Operationelle Risikoereignisse: Interne und Externe Daten

Praxisleitfaden Operationelles Risiko

Gesponsort von:

DGOR
Deutsche Gesellschaft für Operational Risk Management e.V.

IBM OpenPages® with Watson®

THE INSTITUTE OF OPERATIONAL RISK
An IRM Group Company

Vorwort

Das Institute of Operational Risk (IOR) wurde im Januar 2004 gegründet und ist seit 2019 Teil des Institute of Risk Management. Die Aufgabe des IOR besteht darin, die Entwicklung des operationellen Risikos als Berufszweig zu fördern und eine solide Praxis für das Management operationeller Risiken zu entwickeln und zu verbreiten.

Die Notwendigkeit eines effektiven Managements operationeller Risiken ist akuter denn je. Ereignisse wie die globale Finanzkrise oder die COVID-19-Pandemie verdeutlichen die weitreichenden Auswirkungen von operationellen Risiken sowie die Konsequenzen eines Versagens ihres Managements. Vor dem Hintergrund dieser und zahlreicher anderer Ereignisse müssen Unternehmen sicherstellen, dass ihre Richtlinien, Vorgehensweisen und Prozesse für das Management operationeller Risiken den Anforderungen ihrer Stakeholder gerecht werden.

Dieser Leitfaden soll bestehende Standards und Normen für das Risikomanagement (wie z.B. ISO31000) ergänzen. Ziel ist es, einen Leitfaden zur Verfügung zu stellen, der sowohl auf das Management operationeller Risiken fokussiert, als auch in der Anwendung praxisnah ist. Dabei handelt es sich um eine Orientierungshilfe für Experten auf dem Gebiet des Managements operationeller Risiken, um die praktische Anwendung in ihren Unternehmen zu unterstützen und zu verbessern. Leser, die an einem allgemeinen Verständnis der Grundlagen des Managements operationeller Risiken interessiert sind, sollten mit dem IOR Certificate in Operational Risk Management beginnen.

Nicht alle Hinweise in diesem Dokument werden für jedes Unternehmen oder jede Branche relevant sein. Es wurde jedoch mit Blick auf ein möglichst breites Spektrum von Unternehmen und Sektoren verfasst. Die Leser sollten individuell entscheiden, was für ihre aktuelle Situation relevant ist. Entscheidend ist eine schrittweise, aber kontinuierliche Verbesserung.

Die Handlungsempfehlungen des Institute of Operational Risk

Obwohl es keinen allgemeingültigen Ansatz für das Management operationeller Risiken gibt, ist es wichtig, dass Unternehmen ihre Vorgehensweise regelmäßig überprüfen und verbessern. Das vorliegende Dokument ist Teil einer Reihe von Papieren, die praktische Anleitungen zu einer Reihe wichtiger Themen in der Disziplin Operational Risk Management bieten. Ziel dieser Papiere ist es:

- Zu erklären, wie man ein (robustes und effektives) Rahmenwerk für das Management operationeller Risiken entwickelt und umsetzt
- Den Wert des Operational Risk Managements aufzuzeigen
- Die Erfahrungen von Risikoexperten zu reflektieren - inkl. der Herausforderungen bei der Entwicklung eines Rahmenwerks für das Management operationeller Risiken

Contents

Abschnitt 1 - Einführung

Ein Schadensereignis bzw. Schadensereignisse sind die Gesamtverluste für den Erst- oder Rückversicherer, die aus einer Ursache/aus mehreren Ursachen resultieren. Die Sammlung, Analyse und Berichterstattung von Daten zu operationellen Schadensereignissen ist das Rückgrat eines soliden Rahmens für das Management operationeller Risiken nicht nur für Versicherungsunternehmen. Daten über tatsächliche Ereignisse stellen eine greifbare Informationsquelle über Wahrscheinlichkeit und Auswirkungen von operationellen Risiken dar und tragen dazu bei, die Subjektivität von Bewertungen und Berichten über operationelle Risiken zu verringern. Daten bieten Unternehmen auch die Möglichkeit, aus vergangenen Ereignissen zu lernen, wobei eine effektive Rückschau eine genauere Vorausschau fördern kann.

Dieser Leitfaden erläutert, wie Prozesse für die Sammlung und Nutzung interner operationeller Schadensfalldaten und ggf. für die Nutzung externer Schadensfalldaten gestaltet und umgesetzt werden können. Dabei kombiniert und aktualisiert der Praxisleitfaden die separaten Praxisleitfäden, die zuvor vom IOR zu externen und internen Schadensfalldaten herausgegeben wurden.

Abschnitt 2 – Nutzenvergleich von internen und externen Ereignisdaten

Die Sammlung interner Daten über operationelle Schadensfälle ermöglicht es einem Unternehmen, sich ein Bild von seiner tatsächlichen Gefährdung durch operationelle Risiken zu machen. Je zeitnaher die Sammlung dieser Daten erfolgt, desto realistischer wird dieses Bild sein. Und je umfassender die Datenerfassung ist, desto genauer wird das Bild sein.

Interne Ereignisdaten können zur Unterstützung einer Reihe von Aktivitäten innerhalb des Prozesses zum Management des operationellen Risikos verwendet werden. Tabelle 1 fasst die wichtigsten Vorteile zusammen.

Prozessziel	Vorteile interner Verlustdaten
Identifikation	Kann neue operationelle Risiken aufdecken, die zuvor nicht identifiziert wurden.
Bewertung	Stellt Informationen zur Verfügung, um die Bewertung der Eintrittswahrscheinlichkeit und des Umfangs der möglichen Auswirkungen zu unterstützen.
Überwachung	Liefert Informationen über die aktuelle Risikolage und die Wirksamkeit der Kontrollen. Anhand von Trends lässt sich feststellen, ob das Risikovolumen zu- oder abnimmt.
Steuerung	Im Rahmen der Steuerung kann die Wirksamkeit von Kontrollen beurteilt und verbessert werden. Schadensfälle bieten einen Live-Test zur Wirksamkeit von Kontrollen. Sie können auch Aufschluss darüber geben, wie Kontrollen in Zukunft verbessert werden können.

Tabelle 1: Verwendung interner Daten zur Unterstützung des operationellen Risikomanagementprozesses

Externe Datenbanken können verwendet werden, um interne Daten zu ergänzen. Nur wenige Unternehmen werden das gesamte Spektrum an operationellen Schadensereignissen erleben, denen sie ausgesetzt sind, insbesondere in Bezug auf seltene, unwahrscheinliche Ereignisse mit hohen Auswirkungen. Externe Daten ermöglichen es, die von vergleichbaren Unternehmen erlebten Ereignisse einzubeziehen, die verfügbare Stichprobengröße für die Datenanalyse zu erhöhen und die in Tabelle 1 genannten Vorteile zu steigern.

Quellen für externe Daten lassen sich hauptsächlich in zwei Typen einteilen. Die verfügbaren Daten jedes Typs unterscheiden sich in einer Reihe von Aspekten.

Datenkonsortien beruhen auf Zulieferungen von Mitgliedern, die verpflichtet sind, Daten innerhalb des Konsortiums zu teilen. Es gibt strenge Berichtskriterien, die sicherstellen, dass jedes Mitglied alle Ereignisse meldet, die durch den Konsortiumsvertrag abgedeckt sind. Die Identität der Mitglieder ist dabei durch ein gewisses Maß an Anonymisierung geschützt. In den meisten Fällen ist die Anzahl der Datenelemente viel höher als bei öffentlichen Datenquellen, da die Mitglieder alle Schadenereignisse an das Konsortium melden müssen, auch solche, die vielleicht weniger berichtenswert sind und in der Finanzpresse wenig oder gar keine Berichterstattung erhalten.

Die größten Vorteile von Daten des Konsortiums sind ihre Vollständigkeit, Genauigkeit und Relevanz für die Mitglieder. Konsortien achten darauf, sinnvolle Gruppierungen von Unternehmen zu bilden, um sicherzustellen, dass die von den anderen Mitgliedern gelieferten Daten relevant sind. In dieser Hinsicht können die Daten aus dem Konsortium oft mit internen Daten auf eine statistisch robuste Weise kombiniert werden. Allerdings können die Mitgliedsbeiträge hoch sein, und die Mitglieder müssen strenge Datenzulieferanforderungen erfüllen.

Auf öffentlichen Quellen basierende Datenquellen filtern und analysieren öffentliche und spezialisierte Nachrichtenquellen und veröffentlichen die Daten erneut in einer für die Analyse des operationellen Risikos geeigneten Form. Solche Quellen haben nur Zugang zu den Fällen mit größerem Nachrichtenwert, fügen aber in der Regel weitere Informationen zu jedem Ereignis hinzu, einschließlich Angaben darüber, welches Unternehmen den Verlust erlitten hat, Details zum Versagen von Kontrollen sowie begünstigende Faktoren und Folgen des Ereignisses.

Datenbanken aus öffentlichen Quellen sind in der Regel kostengünstiger und es gibt keine Datenzulieferpflichten. Allerdings bedeutet die öffentliche Natur der Daten, dass sie wahrscheinlich nicht so genau oder vollständig sind. Nichtsdestotrotz können öffentliche Daten eine wertvolle Informationsquelle für Ereignisse mit geringer Wahrscheinlichkeit und großen Auswirkungen sein, da diese in der Regel die Medien erreichen. Sie können auch auf neu auftretende operationelle Risiken hinweisen, wenn Ereignisse bereits öffentlichkeitswirksam in anderen Unternehmen aufgetreten sind (z.B. neue Arten von Cyber-Risiken).

Abschnitt 3 - Die Elemente operationeller Risikoereignisse: Schlüsselkonzepte

Durch die vielschichtige Natur von operationellen Risikoereignissen gibt es eine Reihe von Konzepten, die vor der Implementierung eines wirksamen Prozesses zur Erfassung von Schadensfällen verstanden werden müssen.

Abschnitt 3.1 – Tatsächliche Schäden und Beinaheschäden

Definitionsgemäß erfordert die Sammlung von Daten über Schadensereignisse die Erfassung von Informationen über tatsächliche Verluste. Einige Unternehmen entscheiden sich, darüber hinaus Informationen über “Beinaheschäden” (so genannte „Near Misses“) zu sammeln.
Ein Beinaheschaden ist ein Ereignis, das zwar eingetreten ist, aber zu keiner Art von Verlust geführt hat (z.B. finanzieller Verlust, Reputationsverlust, menschlicher Verlust). Verluste können durch Glück oder durch die Wirksamkeit bestimmter Kontrollen abgewendet worden sein. Zum Beispiel kann eine Zahlung an einen Lieferanten zweimal erfolgt sein, aber der Lieferant meldete den Fehler und das Geld wurde zurückgegeben. Ebenso kann ein Kontoabgleich nach der Zahlung den Fehler aufgedeckt haben.

Informationen über Beinaheschäden können sehr wertvoll sein. Sie liefern ein Frühwarnsignal für Ereignisse, die in der Zukunft zu Verlusten führen können. Untersuchungen in diesem Bereich zeigen, dass eine Reihe von Beinaheschäden oft vor einem größeren operationellen Verlust auftritt. Wenn Unternehmen also Informationen darüber sammeln können, kann dies dazu beitragen, größere Verluste in der Zukunft abzuwenden. Ebenso geben Informationen über Beinaheschäden Aufschluss über die Wirksamkeit von Kontrollen.

Abschnitt 3.2 – Datum und Dauer des Ereignisses

Anhand dieser Informationen kann ein Unternehmen historische Trenddaten erstellen, die Aufschluss darüber geben, wie sich die Exposition im Laufe der Zeit verändert.
Es ist üblich, Daten zu zwei Zeitpunkten zu sammeln. Der Zeitpunkt, an dem das Ereignis zum ersten Mal erkannt wurde, und der Zeitpunkt, an dem das Ereignis beendet wurde. Viele operationelle Risikoereignisse dauern Tage, sogar Wochen, Monate oder Jahre. Zum Beispiel dauert es oft Jahre, bis Haftungsansprüche geklärt sind.

In Bezug auf den Beginn eines Ereignisses gehen einige Unternehmen über das Datum der ersten Entdeckung hinaus und suchen nach dem Datum, an dem sich das Ereignis zum ersten Mal manifestiert hat - was einige Zeit vor seiner Entdeckung liegen kann. Zum Beispiel kann eine Verschmutzung an einem Standort auftreten, aber erst nach einigen Wochen, Monaten oder sogar Jahren entdeckt werden. Die Identifizierung des ersten Datums, an dem sich ein Ereignis manifestiert hat, kann jedoch eine zeitaufwändige Aufgabe sein, die viel Detektivarbeit erfordert. Es kann jedoch z.B. bei Versicherungsansprüchen vorteilhaft sein und einem Unternehmen helfen, seine Fähigkeit zur rechtzeitigen Erkennung von Ereignissen in der Zukunft zu verbessern. Sollte sich herausstellen, dass ein Ereignis in einem früheren Geschäftsjahr eingetreten ist, kann es sinnvoll sein, die Buchführung zu ändern, insbesondere wenn es sich auf die ausgewiesenen Gewinne und damit z.B. die Körperschaftssteuer ausgewirkt hat.

Abschnitt 3.3 – Art des Risikoereignisses

Die Zuordnung eines Ereignisses zu einer bestimmten Kategorie des Ereignistyps für das operationelle Risiko ist ein wesentlicher Bestandteil jedes Prozesses zur Erfassung von Ereignissen für das operationelle Risiko sowie zur Berichterstattung. Durch die Zuordnung von Ereignissen ist es möglich, ein Bild des aktuellen Risikoprofils eines Unternehmens zu erstellen. Dies kann dann genutzt werden, Bereiche mit hoher Gefährdung zu identifizieren und die Ressourcen entsprechend zu priorisieren. Weitere Informationen finden Sie im IOR-Praxisleitfaden zur Kategorisierung operationeller Risiken.

Abschnitt 3.4 - Ort

Neben der Kategorisierung von operationellen Risikoereignissen ist es wichtig, Daten über den Ort des Ereignisses zu sammeln, um ein “geografisches” Profil der Ereignisse zu erstellen.

Der Standort umfasst den physischen Ort eines Ereignisses (z.B. die Einrichtung oder den Standort, in der/dem das Ereignis aufgetreten ist) und die Geschäftseinheit(en), Funktion(en) oder Abteilung(en), von der/denen das Ereignis ausging (z.B. Finanzen, Operations, Personal).

Abschnitt 3.5 - Ursachen

Alle operationellen Risikoereignisse haben Ursachen. Oftmals mehrere Ursachen. Diese Ursachen können Ketten bilden, die aus der unmittelbaren Ursache, einer Zwischenebene oder der Basisursache bestehen, wie in Abbildung 1 dargestellt.

Was die Risikomodellierung betrifft, können Risiko- und Kontrollindikatoren als Variablen in statistischen Modellen verwendet werden. Alternativ können sie auch zur Validierung dieser Modelle verwendet werden. Fragen sollten gestellt werden, wenn es eine wesentliche Änderung in den Vorhersagen eines Risikomodells gibt, aber keine Änderung in den zugehörigen Risiko- und Kontrollindikatoren oder andersherum. Eine solche Situation kann darauf hinweisen, dass entweder das Risikomodell unvollkommen ist oder dass die falschen Indikatoren identifiziert wurden.

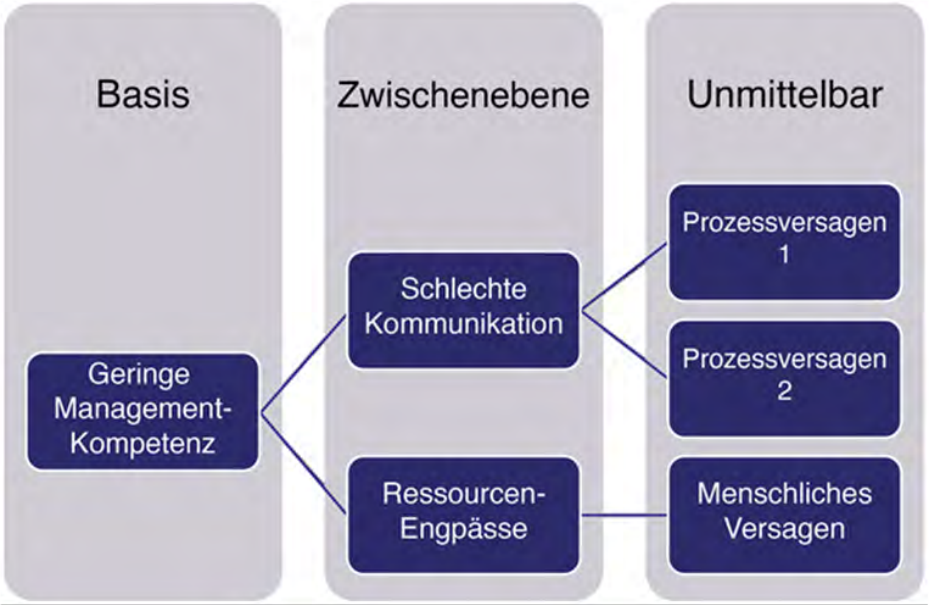

Abbildung 1: Ursachenebenen

Kausalketten können sich über mehrere Ursachenebenen erstrecken, manchmal sogar über mehr als drei. Bei der Erfassung von Daten zu operationellen Risikoereignissen wird diese Detailtiefe jedoch nur selten erfasst. Viele Unternehmen sammeln lediglich Informationen über die primäre Ursachenkategorie (z.B. Menschen, Prozessversagen, Systemversagen oder externes Ereignis). Andere verwenden detailliertere Kategorien, die zwar ein genaueres Bild der Kausalkette ermöglichen, aber die Komplexität und Kosten der Datenerfassung erhöhen.

Ein Kompromiss ist es, die Kausalketten von Großschäden zu untersuchen, aber nicht für Ereignisse mit geringen Auswirkungen, sofern dort der Aufwand aus Kosten-Nutzen-Gründen weniger gerechtfertigt ist. Weitere Informationen zur Kategorisierung von Ursachen finden Sie im IOR-Praxisleitfaden zur Kategorisierung operationeller Risiken.

Abschnitt 3.6 - Kontrollversagen

Kontrollversagen kann als Ursache behandelt oder die Daten können separat gesammelt werden. Die meisten operationellen Schadensfälle sind mit dem Ausfall einer oder mehrerer Kontrollen verbunden. Daher können sie eine wertvolle Informationsquelle für die Wirksamkeit von Kontrollen sein. Durch das Verständnis, wie und warum Kontrollen versagt haben, können gezielte Maßnahmenpläne erstellt werden, um ähnliche Fehler in Zukunft zu vermeiden. Neben der Aufdeckung potenzieller Fehler können operationelle Risikoereignisse auch wirksame Kontrollen aufzeigen, insbesondere in Bezug auf investigative und mitigierende Kontrollen. Wirksame investigative Kontrollen werden dem Unternehmen geholfen haben, zu erkennen, dass ein Ereignis eingetreten ist. Mitigierende Kontrollen können dazu beigetragen haben, die Auswirkungen des Ereignisses zu reduzieren.

Abschnitt 3.7 – Direkte und indirekte Einflüsse

Bei der Bestimmung der Auswirkungen eines operationellen Risikoereignisses auf ein Unternehmen werden zwei Elemente berücksichtigt: direkte Auswirkungen, z.B. eine Geldstrafe, Strafe oder Überstundenzahlungen, und indirekte Auswirkungen, z.B. ein Verlust von Marktanteilen oder Umsatzeinbußen.

Bei der Untersuchung eines Ereignisses sind direkte Auswirkungen relativ einfach festzustellen, während indirekte Auswirkungen möglicherweise nicht sofort identifizierbar sind und erst bei der Bewältigung des Ereignisses zutage treten (z.B. die Auswirkungen eines Ereignisses auf die Verkaufszahlen).

Abschnitt 3.8 – Finanzielle und nicht-finanzielle Auswirkungen

Operationelle Risikoereignisse können sowohl finanzielle als auch nicht-finanzielle Auswirkungen haben. Wie bereits erwähnt, können die finanziellen Auswirkungen direkt oder indirekt sein und sich auf die Kosten beziehen, die mit dem Ersatz verlorener Vermögenswerte, Aufräumarbeiten, Haftungsansprüchen, Geldbußen usw. verbunden sind.

Nicht-finanzielle Auswirkungen sind per Definition schwer zu quantifizieren, insbesondere da sie nicht sofort als mit einem bestimmten Ereignis verbunden identifiziert werden können und möglicherweise erst einige Zeit nach dem Ereignis auftreten. Beispiele für nicht-finanzielle Auswirkungen sind u.a. Reputationsschäden, Verlust von Firmenwert und Kundenvertrauen. Solche Auswirkungen können anhand eines definierten Bereichs - z.B. niedrig, mittel, hoch - bewertet werden, der durch Bezugnahme auf ein geeignetes Maß kalibriert wird, wie z.B. bei der Auswirkung auf eine Dienstleistung die Anzahl der betroffenen Kunden und die Dauer des Serviceausfalls.

Abschnitt 4 - Umsetzung

Aufgrund der vielschichtigen Natur von operationellen Risikoereignissen gibt es eine Reihe von Konzepten, die vor der Implementierung eines wirksamen Prozesses zur Erfassung von Schadensfällen verstanden werden müssen.

Abschnitt 4.1 - Anpassung an das breitere Rahmenwerk für operationelle Risiken

Um wirksam zu sein, müssen die Prozesse zur Erfassung von Ereignisdaten für operationelle Risiken in die Prozesse und Verfahren zum Management operationeller Risiken integriert werden. Dies sollte Folgendes beinhalten:

- Sicherstellen, dass die Governance-Regelungen des Unternehmens die Erfassung von Ereignisdaten zum operationellen Risiko unterstützen. Dies kann interne Prüfungen der Erfassungsprozesse und der Einhaltung dieser Prozesse beinhalten, die Zuweisung von Rollen und Verantwortlichkeiten für die Datenerfassung und das Berichtswesen, Verfahren für die Eskalation von Ereignissen entsprechend ihrem Schweregrad

- Anpassung von Melde- oder Eskalationsschwellenwerten an den allgemeinen Risikoappetit bzw. die Risikotoleranz des Unternehmens für operationelle Risiken. Für weitere Informationen zu Meldeschwellen beachten Sie bitte den nächsten Abschnitt

- Sicherstellung, dass die Klassifizierung der erfassten Risikoereignisse mit dem Unternehmensansatz zur Kategorisierung des operationellen Risikos übereinstimmt

- Berücksichtigung der Frage, wie sich die Risikokultur des Unternehmens auf die Erfassung oder Analyse der gemeldeten Ereignisse auswirken kann. Weitere Hinweise finden Sie im IOR-Leitfaden zur Risikokultur.

Abschnitt 4.2 - Felder zur Datenerfassung

Datenfeld	Erklärung
Betroffene Geschäftsfelder und deren Standort	Die Geschäftsbereiche, Funktionen und/ oder Abteilungen, in denen das Ereignis aufgetreten ist
Standort	Unternehmen mit mehreren Standorten sollten aufzeichnen, welche dieser Standorte betroffen sind
Betroffene Geschäftsaktivitäten	Die Aktivitäten, Prozesse und Vorgänge, die von dem Risikoereignis betroffen waren
Ereignistyp	Verwendung der OpRisk-Kategorisierungen des Unternehmens
Datum	Das Datum und der Zeitpunkt, zu der das Ereignis erkannt wurde und wann das Ereignis geschlossen wurde
Ereignisbeschreibung	Eine kurze Erläuterung des aufgetretenen Ereignisses
Ursachen	Die Umstände, die zur Entstehung des Ereignisses beigetragen haben. Dies kann verfeinert werden, sobald das Ereignis nach einer detaillierten Ursachenanalyse abgeschlossen ist
Einflüsse und Rückflüsse	Mindestens die direkten finanziellen Auswirkungen des Ereignisses und alle Rückflüsse (z.B. Entschädigungszahlungen, Zahlungen aus Versicherungsansprüchen). Kann auch die indirekten und nicht-finanziellen Auswirkungen des Ereignisses beinhalten (s.o.)
Maßnahmen	Dies kann kurz- und längerfristige Maßnahmen umfassen. Kurzfristige Maßnahmen sind solche, die dazu beitragen, die Auswirkungen des Ereignisses zu mildern (z.B. Kulanzzahlungen an Kunden). Langfristige Maßnahmen sind solche, die dazu dienen, ähnliche Ereignisse in Zukunft zu verhindern (z.B. Verbesserungen der Kontrolleffektivität)

Tabelle 2: Empfohlene Mindest-Datenfelder

Unternehmen können zusätzliche Felder hinzufügen, wie z.B. die Abgrenzung von zugrundeliegenden und unmittelbaren Ursachen. Sie können auch versuchen, Daten sowohl zu finanziellen als auch nicht-finanziellen Auswirkungen zu sammeln. Wenn sie dies tun, sollten sie die Kosten und den Nutzen abwägen. Obwohl zusätzliche Daten dazu beitragen werden, die Vollständigkeit der erfassten Daten zu verbessern, können die Kosten für die Erfassung erheblich sein. Wie im IOR-Praxisleitfaden zur Integration eines Rahmenwerks für das operationelle Risiko erörtert, kann ein kostenintensiver Ansatz für das Management operationeller Risiken den Widerstand von Geschäftsmanagern hervorrufen, insbesondere dann, wenn ihre Ressourcen von Aktivitäten abgezogen werden, die sie priorisieren.

Abschnitt 4.3 - Schwellenwerte für die Datenerfassung

Idealerweise sollten Daten zu allen operationellen Risikoereignissen erfasst werden, um eine umfassende Datengrundlage zu gewährleisten. In der Praxis kann ein solches Ziel zu kostspielig sein. Unternehmen könnten sich daher für einen Kompromiss entscheiden, indem sie nur Daten zu Ereignissen erfassen, deren finanzielle Auswirkungen einen bestimmten Schwellenwert überschreiten.

Schwellenwerte können in beliebiger Höhe festgelegt werden, z B. für Ereignisse, deren Auswirkung 5.000 oder 50.000 übersteigt. Der von einem Unternehmen gewählte Schwellenwert sollte seine Größe und den Risikoappetit für operationelle Risiken wiederspiegeln.

Große Unternehmen mit großem Risikoappetit für operationelle Risiken können einen hohen Schwellenwert wählen. Kleinere Unternehmen mit einem kleineren Risikoappetit wählen einen niedrigeren Schwellenwert.

Unternehmen, die zum ersten Mal Ereignisdaten für operationelle Risiken erfassen, können auch einen hohen Schwellenwert wählen, um die anfänglichen Erfassungskosten zu reduzieren. Mit der Zeit, wenn sich die Benutzer an den Prozess gewöhnen, kann der Schwellenwert gesenkt werden.

Abschnitt 4.4 - Datenintegrität

Alle gesammelten Daten sollten so zeitnah, genau und vollständig wie möglich sein. Veraltete, ungenaue oder unvollständige Daten können ein irreführendes Bild von der Anfälligkeit eines Unternehmens gegenüber operationellen Risiken und der Wirksamkeit seiner Kontrollen vermitteln.

- Aktualität: Die Daten sollten so schnell wie möglich gesammelt und gemeldet werden, d.h., kurz nach der Identifizierung eines Ereignisses. Um die Aktualität der Daten zu gewährleisten, ist es hilfreich, eine Frist zu setzen, ab der neue Daten spätestens erfasst werden müssen. Diese Frist sollte die Art, den Umfang und die Komplexität eines Unternehmens widerspiegeln, ebenso wie seinen Risikoappetit und seine Risikokultur. Einige Unternehmen geben eine Datenerfassung innerhalb von einem Arbeitstag vor, andere innerhalb von fünf Arbeitstagen oder mehr. In allen Fällen sollte sich die (operationelle) Risikofunktion mit denjenigen abstimmen, die die Daten liefern müssen, um sicherzustellen, dass die Zeitvorgaben realistisch sind, und um die Akzeptanz zu maximieren.

- Genauigkeit: Daten zu operationellen Risikoereignissen sind selten perfekt, vor allem in den frühen Phasen des Ereignisses, wenn die Schadenshöhe noch nicht mit Sicherheit bekannt ist. Es sollte jedoch versucht werden, sicherzustellen, dass die Daten so genau wie möglich sind und dass sie aktualisiert werden, wenn neue Informationen ans Licht kommen. Darüber hinaus sollten Validierungsprozesse eingerichtet werden, um die Genauigkeit zu überprüfen. Dies kann den Vergleich von Daten aus ähnlichen Ereignissen in verschiedenen Geschäftsbereichen, Abteilungen oder Funktionen und den Vergleich mit externen Ereignissen oder internen Prüfungen der Datenerfassungsprozesse beinhalten.

- Vollständigkeit: Alle erforderlichen Felder sollten für jedes Ereignis befüllt und Informationen zu allen in Frage kommenden Ereignissen gesammelt werden. Dies kann alle Schadensfälle oder Ereignisse umfassen, deren finanzielle Auswirkungen den vereinbarten Schwellenwert überschreiten. Es können auch Informationen über Beinaheschäden gesammelt werden, obwohl selten alle Beinaheschäden erfasst werden. Die Tatsache, dass Beinaheschäden keine finanziellen oder nicht-finanziellen Auswirkungen haben, macht ihr Erkennen schwieriger.

Abschnitt 5 – Berichte über operationelle

Es ist unwahrscheinlich, dass die (operationelle) Risikofunktion Daten direkt sammelt. Stattdessen wird sie sich darauf verlassen, dass die Mitarbeiter im gesamten Unternehmen Informationen über Ereignisse liefern, die in ihren Bereichen aufgetreten sind. Dies bedeutet, dass ein Prozess implementiert werden muss, der die Rollen und Verantwortlichkeiten für die Meldung von Ereignissen festlegt und Punkte wie erforderliche Informationen und deren Fälligkeit abdeckt.

Abschnitt 5.1 – Rollen und Verantwortlichkeiten

Wenn ein Unternehmen Risikoverantwortliche hat, ist es üblich, diese für die rechtzeitige, korrekte und vollständige Meldung von operationellen Risikoereignissen verantwortlich zu machen. Alternativ dazu können Unternehmen, die “Risk-Champions“ einsetzen, diese für die Meldung von Ereignissen einsetzen.

In jedem Fall muss mindestens eine Person in jeder Abteilung, Funktion oder an jedem Standort die Verantwortung dafür übernehmen, dass Ereignisse gemeldet werden.

Wo vorhanden, ist die (operationelle) Risikofunktion für die Überwachung des Meldeprozesses verantwortlich. Die Interne Revision kann in regelmäßigen Abständen überprüfen, ob der Meldeprozess wie vorgesehen funktioniert und ob Risikoereignisse nicht ungemeldet bleiben.

Abschnitt 5.2 - Eskalation

Es sollten Verfahren für die Eskalation von gemeldeten Risikoereignissen vereinbart werden. Idealerweise sollten diese vom Risikokomitee oder einem gleichwertigen Gremium freigegeben werden. Wenn möglich, sollten diese Verfahren mit dem operationellen Risikoappetit des Unternehmens und den vereinbarten Schwellenwerten für finanzielle Auswirkungen abgestimmt werden.

Ein Eskalationsprozess könnte z.B. wie folgt aussehen:

1. Verluste unter 5.000 werden nicht außerhalb des betreffenden Geschäftsbereichs gemeldet
2. Verluste von 5.000 oder mehr werden der (operationellen) Risikofunktion gemeldet
3. Verluste von 50.000 oder mehr werden der zuständigen Geschäftsleitung gemeldet (z.B. Bereichsleiter, Leiter des Geschäftsbereichs)
4. Verluste von 250.000 oder mehr werden an die Geschäftsleitung des Unternehmens gemeldet
5. Verluste von 500.000 oder mehr werden dem vom Aufsichtsrat beauftragten Risikoausschuss oder einem gleichwertigen Gremium gemeldet
6. Verluste von 1 Mio. oder mehr werden sofort an den Aufsichtsrat gemeldet.

Auch wenn ein Ereignis bei der ersten Meldung nicht den Anschein erweckt, dass es einen bestimmten Schwellenwert überschreitet, sollte dies überprüft werden, sobald neue Daten vorliegen.

Abschnitt 5.3 - Maßnahmen

Operationelle Risikoereignisse erfordern eine Form der Reaktion. Zu den üblichen Optionen gehören:

Akzeptanz	Akzeptanz des Ereignisses, weil es innerhalb des Risikoappetits oder der Risikotoleranz des Unternehmens für operationelle Risiken liegt.
Minderung	Reduktion der finanziellen oder nicht-finanziellen Auswirkungen des aktuellen Ereignisses (z.B. Öffentlichkeitsarbeit, Goodwill-Zahlungen, außergerichtliche Einigungen usw.).
Maßnahmen	Maßnahmen, die ergriffen werden, um die finanziellen oder nicht-finanziellen Auswirkungen zukünftiger Ereignisse zu reduzieren.
Transfer	Rückwirkende Versicherungsabschlüsse für das aktuelle Ereignis. Versicherungssumme für zukünftige Ereignisse erhöhen.
Finanzierung	Bildung von Rückstellungen, Inanspruchnahme von Kreditlinien oder Ausübung von Kapitalisierungsmöglichkeiten im Falle eines Großschadens.
Vorkehrung	Maßnahmen, um ähnliche Ereignisse in der Zukunft zu verhindern.

Tabelle 3: Mögliche Reaktionen

Es ist wichtig, zwischen Maßnahmen zu unterscheiden, die zur Bewältigung des aktuellen gemeldeten Ereignisses ergriffen werden, und solchen, die zur Bewältigung möglicher zukünftiger Ereignisse ergriffen werden. Maßnahmen, die zur Bewältigung des aktuellen Ereignisses ergriffen werden, haben in der Regel einen kurzen Zeitrahmen. Maßnahmen zur Bewältigung zukünftiger Ereignisse können einen längeren Zeitrahmen haben und werden möglicherweise erst vereinbart, wenn das aktuelle Ereignis abgeschlossen ist (d.h., wenn alle verfügbaren Informationen gesammelt wurden).

Abschnitt 6 – Die Nutzung der Daten zu operationellen Risikoereignissen

Daten zu operationellen Risikoereignissen können für drei Hauptzwecke verwendet werden:

1. als Input für Risikobewertungsaktivitäten und zur Validierung von Risikobewertungen.
2. um Unternehmen dabei zu helfen, aus vergangenen Ereignissen zu lernen (Einblicke) und um Governance-Aktivitäten zu unterstützen (Übersicht).
3. als statistische Daten für quantitative Risikomodelle.

Abschnitt 6.1 - Eingaben und Validierung

Wie in der Einleitung erwähnt, liefern Ereignisdaten zu operationellen Risiken Informationen über die aktuelle, tatsächliche Anfälligkeit eines Unternehmens gegenüber operationellen Risiken. Diese Informationen können wiederum dazu verwendet werden, das zukünftige Ausmaß der Gefährdung eines Unternehmens abzuschätzen und frühere Schätzungen zu validieren.

Abschnitt 6.2 - Verwendung von Verlustdaten zur Unterstützung von Risikobewertungen und Überwachung

Operationelle Schadensfalldaten können zur Unterstützung einer Reihe von Bewertungs- und Überwachungsaktivitäten verwendet werden:

- Risk and Cotrol Self Assessments (RCSA) - indem Wahrscheinlichkeits- und Auswirkungsschätzungen validiert werden, Informationen über die Wirksamkeit von Kontrollen bereitgestellt werden und Risiken identifiziert werden, die derzeit nicht bewertet werden. Weitere Hinweise finden Sie im IOR-Praxisleitfaden zu Risk Self Assessments
- Szenarioanalyse - bei der tatsächliche Ereignisdaten verwendet werden können, um die Schätzungen der Wahrscheinlichkeit und der Auswirkungen zu untermauern und um Informationen darüber zu erhalten, wie Kontrollen versagen könnten. Einzelne operationelle Risikoereignisse können “vergrößert” werden, um zu untersuchen, wie sich ein Ereignis größeren Ausmaßes auf das Unternehmen auswirken könnte. Ebenso könnten Elemente aus mehreren gemeldeten Ereignissen genommen werden, um ein schwerwiegenderes Szenario zu erstellen
- Wenn Informationen über Ursachen gesammelt werden, können diese verwendet werden, um potenzielle Kausalketten für Szenarien zu konstruieren. Externe Verlustdaten können besonders nützlich für die Szenarioerstellung sein, vor allem, wenn sie sich auf seltenere Ereignisse mit geringer Wahrscheinlichkeit und hohen Auswirkungen beziehen. Weitere Hinweise finden Sie im IOR-Praxisleitfaden zur Szenarioanalyse.
- Die Identifizierung und Verwendung von Risiko- und Kontrollindikatoren. Die Entwicklung der Schadenshöhe nach Risikokategorie ist für sich betrachtet ein wertvoller Indikator. In ähnlicher Weise könnten gemeldete Fälle von Kontrollversagen als Kontrollindikator verwendet werden. Es kann auch möglich sein, die Anzahl und den Wert der gemeldeten Verluste mit den Trends der Risiko- und Kontrollindikatoren zu vergleichen. Dies kann helfen, die Indikatoren mit der höchsten Vorhersagekraft zu identifizieren. Es können auch Indikatoren identifiziert werden, die keine wirksamen Vorhersage-Indikatoren sind und entfernt werden können. Weitere Hinweise finden Sie im IOR-Praxisleitfaden zu Risikoindikatoren.

Abschnitt 6.3 - Verwendung von Verlustdaten zur Unterstützung der Risikoappetit- und/oder -toleranzaktivitäten

Unternehmen können einen angemessenen Risikoappetit und/oder Toleranzschwellen für operationelle Risiken besser bestimmen und aufrechterhalten, wenn sie über tatsächliche Verlustdaten verfügen, auf deren Grundlage sie Entscheidungen treffen können.

Einer der Faktoren, der zur Festlegung von Toleranzschwellen für den operationellen Risikoappetit beiträgt, ist die Berücksichtigung der historischen Performance eines Unternehmens. Zum Beispiel, ob die Erfahrung auf systemische, häufige Schadensfälle in einer bestimmten Produktlinie, in einigen Geschäftsbereichen oder auf einen Großschaden hinweist.

Eine Auswertung der Schadensfalldaten der letzten 12 Monate (um eventuelle saisonale Schwankungen zu berücksichtigen) kann zur Festlegung von Toleranzschwellenwerten genutzt werden:

- Der Mittelwert der aufgezeichneten Daten könnte als Schwellenwert für den Übergang von grün/ akzeptabel zu gelb/ tolerabel angenommen werden, auf der Grundlage, dass er eine Abweichung von “normalen” Werten anzeigt und eine Untersuchung wert ist
- Der schlechteste aufgezeichnete Wert könnte den Schwellenwert für den Übergang von gelb zu rot / inakzeptabel darstellen, sofern eine Verschlechterung über diesen Wert hinaus in der Zukunft nicht bewusst als Teil des Risikoappetits in Kauf genommen wird

Darüber hinaus können interne Schadensfalldaten zur Unterstützung der folgenden Aktivitäten genutzt werden:

- Echte Ereignisdaten können verwendet werden, um die tatsächliche Verlusterfahrung im Vergleich zu den vom Unternehmen gewünschten Toleranzwerten für Verluste zu überwachen. Wenn die Auswirkungen eines Schadensereignisses innerhalb der festgelegten Toleranzschwelle liegen, ist es weniger wahrscheinlich, dass eine Reaktion erforderlich ist (außer einer fortgesetzten Überwachung), d.h. diese Schäden können als gewöhnlicher Aufwand für die Geschäftstätigkeit akzeptiert werden.
- Liegt die Auswirkung eines Schadensfalles auf einem Niveau, das verkraftet werden kann, und sind die Kosten für eine Schadensbegrenzung unerschwinglich, dann wird das Risiko wahrscheinlich akzeptiert. Dies kann eine Erhöhung des Risikoappetits/ der Toleranz bedeuten
- Wenn ein Ereignis wesentliche Folgen hatte und die bestehenden Appetit-/Toleranzschwellen überschreitet, ist es wahrscheinlich, dass Maßnahmen zur Risikominderung erforderlich sind.

Wenn ein Unternehmen Toleranzschwellen für interne Schadensfälle festgelegt hat, kann es entsprechende Risikoindikatoren entwickeln, um den Wert oder das Volumen von eintretenden Verlusten zu messen und zu überwachen.

Abschnitt 6.4 - Verwendung externer Daten zum Benchmarking interner Verlustdaten

Die Analyse von internen Vorfällen kann durch Vergleiche mit externen Daten verbessert werden. Es ist möglich, ein Benchmarking durchzuführen, bei dem die externen Verlustdaten nach Unternehmensart und Risikokategorie sortiert werden können. Das Benchmarking kann Vergleiche von Ereignishäufigkeiten und durchschnittlicher Verlusthöhe beinhalten. Dies kann die Notwendigkeit aufzeigen, Kontrollen zu verbessern, wenn ein Unternehmen im Vergleich zu seinen Mitbewerbern anfälliger ist für häufigere oder höhere Verluste in bestimmten Risikokategorien. Wenn die Verluste jedoch unter dem Branchendurchschnitt und innerhalb von Risikoappetit/ Toleranzgrenze liegen, kann dies möglicherweise eine Reduzierung der Kontrollen rechtfertigen, um Kosten zu sparen und die Effizienz zu verbessern.

Ein Vergleich von Häufigkeit und Höhe interner Verluste mit externen Verlustdaten kann auch Schwachstellen in den aktuellen Meldeprozessen aufzeigen, z. B. wenn Geschäftsbereiche innerhalb des Unternehmens zu selten Verluste melden. Dies kann dann durch eine interne Überprüfung oder das Testen von Meldeprozessen behandelt werden und kann zusätzlichen Schulungsbedarf identifizieren. Das Versäumnis, interne Vorfälle zu erfassen, stellt ein erhebliches Risiko für Unternehmen dar, da versagende Kontrollen oder Prozesse, die nicht als Ergebnis der Berichterstattung über Vorfälle identifiziert werden, letztendlich zu einem für das Unternehmen bedrohliche Ereignis führen könnte. Alternativ kann eine Reihe von häufigen Verlusten mit geringem Wert zu Auswirkungen auf Kunden sowie zu Reputations-/ Regulierungsproblemen führen, wenn sie nicht adressiert werden.

Eine weitere Möglichkeit, externe Daten zum Benchmarking der Qualität interner Verlustmeldeverfahren zu nutzen, besteht darin, dass die externen Daten Informationen über das Datum des Ereignisses und das Datum der Entdeckung/ Meldung enthalten. Wenn bei den Vorfällen in der externen Datenbank im Durchschnitt ein kürzerer Zeitraum zwischen Entdeckung und Meldung liegt als im Unternehmen, muss dieses möglicherweise strengere Meldefristen und Eskalationsverfahren einführen oder Schulungen auffrischen, um sicherzustellen, dass die interne Verlustdatenmeldung auf dem neuesten Stand ist und Managementmaßnahmen zeitnah ergriffen werden können.

Abschnitt 6.5 - Verwendung von Verlustdaten zur Unterstützung der Identifizierung von neu auftretenden Risiken

Für einen vollständig effektiven Risikobewertungsprozess muss ein Unternehmen das gesamte Spektrum der Risiken berücksichtigen, denen es ausgesetzt sein kann. Nur wenn es alle Risiken identifiziert und die wichtigsten auswählt, kann das Unternehmen sicherstellen, dass es durch ein vollständiges und effektives Kontrollsystem geschützt ist.

Die Verwendung von Verlustdaten, insbesondere von externen Verlustdaten, kann dem Unternehmen helfen, die Art der Risiken, denen es ausgesetzt ist, zu verstehen. Ein wichtiger Vorteil von externen Verlustdaten ist, dass sie Risiken aufdecken können, denen ein Unternehmen ausgesetzt ist, die sich aber bisher nicht auf das Unternehmen ausgewirkt haben. Auf diese Weise ermöglichen externe Verlustdaten ein Verständnis für neu auftretende Risiken (einschließlich Trends bei Volumen und Art/ Schwere der Auswirkungen).

Außerdem kann ein Unternehmen durch die Verwendung externer Daten, die Informationen über Ursachen liefern, besser über die Art des erforderlichen Kontrollrahmens zur Abschwächung bestimmter Risikotypen informiert werden, auch wenn es möglicherweise noch keine Verluste für dieses Risiko erlitten hat. Das aus der externen Verlustdatenbank gewonnene Wissen über Kontrollversäumnisse, die zu Ereignissen bei anderen Unternehmen geführt haben, kann dem Management helfen, kosteneffektive Kontrollmaßnahmen zu bestimmen, wenn im Rahmen des des Risk Control Self Assessement (RCSA)Prozesses Verbesserungen des Kontrollrahmens identifiziert werden.

Ähnlich verhält es sich, wenn die externe Datenbank Aufschluss über die Auswirkungen von Ereignissen liefert. Dies kann dem Unternehmen helfen, festzustellen, wo Investitionen in Kontrollen vorteilhaft sein könnten.

Abschnitt 6.6 – Einblick und Übersicht

Daten über operationelle Verluste können dazu beitragen, das Bewusstsein und das Verständnis eines Unternehmens für operationelle Risiken zu verbessern, einschließlich der Folgen eines ineffektiven operationellen Risikomanagements. Darüber hinaus sind sie eine wertvolle Datenquelle, die zur Verbesserung der Aufsichts- und Kontrolltätigkeiten, einschließlich der Arbeit der (operationellen) Risikofunktion, der Internen Revision, Compliance und des Leitungsorgans, genutzt werden kann.

Abschnitt 6.7 – Unterstützung der Risiko-Governance

Als Teil der Governance des Managements operationeller Risiken, sei es durch Komitees oder eine Risikofunktion der zweiten Verteidigungslinie, können interne Schadensfalldaten die Grundlage für die Übersicht über das gesamte Rahmenwerk bilden, und zwar durch:

- Bereitstellung aktueller Informationen über das tatsächliche Risikoprofil des Unternehmens für die Geschäftsleitung und die Gremien
- Verifizierung/Validierung der Ergebnisse von Informationen, die von anderen Teilen des Rahmenwerks generiert werden, wie z.B. RCSAs
- Bewertung des Ausmaßes, in dem die Ergebnisse von Schadensfällen als Input für die Identifizierung und Bewertung von Risiken in anderen Teilen des Rahmenwerks verwendet werden
- Überprüfung der Effektivität des Kontrollrahmens - sowohl aus der Perspektive eines Kontrollversagens, das zu einem Schadensfall beiträgt, als auch aus der Perspektive eines Beinaheschadens, der auf einen gewissen Kontrollerfolg schließen lässt.

Wo interne Verlustdaten gesammelt werden, wird dringend empfohlen, sie in die Risikoberichterstattung einzubeziehen, insbesondere in Berichte, die dem Risikoausschuss oder einem gleichwertigen Gremium sowie dem Prüfungsausschuss vorgelegt werden.

Abschnitt 6.8 - Training und Awareness

Interne und externe Schadensfalldaten können, wenn sie gesammelt und interpretiert werden, dazu verwendet werden, das Bewusstsein der Mitarbeiter für die Art und die Auswirkungen von Schäden zu schärfen, indem reale Informationen genutzt werden, um die Folgen einer unzureichenden Kontrolle des operationellen Risikos aufzuzeigen. Dies ist eine aussagekräftige Botschaft, insbesondere, wenn sie mit Erfahrungsberichten über größere Schadensereignisse verbunden wird. Es können Details darüber gegeben werden, wie und wo das Schadensereignis seinen Anfang nahm, wie die Dinge schiefliefen, welche Prozesse und Kontrollen möglicherweise versagt haben, die verschiedenen Auswirkungen, die tatsächlichen Kosten und die daraufhin ergriffenen Maßnahmen, um eine Wiederholung zu verhindern oder abzuschwächen. Es besteht auch die Möglichkeit, alle Maßnahmen zu überprüfen, die als Reaktion auf den Schadensfall zur Stärkung der Kontrollumgebung ergriffen wurden.

Darüber hinaus kann ein Unternehmen seine internen und externen Schadensfalldaten nutzen, um:

- Aufzuzeigen, wie sich verschiedene kleinere Schadensereignisse zu einer großflächigen oder komplexen Auswirkung summieren können
- Die Botschaft zu verstärken, dass ein bestimmter Ereignistyp in einem Teil des Unternehmens (oder im Fall von externen Daten in einem anderen Unternehmen) auch anderswo auftreten könnte.

Solche Einblicke können den Mitarbeitern helfen, zukünftige Warnzeichen für potenzielle größere Verluste zu verstehen und darauf zu reagieren sowie sicherzustellen, dass Maßnahmen ergriffen werden, die solche Verluste verhindern bzw. eindämmen können.

Abschnitt 6.9 – Thematische Überprüfungen

Durch die Überwachung externer Ereignisse können neue oder neu aufkommende Risikoarten oder (nach Art oder Umfang) ungewöhnliche Ereignisse (z.B. die isländische Vulkanaschewolke oder COVID-19) thematische Überprüfungen innerhalb des Unternehmens auslösen, oft nach dem Motto “Könnte das hier passieren?” oder “Wenn das hier passieren würde, wie robust wären unsere Kontrollen, um die Auswirkungen zu mindern?”

Durch die Berichterstattung über die externen Ereignisse und die Durchführung spezifischer Maßnahmen wird das Bewusstsein des Managements und anderer Mitarbeiter für die Möglichkeit eines wesentlichen Ereignisses geschärft und es können klare Abhilfemaßnahmen zur Verbesserung des Kontrollrahmens beschrieben und überwacht werden.

Abschnitt 6.10 - Risikomodellierung

Sowohl externe als auch interne Verlustdaten können zur Unterstützung der Risikomodellierung verwendet werden, insbesondere in Bezug auf die Schätzung von Wahrscheinlichkeit und Verlusthöhe. Wie immer gilt: je größer die Menge und Qualität der verfügbaren Daten, desto robuster ist die resultierende statistische Analyse. Insbesondere sollte immer bedacht werden, dass die einem Unternehmen zur Verfügung stehenden Verlustdaten, wie zeitnah, genau und vollständig sie auch sein mögen, nur eine Stichprobe der gesamten Verteilung potenzieller Ereignisse darstellen werden. Außerdem sind die verfügbaren Daten per Definition historisch und es gibt keine Garantien dafür, dass sich vergangene Trends zwangsläufig fortsetzen werden.

Wenn Verlustdaten für Risikomodelle verwendet werden, wird empfohlen, dass regelmäßige Vergleiche der tatsächlichen Verluste mit den vorhergesagten durchgeführt werden. Dadurch kann das Modell auf Basis laufender Erfahrungen verfeinert werden.

Abschnitt 7 - Bewältigung praktischer Herausforderungen

Die Implementierung eines Prozesses zur Erfassung von operationellen Verlusten kann Unternehmen vor eine Reihe von praktischen Herausforderungen stellen. Diese Herausforderungen beziehen sich oft auf die mit der Datenerfassung verbundenen Kosten im Vergleich zum Nutzen der erfassten Daten.

Abschnitt 7.1 - Risikokultur

Bei der Implementierung eines Prozesses zur internen Verlustdatensammlung ist es wichtig, eine “Schuldzuweisungskultur” zu vermeiden, die eine offene und ehrliche Berichterstattung erschwert.

Dies ist von besonderer Bedeutung, wenn interne Schadensfälle als Grundlage für die Anpassung individueller Leistungs-/Bonusregelungen verwendet werden und Gegenstand von Prüfungen durch Aufsichtsbehörden sein können. Einige Unternehmen haben sich dieser Herausforderung gestellt, indem sie die variablen Zahlungen an die Einhaltung von Risikomanagementverfahren geknüpft haben, z.B. an die Einreichung vollständiger, genauer und zeitnaher Berichte über Schadensfälle. Sie verhängen also eine Strafe (z.B. eine Kürzung der erwarteten Bonuszahlung) als Reaktion auf ein unangemessenes Verhalten der verantwortlichen Person.

In größeren Unternehmen ist es gängige Praxis, Ranglisten über die Leistung der Geschäftseinheit und/oder des Standorts in Bezug auf Schadensfälle zu veröffentlichen, dies kann jedoch die Vergleichsgruppen unter Druck setzen, die Berichterstattung zu reduzieren oder sogar zu vermeiden. Umgekehrt können solche Informationen zur Förderung der kontinuierlichen Verbesserung genutzt werden, d.h., die Details des Ereignisses bieten die Möglichkeit, eine potenziell schädlichere Wiederholung zu vermeiden, indem Schwachstellen in Verfahren und Kontrollen behoben werden.

Eine Kommunikationsstrategie ist der Schlüssel zur Förderung einer wirksamen Kultur der Berichterstattung über Schadensereignisse. Dabei werden die verschiedenen Zielgruppen - von leitenden Angestellten bis hin zu Nachwuchskräften - sowie die entsprechenden Botschaften, der Detaillierungsgrad und die Art der Übermittlung festgelegt. In allen Fällen besteht das Ziel darin, ein Bewusstsein und dann ein Verständnis zu schaffen, um ein Engagement für angemessene Maßnahmen zu erreichen. Dies kann erfolgreicher sein, wenn der Schwerpunkt auf die Vorteile und den Nutzen einer offenen und ehrlichen Berichterstattung gelegt wird.

Weitere Informationen finden Sie im IOR-Praxisleitfaden zur Risikokultur.

Abschnitt 7.2 – Kategorisierung von Ereignissen

Es gibt zwei potenzielle Herausforderungen bei der Kategorisierung. Erstens kann es schwierig sein, zwischen einem Schaden und einem Beinaheschaden zu unterscheiden, insbesondere wenn die finanziellen Auswirkungen begrenzt sind (obwohl die nicht-finanziellen Auswirkungen viel höher sein können). Zweitens sind Schadensfälle nicht immer leicht in diskrete Risikoereigniskategorien zu trennen.

Bei der Unterscheidung zwischen Schäden und Beinaheschäden ist es wichtig, eine klare und konsistente Definition zu haben. Im Allgemeinen kann ein Beinaheschaden als ein Ereignis definiert werden, das keinen finanziellen oder nicht-finanziellen Verlust zur Folge hat, entweder durch Glück oder durch die effektive Anwendung bestimmter Kontrollen. Im Gegensatz dazu hat ein Schadenfall eine finanzielle und/oder nicht-finanzielle Auswirkung.

Manchmal kommen Ereignisse ans Licht, die eine potenzielle finanzielle oder nicht-finanzielle Auswirkung haben, die aber zum Zeitpunkt der Entdeckung möglicherweise unklar ist. Solche Ereignisse sollten zunächst als Schadenfälle klassifiziert werden und können als Beinaheschäden reklassifiziert werden, wenn die Auswirkungen nicht eintreten. Ebenso können finanzielle oder nicht-finanzielle Auswirkungen nach oben oder unten korrigiert werden, wenn neue Informationen bekannt werden.

Abschnitt 7.3 – Verbindung von verschiedenen, zusammenhängenden Ereignissen

Wenn viele Ereignisse zusammenhängen (z.B. durch dieselbe zugrundeliegende Ursache oder einen Kontrollfehler), aber über einen längeren Zeitraum auftreten, ist es hilfreich, diese zusammenzufassen und für die Maßnahmenplanung und Analyse als ein einziges Ereignis zu behandeln.

Durch die Verbindung von Ereignissen auf diese Weise ist es möglich, besser zu verstehen, wie operationelle Risikoereignisse zusammenhängen. Insbesondere dann, wenn das Auftreten eines Ereignisses ein anderes verursacht und so weiter. Durch Verstehen und Berücksichtigung dieser Zusammenhänge kann ein Unternehmen die Effektivität seines OpRisk-Managements erheblich verbessern, z.B. durch die Fokussierung von Ressourcen auf die wichtigsten zugrundeliegenden Ursachen oder Kontrollprobleme.

Weitere Informationen finden Sie im IOR-Praxisleitfaden zur Riskokultur.

Abschnitt 7.4 – Validierung von Verlustschätzungen

Es wäre sehr schwierig - wenn nicht sogar unmöglich - und würde einen erheblichen Zeit- und Arbeitsaufwand erfordern, alle direkten finanziellen Verluste zu validieren, z.B. durch den Vergleich von Verlustschätzungen mit den verfügbaren Buchhaltungsunterlagen.

Dies liegt zum Teil daran, dass die finanziellen Auswirkungen von Ereignissen in der Regel auf einer Vielzahl von Ausgabenkonten und möglicherweise auch auf Ertragskonten (z.B. in Bezug auf die Rückerstattung einer verdienten Provision) verbucht werden. Eine weitere Herausforderung besteht darin, dass sich die direkten und indirekten finanziellen Auswirkungen über einen längeren Zeitraum akkumulieren.

In der Praxis verfolgen die meisten Unternehmen, die sich um eine Validierung bemühen, einen “80/20”-Ansatz, d.h. sie konzentrieren sich auf das, was in den Konten leicht identifizierbar ist, und versuchen, nur die größten Einzelereignisse vollständig zu validieren.

Abschnitt 7.5 – Wann ein Ereignis geschlossen werden kann

Der naheliegende Punkt, an dem die Verfolgung und Aktualisierung eines Schadensfall-Datensatzes beendet werden sollte, ist zum Zeitpunkt der Umsetzung der vereinbarten Maßnahmen.

Wenn jedoch eine langwierige Wiederherstellung involviert ist, werden einige Unternehmen die Beendigung aufschieben, bis diese abgeschlossen ist und der endgültige Nettoverlust bestimmt werden kann. Andere wählen einen pragmatischen Ansatz und setzen ein Zeitlimit für die Erwartung der Wiederherstellung - zum Beispiel das Ende der aktuellen Rechnungsperiode. Dadurch wird vermieden, dass offene Ereignisse auf einer fast unbestimmten Basis aufrechterhalten werden.

Abschnitt 8 - Fazit

Obwohl sie kostspielig und störend sind, bieten operationelle Schadensereignisse eine Gelegenheit zum Lernen. Oft sind sie keine einmaligen Ereignisse und treten nicht isoliert auf. Durch das Sammeln von Schadensfalldaten sind Unternehmen in der Lage, diese Möglichkeit voll auszuschöpfen und dabei ihr Rahmenwerk für das Management operationeller Risiken zu bereichern.

Perfektion bei der Verlustdatenerfassung ist selten erforderlich. Vorrangig geht es darum, mit der Analyse zu beginnen und aus vergangenen Ereignissen zu lernen, insbesondere dann, wenn sie verbesserungswürdige Faktoren aufzeigen (z.B. Kontrollen oder menschliche/kulturelle Verhaltensweisen). Ziel ist es, ein besseres Verständnis für Ursachen, Kontrollen und Auswirkungen aufzubauen und den Wert des Managements operationeller Risiken hervorzuheben.

www.theirm.org

irm

Developing risk professionals