Kategorisierung des operationellen Risikos

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

Organisationen sind einer Palette von Risikoarten ausgesetzt. Operationelle Risiken sind eine dieser Risikoarten. Tabelle 1 fasst einige der üblichen Risikotypen, denen Organisationen ausgesetzt sind, zusammen.

Risikoart	Beschreibung
Kredit	Das Risiko, dass ein Schuldner in Zahlungsverzug geraten kann (eine bestehende Forderung wird nicht oder nur teilweise gezahlt) oder dass sein Kreditrating herabgestuft wird.
Liquidität	Die Gefahr, dass eine Organisation anstehenden Zahlungsverpflichtungen nicht mehr uneingeschränkt und fristgerecht nachkommen kann.
Markt	Risiken, die sich aus Veränderungen des Marktwerts bzw. der Einnahmen aus den Vermögensgegenständen einer Organisation ergeben.
Operationell	Die Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge von externen Ereignissen eintreten.
Reputation	Bedrohung der öffentlichen Wahrnehmung einer Organisation und der Wertschätzung der Organisation durch ihre Stakeholder
Strategisch	Risiken, die sich aus der von einer Organisation gewählten Strategie ergeben oder davon beeinflusst werden.

Tabelle 1: Übliche Risikoarten

Während der Schwerpunkt dieses Papiers auf der Kategorisierung von operationellen Risiken liegt, existieren diese in einem größeren organisatorischen Kontext. Insbesondere wird es Zeiten geben, in denen sich Risikolage und Ereignisse mit diesen Risikotypen überschneiden oder in denen ein Ereignis in einem Risikotyp Risiken in einem anderen verursacht. Z.B. könnte das Auftreten eines operationellen Risikos ein strategisches Risiko auslösen, und die Kombination könnte wiederum zu einer Beeinträchtigung der Reputation führen. In Anbetracht dessen darf eine Kategorisierung von operationellen Risiken nicht darauf abzielen, Risiken abzusondern oder zu isolieren, sondern sollte innerhalb eines ganzheitlichen Rahmens für die Kategorisierung aller Risiken erfolgen, denen eine Organisation ausgesetzt ist (z. B. ein Enterprise-Risk-Management-Rahmen).

Abschnitt 2 – Die Logik hinter der Kategorisierung operationeller Risiken

Operationelle Risiken ergeben sich aus dem Tagesgeschäft von Organisationen. Diese Abläufe umfassen viele Aktivitäten und Prozesse und erfordern Menschen, Systeme und Ausrüstung, um sie effizient und kostengünstig durchzuführen. In Anbetracht der Breite der organisatorischen Aktivitäten und der verschiedenen Prozesse, Menschen, Systeme und Geräte, die zu ihrer Erfüllung erforderlich sind, ist das potenzielle Spektrum an operationellen Risiken und Ereignissen vielschichtig. Es reicht von z.B. IT-Sicherheitsverletzungen, arbeitsrechtlichen Streitigkeiten, Betrug und Kundenbeschwerden bis hin zu Bränden, Überschwemmungen und anderen Auswirkungen sogenannter “höhere Gewalt”.

In Anbetracht des breiten Spektrums an operationellen Risiken und Ereignissen kann eine Kategorisierung dabei helfen, die Identifizierung, Bewertung, Überwachung und Kontrolle bestimmter Arten von Risiken sowie die Arten von möglichen Verlusten zu organisieren. Unterschiedliche Risikokategorien können spezifische Risikobewertungstechniken und Kontrollansätze erforderlich machen. So können einige Risikokategorien versicherbar sein (Haftpflichtansprüche und Sachschäden) und andere nicht (behördliche Bußgelder). Die spezifischen Vorteile sind Folgende:

- Identifizierung: Eine Kategorisierung der operationellen Risiken bietet ein “Menü” potenzieller Risiken, das als Anhaltspunkt für die Bestimmung derjenigen Risiken verwendet werden kann, die für eine Organisation oder ihre spezifischen Abteilungen und Funktionen relevant sind. Dies sollte verhindern, dass Risiken übersehen werden
- Messung: Die Verwendung einheitlicher Begriffe und Beschreibungen erleichtert Vergleiche zwischen operationellen Risiken und unterstützt die Datenaggregation (insbesondere, wenn Risiken in Unterkategorien eingeteilt sind, siehe unten)
- Überwachung und Berichterstattung: Ein gemeinsamer Bezugsrahmen ermöglicht eine aussagekräftigere Analyse und Übersicht über die Ergebnisse, die durch ein Rahmenwerk für das Management operationeller Risiken erzeugt werden. Beispielsweise sollte das Management besser in der Lage sein, Ressourcen für die wichtigsten operationellen Risiken zu priorisieren, die Risikolage in verschiedenen Abteilungen und Funktionen zu vergleichen und detailliertere Ziele, Limits und Schwellenwerte festzulegen
- Kontrolle: Angesichts des Umfangs der operationellen Risiken können verschiedene Kategorien sehr unterschiedliche Kontrollmaßnahmen erfordern. Durch die Kategorisierung dieser Risiken können daher maßgeschneiderte Kontrollstrategien entwickelt werden

Schließlich grenzt die Kategorisierung von operationellen Risiken diese von anderen Risikoarten (Markt, Kredit, etc.) ab. Wenn eine Organisation mehrere Risiken und andere damit verbundene Kontrollfunktionen besitzt, hilft dies, das Potenzial für Lücken und Überschneidungen zu minimieren, auch wenn diese selten beseitigt werden können - insbesondere Überschneidungen. Abgrenzungsprobleme zwischen operationellen Risikokategorien und anderen Risikoarten kommen vor und werden im Folgenden diskutiert.

Abschnitt 3 – Wesentliche Prinzipien bei der Kategorisierung operationeller Risiken

Es ist wichtig, das Potenzial für Lücken und Überschneidungen in jeder Kategorisierung von operationellen Risiken zu minimieren. Das Vermeiden von Lücken ist besonders wichtig, da diese dazu führen können, dass wichtige Risiken ignoriert werden.

Abschnitt 3.1 – Risikokategorisierungen sollten auf etablierten externen Rahmenwerken basieren

Verschiedene Organisationen stellen Beispiele für Risikokategorisierungen zur Verfügung. Die gängigste für das operationelle Risiko wird vom Basler Ausschuss für Bankenregulierung bereitgestellt. Obwohl dieser sich auf Banken konzentriert, stellt er einen guten Ausgangspunkt für jede Kategorisierung des operationellen Risikos dar. Dieses externe Rahmenwerk wird in Anhang A zusammen mit einem anderen, dem “Orange Book” des britischen Finanzministeriums, beschrieben.

Abschnitt 3.2 – Risikokategorisierungen sollten individuell zugeschnitten sein

Obwohl ein etabliertes externes Rahmenwerk einen nützlichen Ausgangspunkt für jede Kategorisierung darstellt, müssen Organisationen dieses möglicherweise an die Art, den Umfang und die Komplexität ihrer Geschäftstätigkeiten anpassen. Wenn Organisationen von einem externen Rahmenwerk abweichen, wird empfohlen, eine Zuordnung vorzunehmen, um sicherzustellen, dass alle relevanten Kategorien enthalten sind. Es kann auch sein, dass eine Organisation verpflichtet ist, ein externes Rahmenwerk (z. B. das Baseler Rahmenwerk) für die aufsichtsrechtliche Berichterstattung zu verwenden. Hierbei darf keine Kategorie ausgelassen werden.

Abschnitt 3.3 – Konsultation ist unerlässlich

Die Direktoren, Manager und Mitarbeiter einer Organisation müssen alle mit den Kategorisierungen einverstanden sein. Insbesondere müssen sie die verwendeten Begriffe und Beschreibungen verstehen. Die Kategorisierung muss nutzerfreundlich sein und ihre Arbeit unterstützen.

Es wird empfohlen, dass die (operationelle) Risikofunktion einen ersten Entwurf einer Kategorisierung entwickelt und dabei eines der etablierten externen Rahmenwerke als Grundlage verwendet. Anschließend sollten alle, die die Kategorisierung nutzen werden (Risikoverantwortliche, ein Leitungsgremium, die Interne Revision, Compliance etc.), um Anmerkungen gebeten werden, um sicherzustellen, dass sie die verwendeten Begriffe und Beschreibungen verstehen. Sie könnten auch aufgefordert werden, ausgelassene Kategorien vorzuschlagen, die für die Organisation relevant sein könnten, aber nicht von einem externen Rahmenwerk erfasst werden. In diesem Fall sollte jedoch darauf geachtet werden, dass die zusätzlichen Kategorien nicht einfach nur eine Umformulierung einer bestehenden Kategorie sind bzw. ob sie einer der Kategorien des externen Rahmens zugeordnet werden können, der als Grundlage für die Kategorisierung verwendet wurde.

Abschnitt 3.4 – Regelmäßige Überprüfung

Die Geschäfte einer Organisation und die damit verbundenen operationellen Risiken werden sich regelmäßig ändern. Es kann auch sein, dass durch die Anwendung der Kategorisierung Lücken und Überschneidungen festgestellt werden, die in der ursprünglichen Entwurfsphase nicht berücksichtigt wurden. Ebenso können neue Arten von Risiken auftauchen, wie dies beim Cyber-Risiko der Fall war. Um sicherzustellen, dass ein Kategorisierungsrahmen gültig bleibt, ist

daher eine regelmäßige Überprüfung erforderlich. In der Regel sollte diese auf jährlicher Basis durchgeführt werden.

Bei der Änderung einer bereits bestehenden Kategorisierung ist Vorsicht geboten. Änderungen an der Kategorisierung können die Verfolgung von Trends erschweren oder die Aggregation historischer Daten beeinträchtigen. Wenn eine Änderung an einer bereits bestehenden Kategorie vorgenommen wird, sollte diese auf die vorherige Kategorisierung zurückverfolgt werden, damit die Daten z. B. in nachfolgende Risikobewertungen übertragen werden können. Dies ist besonders wichtig, wenn statistische Werkzeuge und Modelle zur Unterstützung der Risikobewertung verwendet werden.

Das Hinzufügen neuer Kategorien ist einfacher, aber es ist wichtig, genau zu überprüfen, ob eine “neue” Kategorie nicht einfach die Neuinterpretation einer bereits vorhandenen ist. Das Hinzufügen mehrerer neuer Kategorien kann die Kategorisierung auch unnötig komplex machen, insbesondere, wenn sie das Potenzial für Überschneidungen und Fehlklassifikationen erhöhen.

Abschnitt 4 – Entwurf eines Frameworks zur Kategorisierung operationeller Risiken

Wie oben erläutert, erfordert die Gestaltung eines Rahmenwerks zur Kategorisierung des operationellen Risikos große Sorgfalt. Fehler in der Entwurfsphase können dazu führen, dass das Rahmenwerk ineffizient und zeitaufwändig in der Anwendung ist. Schlimmer noch, sie können dazu führen, dass wichtige operationelle Risiken übersehen werden.

Abschnitt 4.1 – Die Grundlage der Kategorisierung: Ursache, Ereignis oder Auswirkung?

Wie jede Art von Risiko sind auch operationelle Risiken vielschichtig. Das bedeutet, dass sie eine Kombination aus Ursachen, Ereignissen und Auswirkungen sind. Abbildung 1 veranschaulicht die Beziehung zwischen ihnen.

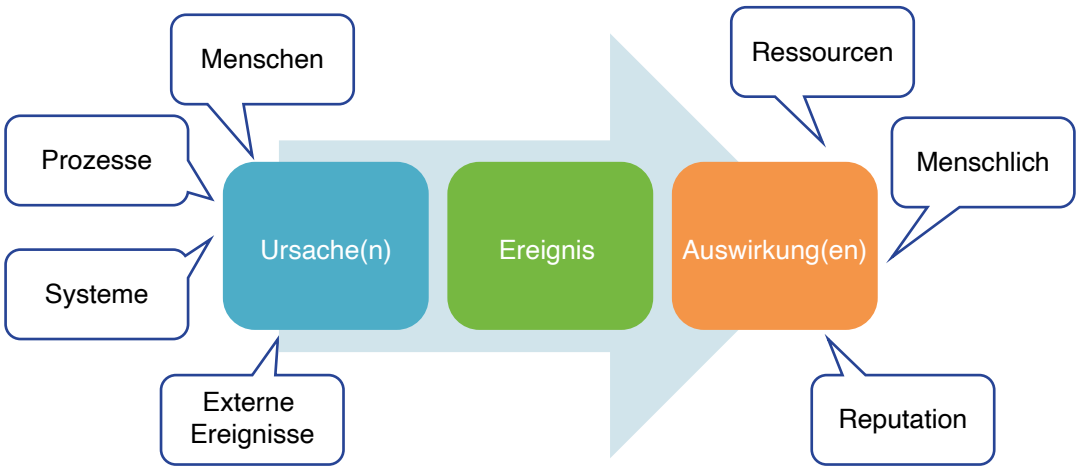

Abbildung 1: Ursache, Ereignis, Auswirkung

Die gängige Definition des operationellen Risikos in Tabelle 1 grenzt das operationelle Risiko nach seinen Ursachen ab: Menschen, Prozesse und Systeme sowie externe Ereignisse. Diese Ursachen können zu einer Vielzahl von operationellen Risikoereignissen führen (Brände, Überschwemmungen, Diebstahl, Fehler und Versäumnisse usw.). Diese Ereignisse wiederum haben vielfältige Auswirkungen (finanzielle Verluste, körperliche Verletzungen usw.). Eine Kategorisierung kann auf jeder dieser drei Facetten des operationellen Risikos basieren.

Am gebräuchlichsten sind Kategorisierungen, die auf operationellen Risikoereignissen basieren. Die Baseler Kategorisierung in Anhang A ist ereignisbasiert, so dass Banken häufig verpflichtet sind, ihre operationellen Verluste unter Verwendung dieser Kategorisierung zu melden, und sich daher entschließen, diese Kategorisierung auch an anderer Stelle zu verwenden, um Konsistenz zu gewährleisten. Außerdem werden Verlustdaten auf einer ereignisbezogenen Basis gesammelt. Einer der Vorteile eines ereignisbasierten Ansatzes ist, dass er eine weitere Unterteilung der Ereignisse in ihre einzelnen Ursachen und Auswirkungen nicht ausschließt. Dadurch kann sich eine Organisation ein besseres Bild von den Beziehungen zwischen Ursachen, Ereignissen und Auswirkungen machen und mögliche Korrelationen oder Risikokonzentrationen hervorheben.

Der Nachteil eines ereignisbasierten Ansatzes ist jedoch, dass der zugehörige Kategorisierungsrahmen sehr detailliert werden kann in dem Versuch, die Gesamtheit der Ereignisse, die auftreten können, wiederzugeben. Dies erfordert eine sorgfältige Betrachtung der Frage der Granularität (siehe Abschnitt 4.3, unten).

Ursachenbasierte Kategorisierungen haben eine intuitive Anziehungskraft, da sie den Ausgangspunkt für die einzelnen operationellen Risikopositionen darstellen und somit helfen können, das operationelle Risikomanagement vorausschauender und proaktiver zu gestalten. Allerdings lassen sich wirksame Klassifizierungen in der Praxis nur schwer umsetzen. Obwohl die Anzahl der allgemeinen Ursachenkategorien klein ist, sind die jeweiligen spezifischen Ursachen zahlreich, oft zahlreicher als die potenziellen Ereignisse.

Das Fehlen etablierter externer Rahmenwerke für die Kategorisierung von operationellen Risiken nach ihren Ursachen macht diese ebenfalls herausfordernder. Die gleichen Argumente gelten für wirkungsbasierte Kategorisierungen (zahlreiche Unterwirkungen, insbesondere nicht-finanzielle Auswirkungen, und kein externes Rahmenwerk).

Das IOR ist der Ansicht, dass operationelle Risiken am besten ereignisbasiert kategorisiert werden. Wo es jedoch möglich ist, sollten grobe Sub-Kategorisierungen für ihre Ursachen und Auswirkungen zur Ergänzung der ereignisbasierten Kategorisierung verwendet werden. Dies ermöglicht es einer Organisation, Ursachen, Ereignisse und Auswirkungen besser zu verknüpfen und potenziell gefährliche Muster in diesen Ursachen und Auswirkungen zu identifizieren und abzuschwächen.

Abschnitt 4.2 – Lücken und Überschneidungen minimieren

Keine Kategorisierung des operationellen Risikos ist perfekt. Kompromisse sind immer erforderlich. Eine sehr detaillierte Kategorisierung kann vielleicht die meisten Lücken beseitigen, führt aber zu häufigen Überschneidungen und Klassifizierungsproblemen. Fehlklassifizierung ist ein ebenso ernstes Problem wie mögliche Lücken oder Überschneidungen. Im Gegensatz dazu sollte eine weniger detaillierte Klassifizierung die Einstufung von Risiken erleichtern, könnte aber zur Folge haben, dass wichtige Risiken übersehen werden.

Der beste Ansatz ist die Entwicklung von Klassifizierungsebenen. Die oberste Klassifizierungsebene wird relativ breit gehalten, wobei weitere Ebenen hinzugefügt werden, um weitere Details zu liefern (siehe 4.3 unten). Die Vorteile eines solchen Ansatzes liegen darin, dass alle operationellen Risikoereignisse klassifizierbar sein sollten, während die Detailebenen den Benutzern helfen, die Ereignisse zuzuordnen und so Überschneidungen und Lücken zu vermeiden. Weitere Informationen zum Umgang mit Abgrenzungsproblemen finden sich in Abschnitt 5.3.

Abschnitt 4.3 – Granularität

Die Festlegung des Detaillierungsgrads einer Kategorisierung des operationellen Risikos ist eine wesentliche Entscheidung.

Eine geringere Granularität erleichtert die Verwaltung der Kategorisierung und die Aggregation von Daten für Bewertungs- und Berichtszwecke, während eine höhere Detailtiefe zur Fokussierung des Managements beiträgt und Risikominderungsmaßnahmen unterstützt. Einige Organisationen wählen eine Kompromisslösung, die eine höhere Granularität für kritische Kategorien beinhaltet, aber weniger Details für Kategorien mit geringerer Bedeutung akzeptiert (in Bezug auf Anzahl und/oder Höhe). Dies vermeidet die Falle, dass zu wenige Risiken auf zu viele Kategorien verteilt sind, was eine Aggregation unmöglich macht.

Es sind verschiedene Ebenen der Granularität möglich. Tabelle 2 fasst die gebräuchlichsten zusammen.

Ebene	Erklärung
1	Eine kleine Anzahl von Kennzeichnungen auf hoher Ebene, die z. B. gemeinsame Kategorien von Ereignissen, die generischen Systeme und Prozesse einer Organisation, regulatorisch relevante Bereiche oder die Ziele der Organisation widerspiegeln. Zum Beispiel: Höhere Gewalt (Brände usw.), Geschäftskontinuität, IT-Systeme, rechtliche und regulatorische Aspekte, Finanzkriminalität usw.
2	Die Kategorien der Stufe 1 teilen sich in ihre logischen Bestandteile auf, abhängig von den spezifischen Erscheinungsformen dieser Ereignisse. Zum Beispiel könnte höhere Gewalt in Brände, Überschwemmungen, Stürme usw. aufgeteilt werden, Finanzkriminalität in internen und externen Betrug oder IT-Systeme in Hackerangriffe und Geräteausfälle
3	Kategorien der Ebene 2 sind weiter unterteilt, um die betrieblichen Aktivitäten widerzuspiegeln, die innerhalb der Geschäftsbereiche, Abteilungen oder Funktionen einer Organisation auftreten können
4	Eine detaillierte Beschreibung der operationellen Risikoereignisse der Stufen 2 oder 3 (sofern vorhanden), die in einem bestimmten Kontext (z. B. Lohnbuchhaltung, Fertigung, Vertrieb usw.) auftreten können

Tabelle 2: Granularitätsebenen bei der Kategorisierung operationeller Risken

Die in Anhang A dargestellte Baseler Klassifizierung von operationellen Verlustereignissen veranschaulicht die ersten drei Stufen der Tabelle 2.

Der Vorteil der Stufen 2 und 3 ist, dass sie zusätzliche Details hinzufügen. Dieser Detailgrad kann den Anwendern helfen, sicherzustellen, dass die Risiken konsistent kategorisiert werden. Außerdem kann es die Gefahr verringern, dass Risiken übersehen werden, weil Anwender einen bestimmten Aspekt eines Risikoereignisses nicht berücksichtigt haben (z. B. sowohl interne als auch externe Hackerangriffe).

Nicht alle Organisationen werden sich für die Stufen 2 oder 3 in Tabelle 2 entscheiden. Die meisten werden jedoch die Stufe 4 haben. Dies soll es bestimmten Abteilungen, Funktionen usw. ermöglichen, die Kategorisierung an ihre spezifischen Bedürfnisse anzupassen, während gleichzeitig sichergestellt wird, dass alle Risiken auf eine Kategorie der Stufe 1 zurückgeführt werden können.

Abschnitt 4.4 – Weitere Gestaltungsüberlegungen

Im Laufe der Erstellung von Kategorisierungen des operationellen Risikos haben Praktiker eine Reihe weiterer zu berücksichtigender Faktoren entdeckt. Diese sind im Folgenden zusammengefasst.

- Das Design der Kategorisierung muss angemessen und verhältnismäßig sein. Ein granularer/detaillierterer Ansatz ist nicht unbedingt besser und kann zu Verwirrung führen, was den Zeit- und Ressourcenaufwand für das Management operationeller Risiken erhöht. Für viele Organisationen bedeutet dies, dass eine Granularität der Stufe 1 ausreichend sein sollte, höchstens Stufe 2
- Konsistenz in der Anwendung ist der Schlüssel - das bedeutet, dass klare und unmissverständliche Erklärungen für jede Risikokategorie sichergestellt werden müssen. Nicht-technische Sprache (z.B. sogenanntes “plain English”) wird empfohlen, da dies die Möglichkeit von Missverständnissen reduziert

- Sicherstellen der Relevanz für alle Teile der Organisation. Das Rahmenwerk muss für die Anwender sinnvoll und in einer Weise strukturiert sein, die mit ihren Aktivitäten und Zielen übereinstimmt
- Es ist ratsam, eine Kategorie “Sonstiges” zu vermeiden. Solche Kategorien können mit Risiken überfrachtet werden, die anderswo kategorisiert werden könnten. Wenn eine spezifische neue Risikokategorie tatsächlich auftaucht, sollte sie dem Rahmenwerk hinzugefügt werden.

Abschnitt 5 - Implementierung

Dieser Abschnitt beschreibt die Faktoren, die bei der Implementierung einer Kategorisierung des operationellen Risikos berücksichtigt werden sollten, sowie einige häufige Herausforderungen und wie diese Herausforderungen gemeistert werden können.

Abschnitt 5.1 – Rollen und Verantwortlichkeiten

Eine Klassifizierung operationeller Risiken wird viele Aktivitäten des operationellen Risikomanagements in allen Abteilungen und Funktionen einer Organisation beeinflussen. In Tabelle 3 sind die Hauptnutzer der Klassifizierung und ihre Verantwortlichkeiten aufgeführt.

Rolle	Verantwortlichkeiten
Leitungsorgan und leitende Angestellte	Das Leitungsorgan, unterstützt von der Geschäftsleitung, ist dafür verantwortlich, dass ein solides System für das operative Risikomanagement vorhanden ist. Dazu gehört auch, dass es ein angemessenes Rahmenwerk zur Risikokategorisierung gibt und dass das Rahmenwerk wie vorgesehen wirksam ist.
Risikoeigner und andere Mitarbeiter mit Verantwortung für das operationelle Risikomanage-ment	Risikoeigner sind Geschäftsmanager, welche die Verantwortung für das Management einiger oder aller operationellen Risiken in ihrem Bereich tragen. Die Risikoeigner sollten sicherstellen, dass sie und ihre Mitarbeiter das Kategorisierungssystem für operationelle Risiken verstehen und dass es richtig verwendet wird, um die Risikoidentifizierung, das Berichtswesen usw. zu unterstützen. Alle anderen Mitarbeiter mit Verantwortung für das Management operationeller Risiken müssen ebenfalls sicherstellen, dass sie das Kategorisierungsrahmenwerk verstehen und es korrekt anwenden.
Risikofunktion	Die Risikofunktion bzw. sofern vorhanden die Funktion für das operationelle Risiko, ist für die Gestaltung des Kategorisierungsrahmenwerks für das Management operationeller Risiken verantwortlich und muss sicherstellen, dass dieses in der gesamten Organisation einheitlich verwendet wird. Um die Umsetzung des Rahmenwerks zu unterstützen, sollte die (operationelle) Risikofunktion sicherstellen, dass es dokumentiert ist und dass eine klare Beschreibung für jede Kategorie vorliegt. Auch die Mechanismen für den Umgang mit etwaigen Abgrenzungsfragen (siehe unten) sollten erläutert werden. Diese Dokumentation könnte durch Schulungs- und Sensibilisierungsmaßnahmen unterstützt werden, um sicherzustellen, dass alle relevanten Mitarbeiter das Rahmenwerk verstehen und effektiv nutzen können.
Interne Revision	Die Innenrevision ist dafür verantwortlich, dem Leitungsorgan und der Geschäftsleitung zu versichern, dass das Rahmenwerk zur Einstufung des operationellen Risikos zweckmäßig ist und wie beabsichtigt wirksam ist. Die Innenrevision kann sich auch dafür entscheiden, die Klassifizierung des operationellen Risikos zur Unterstützung der Prüfungsplanung und zur Strukturierung der Managementmaßnahmen in den Prüfungsberichten zu verwenden, indem sie jede Maßnahme mit einer oder mehreren Kategorien des operationellen Risikos verknüpft. Dieser Ansatz wird empfohlen, da er dazu beitragen kann, den Kategorisierungsansatz einzubetten und einen konsistenten Ansatz für operationelle Risiken zu gewährleisten.

Abschnitt 5.2 – Sicherstellung der konsistenten Verwendung

Die Konsistenz bei der Anwendung ist entscheidend. Wenn verschiedene Manager oder Teile der Organisation ähnliche Risiken unterschiedlich klassifizieren, ist es unmöglich, einen genauen organisationsweiten Überblick über die betrieblichen Risiken zu erhalten.

Eine zentrale Herausforderung für die Konsistenz ist, dass sich Kategorien selten gegenseitig ausschließen. Das bedeutet, dass die Benutzer eines Kategorisierungsrahmens für operationelle Risiken manchmal feststellen werden, dass ein Risiko potenziell in zwei oder mehr Kategorien eingeordnet werden könnte. Beispielsweise könnte ein Betrug, der von einem ehemaligen Mitarbeiter begangen wurde, entweder als interner oder als externer Betrug eingestuft werden.

Eine ähnliche Herausforderung besteht darin, dass Risikoereignisse miteinander verbunden sein können, wobei das Auftreten eines Ereignisses das Auftreten eines anderen verursachen kann. So kann beispielsweise ein externer Hackerangriff sowohl einen Systemausfall als auch einen Datendiebstahl nach sich ziehen. Wie sollte ein solches Ereignis kategorisiert werden? Als externer Betrug oder Cyberangriff (die zugrundeliegende Ursache) oder als Systemausfall oder Datendiebstahl als Risikoereignis? Es gibt keine einzig richtige Lösung dafür. Aber es ist wichtig, sich innerhalb einer Organisation auf eine einheitliche Vorgehensweise zu einigen. Als allgemeine Regel empfiehlt das IOR Folgendes:

- Operationelle Risikoereignisse sollten entsprechend dem zugrundeliegenden oder ursprünglichen Ereignis kategorisiert werden. Im Fall des obigen Beispiels eines Hackerangriffs bedeutet dies, dass das Ereignis als externer Hackerangriff (Cyberangriff) und nicht als Systemausfall oder Datendiebstahl klassifiziert wird. Das Potenzial eines solchen Ereignisses, die Systemkontinuität und -sicherheit zu beeinträchtigen, sollte jedoch beachtet und in jeder Managementreaktion berücksichtigt werden.
- Es sollten Verfahren dokumentiert werden, wie etwaige Klassifizierungsschwierigkeiten gelöst werden können. In der Regel sollten sich Manager bei Zweifeln über die Klassifizierung eines operationellen Risikos mit der Angelegenheit an die (operationelle) Risikofunktion wenden, damit diese eine Entscheidung trifft.
- Die Verfahren sollten durch Schulungen zur konsistenten Einstufung von operationellen Risiken unterstützt werden. Idealerweise sollten diese Trainings lokale Beispiele von Risiken beinhalten und erklären, wie diese kategorisiert werden sollten.
- Wenn ein IT-System zur Unterstützung des Managements operationeller Risiken eingesetzt wird, sollte das Rahmenwerk zur Risikokategorisierung in dieses System eingebettet sein und Anleitungen zur angemessenen Klassifizierung von Risiken enthalten (z. B. Dropdown-Beschreibungen für jede Risikokategorie).
- Als Teil des regelmäßigen Überprüfungsprozesses der Kategorisierung des operationellen Risikos sollte das Augenmerk auf solche Problemkategorien gerichtet werden, bei denen es für das Management am schwierigsten ist, die Risiken konsistent zuzuordnen. Wenn möglich, sollten diese Kategorien in Absprache mit dem Management angepasst werden, um etwaige Probleme zu beheben.

Abschnitt 5.3 – Berichtswesen

Die Struktur der Berichte zum operationellen Risiko sollte, soweit möglich, die vereinbarte Kategorisierung des operationellen Risikos widerspiegeln. Dies sollte die genaue Aggregation der OpRisk-Daten sicherstellen und dazu beitragen, die Kategorisierung in der gesamten Organisation weiter zu einzubetten.

Die Kategorisierung des operationellen Risikos sollte auch zur Anpassung des Detaillierungsgrads der Berichte verwendet werden. In der Regel wird das Leitungsorgan Berichte verlangen, in denen alle Risikoausprägungen oder Verlustereignisse mit den operationellen Risikokategorien der Stufe 1 (siehe Tabelle 2) einer Organisation zusammengefasst sind. das Die leitenden Angestellten könnnen wesentliche Risiken/ Verlustereignisse in den Kategorien der Stufe 2 benötigen, die Abteilungs-/Funktionsmanager eine Aufgliederung der Risiken in der der Stufe 2 oder 3 (falls verwendet).

Abschnitt 5.4 – Addressierung von Grenzereignissen („boundary event“)

Ein Grenzereignis kann als ein Ereignis definiert werden, das sich in einer Risikoart bemerkbar macht, aber seine Ursachen in einer anderen Risikoart hat, z. B. ein Versicherungsrisiko oder ein Verlust aus einem Kreditrisiko, der durch ein zugrundeliegendes operationelles Risikoereignis (z. B. ein Versagen der Prozessorkontrolle) entstanden ist. So ist z. B. ein Kreditausfall ein Beispiel für ein Kreditrisiko, aber die zugrundeliegende Ursache können Fehler im Due-Diligence-Prozess gewesen sein, die dazu führten, dass ein Kredit an einen Kontrahenten mit schlechter Bonität vergeben wurde.

Der Begriff „Grenzereignis“ wurde in den internationalen Vorgaben zur Bankenregulierung als „bounday event“ eingeführt. In den für Institute in Deutschland maßgeblichen Mindestanforderungen an das Risikomanagement werden „boundary events“ umschrieben als „nicht eindeutig zuordenbare Schadenfälle“ (s. MaRisk, Erläuterungen zu BTR 4 Tz. 1).

Grenzereignisse sind für die meisten Organisationen unvermeidlich. Besonders problematisch können sie in Organisationen sein, die über risikoartenspezifische Risikofunktionen verfügen (z. B. eine Kreditrisikomanagementfunktion und eine operationelle Risikomanagementfunktion). Dies liegt daran, dass es zu Streitigkeiten darüber kommen kann, welcher Funktion das Risiko “gehört”. Es kann auch zu einer Verschwendung von Management-Ressourcen führen, weil es doppelt verwaltet wird. Noch schlimmer ist, dass Risiken übersehen werden können, weil jede Funktion davon ausgeht, dass die andere dafür zuständig ist.

Grenzfälle sind weniger problematisch in Organisationen, die über Mechanismen zur Koordinierung des Managements verschiedener Risikotypen verfügen, wie z. B. ein Enterprise Risk Management Framework oder eine ganzheitliche Risikofunktion, die von einem Chief Risk Officer geleitet wird. Auch interdisziplinäre Schulungen können helfen, bei denen spezialisierte Risikofunktionen etwas über die Arbeit ihrer Kollegen lernen (z. B. Schulungen zum operationellen Risiko für die Kreditrisikofunktion und umgekehrt), ebenso wie die Einrichtung eines disziplinübergreifenden Risikokomitees, das potenzielle Grenzereignisse bespricht und die Verantwortung für deren Management der jeweiligen Risikofunktion zuweist.

Abschnitt 6 - Fazit

Angesichts der großen Vielfalt an operationellen Risiken müssen diese konsistent organisiert werden. Die Kategorisierung ist ein wichtiger Teil dieser Zielsetzung. Sie hilft, die begrenzten Managementressourcen effizient zu verteilen und verhindert, dass Risiken übersehen werden.

In gewissem Sinne ist eine solide Kategorisierung der operationellen Risiken das Skelett, das das gesamte Rahmenwerk für das Management operationeller Risiken stützt. Ein schwacher Ansatz zur Kategorisierung bedeutet ein schwaches Rahmenwerk - für wie effektiv auch immer die anderen Elemente gehalten werden.

Anhang A: Beispiele für die Kategorisierung des operationellen Risikos

Nachfolgend sind zwei externe Kategorisierungen aufgeführt, die eine signifikante Anzahl von operationellen Risikoereignissen beinhalten Es wird empfohlen, eine dieser Kategorisierungen (diejenige, von der man annimmt, dass sie der Art, dem Umfang und der Komplexität der Organisation am ehesten gerecht wird) als Ausgangspunkt für die individuelle Klassifizierung des operationellen Risikos der Organisation zu verwenden.

Obwohl die Baseler Verlustereignistypen für Banken entwickelt wurden, bleiben sie eine nützliche Referenzquelle für Organisationen außerhalb des Finanzsektors, insbesondere für solche im privaten Sektor. Die “Orange Book”-Klassifizierung des britischen Finanzministeriums (aktualisiert im Jahr 2020) ist in erster Linie für Organisationen des öffentlichen Sektors gedacht, ist aber auch für den privaten Sektor relevant - insbesondere für kleinere, weniger komplexe Organisationen.

Die Baseler Klassifizierung ist auf operationelle Risikoereignisse ausgerichtet. Im Gegensatz dazu umfasst die Orange Book-Klassifizierung auch andere Risikoarten. Dennoch fällt eine beträchtliche Anzahl der Orange Book-Risikoarten in den Bereich des operationellen Risikos.

Ereigniskate-gorie (1. Ebene)	Definition	Ereigniskategorie (2. Ebene)	Beispiele (3. Ebene)
Interne betrügerische Handlungen	Verluste aufgrund von Handlungen mit betrügerischer Absicht, Veruntreuung, Umgehung von Vorschriften, Gesetzen oder internen Bestimmungen, an denen mindestens eine interne Partei beteiligt ist; ausgenommen sind Ereignisse, die auf Diskriminierung oder (sozialer und kultureller) Verschiedenheit beruhen	Unbefugte Handlungen Diebstahl und Betrug	• Nicht gemeldete Transaktionen (vorsätzlich) • Unzulässige Transaktionen (mit finanziellem • Schaden) • Falschbezeichnung einer Position (vorsätzlich) • Betrug/Kreditbetrug/Ein-lagen ohne Wert • Diebstahl/Erpressung/ • Unterschlagung/Raub • Veruntreuung von Vermögenswerten • Böswillige Vernichtung von Vermögenswerten • Fälschung • Scheckbetrug • Schmuggel • Kontoübernahme/ Identi-tätstäuschung/usw. • Steuerdelikt/Steuerhinter-ziehung (vorsätzlich) • Bestechung/Schmier-geldzahlung • Insidergeschäft (nicht auf Rechnung des Arbeitgebers)
Externe betrügerische Handlungen	Verluste aufgrund von Handlungen mit betrügerischer Absicht, Veruntreuung oder der Umgehung von Gesetzen durch einen Dritten	Diebstahl und Betrug Systemsicherheit	• Diebstahl / Raub • Fälschung • Scheckbetrug • Schäden durch Hackeraktivitäten • Diebstahl von Informationen (mit finanziellem Schaden)
Beschäftigungs-praxis und Arbeitsplatz-sicherheit	Verluste aufgrund von Handlungen, die gegen Beschäftigungs-, Gesundheits- oder Sicherheits-vorschriften bzw. -abkommen verstoßen; Verluste aufgrund von Zahlungen aus Ansprüchen wegen Körperverletzung; Verluste aufgrund von Diskriminierung bzw. sozialer und kultureller Verschiedenheit	Ereignisse in Verbindung mit Arbeitneh-mern Sicherheit des Arbeitsum-feldes Soziale und kulturelle Verschieden-heit/ Diskriminie-rung	• Ereignisse im Zusammenhang mit Löhnen und • Gehältern, Sozialleistungen, Beendigung des • Arbeitsverhältnisses • Gewerkschaftsakti-vitäten • Allgemeine Haftpflicht (Ausrutschen und Stürzen usw.) • jede Art von Diskriminierung

Kunden, Produkte und Geschäftsge-pflogenheiten	Verluste aufgrund einer unbeabsichtig-ten oder fahrlässigen Nichterfüllung geschäftlicher Verpflichtungen gegenüber bestimmten Kunden (einschl. treuhände-rischer und auf Angemessenheit beruhender Verpflichtungen); Verluste aufgrund der Art oder Struktur eines Produkts	Angemessenheit, Offenlegung und treuhänderische Pflichten	• Verstoß gegen treuhände-rische • Pflichten/Ver-letzung von Richtlinien • Angelegenhei-ten in Bezug auf Angemessen-heit und • Offenlegung („Know your customer“-Regelungen • usw.) • Verletzung von Informations-pflichten gegenüber • Verbrauchern/ Privatkunden • Verletzung von Datenschutzbe-stimmungen • Aggressive Verkaufsprak-tiken • Provisions-schneiderei • Missbrauch vertraulicher Informationen • Haftung des Darlehens-gebers
		Unzulässige Geschäfts- oder Marktpraktiken	• Kartell • Unzulässige Geschäfts-/ Marktpraktiken • Marktmanipulationen • Insidergeschäfte (auf Rechnung des Arbeitgebers) • Nicht genehmigte Geschäfts- • tätigkeit • Geldwäsche
		Produktfehler	• Produktmängel (unbefugt usw.) • Modellfehler
		Kundenauswahl, Kreditbetreuung und Kreditumfang	• Versagen bei der Kundenprüfung gemäß Richtlinien • Überschreitung des Kundengesamt-limits
		Beratungstätig-keiten	• Auseinandersetzungen über Erfolg der Beratung
Sachschäden	Verluste aufgrund von Beschädigungen oder Verlust von Sachvermögen durch Naturkatastrophen oder andere Ereignisse	Katastrophen und andere Ereignisse	• Verluste durch Naturkatastrophen • Personenschäden aufgrund von externen Ereignissen (Terrorismus, Vandalismus)
Geschäftsunter-brechung und Systemausfälle	Verluste aufgrund von Geschäftsunter-brechungen oder Systemausfällen	Systeme	• Hardware • Software • Telekommunikation • Ausfall/Störung der Stromversorgung

Abwicklung, Lieferung und Prozess-management	Verluste aufgrund von Fehlern bei der Geschäftsabwicklung oder im Prozessmanagement; Verluste aus Beziehungen mit Handelspartnern und Lieferanten/ Anbietern	Erfassung, Abwicklung und Betreuung von Transaktionen Überwachung und Meldung Kundenaufnahme und -dokumentation Kundenkonto-führung Geschäftspartner im Handel Lieferanten und Anbieter	• Kommunikations-störungen • Fehler bei der Dateneingabe, -pflege oder -speicherung • Überschreiten eines Termins oder Nichterfüllung • einer Aufgabe • Fehlerhafte Anwendung von Modellen/Systemen • Buchungsfehler/falsche Kontozuordnung • Fehler bei der Durchführung sonstiger Aufgaben • Fehlerhafte Lieferung • Fehlerhafte Verwaltung von Besicherungs-instrumenten • Pflege der Referenzdaten • Nichteinhaltung zwingender Meldepflichten • Ungenauer externer Bericht (Schaden eingetreten) • Freigabe durch Kunden/ Haftungs-ausschluss fehlt • Rechtsdokumente fehlen/ unvollständig • Ungenehmigter Zugriff auf Konten • Fehlerhafte Kundenunterlagen (Schaden • eingetreten) • Fahrlässiger Verlust/Schaden bei Kundenvermögenswerten • Fehlerhafte Erfüllung durch Geschäftspartner • (Nichtkunden) • Verschiedene Unstimmigkeiten mit • Geschäftspartnern (Nichtkunden) • Auslagerungen • Unstimmigkeiten mit Lieferanten

Tabelle 3: Detaillierte Klassifizierung von Verlustereignissen nach Basel II (Quelle Basel II konsolidierte Fassung, Anhang 9, Baseler Ausschuss, Juni 2006)

Klassifizierung Risikoarten	
Strategische Risiken	Risiken, die sich aus der Identifizierung und Verfolgung einer Strategie ergeben, die unzureichend definiert ist, auf fehlerhaften oder ungenauen Daten basiert oder die Umsetzung von Verpflichtungen, Plänen oder Zielen aufgrund eines sich ändernden Makroumfelds (z. B. politische, wirtschaftliche, soziale, technologische, umweltbezogene und gesetzliche Veränderungen) nicht unterstützt.
Governance-Risiken	Risiken, die sich aus unklaren Plänen, Prioritäten, Befugnissen und Verantwortlichkeiten und/oder unwirksamer oder unverhältnismäßiger Übersicht über die Entscheidungsfindung und/oder Leistung ergeben.
Operative Risiken	Risiken, die sich aus unzureichenden, schlecht gestalteten oder ineffektiven/ineffizienten internen Prozessen ergeben, die zu Betrug, Fehlern, beeinträchtigtem Kundenservice (Qualität und/oder Quantität der Dienstleistung), Nichteinhaltung von Vorschriften und/oder schlechtem Preis-Leistungs-Verhältnis führen.
Rechtsrisiken	Risiken, die sich aus einer fehlerhaften Transaktion, der Geltendmachung eines Anspruchs (einschließlich der Abwehr eines Anspruchs oder einer Gegenforderung) oder dem Eintritt eines anderen rechtlichen Ereignisses ergeben, das eine Haftung oder einen anderen Verlust zur Folge hat, oder das Versäumnis, angemessene Maßnahmen zur Erfüllung gesetzlicher oder regulatorischer Anforderungen oder zum Schutz von Vermögenswerten (z. B. geistiges Eigentum) zu ergreifen.
Immobilienrisiken	Risiken, die sich aus Sachmängeln oder schlecht konzipiertem oder ineffektivem/ ineffizientem Sicherheitsmanagement ergeben und zur Nichteinhaltung von Vorschriften und/oder zu Schäden und Leid für Mitarbeiter, Auftragnehmer, Dienstleistungsnutzer oder die Öffentlichkeit führen.
Finanzielle Risiken	Risiken, die sich daraus ergeben, dass die Finanzen nicht in Übereinstimmung mit den Anforderungen und finanziellen Beschränkungen verwaltet werden, was zu schlechten Erträgen aus Investitionen, dem Versagen bei der Verwaltung von Vermögenswerten/ Verbindlichkeiten oder der Erzielung eines guten Preis-Leistungs-Verhältnisses der eingesetzten Ressourcen führt und/oder eine nicht konforme Finanzberichterstattung.
Kommerzielle Risiken	Risiken, die sich aus Schwächen im Management von kommerziellen Partnerschaften, Lieferketten und vertraglichen Anforderungen ergeben und zu schlechter Leistung, Ineffizienz, schlechtem Preis-Leistungs-Verhältnis, Betrug und/oder Nichterfüllung von Geschäftsanforderungen/-zielen führen.
Menschliche Risiken	Risiken, die sich aus ineffektiver Führung und Engagement, suboptimaler Kultur, unangemessenem Verhalten, der Nichtverfügbarkeit ausreichender Kapazitäten und Fähigkeiten, Arbeitskampfmaßnahmen und/oder der Nichteinhaltung relevanter Arbeitsgesetze/HR-Richtlinien ergeben und sich negativ auf die Leistung auswirken.

Technologierisiken	Risiken, die sich daraus ergeben, dass die Technologie die erwarteten Leistungen aufgrund unzureichender oder mangelhafter System-/Prozessentwicklung und Leistung oder unzureichender Ausfallsicherheit nicht erbringt
Informationsrisiken	Risiken, die sich aus dem Versäumnis ergeben, robuste, geeignete und angemessene Daten/Informationen zu erstellen und das volle Potenzial der Daten/Informationen zu nutzen.
Sicherheitsrisiken	Risiken, die sich aus dem Versäumnis ergeben, unbefugten und/oder unangemessenen Zugriff auf das Gebäude und die Informationen zu verhindern, einschließlich Cybersicherheit und Nichteinhaltung der Anforderungen der General Data Protection Regulation.
Projekt-/ Programmrisiken	Risiken, dass Change Programme und -projekte nicht auf die strategischen Prioritäten abgestimmt sind und die Anforderungen und beabsichtigten Vorteile nicht erfolgreich und sicher in Bezug auf Zeit, Kosten und Qualität erfüllen.
Reputationsrisiken	Risiken, die sich aus unerwünschten Ereignissen ergeben, einschließlich ethischer Verstöße, mangelnder Nachhaltigkeit, systemischer oder wiederholter Fehler oder schlechter Qualität oder mangelnder Innovation, die zu einer Schädigung des Rufs und/oder der Zerstörung von Vertrauen und Beziehungen führen.

Tabelle 4: Risikokategorien Orange Book Version 2020

www.theirm.org

irm

Developing risk professionals