (vgl. [Brüh03], S. 110 ff).

11.1.3 IT-RM im Gesamt-RM

Die Unterstützung fast aller Geschäftsprozesse durch die IT führt dazu, dass die IT-Risiken fast in allen Bereichen anfallen. Im vorigen Abschnitt haben wir die lokale Behandlung der Risiken als notwendig herausgehoben.

Risiko-Ownership

Bei der Frage, wie Risiko-Ownership den IT-Risiken zugeordnet werden könnte, bietet sich beispielsweise die IT-System-Ownership an. Bei der IT-System Ownership werden aus der Geschäftsperspektive die verschiedenen IT-Verantwortlichkeiten rund um ein zuvor in seinen Funktionen abgegrenztes IT-System aufgeteilt.

Im Falle eines kleinen Unternehmens mit nur wenigen IT-Systemen wird pro IT-System (komplette Anwendung mit Server-Plattform) eine verantwortliche Person bzw. ein sog. Owner bestimmt. (Für mehrere IT-Systeme kann es durchaus dieselbe Person sein.)

Diese Person erhält die Verantwortlichkeit über die Risiken im Zusammenhang mit den durch das IT-System zu bearbeitenden

Informationen und Prozesse. Diese Person sollte auch in der Lage sein, mit entsprechendem Coaching durch einen Risiko-Manager, die Risiken zu erkennen und einzustufen.

Risk Owner

Als „Risk Owner" wird diese Person die IT-Risiken an den Gesamt-RM-Prozess berichten. Im Sinne der Sicherheits-Verantwortung wird diese Person auch für die Anfertigung eines IT-Sicherheitskonzeptes verpflichtet sein. Meist fallen auch andere Risiken in den Verantwortlichkeitsbereich dieser Person, für die sie dann ebenfalls Risk Owner ist.

Unterschiedliche Verantwortlichkeiten

In grossen Unternehmen mit vielen Geschäfts-Anwendungen und Server-Plattformen können verschiedene Owner mit unterschiedlichen Verantwortlichkeiten einer IT-Anwendung zugeordnet werden. Z.B.

- Owner für den Geschäftsprozess (oder die Anwendung)
- Owner für den Betrieb der Applikation und
- Owner für die Server-Plattform und Hardware

Geschäftsprozess-Owner

Der Owner des Geschäftsprozesses wird die SLA*s bestimmen und für die Erstellung eines IT-Sicherheitskonzepts sorgen. Die anderen am Geschäftsprozess beteiligten IT-Owner werden im Rahmen der SLA's und der unternehmensweiten Sicherheitsweisungen den Beitrag ihres Verantwortlichkeitsbereichs zum Sicherheitskonzept beisteuern (s. Abschnitt 10.1). Das Sicherheitskonzept weist u.a. die Massnahmen und verbleibenden Restrisiken aus.

Die grossen Restrisiken und wichtigen Massnahmen (Ist- und Soll-Massnahmen) werden durch den Owner des Geschäftsprozesses an den Gesamt-RM-Prozess berichtet.

Neben dem Risiko-Management über zwangsläufig zu erstellende Sicherheitskonzepte wird es notwendig sein, im Jahres-Rhythmus die wichtigsten Geschäftsprozesse und Supportprozesse eines Unternehmens auf IT-Risiken hin zu untersuchen.

Berichterstattung

Die daraus resultierenden Berichterstattungen an den Gesamt-RM-Prozess müssen entsprechend den regulativen Erfordernissen für die Geschäfts-Berichterstattung sowie zum Startzeitpunkt des jährlichen Strategieprozesses (s. Abbildung 11.4) jeweils verfügbar sein.

* SLA: Service Level Agreement

Koordination und Schulung

In einem grossen Unternehmen mit vielen IT-System-Ownern (resp. Risk-Ownern) bedarf die ständige Aufrechterhaltung einer solchen Organisation eines gewissen Koordinations-Aufwandes. Ebenso bedarf die Durchführung der lokalen Risiko-Management-Prozesse ein gewisses Mass an Schulung.

Chief Information Security Officer

Für die Aspekte der IT-Risiken gehören die Koordinations- und Schulungsaufgaben sicherlich in das Pflichtenheft eines Chief Information Security Officers.

Chief Risk Officer oder Risk Manager

Die Koordiantions- und Coaching-Aufgabe für die adäquate Lieferung der Risiko-Informationen an den Gesamt-RM-Prozess fällt in die Verantwortung eines Chief Risik Officer oder eines Risk Managers.

Die Rechte und Pflichten der in einem solchen Rollenkonzept eingebundenen Funktionsträger werden in entsprechenden Weisungen und Ausführungsbestimmungen geregelt.

11.2 Risiko-Management im Strategie-Prozess

Gesamtprozess und kompatible Sub-Prozesse

Bei der Verankerung des RM-Prozesses im Strategieprozess stellen wir fest, dass es, wie eine Gesamtstrategie und dazu kompatible Unterstrategien, auch ein Gesamt-RM-Prozess und dazu kompatible Sub-Prozesse geben muss (Abbildung 11.3).

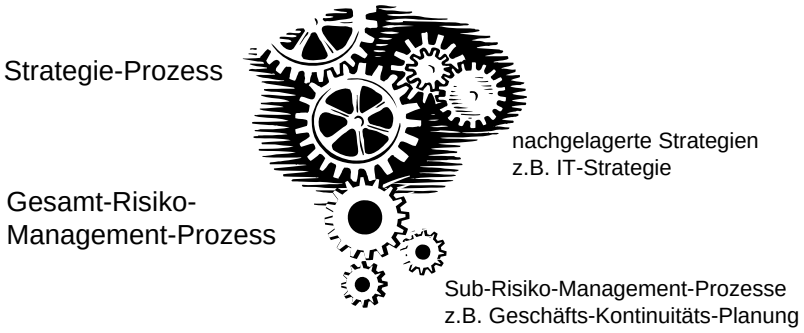


Abbildung 11.3 Risiko-Management-Prozess im Strategie-Prozess

Damit erhalten wir eine Makrobetrachtung auf der Ebene des Gesamt-Risiko-Prozesses.

In den einzelnen Teilbereichen (z.B. Geschäftsbereiche, Organisationseinheiten, Informatik mit ihren kritschen IT-Systemen) finden die Mikro-Betrachtungen über die spezifischen Risiken

des Bereichs statt. Verfügt das Unternehmen über einen Strategie-Prozess, dann sollte der Risiko-Management-Prozess fest mit dem Strategie-Prozess gekoppelt oder noch besser integriert werden (s. Abbildung).

Chancen / Risiken-Abwägung

Auf diese Weise sind die Vorraussetzungen vorhanden, dass die Risiken mit den Chancen abgewogen werden können. Auch der Entstehung von Folgerisiken in den Support-Prozessen (z.B. IT-Strategie) infolge der Geschäfts-Strategien kann damit Rechnung getragen werden.

11.2.1 Risiko-Management und IT-Strategie im Strategie-Prozess

Unternehmens-Strategie

Im Rahmen dieses Abschnitts gilt es zu zeigen, wie das IT-Risiko-Management in einen Gesamt-RM-Prozesse und in die Unternehmens-Strategie einfliesst.

Der Strategieprozess könnte ja so definiert sein, dass er einen Zeithorizont von 3 Jahren im Sinne einer Mittelfristplanung abdeckt und jährlich durchgeführt wird.

Im Folgenden wird der in Abbildung 11.4 gezeigte Prozess kurz erläutert, ohne dabei in die näheren Details einzugehen.

Praxistipp

Die Einrichtung eines RM-Prozesses in einem Unternehmen bedarf oft tief greifender Veränderungen des Risiko-Bewusstseins. Die Einführung sowie die regelmässige Fortführung des Prozesses müssen auf allen Ebenen des Unternehmens durch das Management getragen werden und integrierender Bestandteil des Führungssystems sein. Oft sind die Erfahrungen für die Einführung in einem Unternehmen zu wenig vorhanden, weshalb es dann ratsam ist, die Einführung mittels externem Coaching vorzunehmen. Wichtig ist vor allem, dass das Risiko-Management durch die Führungspersonen und die Mitarbeitenden des Unternehmens getragen und gelebt wird.

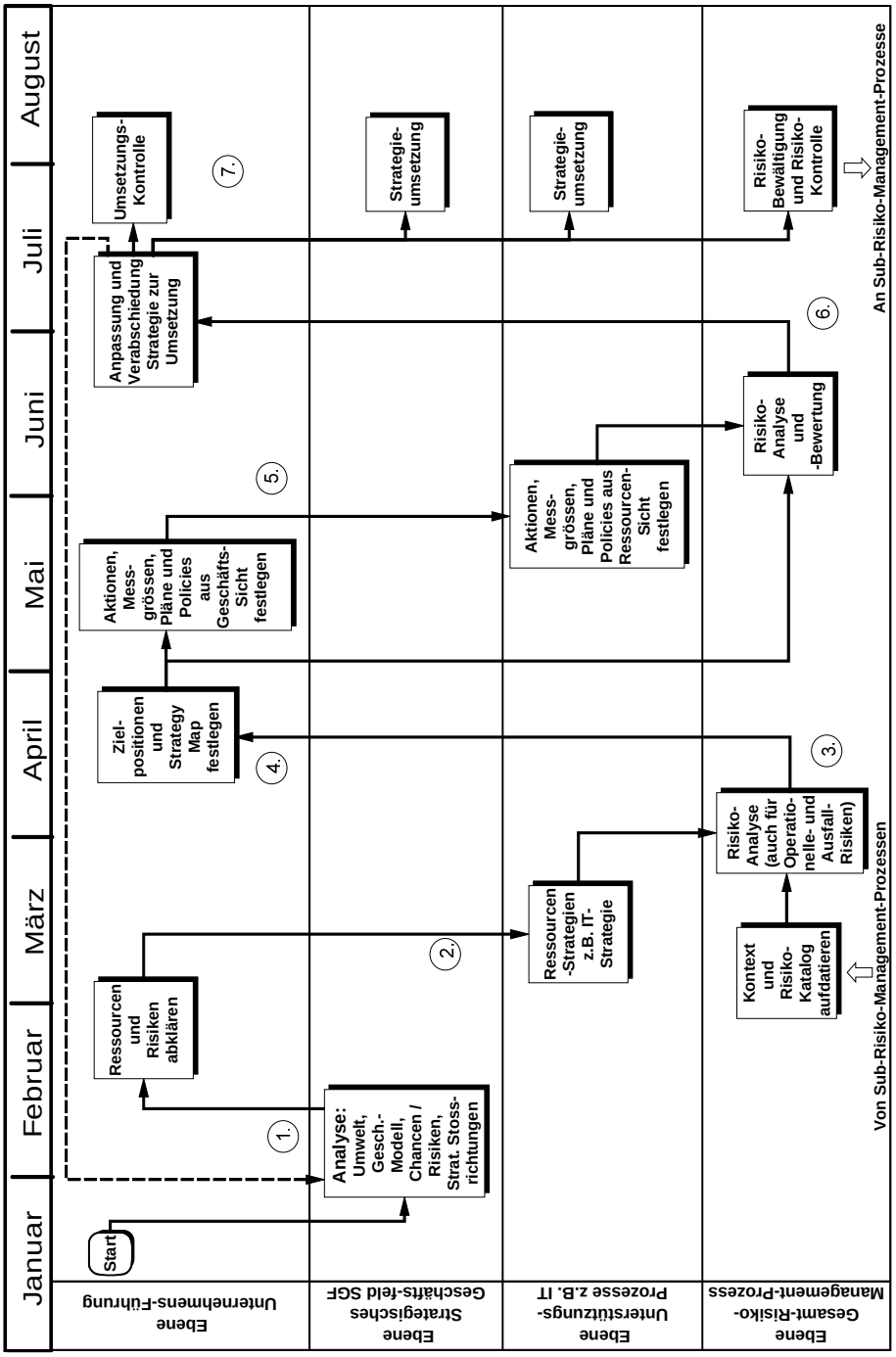


Abbildung 11.4 Integrierter Risiko-Management-Prozess

Ablauf Strategie- und Gesamt-RM-Prozess

1. In den strategischen Geschäftsfeldern werden aufgrund einer Umweltanalyse für das Geschäftsfeld die Chancen und Risiken sowie die Stärken und Schwächen des Geschäftsmodells und entsprechende strategische Stossrichtungen entwickelt.
2. In weiteren Schritten werden nun die Ressourcen, u. a. die benötigten IT-Ressourcen abgeklärt.
3. Danach wird in den Gesamt-RM-Prozess verzweigt, wo die Risiken im Zusammenhang mit den strategischen Stossrichtungen untersucht werden. Der Risiko-Katalog muss dazu bereits in einer aktualisierten Version vorliegen. Im Gesamt-RM-Prozess werden die Risiken im Kontext des Gesamtunternehmens analysiert und zusätzliche Angaben bezüglich Stärken und Schwächen des Unternehmens für die zu betrachtenden strategischen Stossrichtungen gemacht.

   Beispiel:

   Bedarf die strategische Stossrichtung einer hohen IT-Verfügbarkeit über die Kommunikationsschiene „Internet“, dann sind an dieser Stelle die Bedrohungen und Risiken aus Untenehmenssicht (z.B. Denial of Service-Attacken) aufzuzeigen.
4. Zur Festlegung der konkreten strategischen Ziele und deren Wirkungszusammenhänge in der „Strategy-Map“ liegen nun eine komplette und bereinigte SWOT-Analyse* sowie weitere Informationen über die mit strategischen Stossrichtungen zusammenhängenden Risiken vor.
5. Zur Umsetzung der strategischen Ziele werden die Messgrössen, strategischen Aktionen, Pläne und Policies auf der Ebene der Unternehmensführung und anschliessend auf der Ebene der Ressourcen (Unterstützungsprozesse) definiert.
6. Die gewählten strategischen Aktionen einschliesslich der Messgrössen und Pläne, etc. werden noch einer Risiko-Betrachtung aus Gesamtsicht des Unternehmens (einschl. der Unterstützungsprozesse) unterzogen bevor sie im nächsten Schritt verabschiedet werden.
7. Die Umsetzung der Strategie wird vor allem im Rahmen des regulären Risiko-Reportings überwacht.

* (S=Strengths, Weaknesses, O=Opportunities, T=Threats)

11.2.2 Periodisches Risiko-Reporting

Regelmässiges Reporting an Geschäftsleitung

Risiko-Katalog mit wichtigsten Positionen

Das Risiko-Reporting sollte im Rahmen der normalen Berichtssysteme eines Unternehmens erfolgen. So werden, ähnlich dem Budgetreporting, der Geschäftsleitung die Risiko-Positionen unterbreitet. Zum Reporting eignet sich beispielsweise ein monatlich angepasster Risiko-Katalog. Dieser sollte sowohl in seiner detaillierten Form und für einen möglichst raschen Überblick jeweils auf die wichtigsten Positionen zusammengefasst werden. Ebenfalls im Risiko-Katalog enthalten sollten die Massnahmen-Entscheide sowie der Stand und die Wirksamkeit der Massnahmen veranschaulicht sein. Zu den Terminen für die Behandlung in der Geschäftsleitung und im Verwaltungsrat müssen die Erhebungen und Auswertungen aktualisiert und zusammengestellt werden.

11.3 Zusammenfassung

In einem integrativen Risiko-Management müssen die verschiedenen Risiko-Management-Prozesse mit dem Gesamt-Risiko-Management-Prozess und dem Strategie-Prozess „verzahnt“ werden. Für einen sinnvollen Gesamt-Risiko-Management-Prozess müssen die untergeordneten, nachgeordneten und übergeordneten Risiko-Management-Prozesse zueinander kompatibel sein.

Zur Gesamt-Risiko-Betrachtung ist es sinnvoll, die Risiken zu ordnen.

Die Risiken müssen dort behandelt werden, wo sie entstehen und/oder primären Schaden anrichten können. Die in einzelnen IT-Sicherheitskonzepten verbleibenden grossen Restrisiken sind Risiken, die in den übergeordneten RM-Prozess eingehen sollten.

Im übergeordneten RM-Prozess können auch Risiken zusammengefasst werden, so werden verschiedene Ausfallrisiken auf der Ebene eines Prozesses zu einem einzigen Ausfall-Risiko des gesamten Geschäftsprozesses aggregiert. Dem Prinzip der „Wesentlichkeit“ gehorchend, sollte die oberste Führungsstufe eines Unternehmens höchsten die zwanzig höchsten Risiken behandeln Die kleineren Risiken werden lokal behandelt und dem zuständigen Management oder Risiko-Owner berichtet.

Ein „Owner“ über ein bestimmtes IT-System kann gleichzeitig auch Risiko-Owner sein. In grossen Unternehmen mit vielen Geschäfts-Anwendungen und Server-Plattformen können einem System verschiedene Owner mit unterschiedlichen Verantwortlichkeiten zugeordnet werden. Z.B.

- Owner für den Geschäftsprozess (oder Anwendung)
- Owner für den Betrieb der Applikation und
- Owner für die Server-Plattform und Hardware

Neben dem Risiko-Management mittels zwangsläufig zu erstellenden Sicherheitskonzepten wird es notwendig sein, im Jahres-Rhythmus die wichtigsten Geschäftsprozesse und Supportprozesse eines Unternehmens auf IT-Risiken hin zu untersuchen.

Die daraus resultierenden Berichterstattungen an den Gesamt-RM-Prozess müssen entsprechend den regulativen Erfordernissen für die Geschäfts-Berichterstattung sowie zum Startzeitpunkt des jährlichen Strategieprozesses jeweils verfügbar sein.

Der Risiko-Management-Prozess sollte in den Strategie-Prozess integriert oder fest an ihn gekoppelt werden. Auf diese Weise werden auf der Geschäftsleitungs-Ebene die Vorraussetzungen geschaffen, dass die Risiken und Chancen gegeneinander abgewogen werden können. Auch der Entstehung von Folgerisiken in den Support-Prozessen (z.B. IT-Strategie) aufgrund der Geschäfts-Strategien kann damit Rechnung getragen werden. Für das Risiko-Reporting werden, ähnlich dem Budgetreporting, der Geschäftsleitung die wichtigsten Risiko-Positionen unterbreitet. Zum Reporting eignet sich ein monatlich angepasster Risiko-Katalog.

11.4 Kontrollfragen und Aufgaben

1. Welche Parameter müssen an den Schnittstellen der RM-Prozesse kompatibel sein?
2. Welchen Vorteil bringt die Integration des RM-Prozesses in den Strategie-Prozess eines Unternehmens?
3. Wie kann die Umsetzung der Strategie überwacht werden?
4. Bei der Zuordnung untenstehender Verantwortlichkeiten für eine IT-Anwendung wird welcher Owner die SLAs für den Betrieb einer Applikation bestimmen?
   - Owner für den Geschäftsprozess (oder Anwendung)
   - Owner für den Betrieb der Applikation und
   - Owner für die Server-Plattform und Hardware
5. In einem Unternehmen mit einem fortgeschrittenen Strategie-Prozess und einem vorhandenen Risiko-Management werden Sie welche Variante eines Risiko-Managements antreffen?

a) Explizites einfaches Risiko-Management, das wenigen Mitarbeitenden und Führungspersonen bekannt ist.

b) Explizites, in das Führungssystem und den Strategieprozess des Unternehmens integriertes Risiko-Management, das unternehmensweit kommuniziert ist.

6. Kann die Unternehmens-Strategie verabschiedet werden, ohne die Vorlage der strategischen Aktionen der Ressourcen-Strategien (z.B. IT-Strategie) und ohne eine entsprechende Risiko-Analyse?

   Begründen Sie.