Szenarioanalyse, Stresstest und Inverser Stresstest

Praxisleitfaden Operationelles Risiko

Gesponsort von:

DGOR
Deutsche Gesellschaft für Operational Risk Management e.V.

IBM OpenPages® with Watson®

THE INSTITUTE OF OPERATIONAL RISK
An IRM Group Company

Vorwort

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

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

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

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

Die Handlungsempfehlungen des Institute of Operational Risk

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

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

Inhaltsverzeichnis

Abschnitt 1 - Einführung

Die genaue Bewertung des operationellen Risikos ist eine große Herausforderung für Unternehmen. Oft sind historische Daten zu Wahrscheinlichkeit und Auswirkung begrenzt und selbst wenn sie verfügbar sind, gibt es keine Garantie, dass sich historische Trends wiederholen werden.

Besonders problematisch sind “Tail”-Ereignisse mit geringer Wahrscheinlichkeit und hoher Auswirkung, für die oft keine Daten vorhanden sind. Ebenso reduzieren dynamische Unternehmensumfelder, in denen es ein hohes Maß an internen oder externen Veränderungen gibt (z.B. politische, technologische oder soziale Veränderungen), den Wert der Verfolgung historischer Tendenzen weiter.

Die Szenarioanalyse und die damit verbundenen Instrumente des Stresstests und des Inversen Stresstests haben sich als gängige Antworten auf die Probleme begrenzter Daten und unzuverlässiger Trends entwickelt. Werden sie effektiv eingesetzt, können diese Instrumente Unsicherheiten aufklären und Unternehmen helfen, sich auf Ereignisse im Zusammenhang mit operationellen Risiken vorzubereiten und proaktiv darauf zu reagieren. Dies beinhaltet, ist aber nicht beschränkt auf:

- Das Management in die Lage zu versetzen, die Widerstandsfähigkeit des Unternehmens in Bezug auf größere operationelle Risikoereignisse zu testen. Es wird die Möglichkeit geboten, im Voraus zu besprechen, wie darauf zu reagieren ist
- Eine vorausschauende Perspektive zu bieten, indem die Aufmerksamkeit der Manager auf zukünftige operationelle Risikoereignisse gelenkt wird, die sich von denen der Vergangenheit unterscheiden können
- Eine Abwechslung zu den täglichen Risikomanagement-Aktivitäten zu bieten, indem sie den Managern helfen, kreativ über zukünftige operationelle Risikoereignisse nachzudenken und ihr Wissen und ihre Expertise in einer Umgebung mit weniger Zeitdruck zu teilen
- Ergänzung anderer Techniken zur Risikoidentifizierung und -bewertung, wie z.B. die Analyse von Verlustereignissen und das Risiko Self Assessment durch die Einbeziehung der von diesen Techniken erzeugten Daten und die Bereitstellung strukturierter Methoden zum Füllen von Wissenslücken
- Verbesserung der Kontrollumgebung, wenn im Rahmen der Analyse potenzielle Lücken oder Schwachstellen in bestehenden Kontrollen identifiziert werden.

Abschnitt 2 – Abgrenzung von Szenarioanalyse, Stresstest und Inversem Stresstest

Abbildung 1 veranschaulicht die Beziehung zwischen Szenarioanalyse, Stresstest und Inversem Stresstest.

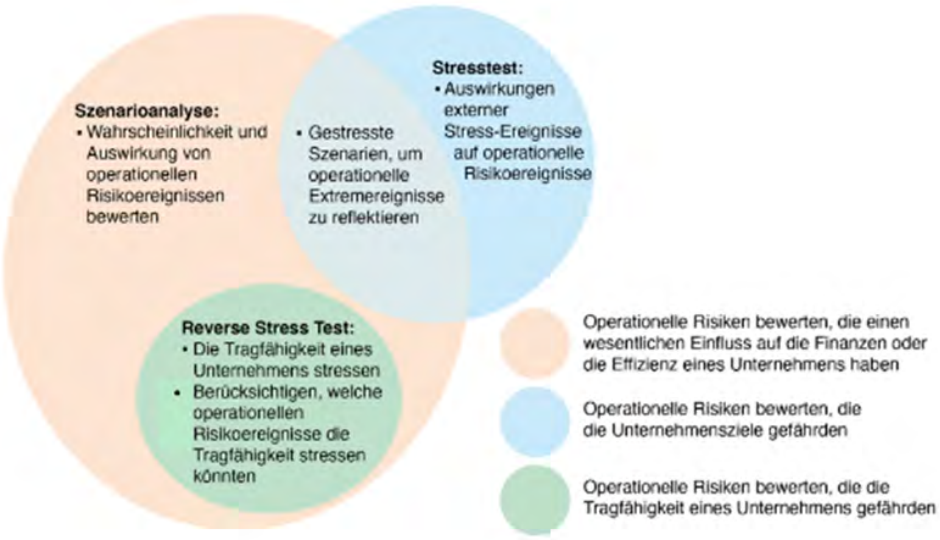

Abbildung 1: Vergleich Szenarioanalyse, Stresstest und Inverser Stresstest

Stresstests beinhalten die Bewertung spezifischer Stressereignisse, die innerhalb des externen Betriebsumfelds eines Unternehmens auftreten könnten und die sich auf eine Reihe von Risikoarten, einschließlich des operationellen Risikos, auswirken können. Beispiele sind eine wirtschaftliche Rezession, eine Pandemie oder politische Ereignisse wie der Brexit. Stressereignisse haben das Potenzial, die Strategie und den Unternehmensbetrieb ernsthaft zu stören, wodurch sie eine hohe Auswirkung haben, auch wenn die Eintrittswahrscheinlichkeit in der Regel gering ist.

Inverse Stresstests beinhalten die Analyse von Ereignissen, die die Lebensfähigkeit eines Unternehmens bedrohen und eine Insolvenz oder einen Konkurs verursachen. Der Ausgangspunkt des Inversen Stresstests ist die Identifizierung des Punktes, an dem die Lebensfähigkeit nicht mehr gegeben ist. Dies geschieht in der Regel durch die Bestimmung des maximalen finanziellen Verlusts, den ein Unternehmen verkraften kann, und die anschließende Betrachtung der Arten von internen Risikoereignissen, die Verluste verursachen können, die diesen Wert übersteigen. Aus Sicht des operationellen Risikos kann dies zum Beispiel ein größerer IT-Ausfall oder Betrug sein.

Die Szenarioanalyse umfasst ein Element des Stresstests und des Inversen Stresstests, kann aber in einem breiteren Spektrum von Anwendungen eingesetzt werden. Bei den Szenarien muss es sich zum Beispiel nicht um extreme Stressereignisse handeln, sondern um Situationen, die eine höhere Eintrittswahrscheinlichkeit haben, bis hin zu Ereignissen, die voraussichtlich einmal oder mehrmals im Jahr auftreten werden. Im Gegensatz dazu werden die Ereignisse, die im Rahmen des Stresstests und insbesondere des Inversen Stresstests betrachtet werden, viel seltener auftreten und eine deutlich höhere Auswirkung haben.

Eine alternative Perspektive zur Abgrenzung von Stress- und Szenariotests ist die der Anzahl der analysierten Variablen.

Aus dieser Perspektive geht es beim Stresstest um die Analyse der Auswirkungen größerer Veränderungen bei einer begrenzten Anzahl von Variablen (in der Regel eine oder zwei), während es bei der Szenarioanalyse um die Analyse von Veränderungen bei einer größeren Anzahl von Variablen geht.

Ein Stresstest könnte zum Beispiel die finanziellen Auswirkungen einer signifikanten Änderung der Zinssätze oder der Inflationsrate analysieren. Im Gegensatz dazu würde die Szenarioanalyse die breiteren Auswirkungen einer wirtschaftlichen Rezession (erhöhte Arbeitslosigkeit, reduzierte Kreditwürdigkeit, etc.) betrachten.

Das IOR ist der Ansicht, dass eine auf Variablen basierende Unterscheidung zwar aus der Perspektive des Rechnungswesens, der Finanzen oder des strategischen Risikos zutreffen mag, nicht aber aus der Perspektive des operationellen Risikos. Dies liegt daran, dass operationelle Risikoereignisse vielschichtig sind und notwendigerweise Änderungen in einer Reihe von Variablen beinhalten. Diese Änderungen können relativ klein oder erheblich ausgeweitet sein. Eine bessere Unterscheidung zwischen Szenarioanalyse und Stresstest ist daher eher in Bezug auf die Schwere der Auswirkungen als in Bezug auf die Anzahl der zu berücksichtigenden Variablen möglich.

Abschnitt 3 – Die Durchführung von effektiver Szenarioanalyse, Stresstest und Inversem Stresstest

Wie die meisten Instrumente zur Risikoidentifizierung und -bewertung sind auch die effektive Szenarioanalyse, das Stresstesting und das Inverse Stresstesting Prozesse, die eine Reihe von Schritten umfassen. Diese sind:

- Identifizieren und Vereinbaren des Analyseschwerpunkts
- Festlegen des Analysegrads
- Vorbereitung auf einen Workshop
- Durchführen eines Workshops
- Validierung der Ergebnisse
- Prozess-Governance

Jedes dieser Unterelemente wird im Folgenden näher erläutert.

Abschnitt 3.1 – Analyseschwerpunkt identifizieren und vereinbaren

Effektive Szenarioanalysen, Stresstests und Inverse Stresstests können viel Zeit und Ressourcen in Anspruch nehmen. Dies bedeutet, dass die potenzielle Anzahl von Themen, die zu einem bestimmten Zeitpunkt analysiert werden können, begrenzt ist. Infolgedessen ist es wichtig, sicherzustellen, dass die ausgewählten Themen die relevantesten sind.

Für Unternehmen, die ihre operationellen Risiken kategorisieren (siehe IOR-Praxisleitfaden zu Kategorisierung operationeller Risiken), besteht ein gängiger Ansatz darin, ein Thema für jedes der operationellen Risiken der Stufen 1 oder 2 auszuwählen, denen das Unternehmen ausgesetzt ist. Dies ist jedoch ein eher willkürlicher Ansatz, insbesondere, wenn einige Kategorien als mehr oder weniger bedeutsam angesehen werden als andere. Letztlich sollte die Anzahl der Themen pro Risikokategorie variieren, abhängig von der Art, dem Umfang und der Komplexität eines Unternehmens sowie der Stabilität seines operationellen Risikoumfelds. Es ist nicht sinnvoll, ein Thema für eine nicht signifikante Risikokategorie auszuwählen. Gleichermaßen können die bedeutendsten Risikokategorien die Analyse mehrerer Themen erfordern.

Bei der Auswahl der Themen, auf die man sich konzentrieren will, wird ein konsultativer Ansatz empfohlen. Die (operationelle) Risikofunktion sollte mit dem breiteren Management des Unternehmens zusammenarbeiten, um die Themen auszuwählen, die als am relevantesten angesehen werden. Dazu gehört auch die Zusammenarbeit mit der Konzernleitung und ggf. dem Management der Geschäftsbereiche. Auch die Zusammenarbeit mit dem Vorstand bei der Analyse der wichtigsten konzernweiten operationellen Risiken ist möglich, insbesondere in Bezug auf Themen für Inverse Stresstests. Aus der Perspektive des operationellen Risikos werden relevante Themen für die Analyse/Tests aus dem externen und internen Unternehmensumfeld stammen. Tabelle 1 fasst einige gängige Quellen zusammen:

Externes Umfeld	Internes Umfeld
Operationelle Risikoereignisse, die kürzlich ähnliche Unternehmen betroffen haben. Darüber hinaus operationelle Risikoereignisse, die als besonders wichtig für das kommende Jahr identifiziert wurden (z.B. von Fachorganisationen, Aufsichtsbehörden oder Institutionen wie dem Weltwirtschaftsforum)	Verlustereignisse und Beinaheschäden, die innerhalb des Unternehmens aufgetreten sind.
Beinaheschäden können bei der Themenauswahl besonders hilfreich sein - so kann das Unternehmen untersuchen, welche Auswirkungen sie gehabt hätten, hätten sie sich als Verluste herauskristallisiert	RSA-Ergebnis, insbesondere die wichtigsten Risiken in Bezug auf Wahrscheinlichkeit und Auswirkung oder Risikoexpositionen, die sich deutlich erhöht haben
Regulatorische oder gesetzgeberische Änderungen, wie z.B. die Risiken im Zusammenhang mit neuen Gesetzen oder Vorschriften (z.B. DSGVO)	Informationen über Kontrollschwächen, einschließlich der Ergebnisse interner Revisionsprüfungen, um zu verstehen, wie Kontrollversagen zu einem Szenario oder Stressereignis beitragen könnte
Gesellschaftliche Veränderungen, wie z.B. Änderungen von Normen und Verhaltensweisen (Einstellungen zum Datenschutz, zur Umwelt usw.)	Trends bei Risiko- oder Kontrollindikatoren, insbesondere solche, die auf einen starken Anstieg der potenziellen Risikoexposition hinweisen
Wirtschaftliche Veränderungen, wie z.B. eine Rezession	Änderungen in der finanziellen oder betrieblichen Leistung des Unternehmens
Technologischer Wandel, wie das “Internet der Dinge” und andere IT-Innovationen	Strategische Veränderungen, wie die Einführung von IT-Systemen, neuen Produkten usw.
Umweltereignisse, wie z.B. Pandemien oder die Auswirkungen des Klimawandels	Operative Änderungen wie Prozessverbesserungen, Änderungen in der Lieferkette, Auslagerung usw.

Tabelle 1: Themen aus dem externen und internen Unternehmensumfeld

Betrachtet man alle oben genannten Quellen, so ist ein Schlüsselfaktor bei der Auswahl der Themen, auf die man sich konzentrieren sollte, das Potenzial für einen signifikanten Anstieg des operationellen Risikos. Wenn Daten zu Risikoereignissen, Bewertungs- und Überwachungsinstrumente oder eine Überprüfung des externen Umfelds ergeben, dass eine signifikante Erhöhung der Wahrscheinlichkeit oder der Auswirkungen bestimmter operationeller Risiken eingetreten ist oder wahrscheinlich eintreten wird, dann sollte dies ein besonderer Aufmerksamkeitsschwerpunkt sein und die betreffenden Risiken sollten in die Themen für die Analyse/Tests eingearbeitet werden.

Ein weiterer Einfluss auf die Fokussierung der Aufmerksamkeit auf die oben genannten Umfeldquellen ist der Grad des Vertrauens, der in die aktuellen Risikobewertungen und die Genauigkeit und Vollständigkeit der Daten zu Schadensfällen und Beinaheschäden gesetzt werden kann. Hat ein Unternehmen beispielsweise kein Vertrauen in die Genauigkeit von RSAs, insbesondere wenn es nicht über ausreichende Daten zu tatsächlichen Ereignissen verfügt und historische Trends instabil erscheinen, sollten diese Einschätzungen durch Szenarioanalysen und Stresstests/ Inverse Stresstests ergänzt werden, um die Lücken zu schließen.

Dazu könnte die Verwendung von Szenarien gehören, um die Beziehungen zwischen den Ursachen eines oder mehrerer Risikoereignisse zu analysieren (Ursachen, die wahrscheinlich aus den in Tabelle 1 identifizierten Quellen stammen), oder Stresstests, die das Ausmaß der Auswirkungen testen (z.B. die Auswirkungen von IT-Ausfällen unterschiedlicher Dauer).

Weitere Faktoren, die den Fokus der Aufmerksamkeit auf die in Tabelle 1 skizzierten Quellen erhöhen können, sind:

- Das Tempo des Wandels: Je schneller sich ein Bereich verändert (z.B. technologische Innovation), desto größer sollte der Fokus sein

- Bedenken hinsichtlich zukünftiger Veränderungen, die zu großen, neu entstehenden Risiken führen könnten

- Das Ausmaß interner strategischer oder operativer Veränderungen; je größer das Ausmaß der Veränderungen, desto größer der Fokus

- Die Fähigkeit eines Unternehmens, potenzielle Quellen von operationellen Risiken zu managen. Ein Unternehmen, das sich um den technologischen Wandel und seine Fähigkeit sorgt, die damit verbundenen Risiken zu managen, könnte beispielsweise das Cyber-Risiko als wichtiges Thema für Szenarioanalysen und Stresstests wählen

Letztlich sind diese Faktoren mit zwei grundlegenden Elementen verknüpft, die die Wahl der Themen für die Analyse/Tests beeinflussen sollten: die Nähe eines Unternehmens zu potenziellen operationellen Risikoszenarien/Stressereignissen und seine Anfälligkeit für diese Szenarien/ Stressereignisse. Je dringlicher oder drängender eine Quelle ist (z.B. eine bevorstehende regulatorische Änderung), desto höher ist die Priorität für ihre Berücksichtigung.

Ebenso gilt: Je weniger sich ein Unternehmen in der Lage fühlt, eine Quelle zu kontrollieren (z.B. schnelle interne Veränderungen), desto höher ist die Priorität für die Berücksichtigung. In einigen Sektoren können die Aufsichtsbehörden bestimmte Szenarien oder Stresstests/ Inverse Stresstests zur Analyse vorschreiben. Dies ist am häufigsten bei Finanzdienstleistungen der Fall, kann aber auch in anderen stark regulierten Sektoren wie dem sozialen Wohnungsbau vorkommen. Es ist zwingend erforderlich, dass Unternehmen ihre regulatorischen Verpflichtungen erfüllen und alle Szenarien oder Stresstests/ Inverse Stresstests analysieren, die von ihren Aufsichtsbehörden vorgegeben werden.

Abschnitt 3.2 – Den Analysegrad bestimmen

Zumindest sollten Szenarioanalysen und Stresstests/ Inverse Stresstests auf der unternehmensweiten (Konzern-) Ebene durchgeführt werden. Darüber hinaus können sich Unternehmen dafür entscheiden, Analysen/Tests auf Geschäftsbereichsebene oder sogar auf Abteilungs- und Funktionsebene durchzuführen, wobei die beiden letztgenannten Varianten (Abteilung und Funktion) weniger üblich sind.

Stresstests und Inverse Stresstests sind auf der unternehmensweiten Ebene besonders wichtig. Dies soll dem Unternehmen (insbesondere dem Vorstand/ der Geschäftsleitung) helfen, seine finanzielle Nachhaltigkeit zu verstehen. Auch wenn ein Unternehmen scheinbar eine starke Bilanz hat, kann es sein, dass künftige operationelle Risikoereignisse (wie z.B. eine Pandemie) diese stark schwächen. Je früher die Geschäftsführung/ das Senior Management diese Ereignisse versteht und sich darauf vorbereiten kann, desto stärker wird das Unternehmen langfristig sein.

Unternehmensweite Analysen/ Tests sollten auf einer Top-Down-Basis festgelegt werden, wobei die (operationelle) Risikofunktion mit dem Senior Management zusammenarbeiten sollte, um sich auf die Themen für die Analyse zu einigen. Analysen und Tests für Geschäftsbereiche oder Abteilungen/Funktionen können auf einer Bottom-up-Basis vereinbart werden. Es wird jedoch empfohlen, dass die Wahl des Themas von der (operationellen) Risikofunktion überprüft und freigegeben wird, um – sofern möglich - maximale Relevanz zu gewährleisten und die Konsistenz der Berichterstattung im gesamten Unternehmen zu erhalten.

Abschnitt 3.3 – Einen Workshop vorbereiten

Szenarioanalysen, Stresstests oder Inverse Stresstests im Kontext des operationellen Risikos lassen sich am besten im Rahmen eines Workshops durchführen. Angesichts der vielschichtigen Natur des operationellen Risikos (mehrere Ursachen, Auswirkungen usw.) wird keine einzelne Person, Abteilung oder Funktion über das Wissen und die Fachkenntnisse verfügen, die zur Durchführung einer effektiven Analyse/ eines effektiven Tests erforderlich sind.

Workshops sind jedoch ressourcenintensiv und es ist wichtig, sie so effizient wie möglich durchzuführen. Das bedeutet, dass im Vorfeld des Workshops Recherchen erforderlich sind, um Zeit für unnötige Details zu sparen und um Missverständnisse oder den Verlust des Fokus auf das zentrale Thema für die Analyse/ den Test zu vermeiden. Tabelle 2 fasst die wichtigsten Aufgaben vor dem Workshop zusammen:

Aufgabe	Beschreibung
Thema und Ziel vereinbaren	Idealerweise sollte sich jeder Workshop nur auf ein Thema konzentrieren. So wird Verwirrung vermieden und sichergestellt, dass keine Ermüdung eintritt. Hinsichtlich der Zielsetzung sollte der Schwerpunkt der Analyse vereinbart werden (eine Routine oder ein gestressteres Szenario usw.), ebenso wie die zu sammelnden Informationen (Wahrscheinlichkeits- und oder Auswirkungsabschätzungen, Aktionspläne, usw.)
Hintergrund-recherche	Die (operationelle) Risikofunktion sollte die verfügbaren Informationen zu dem betreffenden Thema zusammentragen und sicherstellen, dass diese den Teilnehmern auf klare Weise vermittelt werden. Dazu können Informationen über jüngste Schadensfälle oder Beinaheschäden, RSA-Informationen, Berichte über Risikoindikatoren usw. gehören.
Teilnehmer bestimmen & einladen	Siehe 3.4.1 unten für Hinweise zu Teilnehmern
Moderation vereinbaren	Die Workshops sollten moderiert werden. Dies kann durch jemanden aus der (operationellen) Risikofunktion o.ä. geschehen oder durch einen externen Moderator. Die Person sollte Erfahrung mit der Moderation von Workshops haben und mit dem Analyse-/ Testverfahren des Unternehmens vertraut sein. Es sollte auch ein Protokollant anwesend sein, um sicherzustellen, dass die Diskussionen und Entscheidungen festgehalten werden.
Analysemethode festlegen	Siehe 3.4.3 unten.
Tagesordnung vereinbaren und verteilen	Stellen Sie sicher, dass alle Teilnehmer Zeit und Ort des Workshops kennen und wissen, wer neben ihnen teilnimmt, welche Ziele der Workshop hat usw.

Tabelle 2: Aufgaben zur Vorbereitung des Workshops

Abschnitt 3.4 – Die Durchführung eines Workshops

Die Workshops sollten in einer geeigneten Umgebung stattfinden, die ruhig und vom "Arbeitsalltag" der Teilnehmer entfernt ist.

Workshops sollten in der Regel 2-3 Stunden dauern. Längere Zeiträume führen zu Ermüdung. Alle 1-2 Stunden sollte eine kurze Pause eingeplant werden.

Wie oben erwähnt, sollten Workshops moderiert werden und der vereinbarten Tagesordnung folgen.

Abschnitt 3.4.1 – Die Teilnehmer

Die Teilnehmer hängen von der Zielsetzung des Workshops ab (z.B. von der Art des Risikos und dem Schwerpunkt). In der Regel sollten die folgenden Personen teilnehmen:

- Der jeweilige Risikoverantwortliche
- Die für das Schwerpunktthema verantwortliche Führungskraft, sofern sie nicht die Risikoverantworliche ist
- Andere Fachexperten, die wichtige Kontrollbereiche wie IT-Systeme und Sicherheit, Kundenbeziehungen, Marketing, Personalwesen, Finanzen usw. abdecken
- Ein unabhängiger Beobachter, z.B. ein interner Prüfer oder ein Vertreter der Risikofunktion

Etwa 6-8 Teilnehmer sind optimal, maximal sollten es 12 sein. Je größer die Workshops werden, desto schwieriger wird die Moderation und desto weniger Zeit steht zur Verfügung, um sicherzustellen, dass alle Stimmen gehört werden.

Die Rolle des unabhängigen Beobachters ist es, auf mögliche Befangenheit zu achten. Der Beobachter sollte nur dann das Wort ergreifen, wenn er Bedenken hat, dass eine Risikoexposition oder die Bewertung der Wirksamkeit von Kontrollen über- oder unterschätzt wird.

Auch wenn sie sich nicht zu Wort melden, spielen die Führungskräfte eine wichtige Rolle in Szenario-/ Stress-Workshops. Die Erfahrung zeigt, dass die Qualität des Workshop-Outputs oft gemindert wird, wenn diese Aufgabe an unerfahrenere Teammitglieder delegiert wird, und es folglich an einem Buy-In des Senior Managements mangelt. Die Geschäftsleitung und das Senior Management sind oft diejenigen, die die letzte Verantwortung tragen, wenn bestimmte Arten von schwerwiegenden Szenarien eintreten, daher sollten sie in den Prozess eingebunden werden.

Abschnitt 3.4.2 – Die wichtigsten Ergebnisvariablen

Obwohl die offene Diskussion wichtig ist, muss diese Diskussion darauf ausgerichtet sein, brauchbare Managementinformationen zu erzeugen, um Risikobewertung, Überwachung und Kontrolle zu unterstützen. Tabelle 3 fasst die wichtigsten Variablen zusammen, die während eines Workshops diskutiert werden sollten. Die Ergebnisse der Diskussion über diese Variablen sollten

Variable	Erklärung
Szenario-beschreibung	Eine kurze Beschreibung (Storyline) des fraglichen Szenarios oder Stressereignisses. Was ist passiert und in welchem Kontext (z.B. ein großer Betrug, der während einer Rezession auftritt, eine Geschäftsunterbrechung während einer Pandemie)
Ursachen	Die Ereignisse, die zu dem Szenario/ Stressereignis führen, einschließlich Personen-, Prozess- und Systemausfällen oder externen Ereignissen.
Wirkungen	Die Auswirkungen des Szenarios/ Stressereignisses, insbesondere, ob finanzielle oder reputationsbezogene Auswirkungen erwartet werden, sowie mögliche Auswirkungen auf Menschen (z.B. Gesundheit und Sicherheit oder Arbeitsmoral)
Kontrollen	Eine Einschätzung, wie gut die Kontrollen während des Szenarios, insbesondere eines Stressszenarios, funktionieren könnten. Die Teilnehmer sollten erörtern, ob die Kontrollen wirksam bleiben und welche Kontrollen gegebenenfalls versagen könnten
Mitigierende Maßnahmen während des Szenarios	Maßnahmen, die während des Szenarios/Stressereignisses ergriffen würden, um dessen Auswirkungen zu mindern.
Bewertung von Wahrscheinlichkeit und Auswirkung	Siehe 3.4.3 unten
Aktuelle Maßnahmen	Maßnahmen, die im Anschluss an den Workshop ergriffen werden sollten, um die Wahrscheinlichkeit oder die Auswirkungen des betreffenden Szenarios oder Stressereignisses zu verringern. Dazu gehört in der Regel die Verbesserung bestehender Kontrollen oder das Hinzufügen neuer Kontrollen. Weitere Informationen hierzu finden Sie im IOR-Praxisleitfaden zum Risiko Self Assessment.

Tabelle 3: Wichtige Ergebnisvariablen

Abschnitt 3.4.3 – Wahrscheinlichkeit und Auswirkung bewerten

Wahrscheinlichkeit

Der IOR-Praxisleitfaden zum Risiko Self Assessment enthält allgemeine Hinweise zur Bewertung von Wahrscheinlichkeit und Auswirkungen. Diese sollten die Grundlage für jede Bewertung während eines Workshops zur Analyse von Szenarien oder Stressereignissen bilden.

Ein wesentlicher Unterschied bezieht sich auf den Schweregrad von Szenarien und insbesondere Stressereignissen. Daher können sich die Wahrscheinlichkeits- und Auswirkungsskalen, die für die routinemäßigen RSAs verwendet werden, als unzureichend erweisen. Darüber hinaus können genaue Wahrscheinlichkeitsbewertungen für Szenarien und insbesondere Stressereignisse aufgrund eines Mangels an objektiven Daten schwierig, wenn nicht gar unmöglich sein.

Wahrscheinlichkeiten können wie folgt ausgedrückt werden:

1. In formalen statistischen Begriffen (z.B. 1 % oder 0,01 Wahrscheinlichkeit des Auftretens)

2. In Bezug auf die Dauer, z.B. 1 von 10 oder 1 in 100 Jahren

3. In qualitativen Begriffen (erwartet/ routinemäßig, unerwartet/ gestresst und “tail/ worst-case”)

Wenn formale Wahrscheinlichkeiten verwendet werden, wird empfohlen, diese in Form von Bereichen darzustellen, z.B. 1%-10%, 10-20%. Dies liegt an den Schwierigkeiten, genaue Wahrscheinlichkeiten zuzuordnen. Die Verwendung von statistischen Wahrscheinlichkeiten wird jedoch nicht empfohlen, da Nicht-Risikoexperten oft mit formalen statistischen Darstellungen von Wahrscheinlichkeiten zu kämpfen haben. Im Allgemeinen ist es besser, Zeiträume oder qualitative Begriffe zu verwenden. Zum Beispiel:

- 1 in 10 Jahren oder “Routine”-Ereignis - das voraussichtlich mehrmals im Laufe eines Arbeitslebens auftritt. Es ist wahrscheinlich, dass ein Unternehmen im Laufe des Arbeitslebens der Teilnehmer bereits Erfahrungen damit gemacht hat

- 1 in 40 Jahren oder “gestresstes” Ereignis - das, wenn überhaupt, nur einmal im Laufe eines Arbeitslebens auftritt. Es ist weniger wahrscheinlich, dass die Teilnehmer persönliche Erfahrungen mit einem solchen Ereignis haben, aber sie können beobachtet haben, dass andere Unternehmen davon betroffen sind

- 1 in 80 Jahren oder “Tail”-Ereignis - das einmal während des gesamten Lebens einer Person auftritt. Es gibt möglicherweise keine Beispiele für solche Ereignisse, außer vielleicht in historischen Aufzeichnungen. Allerdings müssten solche historischen Beispiele umfangreich überarbeitet werden, um sie auf den neuesten Stand zu bringen. Den Workshop-Teilnehmern sollten Definitionen wie die drei oben genannten während eines Workshops zur Verfügung gestellt werden, damit sie über die Wahrscheinlichkeit des Auftretens diskutieren und einen Konsens finden können

Unterschiedliche Versionen eines Szenarios oder Stressereignisses haben unterschiedliche Wahrscheinlichkeiten. Man muss nicht versuchen, jede mögliche Version eines Szenarios zu definieren. Es geht darum, Szenarien und Stressereignisse zu untersuchen, die repräsentativ für hypothetische, aber vorhersehbare operationelle Risikoereignisse sind, deren Erörterung einen Nutzen für das Management hat. Dennoch nehmen einige Unternehmen ein zentrales Szenario für eine bestimmte Risikokategorie (z.B. Schäden an Sachanlagen) und arbeiten dann an verschiedenen Versionen für 2-3 Wahrscheinlichkeitsstufen. Beispielsweise eine Routineversion des Szenarios (z.B. reparierbarer Schaden an einem Bereich eines Gebäudes), gefolgt von einem Stress- (reparierbarer Schaden am gesamten Gebäude) und Tail-Ereignis (Zerstörung des Gebäudes).

Auswirkungen

Szenarien, insbesondere, wenn sie zu Stresstest- oder Inversen Stressereignissen verarbeitet werden, haben per Definition hohe Auswirkungen. Bei inversen Stressereignissen wird die Auswirkung effektiv im Voraus bestimmt, da solche Ereignisse per Definition solvenzbedrohend sind. Die Auswirkungen müssen bei Szenarien und Stressereignissen nicht quantifiziert werden. Stattdessen können die Ereignisse einfach als routinemäßig/ erwartet, gestresst/ unerwartet oder extrem/ ‚tail‘ bezeichnet werden, wie oben angegeben.

Wenn ein Unternehmen die Auswirkungen quantifizieren möchte, ist es empfehlenswert, mit einer Diskussion der Auswirkungen zu beginnen und dann über das Ausmaß dieser Auswirkungen nachzudenken, typischerweise in finanzieller Hinsicht - aber auch Auswirkungen auf die Reputation können in Betracht gezogen werden (z.B. Auswirkungen auf den Goodwill der Kunden). Tabelle 4 fasst einige finanzielle und reputationsbezogene Auswirkungsfaktoren zusammen, die quantitativ geschätzt werden könnten.

Finanziell	Reputation
Kosten für das Ersetzen oder Reparieren von Vermögenswerten	Verlust von Kunden/Marktanteil (Anzahl der Kunden oder Verlust des Marktanteils in Prozent)
Bußgelder oder Haftungsansprüche	Negative Presse (Umfang und Dauer)
Sanierungskosten	Auswirkungen auf die Arbeitsmoral (z.B. Mitarbeiterbindung)
Kosten für Dritte, z.B. Prozesskosten	Herabstufung der Kreditwürdigkeit
Umsatzverluste durch Betriebsunterbrechung	Regulatorische Zensur (Anzahl von Erwähnung und Anprangern des Unternehmens sowie Dauer der regulatorischen Aufmerksamkeit)
Uneinbringliche Forderungen und sonstige uneinbringliche Vermögenswerte	
Verlust von Kapitalerträgen	

Tabelle 4: Beispiele von quantifizierbaren Auswirkungen

Wenn Quanten verwendet werden, wird empfohlen, sie in Form eines Bereichs darzustellen. Genaue Schätzungen der Auswirkungen sind aufgrund des hypothetischen Charakters der Szenarien unmöglich und vermitteln ein falsches Gefühl von Genauigkeit und Objektivität. Zusätzliche Hinweise zu Auswirkungen in Bezug auf Stresstests und Inverse Stresstests finden Sie in Abschnitt 5 unten.

Abschnitt 3.4.4 – Workshop-Analysetechniken

Workshops können im Wesentlichen auf zwei Arten durchgeführt werden:

1. Unstrukturiert - offene Diskussion über das Szenario oder das Stressereignis. Die Teilnehmer können die Punkte hervorheben, die für sie am wichtigsten sind.
2. Strukturiert - die Diskussion wird durch eine bestimmte Analysetechnik gelenkt, wie z.B. Fehler- und Ereignisbäume oder die Delphi-Technik

Ein strukturierter Ansatz ist nicht unbedingt besser. Dies liegt daran, dass er die Kreativität der Teilnehmer einschränken und ihre Aufmerksamkeit von wichtigen Aspekten eines Szenarios ablenken kann, die für ein Unternehmen besonders relevant sind. Ebenso bedeutet ein unstrukturierter Ansatz nicht, dass es keine Agenda gibt. Es bedeutet nur, dass die Diskussion bestimmter Tagesordnungspunkte nicht durch formale Analysetechniken strukturiert wird.

Abschnitt 3.5 - Ergebnisvalidierung

Um subjektive Verzerrungen zu vermeiden, wird empfohlen, die Ergebnisse von Szenario-Workshops systematisch zu validieren. Anders als beim Risiko Self Assessments ist ein Vergleich der Ergebnisse ähnlicher Szenario-Workshops selten möglich, da jedes Szenario einzigartig sein wird. Es gibt jedoch andere Ansätze, die verwendet werden können. Zum Beispiel:

- Vergleich mit den verfügbaren Daten zu externen Ereignissen, durch Verwendung von öffentlichen Daten oder einer externen Verlustdatenbank. Auch wenn ein Unternehmen kein Stress- oder Tail-Szenario erlebt hat, kann es sein, dass andere, ähnliche Unternehmen eines erlebt haben
- Wenn ein Unternehmen Zugang zu einer externen Verlustdatenbank hat, kann es sogar möglich sein, die Eintrittswahrscheinlichkeit für extremere Ereignisse zu bestimmen, vorausgesetzt, es sind genügend Daten vorhanden, um eine zuverlässige Wahrscheinlichkeitsverteilung zu erstellen

- Bei Szenarien auf der Ebene von Geschäftsbereichen oder Abteilungen/ Funktionen können Vergleiche innerhalb eines Unternehmens möglich sein, sofern diese ähnliche Szenarien untersucht haben

- Wenn die (operationelle) Risikofunktion an Praxisforen mit Vertretern der Risikofunktionen anderer Unternehmen teilnimmt, können sie vereinbaren, Informationen über operationelle Risikoszenarien auszutauschen, um die Ergebnisse zu vergleichen. Die Informationen können vor der Weitergabe auf kommerzielle Sensibilität geprüft werden

- Einige Anbieter bieten standardisierte Listen mit fertigen Szenarien für Unternehmen in bestimmten Branchen an. Diese standardisierten Szenarien spiegeln zwar nicht die Art, den Umfang und die Komplexität eines Unternehmens wieder, können aber als einfache Benchmark dienen, mit der sich die Ergebnisse vergleichen lassen. Unternehmen können diese Listen sowohl für die Auswahl von Szenarien als auch für den Vergleich von Ergebnissen nutzen. Wenn die Auswahl und die Ergebnisse des Unternehmens erheblich von den standardisierten Szenarien abweichen, sollten die Gründe dafür untersucht werden.

Schließlich sollte der Prozess der Szenarioanalyse einer regelmäßigen Überprüfung durch die Interne Revision unterzogen werden. Dies sollte die Überprüfung der Prozessumsetzung und den Vergleich seiner Gestaltung mit verfügbaren Praxisleitfäden, wie z.B. diesem Papier, beinhalten.

Abschnitt 3.6 – Den Prozess leiten

Die (operationelle) Risikofunktion ist im Unternehmen für die Gestaltung und Umsetzung der Szenarioanalyse und den Prozessen zu Stresstest und Inversem Stresstest für operationelle Risikoereignisse verantwortlich. Die Funktion sollte sicherstellen, dass diese Prozesse effektiv sind, und ihre Gestaltung und Umsetzung regelmäßig überprüfen.

Wenn ein Unternehmen ein Risikokomitee hat, kann es beschließen, diesem Komitee die Befugnis zu geben, die Gestaltung und Umsetzung dieser Prozesse zu überprüfen und freizugeben. Dies ist besonders wichtig, wenn die Szenarioanalyse und die Stresstests bzw. Inversen Stresstests eine aufsichtsrechtliche Anforderung darstellen.

Wenn Szenarioanalysen oder Stresstests/ Inverse Stresstests vorgeschrieben sind, es aber keinen Risikoausschuss gibt, sollte der Prüfungsausschuss Gestaltung und Umsetzung freigeben, um sicherzustellen, dass die Prozesse regelkonform sind. Berichte der Internen Revision über Szenarioanalysen und Stresstestprozesse sollten wie alle anderen Berichte der Internen Revision auch an den Prüfungsausschuss weitergeleitet werden.

Vorstände werden selten aufgefordert, Prozesse für Szenarioanalysen oder Stresstests/ Inverse Stresstests für operationelle Risiken freizugeben. Es ist jedoch üblich, dass sie Berichte über die Ergebnisse von Szenarioanalysen für operationelle Risiken und Stresstests/ Inverse Stresstests erhalten, um ihre Governance-Verantwortlichkeiten zu unterstützen.

Über die unmittelbaren Grenzen des operationellen Risikos hinaus können Vorstände aufgefordert werden, die vereinbarten Themen für Szenarien und Stresstests zu überprüfen und zusätzliche Themen vorzuschlagen, die sie für notwendig erachten, darunter auch Szenarien/ Tests, die ein Element des operationellen Risikos beinhalten. In einigen Sektoren kann dies eine aufsichtsrechtliche Anforderung sein, wie auch die Anforderung an Vorstände, Informationen über die wichtigsten, unternehmensweiten Szenarioanalysen und Stresstests zu erhalten. In der Finanzdienstleistungsbranche ist es beispielsweise üblich, dass Szenarioanalysen und Stresstests als Teil des regulatorischen Überprüfungs- und Bewertungsprozesses (Supervisory Review and Evaluation Process, SREP) der Säule II eingesetzt werden, der Teil der Eigenkapitalvorschriften für Banken und Versicherungen ist.

Dieser Prozess deckt Exponierungen gegenüber einer Reihe von Risikoarten ab, einschließlich des operationellen Risikos.

Wenn Inverse Stresstests durchgeführt werden, sollten diese immer an die Vorstände berichtet werden. Inverse Stresstests liefern wichtige Informationen über die langfristige Überlebensfähigkeit von Unternehmen und ihre Fähigkeit, den Betrieb aufrechtzuerhalten.

Schließlich sind einige Unternehmen verpflichtet, die Ergebnisse ihrer Szenarioanalysen und Stresstests bzw. Inversen Stresstests an die Aufsichtsbehörden zu melden. Dies ist der Fall bei systemrelevanten Finanzinstituten und in Nicht-Finanzsektoren wie dem sozialen Wohnungsbau.

Abschnitt 4 – Die Ergebnisse effektiv nutzen

Angesichts der erforderlichen Ressourcen ist es wichtig, die Ergebnisse von Szenarioanalysen, Stresstests oder Inversen Stresstests vollständig zu nutzen. Dies beinhaltet die Verwendung dieser Ergebnisse für Governance- und Compliance-Zwecke sowie zur Unterstützung der strategischen und operationellen Entscheidungsfindung.

Abschnitt 4.1 – Die Ergebnisse berichten

Wie oben erläutert, sollten Vorstände Berichte über abgeschlossene Szenarioanalysen, Stresstests und Inverse Stresstests für operationelle Risiken erhalten. Insbesondere dann, wenn diese sich auf Ereignisse und Auswirkungen beziehen, die sich auf die Strategie, den Geschäftsplan und die finanzielle Lebensfähigkeit eines Unternehmens auswirken könnten.

Die Geschäftsleitung und ggf. der Risikoausschuss sollten auch Berichte über die Ergebnisse erhalten, einschließlich der Maßnahmen, die ergriffen werden, um die Wahrscheinlichkeit und die Auswirkungen der im Rahmen dieses Prozesses analysierten operationellen Risikoereignisse zu mindern.

Die Berichte sollten keine unnötigen Details enthalten. Vorstände und leitende Angestellte haben nur begrenzte Zeit und müssen diese für eine Vielzahl von Aufgaben aufwenden. Der Schwerpunkt dieser Berichte sollte auf den potenziellen Auswirkungen von Ereignissen (finanziell oder reputationsbezogen) und den Folgen für die Finanzlage und den Geschäftsplan des Unternehmens liegen. Gegebenenfalls können auch Informationen zu den Maßnahmen geliefert werden, die ergriffen wurden, um identifizierte Kontrollschwächen abzumildern. Dies ist vor allem für die Geschäftsleitung und den Risikoausschuss oder ein gleichwertiges Gremium relevant.

Abschnitt 4.2 – Die Nutzung von Szenarien zur Unterstützung der RSAs

Die Ergebnisse der Szenarioanalyse und Stresstests zu operationellen Risiken können als Grundlage für das Risiko Self Assessment dienen. Dies gilt insbesondere für Bewertungen des inhärenten (Brutto-)Risikos. Dies liegt daran, dass Bewertungen des inhärenten Risikos ein hypothetisches Ausmaß der Gefährdung wiederspiegeln, wobei das Fehlen bzw. die Unwirksamkeit von Schlüsselkontrollen angenommen wird. Aufgrund des hypothetischen Charakters des inhärenten Risikos kann es für das Management schwierig sein, zuverlässige Bewertungen zu ermitteln. Szenarioanalysen und Stresstests bieten ein strukturiertes Mittel, um solche Bewertungen zu erreichen. Weitere Informationen zur Risikobewertung finden Sie im IOR-Praxisleitfaden zum Risiko Self Assessment.

Abschnitt 4.3 – Risiko- und Kapitalmodellierung

Einige wenige Unternehmen, insbesondere im Finanzdienstleistungssektor, konstruieren statistische Modelle, um Wahrscheinlichkeits- und Auswirkungsverteilungen für operationelle Risikoereignisse zu schätzen. Ziel ist es, die größtmögliche Bandbreite an Ergebnissen zu verstehen und jedem dieser Ergebnisse Wahrscheinlichkeiten zuzuordnen.

Ein wichtiger Input für diese Modellierung sind interne und externe Verlustdaten. Diese Daten sind jedoch historisch und oft unvollständig. Daher werden häufig Szenarioanalysen, Stresstests und Inverse Stresstests verwendet, um interne und externe Verlustdaten zu ergänzen.

Wenn Unternehmen versuchen, statistische Modelle für das operationelle Risiko zu erstellen, wird dringend empfohlen, die Ergebnisse ihrer Szenarioanalysen und Stresstests/ Inversen Stresstests in diese Modelle einzubeziehen. Diese Ergebnisse können wertvolle Informationen über den “Tail” der Wahrscheinlichkeits- und Auswirkungsverteilungen, die sie konstruieren, liefern. Risikomodelle sind nur dann effektiv, wenn sie die gesamte Bandbreite der Ergebnisse für ein bestimmtes Risikoereignis darstellen.

Abschnitt 5 – Weitere Empfehlungen zu Stresstest und Inversem Stresstest

Abschnitt 5.1 - Stresstest

Im Zusammenhang mit operationellen Risiken beinhaltet der Stresstest die Bewertung eines größeren Stressereignisses über eine Reihe von Risikofaktoren hinweg. Solche Ereignisse können Krisen und natürliche/ menschlich verursachte Katastrophen umfassen. Beispiele hierfür sind:

1. Umweltkatastrophen (z.B. Überschwemmungen, Stürme, Vulkane)
2. Eine Pandemie, COVID-19 ist ein Beispiel
3. Eine signifikante wirtschaftliche Rezession
4. Politische Störungen, wie z.B. Handelskriege
5. Der Ausfall einer wichtigen Gegenpartei (z.B. Lieferant, Outsourcing-Dienstleister oder Kunde)
6. Dedeutender Cyber-Angriff
7. Ungünstige Social-Media-Kampagne
8. Terroristische Angriffe

Es geht darum, die operationellen Risiken eines Unternehmens zu betonen und zu untersuchen, wie Kontrollen durch solche Ereignisse beeinträchtigt werden können. Zu den Schlüsselfragen gehören:

- Werden die Kontrollen wirksam bleiben? Was könnte passieren, wenn Kontrollen versagen?
- Was wären die finanziellen und reputationsbezogenen Auswirkungen eines solchen Ereignisses? Wie könnten Kontrollversagen/ Unwirksamkeit diese Auswirkungen verstärken?
- Können diese Auswirkungen während des Ereignisses abgemildert werden?
- Könnten zusätzliche Kontrollen erforderlich sein, um die Wahrscheinlichkeit und/oder die Auswirkungen von Stressereignissen zu verringern?

Sollten bestehende Kontrollen verstärkt werden, um sicherzustellen, dass sie bei Stressereignissen wirksam sind? Beeinflussen andere Faktoren, wie z.B. der Zeitpunkt eines Ereignisses, das Ausmaß des Stressereignisses? Könnten mehrere Stressereignisse gleichzeitig auftreten, wie würde sich dies auswirken?

In Bezug auf das Timing eines Ereignisses kann eine Sensitivitätsanalyse verwendet werden, um zu untersuchen, ob Timing ein Faktor ist. Beispielsweise könnte ein Unternehmen, das ein Stressereignis während einer saisonal stark frequentierten Zeit (z.B. Weihnachten) erlebt, zu diesem Zeitpunkt einen höheren Verlust erleiden als in einer weniger stark frequentierten Zeit. Sensitivitäten können auch durchgeführt werden, um Unterschiede im Konjunkturzyklus oder andere wirtschaftliche Variablen wie Änderungen der Inflationsrate oder der Zinssätze zu berücksichtigen. Zum Beispiel werden die finanziellen Auswirkungen von COVID-19 auf Unternehmen in Europa und den USA im Vergleich zu anderen Pandemien der letzten Zeit (SARS, Vogelgrippe usw.) aufgrund des niedrigen Wirtschaftswachstums vor der Pandemie höher eingeschätzt als in anderen Ländern.

In Bezug auf mehrere Stresstests wird empfohlen, einzelne Tests zu kombinieren, um die kumulativen finanziellen Auswirkungen auf ein Unternehmen zu untersuchen.

Dabei könnten sowohl potenziell korrelierende Stressereignisse (z.B. ein Cyberangriff gefolgt von einer negativen Social-Media-Kampagne) als auch solche, die zusammen auftreten könnten (z.B. eine neue Welle von COVID-19 in Verbindung mit einem No-Deal-Brexit), kombiniert werden.

Darüber hinaus könnten Unternehmen untersuchen, wie viele der identifizierten Stressereignisse sie zum gegenwärtigen Zeitpunkt aushalten könnten. Es ist unwahrscheinlich, dass ein Unternehmen allen identifizierten Ereignissen standhalten könnte, wenn sie gleichzeitig eintreten würden. Es ist aber nützlich, die Anzahl zu kennen, die zu einem bestimmten Zeitpunkt überlebt werden könnte. Eine solche Analyse sollte dem Vorstand und der Geschäftsleitung vorgelegt werden, damit sie die zukünftige finanzielle Lebensfähigkeit des Unternehmens besser einschätzen können.

Abschnitt 5.2 – Inverser Stresstest

Wie oben erläutert, besteht der Zweck des Inversen Stresstests darin, zu verstehen, wann ein Unternehmen nicht mehr lebensfähig ist. Dies kann sowohl die Tragfähigkeit des Geschäftsplans des Unternehmens als auch seine finanzielle Tragfähigkeit (Solvenz) umfassen.
Der Ausgangspunkt für Inverse Stresstests ist normalerweise die Finanzbuchhaltung eines Unternehmens. Gemeint sind:

1. Die Einnahmen- und Ausgabenrechnung (jährliche Gewinn- und Verlustrechnung)
2. Die Vermögensaufstellung (Bilanz)
3. Die Kapitalflussrechnung

Bei der Ertrags- und Aufwandsrechnung könnte ein Unternehmen mit dem Gewinn oder Überschuss des Vorjahres oder, bei einem eher vorausschauenden Ansatz, mit dem prognostizierten Gewinn oder Überschuss für das laufende Jahr beginnen und die Auswirkungen einer Verringerung dieses Wertes auf Null betrachten. Alternativ könnte es den Punkt bestimmen, an dem das Nettoeinkommen (EBITDA) die Zinsdeckung der Schuldverpflichtungen verletzt.

In Bezug auf die Erfolgsrechnung könnte ein Unternehmen den Punkt der Nichtlebensfähigkeit bestimmen, an dem sein Going Concern endet (z.B. wenn das gesamte Kapital verloren ist und der Wert der Verbindlichkeiten den der Vermögenswerte übersteigt).

Schließlich könnte ein Unternehmen im Hinblick auf die Kapitalflussrechnung den Punkt bestimmen, an dem es seine Verbindlichkeiten bei Fälligkeit nicht mehr erfüllen kann.
Nach der Bestimmung dieser Punkte ist ein üblicher nächster Schritt die Betrachtung der Stressereignisse oder einer Kombination von Stressereignissen, die solch schwerwiegende finanzielle Auswirkungen verursachen könnten. Im Kontext des operationellen Risikos könnte dies Folgendes umfassen:

- Ereignisse, die die Kapitalbasis eines Unternehmens zerstören, wie z.B. eine große Umweltkatastrophe, die zu lähmenden Aufräum- und Prozesskosten führt

- Ereignisse, die die Infrastruktur des Unternehmens zerstören und damit seine Fähigkeit, Einnahmen zu generieren, (z.B. ein größerer Systemausfall, der Verlust wichtiger Gebäude, ein längerer Ausfall der Lieferkette)

- Plötzlicher Liquiditätsverlust, wie z.B. ein schwerwiegender Bruch von Kreditvereinbarungen oder der Verlust des Investment-Grade-Ratings

- Großer Reputationsverlust, der zum Verlust vieler Kunden, Mitarbeiter, Lieferanten etc. führt

- Schwerwiegende regulatorische oder rechtliche Sanktionen (z.B. Zwangsschließung).

Es ist unwahrscheinlich, dass jedes potenzielle Extremszenario berücksichtigt wird oder werden kann. Dies ist nicht der Sinn eines Inversen Stresstests. In erster Linie geht es darum, dem Vorstand und der Geschäftsleitung zu vermitteln, wann das Unternehmen nicht mehr lebensfähig ist, damit sie sicherstellen können, dass das Unternehmen über ausreichende Mittel (Kapital und Liquidität) verfügt. Es ist jedoch auch für sie und ihr Unternehmen ratsam, die Arten von Ereignissen zu verstehen, die eine Nicht-Überlebensfähigkeit verursachen können. Aus Sicht des operationellen Risikos gibt es viele solcher Ereignisse, und die Vorstände bzw. die Geschäftsleitung werden den Wert des operationellen Risikos besser verstehen, wenn solche Ereignisse identifiziert werden.

Abschnitt 6 - Fazit

Das IOR ist der Ansicht, dass Szenarioanalysen, Stresstests und Inverse Stresstests wichtige Komponenten im Rahmen des Managements der operationellen Risiken eines Unternehmens sind. Operationelle Risikoereignisse sind für Unternehmen oft die schwerwiegendsten von allen und stellen reine Markt-, Kredit- oder Geschäftsrisikoereignisse in Bezug auf ihr Ausmaß in den Schatten. Die COVID-19-Pandemie ist ein aktuelles Beispiel, ebenso wie die globale Finanzkrise von 2007/08.

Es ist zwingend erforderlich, dass sich Unternehmen auf das Unerwartete vorbereiten, einschließlich sogenannter “Tail”-Ereignisse, die ihre Lebensfähigkeit bedrohen können. Es mag zwar unmöglich sein, jedes mögliche Ereignis vorherzusehen, das ist nicht der Punkt. Es geht darum, dem Management, insbesondere dem Vorstand und der Geschäftsleitung, zu helfen, die Arten von Ereignissen zu verstehen, die ihr Unternehmen bedrohen können, und sicherzustellen, dass ihre strategischen und operativen Entscheidungen die Gefährdung durch solche Ereignisse nicht signifikant erhöhen oder das Unternehmen übermäßig anfällig für deren Auswirkungen machen.

www.theirm.org

irm

Developing risk professionals