Bericht

KMU SWISS EVENT
lernen • verstehen • umsetzen

Whiteboard Bericht
Management

Pro-Aktives Risiko-Management

www.kmuswiss.ch

Verfasser
Peter Fierz
CEO
Yellow Consulting AG
CH-6052 Hergiswil

KMU SWISS EVENT
lernen • verstehen • umsetzen

Danke

Herrn Peter Fierz, Yellow Consulting AG, danken wir für das Schreiben des vorliegenden Berichts.

Ein spezieller Dank gilt allen Sponsoren der Plattform **KMU SWISS EVENT** im Jahr 2006, welche die Durchführung aller Aktivitäten ermöglichen.

Exklusiv-Sponsoren:

axpo gibt Energie.
sage Schweiz Suisse Svizzera

Haupt-Sponsoren:

Dr.W.A.Günther media rent
JUST FLY helvetic.com
Victor Hotz AG für Satz, Bild und Druck
hp invent

Patronat:

STADT BADEN
osec business network switzerland
phw PRIVATE HOCHSCHULE WIRTSCHAFT
nw Fachhochschule Nordwestschweiz

Medienpartner:

AARGAUER ZEITUNG
CASH
ORGANISATOR
InfoWeek.ch
netzwoche online
TELE M1

Verbandspartner:

aargau kmu
city com baden
SWISS ENGINEERING
SMC SWISS MARKETING
ODEC

Co-Sponsoren:

AVISTA – AZ Direct AG – Gebrüder Weiss AG – Geissmann Kuhn Kern – Genevoise – Intertime AG – Océ Schweiz – Kenny's Autocenter – Kultur- und Kongresszentrum TRAFO – Nexell GmbH – Orange Communications AG – Rent a Person – Schmocker AG – Swisscom Directories AG – SWICA – Telag Communications AG

www.kmuswiss.ch

KMU SWISS EVENT
lernen • verstehen • umsetzen

Whiteboard Bericht

Pro-Aktives Risiko-Management

Autor:

Peter Fierz
Geboren 1957, Inhaber der Firma Yellow Consulting AG. Als IT-Professional mehr als 25 Jahre nationale und internationale IT und Business Erfahrung. Davon mehr als 20 Jahre Führungserfahrung; 3 1/4 Jahre als CIO in der USA, 2 Jahre als CIO einer Software Entwicklungsfactory in Europa, 1 1/4 Jahre als CIO in der Schweiz und 14 Jahre als Team und Projekt Manager.

Mehrjährige nationale und internationale Risiko Management-,Outsourcing-, und Governance-Projekt Erfahrungen. Mehrere Organisations- „Rightsizing“ Projekte erfolgreich umgesetzt. In über 20 Ländern Projekte initialisiert und umgesetzt. Mehrere Jahre im Ausland gelebt und gearbeitet wie USA, Australien, Luxemburg, Kenia und Marokko

Firma: **Yellow Consulting AG**
Bahnhofstrasse 4
CH-6052 Hergiswil
Tel: +41 79 247 87 43
Internet: www.yellowconsulting.ch

Datum: 11.06.06

Inhaltsverzeichnis

1. **Zusammenfassung (Management Summary) 4**
2. **Unternehmensweite Risikopositionen 5**
3. **Die Vielfalt und die Komplexität der Risiken 6**
4. **Die Schritte im Management Prozess 6**
5. **Die wichtigsten Erfolgsfaktoren 6**
6. **Vorgehen zur Risiken- Identifizierung und -Beurteilung 7**
7. **Das Reporting des Risiko-Managements 8**
8. **Zeitpunkt der Durchführung des Risiko-Assessment 9**
9. **Welche Software sollte eingesetzt werden 9**
10. **Darstellung der Selbsteinschätzung und Bewertung 10**
11. **Minimale Anforderungen 10**
12. **Quellenverzeichnis 11**

1. Zusammenfassung (Management Summary)

Nehmen Sie als Führungskraft Ihre Verantwortungen im Risikomanagement wahr?

Jedes Unternehmen, ob gross oder klein, national oder international, an der Börse kotiert oder nicht, ist täglich einer Vielzahl von Risiken ausgesetzt.

Finanzskandale, Betrügereien, Veruntreuungen, Umweltkatastrophen, Terroranschläge, Virusattacken, fehlgeschlagene Fusionen, misslungene IT- Projekte und andere Probleme haben bei vielen Führungskräften und Verantwortlichen zu einem Umdenken in einem speziellen Bereich geführt – wie kann man Risiken identifizieren, bewerten und vermindern? Die Realität zeigt, dass in vielen Unternehmen das Managen von Risiken durch fehlende oder ungenügende Corporate Governance Strukturen und Prozesse eine Alibiübung ist.

2. Unternehmensweite Risikopositionen

Oft wird Risikomanagement aus Kosten- oder Zeitgründen vernachlässigt oder umgangen. Können Sie dies verantworten?

In vielen kleinen und mittelständischen Unternehmen (KMU) sind die Führungskräfte der Ansicht, gegen Ereignisse aller Art genügend abgesichert zu sein. Die finanziellen, infrastrukturellen und / oder personellen Auswirkungen hat man unter Kontrolle. Hohe Versicherungsprämien sind schliesslich ein Schutz für alle Eventualitäten.

Sind Sie sich als Mitglied des Verwaltungsrates, der Geschäftsleitung, als Linienverantwortlicher oder Mitarbeiter der unternehmensweiten Risikopositionen der Auswirkungen und Ihrer Verantwortung in diesem Zusammenhang bewusst?

Viele mussten bereits die Erfahrung machen, dass man nach dem Eintreffen eines grösseren, schädigenden Ereignisses feststellt:

- das auslösende Ereignis hätte vermieden, verzögert oder vermindert werden können
- keine Rückstellungen zur finanziellen Absicherung gemacht wurden
- Notfallpläne (contingency plans), die einmal für das Jahr-2000 -Problem erstellt wurden, sind veraltet und nutzlos
- der vor Jahren definierte Krisenstab ist durch das Ausscheiden von Mitarbeitern nicht mehr handlungsfähig
- Entscheidungen (z.B. das Akzeptieren eines Risikos) sind nicht mehr nachvollziehbar.

Jedes schädigende Ereignis ist mit Störungen und Kosten verbunden. Die Leistungserbringung wird negativ beeinflusst, der Profit geschmälert – oftmals nachhaltig.

Folgende Fragen ergeben sich: Wie können Risiken identifiziert, dokumentiert, bewertet und vermindert werden? Wie können Gefahren möglichst vermieden werden? Wie stelle ich die Leistungserbringung sicher, ohne die Kosten für die Risikobehandlung ins Unermessliche steigen zu lassen?

Das Definieren der notwendigen Governance, der Risk Policy, des Risiko-Management Prozesses und die Durchführung eines ersten Assessments erfordern einen grossen Einsatz. Für Folge-Assessments ("Follow Ups") sind der Aufwand und die Kosten deutlich geringer. Voraussetzung ist, dass der Prozess richtig implementiert und angewendet wurde.

3. Die Vielfalt und die Komplexität der Risiken

Werden die Vielfalt und die Komplexität der Risiken zunehmen? Diese Frage kann mit einem klaren „Ja“ beantwortet werden.

Es ist eine unbestreitbare Tatsache, dass jede Unternehmung täglich den verschiedensten Risiken ausgesetzt ist. Die Vielfalt der potenziellen Risiken und ihre Behandlung werden komplexer, aufwendiger und schwieriger. Gefahren wie Betrug, Diebstahl, Veruntreuung und Virusattacken werden zunehmen. Die Folge sind vermehrte Ressourcen und Prozesse, die solche Risiken behandeln, grössere finanzielle Rückstellungen müssen getätigt werden.
Für die Mitglieder des Verwaltungsrats und der Geschäftsleitung ist für die Erfüllung ihrer Aufgaben eine hohe Risikotransparenz unerlässlich. Fehlerhafte Geschäftsführung kann strafrechtliche Folgen haben.

Frage an die Führungskräfte: Haben Sie die Risiken in Ihrem Unternehmen schon bewertet und Massnahmen zur Behandlung ausgearbeitet? An den Antworten wären wir sehr interessiert!

4. Die Schritte im Management Prozess

Zur Identifizierung, Analyse, Beurteilung und Behandlung von Risiken empfiehlt sich folgender Prozess:
1. Die Identifikation der Gefahren, Bedrohungen, Verletzbarkeiten
2. Die Analyse der auslösenden Ereignisse
3. Das Aufzeigen der Konsequenzen für die Unternehmung, die Mitarbeiter, die Anteilseigner, die Bevölkerung (in messbaren Grössen)
4. Die Wahrscheinlichkeit bestimmen, mit der das auslösende Ereignis eintrifft (auf einer Skala)
5. Die Bestimmung des Schweregrades eines Schadens (auf einer Skala)
6. Die Entscheidung, welche der Risiken akzeptiert oder behandelt werden sollen
7. Massnahmen mit klaren Verantwortlichkeiten und Terminen treffen
8. Die Bestimmung des weiteren Vorgehens für den Follow-Up.

5. Die wichtigsten Erfolgsfaktoren

Die meisten Risiko-Management Frameworks haben einen ähnlichen Aufbau. Es gibt kein richtiges oder falsches Framework. Wichtig ist, das gewählte Framework unternehmensweit auf allen Stufen durchgängig in die Kultur einzubetten. Alle Bausteine müssen sorgfältig durchgeführt und die erarbeiteten Resultate verständlich dokumentiert werden.

Der Risiko-Management Prozess muss in der „Corporate Governance“ fest verankert und dokumentiert sein. Die Geschäftsleitung unterstützt das gewählte Framework und Vorgehen und stellt die notwendigen Ressourcen zur Verfügung. Abweichungen oder das Nicht-Einhalten der „Corporate Risk Policy“ müssen adressiert und die notwendigen Konsequenzen eingeleitet werden.

Risiko-Management ist weder eine „one-man-show“ noch ein Projekt mit einem Start- und Enddatum. Risiko-Management ist fester Bestandteil der Unternehmensstrategie, der operativen

Planung und der Unternehmungskultur. Der Risiko-Management Prozess muss ständig dem Geschäftsverlauf und der wirtschaftlichen Situation angepasst werden.

Die Verantwortlichkeiten müssen verständlich, klar dokumentiert und bekannt sein. Ein Mitglied der Geschäftsleitung ist für den Risiko-Management Prozess verantwortlich und hat die Kompetenz, Entscheidungen zu treffen und diese auch durchzusetzen.

Risikobeurteilungen der Geschäftsleitung müssen periodisch (zum Beispiel halbjährlich) in einem Workshop überprüft und angepasst werden.

Risiko-Management ist Chefsache!

6. Vorgehen zur Risiken- Identifizierung und -Beurteilung

Das Identifizieren, Beurteilen und Behandeln von unternehmensweiten Risiken ist eine kontinuierliche Aktivität, die von allen Geschäftsbereichen am Idealsten top-down durchgeführt wird.

In einem ersten Schritt wird für die Unternehmung und jede Geschäftseinheit ein Risiko-Katalog bestimmt, verabschiedet und bearbeitet.

Der erste Aufwand richtet sich nach der Grösse des Unternehmens, seiner Produktpalette, der Komplexität der Infrastruktur und seiner Prozesse. Die Erfahrung zeigt, dass die Dauer dieser ersten Schritte von mehreren Wochen bis zu mehreren Monaten dauern kann.

Folgender Prozess hat sich als „Best Practice“ durchgesetzt. Der Aufwand variiert, je nach Komplexität.

<u>Phase 1: Initialisierung</u>
(Aufwand: mehrere Tage bis mehrere Wochen)
- Ausarbeiten eines groben Risiko-Management Plans.
- Bewilligung dieses Vorgehensplans von der Geschäftsleitung.

<u>Phase 2: Ausarbeiten eines Risiko-Management Frameworks</u>
(Aufwand: mehrere Tage bis mehrere Monate)
- Definieren der Risiko-Strategie.
- Definieren einer „Risk Policy“.
- Definieren der Verantwortlichkeiten.
- Definieren der Risiko-Management Prozesse.
- Definieren der Risiko-Management Qualitätssicherung.
- Definieren des Risiko-Management Reportings.

<u>Phase 3: Ausarbeiten eines generischen Risiko-Kataloges für die Unternehmung / Geschäftsbereiche</u>
(Aufwand: mehrere Tage bis mehrere Wochen)
- Erarbeiten, konsolidieren und verabschieden eines Risiko-Kataloges für die Unternehmung / den Geschäftsbereich.

Phase 4: Risiko-Management Workshop
(Aufwand: Vorbereitung mehrere Tage; Durchführung des Workshops 1 bis 3 Tage)
- Planung und Vorbereitung des Workshops.
- Durchführen des Workshops.

Phase 5: Umsetzung der festgelegten Massnahmen
(Aufwand: je nach identifizierten Risiken und definierten Massnahmen mehrere Monate)
- Ausarbeitung und Implementierung von Massnahmen zur Risikobehandlung.

Phase 6: Überprüfung des Risiko-Katalogs, halbjährlich
(Aufwand: ½ bis 1 Tag)
- Planung und Vorbereitung des Meetings.
- Durchführen des Meetings.

Viele KMU starten mit der Phase 4, um erste Erfahrungen zu sammeln und das Risiko-Management-Bewusstsein zu fördern. Für dieses erste Assessment (Vorbereitung, Durchführung und Nachbearbeitung des Workshops) werden je nach Komplexität ca. 20 bis 40 Personentage benötig. Das Definieren der Governance, der Risk Policy und des generischen Risiko-Kataloges sind nicht beinhaltet. Bei diesem Vorgehen ist es empfehlenswert, einen externen Risiko-Management-„Profi“ zu beauftragen.

7. Das Reporting des Risiko-Managements

Sinnvoll ist ein Reportingprozess zur Definition und Implementierung der wichtigsten Ereignisse und Aktivitäten.

Dazu gehört das Informieren über
- beobachtete Ereignisse, z.B. Virusprobleme, Diebstähle, …
- gemessene / bemerkte Auswirkungen (Produktivität, Kosten, Verlust von Kunden/Daten, …)
- getroffene Massnahmen zur Behebung des Problems
- getroffene Massnahmen zum Verhindern von gleichen oder ähnlichen Vorkommnissen
- Ziele im Erarbeiten von behandelnden Massnahmen.

Auch über die beanstandeten Problemkreise der internen und externen Revision muss Bericht erstattet werden.

In der Praxis bewährte sich
- pro Monat einen „Executive Level“ Bericht für den Verwaltungsrat und die Geschäftsleitung
- pro Quartal einen ausführlichen Bericht für die Geschäftsleitung.

Selbstverständlich müssen alle besonderen Ereignisse innerhalb kürzester Zeit der Geschäftsleitung mitgeteilt und gegebenenfalls ein Krisenstab gebildet werden.

8. Zeitpunkt der Durchführung des Risiko-Assessment

Wurde noch nie ein Risiko-Assessment und/oder Notfall-Szenarios dokumentiert und getestet, sollte ein solches Assessment dringend eingeplant und durchgeführt werden.

Ist bereits ein Risiko-Management Prozess in die Unternehmung eingebettet, wird ein Assessment im idealen Fall einige Wochen vor der operationellen Planung durchgeführt. Grössere Aktivitäten und Projekte können so für das Risiko-Management geplant und budgetiert werden.

Unternehmensweite Risiko-Assessments sollten alle 6 Monate eingeplant und durchgeführt werden. Somit ist die Aktualität und Qualität sichergestellt und der Aufwand und die Kosten werden so in Grenzen gehalten.

Risiko-Assessments von umfangreichen Projekten benötigen einen monatlichen Aufwand von 2 bis 3 Stunden.

9. Welche Software sollte eingesetzt werden

Eine der ersten Fragen gilt immer dem richtigen und besten unterstützenden Werkzeug, der Software.

Ein gutes Tool ist natürlich hilfreich und wichtig - aber zweitrangig. Viel bedeutender sind das konsequente Einhalten des Risiko-Management Prozesses und die Einbettung in die Unternehmenskultur.

Es gibt verschiedene Produkte auf dem Markt, die ein weites Spektrum der Anforderungen abdecken. Viele Unternehmen haben innerhalb kurzer Zeit eigene zweckmässige Tools mit MS Office Produkten entwickelt.

10. Darstellung der Selbsteinschätzung und Bewertung

Wenn Sie eine der folgenden Fragen mit „Nein“ beantworten empfiehlt sich, die Corporate Governance und den Risiko-Management Prozess Ihres Unternehmens zu überprüfen.

Fragen	JA	NEIN
Gibt es einen Mitarbeiter (Risiko-Manager), der für den operativen Risiko-Management Prozess, die Durchführung von Risiko-Assessment und das Risiko Reporting verantwortlich ist?	☐	☐
Sind die Risiken und die damit verbundenen Auswirkungen dem Verwaltungsrat und der Geschäftsleitung bekannt?	☐	☐
Wird periodisch (z.B. einmal pro Quartal) ein Risiko-Management Statusbericht dem Verwaltungsrat und der Geschäftsleitung präsentiert? Ist "Risiko-Management" ein fester Agendapunkt von Verwaltungsrats- und/oder Geschäftsleitungssitzungen?	☐	☐
Werden Rücklagen gebildet um folgenschwere Ereignisse finanziell absichern?	☐	☐
Gibt es eine „Corporate Risk Policy“, die allen Mitarbeitern bekannt ist?	☐	☐
Sind in der operationellen Planung Risikobehandlungsmassnahmen eingeplant (Budget, Ressourcen und Zeitrahmen)?	☐	☐
Werden bei grösseren Projekten Risiko-Beurteilungen periodisch durchgeführt und Massnahmen zur Risikobehandlung eingeleitet?	☐	☐
Existieren Notfallpläne, sind diese zugänglich und werden auch Notfallszenarios durchgespielt?	☐	☐
Welche Handlungsanweisungen haben Ihre Mitarbeiter, wenn ein Schadensereignis eintritt, z.B. Feuer, Bombenalarm, Virus, Veruntreuung, etc.?	☐	☐
Sind eindeutige Richtlinien für Ihre Mitarbeiter und SIE vorhanden, wie man Risiken begegnet und sie verringert? Existieren klare Weisungen für den Umgang z.B. mit dem Internet, Daten Up- und Downloads, clean desk policy?	☐	☐

11. Minimale Anforderungen

Minimale Anforderungen an ein „Risiko-Management Framework“

- „Corporate Risk Policy“ der Unternehmung
- Klar definierte Verantwortlichkeiten, „top-down“
- Detailbeschreibung des Risiko-Management Prozesses
  - Vorgehen / Methode
  - Tools
  - Gewünschte Resultate und deren Darstellung
  - Berichtswesen (Was, wann und an wen)
  - Kommunikation
- Detailbeschreibung über die Dokumentation von Entscheidungen (Audit Trail).

Minimale Anforderungen an eine „Risk Policy“

- Beschreibung der Verantwortlichkeiten
- Handhabung von strategischen Risiken
- Handhabung von operationellen Risiken
- Handhabung von finanziellen Risiken
- Handhabung von Markt-Risiken
- Handhabung von Umwelt-Risiken
- Handhabung von Infrastruktur-Risiken
- Handhabung von Investitions-Risiken
- Handhabung von Reputations-Risiken
- Handhabung der Qualitätskontrolle / Audit Trails
- Berichtswesen.

Minimale Anforderungen an die „Corporate Governance“

- Regelung der „Risk Policy“ Verantwortlichkeiten
- Regelung der „Risk Policy“ Änderungen
- Regelung der Durchführung von „Risiko-Assessments“
- Regelung des „Risiko-Management“ Berichtwesens
- Regelung des Vorgehens bei „Risk Policy“ Abweichungen.

12. Quellenverzeichnis

Internet:

http://www.sei.cmu.edu/risk/index.html
http://www.answers.com/risk%20management
http://www.answers.com/risk%20assessment
http://www.risknet.de