Operationeller Risikoappetit und Toleranz

Praxisleitfaden
Operationelles Risiko

Gesponsort von:

DGOR
Deutsche Gesellschaft für
Operational Risk Management e.V.

IBM
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

Inhaltsverzeichnis

Einleitung

Der Risikoappetit ist ein Bereich, der unter den Praktikern des operationellen Risikos unterschiedliche Ansichten hervorruft. Je nach Branche, Größe und Risikoprofil eines Unternehmens sind die Rahmenwerke für den operationellen Risikoappetit unterschiedlich komplex und umfangreich. Unterschiede gibt es auch in der Terminologie, wobei einige Praktiker den Begriff Toleranz dem Appetit vorziehen, wenn sie sich auf operationelle Risiken beziehen. Aus diesen Gründen wird im folgenden Papier keine Einheitslösung empfohlen. Vielmehr wird eine Reihe von bewährten Praktiken skizziert, aus denen eine Sammlung geeigneter, relevanter und angemessener Ideen abgeleitet werden kann.

Im Grunde geht es beim Risikoappetit um die Entscheidungsfindung - unabhängig vom Risiko, auf das man sich konzentriert. Jede Handlung oder Entscheidung innerhalb eines Unternehmens beinhaltet ein Risikoelement. Das Unternehmen muss daher in der Lage sein, zwischen Risiken zu unterscheiden, die wahrscheinlich zu wertschöpfenden Ergebnissen (Gewinn, Reputation, verbesserte Dienstleistungen usw.) führen, und solchen, die Werte zerstören können. Durch die Festlegung eines angemessenen Risikoappetits und die Implementierung eines Rahmens, der sicherstellt, dass dieser Risikoappetit eingehalten wird, können Unternehmen sicherstellen, dass die Entscheidungsträger sie weder einem zu hohen noch einem zu niedrigen Risiko aussetzen.

Auch wenn der Schwerpunkt dieses Papiers auf dem operationellen Risiko liegt, geht das IOR davon aus, dass der operationelle Risikoappetit eines Unternehmens Teil einer breiteren, unternehmensweiten Risikobereitschaft ist. Operationelle Risiken sind für alle Unternehmen wichtig, und der Vorstand und die Geschäftsleitung müssen sich mit ihrem Management befassen. Effektive Governance und Compliance erfordern das Management von Risiken, die typischerweise operationell sind (z.B. Betrug, Gesundheit und Sicherheit sowie verhaltensbezogene Risiken). Auch strategische Entscheidungen (z.B. die Entwicklung neuer Produkte) erfordern oft das Eingehen operationeller Risiken. Es ist wichtig, dass der Vorstand und die Geschäftsleitung diese Risiken kennen und davon überzeugt sind, dass die das Unternehmen sie eingehen kann.

Unternehmen, die ein Rahmenwerk zur Bestimmung und zum Management ihres operationellen Risikoappetits einführen, können mehrere Vorteile erzielen:

- Dem Vorstand eine angemessene Übersicht und Unternehmensführung ermöglichen, indem er die Art und Höhe der operationellen Risiken definiert, die er für akzeptabel (und inakzeptabel) hält, und so angemessene Grenzen für Geschäftsaktivitäten und Verhaltensweisen setzt
- die Einstellung der Unternehmensleitung zu operationellen Risiken zum Ausdruck bringen, die dann im gesamten Unternehmen kommuniziert werden kann, um eine risikobewusste Kultur zu fördern
- Schaffung eines Rahmens für die Entscheidungsfindung bei operationellen Risiken, um zu bestimmen, welche Risiken akzeptiert/ beibehalten werden können und welche Risiken verhindert oder gemindert werden sollten
- Verbesserung der Zuweisung von Risikomanagement-Ressourcen durch die Konzentration auf Themen mit höherer Priorität. Insbesondere operationelle Risikoexpositionen oder Kontrollschwächen, die außerhalb der Risikobereitschaft oder -toleranz liegen
- Sicherstellen, dass die Kosten des operationellen Risikomanagements den Nutzen nicht übersteigen
- Ausrichtung strategischer Ziele und operativer Aktivitäten durch Optimierung des Gleichgewichts zwischen Geschäftsentwicklung/ Wachstum/ Rendite und den operationellen Risiken, die mit der Verfolgung dieser Ziele verbunden sind

Schlüsselbegriffe und Definitionen

Es gibt keine allgemeingültigen Definitionen von Risikoappetit oder Risikotoleranz. Die Einigung auf eine allgemeingültige Definition ist im Zusammenhang mit operationellen Risiken besonders schwierig, da die meisten operationellen Risiken als “Downside”-Risiken bezeichnet werden, die nur zu einem Verlust für ein Unternehmen führen können.

Risikoappetit

Unabhängig von der akademischen Debatte über Definitionen sollten Praktiker des operationellen Risikos sicherstellen, dass ihr Unternehmen über eine klare Definition des Risikoappetits für operationelle Risiken verfügt, die von der Geschäftsführung und dem Vorstand akzeptiert und verstanden wird. Ein nützlicher Ausgangspunkt ist die IRM-Definition des Risikoappetits in einem unternehmensweiten Kontext:

‚Die Höhe und Art des Risikos, das ein Unternehmen bereit ist einzugehen, um seine strategischen Ziele zu erreichen”.

Aus der Perspektive des operationellen Risikos könnten Unternehmen “ist bereit, Risiken einzugehen” durch “ist bereit, Risiken zu akzeptieren” oder Ähnliches ersetzen. Operationelle Risiken sind in unternehmerischen Aktivitäten inhärent vorhanden, werden aber selten gesucht, da sie keine wesentlichen Vorteile in Bezug auf Rendite/ Ertragsgenerierung haben.

Bei der Festlegung eines angemessenen Gleichgewichts zwischen der Inkaufnahme potenzieller Verluste auf der einen Seite und den Kosten für Vorbeugung und Minderung auf der anderen Seite (einschließlich der damit verbundenen betrieblichen Ineffizienzen, die die Einführung einer neuen Kontrolle mit sich bringen könnte) sind jedoch Kosten-Nutzen-Entscheidungen erforderlich. Eine Reduzierung des operationellen Risikos auf Null ist in der Regel weder möglich noch praktikabel. Die einzige Möglichkeit, ein Nullrisiko zu erreichen, besteht darin, die Aktivitäten einzustellen, und das kann ein Unternehmen daran hindern, seine strategischen Ziele zu erreichen.

Das IOR ist der Ansicht, dass Finanzdienstleistungsunternehmen und solche, die in sicherheits- oder umweltkritischen Sektoren tätig sind (Nuklearindustrie, chemische Industrie usw.), eine akzeptanzorientierte Definition des Risikoappetits für operationelle Risiken annehmen sollten. Dies liegt darin begründet, dass ihre operationellen Risiken das Potenzial haben, den Stakeholdern ernsthaften finanziellen und physischen Schaden zuzufügen. In nicht-finanziellen Unternehmen und solchen, die kein signifikantes Sicherheits- oder Umweltrisiko darstellen, insbesondere in unternehmerisch geprägten Sektoren wie dem Technologiesektor, ist eine Definition angemessen, die eine Risikobereitschaft wiederspiegelt. Grund ist, dass das Eingehen von Risiken, einschließlich eines gewissen Maßes an operationellem Risiko, ein notwendiger Bestandteil der Nutzung von Geschäftschancen sein kann, insbesondere im Hinblick auf die Entwicklung neuer Produkte, Lieferketten oder Herstellungsprozesse.

Risikotoleranz

Wie oben erläutert, spiegelt der Risikoappetit eines Unternehmens für operationelle Risiken das Gleichgewicht wieder, das es zwischen den Kosten für die Kontrolle der operationellen Risiken und den Kosten von operationellen Risikoereignissen zu wahren bereit ist. Dabei handelt es sich um eine strategische Entscheidung auf hoher Ebene, die sowohl die für das Management operationeller Risiken eingesetzten Ressourcen als auch die Höhe des Risikos beeinflusst, das mit den Unternehmensaktivitäten verbunden ist.

Im Gegensatz dazu wird der Begriff Risikotoleranz typischerweise als spezifischer Maßstab für die Akzeptanz einer bestimmten operationellen Risikoexposition (z.B. interner oder externer Betrug) oder einer Kennzahl, wie z.B. einem Risiko- oder Kontrolleffektivitätsindikator, verwendet. In diesem Zusammenhang kann ein Unternehmen entscheiden, dass es bereit ist, eine bestimmte Anzahl von operationellen Fehlern oder Kontrollschwächen zu tolerieren, weil deren Beseitigung nicht kosteneffektiv wäre.

Die Toleranz kann mit einem Ampelsystem ausgedrückt werden:

Status	Bedeutung	Maßnahmen zur Einbettung in die Risikokultur
Grün	Akzeptabel	Keine sofortigen Maßnahmen erforderlich, außer Routineüberwachung
Gelb	Tolerabel	Untersuchen (um die zugrundeliegenden Ursachen zu verifizieren und zu verstehen) und Möglichkeiten zur Abschwächung/Vermeidung innerhalb einer bestimmten Zeitspanne erwägen
Rot	Inakzeptabel	Sofortige Maßnahme zur Mitigierung oder Vermeidung erforderlich

Die Schwellenwerte, die bestimmen, wann ein Risiko oder eine Kennzahl von grün auf gelb und dann von gelb auf rot wechselt, spiegeln den Toleranzgrad eines Unternehmens wieder. Je breiter diese Schwellenwerte sind, desto größer ist der Grad der Toleranz.

Gelegentlich kann ein Unternehmen entscheiden, dass es nicht bereit ist, etwas zu tolerieren. Normalerweise ist dies bei bestimmten operationellen Risikoereignissen, einschließlich höchst unerwünschter Ereignisse wie Betrug oder Arbeitsunfälle, nicht möglich. Es ist jedoch möglich, die Auswirkungen, die mit diesen Ereignissen verbunden sein können, wie z.B. das Potenzial für behördliche Eingriffe und Durchsetzungsmaßnahmen zu vermeiden. Ein Unternehmen kann z.B. die Anzahl der Arbeitsunfälle nie auf Null reduzieren, aber es kann sicherstellen, dass es nicht gegen Gesundheits- und Sicherheitsvorschriften verstößt. Daher ist es möglich, eine Nulltoleranz für Compliance-Verstöße festzulegen, nicht jedoch für Unfälle.

Wo sowohl Toleranz als auch Appetit verwendet werden, können Unternehmen entweder:

- Toleranzgrenzen und Schwellenwerte unterhalb des vereinbarten Appetits für das operationelle Risiko festlegen. Für die Ampel bedeutet dies, den Appetit auf die rote Stufe und die Toleranz auf die gelbe Stufe zu setzen.
- Toleranzgrenzen oberhalb der vereinbarten Risikobereitschaft für das operationelle Risiko festlegen. Somit würde der Appetit den gelben Schwellenwert wiederspiegeln und die Toleranzgrenze den Schwellenwert für rot

Der erste Ansatz eignet sich am besten in Umgebungen mit hoher Kontrolldichte, wie z.B. Finanzdienstleistungen. Der wesentliche Vorteil besteht darin, dass ein Risiko (oder ein damit verbundener Risiko- oder Kontrolleffektivitätsindikator), das die gelbe Toleranzgrenze überschreitet, als frühzeitige Warnung vor einem potenziellen Verstoß gegen den Risikoappetit dient.

Der zweite Ansatz eignet sich am besten in einem eher unternehmerischen Umfeld, in dem das Eingehen von Risiken, einschließlich des Eingehens bestimmter operationeller Risiken (z.B. Risiken bei der Entwicklung neuer Produkte), ein notwendiger Bestandteil der strategischen Unternehmensziele ist. Der Vorteil eines solchen Ansatzes in diesem Umfeld ist, dass der Risikoappetit für operationelle Risiken überschritten werden kann, wenn sich daraus ein potenzieller geschäftlicher Nutzen ergibt. Es wäre jedoch ratsam, eine solche Entscheidung

auf Vorstandsebene zu genehmigen, insbesondere, wenn die Corporate-Governance-Regeln vorsehen, dass der Vorstand den Risikoappetit seines Unternehmens überwacht.

Unabhängig davon, welcher Ansatz gewählt wird, bleiben zwei Grundprinzipien bestehen - ein Expositionsniveau von operationellen Risiken, das unter außergewöhnlichen Umständen überschritten werden kann, und ein Niveau, das unter keinen Umständen überschritten werden darf. In Bezug auf Letzteres dürfen alle Unternehmen nicht wissentlich operationelle Risiken eingehen, die mit hoher Wahrscheinlichkeit Folgendes verursachen:

1. Tod oder Verletzungen
2. einen Verstoß gegen geltende Gesetze und Vorschriften
3. finanzielle Notlage und Konkurs.

Die Bestimmung von operationellem Risikoappetit und Toleranz

Die Bestimmung eines angemessenen Niveaus des Risikoappetits und der Risikotoleranz für das operationelle Risiko beinhaltet viele Überlegungen, einschließlich der “Maßstäbe”, die verwendet werden sollten, und der angemessenen Höhe dieser Maßstäbe. Wie so oft gibt es nicht den einen optimalen Ansatz, obwohl es eine solide Praxis gibt. Die wichtigsten Schritte in diesem Prozess sind:

- Festlegung, wer für die Bestimmung des operationellen Risikoappetits und der Risikotoleranz verantwortlich ist
- Festlegung, wie Risikoappetit und -toleranz ausgedrückt werden sollen
- Entscheidung über die angemessene Höhe dieser Ausdrucksformen

Rollen und Verantwortlichkeiten bei der Bestimmung von OpRisk Appetit und Toleranz

Der Vorstand

In vielen Unternehmen ist es gängige Praxis, dass der Vorstand die von der Geschäftsleitung verfassten Erklärungen zum Risikoappetit berücksichtigt. Dieser Ansatz spiegelt oft die komplexe Natur vieler Finanzunternehmen wider. Leider kann diese Praxis zum Anchoring (Beeinflussung einer Entscheidung oder eines Urteils durch eine zugegangene oder selbst generierte Information) führen und ist angreifbar für Anfechtungen durch Aufsichtsbehörden und bei Überprüfungen der Effektivität des Vorstands, wenn argumentiert werden könnte, dass Vorstände keine ausreichend große Auswahl an Empfehlungen haben und sich zu sehr von der Arbeit des Senior Managements leiten lassen.

Das Institut ist der Ansicht, dass Vorstände nach Möglichkeit stärker in den Prozess der Festlegung des Risikoappetits einbezogen werden sollten und eine aktivere Rolle bei der Überlegung und Festlegung des Risikoappetits spielen sollten, auch wenn sie von den entsprechenden Experten geleitet werden.

Eine Alternative zur Verbesserung des Vorstands-Engagements besteht darin, dass sich die Experten für operationelles Risiko darauf beschränken, den Prozess zur Festlegung des Risikoappetits zu gestalten. Dazu könnte die Bereitstellung einer Vorlage gehören, die der Vorstand verwenden kann (siehe Anhang A), oder die Moderation von Diskussionen im Vorstand. Es würde jedoch nicht beinhalten, spezifische Empfehlungen über die angemessene Höhe des Risikoappetits für operationelle Risiken zu geben.

Ein weiterer Vorteil dieses Ansatzes besteht darin, dass die Mitglieder des Vorstands (unabhängig davon, ob es sich um geschäftsführende oder nicht geschäftsführende Mitglieder handelt) über eine möglichst umfassende strategische Perspektive verfügen und ein klares Verständnis der Risikopräferenzen der Stakeholder haben sollten. Dadurch können sie sicherstellen, dass der operationelle Risikoappetit des Unternehmens mit den strategischen Zielen übereinstimmt und gleichzeitig die Bedürfnisse der Stakeholder erfüllt.

Eine Möglichkeit, wie ein Vorstand den Risikoappetit eines Unternehmens für operationelle Risiken bestimmen kann, besteht darin, ihm eine Vorlage zu präsentieren, wie sie in Anhang A zu finden ist. Zunächst sollten die einzelnen Vorstandsmitglieder gebeten werden, darüber abzustimmen, welches Maß an Risikoappetit sie für jedes der Elemente in der Vorlage für angemessen halten. Zweitens sollte der Vorstand diese Abstimmung überprüfen und diskutieren, um einen Konsens zu erzielen. Drittens sollte der Vorstand ein zweites Mal abstimmen und die Ergebnisse zur Festlegung des ursprünglichen Risikoappetits für das operationelle Risiko

verwenden. Der Prozess könnte bei Bedarf wiederholt werden, falls kein Konsens erzielt werden kann. Es wird empfohlen, diesen Ansatz außerhalb einer geplanten Vorstandssitzung durchzuführen, z.B. während einer Off-Site, um Zeit für Diskussionen zu haben. Sobald der Risikoappetit für das operationelle Risiko vereinbart wurde, sollte er innerhalb kürzerer Zeit überprüft und bei Bedarf aktualisiert werden (mindestens jährlich).

Das Business Management

Manager in einem Unternehmen sind in das tägliche Management einer Vielzahl von operationellen Risiken involviert. Einige können als Risiko- oder Kontrollverantwortliche benannt werden, um ihrer Verantwortung für ein effektives Risikomanagement gerecht zu werden.

Bereichsleiter sind normalerweise nicht an der Festlegung des operationellen Risikoappetits eines Unternehmens beteiligt, da dies Teil der Governance-Verantwortung des Vorstands ist. Sie können jedoch an der Festlegung von Ampel-Toleranzschwellen für bestimmte operationelle Risiken oder Risiko- und Kontrollkennzahlen beteiligt sein. Wenn sie an der Festlegung von Risikotoleranzen beteiligt sind, sollten diese nicht im Widerspruch zum übergreifenden Risikoappetit für operationelle Risiken stehen.

Die OpRisk Funktion oder ihr Äquivalent

Die Funktion des operationellen Risikos hat eine doppelte Aufgabe:

- Unterstützung der Arbeit des Vorstands (siehe oben)
- Beaufsichtigung der Arbeit der Bereichsleiter bei der Festlegung der Ampel-Toleranzschwellen

Bei der Überwachung der Arbeit der Bereichsleiter sollte die Funktion für operationelle Risiken die Aktivitäten und Ziele bestimmter Geschäftseinheiten, Abteilungen oder Funktionen mit dem vom Vorstand festgelegten Risikoappetit für operationelle Risiken abgleichen. Die Bereichsleiter sollten keine Ampel-Toleranzgrenzen festlegen, die Entscheidungen ermöglichen, die mit dem Risikoappetit des Vorstands für operationelle Risiken unvereinbar sind (z.B. die Festlegung von Schwellenwerten, die eine übermäßige oder unzureichende Risikobereitschaft und -kontrolle fördern). Die Funktion für operationelles Risiko sollte Toleranzgrenzen in Frage stellen, wenn sie Bedenken hinsichtlich der Konsistenz hat. Gegebenenfalls kann das Risiko- oder OpRisk-Komitee zur Unterstützung dieser Überwachung herangezogen werden.

Die Interne Revision

Unternehmen, die über getrennte Funktionen für Risiko und Interne Revision verfügen, sollten die Interne Revision normalerweise nicht in die Bestimmung des Risikoappetits oder der Toleranzschwellen für operationelle Risiken einbeziehen. Sie können jedoch beschließen, die Interne Revision zu nutzen, um den Prozess zur Bestimmung des Risikoappetits für operationelle Risiken zu überprüfen und ggf. Empfehlungen für Verbesserungen abzugeben.

OpRisk Appetit und Toleranz ausdrücken: Qualitativ versus quantitativ

Der Risikoappetit und die spezifischen Toleranzen für das operationelle Risiko können auf unterschiedliche Weise ausgedrückt werden. Grob lassen sich diese in qualitative und quantitative Ansätze einteilen.

Qualitativ

Qualitative Ausdrücke beruhen auf schriftlichen Aussagen, die keine Quantifizierung beinhalten. Sie sind nützlich, wenn operationelle Risiken schwer zu quantifizieren sind und um die Beziehung zwischen dem operationellen Risiko und den strategischen/ geschäftlichen Managementzielen zu verstärken. Qualitative Aussagen können auch verwendet werden, um bestimmte

Verhaltensweisen oder Einstellungen zu betonen und so die Risikokultur eines Unternehmens zu steuern.

Insbesondere können qualitative Äußerungen zur Risikobereitschaft oder -toleranz verwendet werden, um mehreren wichtigen Botschaften Ausdruck zu verleihen, wie z.B.:

- Anerkennen, dass bestimmte operationelle Risiken, so unwillkommen sie auch sein mögen, nicht vermeidbar sind (z.B. Terrorismus, Naturkatastrophen, Pandemien), obwohl die Auswirkungen dieser Risiken durch ein angemessenes Business Continuity- und Krisenmanagement gemildert werden können
- Es ist sinnvoll, operationelle Risiken zu akzeptieren, bei denen die Kosten für die Abmilderung/ Vermeidung den erwarteten Verlust übersteigen, vorausgesetzt, es besteht kein Risiko eines Konkurses, einer Vollstreckung oder eines Schadens für die Stakeholder
- Risiken werden akzeptiert, wenn die geschätzten Verluste innerhalb der vorgeschriebenen Toleranzgrenzen liegen
- Verhaltensweisen, die als inakzeptabel gelten, wie z.B. wissentlicher Gesetzesbruch, Verstoß gegen behördliche Vorschriften oder Unternehmensrichtlinien, Schädigung der Umwelt, schlechter Kundenservice oder Gefährdung von Menschen durch körperliche Schäden
- Risiken, die als inakzeptabel erachtet werden, wie z.B. die Tätigkeit in bestimmten Ländern oder der Verkauf bestimmter Produkte
- Die Bedeutung der Aufrechterhaltung einer guten Reputation.

Quantitativ

Quantitative Ausdrücke beinhalten harte Daten, die in der Regel auf betriebswirtschaftlichen Informationen beruhen und eine beliebige Kombination von Leistungs-, Risiko- oder Kontrollindikatoren darstellen können.

Quantitative Ausdrücke sind in der Regel risiko- oder kontrollspezifisch und sind daher in erster Linie ein Hinweis auf die operationelle Risikotoleranz und nicht auf den gesamten Risikoappetit. Solche Maßnahmen können von gelben und roten Schwellenwerten begleitet werden, so dass klar ist, wann ein Verstoß stattgefunden hat oder unmittelbar bevorsteht. Das Konzept der Festlegung von Null-Toleranz-Schwellenwerten mag unpraktisch erscheinen, aber sie können einen kulturellen Zweck erfüllen, indem sie die Botschaft verstärken, dass es nicht angemessen ist, vermeidbare Verluste ohne Weiteres zu akzeptieren.

Leistungskennzahlen auf strategischer Ebene, die den Risikoappetit für das operationelle Risiko isoliert ausdrücken, sind selten. Eine mögliche Messgröße ist die Höhe des ökonomischen oder regulatorischen Kapitals, das dem operationellen Risiko zugeordnet ist. Unternehmen außerhalb des Finanzsektors neigen nicht dazu, Kapital für bestimmte Risikokategorien zu berechnen oder zuzuweisen, während dies bei Finanzdienstleistungen üblicher ist. Wenn dem operationellen Risiko Kapital zugewiesen wird, kann ein Unternehmen seinen OpRisk-Appetit in Form eines risikospezifischen Kapitalpuffers ausdrücken. Zum Beispiel kann ein Unternehmen ein Minimum von

£ 10 Mio. an Kapital für das operationelle Risiko zuweisen, plus einen Puffer von 10 % (zusätzlich £ 1 Mio.), um der Tatsache Rechnung zu tragen, dass unerwartete Kosten die Mindestzuweisung übersteigen können. Je größer der Puffer ist, desto höher ist der Risikoappetit des Unternehmens für das operationelle Risiko.

Risiko- und kontrollspezifische operationelle Risikotoleranzkennzahlen sind üblich, Beispiele hierfür sind:

- Delegierte Autoritätsgrenzen, jenseits derer untergeordnete Mitarbeiter zur Genehmigung eskalieren müssen
- Maße für die System- oder Prozesszuverlässigkeit, z.B. nicht mehr als xx % Wahrscheinlichkeit, dass ein geschäftskritisches System für mehr als einen Tag im Jahr nicht verfügbar ist
- Gemeldete Schadenssummen auf Basis der Budgetierung, der jährlichen Gesamtsumme nach Geschäftsbereich/ Verlustart und/ oder Sensitivität, d.h. ein negativer Trend von 5 % kann akzeptabel sein, 10 % tolerierbar, aber 15 % inakzeptabel. Beachten Sie, dass Schwellenwerte pro Ereignis, für bestimmte Risikokategorien über einen vereinbarten Zeitraum oder auf aggregierter Basis für alle operationellen Risiken festgelegt werden können. Ziel ist es, sowohl Ereignisse mit hohem Volumen/ geringem Wert als auch solche mit geringem Volumen/ hohem Wert abzudecken. Schwellenwerte können auch zur Unterstützung von Berichts- und Eskalationsprozessen verwendet werden, um den Grad der Aufmerksamkeit des Managements oder der Geschäftsleitung zu ermitteln
- Grenzen der Risiko-/ Kontrollbewertung zur Unterscheidung von akzeptablen/ tolerierbaren/ inakzeptablen Werten der Exposition gegenüber bestimmten Risikotypen
- Gelbe und rote Schwellenwerte für Risiko- und Kontrollindikatoren, ausgedrückt in Einheiten, die für den jeweiligen Indikator geeignet sind, d.h. numerische Anzahl, finanzieller Wert, Prozentsatz oder Abweichung.

Die Entscheidung über das angemessene Niveau von OpRisk Appetit und der dazugehörigen Toleranzen

Wie erläutert, ist der Vorstand verantwortlich für die Entscheidung über die angemessene Höhe des operationellen Risikoappetits, während die Geschäftsleitung die operationelle Risikotoleranz für bestimmte Risiken und Kontrollen festlegt, die mit dem Gesamtrisikoappetit vereinbar sind.

Bei der Entscheidung über die Höhe des operationellen Risikoappetits sollte der Vorstand drei Hauptfaktoren berücksichtigen:

1. die strategischen Unternehmensziele. Ein Unternehmen, das wachsen oder seinen Marktanteil halten will, kann beispielsweise entscheiden, ein höheres Maß an operationellen Risiken zu akzeptieren
2. die Risikopräferenzen der wichtigsten Stakeholder. Wenn die Stakeholder dem operationellen Risiko eher abgeneigt sind, ist eine geringere Risikobereitschaft angemessen und umgekehrt
3. die finanzielle Stärke des Unternehmens. Schwächere Unternehmen sollten normalerweise keinen hohen Appetit auf Risiken haben, da die Gefahr besteht, dass ihr Ausbruch zum Konkurs führt. Stärkere Unternehmen haben mehr Spielraum für das Eingehen von Risiken, einschließlich operationeller Risiken, da sie über die notwendigen Mittel verfügen sollten, um die mit den Risikoereitgnissen verbundenen Kosten zu finanzieren

Bei der Festlegung von Toleranzschwellen für bestimmte operationelle Risiken oder Kontrollen sollten Geschäftsbereichsleiter sicherstellen, dass diese mit dem operationellen Risikoappetit des Vorstands für übereinstimmen. Sobald inkonsistente Toleranzgrenzen festgelegt werden, insbesondere solche, die nicht mit dem vereinbarten Risikoappetit übereinstimmen, sollte dies dem Vorstand (oder dem Risikoausschuss, sofern vorhanden) zur Genehmigung vorgelegt werden.

Zu den Techniken, die zur Festlegung von Toleranzgrenzen verwendet werden können, gehören:

- Betrachtung historischer Trends in Datenreihen, um normale gegenüber außergewöhnlichen und potenziell weniger tolerierbaren Werten zu verstehen
- Benchmarking mit ähnlichen Unternehmen oder Industriestandards, z.B. ein unternehmensübergreifender Vergleich der Personalfluktuation oder des Krankenstandes oder ein Vergleich der Systemverfügbarkeit, um Verfügbarkeitsstandards zu empfehlen
- Benchmarking zwischen verschiedenen Abteilungen oder Funktionen innerhalb des Unternehmens

Wenn keine Trends oder Benchmarking-Informationen verfügbar sind, sollten die Schwellenwerte auf Grundlage von ‚Experteneinschätzungen', d.h. dokumentierten und freigegebenen Annahmen festgelegt werden und die Schwellenwerte verfeinert werden, wenn zusätzliche Informationen verfügbar werden.

Praktische Beispiele

Beispiel 1

Ein Unternehmen möchte rote und gelbe Toleranzschwellen für die Personalfluktuation festlegen. Eine hohe Fluktuation kann ein Signal für eine sinkende Arbeitsmoral sein und neue Mitarbeiter machen eher Fehler, daher ist das Unternehmen höchst besorgt über einen plötzlichen Anstieg. Die monatliche Personalfluktuation liegt im Durchschnitt bei 3 % mit einer normalen Abweichung von 1 % (d. h. die Fluktuation bewegt sich tendenziell zwischen 2 % und 4 %). Als die Fluktuation im Unternehmen für mehrere Monate auf 6 % anstieg, wurde ein Problem mit der Arbeitsmoral identifiziert. Daher beschließt das Unternehmen, den gelben Schwellenwert auf 4,5 % und den roten Schwellenwert auf 6 % zu setzen.

Beispiel 2

Für die Verfügbarkeit eines neuen Kernsystems müssen rote und gelbe Toleranzschwellen festgelegt werden. Obwohl umfangreiche Tests darauf hindeuten, dass das System sehr zuverlässig ist, gibt es keine historischen Daten über die Stabilität des Systems im regulären täglichen Gebrauch. Das Management legt rote und gelbe Grenzwerte fest, basierend auf den Erfahrungen mit anderen IT-Systemen und den Reaktionen der Benutzer auf Ausfälle. Es gibt Hinweise darauf, dass eine Nichtverfügbarkeitsrate von weniger als 1 % tolerierbar ist, aber 2 % oder mehr den Geschäftsbetrieb stören können. Daher wird der gelbe Grenzwert bei 99 % Verfügbarkeit und der rote bei 98 % festgelegt.

Die Implementierung von operationellem Risikoappetit und Toleranz

Ein Rahmenwerk ist erforderlich, um sicherzustellen, dass Entscheidungen zum Management operationeller Risiken im gesamten Unternehmen mit dem Risikoappetit des Vorstands für operationelle Risiken sowie den risiko- oder kontrollspezifischen Toleranzen übereinstimmen. Die Ausgestaltung eines solchen Rahmenwerks hängt von der Art, dem Umfang und der Komplexität der Unternehmensaktivitäten ab. Die grundlegenden Elemente dieser Ausgestaltung bleiben jeoch gleich.

Kommunikation

Um angemessene Entscheidungen zu gewährleisten, müssen der Risikoappetit eines Unternehmens und die damit verbundenen Toleranzen allen Mitarbeitern mitgeteilt werden, die an Entscheidungen zum Management operationeller Risiken beteiligt sind. Dies kann diejenigen einschließen, die an Aktivitäten beteiligt sind, die ohnehin eine OpRisk-Komponente beinhalten (z.B. der Betrieb von Systemen, Prozessen und Verfahren) sowie diejenigen, die an der Überwachung und Kontrolle von operationellen Risikoexpositionen beteiligt sind (z.B. Personal- und IT-Mitarbeiter).

Unternehmen können ihren allgemeinen Risikoappetit für operationelle Risiken verschiedentlich kommunizieren, z.B. durch Mitarbeitereinführungen und -schulungen, Mitarbeiterversammlungen, Intranetressourcen und Leistungsbeurteilungen. Es wird empfohlen, mehrere Kanäle zu nutzen, um sicherzustellen, dass die Botschaft ankommt und verstanden wird.

Die Toleranzschwellen für bestimmte operationelle Risiken und Kontrollen sollten allen Mitarbeitern mitgeteilt werden, die am Management dieser Risiken und Kontrollen beteiligt sind, insbesondere den Risiko- und Kontrollverantwortlichen, falls diese eingesetzt werden.

Überwachung

Es sollten Verfahren eingeführt werden, die sicherstellen, dass ein Unternehmen innerhalb des von ihm gewählten Risikoappetits und der Toleranzen für operationelle Risiken bleibt. Dadurch wird gewährleistet, dass das Unternehmen seine Ressourcen für das Management operationeller Risiken möglichst effizient einsetzt und gleichzeitig die wichtigsten Risiken für das Management operationeller Risiken vermeidet und abmildert.

Die Gestaltung und Umsetzung dieser Verfahren erfolgt in zwei unterschiedlichen Schritten:

1. Veranlassen, dass die erforderlichen Daten von der entsprechenden Partei in einer vereinbarten Häufigkeit berichtet werden. Es ist wichtig, von Anfang an alle angemessenen Schritte zu unternehmen, um die Integrität der Daten in Bezug auf Vollständigkeit, Genauigkeit und Aktualität sicherzustellen. Es wird empfohlen, die Berichte zu Risikoappetit und -toleranz in die bestehenden Berichte zum operationellen Risiko zu integrieren, um Zeit für die Erstellung neuer Berichte zu sparen und eine Überlastung des Managements zu vermeiden. Eine solche Integration wird dem Management auch helfen, die Bedeutung einer Veränderung der Risikoexposition zu verstehen, z.B. operationelle Risiken, die in ihrer Exposition zunehmen, aber innerhalb von Risikoappetit oder -toleranz bleiben, im Vergleich zu denen, die außerhalb der vereinbarten Risikoappetit oder -toleranzschwellen liegen.
2. Der zweite Schritt ist die entscheidende Phase der Umwandlung von Daten in Informationen, indem Kontext und Interpretation hinzugefügt werden (z.B. wie die Daten mit den Geschäftskennzahlen verglichen werden, ob die Daten auf das Auftreten eines erhöhten oder reduzierten Risikos hindeuten, d.h. ob die Bewegung relativ positiv oder negativ ist).

Dies beinhaltet die Identifizierung und Untersuchung von negativen Abweichungen und Trends sowie die Analyse der zugrundeliegenden Ursachen. Einige wichtige Überlegungen beinhalten, ob:

- wiederkehrendes “gelb” eine statische oder sich verschlechternde Position wiederspiegelt
- eine Gruppe von “Gelben” insgesamt ein “rot” darstellt
- wiederkehrende “grüne” Werte darauf hindeuten können, dass die Schwellenwerte nicht ausreichend sensitiv sind und überprüft werden sollten

Die Überwachung der Leistung gegenüber qualitativen Aussagen zu Risikoappetit oder -toleranz ist anspruchsvoller, sollte aber nach Möglichkeit versucht werden. Eine Lösung besteht darin, regelmäßige Gespräche auf Vorstands-, Risikoausschuss- und Risikofunktionsebene darüber zu führen, ob das Verhalten der Mitarbeiter und die Unternehmensaktivitäten mit diesen Aussagen übereinstimmen. Andere relevante Funktionen wie die Interne Revision, die Personalabteilung und die IT-Sicherheit können ebenfalls einbezogen werden, um deren Meinung zu erfahren. Der Wert von Gesprächen über operationelle Risiken sollte nicht unterschätzt werden. Er kann dazu beitragen, das Risikobewusstsein zu fördern und potenzielle Problembereiche zu identifizieren.

Zu den formelleren Mechanismen zur Überwachung der Leistung in Bezug auf die qualitativen Aussagen gehören Überprüfungen durch die Interne Revision, Informationen aus den Leistungsbeurteilungen der Mitarbeiter (bei denen die Einhaltung der wichtigsten qualitativen Aussagen bewertet werden könnte) und Untersuchungen von Schadensfällen, um festzustellen, ob sie teilweise das Ergebnis von Verhaltensweisen oder Handlungen waren, die in den qualitativen Aussagen enthalten sind (z.B. Verstöße gegen aufsichtsrechtliche Bestimmungen).

Aggregation und Berichtswesen

Einige der Herausforderungen bei der Aggregation und Berichterstattung ergeben sich aus dem Sinn von Toleranzschwellen, die in verschiedenen Teilen des Unternehmens festgelegt werden.

Wenn ein Geschäftsbereich die Toleranzen auf Konzernebene übernimmt, wird er mit ziemlicher Sicherheit einen dauerhaften “grünen” Status melden, da der Umfang seiner Tätigkeit nicht ausreicht, um die Konzernschwellenwerte zu verletzen - somit würde es nirgendwo im Unternehmen einen Auslöser für Maßnahmen geben. Andererseits kann ein “roter” Status auf Ebene des Geschäftsbereichs auf Konzernebene wenig oder gar keine Bedeutung haben und somit den Wert der “inakzeptabel”-Flagge auf der Ebene der Geschäftsbereichsleitung verwässern.

Eine Lösung, die von einigen Unternehmen angewandt wird, beinhaltet die Neukalibrierung von Schwellenwerten auf verschiedenen Unternehmensebenen. Abbildung 1 zeigt ein Beispiel.

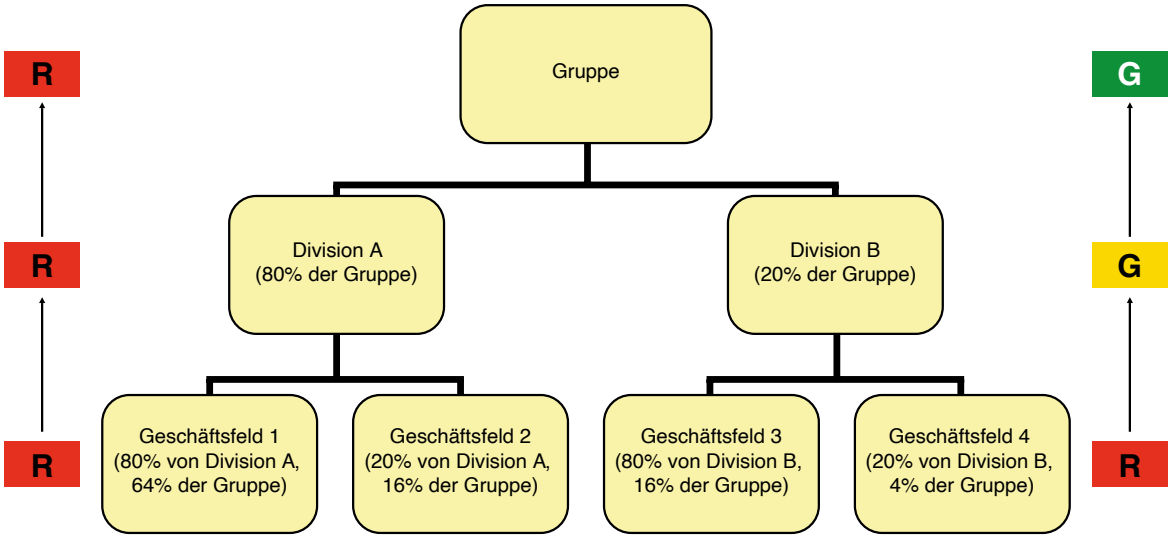

Abbildung 1

Die Risikoexposition auf der linken Seite dieses Diagramms gehört zu Geschäftsbereich 1, der 80% der Division A darstellt, die wiederum 80% des Konzerns bildet. In diesem Fall ist der "rote" Status auf Geschäftsbereichsebene von ähnlicher Bedeutung im Kontext der Division und des Konzerns als Ganzes. Das Risiko auf der rechten Seite dieses Diagramms ist ebenfalls ein "rotes" Risiko auf Geschäftsbereichsebene, da es für das Management des Geschäftsbereichs 4 von Bedeutung ist. Da dieser Geschäftsbereich jedoch nur ein kleiner Teil der Division B ist, die wiederum nur ein kleiner Teil des Konzerns ist, nimmt die Bedeutung mit der Eskalation nach oben im Unternehmen ab.

Eine Rekalibrierung auf Divisions- und/oder Konzernebene kann erreicht werden, indem die berichteten Daten entsprechend der relativen Größe des auslösenden Geschäftsbereichs gewichtet werden. Die Gewichtung darf jedoch nicht so niedrig sein, dass sie sich der Kontrolle auf höchster Ebene entzieht:

- Die Auswirkungen eines schlecht gemanagten operationellen Risikos in einem Geschäftsbereich können sich ansteckend auf den Ruf des gesamten Konzerns auswirken.
- Schwächen im Management des operationellen Risikos können systemisch sein, d.h., dass Probleme in einem Geschäftsbereich ein Signal für Probleme in anderen Bereichen sein können.

Daher muss die aggregierte Position auf Basis von gesundem Menschenverstand verwaltet werden. Wie gut ein aggregiertes Berichtssystem auch sein mag, es entbindet nicht von der Notwendigkeit eines qualitativen und bewertenden Ansatzes in der Konzernzentrale.

Management und Entscheidungsfindung

Der Risikoappetit eines Unternehmens für operationelle Risiken und die damit verbundenen Toleranzen sollte zur Steuerung von Maßnahmen genutzt werden. Unternehmen sollten keine Risiken oder Kontrollschwächen akzeptieren, die außerhalb ihres allgemeinen Risikoappetits für operationelle Risiken oder der vereinbarten Toleranzschwellen liegen. Zu den wichtigsten Entscheidungen gehören:

- Ob es angemessen ist, die Verletzung für einen begrenzten Zeitraum zu akzeptieren. Nach Abwägung aller Hinweise kann es sein, dass es sich bei einem Verstoß um eine wirklich einmalige Ausnahme handelt. In anderen Fällen kann es angemessen sein, frühere Toleranzschwellen zu überprüfen und neu zu kalibrieren, wenn sie als zu empfindlich erachtet werden. Es wird empfohlen, solche Akzeptanzen aufzuzeichnen und regelmäßig zu überprüfen.
- Ergreifen von Maßnahmen zur Abschwächung/ Vermeidung und Verhinderung eines erneuten Auftretens. Dies ist wahrscheinlich die angemessenste Reaktion auf einen Verstoß gegen den operationellen Risikoappetit oder die Risikotoleranz und erfordert die Genehmigung zur Umsetzung einiger zusätzlicher oder alternativer Kontrollmaßnahmen.
- Einige Zwischenmaßnahmen des Managements - z.B. die Durchführung einer erweiterten oder intensiveren Überwachung, die Durchführung einer zusätzlichen Ursachenanalyse oder die Untersuchung des Kosten-Nutzen-Verhältnisses von Optionen zur Mitigation.

Fazit

Die Gestaltung und Umsetzung eines Rahmenwerks für den operationellen Risikoappetit/die Risikotoleranz ist eine Herausforderung. Die Vorteile können jedoch beträchtlich sein. Unternehmen scheitern entweder an einer übermäßigen oder unzureichenden Risikobereitschaft. Durch die Festlegung eines Rahmens für Risikoappetit und -toleranz können sie sicherstellen, dass bei der Verfolgung ihrer Ziele ein angemessenes Maß an Risiken, einschließlich operationeller Risiken, eingegangen wird.

Anhang A: Beispiel für ein OpRisk Appetit Formular

	1 Avers	2 Vorsichtig	3 Offen/ Optimistisch	4 Bedeutend
Beschreibung der Risikobereitschaft	**Vermeidung von operationellem Risiko ist ein wichtiges Ziel**	**Vorliebe für sichere Optionen, die ein geringes operationelles Risiko aufweisen und möglicherweise nur ein begrenztes Gewinnpotenzial haben**	**Darauf vorbereitet, alle Optionen in Betracht zu ziehen und diejenige zu wählen, die am wahrscheinlichsten zu einer positiven Rendite führt, auch wenn diese ein Element des operationellen Risikos beinhaltet**	**Bereitschaft, innovativ zu sein und sich für Optionen zu entscheiden, die potenziell höhere geschäftliche Vorteile bieten (trotz eines größeren inhärenten operationellen Risikos)**
Operationelles Risiko Strategische Auswirkungen	**Beispiele für Verhaltensweisen bei wichtigen Entscheidungen…**			
Finanziell • Einkommen • Ausgaben • Beschaffung • Betrug • Wirtschaftlichkeit	• Vermeidung von finanziellen Verlusten ist ein wichtiges Ziel • Keine Akzeptanz von Budgetabweichungen • Abzug von Ressourcen aus nicht-wesentlichen Aktivitäten, die das Unternehmen einem operationellen Risiko aussetzen	• Bereitschaft, für hohe Gewinne die Möglichkeit eines begrenzten finanziellen Verlusts zu akzeptieren • Risikoreduzierung bleibt das Hauptanliegen, vor allem, wenn Budgets gefährdet werden können	• Bereitschaft, für eine Rendite zu investieren und die Möglichkeit eines finanziellen Verlusts zu minimieren, indem operationelle Risiken auf ein tolerierbares Niveau gebracht werden • Wert und Nutzen berücksichtigt (nicht nur das geringste Risiko) • Das Budget ist nicht festgelegt und wird fließend nach Priorität zugewiesen • Ressourcen werden zugewiesen, um potenzielle Chancen zu nutzen	• Bereitschaft, für die bestmögliche Rendite zu investieren und die Möglichkeit eines finanziellen Verlusts zu akzeptieren (obwohl Kontrollen vorhanden sein können) • Das Budget wird entsprechend der Chance auf die höchste Rendite zugewiesen • Ressourcen werden auch dann zugewiesen, wenn sich operationelle Risiken auf die Rendite auswirken könnten
Regulatorisch und rechtlich • Einhaltung gesetzlicher Vorschriften • Governance • Rechtliche Herausforderung	• Alles vermeiden, was angefochten werden könnte, auch erfolglos • Compliance-getrieben/ überinvestiert in Kontrolle • Immer auf Nummer sicher gehen	• Begrenzte Toleranz für das Eingehen von Risiken. Wollen einigermaßen sicher sein, dass wir jede Herausforderung gewinnen oder eine Prüfung überstehen würden • Normale Investition in Compliance	• Bereitschaft zur Anfechtung der allgemeinen Verordnung, wenn eine ordnungsgemäße Bewertung der Optionen erfolgt ist, die im Zusammenhang mit dem spezifischen/ unterschiedlichen Betriebsumfeld des Unternehmens gerechtfertigt werden kann	• Die Chancen, Herausforderungen nicht zu meistern sind hoch und die Konsequenzen schwerwiegend, aber ein Erfolg würde enorme, standardsetzende Vorteile mit sich bringen • Hat das Potenzial, die Aufmerksamkeit der Aufsichtsbehörde auf sich zu ziehen
Reputation und Kundenbetreuung • Reputation • Gesellschaft	• Minimale Toleranz für alle Entscheidungen, die zu Anfechtungen, negativer Publizität oder Überprüfung führen könnten	• Die Toleranzen für das Eingehen von Risiken beschränken sich auf Ereignisse, bei denen im Falle eines Fehlers nur eine geringe Chance auf erhebliche Auswirkungen besteht	• Bereitschaft, Entscheidungen zu treffen, um die Reputation zu verbessern, mit einem gewissen Potenzial für zusätzliche Publicity, aber nur, wenn geeignete Schritte unternommen wurden, um Risikoexpositionen zu minimieren	• Bereitschaft, Entscheidungen zu treffen, die wahrscheinlich Herausforderungen mit sich bringen, bei denen aber der potenzielle Nutzen die Risiken überwiegt
Personal • Gleichberechtigung • Menschen • Sozial	• Mitarbeiter schützen • Status quo so weit wie möglich beibehalten	• Schützen Sie das Personal so gut wie möglich	• Flexibles Management von Mitarbeitern	• Maximierung von Effizienz und Kosteneinsparungen

www.theirm.org

irm

Developing risk professionals