Moritz´sche Risikomühle

Relevante Risikoinformationen erfassen

Frank Moritz 22.12.2017, 08:01

Viele Unternehmen beschäftigen sich derzeit damit ein Risk Management-Systems einzuführen oder ihr bestehendes System in Richtung operationeller Risiken, Risiken aus Prozessen, Personen, Technik sowie externen Einflüssen, zu erweitern. Die ISO 31000 ist hierfür ein guter Leitfaden. Nach ihr ist eine Einführung gut strukturiert möglich, standardisiert durchführbar und somit kein Hexenwerk mehr. Umso mehr verwundert es, dass sich einige Unternehmen schwertun, ein aktiv gelebtes und aktuelles Risikoinventar zu etablieren, mit Risiken, die aktuell, realistisch bewertet und steuerbar sind sowie schrittweise minimiert werden.

Oftmals werden die Systeme als Alibisysteme zur Befriedigung regulatorischer Anforderungen benutzt oder zunächst mit viel Elan gestartet um dann, einige Monate später, mit gleicher Geschwindigkeit zurückgeschraubt zu werden. Die Risiken, die in das System eingepflegt werden, verkommen zu Dauermeldungen,

werden nicht regelmäßig aktualisiert oder hängen seit der Aufnahme unverändert ohne eingeführte Gegenmaßnahmen „in der Luft“. Im Extremfall wird das Risikoinventar ein Kummerkasten für Mitarbeiter, die nicht mehr wissen, wohin mit Ihren Sorgen. Beispielhafte Risikomeldungen aus solchen Systemen können dann sein:

1. Eine mangelhafte Projektplanung verursacht Folgekosten.
2. IT-Sicherheitslücken durch fehlenden Kauf der Software xy.
3. Personalausfall kann zu Verzögerungen im Projekt führen.
4. Die neue Baustelle auf der Autobahnbrücke kann zu Verzögerungen im Lieferprozess führen.
5. Das Kantinenessen ist ein einziges Risiko.
6. Unser First-Level-Support ist ein Risiko, da erreiche ich nie jemanden.

Was können die Gründe sein für ein solches stumpfes Schwert? Ein Risk Management-System ist ein sprachlich sehr anfälliges Gebilde.

Nehmen wir das zweite Beispiel des fehlenden Software-Kaufs. Nehmen wir an, ein Mitarbeiter meldet uns dieses „Risiko“. Ist dieses wirklich ein akzeptables Risiko? Fragen wir uns einmal: Was kann ein Entscheider gegen dieses „Risiko“ tun? Es gibt nur eine einzige Möglichkeit, er kann lediglich diese Software kaufen. Weitere Alternativen bleiben ihm nicht. Er wird demnach die Risikowerte, wie Schadenhöhe und Eintrittswahrscheinlichkeit den Kosten für die Gegenmaßnahme (Lizenz- und Prozesskosten) entgegenstellen und sich für oder gegen den Kauf entscheiden.

Schaut man sich das „Risiko“ aber mal genauer an, stellt man schnell fest, dass es sich hier um gar kein „echtes Risiko“ handelt. Zunächst einmal ist das Ereignis bereits aufgetreten, liegt also in der Gegenwart. Risiken liegen immer in der Zukunft. Hier mag man noch Argumentieren: „... aber ein Schaden kann ja erst in der Zukunft eintreten.“ Betrachtet man den Satz jedoch etwas genauer, wird klar, dass sich das eigentliche Risiko noch hinter dieser Meldung versteckt. Das Risiko oder vielmehr die Risiken sind: „Produktionsausfälle ...“ oder „Erpressbarkeit aufgrund einer Attacke auf die IT-Systeme von außen.“ Das Fehlen der Software ist demnach eine fehlende Gegenmaßnahme gegen das eigentliche Risiko. Und vor allem: Es ist

nur eine von mehreren möglichen Gegenmaßnahmen. Eventuell gibt es organisatorische, prozessuale, strukturelle Lösungen oder noch andere Softwarepakete. Vielleicht liegen mögliche Maßnahmen auch in der Nutzung (oder Nicht-Nutzung) von Cloud-Systemen und weiteren, neuen Sicherheitsstufen. Aus diesem Grunde bezeichne ich diese Erstmeldungen, als „Risikomeldungen“ aus denen erst die eigentlichen Risiken extrahiert werden müssen.

Plötzlich, durch einfache Umformulierung einer „Risikomeldung“ zu einem echten „Risiko“, sind weitere Gegenmaßnahmen denkbar und abzuwägen. Der Risikomelder gibt nicht die einzige Lösung vor, sondern wird zu einem Teil der Lösungsfindung.

Dieses Beispiel zeigt, wieso die falsche Formulierung eines Risikos den gesamten Risk-Management-Prozess aushebeln kann und warum diese „Risikomeldungen“ den Prozess blockieren können.

Die Risikomühle zur strukturierten Formulierung von Risiken

Auf eine Stufe mit den „als Risiko formulierten fehlenden Gegenmaßnahmen“ lassen sich weitere Arten von „Risikomeldungen“ stellen, wie beispielsweise etwas anders formulierte Schäden (siehe Beispiele 1 und 5), globalen Allgemeinplätzen (Beispiel 3), Meldungen die außerhalb des Einflussbereichs des Risk Managements liegen (Beispiel 4) und einige weitere. Die Bezeichnung eines Betrages als „Risikomeldung“ soll daher die Meldung nicht abwerten, aber vorbereiten, dass bis zur Erarbeitung des eigentlichen Risikos noch ein Weg vor den Protagonisten liegt.

Um aus den „Risikomeldungen“ die echten Risiken herauszuarbeiten, hat sich in der Praxis ein Tool bewährt, dass durch die richtigen Fragestellungen die relevanten Daten aus der Risikomeldung zieht und für den Risikomanagement-Prozess vorbereitet: Die Moritz´sche Risikomühle [siehe ► Abb. 01].

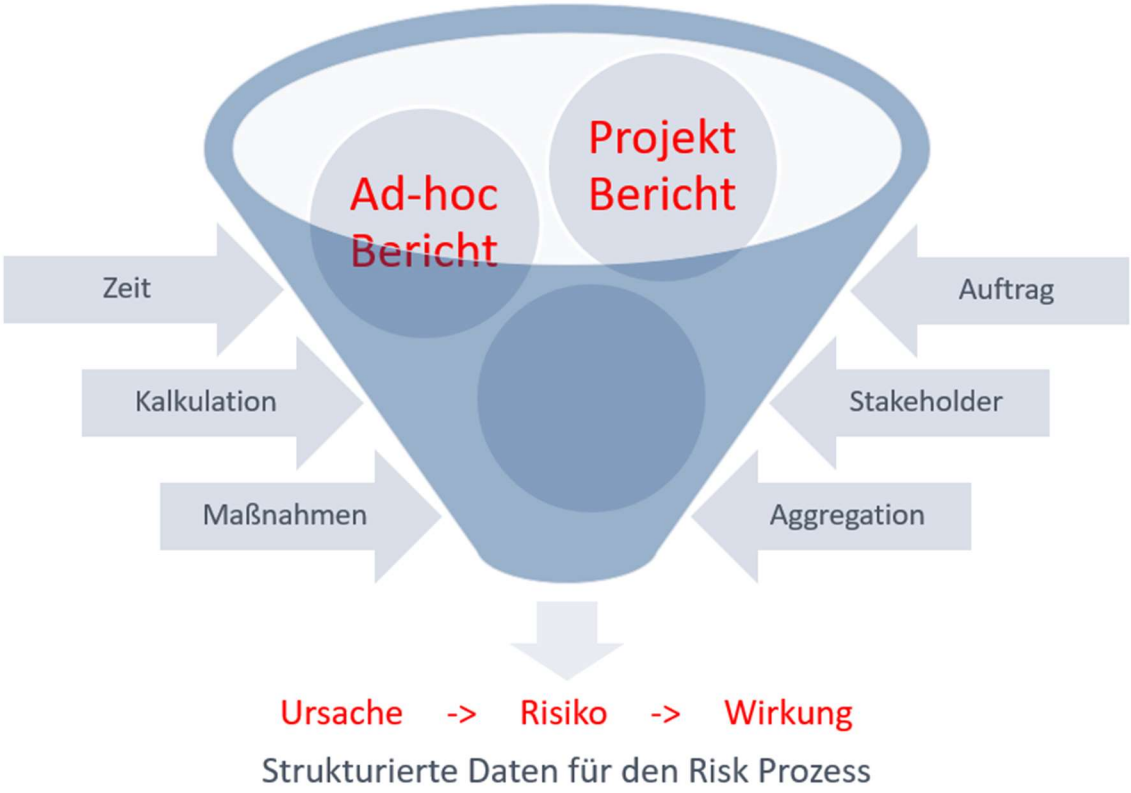

Abb. 01: Die Moritz´sche Risikomühle [Quelle: Frank Moritz]

In die Risikomühle werden Ad-hoc-Risiko-Meldungen genauso wie Risiken aus dem Reporting eingefüllt.

In sechs Schritten zum Ziel

Im **Schritt 1** wird der Zeitfaktor geprüft. Risiken müssen per Definition immer in der Zukunft liegen, denn sie sind eine mögliche Abweichung einer Zielerreichung in der Zukunft. Alle Dinge, die bereits passiert sind oder, bei denen der Eintritt sicher ist, sind Schäden und keine Risiken. Gemeldete Schäden sind beim Risikomanagement falsch platziert, hier müssen, je nach Schaden der Projektleiter, das Controlling, Vorgesetzte oder ein Krisenmanager informiert werden. Sehr wohl kann jedoch ein Risikomanager einen

gemeldeten Schaden aufnehmen und bewerten um daraus mögliche Risiken in der Zukunft abzuleiten.

Bei Beispiel Nr. 1 können wir unterscheiden zwischen existentem Schaden aus einer mangelhaften Projektplanung (die Formulierung lässt darauf schließen, dass der Melder dies derzeit bereits so sieht) und möglichen Schäden (also Risiken, wie beispielsweise Spätwirkungen) in der Zukunft. Bei der Formulierung des Risikos darf ausschließlich der zweite Teil mit einbezogen werden. Der bereits existierende Schaden liefert dagegen eventuell Zahlen zur Risikobewertung.

Im **zweiten Schritt** wird geprüft, ob die Risikomeldung im Verantwortungsbereich der Linienfunktion beziehungsweise des Projektes liegt. An Risiken kann nur derjenige arbeiten, d.h. sie korrekt einschätzen und minimieren oder wahlweise auch akzeptieren, der Kompetenz und Verantwortung für diesen Bereich trägt.

Nehmen wir das Beispiel Nr. 5 mit der Kantine als Risikomeldung für ein IT-Projekt. Kann es in der Verantwortung des IT-Projektleiters liegen für die Qualität des Kantinenessens verantwortlich zu sein? Nein, natürlich nicht. Was kann er dagegen tun? Wo endet sein Verantwortungsbereich? Er kann relevante Daten besorgen und an verantwortliche Stellen weiterleiten und sich auf seinen Risikoteil beschränken und der wäre ein eventueller Personalausfall. Wir sehen hier, dass die Meldung zu dem schlechten Kantinenessen lediglich die Eintrittswahrscheinlichkeit zu dem relevanten Risiko „Personalausfall“ beeinflusst.

Wir müssen uns die Fragen stellen:

- Wer ist betroffen, wenn der Schaden eintritt?
- Um welchen möglichen Schaden handelt es sich konkret?
- Wer hat ein Interesse an Gegenmaßnahmen und ist auch bereit dafür zu zahlen?

Dann haben wir unseren, relevanten Teil der Risikomeldung extrahiert. Was tun wir mit Risiken, die z.B. über zwei Unternehmensbereiche reichen? Wir können diese Risiken aufteilen

oder, wenn die Gegenmaßnahmen ausschließlich zusammen durchgeführt werden können, das Risiko eine Ebene höher allokieren bzw. einen Ausschuss beauftragen dieses Risiko zu bearbeiten.

Der **dritte Schritt** betrifft die Kalkulation eines Risikos. Risiken, die nicht messbar sind, sind keine Risiken. In der Regel besitzt der Risikomelder viele zahlenbasierte Informationen zu der Risikomeldung, wie z.B.:

- Wie oft ist das Risiko bisher eingetreten?
- Welche Schäden wurden verursacht?
- Sind es überhaupt relevante Schäden, die die Aufnahme ins Risikoinventar rechtfertigen?
- Gibt es offizielle aktuelle Statistiken, die zur Zahlengewinnung herangezogen werden können?
- Wie viele Personen sind bei einem möglichen Schadeneintritt betroffen?

Mit diesen Werten lässt sich ein Risiko einschätzen, bei weiter fortgeschrittenen Risk-Management-Prozessen sogar simulieren, so dass Entscheidungen über mögliche Gegenmaßnahmen oder Akzeptanz des Risikos getroffen werden können.

In einem **vierten Schritt** werden die vorhandenen Stakeholder identifiziert. Wichtig ist es hier ein belastbares Rollenmodell zu besitzen, so dass die betroffenen und beteiligten Personen zugeordnet werden können. Wer ist befugt über das Risiko zu entscheiden? Wer führt operativ Gegenmaßnahmen durch? Gibt es hier eventuell mehrere Maßnahmen-Manager? Welche Experten können noch bei der Einschätzung des Risikos helfen? Wer soll die Entwicklung des Risikos im weiteren Ablauf beobachten und reporten?

Der **fünfte Schritt** betrifft die möglichen Gegenmaßnahmen. In der Regel weiß ein Risiko-Melder bereits sehr genau was gegen dieses Risiko gemacht werden kann. Oft ist eine dieser Gegenmaßnahmen auch die Motivation für die Risiko-Meldung. Wird beispielsweise Geld

benötigt, um die Maßnahme zu finanzieren oder benötigt man Zugriff auf Personen oder Daten dann ist der Melder oft nicht in der Lage dies selbst zu entscheiden.

Wichtig ist es hier darauf zu achten, dass der Risiko-Prozess-Verantwortliche in Zusammenarbeit mit dem Melder nicht nur die präferierte Gegenmaßnahme beleuchtet, sondern alle möglichen, sofern dies wirtschaftlich sinnvoll ist. Sind es präventive Maßnahmen, die gegen den Eintritt des Risikos wirken? Sind es reaktive Maßnahmen, die als Sofortmaßnahme beim Eintritt des Risikos wirken oder als Korrekturmaßnahme dann dafür Sorge tragen, dass das Risiko nicht erneut eintritt? Oder sind es evtl. nur Maßnahmen, die Informationen über das Risiko besorgen, also analysierend wirken oder bei dessen Beobachtung helfen? Welche Kosten und welche Wirkung haben diese Maßnahmen? An dieser Stelle kann der Risiko-Prozess-Verantwortliche auf bereits laufende oder vorgeschlagene Maßnahmen zu anderen Risiken aufmerksam machen und somit zusätzliche Seiteneffekte erzielen oder Bedeutungen herausheben.

Als **sechster und letzter Schritt** muss schließlich die Risiko-Aggregation durchgeführt werden. Wir haben nun eines oder mehrere Risiken aus der „Risiko-Meldung“ herausgearbeitet und müssen überprüfen, ob das Risiko nicht bereits in Gänze oder in Teilen im Inventar vorhanden ist. Gibt es evtl. ein verwandtes Risiko oder muss eines neu aufgeteilt werden? Evtl. ergibt sich ja auch einfach nur die Notwendigkeit ein bereits vorhandenes Risiko im mathematischen Modell zu ergänzen. Auch müssen evtl. positive Szenarien, also Chancen überprüft werden.

Erst jetzt ist es an der Zeit den richtigen Risikotitel zu finden und zu verankern, der das Risiko voll umfänglich beschreibt. Das Analyseformular beherbergt nun alle Daten, die Sie zur Unterscheidung in Ursache, Risiko und Wirkung oder zur Befüllung Ihrer Risiko-Datenbank benötigen.

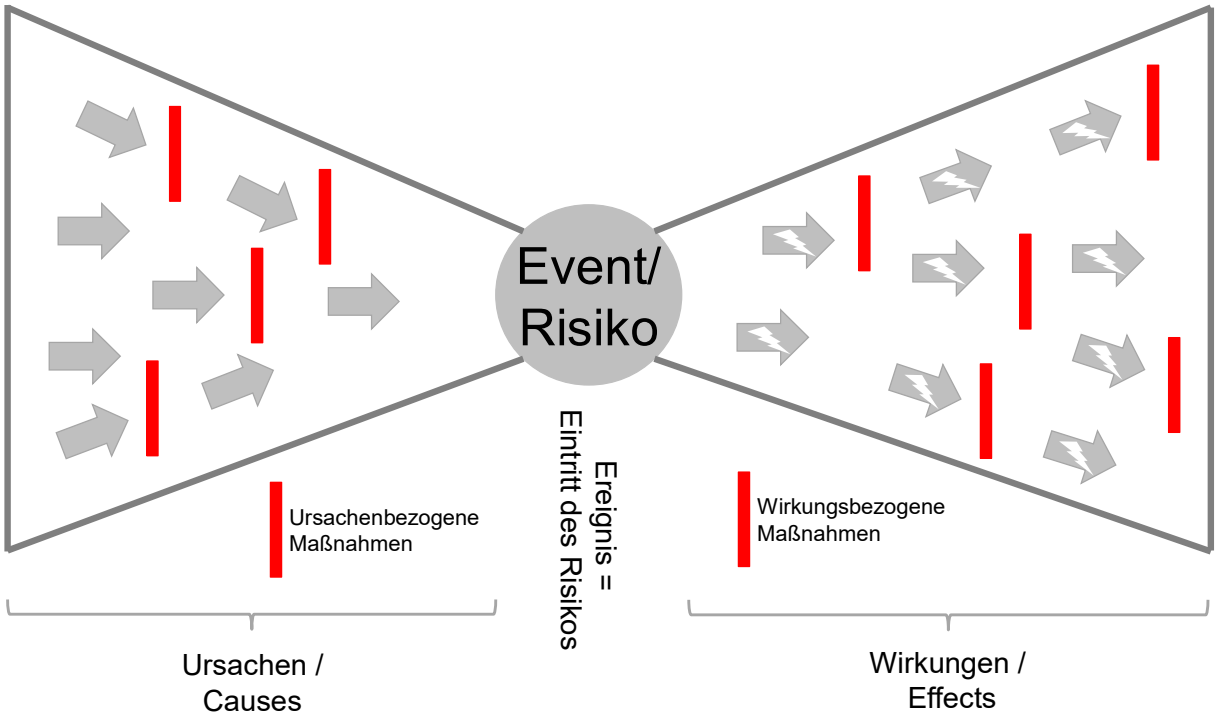

Abb. 02: Grafik Ursache, Risiko, Wirkung [Quelle: Romeike 2018]

Fazit und Ausblick

Für eine Analyse einer solchen Risiko-Meldung benötigt der erfahrene Risiko-Prozess-Verantwortliche zusammen mit dem Melder rund eine Stunde Zeit. Vor allem aufgrund dieses Zeitbedarfs ist es wichtig, nicht jede Meldung im Detail zu analysieren, sondern bereits eine Vorauswahl zu treffen. Hierzu kann es sinnvoll sein einem Risiko-Melder diese Definition mit Hilfe der Risiko-Mühle zu erläutern, denn somit erhält er eine realistische Chance direkt werthaltige Beiträge zu dem Risiko-Inventar zu leisten. Meldungen, wie die Nr. 6 „Unser First-Level-Support ist ein Risiko, da erreiche ich nie jemanden“ wird er dann hoffentlich in Zukunft nicht mehr abgeben und erst recht werden diese nicht mehr in einem Risiko-Inventar landen.

Im Risk Management-Prozess kann die Risikomühle als zentrales Tool der Phase der Risikoanalyse am sinnvollsten eingesetzt werden.

Quellenverzeichnis sowie weiterführende Literaturhinweise:

Romeike, F. (2018): Risikomanagement, Springer Verlag, Wiesbaden 2018.

Autor:

Frank Moritz, aus Neuss, geb. 1967, ist seit 2002 im den Themenfeldern Risikomanagement und Projektmanagement unterwegs. Er war bereits tätig als Interim Manager, Projektleiter, als Trainer und Coach. Weiterhin ist er zertifizierter Auditor zur ISO 20000 und DSGVO, weitere Informationen gibt es unter: www.frankmoritz.de

Quelle: Fachzeitschrift RiskNet, 22.12.2017

Link: https://www.risknet.de/themen/risknews/relevante-risikoinformationen-erfassen/