

» Ultimativer Leitfaden: **Compliance-Risikoanalyse** leicht gemacht «



Inklusive
kostenloser
Excel-Vorlage zur
Compliance-
Risikoanalyse

Tipps, wie Sie erfolgreich eine Analyse der Compliance-Risiken in Ihrem Unternehmen durchführen – vom initialen Erfassen und Bewerten der Risiken, dem Festlegen von Strategien und Maßnahmen bis hin zur laufenden Überprüfung der Risikolandschaft

Inhalt

03

Einführung

Risikoanalyse als Grundlage jedes Compliance-Programms

04

Was sind Compliance-Risiken überhaupt?

05

Identifikation und Analyse der Compliance-Risiken

Verschiedene Ansätze: Top-down und Bottom-up
Top-Down-Ansatz: Identifizieren erster Risikofelder
Typische Rechtsfelder mit Compliance-Risiken
Bottom-Up-Ansatz: Durchführen von Interviews und Workshops

11

Erfassen der Compliance-Risiken

Die Bewertung des Risikos
Maßnahmen zur Risikoreduzierung

17

Laufende Überprüfung der Compliance-Risiken

19

Digitale Unterstützung für die Compliance-Risikoanalyse

Die Integration in das allgemeine Risikomanagement

22

Die Auswertung der Compliance-Risikoanalyse

Der Risiko-Bericht: Regelmäßig, präzise, auf das Wesentliche konzentriert
Risiko-Heatmaps und -Matrizen
Risiko-Landkarten

25

Fazit

26

Zusätzliche Ressourcen

26

Über EQS Group

Einführung

Aller Anfang ist schwer – das gilt insbesondere, wenn es um die Einrichtung eines effektiven Compliance-Systems geht. Selbst wenn Unternehmen noch relativ am Anfang ihrer Compliance-Bemühungen stehen, wurden häufig bereits erste Compliance-Maßnahmen implementiert: Richtlinien sind geschrieben, Schulungen werden durchgeführt und Kontrollprozesse eingerichtet. Was jedoch häufig fehlt – und eigentlich am Beginn stehen sollte – ist die Compliance-Risikoanalyse.

Die gängigen Compliance-Frameworks (ISO 19600, IDW PS 980) sowie die relevanten internationalen Regularien und deren Leitlinien (wie DoJ-Guidelines oder der UK Bribery Act) sind sich einig: Eine umfassende Compliance-Risikoanalyse sollte das Fundament eines jeden Compliance-Programms bilden. Ohne die Analyse der Risiken laufen Unternehmen Gefahr, falsche Schwerpunkte zu setzen, ineffektive Maßnahmen einzusetzen und möglicherweise relevante Risiken völlig außer Acht zu lassen.

Risikoanalyse als Grundlage jedes Compliance-Programms

In den wichtigsten Compliance-Frameworks und internationalen Antikorruptions-Gesetzgebungen wird die Risikoanalyse als essenzieller Teil des Compliance-Programms diskutiert. Einige Beispiele:

- **ISO 19600¹:** In dieser ISO-Norm, nach der Compliance-Systeme auch zertifiziert werden können, bilden das Identifizieren, Analysieren und Bewerten von Compliance-Risiken einen besonderen Schwerpunkt.
- **IDW PS 980:** Der Prüfstandard 980 des Instituts der Wirtschaftsprüfer definiert sieben Grundelemente eines Compliance Management Systems – die Erfassung und Analyse der Compliance-Risiken ist eines davon.
- **FCPA/DoJ-Guidelines²:** Das US-Justizministerium nennt in seinem Leitfaden zur „Evaluation of Corporate Compliance Programs“ die Compliance-Risikoanalyse als ersten Punkt. Strafverfolger sollen hinterfragen, ob Unternehmen ihr Risikoprofil „identifiziert, beurteilt und definiert“ haben.
- **UK Bribery Act³:** Ähnlich wie der FCPA, stuft auch das britische Justizministerium die Risikoanalyse und deren laufende Aktualisierung als höchst relevant ein.
- **Sapin II⁴:** Das seit 2018 geltende französische Antikorruptionsgesetz Sapin II sieht eine strukturierte und vor allem regelmäßig aktualisierte Betrachtung der Korruptionsrisiken ebenfalls als essenziell an.

¹ Vgl. Fissenewert, Prof. Dr. Peter (2015): ISO 19600. Der neue Standard zur Zertifizierung von Compliance-Management-Systemen, in: ZRFC – Risk, Fraud & Compliance, S. 199.

² Vgl. U.S. Department of Justice, Criminal Division (2019): Evaluation of Corporate Compliance Programs

³ UK Ministry of Justice: The Bribery Act 2010. Quick start guide

⁴ Vgl. White & Case LLP (2017): Update on Spain II law, in

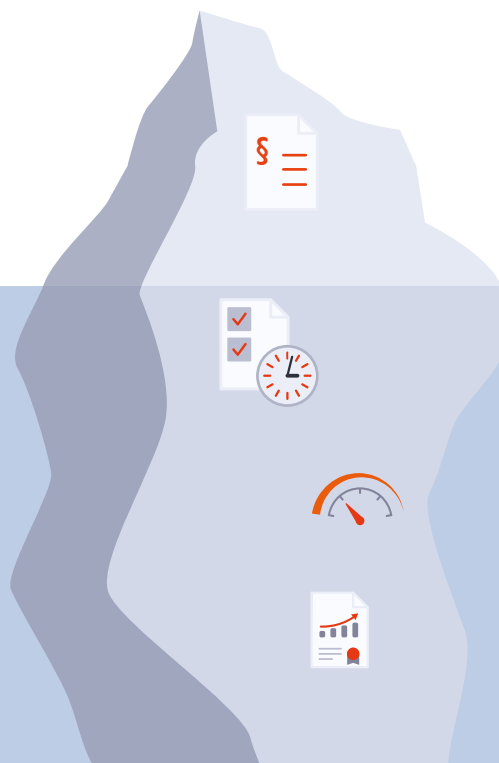
Was sind Compliance-Risiken überhaupt?

Compliance ist die Bemühung, regelkonformes Verhalten herzustellen. Dazu zählt die „klassische“ Einhaltung geltender nationaler und internationaler Gesetze und Regularien, aber auch die Erfüllung ethischer und moralischer Grundsätze, die beispielsweise im Code of Conduct des Unternehmens festgehalten sind. Ein Compliance-Risiko besteht, wenn eine Organisation Gefahr läuft, gegen Regeln aus diesen beiden Bereichen zu verstoßen.

Welche Risiken das genau sind, ist von Unternehmen zu Unternehmen sehr unterschiedlich. Und auch die potenziellen Folgen können sehr verschieden sein: Sanktionen, Schadenersatzforderungen, Geldstrafen oder Haftstrafen sind denkbar, aber auch massive Reputationsverluste – Beispiele dafür finden sich zuhauf in der jüngeren Wirtschaftsgeschichte.

Letztlich ist die Compliance-Risikoanalyse vor allem ein Werkzeug zur Steigerung der Effektivität des Compliance-Programms. Das Wissen über relevante Risiken und mögliche negative Konsequenzen hilft dabei, Compliance-Ressourcen optimal einzusetzen und gegebenenfalls mehr Ressourcen einzuplanen. Somit ist die Risikoanalyse auch ein wichtiger Nachweis der effektiven und effizienten Ausgestaltung des Compliance-Programms – nicht nur gegenüber Wirtschaftsprüfern und Strafverfolgern, sondern auch gegenüber den internen Stakeholdern.

Dieser Leitfaden soll Unternehmen dabei helfen, ihre Compliance-Risikoanalyse und das kontinuierliche Management der Compliance-Risiken effizient umzusetzen. Er richtet sich sowohl an Unternehmen, die noch kein initiales Risiko-Assessment durchgeführt haben – als auch an Unternehmen, die ihre aktuelle Risikoanalyse auf den Prüfstand stellen möchten



Identifikation und Analyse der Compliance-Risiken



Verschiedene Ansätze: Top-down und Bottom-up

Wenn in Ihrem Unternehmen noch keine Compliance-Risikoanalyse durchgeführt wurde (oder sich seit der letzten Analyse viel verändert hat), stellt sich die Frage: Wo anfangen?

Grundsätzlich lässt sich zwischen dem Top-down- und dem Bottom-up-Ansatz unterscheiden:

Top-down

Analyse der Compliance-Risiken ausgehend vom Management, Strategien und Geschäftsmodellen

Bottom-up

Analyse der Compliance-Risiken durch Workshops und Interviews mit den im Tagesgeschäft tätigen operativen Einheiten

In der Praxis bietet sich eine Kombination beider Ansätze an. Denn feststeht: Sie können als Compliance-Verantwortlicher nicht alle unternehmensrelevanten Compliance-Risiken kennen, und je nach Unternehmensgröße und -struktur kann auch das Management zu weit von den konkreten Situationen und Fragestellungen der operativen Einheiten entfernt sein. Daher: Nutzen Sie unbedingt die Möglichkeit, verschiedene Wissensquellen anzuzapfen.



Top-Down-Ansatz: Identifizieren erster Risikofelder

Um grundsätzliche Risikobereiche im Unternehmen festzulegen, gibt es einige Fragen, an denen Sie sich orientieren können:

- Welche Gesetze und Regularien sind für Ihr Unternehmen relevant?
- Welche Produkte stellt das Unternehmen her, welche Dienstleistungen bietet es an?
- Welche branchenspezifischen Risiken kommen zum Tragen?
- In welchen Ländern ist das Unternehmen direkt oder indirekt tätig?
- Welche konkreten Geschäftsmodelle kommen in welchen Einheiten zum Einsatz

Um diese Fragen zu beantworten, kann eine Vielzahl an internen und externen Quellen genutzt werden:

Intern:

- Geschäftsberichte
- Pressemitteilungen
- Organisationshandbücher
- Prüfberichte
- Interne Meldungen und Compliance-Anfragen

Extern:

- Brancheninformationen
- Korruptionsindizes
- Compliance-Vorfälle bei Wettbewerbern
- Gerichtsentscheide
- Jahresberichte oder sonstige Veröffentlichungen von NGOs (Transparency International, o.ä.)

Mit Hilfe des Top-Down-Ansatzes sollte ein erstes, ungefähres Bild entstehen, wo die relevantesten Compliance-Risiken liegen könnten – und wo es sich lohnt, genauer hinzuschauen. Denn auch die Compliance-Risikoanalyse selbst kann und sollte risikobasiert erfolgen. Beginnen Sie anschließend mit Ihren Workshops und Interviews in den Geschäftseinheiten, in denen am ehesten Probleme auftreten können. Anschließend fahren Sie mit weniger risikobehafteten Bereichen fort.

Typische Rechtsfelder mit Compliance-Risiken

Jedes Unternehmen muss eine nahezu endlose Zahl an Gesetzen und Regularien beachten. Auch wenn sich hier kaum verallgemeinern lässt, gibt es doch einige Gesetzesgruppen, die häufig mit besonders hohen Schadensrisiken einhergehen

- | | |
|--|-----------------------------------|
| ■ Antikorruptionsgesetze | ■ Arbeitsrecht |
| ■ Kartell- und Wettbewerbsrecht | ■ Sozialversicherungsrecht |
| ■ Geldwäschegesetze | ■ Produktsicherheitsrecht |
| ■ Buchhaltungs- und Rechnungslegungsvorschriften | ■ Beihilfe- und Fördermittelrecht |
| ■ Datenschutzrecht | ■ Gesellschaftsrecht |
| ■ Exportkontrolle | ■ Umweltrecht |

Manche Compliance- oder Juristenverbände bieten noch umfangreichere Risikokataloge an, die beim strukturierten Erfassen der Compliance-Risiken nach Rechtsgebieten helfen können⁵.

⁵ In Deutschland beispielsweise das Deutsche Institut für Compliance (DICO)

Bottom-Up-Ansatz: Durchführen von Interviews und Workshops

Sobald mit Hilfe des Top-Down-Ansatzes erste Risikofelder identifiziert sind, sollten diese mit Hilfe von Gesprächen mit den operativen Einheiten validiert bzw. konkretisiert werden (Bottom-up-Ansatz). Doch wer sollte befragt werden und welche Fragen stellt man am besten?

Natürlich hängt die Auswahl der Interviewpartner sehr vom konkreten Unternehmen und den identifizierten Risikofeldern ab. Geeignete Ansprechpartner können sein:

- Compliance-Abteilung
- Rechtsabteilung
- Interne Revision
- Datenschutzbeauftragter
- Einkauf und Vertrieb
- IT
- Personalabteilung

Grundsätzlich zu beachten: Für die allermeisten operativ tätigen Mitarbeiter sind Themen wie Kartellrecht, Geldwäsche und möglicherweise sogar Korruptionsgesetze sehr abstrakt. Der Bezug zur eigenen Tätigkeit ist zunächst nicht erkennbar – auch wenn er durchaus bestehen kann.

Daher lohnt es sich, auf Compliance-Seite eine gewisse Übersetzungsleistung zu leisten: Konkrete Szenarien machen es den Personen im operativen Geschäft wesentlich leichter, Fragen zu beantworten. Kann es vorkommen, dass auf einem Kongress mit Wettbewerbern über die Preisgestaltung gesprochen wird? Machen wir Geschäfte mit Amtsträgern, und falls ja, sind hier manchmal besondere Gebühren oder Gefälligkeiten im Spiel?

Solche Szenarien und daraus abgeleitete Fragen können mit Hilfe der bereits erwähnten internen und externen Quellen im Vorfeld vorbereitet werden. Dennoch empfiehlt es sich, bei den Interviews offen zu bleiben: Gut möglich, dass ein ganz anderes Risiko im operativen Geschäft besteht, das sich aus keinem Geschäftsbericht oder Strategiepapier herauslesen lässt.

Persönliche Interviews oder Online-Fragebögen?

Gerade wenn die erstmalige Erfassung der Compliance-Risiken ansteht, kann es verlockend sein, einen standardisierten Fragebogen als Online-Umfrage aufzusetzen und mit einem Klick an alle zu befragenden Personen zu schicken. Und natürlich sind Online-Fragebögen eine prima Möglichkeit, strukturiert Informationen von einer Vielzahl von Teilnehmern zu erheben.

Dennoch spricht vieles dafür, insbesondere zu Beginn der Compliance-Risikoanalyse, persönliche Interviews und Workshops durchzuführen. Mit standardisierten Fragebögen laufen Sie Gefahr, möglicherweise relevante Themen nicht zu erfassen, die im Rahmen eines explorativen Interviews aufgekommen wären. Denn häufig kommen in persönlichen Interviews Themen und Risiken zur Sprache, die sich aus der Lektüre der zuvor erwähnten Quellen nicht ableiten ließen.

Dennoch können Online-Fragebögen eine gute Ergänzung sein: Beispielsweise für die quantitative Validierung eines möglichen Risikos oder zur Überprüfung, ob ein in einem Geschäftsbereich identifiziertes Risiko auch in anderen Geschäftsbereichen besteht

Externe Unterstützung für die Compliance-Risikoanalyse

Je nach Komplexität des Unternehmens und der zur Verfügung stehenden Ressourcen kann eine erstmalige Compliance-Risikoanalyse ein größeres Unterfangen werden. Sollten Sie feststellen, dass Ihnen das Projekt über den Kopf wächst, können Sie externe Hilfe hinzuziehen. Viele Anwaltskanzleien, auf Compliance-Themen spezialisierte Beratungsfirmen oder auch die „Big Four“ der Wirtschaftsprüfer bieten hier ihre Dienste an.

Wichtig: Lassen Sie sich nicht dazu verleiten, das Thema nach einem Initialprojekt abzuhaken – das Management der Compliance-Risiken ist eine kontinuierliche Aufgabe.



Erfassen der Compliance-Risiken

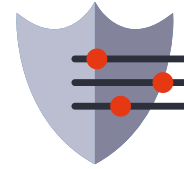


Sobald sich durch die geschilderten Ansätze die ersten konkreten Compliance-Risiken herauskristallisieren, wird es Zeit, diese strukturiert zu erfassen. Hierfür müssen Sie das Rad nicht neu erfinden – es existieren viele Vorlagen, die eine Grundstruktur für die Erfassung der Compliance-Risiken bereitstellen. In der Regel geht es um die Erfassung folgender Eigenschaften:

- Risikobetreff
- Beschreibung/Szenario
- Risiko-Owner
- Rechtsgebiet(e)
- Geschäftseinheit(en)
- Geschäftsprozess(e)
- Brutto-Risiko
- Eintrittswahrscheinlichkeit
- Schadenshöhe
- Risikobewertung
- Risikostrategie
- Maßnahmen
- Name der Maßnahme
- Beschreibung
- Maßnahmen-Owner
- Netto-Risiko
- Eintrittswahrscheinlichkeit
- Schadenshöhe
- Risikobewertung

Risikobetreff	Eine stark komprimierte Kurzbezeichnung des Risikos.
Beschreibung/Szenario	Das Compliance-Risiko ggf. als konkretes Szenario im Detail beschrieben, ggf. mit zusätzlichen Dokumenten versehen.
Risiko-Owner	Die Person im Unternehmen, die für die laufende Überwachung des Risikos verantwortlich ist. Das kann ein Compliance-Verantwortlicher sein, aber auch jemand aus dem operativen Geschäft (IT-Leiter, o. ä.).
Rechtsgebiet(e)	Ein oder mehrere Rechtsgebiete, aus denen das Risiko resultiert. Das können abstrakte Rechtsgebiete (wie „Geldwäschegesetz“) sein, oder konkrete Regularien (wie „Sapin II“), wobei letztere ggf. häufigeren Änderungen unterworfen sind.
Geschäftseinheit(en)	Die Geschäftseinheit(en), in denen das Risiko besteht. Das können formelle Tochtergesellschaften oder auch künstlich gebildete „business lines“ sein.
Geschäftsprozess(e)	Geschäftsprozesse, in denen das Risiko besteht, beispielsweise Vertrieb, Marketing, Einkauf, usw.
Brutto-Risiko	Das Compliance-Risiko, wie es ohne jegliche Einflussnahme derzeit bewertet wird.
Risikostrategie	Die Strategie, mit der das Unternehmen dem Risiko begegnen möchte.
Maßnahmen	Je nach Strategie werden Maßnahmen definiert, um das Risiko zu reduzieren.
Netto-Risiko	Das Compliance-Risiko, wie es nach Anwendung der Maßnahmen bewertet wird.





Die Bewertung des Risikos

Es gibt viele Möglichkeiten der Risikobewertung. Für Compliance-Risiken hat sich die Bewertung nach Eintrittswahrscheinlichkeit und Schadenshöhe für Brutto- und Nettorisiken durchgesetzt. Sowohl Brutto- als auch Nettorisiko werden dabei als eine Kombination aus Eintrittswahrscheinlichkeit und Schadenshöhe bewertet.

Eintrittswahrscheinlichkeit

Natürlich kann es sehr schwer sein, die Eintrittswahrscheinlichkeit zuverlässig einzuschätzen. Dabei helfen können beispielsweise Statistiken, Studien oder auch Rankings, wie der Corruption Perception Index, den Transparency International regelmäßig für Länder und Branchen erhebt⁶. Mit Hilfe dieser Daten fällt es zumindest etwas leichter, Relationen zwischen einzelnen Risiken zu erkennen.

Die Eintrittswahrscheinlichkeit wird dann in der Regel als Prozentzahl zwischen 0 und 100 Prozent angegeben. Falls in Ihrem Unternehmen mehrere Personen an der Risikoanalyse arbeiten, empfiehlt es sich unbedingt, ein gemeinsames Verständnis für Größen wie Eintrittswahrscheinlichkeit oder Schadenshöhe zu etablieren. So wird verhindert, dass lokale Risikoverantwortliche stark abweichende Vorstellungen der Wahrscheinlichkeiten haben.

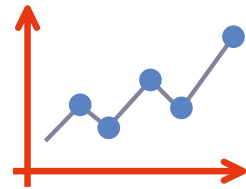
Prozentzahl	Erklärung
> 90 %	Nahezu sicher
65 % - 90 %	Wahrscheinlich
35 % - 65 %	Möglich
10 % - 35 %	Unwahrscheinlich
< 10 %	Selten

Beispiel für eine Klassifizierung der Prozentwerte für die Eintrittswahrscheinlichkeit

Schadenshöhe

Hier stellen sich ähnliche Herausforderungen wie bei der Eintrittswahrscheinlichkeit. Die Schadenshöhe kann beispielsweise anhand von drohenden Strafzahlungen bei Gesetzesverstößen, Ausschluss von Ausschreibungen, Kosten für Rückrufaktionen oder Umsatzeinbrüchen aufgrund von Reputationsverlust näherungsweise bestimmt werden.

⁶ Transparency International (2019): Corruption Perceptions Index 2019



Die Schadenshöhe wird üblicherweise in fünf Stufen definiert. Das COSO-ERM-Modell⁷ bildet dabei bei einigen Unternehmen eine verlässliche Grundlage:

Impact Scale

Rating	Descriptor	Definition
5	Extreme	<ul style="list-style-type: none"> Financial loss of \$X million or more International long-term negative media coverage; game-changing loss of market share Significant prosecution and fines, litigation including class actions, incarceration of leadership Significant injuries or fatalities to employees or third parties, such as customers or vendors Multiple senior leaders leave
4	Major	<ul style="list-style-type: none"> Financial loss of \$X million up to \$X million National long-term negative media coverage; significant loss of market share Report to regulator requiring major project for corrective action Some senior managers leave, high
3	Moderate	<ul style="list-style-type: none"> Financial loss of \$X million up to \$X million National short-term negative media coverage Report of breach to regulator with immediate correction to be implemented Out-patient medical treatment required for employees or third parties, such as customers or vendors Widespread staff morale problems and high turnover

⁷ Deloitte & Touche LLP: Risk Assessment in Practice (2012)

2	Minor	<ul style="list-style-type: none"> ■ Financial loss of \$X million up to \$X million ■ Local reputational damage ■ Reportable incident to regulator, no follow up ■ No or minor injuries to employees or third parties, such as customers or vendors ■ General staff morale problems and increase in turnover
1	Incidental	<ul style="list-style-type: none"> ■ Financial loss up to \$X million ■ Local media attention quickly remedied ■ Not reportable to regulator ■ No injuries to employees or third parties, such as customers or vendors ■ Isolated staff dissatisfaction

Strategien zur Risikosteuerung

Ist ein Risiko identifiziert, existieren unterschiedliche Strategien, mit denen dem Risiko begegnet werden kann:

Reduzieren	Diese Strategie soll ein erkanntes Compliance-Risiko verringern, indem organisatorische, personelle oder technische Maßnahmen eingesetzt werden.
Akzeptieren	Die Akzeptanz eines Risikos ohne das Einsetzen von Gegenmaßnahmen empfiehlt sich bei Compliance-Risiken in der Regel nur bei verhältnismäßig unbedeutenden Risiken (geringe Eintrittswahrscheinlichkeit, geringe Schadenshöhe).
Überwälzen	Bei der Überwälzungsstrategie wird versucht, das Compliance-Risiko auf Dritte abzuwälzen. Das kann beispielsweise durch den Abschluss einer Versicherung geschehen, ein klassischer Fall ist die D&O-Versicherung.
Vermeiden	Das Vermeiden eines Compliance-Risikos kann durch Reduzieren oder Einstellen einer bestimmten geschäftlichen Tätigkeit erreicht werden. Diese Strategie bedeutet häufig den größten Einschnitt für die Business-Seite, kann je nach Risiko jedoch auch dringend anzuraten sein.

Maßnahmen zur Risikoreduzierung

In einigen Unternehmen wird die Compliance-Funktion immer noch als „Business-Verhinderer“ gesehen, wenngleich viele Compliance-Verantwortliche sich vielmehr als strategischer Partner der Business-Seite verstehen. Maßnahmen zur Risikoreduzierung können ein gutes Werkzeug sein, mit Hilfe derer Geschäftschancen wahrgenommen und gleichzeitig damit verbundene Compliance-Risiken eingedämmt werden können.

Einige Beispiele für solche Maßnahmen:

- Compliance-Schulungen für Mitarbeiter
- Interne Kommunikationsmaßnahmen
- Richtlinien
- Vier-Augen-Prinzip
- Personalrotationsprinzip
- Geschäftspartnerprüfung
- Kontrollmaßnahmen



Die Verantwortung für das Definieren der nötigen Maßnahmen sollte beim Risiko-Owner liegen. Um zu gewährleisten, dass die Maßnahmen auch tatsächlich umgesetzt werden, sollte für jede Maßnahme auch ein Maßnahmen-Owner bestimmt werden. Die können unterschiedliche Personen sein – so könnte bei einem erkannten Korruptionsrisiko die Verantwortung für das Risiko beim Compliance-Verantwortlichen liegen, die Verantwortung für das Durchführen einer entsprechenden Schulung jedoch bei der Personalabteilung.

Je nach Maßnahme empfiehlt sich auch das Definieren einer Deadline, bis zu der die Maßnahme umgesetzt sein soll, falls noch nicht implementiert. So lässt sich regelmäßig nachverfolgen, ob Maßnahmen bereits umgesetzt wurden und ob sie auch die gewünschte Wirkung entfalten.

Eine Maßnahme kann selbstverständlich zur Reduzierung mehrerer Risiken eingesetzt werden. Allgemeine Compliance-Schulungen beispielsweise steigern idealerweise das Bewusstsein der Mitarbeiter für eine ganze Reihe von Compliance-relevanten Themen, und können damit auch zur Reduzierung mehrerer Compliance-Risiken beitragen.

Laufende Überprüfung der Compliance-Risiken



Die Compliance-Risikoanalyse sollte auf keinen Fall ein einmaliges Unterfangen bleiben. Risiken, Strategien und Maßnahmen können sich jederzeit ändern, daher sollte die Risikoanalyse einer regelmäßigen Überprüfung unterzogen werden. Dabei können externe oder interne Faktoren eine Neubewertung des Risikos erfordern.

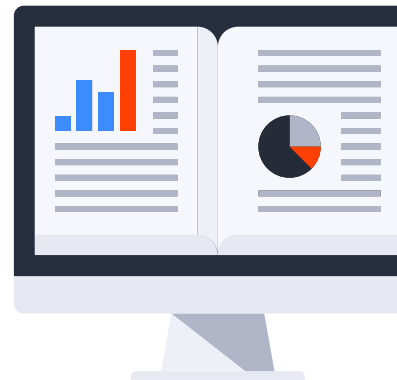
Externe Faktoren

können wirksam werden, wenn sich Länder- oder Branchenrisiken ändern, Gesetze oder Regularien neu eingesetzt, angepasst oder externe Bewertungsmaßstäbe (zum Beispiel zur Evaluierung der Effizienz eines Compliance-Programms) überarbeitet werden.



Interne Faktoren

können wirksam werden, wenn das Unternehmen die Aktivitäten in einem Geschäftsbereich ausbaut oder in einen neuen Geschäftsbereich vorstößt, sich Geschäftsmodelle oder das Produktportfolio ändern.



In beiden Fällen kann eine Anpassung der Eintrittswahrscheinlichkeiten, Schadenshöhen, definierten Maßnahmen oder auch die Erfassung neuer Risiken nötig werden – und das zu jeder Zeit. Es empfiehlt sich daher für Compliance-Verantwortliche, stets ein Auge auf möglicherweise bedeutsame geschäftliche Entwicklungen zu haben, um die Risikoanalyse gegebenenfalls zeitnah anzupassen.

Auch unabhängig von solchen anlassbezogenen Anpassungen der Risikoanalyse ist es ratsam, die erfassten Risiken in regelmäßigen Abständen zu überprüfen: Sind Eintrittswahrscheinlichkeit und Schadenhöhe noch realistisch? Sind die definierten Maßnahmen umgesetzt und entfalten sie die gewünschte Wirkung?

Es existiert kein allgemeingültiger Standard, wie häufig die Compliance-Risikoanalyse wiederholt werden sollte. Manche Leitfäden empfehlen, die erfassten Risiken mindestens einmal im Jahr zu überprüfen. Software-Lösungen zur Unterstützung der Compliance-Risikoanalyse erleichtern die laufende Überprüfung mit einer entsprechenden Erinnerungsfunktion. So können für hohe Risiken kürzere Review-Perioden definiert werden als für geringe Risiken.

Die regelmäßige Überprüfung der Compliance-Risiken trägt nicht nur dazu bei, dass die Effektivität des Compliance-Programms laufend überprüft wird und mögliche neue Risiken besser erkannt werden können – sie ist auch unabdingbar, um gegenüber externen Auditoren – und im Ernstfall Strafverfolgern – ein robustes Compliance-System nachweisen zu können

Digitale Unterstützung für die Compliance- Risikoanalyse



Viele Unternehmen nutzen Excel, um die Compliance-Risikoanalyse durchzuführen. Eine entsprechende Excel-Vorlage (wir bieten selbst ein kostenloses Excel-Template an) kann ein guter Anfang sein. Spätestens bei der laufenden Überprüfung der Risiken stößt Excel jedoch häufig an seine Grenzen. Schließlich sollten auch die historischen Daten aufbewahrt werden, idealerweise sind die Risiken ergänzt um Dokumente, anhand derer die Einschätzung der Eintrittswahrscheinlichkeit und Schadenshöhe vorgenommen wurde, und natürlich sollte auch festgehalten werden, wer die Risiko-Einschätzung wann geändert hat.

**LADEN SIE JETZT UNSERE KOSTENLOSE EXCEL-VORLAGE
ZUR COMPLIANCE-RISIKOANALYSE HERUNTER**



Somit bietet der Einsatz einer Software-Lösung für die Compliance-Risikoanalyse einige Vorteile:

- Übersichtliche Darstellung aller Risiken mit Sortier- und Filter-Möglichkeiten
- Einheitliche Risiko-Einschätzung: Die Compliance-Funktion gibt Kategorien und Bewertungsmaßstäbe vor, die dann von allen Risiko-Ownern verwendet werden
- Audit-Trail: Wann hat welche Person aus welchen Gründen die Risiko-Einschätzung geändert, Maßnahmen entfernt oder neu definiert, neue Risiken erfasst oder bestehende archiviert?
- Reminder-Funktion: Das System erinnert automatisch an die anstehende Überprüfung einzelner Risiken oder Deadlines für definierte Maßnahmen
- Rollen- und Rechte-Konzept: Lokale Risikomanager sehen nur Risikodaten, für die sie verantwortlich sind
- Reporting: Risiko-Heatmaps, Verlaufskurven und Risiko-Datensätze können jederzeit in Echtzeit generiert und exportiert werden

Insbesondere in Organisationen, in denen die Risiko-Erfassung, -Bewertung und -Überprüfung nicht von einer zentralen Stelle durchgeführt wird, macht der Einsatz von Software speziell für Compliance-Risiken Sinn. Einzelne, für bestimmte Regionen oder thematische Risikobereiche verantwortliche Risiko-Manager können kollaborieren und das Risiko-Assessment kann bei der Compliance-Funktion bequem zu einer ganzheitlichen Compliance-Risikobetrachtung zusammengeführt werden.

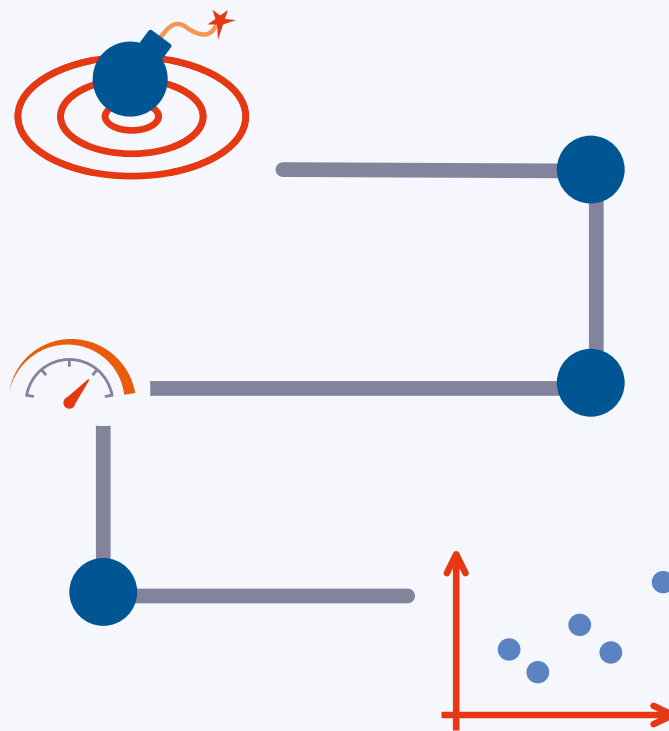
Die Integration in das allgemeine Risikomanagement

Unternehmen ab einer gewissen Größe oder bestimmter Branchen verfügen bereits über Risiko-Abteilungen – man spricht hier vom Enterprise Risk Management (ERM). Diese analysieren in der Regel allgemeine Geschäftsrisiken, lassen Compliance-Risiken jedoch entweder völlig außer Acht oder betrachten sie nicht in der gebotenen Tiefe. Allerdings können hier bereits Strukturen und Prozesse etabliert sein, die sich nutzen lassen.

Es kann jedoch auch vorkommen, dass die im Risikomanagement genutzten Modelle, Prozesse und Tools die Anforderungen der Compliance-Risikoanalyse deutlich übersteigen, und damit eher zu einer unnötigen Verkomplizierung beitragen. Sprich: Solange das Management am Ende in der Lage ist, ein umfassendes und harmonisiertes Bild über alle Risiken zu erhalten (Geschäfts- und Compliance-Risiken), können durchaus auch verschiedene Tools oder Prozesse zum Einsatz kommen.



Die Auswertung der Compliance-Risikoanalyse



Für die Geschäftsleitung ist es von höchster Bedeutung, jederzeit einen zuverlässigen Blick auf die relevantesten (Compliance-) Risiken zu haben. In aller Regel wird die knapp bemessene Zeit der Vorstände und Geschäftsführer aber nicht ausreichen, um sich die gesamte Risikolandschaft zu Gemüte zu führen. Stattdessen sind aussagekräftige Reports gefragt, die den Blick auf das Wesentliche lenken – und mit Visualisierungen arbeiten.

Der Risiko-Bericht: Regelmäßig, präzise, auf das Wesentliche konzentriert

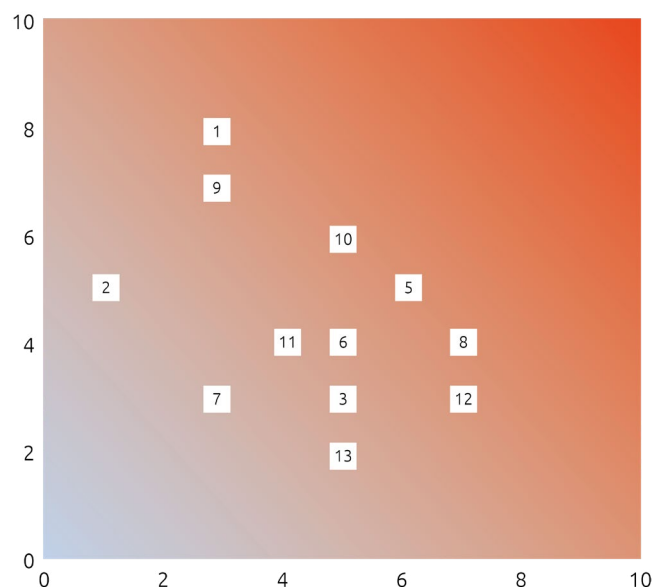
Vorstand, Aufsichtsrat und Prüfer werden sich regelmäßig über den aktuellen Stand und die Effektivität der Compliance-Risikoanalyse informieren wollen. Regelmäßige Berichte sind daher zu empfehlen, wobei es einige Punkte zu beachten gibt:

- Risiken sollten klar und verständlich dargestellt werden, ohne juristische oder technische Fachbegriffe
- Der Bericht sollte insbesondere auf die Risiken eingehen, die mit Hilfe der Risikoanalyse als besonders relevant eingestuft wurden
- Vorgesehene Maßnahmen sowie deren aktueller Status sollten beinhaltet sein
- Visualisierungen helfen, einen Überblick über die gesamte Risikolandschaft zu verschaffen und einzelne Risiken in Kontext zu bringen

Das Einbeziehen des Managements ist eine gute Idee: Ein zweiminütiges Video, in dem Vorstand oder Geschäftsführer erklären, weshalb z.B. das Hinweisgebersystem existiert, bringt allen Mitarbeitern das Thema näher und zeigt die Unterstützung des Managements.

Risiko-Heatmaps und -Matrizen

Die klassischste Art der Risiko-Visualisierung sind Heatmaps und Matrizen. Hierbei werden alle Risiken (oder gefiltert nach Geschäftseinheit, Kategorie, Rechtsgebiet oder Ähnlichem) ihrer Bewertung nach dargestellt, anhand ihrer Schadenshöhe und Eintrittswahrscheinlichkeit. Diese Visualisierung liefert einen ganzheitlichen Überblick über die gesamte Risikolandschaft.

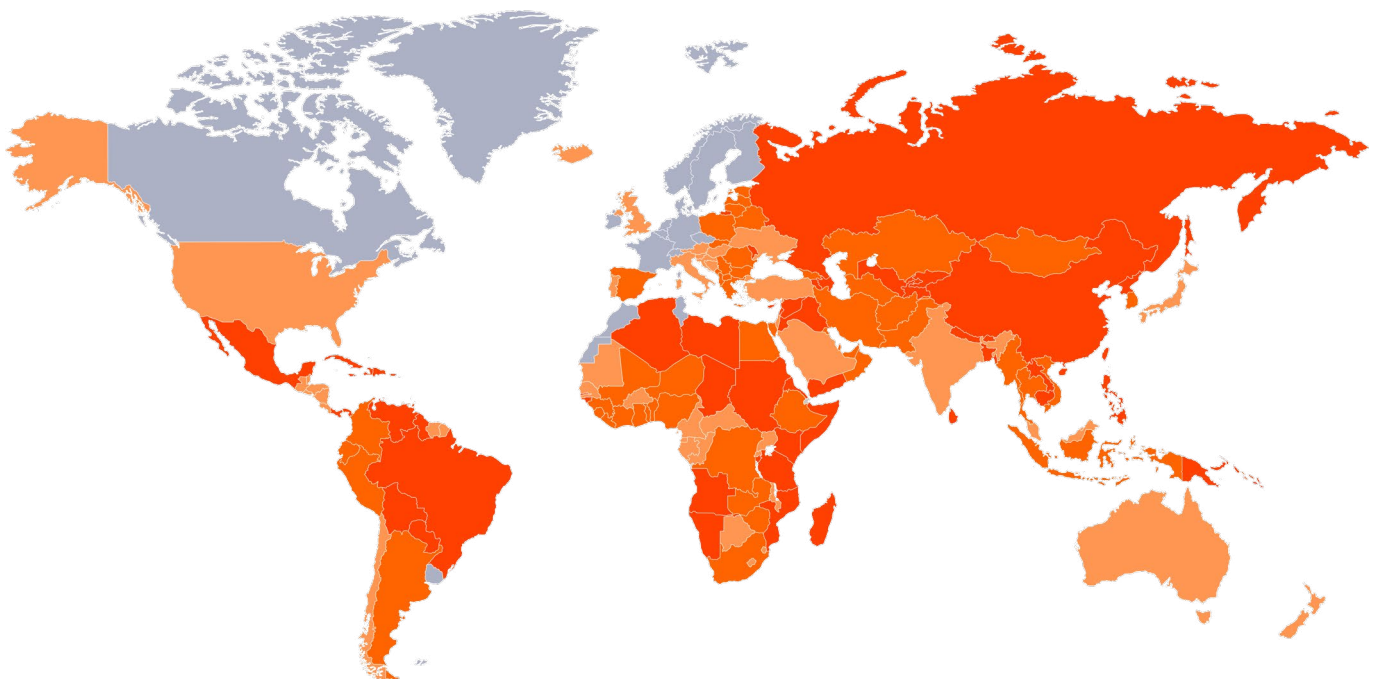


Eine solche Heatmap kann entweder als großflächige Grafik (wie abgebildet) dargestellt werden, aber auch als in Quadranten unterteilte Matrix. Die Matrix erlaubt die grobe Kategorisierung der Risiken in Risiko-Quadranten, sprich bestimmte Kombinationen aus Eintrittswahrscheinlichkeit und Schadenshöhe.

Risiko-Landkarten

Bei international tätigen Unternehmen können Compliance-Risiken in aller Regel in einer Vielzahl von Ländern und Regionen auftreten. Um hier den Überblick zu behalten, bietet sich auch die geographische Darstellung von Risiken an, beispielsweise in einer farbkodierten Weltkarte (oder in spezifischeren Karten für Kontinente oder einzelne Wirtschaftsräume).

Anhand einer solchen Risiko-Landkarte können selbst in Echtzeit schnell die Länder und Regionen identifiziert werden, in denen die gewichtigsten Compliance-Risiken bestehen und auf die innerhalb des Compliance-Programms möglicherweise ein besonderer Fokus gelegt werden sollte. Insbesondere für die laufende Überprüfung der Compliance-Risiken können Landkarten wertvolle Hinweise liefern, wie sich die Risikolandschaft im Laufe der Zeit verändert.



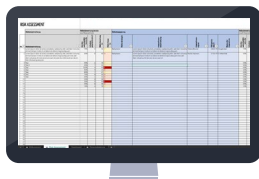
Fazit

Ohne eine vernünftige Analyse der Compliance-Risiken laufen Unternehmen Gefahr, in ihren Compliance-Bemühungen falsche Schwerpunkte zu setzen und relevante Risiken außer Acht zu lassen. Unabhängig von der Größe des Unternehmens ist die Compliance-Risikoanalyse und deren regelmäßige Aktualisierung daher unbedingt zu empfehlen. Wir hoffen, dass Ihnen dieser Leitfaden die Durchführung der Risikoanalyse erleichtert und dabei hilft, die regelmäßige Aktualisierung und Berichterstattung zu etablieren.

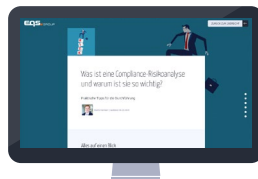
Ein ganzheitliches und kontinuierliches Compliance-Risikomanagement ist nicht nur ein wichtiges Werkzeug, um die Effektivität des Compliance-Programms sicherzustellen. Im Fall von Compliance-Verstößen ermöglicht ein solches System auch den Nachweis, welche Schritte unternommen wurden, um das jeweilige Risiko zu vermeiden oder zu reduzieren. Dieser Nachweis versetzt Unternehmen bei Untersuchungen in eine deutlich bessere Position, als wenn das zugrunde liegende Risiko gar nicht bekannt war.

Es lohnt sich daher aus vielerlei Gründen, in die Compliance-Risikoanalyse zu investieren. Sie erlaubt es, Risiken frühzeitig zu erkennen, entsprechende Strategien und Gegenmaßnahmen zu entwickeln und somit das Compliance-Programm laufend zu verbessern. Nicht umsonst bildet die Compliance-Risikoanalyse das Fundament eines jeden effektiven Compliance-Programms.

Zusätzliche Ressourcen



Excel-Vorlage Risikoanalyse



Blogartikel: Was ist eine Risikoanalyse und warum ist sie so wichtig?



White Paper: Leitfaden zur Einführung eines Hinweisgebersystems

Über EQS Group

Seit ihrer Gründung im Jahr 2000 unterstützt die EQS Group mehrere tausend Unternehmen weltweit bei der Erfüllung komplexer Compliance-Anforderungen.

Egal, ob Sie Insiderlisten anlegen oder Geschenke und Bewirtungen verwalten müssen, Ihre Richtlinien effektiv kommunizieren und speichern wollen, Interessenkonflikte oder Fehlverhalten bekämpfen und Risiken minimieren möchten – wir können Ihnen helfen. Unser Ziel ist es, Compliance-Experten mit einfachen Arbeitsabläufen, automatisierten Prozessen, fortschrittlichen Analysen und übersichtlichen Berichten auszustatten, um ihnen die tägliche Arbeit zu erleichtern. Zusätzlich zu unseren Compliance-Produkten bietet die EQS Group auch digitale Lösungen für Investor Relations an.

Heute ist der Konzern mit mehr als 350 Mitarbeitenden in den wichtigsten Finanzmetropolen der Welt vertreten. Besuchen Sie unsere Website, um mehr zu erfahren: www.eqs.com

