Risk Self Assessment

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

Inhalt

1. Einführung

Das Risiko Self Assessment (RSA) ist integraler Bestandteil der meisten Operational Risk Management Rahmenwerke. RSAs bieten eine strukturierte Vorgehensweise zur Abschätzung von operationellen Risiken und der Effektivität von Kontrollen. Auf diese Weise helfen RSAs Unternehmen dabei, Risikopositionen zu priorisieren, Kontrollschwächen und -lücken zu identifizieren und die Maßnahmen zu nachzuverfolgen, die zur Behebung von Schwächen oder Lücken ergriffen werden.

Ein gut konzipiertes und implementiertes RSA kann dazu beitragen, das Management operationeller Risiken in einem Unternehmen zu verankern, die Einstellung des Managements zum Management operationeller Risiken zu verbessern und die allgemeine Risikokultur zu fördern. Im Gegensatz dazu kann ein ineffizientes oder unnötig komplexes RSA den Ruf der (operationellen) Risikofunktion schädigen und den Eindruck verstärken, dass das operationelle Risikomanagement eine bürokratische, auf die Einhaltung von Vorschriften ausgerichtete Übung ist, die die Unternehmensziele nicht unterstützt.

Es kann nicht genug betont werden, dass ein effektives RSA viel mehr als eine technische Übung ist. RSAs können und sollten zwar dazu dienen, operationelle Risiken zu bewerten und ggf. zu quantifizieren, sie sind jedoch ebenso wichtig als Mechanismus zur Förderung einer offenen Diskussion über operationelle Risiken. Viele operationelle Risiken sind schwer zu identifizieren und noch schwerer zu quantifizieren. Dies liegt am Mangel von genauen Verlustdaten und daran, dass regelmäßig neue Risiken auftauchen. Ebenso lässt sich die Effektivität bestimmter Kontrollen schwer beurteilen. Doch trotz dieser Schwierigkeiten dürfen operationelle Risiken und die damit verbundenen Kontrollen nicht ignoriert werden. Unternehmen, die ihre operationellen Risiken und die Effektivität der zugehörigen Kontrollen offen diskutieren, sollten besser auf die Zukunft vorbereitet sein während sie die Proaktivität ihrer operationellen Risikomanagementaktivitäten verbessern.

Ein effektives RSA kann auch dazu beitragen, die Governance- und Compliance-Aktivitäten eines Unternehmens zu unterstützen. Die Ergebnisse eines RSAs geben dem Leitungsorgan und den Aufsichtsbehörden die Gewissheit, dass ein Unternehmen über ein solides System für das Management von operationellen Risiken verfügt. Ebenso können RSAs die Arbeit interner und externer Prüfer unterstützen, indem sie es ermöglichen, Prioritäten bei der Prüfung zu setzen und Prüfungsberichte zu strukturieren.

Schließlich können RSAs helfen, die Effizienz des Unternehmens zu verbessern. Schwachstellen oder Lücken in den Kontrollen können die Wahrscheinlichkeit von System- und Prozessausfällen und die Auswirkungen externer Ereignisse erhöhen, wodurch die Kosten und das Potenzial für Störungen steigen. Allerdings kann ein übermäßiges Maß an Kontrollen die Systeme und Prozesse unnötig verlangsamen.

2. RSA Grundlagen

Es gibt viele Möglichkeiten, die Gestaltung und Umsetzung eines RSAs anzugehen. Unternehmen sollten sich Zeit nehmen, um die Optionen zu prüfen und den Ansatz auszuwählen, der für die Art, den Umfang und die Komplexität ihrer Aktivitäten sowie für ihre Risikokultur am besten geeignet ist.

Trotz dieser Vielfalt müssen viele grundlegende Entscheidungen getroffen werden. Diese grundlegenden Entscheidungen werden im Folgenden erörtert.

2.1. Anwendung und Umfang

Die erste wichtige Entscheidung ist, ob RSAs für einige oder alle operationellen Risiken, denen ein Unternehmen ausgesetzt ist, gefordert werden sollen.

Die übliche Standardoption ist die Anforderung, dass alle identifizierten operationellen Risiken einem RSA unterzogen werden sollten. Dadurch wird sichergestellt, dass die Ergebnisse des RSA so umfassend und vollständig wie möglich sind. Angesichts der Tatsache, dass die Anzahl der einzelnen operationellen Risiken in einem Unternehmen in die Hunderte oder Tausende gehen kann, kann dies jedoch sehr zeitaufwendig und teuer sein.

Alternative Optionen sind:

1. Die Begrenzung der Granularität des RSAs. Unternehmen, die ihre operationellen Risiken kategorisieren, können z.B. entscheiden, dass RSAs nur für die “Level 1”-Risiken in ihrer Kategorisierung erstellt werden müssen (siehe Praxisleitfaden zur Kategorisierung operationeller Risiken). Dies stellt sicher, dass RSAs für alle Kategorien von operationellen Risiken durchgeführt werden, aber die Anzahl der Bewertungen begrenzt ist. Der Nachteil dieses Ansatzes ist, dass er für einige Nutzer von RSA-Informationen (z.B. Interne Revision, Abteilungsleitung) möglicherweise nicht detailliert genug ist.
2. Die Beschränkung des Fokus‘ auf die wesentlichen operationellen Risiken, die das Erreichen der Unternehmensziele gefährden. Ein solcher Ansatz liefert die Informationen, die das Leitungsgremium und die oberste Führungsebene benötigen, hilft aber der Abteilungs- oder Bereichsleitung nicht, ihre lokalen operationellen Risiken effektiv zu managen.
3. Die Begrenzung des Fokus‘ auf die wesentlichen operationellen Risiken, die das Erreichen der Abteilungs- oder Funktionsziele gefährden. Dadurch wird sichergestellt, dass die Abteilungs- und Bereichsleiter die Informationen erhalten, die sie für das Management ihrer lokalen Risiken benötigen. Zusätzlich kann ein Eskalationsprozess implementiert werden, um zu gewährleisten, dass Risiken, die signifikant genug sind, um das gesamte Unternehmen zu bedrohen, an das Leitungsgremium/die oberste Führungsebene gemeldet werden.

Kombinationen der oben genannten drei Ansätze können verwendet werden, um die Anwendung und den Umfang eines RSAs weiter zu verfeinern. Zum Beispiel könnte Option 2 unter Verwendung der Risiken der Stufe 1 in einer Kategorisierung durchgeführt werden und Option 3 mit Stufe 2, um die Granularität zu erhöhen.

Wie bei jeder Risikomanagement-Aktivität müssen Kosten und Nutzen eines mehr oder weniger umfassenden RSA-Ansatzes abgewogen werden. Ein vollständig umfassender Ansatz ist nicht unbedingt der beste, insbesondere, wenn er zu einem Informationsüberfluss führt und einen übermäßigen Zeit- und Arbeitsaufwand erfordert. RSAs sollten nur dort eingesetzt werden, wo sie wertschöpfend sind, d.h., der Nutzen muss die Kosten übersteigen.

2.2. Prozess- oder ereignisfokussiert

Die meisten operationellen RSAs werden auf Ereignisbasis durchgeführt. Das bedeutet, dass sie mit bestimmten Risikoereignissen wie Feuer, Betrug, Verletzung, Hackerangriff, Stromausfall usw. verbunden sind. Weitere Informationen über die Art und Kategorisierung von Risikoereignissen finden Sie im Praxisleitfaden des IOR zur Kategorisierung operationeller Risiken.

Eine Alternative ist die Prozessbasis. Bei diesem Ansatz werden organisatorische Prozesse abgebildet und potenzielle Fehlerpunkte innerhalb dieser Prozesse identifiziert (z.B. das Potenzial für menschliches Versagen oder Systemausfälle). Ein Prozessfokus erhöht die Übereinstimmung zwischen dem operationellen Risikomanagement und dem Tagesgeschäft eines Unternehmens. Dadurch wird das RSA als relevanter für das Management wahrgenommen und kann dazu genutzt werden, ein effektives operationelles Risikomanagement mit der Effizienz von Geschäftsprozessen zu verbinden.

Der Nachteil eines Prozessansatzes ist die Zeit, die für die Abbildung der Prozesse benötigt wird. Je detaillierter der Prozess abgebildet wird, desto umfassender wird die Anzahl der identifizierten operationellen Risiken sein. Detaillierte Prozesslandkarten können jedoch einen beträchtlichen Zeitaufwand und viel Fachwissen erfordern, um sie genau zu erstellen.

Wenn ein Unternehmen bereits über detaillierte Prozesslandkarten verfügt, wird empfohlen, diese als Grundlage für die Identifizierung der operationellen Risiken für RSAs zu verwenden. Wo solche Karten jedoch nicht vorhanden sind, sind die Kosten für ihre Erstellung wahrscheinlich zu hoch.

2.3. Rollen und Verantwortlichkeiten

In der Regel wird der RSA-Prozess von der (operationellen) Risikofunktion “verantwortet”. Das bedeutet, dass die (operationelle) Risikofunktion für die Gestaltung des RSAs und für die Überwachung der Umsetzung verantwortlich ist, um sicherzustellen, dass das Tool korrekt verwendet wird. Dies kann die Dokumentation des RSA-Prozesses, die Bereitstellung von Coaching und Training zur Durchführung von RSAs und die Moderation von RSA-Workshops beinhalten (siehe 4.1.4 unten).

Tabelle 1 fasst die anderen Rollen und Verantwortlichkeiten in Bezug auf RSAs zusammen. Weitere Informationen zu den Rollen und Verantwortlichkeiten für das operationelle Risiko finden Sie im Praxisleitfaden des IOR zur Governance des operationellen Risikos.

Rolle	Verantwortlichkeit
Leitungsgremium	Sicherstellen, dass ein angemessenes internes Kontrollsystem vorhanden ist. Dies kann die Bestätigung der Wirksamkeit des RSA-Ansatzes und die Überprüfung der Ergebnisse von RSAs für wesentliche operationelle Risiken beinhalten.
Geschäfts-leitung	Verantwortlich für die Unterstützung der Arbeit des Vorstands. Dies beinhaltet die Sicherstellung, dass ein effektiver RSA-Ansatz vorhanden ist. Wo vorhanden, trägt der Chief Risk Officer (CRO) die Hauptverantwortung für die Beaufsichtigung der Gestaltung und Umsetzung des RSAs.

Risiko-verantwortlicher	Verantwortlich für die RSA-Erstellung, um sicherzustellen, dass die Risiken innerhalb Appetit/Toleranz liegen und keine signifikanten Schwächen oder Lücken in den Kontrollen vorhanden sind. Risikoverantwortliche können das RSA entweder selbst beantworten oder die Verantwortung an entsprechend qualifizierte Personen delegieren. Die Risikoverantwortlichen müssen auch die Umsetzung aller Maßnahmen überwachen, die zur Behebung von Kontrollschwächen oder -lücken erforderlich sind.
Kontroll-verantwortlicher	Verantwortlich für die Gestaltung, Umsetzung und Aufrechterhaltung effektiver Kontrollen. Sollte die Risikoverantwortlichen über etwaige Schwächen oder Lücken in den Kontrollen informieren. Sollte auch gewährleisten, dass Maßnahmen ergriffen werden, um alle identifizierten Schwächen ihrer vorhandenen Kontrollen zu adressieren.
Daten-verantwortlicher	Verantwortlich für die Bereitstellung von Daten an die Risiko- und Kontrollverantwortlichen, damit diese das RSA fertigstellen können.
Kontroll-verantwortlicher	Gewährleistung von Gestaltung und Umsetzung des RSAs gegenüber der Geschäftsleitung und dem Leitungsgremium.

Tabelle 1: Andere Rollen und Verantwortlichkeiten für RSAs

Rollen und Rollenterminologie können in den Unternehmen unterschiedlich sein. Möglicherweise werden andere Begriffe verwendet als Risiko, Kontrolle oder Datenverantwortlicher. Wo dies der Fall ist, ist es wichtig, Personen zu identifizieren, die für Folgendes verantwortlich sind:

- Die Erstellung von zeitnahen, genauen und vollständigen RSAs
- Die Identifizierung von Kontrollschwächen oder -lücken
- Die Bereitstellung der für die Erstellung effektiver RSAs erforderlichen Daten
- Die Beaufsichtigung von Maßnahmen zur Behebung von Kontrollschwächen oder -lücken

2.4. Häufigkeit und Zeitpunkt

Nach der erstmaligen Erstellung sollten RSAs regelmäßig überprüft werden, um ihre Aktualität zu gewährleisten. Meistens wird eine jährliche Überprüfung und Aktualisierung gewählt. Häufigkeiten von einem Monat bis zu einem Jahr sind jedoch üblich.

Die von einem Unternehmen gewählte Häufigkeit hängt von der Dynamik ihrer operationellen Risiken ab. Je häufiger sich diese ändern, desto häufiger müssen die RSAs überprüft werden.

Unternehmen können eine vollständige jährliche Überprüfung durch Ad-hoc-Aktualisierungen für diejenigen Risiken ergänzen, die sich innerhalb eines Jahres signifikant ändern. Auf diese Weise können RSAs auf dem neuesten Stand gehalten werden, während die Kosten für die Erstellung auf ein Minimum reduziert werden.

Idealerweise sollten RSAs vor den jährlichen Überprüfungen der Unternehmens- oder Abteilungs-/Bereichsziele und -budgets aktualisiert werden. Auf diese Weise können Informationen aus RSAs in Leistungs- und Budgetüberprüfungen einfließen und dazu beitragen, das operationelle Risikomanagement in die strategischen Aktivitäten eines Unternehmens zu integrieren.

3. Die RSA-Gestaltung

Die Gestaltung eines RSAs beeinflusst seinen Erfolg oder Misserfolg. Entscheidend ist das Abwägen von Kosten und Nutzen eines erweiterten Umfangs oder einer zusätzlichen Komplexität. Je mehr Elemente zu einem RSA hinzugefügt werden, desto länger dauert die Fertigstellung und desto mehr Zeit und Ressourcen sind erforderlich.

3.1. Übliche Elemente eines RSAs

Im Folgenden werden übliche RSA-Elemente skizziert. Jedes dieser Elemente steht für einen anderen Aspekt der operationellen Risikoposition eines Unternehmens. Nicht alle RSAs werden jedes der Elemente enthalten. Wie oben erwähnt, ist es wichtig, den Nutzen eines RSAs gegen die Kosten für die Erstellung abzuwägen, insbesondere, wenn sie regelmäßig aktualisiert werden.

3.1.1. Risikomatrix (Wahrscheinlichkeit und Auswirkung)

Die meisten RSAs beinhalten eine qualitative Bewertung der Risikoexposition unter Verwendung einer Ordinalskala für Wahrscheinlichkeit und Auswirkung und kombinieren diese dann zu einer einfachen Risikomatrix. Diese Skalen reichen typischerweise von 1-3 (niedrig, mittel und hoch) bis zu 1-5. Es ist jedoch jeder Zahlenbereich möglich. Diese werden üblicherweise als 3x3-, 4x4- oder 5x5-Risikomatrizen bezeichnet.

Der wichtigste Aspekt bei einer Ordinalskala ist, dass die Daten nur in der Reihenfolge ihrer Größe angezeigt werden, d.h. 2 ist größer als 1. Bei einer Ordinalskala ist es nicht möglich zu bestimmen, wie viel größer 2 als 1 ist, da es keinen Messstandard für die Unterschiede zwischen diesen beiden Werten gibt. Sportligen sind ein weiteres Beispiel für Ordinalskalen. Es ist möglich zu sagen, dass die Mannschaft an der Spitze die beste Mannschaft ist, aber nicht, wie viel besser diese Mannschaft im Vergleich zu den anderen in der Liga ist. Tabelle 2 veranschaulicht eine einfache 3x3 ordinalskalierte Risikomatrix für Wahrscheinlichkeit und Auswirkung.

Wahrscheinlichkeit		**Auswirkung**	
1	Selten	1	Niedrig
2	Möglich	2	Mittel
3	Häufig	4	Hoch

Wahrschein-lichkeit	**Auswirkung**			
		1	2	3
	1	1	2	3
	2	2	4	6
	3	3	6	9

Tabelle 2: Beispiel einer ordinalskalierten 3x3 Risikomatrix

Um die Verwendung von Ordinalskalen zu unterstützen, sollten Bezugspunkte angegeben werden, um den Benutzern die Auswahl aus der Skala der Wahrscheinlichkeit und der Auswirkungen zu erleichtern. Tabelle 3 zeigt ein einfaches Beispiel.

Wahrschein-lichkeit		Auswirkung	
Selten	Eintrittswahrscheinlichkeit voraussichtlich nicht höher als einmal in 5 bis 10 Jahren	Niedrig	Der finanzielle Verlust wird voraussichtlich 1 % des Cashflows nicht überschreiten und kann leicht in den laufenden Kosten aufgefangen werden
Möglich	Eintrittswahrscheinlichkeit voraussichtlich nicht höher als einmal in 1 bis 5 Jahren	Mittel	Finanzieller Verlust zwischen 1 % und 5 % des Cashflows, kann moderate Kostensenkungen erforderlich machen
Häufig	Wahrscheinlichkeit des Auftretens voraussichtlich mehr als einmal pro Jahr	Hoch	Der finanzielle Verlust übersteigt 5 % des Cashflows und kann größere Kostensenkungen oder die Streichung strategischer Projekte erforderlich machen.

Tabelle 3: Beispielhafte Anhaltspunkte für qualitative Expositionsabschätzungen

Unternehmen sollten immer ihre Bezugspunkte für die Auswirkung festlegen. Diese sollten mit der Unternehmensgröße (insbesondere in Bezug auf Cashflows und Vermögenswerte) und ihren strategischen Zielen verknüpft werden. In Bezug auf die Größe kann ein Verlust von einer Million Pfund für ein kleines Unternehmen erheblich sein, jedoch unerheblich für ein großes Unternehmen mit einer starken Bilanz.

In Bezug auf die Wahrscheinlichkeit ist es üblich, diese entweder mit Wahrscheinlichkeits-bereichen zu verknüpfen (z.B. 0,8-1 für hoch, 0,5-0,79 für mittel usw.) oder mit der zeitlichen Häufigkeit, d.h. mit der Anzahl der Ereignisse pro Jahr oder der Anzahl der Jahre. Tabelle 3 enthält ein Beispiel, das als Ausgangspunkt verwendet werden kann. Die meisten Personen, die Risikomatrizen verwenden, bevorzugen zeitliche Bereiche für die Wahrscheinlichkeit, weil diese weniger technisch sind.

3.1.2. Inhärente Risikoexposition

Das inhärente Risiko bezieht sich auf den Grad der Risikoexposition, wenn keine Kontrollen angewendet werden. Es wird auch als Bruttorisiko bezeichnet.

Eine Bewertung des inhärenten Risikos im Rahmen einer RSAs liefert einen Ausgangswert für das betreffende Risiko. Ein Vorteil ist, dass es die Bedeutung eines Risikos hervorhebt, wenn keine Kontrollen angewendet werden. Ein niedriger Wert für das inhärente Risiko deutet darauf hin, dass das betreffende Risiko von geringer Bedeutung ist und nur wenig Aufmerksamkeit des Managements beanspruchen sollte. Im Gegensatz dazu deutet eine hohe inhärente Exposition darauf hin, dass in die Kontrolle des Risikos Zeit und Aufwand investiert werden sollte.

Unternehmen können entscheiden, dass Risiken mit einem niedrigen Grad an inhärenter Exposition kein vollständiges RSA erforderlich machen. Es ist wenig sinnvoll, Zeit und Ressourcen für die Bewertung der Wirksamkeit von Kontrollen oder die Identifizierung von Kontrolllücken aufzuwenden, wenn das inhärente Risiko sehr gering ist. Es ist besser, diese Zeit und Ressourcen in Risiken mit einem höheren inhärenten Potenzial zu investieren.

Das Hauptproblem bei der Berücksichtigung inhärenter Risiken besteht darin, die inhärente Exposition zu bestimmen. Risiken existieren selten in einer Umgebung ohne jegliche Kontrolle. Daher können inhärente Bewertungen sehr konzeptionell und wertend sein, wodurch sich das Potenzial für eine Über- oder Unterschätzung der inhärenten Exposition erhöht.

3.1.3. Restrisikoexposition

Das Restrisiko ist eine Bewertung des Risikoniveaus nach Einsatz von Kontrollen. Es wird auch als Nettorisiko bezeichnet.

Bei der Bewertung des Restrisikos werden die Anzahl, Art und Wirksamkeit der vorhandenen Kontrollen berücksichtigt. Theoretisch sollte ein gut durchdachter Mix aus effektiven Kontrollen das Restrisiko reduzieren. Die Differenz zwischen dem inhärenten Risiko und dem Restrisiko veranschaulicht den Beitrag, den die entsprechenden Kontrollen zur Reduzierung des Risikos leisten.

Das Restrisiko ist einfacher zu bewerten, da es das tatsächliche Ausmaß der Gefährdung unter Berücksichtigung der vorhandenen Kontrollen widerspiegelt. Daher sollte es sich um eine realistische Einschätzung handeln, die durch tatsächliche Erfahrungen im Umgang mit dem Risiko gestützt wird, einschließlich, falls vorhanden, historischer Verlustdaten. Es ist schwer vorstellbar, wie ein RSA ohne die Bewertung der Restrisikoexposition funktionieren könnte.

3.1.4. Ursachen

Operationelle Risiken werden typischerweise auf Ereignisbasis kategorisiert (siehe IOR-Praxisleitfaden zur Kategorisierung von operationellen Risiken). Das bedeutet, dass sich die Bewertungen des inhärenten Risikos und des Restrisikos in der Regel auf die Gefährdung eines Unternehmens durch bestimmte operationelle Risikoereignisse beziehen (z.B. Wahrscheinlichkeit und Auswirkungen des Ausfalls eines IT-Systems).

Ereignisse treten jedoch selten isoliert auf, sondern können durch eine Reihe von Faktoren verursacht werden. Beispielsweise kann ein Ausfall von IT-Systemen das Ergebnis eines Stromausfalls, eines Hacking-Versuchs oder eines fehlerhaften Updates oder einer Kombination aus allen drei Faktoren sein.

Daher enthalten einige RSAs Informationen zu den Ursachen von Risikoereignissen.
Dies ermöglicht die Bereitstellung weiterer Informationen zur Unterstützung der Wahrscheinlichkeitsbewertung. Außerdem können Kontrollen mit bestimmten Ursachen von Risikoereignissen verknüpft werden und es kann geprüft werden, ob Kontrollen vorhanden sind, um alle wichtigen Ursachen anzugehen.

Durch die Verknüpfung von Ereignissen und insbesondere von Kontrollen mit Ursachen können RSAs zukunftsgerichteter gestaltet werden und ermöglichen es Unternehmen, zukünftige operationelle Risikoereignisse besser zu verhindern. Durch das Sammeln von Informationen über Ursachen ist auch die Verknüpfung von Ereignissen möglich. So kann man erkennen, wie eine bestimmte Ursache oder ein Kontrollversagen in Bezug auf eine bestimmte Ursache eine Kette von operationellen Risikoereignissen auslösen können.

3.1.5. Auswirkungen

Am anderen Ende der Ursache-Ereignis-Wirkungs-Kette stehen die Auswirkungen von operationellen Risikoereignissen. Operationelle Risikoereignisse haben eine Reihe von Auswirkungen (z.B. finanzielle Auswirkungen, Betriebsunterbrechung, Reputationsschäden und physische Schäden). Ebenso kann das Ausmaß dieser Auswirkungen variieren - beispielsweise ein kleiner Brand, der sich auf einen begrenzten Bereich beschränkt, im Vergleich zu einem, der ein ganzes Gebäude oder einen Standort zerstört.

Bestimmte Kontrollen sind darauf ausgelegt, die Auswirkungen von operationellen Risikoereignissen zu reduzieren. Daher werden in einigen RSAs Informationen über die Auswirkungen gesammelt, um entsprechende Kontrollen mit diesen Auswirkungen zu verknüpfen. Eine Sprinkleranlage reduziert beispielsweise die Auswirkungen eines Brandes,

aber nur, wenn sie gut konzipiert ist und gewartet wird. Genauso kann die Einrichtung eines IT-Notfallstandorts nur dann dazu beitragen, die Auswirkungen von Systemausfällen zu verringern, wenn der Standort gut gewartet und regelmäßig getestet wird.

Durch das Sammeln von Informationen über die Auswirkungen kann man feststellen, ob ein angemessener Mix von Kontrollen vorhanden ist, um diese zu adressieren, oder ob es Lücken gibt, die gefüllt werden müssen, z.B. Auswirkungen, für die derzeit keine Kontrollen vorhanden sind.

3.1.6. Kontrolleffektivität (individuell)

Per Definition muss ein RSA eine Bewertung der Kontrollen beinhalten, die eingerichtet wurden, um die Ursachen und Auswirkungen von operationellen Risikoereignissen anzugehen. Unwirksame Kontrollen haben wenig bis gar keinen Einfluss auf die Gefährdung eines Unternehmens durch operationelle Risiken. Schlimmer noch, sie können ein falsches Gefühl der Sicherheit erzeugen, was zu einer Unterschätzung des Risikos führt.

Es gibt zwei Hauptmethoden, um die Effektivität von Kontrollen zu bewerten: eine subjektive Bewertung und objektive Kontrolltests.

Subjektive Bewertungen der Kontrolleffektivität verwenden eine Ordinalskala, ähnlich wie bei der Wahrscheinlichkeit und den Auswirkungen. Die einfachste ist eine Zwei-Punkte-Skala: “wirksam” oder “unwirksam”, aber auch Skalen von 3 oder mehr sind üblich. Tabelle 4 zeigt ein Beispiel für eine 3-Punkte-Skala.

	Kontrolleffektivität	Beschreibung
3	Vollumfänglich	Die Kontrolle ist voll wirksam und arbeitet wie vorgesehen
2	Angemessen	Die Kontrolle ist größtenteils effektiv, aber es gibt kleinere Schwachstellen in ihrer Funktionsweise
1	Verbesserungsbedarf	Die Kontrolle ist lückenhaft, es liegen erhebliche Mängel in der Funktionsweise vor

Tabelle 4: Beispiel einer Kontrolleffektivitätsskala

Subjektive Beurteilungen beruhen auf dem Urteil des Managements, es wird jedoch empfohlen, dass sie durch alle verfügbaren Informationen unterstützt werden, wie z.B. gemeldete Verlustereignisse oder Beinaheschäden (die möglicherweise das Ergebnis eines Kontrollversagens waren) und Berichte der Internen Revision.

Objektive Kontrolltests erfordern die Identifizierung und Überwachung von Indikatoren für die Wirksamkeit von Kontrollen, die üblicherweise als “Kontrollindikatoren” oder “Schlüsselkontrollindikatoren” bezeichnet werden. Beispiele für diese Indikatoren sind:

1. die Häufigkeit, mit der Business-Continuity-Pläne getestet und aktualisiert werden, einschließlich der Frage, ob Tests oder Aktualisierungen überfällig sind,
2. die Ergebnisse von Penetrationstests bei der IT-Sicherheit,
3. die Ergebnisse von Portable Appliance Tests und ob Tests überfällig sind,
4. identifizierte Verstöße gegen Richtlinien und Verfahrensweisen.

Daher können sich die Indikatoren entweder direkt auf die Funktionsweise einer Kontrolle beziehen oder auf die Häufigkeit und Zuverlässigkeit von Überprüfungen, durch die ihre Effektivität getestet werden soll.

Weitere Informationen zur Verwendung von Risikoindikatoren im Allgemeinen finden Sie im Praxisleitfaden des IOR zu Risikoindikatoren.

3.1.7. Kontrolleffektivität (gesamt)

Es ist selten, dass es für operationelle Risiken nur eine einzige Kontrolle gibt. Typischerweise ist eine Vielzahl von Kontrollen erforderlich, einige Ursachenkontrollen, die das Eintreten des Ereignisses verhindern sollen, und andere wirkungsbasierte Kontrollen, die die schädlichen Auswirkungen von operationellen Risikoereignissen aufdecken und abmildern sollen. Dieses Spektrum an ursachen- und wirkungsbasierten Kontrollen wird üblicherweise als “Kontrollumfeld” eines Risikoereignisses bezeichnet.

Schätzungen der Gesamteffektivität der Kontrollumgebung für ein bestimmtes operationelles Risikoereignis sind weniger üblich als die Bewertung spezifischer Kontrollen, liefern aber wertvolle Erkenntnisse darüber, ob ein Risiko über- oder unterkontrolliert ist. Die Identifikation von über- oder unterkontrollierten operationellen Risikoereignissen ist ein wichtiger Nutzen eines effektiven RSAs, daher wird die Einbeziehung einer Bewertung der Gesamteffektivität dringend empfohlen.

Normalerweise sind Bewertungen der Gesamteffektivität von Kontrollen subjektiv und basieren auf einer Drei-Punkte-Skala:

1. das Risiko wird nicht ausreichend kontrolliert, was bedeutet, dass es Lücken in der Kontrollumgebung gibt, die geschlossen werden müssen,
2. das Gesamtkontrollniveau ist angemessen, was bedeutet, dass die Kontrollumgebung eine angemessene Mischung von Kontrollen enthält,
3. das Risiko ist übermäßig kontrolliert, d.h., einige Kontrollen sind unnötig und können möglicherweise gestrichen werden,

Daten zu Schadensereignissen und Beinaheschäden können in Verbindung mit Berichten der Internen Revision wertvolle Informationen über die Gesamteffektivität der Kontrollumgebung liefern. Sie können beide potenzielle Lücken in der Kontrollumgebung aufzeigen, während interne Prüfungen manchmal überflüssige Kontrollen identifizieren können.

3.1.8. Maßnahmenplan

Die meisten RSAs enthalten Felder zur Erfassung von Informationen über vereinbarte Aktionspläne. Typischerweise betreffen diese Pläne entweder Mängel in bestehenden Kontrollen, die Umsetzung neuer Kontrollen oder die Beseitigung überflüssiger oder übertriebener Kontrollen.

Vereinbarte Maßnahmen müssen spezifisch, messbar, angemessen, realistisch und terminiert (SMART) sein (siehe Tabelle 5). Damit sollte sichergestellt sein, dass die Maßnahmen rechtzeitig abgeschlossen werden. Es ist außerdem wichtig, die Maßnahmen einem Verantwortlichen zuzuweisen. In der Regel handelt es sich bei dem Verantwortlichen um einen Manager mit der notwendigen Seniorität, vorzugsweise den für die Kontrolle Verantwortlichen, um zu gewährleisten, dass die Maßnahme abgeschlossen wird.

Spezifisch	Setzen Sie ein bestimmtes Ziel für die Maßnahmen
Messbar	Durch die Festlegung einer Maßnahme, die messbar ist, ist es möglich, auf objektive Weise nachzuweisen, dass sie abgeschlossen ist
Angemessen	Maßnahmen müssen angemessen sein, um sicherzustellen, dass sie rechtzeitig und effektiv abgeschlossen werden
Realistisch	Kontrollen und Kontrollumgebungen sind selten zu 100 % wirksam. Geringfügige Mängel können als tolerierbar angesehen werden, insbesondere wenn die mit der Erhöhung des Kontrollniveaus verbundenen Kosten hoch sind.
Terminiert	Maßnahmen müssen mit einem Enddatum versehen werden, um sicherzustellen, dass sie zeitnah abgeschlossen werden

Tabelle 5: SMART- Maßnahmen

3.1.9. Sonstige

Die oben genannten Elemente kommen am häufigsten in RSAs vor, was jedoch nicht bedeutet, dass sie die einzigen sind. Unternehmen können z.B. Informationen zu folgenden Punkten aufnehmen:

- Organisatorische Ziele, um spezifische operationelle Risikoereignisse mit den Zielen zu verknüpfen
- Risikobeschreibungen, die den identifizierten Risikoereignissen Details und Kontext verleihen
- Risiko-, Kontroll- und Leistungsindikatoren
- Daten zu Schadensfällen und Beinaheschäden
- Identifizierte Probleme und Maßnahmen der Internen Revision

Beim Hinzufügen neuer Elemente ist Vorsicht geboten - es ist immer wichtig, Kosten und Nutzen abzuwägen. Je detaillierter und komplexer ein RSA ist, desto länger dauert seine Fertigstellung.

3.2. Entwerfen der Vorlage

Es stehen zwei Hauptoptionen zur Verfügung:

1. Spreadsheet
2. IT-System

Die meisten Unternehmen beginnen mit der Nutzung eines Spreadsheets. Ein Beispiel finden Sie in Anhang A.

Es wird empfohlen, dass Unternehmen einige Jahre lang einen Spreadsheet-Ansatz verwenden, bevor sie auf ein System umsteigen. So können sie die Gestaltung des RSAs verfeinern, um sicherzustellen, dass es für die Art, den Umfang und die Komplexität ihres Geschäfts sowie für ihre Risikokultur geeignet ist.

Es wird nicht empfohlen, dass Unternehmen RSA-Systeme “von der Stange” kaufen, die die Gestaltung des RSA-Ansatzes vorgeben. Solche Systeme sind möglicherweise nicht mit dem Unternehmen oder seiner Risikokultur kompatibel. Es ist wichtig, dass jedes System so weit wie möglich maßgeschneidert werden kann.

3.3. Top-Down und Bottom-Up

RSAs können für eine Top-Down- oder Bottom-Up-Erstellung konzipiert sein.

Die Top-Down-Erstellung bezieht sich auf RSAs, die typischerweise von der Geschäftsleitung, einschließlich der Geschäftsführung, durchgeführt werden. Ein Top-Down-RSA konzentriert sich in der Regel auf operationelle Risiken auf strategischer Ebene, die das Erreichen der Unternehmensziele gefährden können. Solche Risiken haben wahrscheinlich erhebliche finanzielle, regulatorische oder reputationsbezogene Auswirkungen auf ein Unternehmen und gelten in der Regel unternehmensweit, obwohl sie manchmal spezifisch für eine Abteilung, einen Bereich oder eine Funktion sein können.

Bottom-up-RSAs konzentrieren sich auf operationelle Risiken auf Abteilungs- oder Funktionsebene. Sie sind in erster Linie als lokales Management-Tool konzipiert, um Verlustereignisse und Beinaheschäden zu verhindern/abzuschwächen oder die System- und Prozesseffizienz zu verbessern.

Die meisten Unternehmen werden Top-Down- und Bottom-Up-RSAs entwerfen. Der Vorteil eines Top-Down-Ansatzes besteht darin, dass Risiken auf strategischer Ebene nach unten kaskadiert und mit den Risiken, Kontrollen und Maßnahmen abgestimmt werden können, die in Abteilungen, Bereichen oder Funktionsbewertungen identifiziert wurden. Dies kann dazu beitragen, die operationelle Risiko Governance zu verbessern und sicherzustellen, dass unternehmensweite und lokale Prioritäten aufeinander abgestimmt sind.

Der Vorteil einer Bottom-up-Bewertung ist, dass sich lokale Manager auf die Risiken und Kontrollen konzentrieren können, die für ihren Bereich relevant sind. Zudem können signifikante lokale Risiken zur Betrachtung auf höchster Ebene eskaliert werden, ebenso wie signifikante Korrelationen zwischen Risiken auf lokaler Ebene in verschiedenen Bereichen.

Top-down- und Bottom-up-RSA-Vorlagen müssen konsistent sein und ähnliche Elemente und Terminologien verwenden. Dies erleichtert die Kaskadierung von Informationen über operationelle Risiken nach oben und unten im Unternehmen. In Anbetracht der zeitlichen Beschränkungen des Senior Managements kann es jedoch sinnvoll sein, eine kürzere, weniger komplexe Vorlage für diese Gruppe zu entwickeln.

4. Ein RSA abschließen: Ansätze und Techniken

Es wird nicht empfohlen, dass RSAs von einer Person - z.B. dem Risikoverantwortlichen oder seinem Stellvertreter - erstellt werden. Die urteilende Natur der meisten RSAs macht subjektive Abweichungen sehr wahrscheinlich, die zu einer Über- oder Unterbewertung des Risikopotenzials und der Wirksamkeit von Kontrollen führen können. In jedem Fall führt es zu ungenauen Informationen und verschwendeten Ressourcen.

Der beste Weg, um Verzerrungen zu beseitigen, ist, die Anzahl der am RSA-Prozess beteiligten Personen zu erhöhen. Das Problem individueller Abweichungen sollte entschärft werden, wenn die Gruppe diese effektiv in Frage stellen kann. Ein weiterer Vorteil der Beteiligung vieler Einzelpersonen ist die Vergrößerung des Spektrums an Fachwissen und Erfahrung. Selten verfügt eine einzelne Person über alle Informationen, die für die effektive Erstellung eines RSA erforderlich sind.

4.1. Workshop-Ansatz

Ein Workshop-Ansatz zur Durchführung des RSAs gewährleistet Interaktion zwischen den Teilnehmern und ermöglicht die Anleitung durch einen Risikofachmann während des Prozesses (siehe 4.1.4). Obwohl er zeitaufwändiger sein kann als die Alternativen, kann die Qualität der Informationen, die durch einen Workshop-Ansatz erzeugt werden, beträchtlich sein. Dies liegt an der Bandbreite der Fähigkeiten, Erfahrungen und des Fachwissens, die vorhanden sein sollten.

Ein Workshop ist ein Mechanismus, um Menschen dazu zu bringen, über ihre Risiken, Kontrollen und notwendige Verbesserungen zu sprechen. Weitere potenzielle Vorteile eines Workshop-Ansatzes sind:

- Schärfung des Bewusstseins für operationelle Risiken und die damit verbundenen Kontrollen
- Ermöglichung der Bewertung und Verbesserung von “weicheren”, schwer messbaren Kontrollmechanismen, z.B. Kommunikation, Schulung und Rechenschaftspflicht
- Gelegenheit zum Transfer von Risikomanagement- Knowhow innerhalb des Unternehmens

4.1.1. Planung

Die Vorbereitung ist die Basis für einen erfolgreichen RSA-Workshops. Die Teilnehmer sollten vor dem Workshop eine Anleitung erhalten, damit sie den Kontext und die Ziele der Übung sowie den von ihnen erwarteten Beitrag vollständig verstehen.

Tabelle 6 fasst allgemeine Maßnahmen zusammen, die für die Planung eines erfolgreichen RSA-Workshops getroffen werden sollten.

Thema	Erforderliche Maßnahme
Unter-stützung von Führungs-kräften erhalten	Der Risikoausschuss oder ein gleichwertiges Gremium sollte den Risiko- und Kontrollverantwortlichen seine Unterstützung für die Workshops mitteilen. Die zuständige Führungskraft oder der Senior Manager für den Bereich wird gebeten, in den ersten 5 Minuten des Workshops anwesend zu sein, um dessen Bedeutung zu vermitteln. Wenn die Teilnahme nicht möglich ist, bitten Sie sie, die Teilnehmer per Telefon oder E-Mail zu kontaktieren oder ein kurzes Einführungsvideo zu erstellen.

Vorrangige Bereiche identifizieren	Einige Abteilungen oder Funktionen haben möglicherweise einen dringenderen Bedarf an Workshops. Dies kann durch die Überprüfung von Daten zu Verlusten und Beinaheschäden, Berichten der Internen Revision oder die Identifizierung von inhärent risikoreichen Bereichen festgestellt werden.
Lokale Unterstützung für das RSA sichern	Setzen Sie sich mit dem lokalen Management in Verbindung, um sicherzustellen, dass es den Prozess und die Vorteile eines RSAs versteht und eventuelle Bedenken anspricht. Sichern Sie sich insbesondere deren Unterstützung, um sicherzustellen, dass alle identifizierten Maßnahmen innerhalb des vereinbarten Zeitrahmens abgeschlossen werden.
Prozesse und Aktivitäten im Bereich überprüfen	Identifizieren Sie die wichtigsten Aktivitäten und Prozesse, die der Bereich durchführt. Es ist wichtig, die Abläufe eines Bereichs zu verstehen, um sicherzustellen, dass die richtigen Teilnehmer ausgewählt werden. Prüfen Sie, sofern vorhanden, Bewertungen des operationellen Risikos und alle Daten zu Verlusten oder Beinaheschäden.
Teilnehmer identifzieren und einladen	Legen Sie fest, wer an dem Workshop teilnehmen soll (siehe 4.1.2) und bestätigen Sie die Teilnahme. Wenn wichtige Teilnehmer feststellen, dass sie nicht mehr verfügbar sind, sollten sie einen Vertreter benennen.
Workshop-Umfang und Ziele	Vereinbaren Sie mit den Teilnehmern den Umfang und die Ziele des Workshops. Es kann z.B. sein, dass nur eine bestimmte Kategorie operationeller Risiken betrachtet wird (z.B. IT-Risiken) oder bestimmte operationelle Prozesse (z.B. Kundenprozesse). Manchmal werden Risiken als Teil des RSA-Prozesses identifiziert. Das bedeutet, dass der Workshop mit der Identifizierung der relevanten Risiken beginnt. Es wird jedoch empfohlen, die primären Risikokategorien (z.B. die relevanten Level-1-Kategorien) im Voraus zu identifizieren. Dies spart während des Workshops Zeit.
Standarddokumen-tation bereitstellen (RSA-Prozess und Workshop-Agenda)	Stellen Sie sicher, dass die Teilnehmer verstehen, was ein RSA ist, welche Informationen erforderlich sind und wie der Workshop abläuft.
Einen Moderator organi-sieren	Die Workshops erfordern einen fachkundigen Moderator, der mit RSAs vertraut ist. Der Moderator sollte unparteiisch sein und kann ein Mitglied der (operationellen) Risikofunktion, ein Risikoexperte aus einem anderen Teil des Unternehmens oder ein externer Berater sein.

Darstellung 6: Planung von Themen und Tätigkeiten für einen RSA-Workshop

4.1.2. Teilnehmer

Die Auswahl der Teilnehmer hängt vom Umfang des Workshops ab (z.B. zu behandelnde Risikokategorien, zu überprüfende Prozesse und Aktivitäten). In der Regel sollten die folgenden Personen teilnehmen:

- ein Vertreter des lokalen Managements, einschließlich, wo angegeben, des/der relevanten Risikoverantwortlichen
- sofern angegeben, alle relevanten Kontrollverantwortlichen

- falls nicht durch die relevanten Kontrollverantwortlichen vertreten, Fachexperten, die wichtige Kontrollbereiche wie IT-Systeme und Sicherheit, Kundenbeziehungen, Marketing, Personalwesen, Finanzen usw. abdecken
- ein unabhängiger Beobachter, z.B. ein Mitglied der Risikofunktion oder ein Risikoverantwortlicher aus einem anderen Unternehmensteil

Als allgemeine Regel gilt, dass 6-8 Teilnehmer optimal sind, maximal 12. Je größer die Workshops werden, desto schwieriger wird die Moderation und desto weniger Zeit steht zur Verfügung, um alle Stimmen zu hören.

Die Rolle des unabhängigen Beobachters ist es, auf mögliche Verzerrungen 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.

Bei der Einladung von Managern zu Workshops sollte man Vorsicht walten lassen. Oft müssen sie teilnehmen, weil sie die relevanten Risiko- oder Kontrollverantwortlichen sind. Es besteht jedoch die Gefahr, dass sie die Diskussion dominieren und andere davon abhalten, Bedenken zu äußern. Hier ist die Rolle des Moderators zusammen mit dem unabhängigen Beobachter entscheidend. Sie sollten eine ausreichende Seniorität haben, damit das Management einen Workshop nicht dominiert oder ihn dazu benutzt, eine bestimmte politische Agenda zu verfolgen.

4.1.3. Struktur und Dauer des Workshops

RSAs können mehrere Tage in Anspruch nehmen, insbesondere, wenn sie das gesamte Spektrum der operationellen Risiken für den betreffenden Bereich abdecken. Dies stellt eine Herausforderung für Struktur und Zeitplanung von Workshops dar. Selbst mit regelmäßigen Pausen können Sitzungen, die länger als 2 bis 3 Stunden dauern, ermüdend sein, die Konzentration verringern und zu ungenauen Bewertungen führen.

Um die Konzentration aufrechtzuerhalten, empfiehlt es sich, die Workshops in verschiedene Abschnitte oder Module zu gliedern. Diese Module können innerhalb eines Workshops oder zeitlich aufeinanderfolgend über mehrere Tage hinweg stattfinden.

Modul 1 - Beschreibung der zu beurteilenden Risiken und Beurteilung des inhärenten Risikos.

Modul 2 - Identifizierung und Wirksamkeit von Kontrollen und die Bewertung des Restrisikos.

Modul 3 - Maßnahmenplanung und nächste Schritte.

Durch die Fokussierung der Diskussion in den Workshops auf diese Kernaspekte (d.h. Risiken, Kontrollen und Maßnahmenplanung) können andere zusätzliche Anforderungen, wie z.B. Kontrolltests, die Vereinbarung von Fälligkeitsterminen für Maßnahmen oder die Zuweisung und Änderung der Verantwortung für Risiken und Kontrollen, außerhalb der Workshops abgeschlossen werden.

In allen Fällen ist es wichtig zu berücksichtigen, dass die Verantwortung für die Geschäftsziele, Prozesse, Risiken und Kontrollen und deren korrekte Identifizierung beim lokalen Management liegt. Ein Workshop ist lediglich ein Werkzeug, das sie bei der effektiven Wahrnehmung dieser Verantwortung unterstützen soll.

4.1.4. Vereinfachung

Der Einsatz eines qualifizierten Moderators hilft, Subjektivität und Voreingenommenheit zu reduzieren und potenzielle Interessenkonflikte und politische Manöver (z.B. Über- oder Untertreibung eines Risikos, um das Ressourcenbudget zu beeinflussen) zu identifizieren.

Einige Unternehmen ziehen es vor, ihre eigenen internen RSAs zu moderieren, andere werden externe Moderatoren einsetzen. Wenn interne Moderatoren eingesetzt werden, ist es zulässig, Experten aus den Risiko- oder Prüfungsfunktionen einzusetzen, vorausgesetzt es wird klargestellt, dass die Verantwortung für die Bewertung und ihre Ergebnisse vollständig beim lokalen Management liegt (z.B. bei den jeweiligen Risiko- und Kontrollverantwortlichen).

Die Rolle des Moderators erfordert spezifische Fähigkeiten, wie in Tabelle 7 dargestellt.

Rolle	Fähigkeiten
Schwung beibehalten und sicherstellen, dass die Tagesordnung eingehalten wird	Aktives Zuhören
Sicherstellen, dass der RSA-Prozess eingehalten wird	Einen sicheren Raum für Diskussionen schaffen, sicherstellen, dass alle Perspektiven gewürdigt werden
Hinterfragen möglicher Verzerrungen oder Interessenkonflikte	Durchsetzen von Autorität und Kontrolle zur Aufrechterhaltung der Disziplin
Alle Teilnehmer in die Diskussion einbeziehen	Diskussionen klar und präzise zusammenfassen und Prioritäten setzen
Eine ausgewogene Diskussion gewährleisten	Detaillierte Kenntnisse und Erfahrungen mit dem RSA-Prozess
Sicherstellen, dass Entscheidungen, Maßnahmen und etwaige Unstimmigkeiten aufgezeichnet werden (ggf. dafür Notizen verwenden)	

Tabelle 7: Moderatorenrolle

4.1.5. Validierung

Um subjektiven Verzerrungen entgegenzuwirken, wird empfohlen, die Ergebnisse ähnlicher Workshops zu vergleichen. Dies sollte dazu beitragen, signifikante Ausreißer bei den Antworten aufzudecken. Üblicherweise sollte diese Arbeit von der (operationellen) Risikofunktion erledigt werden.

Zum Beispiel sollte es möglich sein, Risiko- und Kontrollbewertungen für ähnliche Risiken über Abteilungen und Funktionen hinweg zu vergleichen. Wenn die Bewertung eines bestimmten Risikos oder einer bestimmten Kontrollart signifikant abweicht, sollte eine Diskussion mit den betreffenden Managern geführt werden, um zu erfahren, ob es gute Gründe für diese Unterschiede gibt.

Vorsicht ist geboten, wenn Sie um Änderungen an RSAs bitten. Die Risikofunktion muss jederzeit sicherstellen, dass die RSAs in der Verantwortung der dafür verantwortlichen Manager liegen. Dies kann manchmal die Tolerierung von Bewertungen erfordern, die leicht verzerrt sind. Solche Bewertungen sollten jedoch gekennzeichnet werden, insbesondere bei der Berichterstattung über RSA-Ergebnisse an das Senior Management.

4.2. Fragebögen

Fragebögen können verwendet werden, um einige oder alle Informationen zu sammeln, die für ein RSA erforderlich sind. Fragebögen können als Ersatz für einen Workshop verwendet werden, um Zeit und Ressourcen zu sparen. Sie sind jedoch am effektivsten, wenn sie mit Workshops kombiniert werden. Hier können durch den Einsatz eines Fragebogens die ersten Gedanken der Workshop-Teilnehmer gesammelt werden und ein Workshop kann genutzt werden, um Feststellungen zu diskutieren.

Es ist auch möglich, Fragebögen zu nutzen, um ein breiteres Publikum mit einzubeziehen als die wenigen Personen, die zu einem Workshop eingeladen würden. Dies sollte die Gefahr verringern, Risiken oder Kontrollen zu übersehen und helfen, individuelle Voreingenommenheit zu kontrollieren.

4.2.1. Umfang des Fragebogens

Fragebögen können für bestimmte Kategorien von operationellen Risiken (z.B. Betrugs- oder IT-Risiken) konzipiert sein oder sie können versuchen, Informationen über alle Risiken zu erfassen. Beides hat Vor- und Nachteile. Ein fokussierter Fragebogen ist kürzer und nimmt weniger Zeit zum Ausfüllen in Anspruch, was das Risiko der Ermüdung der Befragten verringert und die Genauigkeit der Antworten erhöht. Wenn jedoch viele fokussierte Fragebögen zur Durchführung eines RSAs erforderlich sind, wird empfohlen, diese über mehrere Monate zu verteilen, um eine Überlastung zu vermeiden. Alternativ können auch verschiedene fokussierte Fragebögen an verschiedene Stichproben von Befragten geschickt werden. Dies kann besonders effektiv sein, wenn jede Stichprobe auf der Grundlage von Fachwissen ausgewählt wird (z.B. wird die Umfrage zu IT-Risiken an die relevanten IT-Experten und die Hauptnutzer von IT-Systemen gesendet).

Ebenso können Fragebögen explorativ (z.B. durch die Verwendung von offenen Fragen zur Identifizierung neuer Risiken oder Kontrollen) oder bestätigend sein. Normalerweise sind Fragebögen konfirmatorisch, d.h. sie beginnen mit einem bestimmten Satz von Risiken und Kontrollen.

Für konfirmatorische Fragebögen wird empfohlen, dass unternehmensweit eine konsistente Kategorisierung des operationellen Risikos verwendet wird (siehe IOR-Leitfaden zur Kategorisierung des operationellen Risikos) und dass eine standardisierte Liste von Kontrollen für das Unternehmen erstellt wird. Vorzugsweise sollte jede Risikokategorie mit einer spezifischen Untergruppe dieser standardisierten Kontrollen verknüpft werden. Dadurch erhält der Fragebogen eine einheitliche Struktur und die Antworten können leicht verglichen werden.

4.2.2. Inhalt des Fragebogens

Ein Fragebogen sollte mindestens Fragen zu den folgenden Punkten enthalten:

1. Ein Fragebogen sollte mindestens Fragen zu den folgenden Punkten enthalten:
2. geschätztes Niveau des inhärenten Risikos,
3. geschätzte Wirksamkeit der Kontrollen (individuell und im gesamten Umfeld, falls dies Teil des RSAs ist),
4. geschätzte Höhe des Restrisikos,
5. empfohlene Maßnahmen zur Verbesserung der Kontrolleffektivität.

Der Fragebogen sollte so kurz wie möglich gehalten werden. Je länger der Fragebogen ist, desto größer ist die Wahrscheinlichkeit, dass die Befragten entweder nicht mehr antworten oder zufällige Antworten geben.

Soziodemografische Fragen (z.B. Alter, Geschlecht) sind in der Regel nicht notwendig. Es sollte darauf verzichtet werden, um die Länge des Fragebogens zu reduzieren. Die einzigen potenziell relevanten Fragen sind die Abteilung oder die Funktion, in der die Person arbeitet, und ihre Seniorität.

4.2.3. Entwurf eines Fragebogens

Die Fragen können Standard- oder Nicht-Standardfragen sein:

- Standardfragen werden zentral verfasst, in der Regel von der Zuständigkeit für das operationelle Risiko. Sie beziehen sich auf die oben genannten Mindestinhalte.
- Nicht-Standard-Fragen werden lokal vom jeweiligen Management verfasst, um spezifische operationelle Risiko- und Kontrollthemen oder -anliegen zu behandeln

Wenn die Einbindung des Managements problematisch ist, kann es besser sein, einen Nicht-Standard-Ansatz zu wählen, der dem lokalen Management mehr Verantwortung für die Gestaltung des Fragebogens gibt. Dadurch wird es jedoch schwieriger, die Antworten zusammenzufassen und zu vergleichen. Idealerweise sollten die lokalen Manager gebeten werden, viele Standardfragen einzubeziehen und dann die Freiheit haben, weitere Fragen hinzuzufügen, wenn sie dies wünschen.

Geschlossene Fragen sollten so strukturiert sein, dass sie entweder mit einer geraden Likert-Skala “stimme zu” oder “stimme nicht zu” (z.B. 1 für “stimme voll und ganz zu”, 4 für “stimme überhaupt nicht zu”) oder mit einem binären “Ja” oder “Nein” beantwortet werden können. Dadurch wird sichergestellt, dass die Befragten nicht “zwischen den Stühlen sitzen” und bei den meisten Antworten den Mittelwert angeben (z.B. 3 bei einer 5-Punkte-Skala).

Die Verwendung der Option “Nicht zutreffend” ist zulässig, aber nur, wenn die Befragten dies mit einer Erklärung begründen können (z.B. eine bestimmte Kontrolle wird derzeit in ihrem Zuständigkeitsbereich nicht verwendet).

Offene Fragen sind erwünscht, vor allem um Entscheidungen wie “Nicht zutreffend” oder “Nein” zu begründen. Offene Fragen können auch verwendet werden, um einen Zusammenhang zu schaffen, z.B. um zu erklären, warum die Kontrolle als wirksam oder nicht wirksam angesehen wird.

4.3. Inhalt des Fragebogens

Workshops und Fragebögen sind die gebräuchlichsten Techniken, aber es gibt auch andere, die in Betracht gezogen werden können. Tabelle 8 fasst drei alternative Optionen zusammen.

Rolle	Fähigkeiten
Strukturierte ‚Was-wäre-wenn'-Technik	Die strukturierte Was-wäre-wenn-Technik (SWIFT) ist eine systematische, teamorientierte Technik, die am häufigsten für die Bewertung von Gesundheits- und Sicherheitsrisiken sowie umweltbezogenen Risiken und Kontrollen in Bereichen wie der chemischen Verarbeitung und Fertigung verwendet wird, aber auch auf viele andere Risikoarten angewendet werden kann. Die Technik verwendet eine Reihe von strukturierten "Was-wäre-wenn"- und "Wie-könnte"-Fragen, um zu prüfen, wie Abweichungen vom normalen Betrieb in Systemen, Prozessen und Kontrollen zu Risikoereignissen führen können. Brainstorming wird durch Checklisten unterstützt, um die Diskussion anzuregen. SWIFT verlässt sich auf den Input von Experten und den Einsatz eines "SWIFT-Leiters" zur Strukturierung der Diskussion. Der SWIFT-Schreiber hält die Diskussion auf einem Standardprotokollblatt online fest. Es gibt keinen einheitlichen Standard für SWIFT - eine der Stärken des Ansatzes ist, dass er flexibel an die jeweilige Anwendung angepasst werden kann. SWIFT ist eine teure Technik, da sie viel Zeit und Personal erfordert. Sie erhöht jedoch die Wahrscheinlichkeit, dass alle relevanten Risikoereignisse und Kontrollen berücksichtigt werden. Aus diesem Grund wird sie am häufigsten in gefährlichen Sektoren wie der chemischen Verarbeitung oder der nuklearen Energieerzeugung eingesetzt.
Delphi - Technik	Die Delphi-Technik ist ein Werkzeug zur Informationssammlung, das als Möglichkeit verwendet wird, einen Konsens von Experten zu ei-nem Thema zu erreichen - in diesem Fall die RSA-Erstellung. Jeder Experte nimmt anonym teil, und ein Moderator verwendet einen Fra-gebogen, um Ideen zu den wichtigen Punkten des Themas zu sam-meln. Die Antworten werden zusammengefasst und zur weiteren Kommentierung an die Experten zurückgesandt. Ein Konsens kann in einigen Runden dieses Prozesses erreicht werden. In Bezug auf RSAs hilft die Delphi-Technik, Verzerrungen zu redu-zieren und zu verhindern, dass eine einzelne Person einen unan-gemessenen Einfluss auf die Bewertung hat. Es kann eine Reihe von Experten eingesetzt werden, darunter Risikomanagement-Spezialisten, andere Funktionsspezialisten (IT, HR, Governance usw.) sowie Abteilungs- und Funktionsmanager (z.B. Betriebsleiter, Buchhalter). Anonymität ist wichtig, denn sie ermutigt die Experten, so ehrlich und offen wie möglich zu sein. Studien haben gezeigt, dass die Technik sehr effektiv bei der Vorhersage zukünftiger Ergebnisse sein kann, aber sie ist auch sehr zeitaufwändig, insbesondere wenn ein Kon-sens schwer zu erreichen ist.

Ursachen-analyse	Die Ursachenanalyse geht davon aus, dass operationelle Risikoereignisse mehrere Ursachen haben. Beispielsweise benötigt ein Brandrisikoereignis Material zum Brennen, einen Funken und Sauerstoff, bevor es Schaden verursachen kann. Die Ursachenanalyse vertieft den RSA-Gedanken und untersucht, wie und warum ein Ereignis eintreten kann. Der Schwerpunkt liegt auf der zukünftigen Prävention, indem bestehende Kontrollen verbessert oder neue hinzugefügt werden, um zuvor unvorhergesehene Ursachen anzugehen. Die Ansätze der Ursachenanalyse variieren, aber meistens basieren sie auf vier Prinzipien: 1. die Ursachen eines Ereignisses identifizieren, 2. die Zeitachse vom Normalbetrieb bis zum Risikoereignis festlegen, 3. Unterscheidung zwischen den tieferliegenden Ursachen und den unmittelbareren Ursachen, 4. die Nutzung der Ergebnisse, um die Gefährdung und die Effektivität der Kontrolle zu bewerten, Oft werden die Ursachen eines Ereignisses, sowie die Reihenfolge, in der die Ursachen auftreten können mit Hilfe der Technik der ‚Fünf Warums' identifiziert. Dabei werden Warum-Fragen gestellt, wie z.B.: 1. Warum ist ein Brand entstanden? Weil brennbares Material zu brennen begann. 2. Warum hat das Material gebrannt? Weil ein Funke das Material in Brand gesetzt hat. 3. Warum ist der Funke entstanden? Weil ein elektrischer Fehler in der Verkabelung des Gebäudes auftrat. 4. Warum ist der elektrische Fehler aufgetreten? Weil die Verkabelung alt war. 5. Warum war die Verkabelung alt? Weil die Verkabelung nicht sicherheitsüberprüft war. Es können mehr oder weniger als fünf Warum-Fragen verwendet werden, um die Ursache zu finden, normalerweise ist es jedoch möglich, mit 5 Fragen zum zugrundeliegenden Prozessfehler zu gelangen. In diesem Beispiel könnten noch weitere Fragen verwendet werden, um z.B. herauszufinden, warum eine Sicherheitsinspektion nicht durchgeführt wurde. Die Ursachenanalyse ist zeitaufwändig und es ist selten praktisch oder kosteneffektiv, sie für alle RSAs zu verwenden, sie ist aber eine gute Technik für die Bewertung der wichtigsten operationellen Risiken eines Unternehmens.

Tabelle 8: Andere Ansätze zur RSA-Datensammlung

5. Integration eines RSAs in das OpRisk-Rahmenwerk

Das RSA ist kein eigenständiger Prozess. Um effektiv zu sein, muss er in das breitere Rahmenwerk für das Management operationeller Risiken integriert werden. Dies bedeutet, dass andere Elemente des Rahmenwerks genutzt werden, um Informationen zur Unterstützung der RSA-Erstellung bereitzustellen. Es bedeutet auch, dass die Ergebnisse der RSAs genutzt werden, um andere Elemente zu unterstützen, insbesondere die Berichterstattung zum operationellen Risiko.

5.1. Verbindung mit internen und externen Verlustdaten

Externe und interne operationelle Verlustdaten können zur Unterstützung von RSAs auf zwei Arten verwendet werden:

- Zur Unterstützung der Bewertung des Restrisikos und der Kontrolleffektivität
- Zur Validierung der Bewertungen des Restrisikos und der Wirksamkeit der Kontrollen

Umfang und Häufigkeit tatsächlicher Verlustereignisse geben einen Hinweis darauf, was in Zukunft passieren könnte, wenn die aktuellen Trends unverändert bleiben. Ebenso können operationelle Verlustereignisse oft mit spezifischen Kontrollfehlern oder Lücken in der Kontrollumgebung in Verbindung gebracht werden, was Aufschluss über die Wirksamkeit der Kontrollen gibt.

Wo RSA-Ergebnisse signifikant von den verfügbaren internen oder externen Verlustdaten abweichen, können zusätzliche Validierungen erforderlich sein. Diese sollten sowohl die Genauigkeit des RSA-Ergebnisses als auch die Effektivität der Verlustdatensammlung berücksichtigen. Es kann zum Beispiel sein, dass ein hohes Niveau des vorhergesagten Restrisikos im Verhältnis zu den gemeldeten Verlustereignissen das Ergebnis einer Verzerrung in der Bewertung ist, oder es könnte sein, dass die Verlustdaten unvollständig sind.

5.2. Szenarioanalyse

Signifikante Kontrollschwächen und Risikopositionen, die durch ein RSA identifiziert werden, sind eine wertvolle Quelle für die Szenarioanalyse. Ebenso kann der Prozess der Definition und Bewertung von Risikoszenarien zur Identifizierung von operationellen Risiken und Kontrollschwächen führen, die derzeit nicht im RSA erfasst sind.

Die Szenarioanalyse kann besonders hilfreich sein, wenn es darum geht, das inhärente Risiko zu bewerten, sofern es erfasst wurde. Durch die Berücksichtigung der potenziellen Ursachen und Folgen eines größeren Kontrollversagens kann ein strukturierter Ansatz für die Analyse von Szenarien zu fundierteren Schätzungen des inhärenten Risikos führen.

Es ist selten praktisch oder kosteneffektiv, die Szenarioanalyse für jede Bewertung des inhärenten Risikos zu verwenden. Sie kann jedoch ein nützliches Werkzeug zur Validierung besonders hoher Werte für das inhärente Risiko sein.

Weitere Informationen finden Sie im IOR-Praxisleitfaden “Operational Risk Szenarien”.

5.3. RSA-Ergebnisbericht

Es gibt verschiedene Möglichkeiten, die Ergebnisse von RSAs zu berichten. In der Regel wird eine Kombination verschiedener Formate erforderlich sein - je nach Adressatenkreis des Berichts:

- Beschreibende Berichte (Beschreibungen der verschiedenen Risikoexpositionen und

eventueller Kontrollschwächen, können in Form eines Risikoregisters dargestellt werden)

- Risikolandkarten/Ampelberichte (siehe Anhang B)
- Dashboards (Risiko-, Kontrolleffektivitäts- und Leistungsindikatoren, in der Regel unter Verwendung von Trenddiagrammen, Tortendiagrammen usw. dargestellt)
- Nutzenprotokoll (ein Protokoll aller Verbesserungen, die an der Kontrollumgebung vorgenommen wurden, wie z.B. verbesserte Kontrolleffektivität, Beseitigung veralteter Kontrollen sowie die Auswirkungen dieser Maßnahmen in Form von reduzierten Betriebskosten, verbesserter Effizienz usw.)

Allgemein sollten weniger Details berichtet werden, je höher die Ebene des Adressatenkreises ist. Für das Leitungsorgan und die oberste Führungsebene sollte der Schwerpunkt auf den wichtigsten Risikobereichen/Kontrollschwächen liegen, die das größte Potenzial haben, dem Unternehmen zu schaden und es daran zu hindern, seine Ziele zu erreichen.

Umgekehrt kann die Berichterstattung für Linienmanager mehr Details enthalten, da die zusätzlichen Informationen für sie hilfreich sein können, um die beste Vorgehensweise zu bestimmen und den Fortschritt von Maßnahmen anhand von vereinbarten Meilensteinen und Ergebnissen detailliert zu überwachen. Außerdem sollte unabhängig von der Ebene der Zielgruppe darauf geachtet werden, dass die Berichterstattung sachdienlich und adressatengerecht für die Zielgruppe ist, für die sie bestimmt ist.

Die Führung eines Nutzenprotokolls wird dringend empfohlen. Diese Protokolle können verwendet werden, um die Akzeptanz im Unternehmen zu verbessern und so die Pünktlichkeit und Genauigkeit der RSAs zu erhöhen. Ein solches Protokoll bietet eine greifbare Aufzeichnung darüber, warum RSAs eine lohnende Übung sind, die dem Unternehmen einen Mehrwert bringen können.

5.4. Maßnahmen

Die Ergebnisse des RSA sind eine wertvolle Informationsquelle für die Entwicklung von Maßnahmen für operationelle Risiken. Solche Pläne können die Verbesserung der Wirksamkeit bestehender Kontrollen, die Beseitigung veralteter Kontrollen oder die Einführung neuer Kontrollen zur Schließung von Lücken in der Kontrollumgebung beinhalten.

Maßnahmen müssen immer unter Kosten-Nutzen-Gesichtspunkten gerechtfertigt werden. Nur weil eine Kontrolle “effektiver” gemacht oder eine neue Kontrolle hinzugefügt werden könnte, heißt das nicht, dass der dafür erforderliche Aufwand notwendig ist. Es lohnt sich zum Beispiel nicht, 1 Million Pfund auszugeben, um eine Kontrolllücke zu beheben, die mit einem Verlustrisiko von 100.000 Pfund bewertet wird. Ebenso muss immer bedacht werden, dass eine Erhöhung des Kontrollniveaus die Effizienz von Systemen und Prozessen verringern kann und sogar zu unvorhergesehenen neuen Risiken führen kann. Beispielsweise kann eine deutliche Erhöhung der Häufigkeit von IT-Passwortänderungen dazu führen, dass Mitarbeiter ihre Passwörter aufschreiben und dann verlieren.

Bei der Entscheidung über die Art der Maßnahmen ist es hilfreich, sich an die vier üblichen Reaktionen auf Risikoexpositionen zu erinnern:

- Akzeptanz - es werden keine weiteren Maßnahmen ergriffen, entweder, weil das Restrisiko innerhalb des Risikoappetits liegt oder die Kosten für zusätzliche Kontrollen im Verhältnis zum erzielten Nutzen zu hoch sind
- Mitigierung - dies beinhaltet die Verbesserung des Kontrollniveaus (Verbesserung der Kontrolleffektivität oder Einführung neuer Kontrollen), um die Wahrscheinlichkeit (Verlustvermeidung) und/oder die Auswirkungen des Risikos (Verlustreduzierung) zu verringern

- Übertragung - dies kann die finanzielle Übertragung des Risikos auf einen Versicherer oder die physische Übertragung des Risikos auf einen externen Dienstleister beinhalten[1]
- Vermeidung - wenn Änderungen an einer Tätigkeit, einem Prozess oder einem System vorgenommen werden, um die inhärente Risikoexposition zu reduzieren.

Alle Maßnahmen müssen spezifizieren, was von wem und bis wann zu tun ist. Der Fortschritt bei der Umsetzung von Maßnahmen sollte bis zur Fertigstellung überwacht werden. Je nach Bedeutung der Maßnahme kann der Fortschritt durch das Leitungsorgan, einen vom Vorstand beauftragten Ausschuss, die (operationelle) Risikofunktion oder das lokale Management überwacht werden.

5.5. Prüfungsplanung und Bericht der Internen Revision

Die Verwendung des RSA-Outputs durch die Interne Revision kann eine Reihe von Vorteilen mit sich bringen:

- Durch die Übernahme von mehr Verantwortung für die Aufrechterhaltung des Kontrollumfelds sollten geprüfte Einheiten den Zweck des operationellen Risikomanagements und den Nutzen einer wirksamen Bewertung und Kontrolle besser verstehen.
- Bereitstellung zusätzlicher Informationen zur Unterstützung der Prüfungsarbeit (z.B. die Validierung von Schätzungen zur Kontrollwirksamkeit)
- Gefährdungsbeurteilungen können zur Unterstützung eines risikobasierten Ansatzes für die Interne Revision genutzt werden.

Es wird außerdem empfohlen, dass die Interne Revision regelmäßig die Wirksamkeit des RSAs überprüft, um sicherzustellen, dass es wirksam und verhältnismäßig bleibt.

[1] In einigen Branchen, wie z.B. im Finanzdienstleistungssektor, können Unternehmen bestimmte Risiken nicht vollständig auf externe Dienstleister übertragen und müssen für alle auftretenden operationellen Verluste und die Effektivität des Betriebsrisikorahmens des Dienstleisters verantwortlich bleiben. Es wird empfohlen, dass die Leser ihre lokalen Anforderungen überprüfen, bevor sie versuchen, Dienstleister für die Übertragung von operationellen Risiken zu nutzen.

6. Fazit

Ein effektiver RSA-Ansatz ist ein wichtiger Bestandteil der meisten Rahmenwerke für das operationelle Risikomanagement. Wenn er jedoch schlecht konzipiert und umgesetzt ist, können die Ergebnisse mehr schaden als nutzen. Wie jedes Instrument des Managements operationeller Risiken muss auch ein effektives RSA einen Mehrwert bieten und darf keine bürokratische, auf die Einhaltung von Vorschriften ausgerichtete Übung sein, bei der man nur Kästchen abhakt. Übermäßige Komplexität oder Vorschriften können zu einem Prozess führen, bei dem die Kosten den Nutzen übersteigen. Experten für operationelle Risiken sollten immer daran denken, dass RSAs die geschäftliche Entscheidungsfindung unterstützen müssen.

Anhang A: Beispiel einer RSA-Vorlage

Beispiele für RSA-Vorlagen finden Sie unten.

1. Beispiel für eine Excel basierte Vorlage (einfach)

Nr.	Risikobeschreibung	Risikoverantwortlicher	Inhärentes Risiko	Schlüsselkontrollen	Kontrollverantwortlicher	Restrisiko	Innerhalb des Risikoappetits?	Maßnahme erforderlich?
12c	Erhebliche Störung des normalen Betriebsablaufs	M Smith	Hoch	- Notfallpläne vorhanden - Pläne werden jährlich getestet und aktualisiert - Telefonanrufkaskade vierteljährlich getestet	J Brown	Mittel	Nein	Ja
13a	Verletzung der Vertraulichkeit von Kundendaten	F Jones	Hoch	- Datenschutzrichtlinie ist vorhanden und wird regelmäßig überprüft - Unabhängige Überwachung der Einhaltung der Richtlinie - Eskalation bei Nichteinhaltung - Register für Verstöße	S Thomas	Niedrig	Ja	Nein

Weitere Felder können ergänzt werden, siehe 3.1 oben.

2. Beispiel für einen RSA-Aktionsplan

Nr.	Risikobeschreibung	Restrisiko	Erforderliche Maßnahme	Verantwortlicher für die Maßnahme	Zieldatum	Erwartetes Restrisiko
Außerhalb des Risikoappetits						
12c	Erhebliche Störung des normalen Betriebsablaufs	Mittel	Einführung von Desktop-Walkthrough-Übungen zweimal jährlich	J Brown	30.09.2020	Niedrig

3. Beispiel für einen Fragebogenauszug

Beispielauszug aus einem Fragebogen, der die Zugriffskontrollen innerhalb einer IT-Administrationsfunktion untersucht. Der Kommentarbereich kann dazu verwendet werden, eine Begründung für die gegebene Antwort zu liefern, einschließlich konkreter Beweise.

Frage	Ja	Nein/ nicht relevant	Kommentar falls nein/ nicht relevant
1. Zugangskontrolle			
1.1 Sind Sie davon überzeugt, dass Ihre Admin-IT-Hardware und -Software so sicher wie möglich untergebracht ist und angemessene Sicherheitsmaßnahmen getroffen werden, um Diebstahl zu verhindern (z. B. Sicherheitskennzeichnung der Hardware)?			
1.2 Ist eine schriftliche Genehmigung erforderlich, bevor Mitarbeiter Hardware oder sensible Daten außer Haus bringen dürfen?			
1.3 Haben Sie ein formales Verfahren, um den Computerzugang zu erfassen, zu genehmigen und regelmäßig zu überprüfen?			
1.4 Spiegeln die den Mitarbeitern zugewiesenen Zugriffsebenen nur das wider, was sie für die Ausführung ihrer Arbeit benötigen?			
1.5 Ist Ihr Admin-Netzwerk rein einrichtungsintern, d. h. hat es keine externen Verbindungen (z. B. zum Internet oder Einwahlmöglichkeiten)?			
1.6 Befinden sich Ihre Admin-Rechner und Ihre übrigen Rechner in getrennten Netzwerken?			
1.7 Sind Sie sicher, dass alle angemessenen Sicherheitsmaßnahmen ergriffen wurden, um den unbefugten Zugriff auf Ihr Admin-Netzwerk zu verhindern (entweder intern oder durch externen Zugriff)?			
1.8 Sind die Mitarbeiter angewiesen, die IT-Ausrüstung oder Software der Admin nicht zu benutzen, wenn sie nicht dazu autorisiert sind?			
1.9 Erhalten die Mitarbeiter eine gute Anleitung zur Passwortsicherheit (Passwortlänge, Änderungshäufigkeit usw.)?			
1.10 Gibt es Verfahren, die sicherstellen, dass Besucher angemessen begleitet werden, während sie sich auf dem Betriebsgelände befinden?			

4. Beispiel RSA Ende zu Ende Prozessbewertungsvorlage

Lieferant und Standort		
Kontakt beim Lieferanten		
Untersuchte Dienstleistung		
	Risiko *(Definition des verbundenen Risikos)*	**Vorproduktion** *Vorproduktion bezieht sich auf Aktivitäten, die vor Erstellung des Produkts oder der Dienstleistung auftreten, die beim Lieferanten beschafft werden*
1	Nichteinhaltung der vorvertraglichen Leistungen durch den Lieferanten	Enthält die Qualitätsakte alle spezifischen benötigten Dokumente? *Eine Liste der Dokumente findet sich in den Lieferantenanforderungen, d.h. Dokumente zur Entwurfsprüfung*
2		Wie bezieht der Lieferant das Lernen aus der Praxiserfahrung in seine Ingenieurtätigkeit ein?
3		Hat der Lieferant einen gut definiertes Ablaufdiagramm seiner Prozesse?
4		Wurde der Kontrollplan eingereicht und akzeptiert? *Prüfen, ob die letzte Überarbeitung berücksichtigt wurde*
5		Wurden Engpässe identifiziert und adressiert?
		Sub-Lieferanten Management
6	Mangel an ausreichenden Lieferantenkontingenten zur Sicherstellung der Lieferung	Hat der Lieferant einen wirksamen Prozess für die Zulassung von Sub-Lieferanten? *Den Antrag auf Korrekturmaßnahmen des Unterlieferanten prüfen*
7		Wurden alle vom Sub-Lieferanten gekauften Teile, Materialien und Dienstleistungen durch den Lieferanten in einem formalen Prozess zugelassen? *Erstmusterprüfberichte für jede Komponente und jedes Material prüfen*
8		Hat der Lieferant im Falle eines Sub-Kontrakts den Prozess des Sub-Lieferanten geprüft und liefert der Sub-Lieferant einen Konformitätsbericht an den Lieferanten?
9		Führt der Lieferant eine Eingangskontrolle durch? Wird sie gemäß dem Kontrollplan durchgeführt? *Werden Nichtkonformitäten effektiv im Korrekturmaßnahmensystem behandelt?*
10		Wie dokumentiert der Lieferant den Erhalt von Materialien und Dienstleistungen? *Quittungen sind im lokalen Business System und beinhalten Menge, Chargennummern, Eingangsdatum,... Informationen, die die Rückverfolgbarkeit von Teilen unterstützen*
11		Gibt es einen Prozess für die Leistung des Sub-Lieferanten - Qualität, Lieferung, Überwachung - der definiert ist und zur Verbesserung genutzt wird? *Prüfen Sie auch die Kriterien und die Reaktionsfähigkeit der Sub-Lieferanten bei Kundenreklamationen, Korrekturmaßnahmen der Sub-Lieferanten*
		Produktion/ Ausführung der Dienstleistung
12	Mangel an adäquaten Qualitätsprüfungsprozessen Dritter	Werden alle besonderen Merkmale durch eine Fehlersuche oder Prozesskontrollmethoden wie statistische Prozesskontrolle überprüft? *Anwendbar, wenn die Komponente besondere Merkmale aufweist.* *Wenn nicht durch Fehlersuche kontrolliert, sind Einschließungspläne und Korrekturmaßnahmen vorhanden? Ist dies im Kontrollplan dokumentiert?*
13		Sind vom Kunden freigegebene Erstmuster an den gewünschten Arbeitsplätzen vorhanden? *Zutreffend, wenn dies angefordert wurde*
14		Entspricht die in der Produktion verwendete Verpackung den Sicherheitsanforderungen? Schützt sie effizient Komponenten und Materialien?
15		Gibt es ein Entsorgungssystem für zurückgewiesenes Material/ Komponenten? *Prüfen Sie, ob die Behälter zur einfachen Identifizierung mit einem Farbcode gekennzeichnet sind.*
16		Wie überwacht der Lieferant die Effektivität der Prozesse und setzt Änderungen zur Verbesserung um?
		Logistik
17	Nicht adäquate Service Level Agreements oder Fehlen spezifischer Bedingungen und Konditionen	Ist der Lieferant in der Lage, Bestellfreigaben und Liefertermine zu empfangen und zu verstehen? *EDI- oder Web-Verbindungen prüfen - den Lieferanten bitten, die letzte Freigabe zu überprüfen*
18		Sind die Verpackungs- und Versandanweisungen an den Arbeitsplätzen deutlich sichtbar angebracht und sind sie den Betrieben bekannt? *Prüfen, ob sie mit dem Produkt-/Prozesskontrollplan übereinstimmen. Beschreiben sie ausreichend, wie vorzugehen ist, welche Arbeitsschritte durchzuführen sind und was zu prüfen ist? Kundenreklamationen/Gewährleistungsansprüche aus Fehlern bei Verpackung und Versand prüfen*

Anhang B: Beispiel für eine RSA-Risikolandkarte für die Geschäftsleitung

Eine typische Heatmap für die Bewertung von OpRisk-Wahrscheinlichkeit und Auswirkung

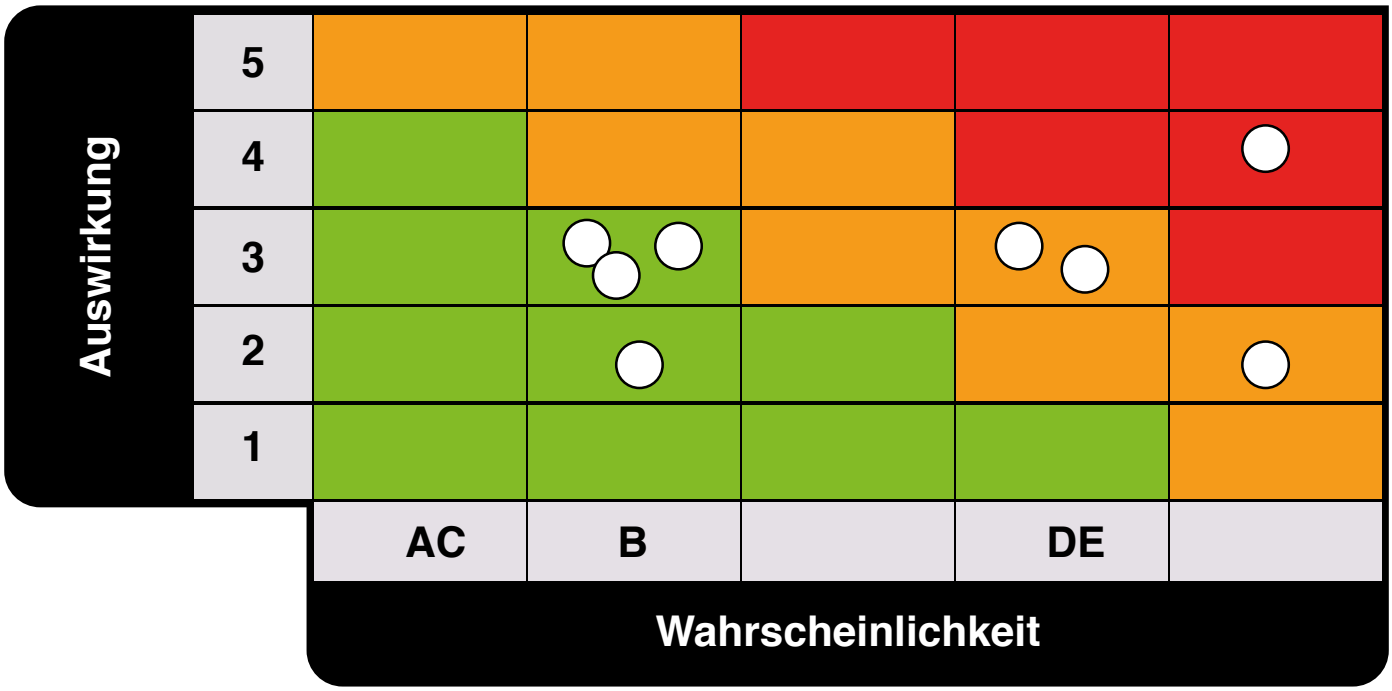
Dies ist ein Beispiel – die Kalibrierung der Skalen sollte proportional zum jeweilig betroffenen Punkt des Assessments sein

WAHRSCHEINLICHKEIT (des Auftretens eines Risikos innerhalb einer bestimmten Zeitspanne)

A – Kaum (alle 10-25 Jahre) B – Unwahrscheinlich (alle 5-10 Jahre) C –Möglich (alle 1-5 Jahre) D-Wahrscheinlich (einmal pro Jahr) E – Häufig (mehrmals pro Jahr)

AUSWIRKUNG (hier aus der finanziellen Perspektive, könnte jedoch auch als Kunden- oder Reputationswirkung gemessen werden)

1= GBP 10.000 – 100.000 2=GBP 100.000-1 Mio. 3= GBP 1 Mio. - 5. Mio. 4= GBP 5 Mio. – 10 Mio. 5= GBP > 10 Mio.



www.theirm.org

irm

Developing risk professionals