Risikobewertung: Wer, wie und wie oft?

written by Christian Hafner | 11 Oktober, 2024

Riskmanagement & IKS News

Risikobewertung: Wer, wie und wie oft?

Warum die Funktion des Risikoeigners matchentscheidend ist – und wer in der Lage ist, gute Risikoentscheide zu fällen.

Für die Wirksamkeit von Risk Management ist ein dynamischer, kontinuierlicher Risikobeurteilungs- und -Bewertungsprozess zentral.

Die folgende Übersicht zeigt die Rollen und Verantwortlichkeiten im Prozess.

	E = Entscheidung *A = Aktion, Verantwortung* *M = Mitarbeit*	***Leitungsorgan***	***Chief Risk Officer CRO***	**Risk Owner**	**Risikobewerter**	**Kontrollen und Massnahmen**
1	Risikoidentifikation und Risk Owner bestimmen	***E***	***A***	***M***		
2	Risikobewerter und Periodizitäten der Bewertungen definieren		***E***	***A***	***M***	
3	Risikobewertung durchführen				***A***	
4	Risikobewertungen auf Durch-führung und Ergebnis prüfen			***A***		
5	Kontrollen und Massnahmen bewilligen und anordnen	***E***	***E***	***A***		***M***
6	Kontrollen und Massnahmen durchführen					***A***
7	Spontane Risikobewertung			***E***	***A***	
8	Monitoring RM-System		***A***	***M***		
9	Reporting an Leitungsorgane	***E***	***A***			

Eine zentrale Rolle hat dabei der Risikoeigner (engl. Risk Owner). Er trägt

die Verantwortung dafür, ein bestimmtes Risiko zu überwachen und zu steuern. Seine Hauptaufgaben sind:

a) Überwachung des Risikos: Sicherstellen, dass das Risiko kontinuierlich beobachtet und analysiert wird.

b) Bewertung und Kontrolle: Massnahmen entwickeln und implementieren, um das Risiko zu mindern oder zu kontrollieren.

c) Berichterstattung: Regelmässiges Berichten über den Status und die Wirksamkeit der Risikomanagementmassnahmen.

d) Verantwortlichkeit: Sicherstellen, dass das Risiko in Übereinstimmung mit den Unternehmenszielen und -richtlinien gemanagt wird.

Kurz gesagt, der Risikoeigner ist für das Management eines spezifischen Risikos verantwortlich und stellt sicher, dass entsprechende Massnahmen ergriffen werden.

Damit das funktioniert, müssen

- die Häufigkeit der Risikobewertung
- der Bewertungsprozess und
- das Anordnen von Kontrollen und Massnahmen

geklärt und prozessual umgesetzt sein.

1. **Häufigkeit**

Die Häufigkeit, mit der eine Risikobeurteilung durchgeführt werden sollte, hängt von verschiedenen Faktoren ab, wie z.B. der Art des Risikos, der Branche, in der das Unternehmen tätig ist, und den gesetzlichen Vorschriften, die in der jeweiligen Region gelten.

Erstaunlicherweise geben nur 23 Prozent der Schweizer Unternehmen an, mehrmals jährlich eine Risikobeurteilung durchzuführen.

Eine gute Praxis ist es, die Häufigkeit der Risikobeurteilung pro Risiko festzulegen. Das Fremdwährungsrisiko z.B. muss häufiger beurteilt werden als die Gefahr eines Felssturzes.

Nur eine regelmässige Durchführung der Risikobeurteilungen stellt sicher, dass die Organisation angemessen auf Risiken vorbereitet ist. In vielen Fällen kann die Periodizität (z.B. quartalsweise) von vornherein festgelegt werden. Sinnvoll kann auch eine Neubewertung bei wesentlichen Änderungen der betrieblichen Abläufe oder des Arbeitsumfelds sein.

Verantwortlich für das Festlegen der Bewertungsperiodizität oder einer Spontanbewertung ist der Risikoeigner.

2. Bewertungsprozess:

2.1 Menschliche Expertise vs. Datenanalyse

Für die Bewertung der Risiken ist in der Praxis oft eine Kombination aus menschlicher Expertise und Datenanalyse am effektivsten.

Experten können wichtige Kontextinformationen liefern und die Ergebnisse der Datenanalyse interpretieren. Gleichzeitig können Datenreihen die objektive Grundlage für fundierte Entscheidungen liefern.

2.2 Bewertungsentscheid

Typischerweise bewertet ein Führungsgremium jährlich in einer Klausurtagung die Risiken neu. Doch dieses Vorgehen hat Nachteile:

1. Gruppendenken erhöht die Risikobereitschaft. Beteiligte gehen gemeinsam grössere Risiken ein, als dies jeder für sich allein tun würde. Potenziell entsteht die Dynamik einer kollektiven Selbstüberschätzung. Im schlimmsten Fall entscheidet die Gruppe als Ganzes schlechter, als wenn der Chef im Alleingang entschieden hätte.
2. Die Dominanz von Personen und Informationen sowie Empfehlungen in den Diskussionen führen zu Verzerrungen in der Meinungsbildung.Teilnehmer haben Angst um ihren Ruf. Ihre Bedenken könnten als persönliche Kränkung empfunden werden; ihre Äusserung könnten andere für töricht halten.

Gute Entscheide fallen, wenn

- die Entscheidungsfindung transparent ist und
- die Meinungen derjenigen, die das Thema am besten beurteilen können, eingeflossen sind.

In der Bewertung von Risiken bewährt sich deshalb ein dezentrales Vorgehen. Experten (interne u/o externe) werden als Risikobewerter ernannt und erhalten den Bewertungsauftrag unabhängig voneinander elektronisch. Jedes einzelne Ergebnis wird im Risikomanagement-System (RMS) erfasst und sofort dem Risikoeigner weitergeleitet.

Wenn dies alles gut funktioniert, kommt die Schwarmintelligenz zum Tragen, und die Konsolidierung der Bewertungen ergibt ein besseres Ergebnis, als wenn

das Gremium entschieden hätte.

Kommt dazu, dass der dezentrale Prozess effizienter ist, da es keine Terminkoordination für das Bewertungsmeeting des Führungsgremiums braucht.

3. Kontrollen und Massnahmen

Der Risikoeigner entscheidet auf der Basis der Risikobewertungen, ob ein Kontrollmechanismus für die Verhinderung des Risikoeintritts oder eine Massnahme zur Risikominderung notwendig ist.

Der Unterschied zwischen einer Kontrolle und einer Massnahme im Rahmen der Risikobewertung liegt in ihrer spezifischen Funktion und Ausrichtung innerhalb des Risikomanagements.

3.1 Kontrollen

Eine Kontrolle (oder auch „Kontrollmechanismus“) ist darauf ausgerichtet, ein Risiko entweder zu verhindern oder es zu erkennen. Kontrollen sind meistens proaktiv und dienen der dauerhaften Überwachung bestimmter Risikofaktoren, um das Auftreten oder die Auswirkungen eines Risikos zu minimieren.

Beispiele: Passwortschutzsysteme, regelmässige Audits, Prozessvorgaben oder IT-Sicherheitsvorkehrungen. Diese sollen das Risiko eines Ereignisses (z. B. eines Datenverlusts) verhindern oder dieses frühzeitig erkennen.

Kontrollen sind Teil eines dauerhaften, etablierten Prozesses. Es sind laufende Mechanismen, die unabhängig vom Auftreten eines Ereignisses aktiv sind und regelmässig durchgeführt werden.

3.2 Massnahmen

Eine Massnahme hingegen bezieht sich auf eine gezielte Handlung, die auf ein spezifisches Risiko oder ein Ereignis reagiert. Massnahmen sind oft reaktiv und zielen darauf ab, das Risiko zu mindern oder vollständig zu beseitigen. Sie werden häufig nach einer Risikobewertung implementiert, um spezifische Schwachstellen zu adressieren.

Beispiele: Schulungen zur Sensibilisierung für bestimmte Risiken, die Einführung neuer Technologien, Änderungen in der Prozessgestaltung oder ein spezifisches Projekt, das einem Risiko entgegenwirkt.

Massnahmen sind eher einmalige oder kurzfristige Initiativen, die als Folge einer Risikobewertung oder eines spezifischen Risikovorfalls beschlossen werden.

3.3 Entscheidungsfindung

Bewährt sich bei der Bewertung von Risiken ein dezentrales Vorgehen, ist für den Beschluss von Kontrollen und Massnahmen ein Gremiumsentscheid (z.B. an einer GL-Sitzung) aus zwei Gründen vorzuziehen.

1. Massnahmen und Kontrollen binden Ressourcen. Von der Nutzen-/Kostenabwägung sind u.U. verschiedene Teile der Organisation betroffen.
2. Beschluss basiert auf einem etablierten Entscheidungsprozesses: Die Alternativen werden klar definiert; die richtigen Informationen wurden zusammengetragen; die Kosten und die Vorteile wurden nicht genau abgewogen.

Alle Überlegungen zum Beschluss sollten reproduzierbar dokumentiert und im Risikomanagement-System (RMS) hinterlegt werden.

Es geht darum festzuhalten, dass die Mitglieder des Leitungsorgans, welche den Entscheid mitgetragen haben, dieselben Annahmen getroffen haben und diese vernünftig abgewogen wurden.

- Wie wurde Einigkeit für das Ziel des Entscheides erreicht?
- Welche Prämissen haben zum Entscheid geführt?

Fazit: Es ist wichtig, dass Risikobeurteilungen nicht nur als einmalige Aufgabe betrachtet werden, sondern als kontinuierlicher Prozess, der regelmässig überprüft und aktualisiert werden muss.

Dreh- und Angelpunkt ist der Risikoeigner (engl. Risk Owner). Er ist für das Management eines spezifischen Risikos verantwortlich und stellt sicher, dass entsprechende Massnahmen ergriffen werden.

So legt er auch die Häufigkeit der Risikobeurteilung für «seine» Risiken fest. Jedes Risiko soll im Idealfall von mehreren Personen unabhängig bewerten werden. Das Ergebnis der Bewertungen dient dem Risikoeigner für seine Überlegungen zu Kontrollmechanismen zur Aufdeckung des Risikoeintritts und Massnahmen zur Risikominimierung.

Die Kontroll- und Massnahmenentscheide sollten allerdings nicht durch den Risikoeigner, sondern das Leitungsorgan gefällt werden, damit die Ressourcenfrage im Kontext der ganzen Organisation beantwortet wird, und der Entscheid auf der Basis eines stabilen, etablierten Prozesses gefällt wird.

Zu guter Letzt: Das oberste Leitungsorgan (VR, Stiftungsrat, Behörde) kann und soll nicht für jede Risikobewertung involviert werden. Wichtig, um einen angemessenen Rahmen für den Umgang mit Risiken zu setzen, ist die Risikokultur eines Unternehmens und der «Tone at the top».

Die oberste Leitung sollte sich selbst immer bewusst sein und im Unternehmen bewusst machen, dass Risikokultur und -management letztlich dazu dienen, das höchste Gut zu schützen – den guten Ruf.