Operational Risk Governance

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

Inhalt

Abschnitt 1 – Einführung

Alle Unternehmen verfügen über Governance-Regelungen, um sicherzustellen, dass sie auf eine Art geleitet und kontrolliert werden, die den Anforderungen ihrer Stakeholder (Aktionäre, Gläubiger, Aufsichtsbehörden usw.) entspricht. Diese Governance-Regelungen erstrecken sich über alle Aspekte der Aktivitäten und Abläufe eines Unternehmens, einschließlich strategischer und taktischer Entscheidungen. Das Management von Risiken ist ein zentrales Element dieser Regelungen. Dazu gehört auch das Management des operationellen Risikos.

Dieses Papier konzentriert sich auf solide Praktiken für das Management operationeller Risiken. Das Papier soll nicht die bestehenden Governance-Kodizes und -Standards ersetzen wie z.B. den UK Corporate Governance Code oder die OECD-Prinzipien der Corporate Governance. Vielmehr sollen Praktiken aufgezeigt werden, die zur Unterstützung eines effektiven und angemessenen Managements von operationellen Risiken als Teil der allgemeinen Governance-Aktivitäten eines Unternehmens eingesetzt werden können.

Mit soliden Praktiken für die Steuerung des Managements operationeller Risiken kann ein Unternehmen sicherstellen, dass seine operationellen Risiken im Rahmen des Risikoappetits bleiben, dass die geltenden Gesetze und Vorschriften (z.B. Gesundheits- und Sicherheitsvorschriften, Umweltvorschriften und Finanzvorschriften) eingehalten werden und dass die internen Richtlinien und Verfahren für das Management operationeller Risiken befolgt werden. Darüber hinaus sollte das Management operationeller Risiken die umfassenderen Corporate-Governance-Aktivitäten eines Unternehmens durch die Kontrolle “menschlicher Risiken” unterstützen, einschließlich unangemessenem Verhalten von Geschäftsführern, Managern und Mitarbeitern, Fahrlässigkeit oder krimineller Aktivitäten.

Operationelles Risikomanagement und Governance sind daher eng miteinander verbunden. Ein integriertes Rahmenwerk für das Management operationeller Risiken ist ohne effektive Corporate-Governance-Regelungen nicht möglich. Ebenso sind effektive Corporate-Governance-Regelungen von einem integrierten Rahmenwerk für das Management operationeller Risiken abhängig. Weitere Informationen zur Integration des operationellen Risikos sowie zum Risikoappetit finden Sie in den IOR-Leitfäden zu diesen Themen.

Abschnitt 2 – Die Rolle der Operational Risk Governance

Die Governance des operationellen Risikos ist die Architektur (Richtlinien, Strukturen, Berichtsvereinbarungen usw.), durch die das Management des operationellen Risikos überwacht und gesteuert wird. Die Rolle dieser Architektur besteht darin, den Überblick über die Aktivitäten des OpRisk-Managements in einem Unternehmen zu erleichtern, um sicherzustellen, dass Entscheidungen zum OpRisk Management konsistent getroffen werden und dass diese Entscheidungen das Erreichen der Unternehmensziele unterstützen, anstatt sie zu behindern. Die Operational Risk Governance erfüllt somit folgende Aufgaben:

- Dem Leitungsgremium eines Unternehmens versichern, dass das Unternehmen über ein solides System interner Kontrollen für das Management operationeller Risiken verfügt
- Eskalation von Bedenken hinsichtlich des OpRisk-Managements an das Leitungsorgan des Unternehmens, insbesondere wenn solche Bedenken das Erreichen der Unternehmensziele gefährden können
- Sicherstellung, dass das operationelle Risiko des Unternehmens innerhalb des vereinbarten Risikoappetits bzw. der Toleranzgrenzen gehalten wird (sofern relevant)
- Einhaltung externer Gesetze und Vorschriften, die sich auf das Management von operationellen Risiken beziehen
- Überwachung der Einhaltung interner Richtlinien und Verfahren für operationelle Risiken
- Zuweisung von Rollen und Verantwortlichkeiten für das Management operationeller Risiken und Sicherstellung, dass diese Rollen und Verantwortlichkeiten korrekt ausgeführt werden
- Das Management von personen- und verhaltensbezogenen Risiken, bei denen das Verhalten von Geschäftsführern, Managern, Mitarbeitern und externen Auftragnehmern nicht mit den Unternehmenszielen vereinbar ist

Abschnitt 3 – Elemente der OpRisk Governance Architektur

Die Governance-Architektur für das operationelle Risiko eines Unternehmens besteht aus einer Reihe von sich ergänzenden Elementen, die im Folgenden beschrieben werden. Es ist wichtig, dass diese Elemente sich gegenseitig unterstützen, da sonst Lücken oder Schwachstellen entstehen können.

Die Elemente dieser Architektur umfassen die formellen und informellen Strukturen eines Unternehmens. Die formellen Strukturen beziehen sich auf die konkreten Richtlinien, Verfahren, Rollen und Instrumente, die für das Management des operationellen Risikos verwendet werden. Das primäre Element der informellen Struktur ist die Risikokultur.

Abschnitt 3.1 – Risikokultur und OpRisk Governance

Das IOR hat einen separaten Leitfaden zum Management der Risikokultur herausgegeben. Weitere Informationen über die Aufrechterhaltung einer angemessenen Risikokultur finden Sie dort.

Aus Sicht der Operational Risk Governance wird die Risikokultur eines Unternehmens durch die Einstellungen, Verhaltensweisen und das Verhalten der Führungskräfte und Mitarbeiter sowohl beeinflusst als auch reflektiert. In dieser Hinsicht wirken sich die formalen Elemente der Operational-Risk-Governance-Architektur eines Unternehmens auf dessen Risikokultur aus und umgekehrt.

Ein zentrales Anliegen ist die Frage, wie Manager und Mitarbeiter die relativen Kosten und Vorteile der formalen Governance-Strukturen für operationelle Risiken in einem Unternehmen wahrnehmen. Wenn die mit diesen Strukturen verbundenen Kosten als übermäßig empfunden werden, können Unmut und Widerstand wachsen und das Vertrauen zwischen der Operational-Risk-Funktion und dem breiteren Unternehmen schwinden. Dies wiederum kann die wirksame Integration des Managements operationeller Risiken verhindern und sogar zu unangemessenem Verhalten und Fehlverhalten führen.

Bei der Gestaltung und Implementierung von formalen Governance-Strukturen für das Management von operationellen Risiken sollte darauf geachtet werden, dass die potenziellen Auswirkungen dieser Strukturen auf die Risikokultur des Unternehmens berücksichtigt werden. Lösungen umfassen:

- Beratung mit Managern und Mitarbeitern über die geschäftlichen Auswirkungen jeglicher neuen Governance-Regelungen für operationelle Risiken (um die Auswirkungen auf Betriebskosten, Effizienz usw. zu bewerten)
- Regelmäßige Überprüfung der formalen Governance-Regelungen, sowohl um die Notwendigkeit neuer Maßnahmen zu prüfen als auch um veraltete Maßnahmen zu entfernen
- Einbindung von Managern und Mitarbeitern in die oben genannten Überprüfungen

Zusammenarbeit mit Kollegen in verwandten Kontrollfunktionen (z.B. Personalabteilung, IT-Sicherheit, Interne Revision, Compliance usw.), um Überschneidungen bei den Governance-Regelungen zu minimieren.

Abschnitt 3.2 – Verantwortung für das operationelle Risiko

Das Leitungsorgan (z.B. der Vorstand) ist letztendlich für die OpRisk Governance verantwortlich. Es wird dabei von den Geschäftsführern und der oberen Führungsebene eines Unternehmens unterstützt, an die in der Regel die Verantwortung für die Umsetzung wirksamer Governance-Regelungen für operationelle Risiken delegiert wird.

Das Leitungsgremium und die unterstützenden Geschäftsführer und leitenden Angestellten sollten:

- die Standards festlegen, nach denen das Unternehmen arbeiten soll; dazu gehört auch, dass sie den Risikoappetit des Unternehmens für operationelle Risiken festlegen und ihre Richtlinie für das operationelle Risikomanagement zusammen mit allen anderen damit verbundenen Richtlinien (z.B. Gesundheit und Sicherheit, IT-Sicherheit) genehmigen
- die Verpflichtung zur Einhaltung der oben genannten Standards durch das, was sie sagen und tun ("walking the walk", nicht nur "talking the talk") demonstrieren
- die Regelungen zur Steuerung des operationellen Risikos regelmäßig überwachen und überprüfen, um sicherzustellen, dass sie korrekt funktionieren

Abschnitt 3.3 – Formen der Verantwortlichkeit

Die formale Governance-Struktur eines Unternehmens sollte klare und diskrete Verantwortlichkeiten für die Umsetzung, Gestaltung und Sicherstellung ihres Rahmenwerks für das Management operationeller Risiken zuordnen. Diese Mechanismen werden in Tabelle 1 erläutert:

Mechanismus	Beschreibung
Umsetzung	Verantwortlich für die tägliche Umsetzung des Rahmenwerks für das Management operationeller Risiken. Dies umfasst in der Regel die Einhaltung des vereinbarten Risikoappetits oder der Toleranzgrenzen für operationelle Risiken, die Sicherstellung der Einhaltung der Richtlinien für das operationelle Risikomanagement und die Sicherstellung der korrekten Einhaltung der Verfahren für operationelle Risiken (z.B. Aktualisieren der Risiko- und Kontrollbewertungen, Eskalieren von Schadenfällen usw.).
Gestaltung	Verantwortlich für die Richtlinien, Verfahren und Instrumente, die ein Rahmenwerk für das Management des operationellen Risikos bilden. Weitere Informationen zu den Inhalten eines Rahmenwerks für das Management des operationellen Risikos finden Sie im Papier des IOR zur Integration des operationellen Risikos.
Sicherstellung	Überprüft die Umsetzung und Gestaltung des Rahmenwerks für das operationelle Risikomanagement. Bietet dem Leitungsorgan die Sicherheit, dass das Rahmenwerk angemessen ist und wie beabsichtigt funktioniert.

Tabelle 1: Die drei Formen der Verantwortlichkeit

Abschnitt 3.4 – Der Ansatz der drei Verteidigungslinien

Eine häufige Nutzung für die oben genannten Formen ist der Ansatz der drei Verteidigungslinien. Dieser Ansatz ist in Unternehmen weit verbreitet, insbesondere im Finanzdienstleistungssektor, wo er in Vorschriften und Standards gefördert wird. Zwei Merkmale zeichnen den Ansatz aus:

- Die drei Arten der Rechenschaftspflicht sind sehr klar voneinander getrennt. Das bedeutet, dass Einzelpersonen und die Funktionen oder Abteilungen, in denen sie angesiedelt sind, nur eine Rolle (Umsetzung, Gestaltung oder Sicherstellung) haben können. In der Regel wird dem sogenannten “Front-Line”-Management die Verantwortung für die Umsetzung zugewiesen, die (operationelle) Risikofunktion ist für die Gestaltung verantwortlich und die Interne Revision ist für die Sicherstellung zuständig
- Den Verantwortlichen für die Gestaltung des Rahmenwerks für das Management operationeller Risiken (in der Regel die zentrale Risiko- oder Operational-Risk-Management-Funktion) wird eine zusätzliche Überwachungsfunktion zugewiesen. Das bedeutet, dass sie die Verantwortlichen für die Umsetzung des Rahmenwerks überwachen und Maßnahmen ergreifen, um etwaige Fehler oder Versäumnisse zu korrigieren

Ein Vorteil des Ansatzes der drei Verteidigungslinien ist, dass er das Potenzial für Interessenkonflikte bei Personen oder Funktionen durch die Trennung der drei Arten der Rechenschaftspflicht abschwächt. Je stärker diese Funktionen getrennt sind, desto wahrscheinlicher ist es, dass Schwächen in der Konzeption oder Implementierung schnell entdeckt und korrigiert werden.

Ein weiterer angeblicher Vorteil des Ansatzes ist, dass durch die Zuweisung einer Aufsichtsfunktion an die Entwickler des Rahmenwerks für das Management operationeller Risiken Fehler oder Versäumnisse bei der Implementierung schnell aufgedeckt werden, anstatt sich auf unregelmäßige interne Prüfungen zu verlassen, um Bedenken zu erkennen.

Der Ansatz hat jedoch auch einige erhebliche Nachteile. Erstens kann die Trennung der drei Arten der Rechenschaftspflicht, insbesondere wenn die dafür verantwortlichen Personen oder Funktionen physisch getrennt werden (z.B. durch Platzierung an verschiedenen Orten), zu einem ernsthaften Bruch von Vertrauen und Zusammenarbeit führen. Vertrauen und Kooperation werden aufgebaut, wenn Kollegen zusammenarbeiten und sich gegenseitig helfen können. Wenn die Zusammenarbeit behindert wird, kann dies sehr schnell zu Widerstand und sogar zu Konflikten führen, die sich z.B. darin äußern, dass die Geschäftsleiter die Richtlinien oder Verfahren für operationelle Risiken nicht korrekt befolgen, dass sie es versäumen, Probleme zu eskalieren, oder dass sie im Extremfall rücksichtslos Risiken eingehen.

Zweitens kann eine strikte Auslegung des Drei-Linien-Ansatzes verhindern, dass diejenigen, die für die Gestaltung und Sicherstellung des Rahmenwerks für das Management operationeller Risiken verantwortlich sind, denjenigen helfen, die mit dessen Umsetzung beauftragt sind. Geschäftsleiter und ihre Teams haben viele Verantwortlichkeiten und sind selten Risikoexperten. Das bedeutet, dass sie oft Schwierigkeiten haben, die Richtlinien und Verfahren für das Management operationeller Risiken zu verstehen, und deren Umsetzung als komplex und zeitaufwändig empfinden können. Ohne Anleitung und Schulung durch die Experten für die Gestaltung und Sicherstellung des Rahmenwerks für das Management operationeller Risiken ist es daher wahrscheinlicher, dass sie Fehler machen und unnötige Ressourcenkosten verursachen.

In Anbetracht der Vor- und Nachteile eines strikten Drei-Linien-Ansatzes sollten Unternehmen sorgfältig über dessen Einführung nachdenken. Wo die Aufsichtsbehörden einen strikten Drei-Linien-Ansatz verlangen, sollte ein solcher implementiert werden - unter anderen Voraussetzungen ist ein strenger Drei-Linien-Ansatz jedoch selten optimal.

Abschnitt 3.5 – Ein alternativer ‘gemischter’ Ansatz

Abbildung 2 veranschaulicht eine Alternative zum Drei-Linien-Ansatz. Dieser “gemischte” Ansatz behält klare Verantwortlichkeiten für die Umsetzung, Gestaltung und Sicherstellung bei, fördert aber die Zusammenarbeit (ein gewisses Maß an Überlappung) zwischen diesen Rollen.

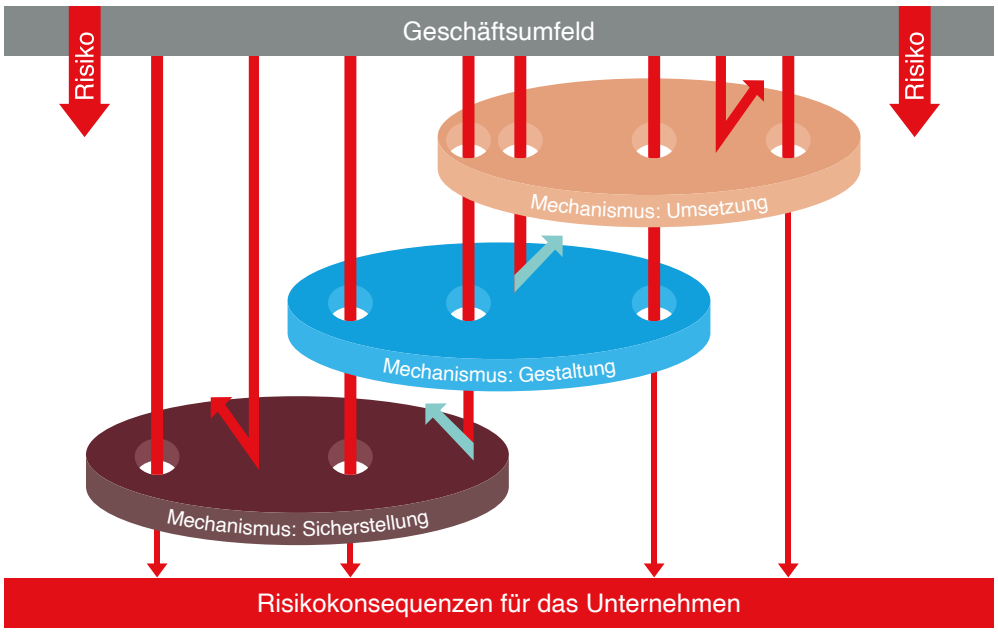

Abbildung 1: Verantwortlichkeiten mischen

Der Vorteil der Zusammenarbeit besteht darin, dass Vertrauen zwischen den Verantwortlichen für jede der drei Formen aufgebaut werden kann. Vertrauen, das durch die Zusammenarbeit dabei entsteht, die effektive Steuerung des Managements operationeller Risiken sicherzustellen. Außerdem können diejenigen, die an der Gestaltung und Sicherung des Rahmenwerks für das Management operationeller Risiken beteiligt sind, die für die Umsetzung Verantwortlichen unterstützen, indem sie Schulungen, Coaching usw. anbieten.

Eine verbesserte Zusammenarbeit kann folglich dazu beitragen, operationelle Risikoereignisse (rote Pfeile im Diagramm) zu verhindern und abzuschwächen, indem potenzielle Ursachen beseitigt und die zugehörige Kontrollumgebung verbessert wird. Außerdem kann sie dazu beitragen, die Governance des operationellen Risikos zu verbessern, und zwar durch Verbesserungen bei der Umsetzung, der Gestaltung und der Sicherstellung des Rahmenwerks für das operationelle Risikomanagement (rote bis blaue Pfeile stellen das Potenzial für wertschöpfende Prozessverbesserungen dar).

Um zu verstehen, wie Zusammenarbeit die Governance des operationellen Risikos verbessern kann, ist es wichtig, sich vor Augen zu führen, dass die Funktionen Operationelles Risiko und Interne Revision zwar über technische Experten für operationelle Risiken verfügen, das Business Management aber in der Regel ein besseres Verständnis für das Tagesgeschäft des Unternehmens hat. Durch die Kombination von Risikoexpertise und operativer Erfahrung können die Regelungen zur OpRisk Governance effektiver und ressourceneffizienter gestaltet werden, was dem Unternehmen einen Mehrwert bringt, da es seine Ziele besser erreichen kann.

Es sollte betont werden, dass dieser gemischte Ansatz nicht impliziert, dass Einzelpersonen oder Funktionen mehrere Rollen haben sollten, sondern lediglich, dass Einzelpersonen und Funktionen zusammenarbeiten sollten. In Bezug auf die operationelle Risikofunktion könnte dies bedeuten:

- Eine separate Berichtslinie zum Business Management und ggf. zur Internen Revision zu haben
- Gute Beziehungen sowohl zum Business Management als auch zur Internen Revision zu pflegen. Dazu gehören regelmäßige Kommunikation, Beziehungsmanagement-Meetings, informelle Treffen usw.
- Teilnahme an Besprechungen mit dem Business Management, die sich auf die Umsetzung des Rahmenwerks für das Management operationeller Risiken beziehen
- Bereitstellung von Schulungen und Coaching für Business Manager und ihre Teams zur Unterstützung der Umsetzung des Rahmenwerks für das Management operationeller Risiken
- Bereitstellung interner Beratungsleistungen zum operationellen Risiko, einschließlich Unterstützung bei der Entscheidungsfindung (es sollte jedoch klargestellt werden, dass die Funktion für operationelles Risiko nicht für die Ergebnisse dieser Entscheidungen verantwortlich gemacht werden kann)
- Wenn möglich sicherstellen, dass das OpRisk Team nahe der für die Umsetzung Verantwortlichen angesiedelt ist und leicht erreicht werden kann (z.B. durch das Management von Zugangskontrollen)

Abschnitt 3.6 – Operational Risk Komitees

Die meisten Governance-Strukturen für das operationelle Risiko umfassen ein oder mehrere Komitees, die für die Überwachung der Gestaltung, Umsetzung und Sicherung des Rahmenwerks für das operationelle Risiko verantwortlich sind.

In größeren Unternehmen können separate Komitees für operationelle Risiken eingerichtet werden. Dazu könnten mehrere abteilungsspezifische Komitees für operationelle Risiken gehören, die an ein konzernweites Komitee für operationelle Risiken berichten, das vom Group Head of Operational Risk oder dem Chief Risk Officer (CRO) geleitet wird. Das konzerweite Operational Risk Komitee wiederum kann an ein gruppenweites, vom Vorstand eingesetztes, delegiertes Risikokomitee oder ein gleichwertiges Gremium berichten.

In kleineren Unternehmen kann es ein einziges Komitee für operationelle Risiken geben oder das operationelle Risiko kann Teil der Aufgabenstellung eines vom Vorstand delegierten Risikoausschusses, eines Prüfungs- und Risikoausschusses oder eines Prüfungsausschusses sein.

Zumindest sollte die Übersicht über die Steuerung des operationellen Risikos Teil der Aufgabenbeschreibung für mindestens einen Ausschuss auf Vorstandsebene sein. Dabei kann es sich um den Vorstand oder häufiger um den vom Vorstand beauftragten Prüfungs- und Risikoausschuss oder Prüfungsausschuss handeln.

In Bezug auf die Steuerung des operationellen Risikos sollte die Aufgabenstellung für die entsprechenden Ausschüsse Folgendes beinhalten: Verantwortung für die Überwachung der Umsetzung und Gestaltung des Rahmenwerks für das Management operationeller Risiken und im Falle eines Prüfungs- oder Prüfungs- und Risikoausschusses Verantwortung für die Überwachung der Sicherstellung des Rahmenwerks für operationelle Risiken, einschließlich der Überprüfung

- aller betrieblichen Risikofragen, die ein zufriedenstellendes Ergebnis externer Finanzprüfungen beeinträchtigen oder die Richtigkeit der Finanzberichte in Frage stellen könnten
- operationeller Schadenfälle, die für die Finanzberichterstattung als wesentlich angesehen werden; und interne Prüfungen, die sich auf das operationelle Risikomanagement beziehen sowie die Genehmigung des jährlichen internen Prüfungsplans

- der OpRisk-Richtlinie auf mindestens jährlicher Basis und Empfehlung an das Leitungsorgan, die Richtlinie zu genehmigen (oder nicht)
- dass angemessene Maßnahmen ergriffen werden, um Verstöße gegen die OpRisk-Richtlinie oder gegen die zugehörigen Verfahren zu beheben
- von Risikoprofilberichten, einschließlich Berichten über operationelle Risikoereignisse und der Wirksamkeit der Kontrollen für operationelle Risiken
- dass das operationelle Risiko innerhalb des genehmigten Risikoappetits oder der Toleranzgrenzen gehalten wird, wo dies relevant ist

Obwohl ein oder mehrere Komitees die Verantwortung für die OpRisk Governance delegiert haben können, muss das Leitungsorgan die Gesamtverantwortung für die Governance behalten. Es müssen geeignete Vorkehrungen getroffen werden, um das Leitungsorgan über die Arbeit dieser Komitees und insbesondere über die Arbeit der vom Vorstand delegierten Risiko- und/oder Prüfungsausschüsse zu informieren. Der gesamte Vorstand muss sich jederzeit darauf verlassen können, dass im gesamten Unternehmen ein solides System zur Steuerung des operationellen Risikos vorhanden ist.

Wo eine Hierarchie von Komitees für das operationelle Risiko besteht, müssen Eskalationsverfahren vereinbart werden, um sicherzustellen, dass wichtige Risikoauslastungen, Ereignisse oder Bedenken zeitnah an die entsprechende Managementebene gemeldet werden. Tabelle 2 fasst die relevanten Bedeutungsebenen für die OpRisk Governance zusammen.

Vom Vorstand delegiertes Komitee	Alle operativen Risikopositionen oder Kontrollschwächen, die das Erreichen der Unternehmensziele oder die Integrität der Finanzberichterstattung gefährden.
Konzernweites Komitee	Systemische Risikopositionen oder Kontrollschwächen, die sich auf mehrere Abteilungen oder Bereiche des Unternehmens auswirken können. Abteilungsspezifische Risiken oder Kontrollschwächen, die das Erreichen der Unternehmensziele gefährden können.
Abteilungsbasiertes Komitee	Alle Risikopositionen oder Kontrollschwächen, die sich auf den effizienten Betrieb der Abteilung oder ihre Fähigkeit, die Leistungsziele zu erreichen, auswirken können.

Tabelle 2: Eskalation von OpRisk Risikopotenzial, -ereignissen oder Bedenken

Abschnitt 4 – Umsetzung der Operational Risk Governance

Erfolg oder Misserfolg der Operational Risk Governance hängen davon ab, wie sie umgesetzt wird. Eine wirksame Umsetzung erfordert die Zuordnung klarer und eindeutiger Rollen und Verantwortlichkeiten für das Management des operationellen Risikos, kombiniert mit geeigneten Richtlinien und Verfahren sowie einer entsprechenden Berichterstattung.

Abschnitt 4.1 – Rollen und Verantwortlichkeiten

Die Rollen und Verantwortlichkeiten variieren je nach formaler Struktur der Operational Risk Governance (z.B. ein Drei-Linien- oder ein gemischter Ansatz) und der Art, dem Umfang und der Komplexität der Unternehmensaktivitäten.

Im Folgenden werden gängige Rollen in Bezug auf die Operational Risk Governance erläutert.

Abschnitt 4.2 – Risikoeigner

Bei den Risikoeignern handelt es sich in der Regel um Business Manager, die für das Tagesgeschäft des Unternehmens verantwortlich sind. Alle Abteilungen oder Funktionen haben einen oder mehrere Risikoeigner (z.B. Finanzen, Marketing, Kundendienst usw.). Dazu gehören auch die Risikofunktion und die Funktion Operationelle Risiken. Der Leiter der Risikofunktion ist z.B. für die Gesundheit und Sicherheit seiner Mitarbeiter verantwortlich, daher ist er der Risikoeigner für Gesundheits- und Sicherheitsrisiken in seiner Funktion.

Risikoeigner sind für das Management einer oder mehrerer Risikokategorien in ihrem Zuständigkeitsbereich verantwortlich. Aus Sicht der OpRisk-Governance sind die Eigner der operationellen Risiken für die Umsetzung des Rahmenwerks für das Management operationeller Risiken in ihrem Bereich verantwortlich. Dazu gehört auch, dass sie und ihre Mitarbeiter die Richtlinie für operationelle Risiken und die zugehörigen Verfahren einhalten. Gegebenenfalls sind sie auch dafür verantwortlich, dass die operationellen Risiken innerhalb des Risikoappetits bzw. der Risikotoleranz gehalten werden.

Es wird empfohlen, Risikoeigner für jede der Hauptkategorien operationeller Risiken, denen eine bestimmte Abteilung oder Funktion ausgesetzt ist, zu benennen. Zum Beispiel Gesundheit und Sicherheit, Betrug, Cybersicherheit. Oftmals übernimmt der Abteilungs- oder Funktionsleiter die Verantwortung als Risikoeigner. Alternativ kann die Verantwortung auch an mehrere spezialisierte Manager delegiert werden. Wo die Verantwortung delegiert wird, sollte den Abteilungs- oder Funktionsleitern verdeutlicht werden, dass sie die letztendliche Verantwortung für die Steuerung des operationellen Risikomanagements in ihrem Bereich behalten.

Abschnitt 4.3 – Der CRO

Einige Unternehmen ernennen einen CRO, der die Tätigkeit ihrer Risikomanagement-Funktion leitet. Wenn ein CRO ernannt wird, muss er über die notwendigen Befugnisse verfügen, um eine effektive Risikosteuerung im gesamten Unternehmen zu gewährleisten, einschließlich der Governance des operationellen Risikos. Um dies zu erreichen, sollte der CRO bei Bedarf auch direkten Zugang zum Leitungsorgan und zu allen vom Vorstand beauftragten Komitees mit Zuständigkeit für die OpRisk Governance haben.

In Bezug auf das operationelle Risiko ist der CRO die Person, die letztlich die Verantwortung für die Gestaltung des OpRisk Management Rahmenwerks und die damit verbundenen Governance-Regelungen trägt, um sicherzustellen, dass dieses Rahmenwerk im gesamten Unternehmen angemessen umgesetzt wird. In dieser Hinsicht sollte der CRO idealerweise

an den Chief Executive Officer und nicht an den Chief Financial Officer (CFO) oder den Chief Operating Officer (COO) berichten. Dies soll sicherstellen, dass völlig unabhängige Berichtslinien für die Umsetzung und Gestaltung des Rahmenwerks für das operationelle Risikomanagement bestehen.

Wenn der CRO nicht direkt an den CEO berichten kann, kann eine Alternative darin bestehen, dass der CRO an den CFO berichtet, allerdings nur unter der Voraussetzung, dass die Berichtslinie des CRO und der Risikofunktion unabhängig vom Tagesgeschäft des Unternehmens bleibt (z.B. Vertrieb, Produktion, Kundendienst). In einem solchen Fall sollte der CRO bei Konflikten in der Berichtslinie einen direkten Zugang zum CEO und zum Leitungsorgan behalten.

Abschnitt 4.4 – Die Risikomanagement Funktion

In den meisten Unternehmen gibt es eine Risikofunktion, auch wenn diese Funktion nur aus einer Voll- oder Teilzeitkraft besteht. In einem größeren Unternehmen kann eine Risikofunktion aus verschiedenen Abteilungen für bestimmte Risikoarten bestehen, einschließlich des operationellen Risikos. In kleineren Unternehmen können ein oder zwei Personen mehrere Risikoarten abdecken.

Die Hauptaufgabe der Risikofunktion besteht in den meisten Unternehmen darin, ein angemessenes Rahmenwerk für das Risikomanagement zu gestalten, das auch das Rahmenwerk für das Management operationeller Risiken umfasst. Abhängig von der Art der Governance-Regelungen des Unternehmens kann die Risikofunktion auch die Umsetzung dieser Rahmenwerke unterstützen und/oder überwachen (siehe Abschnitt 3.3).

Die Risikofunktion muss über ausreichende Befugnisse verfügen, um eine wirksame Governance des operationellen Risikos zu unterstützen. Aus OpRisk-Sicht sollte dies Folgendes beinhalten:

- Zugang zum Leitungsorgan in Bezug auf Angelegenheiten, die die Gestaltung des Frameworks für das Management operationeller Risiken betreffen sowie die Meldung/ Eskalation signifikanter operationeller Risiken oder Kontrollmängel, die das Erreichen der Unternehmensziele gefährden
- Zusammenarbeit mit der Internen Revision, um sicherzustellen, dass Kontrollschwächen, einschließlich der Nichteinhaltung von Richtlinien und Verfahren für operationelle Risiken, identifiziert und behoben werden
- Zusammenarbeit mit den Compliance-Kollegen, um sicherzustellen, dass Regeln und Richtlinien in Bezug auf das Management operationeller Risiken eingehalten werden

Wie im Fall des CRO muss die Risikofunktion eine unabhängige Berichtslinie seitens der Manager haben, die für die Umsetzung des Rahmenwerks für das Management operationeller Risiken verantwortlich sind. Damit sollen Interessenkonflikte zwischen den Verantwortlichkeiten der Risikoeigner und der Risikomanagementfunktion vermieden werden.

Abschnitt 4.5 – Die Funktion Operationelles Risiko

Nicht alle Unternehmen verfügen über eine eigenständige Funktion für das operationelle Risiko, d. h. eine unabhängige/standalone Funktion für das operationelle Risiko. Kleinere Unternehmen können zum Beispiel eine Risikofunktion haben, die alle Risikobereiche abdeckt. Wo eine Funktion für operationelle Risiken vorhanden ist, sollte sie eine zentrale Rolle bei der OpRisk Governance einnehmen.

Die Funktion für das operationelle Risiko sollte die Hauptverantwortung für die Gestaltung des OpRisk-Rahmenwerks und für die Unterstützung seiner Umsetzung durch die Risikoeigner tragen. Die OpRisk-Funktion kann auch die Arbeit der Internen Revision zur Sicherstellung des operationellen Risikos unterstützen.

Zu den spezifischen Governance-bezogenen Aktivitäten, die von der Funktion für operationelle Risiken durchgeführt werden, können gehören:

- Unterstützung der Arbeit des Leitungsorgans und der leitenden Angestellten in Bezug auf das operationelle Risiko (z.B. durch Beratung, Anleitung, Expertenmeinungen)
- Unterstützung der Aktivitäten des Risikokomitees oder eines gleichwertigen Gremiums, Überwachung des operationellen Risikoprofils des Unternehmens und Eskalation von Bedenken hinsichtlich Kontrollschwächen oder Risiken, die den vereinbarten Risikoappetit oder die Toleranzgrenzen überschreiten
- Überwachung der Risikokultur des Unternehmens und falls erforderlich Unterstützung bei der Beeinflussung dieser Kultur
- Zusammenarbeit mit den Risikoeignern, um sicherzustellen, dass die Richtlinien und Verfahren für operationelle Risiken korrekt umgesetzt werden (z.B. durch Schulungen, Coaching)
- Überprüfung und Verbesserung des Rahmenwerks für das Management operationeller Risiken, um sicherzustellen, dass es benutzerfreundlich ist und einen maximalen Mehrwert für das Unternehmen und sein Management bietet

Idealerweise sollte das Management aller Kategorien von operationellen Risiken in die Verantwortung der OpRiks-Funktion fallen. Dadurch wird ein einheitlicher Ansatz für das Management des operationellen Risikos sichergestellt und Lücken oder Überschneidungen werden vermieden.

In einigen Unternehmen können jedoch Bereiche wie Business Continuity, Gesundheit und Sicherheit, Versicherungen oder Sicherheit (Cyber- oder physische Sicherheit) außerhalb der täglichen Verantwortung der OpRisk Funktion liegen. Wo dies der Fall ist, müssen die verschiedenen Funktionen eng zusammenarbeiten. Außerdem wird empfohlen, dass sie eine gemeinsame Berichtslinie haben (z.B. an den Leiter der Risikofunktion des Konzerns oder den CRO).

Wie der CRO und die Risikofunktion muss auch die Funktion für operationelle Risiken in der Lage sein, ihre Unabhängigkeit von den täglichen Entscheidungen des operationellen Risikomanagements zu wahren, die von den Risikoeignern getroffen werden. Dies sollte die Funktion jedoch nicht daran hindern, Ratschläge oder Anleitungen zu geben. Entscheidend ist, getrennte Berichtslinien beizubehalten und sicherzustellen, dass die Richtlinien und Verfahrensweisen deutlich machen, dass die Risikoeigner für alle Entscheidungen zum Management des operationellen Risikos in ihrem Verantwortungsbereich verantwortlich sind.

Zusätzlich zu der konzernweiten Funktion für operationelle Risiken können einige Unternehmen Manager für operationelle Risiken auf Bereichs- oder Abteilungsebene beschäftigen. Solche Funktionen sind nicht unabhängig von den Berichtslinien der Risikoeigner, insbesondere, weil diese Personen an einen Risikoeigner oder ihre direkten Vorgesetzten berichten können.

Die Ernennung von Spezialisten für operationelle Risiken innerhalb der Geschäftsbereiche kann die Umsetzung eines Rahmenwerks für das Management operationeller Risiken erheblich verbessern und wird empfohlen, wenn die Ressourcen dies zulassen. Diese Spezialisten können die zentrale Risiko- oder Operational-Risk-Funktion auch dabei unterstützen, das Design des Operational-Risk-Management-Rahmenwerks zu überprüfen und zu verbessern und die Beziehungen zwischen den Risikoeignern und der Risikofunktion zu verbessern. Es ist jedoch wichtig zu beachten, dass aus der Governance-Perspektive der Einsatz von Spezialisten für operationelle Risiken innerhalb der Geschäftsbereiche kein Ersatz für die Einrichtung einer zentralen (operationellen) Risikomanagementfunktion ist.

Abschnitt 4.6 – Andere Spezialisten-Kontrollfunktionen

Außerhalb des direkten Anwendungsbereichs des operationellen Risikos gibt es eine Reihe von kontrollbezogenen Funktionen, die aus Sicht der Governance des operationellen Risikos relevant sind. Dazu gehören:

- Rechnungswesen und Finanzen
- Vorstands-/Unternehmenssekretariat (sofern relevant)
- Compliance
- Personalwesen
- IT-Dienstleistungen
- Rechtsabteilung

Die (operationelle) Risikofunktion sollte eng mit diesen Funktionen zusammenarbeiten, um die Effektivität der OpRisk Governance zu maximieren. Dies könnte den Austausch von Informationen, die Entwicklung eines gemeinsamen Datenerfassungs- und Berichterstattungssystems, die Bereitstellung von Beiträgen zu den Management-Frameworks der jeweils anderen Funktion sowie regelmäßige Beziehungsmanagement-Meetings beinhalten.

Abschnitt 4.7 – Revision

Externe und interne Prüfer (sofern relevant) spielen eine wichtige Rolle bei der OpRisk Governance.

Die wichtigste Rolle besteht darin, Leitungsorgan und Geschäftsleitung die Wirksamkeit der Regelungen zur Governance des operationellen Risikos Unternehmens zu bestätigen. Dies könnten z.B. Prüfungen sowohl der Gestaltung als auch der Umsetzung des Rahmenwerks für das Management operationeller Risiken sein. Es können auch signifikante Risikopositionen oder Kontrollschwächen aufgezeigt werden. Die (operationelle) Risikofunktion sollte gute Beziehungen zu externen und internen Prüfern pflegen. Dies sollte den gegenseitigen Informationsaustausch beinhalten, idealerweise durch die Nutzung eines gemeinsamen IT-Systems, die Zusammenarbeit zur Sicherstellung der effektiven Übersicht über die Umsetzung des Rahmenwerks für das Management operationeller Risiken und, wenn möglich, die Einholung von Beiträgen der Prüfer zur Gestaltung des Rahmenwerks für das Management operationeller Risiken, um sicherzustellen, dass es ihren Anforderungen entspricht.

Schließlich muss die (operationelle) Risikomanagement-Funktion alle Bedenken, die sie hinsichtlich der Integrität des internen Kontrollumfelds hat, mitteilen. Dazu gehört auch die Weitergabe von Informationen an externe Prüfer über alle operationellen Risikoereignisse, Risikopotenziale oder Kontrollversagen, die die Integrität der Finanzberichterstattung des Unternehmens beeinträchtigen könnten (z.B. Betrugsfälle, disziplinarische Maßnahmen gegen leitende Mitarbeiter in Kontrollfunktionen, Fehler in der Finanzberichterstattung).

Abschnitt 4.8 – OpRisk Richtlinie

Es wird dringend empfohlen, dass Unternehmen entweder eine spezielle Richtlinie für das Management von operationellen Risiken oder eine allgemeine Richtlinie für das Risikomanagement haben, die das Management von operationellen Risiken ausdrücklich einschließt.

Der Vorteil einer Richtlinie für das Management operationeller Risiken aus der Governance-Perspektive ist, dass sie die Erwartungen des Unternehmens an das Management operationeller Risiken, die Rollen und Verantwortlichkeiten und gegebenenfalls Risikoappetit oder -toleranz für operationelle Risiken verdeutlichen. Somit liefert eine solche Politik klare “Spielregeln”, insbesondere für die Risikoeigner, die mit dem täglichen Management des operationellen Risikos beauftragt sind.

Eine Richtlinie für das Management operationeller Risiken sollte in der Regel Folgendes enthalten:

- Den Zweck und den Geltungsbereich der Richtlinie. Insbesondere sollte in diesem Abschnitt erläutert werden, wie Rolle und Ziele des Managements operationeller Risiken die übergeordneten Ziele des Unternehmens unterstützen (bezogen auf die Erzielung von Gewinn, die Sicherstellung von Compliance usw.). Dieser Abschnitt sollte auch die Risikokategorien verdeutlichen, die in den Aufgabenbereich des Managements operationeller Risiken fallen
- Wichtige Begriffe und Definitionen des operationellen Risikos (z.B. die Unterscheidung zwischen inhärentem und Restrisiko oder die Erklärung von Begriffen wie Risikoereignisse, Beinaheschäden usw.). Dies hilft dabei, eine gemeinsame Sprache für das Management operationeller Risiken zu etablieren
- Die Governance-Struktur für das Management operationeller Risiken (z.B. Ausschussstruktur, Risikofunktionsstruktur usw.)
- Rollen und Verantwortlichkeiten (siehe Abschnitt 4.1)
- Die gesamte Gestaltung des Rahmenwerks für das Management operationeller Risiken (weitere Informationen finden Sie im IOR-Leitfaden “Integration eines Operational Risk Managements”). Spezifische Aspekte dieses Rahmenwerks können anschließend in separaten Verfahrensdokumenten erweitert werden
- Risikoappetit oder -toleranz des Unternehmens in Bezug auf operationelle Risiken (siehe IOR-Leitfaden zum Risikoappetit für operationelle Risiken)
- Wie Abweichungen von der Richtlinie genehmigt werden können (z.B. Genehmigung durch den Risikoausschuss)
- Die Häufigkeit, mit der die Richtlinie überprüft wird, und das Gremium, das für ihre Genehmigung verantwortlich ist (idealerweise das Leitungsorgan oder ein vom Vorstand beauftragter Ausschuss)

Abschnitt 4.9 – Leistungsmanagement

Angemessene Leistungsmanagement-Vereinbarungen, die Anreize für die Umsetzung eines effektiven Managements operationeller Risiken schaffen, können die OpRisk Governance verbessern. Es ist jedoch äußerste Vorsicht geboten, um zu gewährleisten, dass diese Vereinbarungen nicht zu unbeabsichtigten Folgen führen, insbesondere, wenn finanzielle Anreize geboten werden. So kann z.B. ein finanzieller Leistungsbonus, der auf dem Wert der gemeldeten operationellen Verluste basiert, dazu führen, dass Verluste verschwiegen oder ihr Wert niedrig geschätzt wird, um die Zahlung des Bonus zu gewährleisten.

Im Allgemeinen ist es besser, Anreize auf Grundlage von Inputs in das Management des operationellen Risikos zu gestalten, als auf der Grundlage von Outputs (z.B. Anzahl und Größe der Verlustereignisse). Zu diesen Inputs könnten gehören:

- Rechtzeitiges und vollständiges Abschließen von Risk Assessments
- Rechtzeitige, korrekte und vollständige Information über Risikoauslastungen und Kontrollschwächen
- Bearbeitung von Feststellungen der Internen Revision innerhalb des vorgegebenen Zeitrahmens
- Vorleben der Unternehmenswerte (soweit sie sich auf das operationelle Risikomanagement beziehen) und Befolgen eines ethischen Verhaltenskodexes

Monetäre Anreize sollten, wenn sie eingesetzt werden, klein gehalten werden. Je höher der Einsatz ist, desto größer ist die Wahrscheinlichkeit, dass die Mitarbeiter versuchen, das System zu manipulieren. Unterschätzen Sie niemals die Macht kleiner, sogar symbolischer Anreize. Dazu könnte für Personen, die gute OpRisk Governance zeigen, eine Auszeichnung als “Mitarbeiter des Monats” oder “Mitarbeiter des Jahres” gehören.

Eine andere Technik besteht darin, das operationelle Risikomanagement in eine allgemeine Leistungsbeurteilung einzubeziehen und keine expliziten Anreize zu setzen. Beispielsweise könnte die (operationelle) Risikofunktion aufgefordert werden, einen Beitrag zu den jährlichen Leistungsbeurteilungen der Risikoeigner zu leisten, um Wege zur Verbesserung ihrer Praxis zu finden (z.B. um Schulungsbedarf zu ermitteln) und um Ziele in Bezug auf die OpRisk Governance festzulegen.

Wenn Leistungsanreize für das Management operationeller Risiken angeboten werden, ist es wichtig, sich mit den Personalverantwortlichen sowie der (operationellen) Risikofunktion über deren Gestaltung abzustimmen. Dies sollte dazu beitragen, ihre Effektivität zu maximieren und das Risiko der Manipulation zu reduzieren.

Wollen wir so weit gehen zu sagen, dass dies “besser” ist - der letzte Satz in diesem Abschnitt wirbt für eine ausgewogenere Sichtweise - Anreize müssen sicherstellen, dass übergeordnete Ziele erreicht werden.

Abschnitt 4.10 – Berichtswesen

Effektive Governance ist ohne Informationen nicht möglich. Aus Sicht des operationellen Risikos sind dafür Informationen über das operationelle Risikoprofil des Unternehmens, wesentliche Kontrollschwächen und die Nichteinhaltung der Richtlinien und Verfahrensweisen für operationelle Risiken erforderlich.

Für weitere Informationen zur Berichterstattung siehe insbesondere das Leitpapier des IOR zu Risikoindikatoren.

Abschnitt 4.11 – Interne Berichterstattung

Um die effektive Steuerung des operationellen Risikos zu unterstützen, ist es wichtig, dass dem vom Vorstand beauftragten Ausschuss, der für das Management des operationellen Risikos verantwortlich ist, sowie allen unterstützenden Komitees für das Management des operationellen Risikos auf Konzern- und Divisionsebene Berichte über die Risikoposition vorgelegt werden.

Diese Berichte sollten Informationen enthalten über:

- die Risikoposition des Unternehmens bei operationellen Risiken, die das Erreichen der Ziele gefährden können oder den vereinbarten Risikoappetit oder Toleranzgrenzen überschreiten

- Signifikante Kontrollschwächen, Risikoereignisse oder Beinaheschäden
- Unerlaubte Verstöße gegen die Richtlinie für operationelle Risiken oder wesentliche Verstöße gegen Verfahrensweisen

Die Bedeutung von Kontrollschwächen usw. sollte mit den Empfängern der Berichte abgestimmt werden. In der Regel ist eine signifikante Schwachstelle eine Schwachstelle, die eine wesentliche Auswirkung auf Cashflows oder die Bilanz eines Unternehmens haben könnte, seinen Ruf schädigt, gegen Schuldverpflichtungen verstößt oder zu rechtlichen oder behördlichen Sanktionen führt.

Abschnitt 4.12 – Externe Berichterstattung

Eine gute Unternehmensführung erfordert eine zeitnahe, genaue und vollständige Berichterstattung über die Risikopositionen eines Unternehmens an seine externen Stakeholder. Die Stakeholder benötigen diese Informationen, um Entscheidungen bezüglich ihrer Beziehung zum Unternehmen zu treffen (z.B. ob sie investieren oder nicht) und um sich davon zu überzeugen, dass das Unternehmen in ihrem Interesse arbeitet. Der einzige Vorbehalt zu dieser Aussage ist die kommerzielle Sensibilität. Es liegt nicht im Interesse der externen Anteilseigner, Informationen zu veröffentlichen, die konkurrierenden Unternehmen einen kommerziellen Vorteil verschaffen könnten.

Verschiedene externe Stakeholder können Informationen über die operationelle Risikoposition eines Unternehmens verlangen. Dazu gehören:

- Aktionäre
- Gläubiger
- Rating-Agenturen
- Aufsichtsbehörden
- Zulieferer
- Kunden
- Mitarbeiter

Die Art und Sensibilität dieser Informationen wird variieren. Es ist besonders wichtig, die Offenlegung gegenüber Rating-Agenturen und Aufsichtsbehörden so umfassend wie möglich zu gestalten. Lieferanten und insbesondere kommerzielle Kunden können ebenfalls detaillierte Informationen über das operationelle Risiko eines Unternehmens und die Gestaltung des operationellen Risikomanagementsystems verlangen.

Es ist wichtig, dass die (operationelle) Risikofunktion in alle Aspekte der externen Berichterstattung eingebunden ist. Diese Funktion hat das beste Verständnis für das Rahmenwerk und das Risikoprofil des Unternehmens. Wenn die Funktion nicht beteiligt ist (z.B. bei der Erstellung des Jahresberichts und des Jahresabschlusses), besteht die Gefahr, dass ungenaue oder unvollständige Informationen berichtet werden.

Abschnitt 4.13 – Regelmäßige Verbesserung

Ein Unternehmen sollte mindestens einmal jährlich die Wirksamkeit ihrer Governance für operationelle Risiken überprüfen. Dies könnte Folgendes beinhalten:

- eine Überprüfung, Aktualisierung und erneute Genehmigung der Richtlinie für das Management operationeller Risiken, einschließlich einer Bewertung ihrer Wirksamkeit (z.B. Anzahl unzulässiger Verstöße)
- Gegebenenfalls eine Überprüfung, Aktualisierung und erneute Genehmigung des Risikoappetits oder der Toleranzschwelle für operationelle Risiken sowie der zugehörigen Limits
- Konsultation der Risikoeigner und Sicherheitsfunktionen, um sicherzustellen, dass die Governance-Regelungen weiterhin ihren Bedürfnissen entsprechen

Regelmäßige (z.B. alle 2-3 Jahre) Prüfungen der Governance-Regelungen für das operationelle Risiko werden empfohlen. Diese können von der Internen Revision oder spezialisierten Beratern durchgeführt werden.

Der Zweck dieser Prüfungen sollte ein Benchmarking gegenüber anderen Unternehmen sein, um sicherzustellen, dass die Vorkehrungen auf dem neuesten Stand sind.

Abschnitt 5 – Fazit

Eine wirksame Governance für operationelle Risiken, vom Leitungsorgan abwärts, ist für ein gutes Management unerlässlich. Eine wirksame Governance verbessert das Management operationeller Risiken und die Berichterstattung, was zu einer besseren Entscheidungsfindung und zur Optimierung der Leistung eines Unternehmens führt.

Die Architektur der Operational Risk Governance und die in diesem Papier beschriebenen Aktivitäten sollten dem Unternehmen einen direkten Nutzen bringen. Zum Beispiel sollte die ordnungsgemäße Analyse von operationellen Risiken und Risikoereignissen zu weniger Verlusten und Beinaheschäden führen, was wiederum die Kosten senkt und die Effizienz steigert. Dabei sollten Governance-Aktivitäten dazu beitragen, das Management operationeller Risiken in das Gesamtunternehmen zu integrieren und nicht als unnötige “Bürokratie” wahrzunehmen. Gute Governance existiert nie um ihrer selbst willen; sie muss wertschöpfend sein, um effektiv zu sein.

www.theirm.org

irm

Developing risk professionals