NAVEX GLOBAL®

UMFASSENDER LEITFADEN FÜR

Ethik- und Compliance-Programme

Ihr maßgeblicher Leitfaden zur Entwicklung und Implementierung eines effektiven Programms

Inhalt

EINLEITUNG

WARUM IST ETHIK UND COMPLIANCE SO WICHTIG?

Ethik und Compliance gewinnt für Unternehmen aller Größenordnungen auf der ganzen Welt immer mehr an Bedeutung, da der Gesetzgeber versucht, die schädlichen Auswirkungen illegaler, korrupter und unethischer Geschäftspraktiken zu bekämpfen. Gleichzeitig erwarten Kunden zunehmend, dass die Unternehmen, mit denen sie umgehen und von denen sie kaufen, verantwortungsvoll, ethisch und nachhaltig handeln. In einer globalisierten Wirtschaft kann es über Erfolg oder Misserfolg eines Unternehmens entscheiden, diese Fragen zu verstehen und die sich darauf beziehenden nationalen und internationalen Bestimmungen zu kennen.

Definition von Ethik und Compliance

Compliance bedeutet die Einhaltung von Gesetzen und Vorschriften sowie die Einhaltung von Standards, Richtlinien und Verfahren einer Organisation. Rechtlich gesehen ist Compliance die Vorgehensweise, mit der Unternehmen sicherstellen wollen, dass Mitarbeiter und Repräsentanten geltende Gesetze und interne Vorschriften einhalten, um Schaden von sich selbst, dem Unternehmen oder anderen abzuwenden. Anhand dieser Definition wird deutlich, dass Compliance eine Form von Risikomanagement ist.

Von modernen Unternehmen wird erwartet, dass sie bei der Einhaltung von Gesetzen und internen Richtlinien mehr tun als nur das absolute Minimum. Sie müssen Maßnahmen ergreifen, um eine ethische Arbeitsplatzkultur zu entwickeln und zu fördern. Ethische Überlegungen bilden die Grundlage eines effektiven Ethik- und Compliance-Programms, weil sie sich mit Konzepten von richtigem und falschem Verhalten befassen und daher in „Werten" verwurzelt sind.

Ob „Ethik" vor der „Compliance" kommt, darüber lässt sich streiten, aber klar ist: Ein effektives Ethik- und Compliance-Programm erfordert heute ein Bekenntnis zu ethischen Prinzipien.

Durch die Kombination beider Ansätze können Unternehmen Risiken effektiver managen und gesetzliche Anforderungen erfüllen.

Glossar

- **Compliance** ist die Einhaltung geltender Gesetze, Vorschriften und interner Standards, Richtlinien und Verfahren.
- **Ethik** bedeutet moralische Prinzipien, die das Verhalten von Menschen steuern oder beeinflussen.[1]
- **Wirtschaftsethik** ist die Anwendung von Ethik auf Geschäftsgebaren[2].
- **Werte** sind Kernideen darüber, wie Menschen leben sollten und welche Ziele sie anstreben sollten[3].
- **Integrität** ist die Eigenschaft, ehrlich zu sein und starke moralische Prinzipien zu haben, die man nicht ändern will[4].
- **Ethik- und Compliance-Programme** helfen Unternehmen beim Risikomanagement, bei der regulatorischen Compliance und bei der Förderung einer ethischen Arbeitskultur.[5]

[1] Oxford Online Dictionary [2] Institute of Business Ethics [3] C. Fisher and A. Lovell, Business Ethics and Values: Individual, Corporate and International Perspectives. 3rd ed., Prentice Hall, 2009, S.153 [4] Cambridge Dictionary of English [5] NAVEX Global

Gründe für die Entwicklung eines Ethik- und Compliance- Programms

Ein effektives Ethik- und Compliance-Programm ist nicht nur „nice to have", sondern auch entscheidend für die Führung eines produktiven, angesehenen und erfolgreichen Unternehmens. Ohne ein solches könnte Ihr Unternehmen einem erheblichen Risiko ausgesetzt sein. Bei der Formulierung der Gründe, die eine Investition in Ihr Programm rechtfertigen, sind die folgenden Faktoren ein guter Ausgangspunkt.

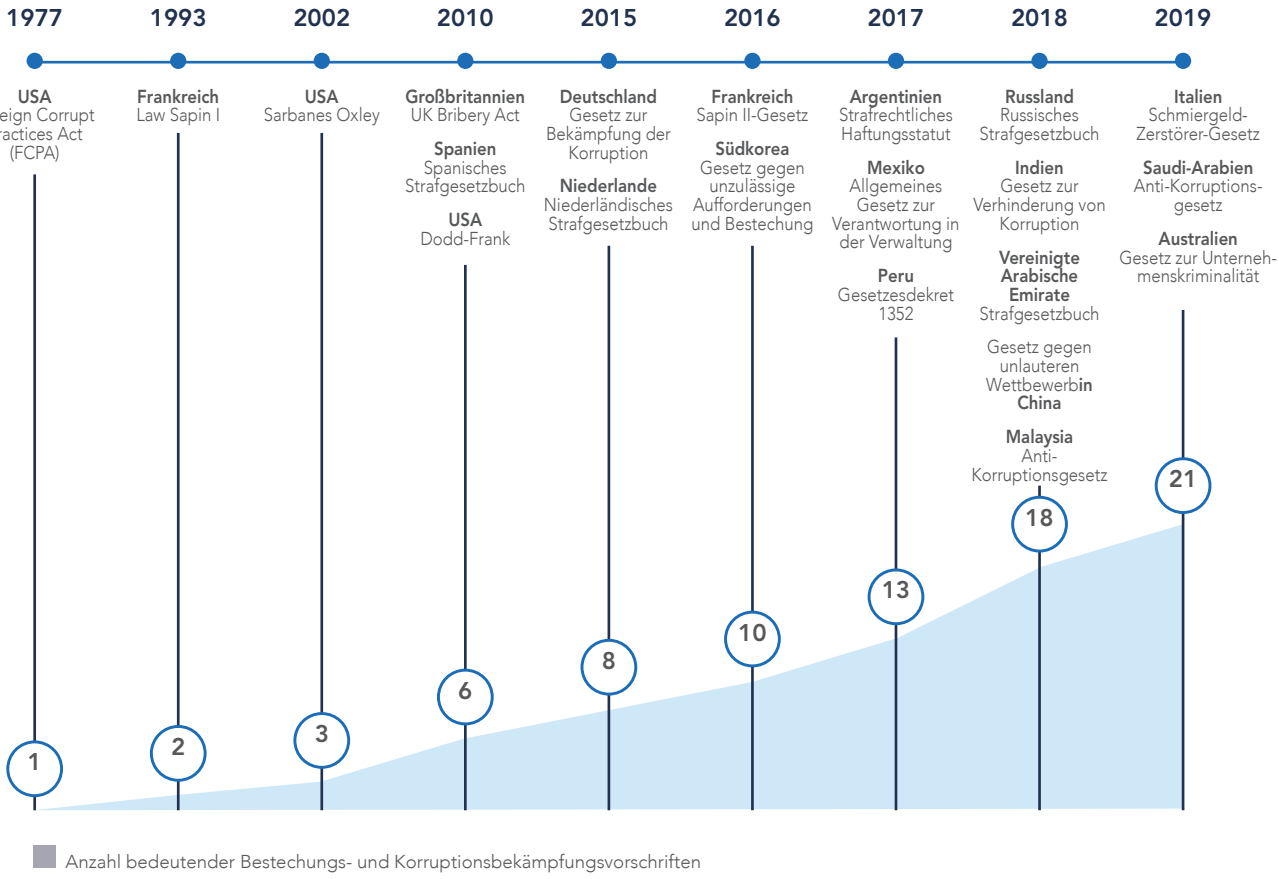
Regulatorische Zwänge

Es gibt zahlreiche und komplizierte Bestimmungen. Diese variieren natürlich von Branche zu Branche und von Standort zu Standort. Aber von modernen Organisationen wird erwartet, dass sie trotzdem alle Vorschriften einhalten.

Seit dem Enron-Skandal im Jahr 2001 und der Einführung des Sarbanes-Oxley Act (SOX) im darauffolgenden Jahr haben sich das Tempo und die Dynamik der regulatorischen Veränderungen nicht nur in den USA erhöht, sondern weltweit. Angefangen mit dem UK Bribery Act (2010) sind in den letzten zehn Jahren in Europa, im asiatisch-pazifischen Raum und darüber hinaus eine beispiellose Reihe von Bestimmungen zur Bekämpfung von Korruption, zu moderner Sklaverei, zum Schutz von Hinweisgebern und zum Datenschutz in Kraft getreten.

Unternehmen, die in der gleichen Branche oder in den gleichen Regionen tätig sind, sehen sich einem ähnlichen regulatorischen Druck ausgesetzt. Indem sie Compliance-bezogene Risiken effektiver managen als ihre Mitbewerber, können sich Unternehmen einen Wettbewerbsvorteil verschaffen. Nach Informationen des Beratungsunternehmens Ethisphere sind Unternehmen, die auf dessen „Most Ethical"-Liste ausgezeichnet wurden, finanziell erfolgreicher als ihre Konkurrenten.[6] Für die Auszeichnung wurde unter anderem das Ethik- und Compliance-Programm eines Unternehmens bewertet.

Die Einführung globaler Vorschriften zur Bekämpfung von Bestechung und Korruption wurde in den letzten Jahren beschleunigt



[6] Ethisphere, World's most ethical companies 2020.

Zunehmende Strafverfolgung

Die Umsetzung geltenden Rechts ist heutzutage intensiv und aktiv an allen Fronten. Ganz gleich, ob es sich um eine neue Vorschrift, eine neue Auslegung oder einfach um eine stärkere Durchsetzung bestehender Gesetze handelt: Compliance-Abteilungen müssen sich des realen und wachsenden Risikos von Geldbußen und Strafverfolgungen bewusst sein.

Statistiken über die Durchsetzung des Foreign Corrupt Practices Act (FCPA) belegen dies. Zwischen 1977 (als der FCPA als US-Gesetz verabschiedet wurde) und 2000 wurden nur bis zu 10 Fälle pro Jahr von den zuständigen Vollzugsbehörden vollstreckt Seit 2001 wurden durchschnittlich mehr als 30 Fälle pro Jahr vollstreckt[7]. Auch die durchschnittlichen Kosten für Bußgelder sind gestiegen, von 5 Mio. US-Dollar im Jahr 2015 auf über 116 Mio. US-Dollar im Jahr 2019[8].

Gleichzeitig arbeiten die Regulierungsbehörden weltweit stärker denn je zusammen, um Vorschriften durchzusetzen. Dies hat dazu geführt, dass Unternehmen für ein und denselben Verstoß von verschiedenen Aufsichtsbehörden mit mehreren Geldbußen belegt werden.

Strafverfolgungsbehörden auf der ganzen Welt erkennen an, dass Ethik- und Compliance-Programme notwendig sind, um die Wahrscheinlichkeit von Rechtsverstößen zu verringern und die Mitarbeiter darüber aufzuklären, was von ihnen erwartet wird. Effektive Ethik- und Compliance-Programme (nicht nur solche, die man einfach „abhakt") können Unternehmen daher helfen, kritische rechtliche Abwehrmechanismen aufzubauen, Schäden zu begrenzen und in einigen Fällen eine strafrechtliche Verfolgung ganz zu vermeiden.

Höhere ethische Standards

Bislang hat der rechtliche Rahmen der Compliance wesentliche Fortschritte erzielt. In den letzten Jahren ist jedoch klar geworden, dass die Auseinandersetzung mit ethischen Erwägungen genauso wichtig (wenn nicht sogar wichtiger) ist.

Der Leitfaden des US-Justizministeriums (DOJ), „Evaluation of Corporate Compliance Programs", unterstreicht, wie wichtig es für ein Unternehmen ist, eine Kultur der Ethik zu schaffen und zu fördern. Bei der Bewertung der Effektivität von Compliance-Programmen sind Staatsanwälte angehalten zu fragen:

- Wie oft und wie misst das Unternehmen seine Kultur der Ethik und Compliance?
- Welche Schritte hat das Unternehmen als Reaktion auf die Ergebnisse seiner Messung der Compliance-Kultur unternommen?
- Wird das Programm ernsthaft und nach Treu und Glauben angewendet? Anders gesagt: Verfügt das Programm über ausreichende Ressourcen und Befugnisse, um effektiv zu funktionieren?

Unternehmen können ihre Compliance-Verpflichtungen nicht mehr mit einem „Häkchen"-Ansatz erfüllen. Um sinnvolle Verhaltensänderungen voranzutreiben, wird eine ethische Kultur als wesentlich angesehen.[9]

Erwartungen der Stakeholder

Die Standards für das Verhalten von Unternehmen entwickeln sich ständig weiter und spiegeln die Forderung der Gesellschaft nach größerer Rechenschaftspflicht wider. Der Wunsch nach Gewinnmaximierung wird nun durch die Notwendigkeit ausgeglichen, im besten Interesse nicht nur der Aktionäre, sondern aller Stakeholder zu handeln - einschließlich der Mitarbeiter, Lieferanten, Kunden, Anwohner und der Gesellschaft im Allgemeinen. Mit anderen Worten: im Interesse aller, die diese Standards direkt oder indirekt beeinflussen.

Um erfolgreich zu bleiben, haben Unternehmen in Übereinstimmung mit ethischen und moralischen Normen die Verantwortung, einen positiven Beitrag zur Gesellschaft zu leisten,.. Das bedeutet, eine umfassende Sichtweise der Stakeholder einzunehmen, um öffentliches Vertrauen zu stärken und zu erhalten.

Die zunehmende Aufmerksamkeit der Investoren für Umwelt-, Sozial- und Governance-Themen (Environmental, Social and Governance, kurz ESG) hat Compliance-Teams dazu veranlasst, über die Bedeutung der Unternehmensverantwortung im Zusammenhang mit dem Unternehmenserfolg nachzudenken. Nach öffentlichen Skandalen, Finanzkrisen und Ausnahmezuständen wie der Covid-19-Pandemie ist klar geworden, dass die Art und Weise, wie sich Unternehmen verhalten, ihren zukünftigen gesellschaftlichen Wert mitbestimmen wird. Diejenigen, die ihre Mitarbeiter schützen und längerfristigen Aktionärsinteressen gegenüber kurzfristigen den Vorrang geben, sind wahrscheinlich besser vor externen wirtschaftlichenBedrohungen und Rufschäden geschützt.

„Die US-Regierung wird weiterhin offensiv mit unseren Partnern weltweit zusammenarbeiten, um Korruption zu bekämpfen."

Brian A. Benczkowski, DOJ Criminal Division.

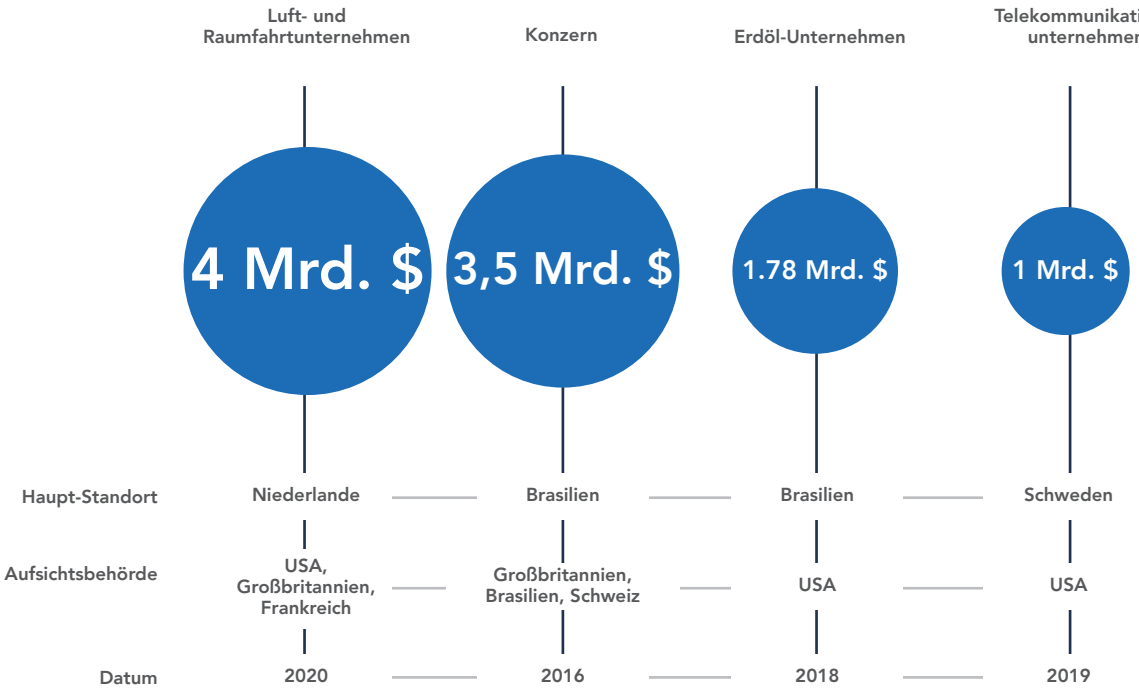
[7] FCPA, 2020 [8] Wilkie, Farr & Gallagher, 2020 [9] DOJ, Evaluation of Corporate Compliance Programs, June 2020, S2, S.16

Die Kosten der Non-Compliance

Zwischen 2016 und 2020 wurden vier Unternehmen mit Korruptionsstrafen von jeweils mehr als einer Milliarde US-Dollar belegt. Die größte davon betraft einen großen Hersteller der Luft- und Raumfahrtindustrie und belief sich auf insgesamt mehr als 3,9 Milliarden US-Dollar. Es waren Strafen von Behörden aus den Vereinigten Staaten, Frankreich und Großbritannien wegen ausländischer Bestechung.

Bußgelder und Geldstrafen können zwar eine ausreichende Motivation darstellen, sich mit dem Compliance-Risiko auseinanderzusetzen, sie machen aber nur einen Bruchteil der Gesamtkosten aus, die mit der Nichteinhaltung von Vorschriften verbunden sind. Rechtliche und laufende Überwachungskosten, Kursverluste der Unternehmensaktie und dauerhafte Reputationsschäden können sich oft weitaus stärker auf den Gewinn des Unternehmens auswirken.

Bedeutende aktuelle Korruptionsstrafen



Die Vorteile eines starken Ethik- und Compliance-Programms

Zu den unmittelbaren Vorteilen eines widerstandsfähigen Ethik- und Compliance-Programms gehört die Verringerung des regulatorischen, rechtlichen und finanziellen Risikos bei gleichzeitiger Schaffung eines erheblichen Wettbewerbsvorteils. Längerfristig kann es die Fähigkeit eines Unternehmens erheblich verbessern, Compliance-bezogene Risiken zu managen, die Erwartungen der Aufsichtsbehörden zu erfüllen und eine ethikzentrierte Kultur zu fördern.

Rechtliche Verteidigung

Obwohl die rechtlichen Standards variieren, gibt es gemeinsame Strategien, die Unternehmen anwenden können, um eine Compliance-basierte Verteidigung aufzubauen, sollten sie mit einer Strafverfolgung oder der Durchsetzung von Vorschriften konfrontiert werden. Gerichte, Jurys und Vollstreckungsbehörden sind bestrebt, Unternehmen zu belohnen, die sich nach bestem Wissen und Gewissen um die Einhaltung der Gesetze bemühen und ihre Mitarbeiter dazu ermutigen, das Gleiche zu tun. Dies kann dazu führen, dass keine Strafverfolgung erfolgt oder die Strafe durch Strafaufschub reduziert wird, sogenannte Deferred Prosecution Agreements (DPAs).

Im Jahr 2012 lehnte das US-Justizministerium (DOJ) beispielsweise die Strafverfolgung einer multinationalen Investmentbank ab, deren Mitarbeiter gegen den FCPA verstoßen hatte. In der Begründung seiner Entscheidung hob das DOJ die Bemühungen der Bank hervor, ihre internen Richtlinien regelmäßig zu aktualisieren, ihre Mitarbeiter regelmäßig zu schulen und alle neuen Geschäftspartner einer umfassenden Due Diligence zu unterziehen.

Im Jahr 2017 erhielt ein global agierendes Maschinenbauunternehmen vom britischen Serious Fraud Office (SFO) einen DPA-Rabatt von 50 %, der sich auf die „umfassende Kooperation" und die „verbesserte Sorgfaltspflicht in Bezug auf Zwischenhändler" bezog, die beim betroffenen Unternehmen umgesetzt wurden.

Diese Beispiele zeigen, wie behördliche Maßnahmen in Fällen abgemildert werden können, in denen Unternehmen nachweisen können, dass sie selbstgesteuerte Maßnahmen ergreifen und in diese investieren, um ihre Compliance-Risiken offensiv zu begrenzen.

Wie erhält man einen Deklinations- oder DPA-Rabatt?

Ein solides Compliance-Programm führen

Ein effektives Ethik- und Compliance-Programm reduziert das Risiko einer strafrechtlichen oder behördlichen Verfolgung von vornherein. Sollte der schlimmste Fall eintreten, wird sein Vorhandensein zeigen, dass Ihr Unternehmen Schritte unternommen hat, um das Compliance-Risiko zu minimieren.

Selbstanzeige

Legen Sie freiwillig einen potenziellen Verstoß gegenüber Strafverfolgern offen, inklusive aller relevanten Fakten und beteiligten Personen, bevor eine staatliche Untersuchung droht. Das Timing ist entscheidend: Wenn es eine unangemessene Verzögerung bei der Meldung eines Verstoßes an die Behörden gibt, nachdem das Unternehmen davon Kenntnis erlangt hat, erhält es möglicherweise keine Anerkennung für ein wirksames Programm.

Mit den Behörden kooperieren

Bewahren Sie alle Beweise auf und legen Sie sie offen, koordinieren Sie die interne Untersuchung des Unternehmens mit der Untersuchung der Aufsichtsbehörde und stellen Sie relevante Personen für Befragungen zur Verfügung. Um eine zeitnahe und gründliche Zusammenarbeit zu gewährleisten, sollte das Unternehmen sicherstellen, dass Compliance-Beauftragte ständig mit Strafverfolgern kommunizieren.

Fehler eingestehen

Zeigen Sie eine zeitnahe und angemessene Behebung des Verstoßes, indem Sie die schuldigen Mitarbeiter disziplinieren und das Ethik- und Compliance-Programm stärken, um weitere ähnliche Verstöße zu verhindern.

Mehr Ethik in der Unternehmenskultur

Ein starkes Ethik- und Compliance-Programm ist mit einer Verbesserung der Unternehmenskultur verbunden. Ein Programm, das auf einem klar definierten Verhaltenskodex aufbaut und auf die Werte und das Risikoprofil des Unternehmens abgestimmt ist, kann dabei helfen, zu artikulieren, wer das Unternehmen ist - oder zu sein anstrebt - und die Stakeholder an diese Vision zu binden.

Ein starker Fokus auf Ethik reduziert nicht nur die Kosten für Fehlverhalten, sondern kann auch zu einer soliden Unternehmensreputation, echter Mitarbeiter-Compliance, robuster Governance und erhöhter Profitabilität beitragen.

Viele Vorschriften, einschließlich derjenigen, die sich auf Bestechung und Korruption, Arbeitsrecht und Datenschutz beziehen, können ihre Ursprünge auf das Ethikkonzept zurückführen. Diese Bereiche der Compliance stehen im Einklang mit den persönlichen Moralvorstellungen und Werten der Mitarbeiterinnen und Mitarbeiter, was bedeutet, dass ein ethikbasierter Compliance-Ansatz für sie wahrscheinlich bedeutsamer ist.

Eine engagierte Belegschaft

Ethische Geschäftspraktiken tragen dazu bei, eine Kultur des Vertrauens, des guten Willens, der Integrität und der Compliance zu pflegen.

Stolz auf das Unternehmen und Zustimmung zu einer ethischen Kultur strahlen oft weit über die Wände der Büros hinaus. Vielmehr reicht sie tief in die Belegschaft und deren Angehörigen, in die gesamte Branche und in positive Beziehungen zur Presse und den Behörden. Die Anerkennung als ethischer Arbeitsplatz erfüllt sich in der Regel von selbst, indem sie hochwertige Führungskräfte, Mitarbeiter, Partner und Kunden anzieht und bindet. Mitarbeiter, die fair behandelt werden, haben ein Gefühl des Wohlwollens und des Vertrauens in das Unternehmen, was sich in einer zufriedeneren und produktiveren Belegschaft niederschlägt.

Eine ethische Orientierung in einem Unternehmen dient als Versicherungspolice gegen Unhöflichkeit am Arbeitsplatz und Fehlverhalten von Mitarbeitern wie Belästigung, Mobbing und Diskriminierung. Akademische Studien haben auch einen Zusammenhang zwischen einem starken Ethik- und Compliance-Programm und weniger Disziplinarmaßnahmen sowie Krankheitszeiten der Mitarbeiter gezeigt, was zu einem Rückgang der Personalkosten geführt hat[10]

33 % der Arbeitnehmerinnen und Arbeitnehmer der Gen Z (geboren 1995-1999) gaben an, dass der Ruf eines Unternehmens für ethisches Verhalten „sehr wichtig" sei, wenn sie sich für einen Arbeitsplatz entscheiden, verglichen mit nur 22 % bei ihren Kolleginnen und Kollegen aus der Millennial-Generation (geboren 1983-1994)[11].

[10] J. Paul McNulty, Jeff Knox & Patricia Harned, What an Effective Corporate Compliance Program Should Look Like, The Journal of Law, Economics and Policy, 9, Nr. 375 (Frühjahr 2013): 383 [11] Deloitte Millennial Survey, 2018

Gesündere Gewinne

Ethische Unternehmen sind erfolgreicher und schneiden in der Regel finanziell besser ab als die Konkurrenz, was den Zusammenhang zwischen guten ethischen Praktiken und Leistungsfähigkeit belegt.[12] Ein starkes Ethik- und Compliance-Programm verbessert die Arbeitsmoral und erhöht das Engagement der Mitarbeiter, was sich positiv auf die Produktivität und das Unternehmensergebnis auswirkt.

Außerdem hilft der Ruf als ethisches Unternehmen, das Vertrauen und die Loyalität der Verbraucher zu gewinnen. Dies gilt insbesondere für jüngere Verbraucher, die mit höherer Wahrscheinlichkeit die ethischen Werte eines Unternehmens berücksichtigen, bevor sie dessen Produkte kaufen.[13]

„Eine starke ethische Kultur unterstützt direkt ein starkes Compliance-Programm."

FCPA-Ressourcenleitfaden

Reputationswert

Schon ein einziger Compliance-Fehler kann das Vertrauen der Öffentlichkeit in ein Unternehmen stark beeinträchtigen.

In der Presse wird häufig darüber berichtet, wie Führungsschwächen beim Management von Compliance-Risiken Unternehmen geschadet und sie sogar erheblichen Geldstrafen und Bußgeldern ausgesetzt haben. Eine finanzielle Strafe kann verbucht werden, aber die Auswirkungen auf den Ruf können weitreichende Folgen für viele Jahre haben.

Stakeholder, Investoren und Aktionäre schätzen Unternehmen, die den Ruf haben, ethisch zu handeln. Eine ethische Reputation signalisiert größere Transparenz, ein geringeres Risiko von Fehlverhalten, eine stärkere Compliance-Kultur und letztlich auch zukünftiges Wachstum und Erfolg. „Sozial verantwortliches Investieren" bedeutet, in gut geführte und profitable Unternehmen zu investieren, die sich auch zur Einhaltung von ESG-Standards verpflichten, die der Gesellschaft zugute kommen. Einst ein Nischenansatz, gewinnt nachhaltiges Investieren an Dynamik: ESG-Fonds verzeichneten 2019 Rekordzuflüsse. Laut einer Umfrage von Morgan Stanley sind rund 85 % der Anleger an nachhaltigen Investitionen interessiert.[14]

Performance der „World's Most Ethical Companies" (Ethisphere 2020 Preisträger) verglichen mit dem Large Cap Index

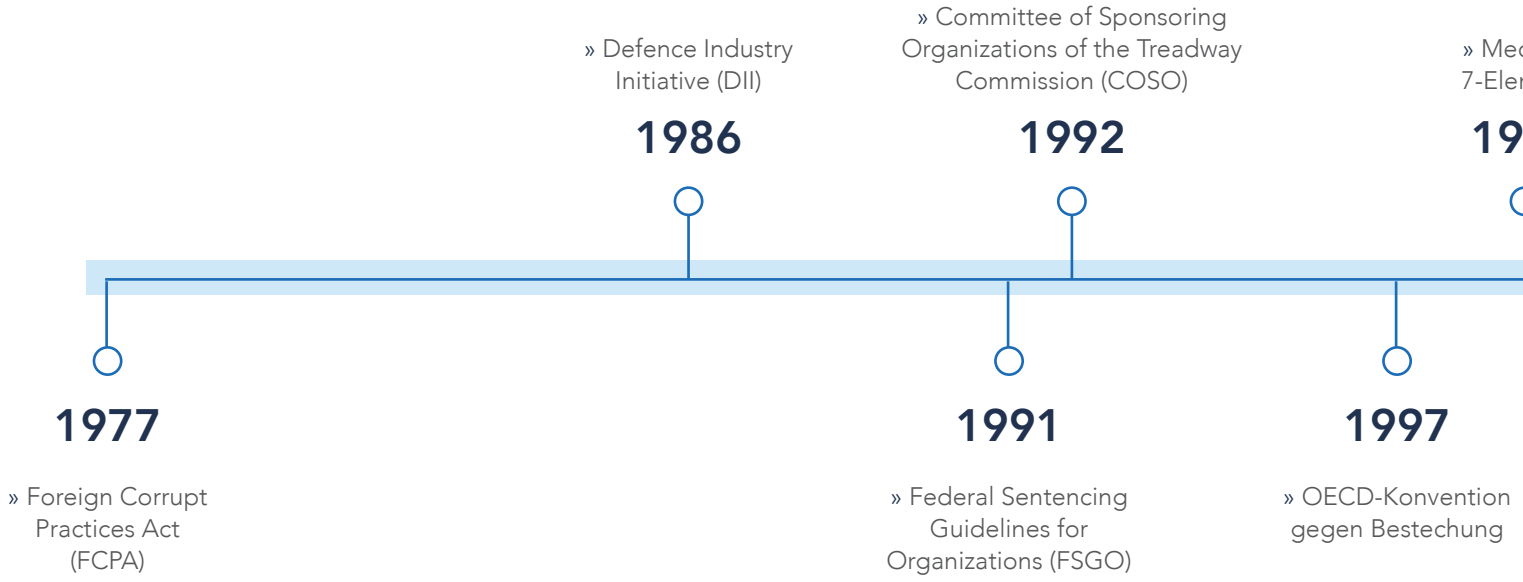
Quelle: Ethisphere. World's most ethical companies 2020. Performance of the 2020 honorees as compared to the large cap index. ›››

[12] Ethisphere, World's most ethical companies 2020 [13] Accenture Strategy Global Consumer Pulse Research, 2018

[14] Morgan Stanley Survey Finds Investor Enthusiasm for Sustainable Investing at an All-Time High. ›››

Entwicklung im Ethik- und Compliance-Management

Die Landschaft des Ethik- und Compliance-Managements hat sich seit seiner Entstehung in den USA in der zweiten Hälfte des 20. Jahrhunderts schnell und signifikant entwickelt.

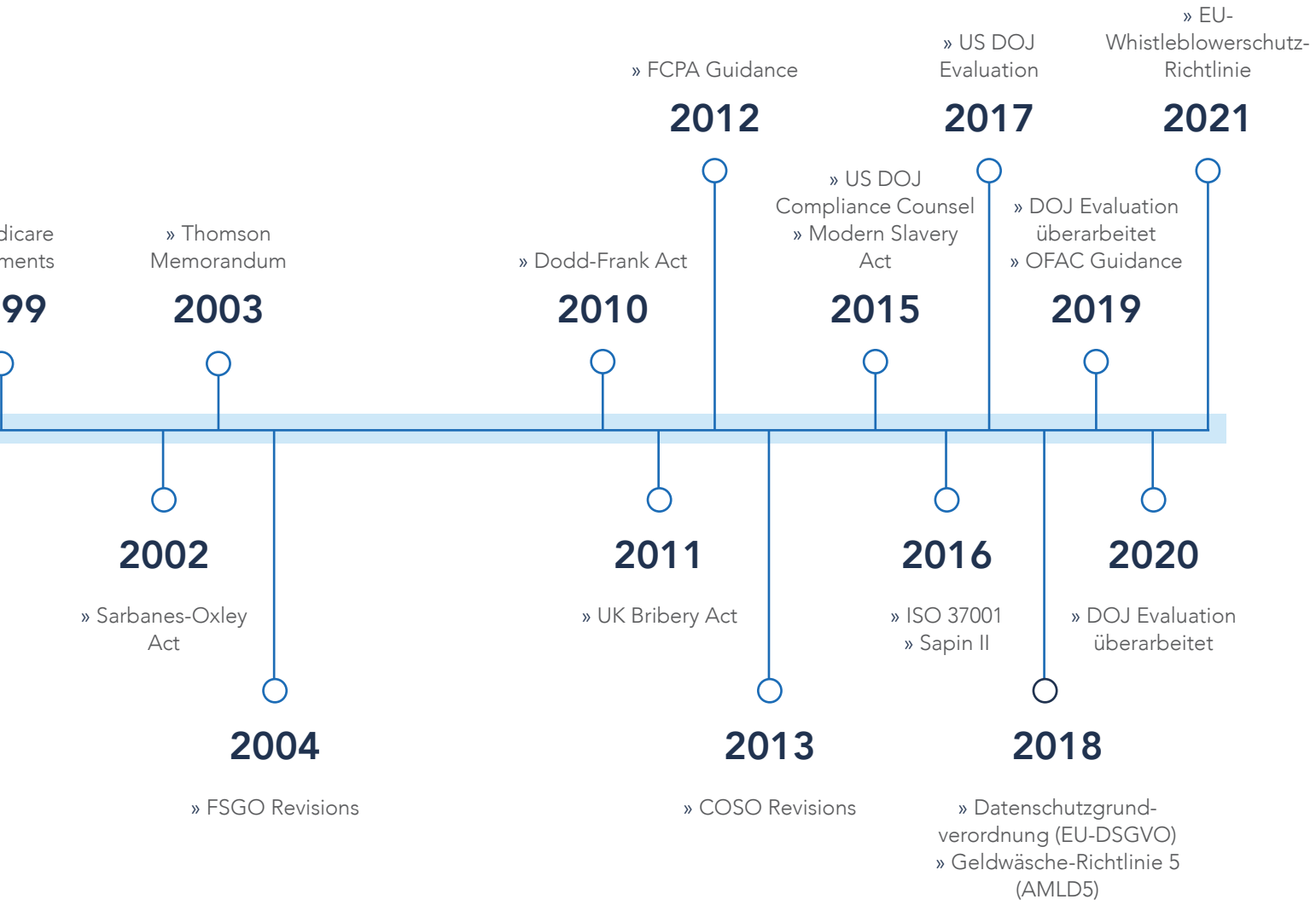


1960er Jahre
Die ersten Compliance-Programme entstanden in den USA, als große Auftragnehmer in der Elektroschwerindustrie wegen Kartellverstößen belangt wurden. Danach begannen die Unternehmen Kartellrechtsschulungen und andere Compliance-Maßnahmen durchzuführen.

1970er Jahre
Eine Reihe von Bestechungsskandalen, die von der US-Börsenaufsichtsbehörde SEC (Securities and Exchange Commission) und dem IRS (Internal Revenue Service - dem Finanzamt) aufgedeckt wurden, führten zur Verabschiedung des Foreign Corrupt Practices Act (FCPA). Multinationale Unternehmen mit Sitz in den USA waren dabei ertappt worden, wie sie ausländische Regierungsbeamte bestachen, um sich geschäftliche Vorteile zu verschaffen, und es wurde klar, dass informelle Compliance-Programme nicht mehr ausreichten.

1980er Jahre
Nach einer Reihe von Skandalen bei der Beschaffung von Verteidigungsgütern gründeten 18 Rüstungsunternehmen die Defense Industry Initiative on Business Ethics and Conduct (DII). Zu den Empfehlungen des DII gehörte die Notwendigkeit, ethische Grundsätze für das Geschäftsverhalten zu entwickeln, die Effektivität der internen Kontrollen zu erhöhen und die Aufsicht durch die Geschäftsleitung sowie die Schulung der Mitarbeiter zu verbessern.

1990er Jahre
Die moderne Ära von Compliance und Ethik begann am 1. November 1991, als die US Federal Sentencing Guidelines for Organizations (FSGO) in Kraft traten. Die Richtlinien waren ein entscheidender Meilenstein in der Entwicklung eines modernen Ansatzes für Compliance. Im Jahr 1992 veröffentlichte das Committee of Sponsoring Organizations of the Treadway Commission (COSO) das Internal Control - Integrated Framework. Das Modell bietet einen prinzipienbasierten Leitfaden für die Gestaltung und Implementierung effektiver interner Kontrollen. Im Jahr 1997 wurde die OECD-Konvention zur Bekämpfung der Bestechung ausländischer Amtsträger im internationalen Geschäftsverkehr von 37 OECD-Ländern und sieben Nicht-OECD-Ländern unterzeichnet.



2000er Jahre
Das 21. Jahrhundert begann mit den Bilanzskandalen von Enron und WorldCom und der anschließenden Verabschiedung des Sarbanes-Oxley Act (SOX) im Jahr 2002. Die Definition eines „effektiven" Programms wurde 2004 im Rahmen der geänderten FSGO noch erweitert, die nun von den Unternehmen verlangt, „eine Organisationskultur zu fördern, die ethisches Verhalten und die Verpflichtung zur Einhaltung der Gesetze fördert "[15]. Seitdem haben Regulierungsbehörden auf der ganzen Welt begonnen, die Rolle der Ethik bei der Prävention und Aufdeckung von kriminellem Verhalten zu betonen.

2010er Jahre - Gegenwart
Die globale Finanzkrise begann im Jahr 2007. Zur Förderung der Finanzstabilität hat der US-Kongress im Jahr 2010 den Dodd-Frank Wall Street Reform and Consumer Protection Act erlassen. Das Gesetz bot Unternehmen einen Anreiz, formale Kanäle für die Aufdeckung und Meldung von Verstößen zu entwickeln. Die SEC wurde ermächtigt, Belohnungen (10-30 % der eingenommenen Gelder) an berechtigte Whistleblower zu zahlen, die qualitativ hochwertige und originelle Informationen liefern, die zu Strafverfolgungen führen, was Bußgelder von mehr als $1 Mio. nach sich zog.[16]

Die globale Compliance-Landschaft hat sich weiter entwickelt, wobei in den letzten zehn Jahren wichtige Entwicklungen in wichtigen Bereichen der Ethik und Compliance stattgefunden haben. Dazu gehört eine beträchtliche Anzahl neuer und aktualisierter Vorschriften, die sich mit der Verhinderung von Korruption und Bestechung, moderner Sklaverei, dem Schutz von Whistleblowern, Sanktionen, der Bekämpfung von Geldwäsche und dem Datenschutz befassen. Gleichzeitig wurden eine Reihe von Initiativen, Richtlinien und Standards veröffentlicht, die versuchen, die Vielfalt der nationalen Rechtssysteme zu harmonisieren und Unternehmen zu ethischen Praktiken zu verpflichten.

[15] USSC Press release, May 3, 2004 [16] SEC

PLANEN

EINE ETHIK- UND COMPLIANCE-STRATEGIE ERSTELLEN

Um das Beste aus Ihrem Ethik- und Compliance-Programm herauszuholen, bedarf es einer sorgfältigen Planung. Ihre Strategie sollte aufbauen auf: einem klaren Verständnis der Compliance-Struktur und der zukünftigen Meldewege; einem gesicherten Budget, das angemessenes Compliance-Personal und -Ressourcen berücksichtigt, und auf einem Überblick über die Compliance- und ethikbezogenen Risiken, die in Ihrem Aufgabenbereich liegen müssen.

Struktur und Meldewege einrichten

Die Positionierung, Struktur und Verantwortlichkeiten der Compliance-Funktion können je nach Unternehmen stark variieren und werden in der Regel durch die Größe, das Geschäftsmodell, das Risikoprofil und die Unternehmenskultur bestimmt. Aufsichtsbehörden und Strafverfolger erkennen an, dass unterschiedliche Strukturen ein effektives Programm unterstützen können.

Dennoch wird von Organisationen erwartet, dass sie die von ihnen getroffenen strukturellen Entscheidungen begründen. Die Strukturen können zentral oder dezentral, funktional (d. h. auf einen bestimmten Risikobereich fokussiert), einer Geschäftseinheit (meist der Rechtsabteilung) zugeordnet oder völlig unabhängig sein.

Für **kleine und mittelständische Unternehmen** werden sich die wichtigsten strukturellen Überlegungen darauf konzentrieren, ob die Compliance-Funktion (oder der/die Compliance-Beauftragte) einen unabhängigen oder halbautonomen Status haben wird:

Unabhängige Struktur
Die Compliance-Funktion ist eine eigenständige operative Einheit, wobei der Chief Ethics and Compliance Officer (CECO) dem Geschäftsführer unterstellt ist. Es überrascht nicht, dass diese Struktur von den Aufsichts- und Strafverfolgungsbehörden als die zur Gewährleistung der Unabhängigkeit des Programms effektivste anerkannt wurde.

Halb-autonome Struktur
Die Compliance-Funktion ist einer anderen Abteilung angegliedert (meist der Rechtsabteilung) und der CECO ist dem General Counsel (Leitung der Rechtsabteilung) unterstellt. Obwohl dem Vorstand nicht unterstellt, sollte der oder die CECO dem Vorstand regelmäßig Bericht erstatten, um eine kontinuierliche Unabhängigkeit des Programms zu gewährleisten. Alternativ nimmt der General Counsel die Rolle des CECO ein. Obwohl die Einhaltung gesetzlicher Vorschriften als natürlicher Teil der Rechtsabteilung eines Unternehmens angesehen werden kann, kann diese Struktur dazu führen, dass die Einhaltung von Vorschriften zu einem „zweitrangigen" Thema wird.

Größere Unternehmen möchten vielleicht auch die Unterschiede zwischen einer zentralisierten und einer dezentralisierten Struktur berücksichtigen:

Zentralisierte Struktur
Compliance-Beauftragte stehen in einer „Dotted-Line"-Beziehung zu ihren Geschäftsleitungskollegen, berichten aber funktional nicht an diese. In größeren oder multinationalen Organisationen berichten sie an eine zentrale Compliance-Abteilung, unabhängig davon, wo sie sich befinden oder welcher Geschäftsfunktion sie zugeordnet sind. Befürworter dieses Ansatzes führen die Unabhängigkeit der Compliance-Beauftragten von den Geschäftseinheiten und die Standardisierung der Compliance-Aktivitäten an.

Dezentralisierte Struktur
Jede Geschäftseinheit verfügt über einen lokalen Compliance-Beauftragten, der die Freiheit und Befugnis hat, ein Programm zu entwickeln, das den eigenen Bedürfnissen und Anforderungen der Geschäftseinheiten entspricht, wobei eine kleine Compliance-Funktion auf Konzernebene die erforderlichen Mindeststandards festlegt. Für größere Organisationen bietet dieser Ansatz Flexibilität und kann ideal sein für stark diversifizierte Organisationen, solche, die über verschiedene Rechtssysteme hinweg operieren oder unterschiedliche Risikofaktoren zwischen den Einheiten haben.

Best Practice: Das sollten Sie beachten

Wählen Sie die Struktur, die für Ihre Organisation am besten geeignet ist. Wenn Sie noch am Anfang stehen, könnten dies einige der wichtigsten Fragen sein, die Sie beantworten müssen:

- Wird das Compliance-Programm eine selbstständige Abteilung sein? Wenn ja, wo wird es arbeiten und wem wird es unterstellt sein (administrativ und operativ)?
- Wird das Compliance-Programm Teil einer anderen Einheit sein? Wenn ja, welche Einheit(en) soll(en) diese Aufgaben übernehmen?
- Gibt es Empfehlungen zur Strukturierung der Compliance-Funktion von der primären Aufsichtsbehörde des Unternehmens?

Beachten Sie, dass die von Ihnen eingerichtete Struktur die folgenden gesetzlichen Anforderungen erfüllen muss, damit Ihr Ethik- und Compliance-Programm als effektiv eingestuft werden kann:

- Es gibt eine Führungskraft (Leitende/r Manager/in), welche die Gesamtverantwortung für das Programm trägt.
- Es gibt designierte Personen, die mit der täglichen operativen Verantwortung für das Programm betraut sind.
- Diese Person(en) berichten regelmäßig der Führungskraft und gegebenenfalls dem Vorstand oder einem zuständigen Vorstandsausschuss über die Wirksamkeit des Programms.[17]
- Um ihre operative Verantwortung wahrnehmen zu können, verfügen diese Personen über ausreichende Ressourcen, angemessene Erfahrung und Qualifikationen, Dienstalter und Status sowie ausreichenden direkten und indirekten Zugang zu relevanten Datenquellen, dem Vorstand oder einem entsprechenden Ausschuss.[18]

[17] FSGO, §8B2.1(b) (2) (A) - (C). [18] DOJ, Evaluation of Corporate Compliance Programs, Juni 2020, S.12.

Den Umfang der Funktion definieren

Es ist wichtig, den Aufgabenbereich Ihrer Compliance-Abteilung von Anfang an zu definieren. Unabhängig davon, wer für was zuständig ist, müssen alle Risiken in der gesamten Organisation effektiv verwaltet werden. Lücken oder Überschneidungen im Compliance-Management schaffen Verwirrung und könnten neue und unvorhergesehene Konsequenzen nach sich ziehen.

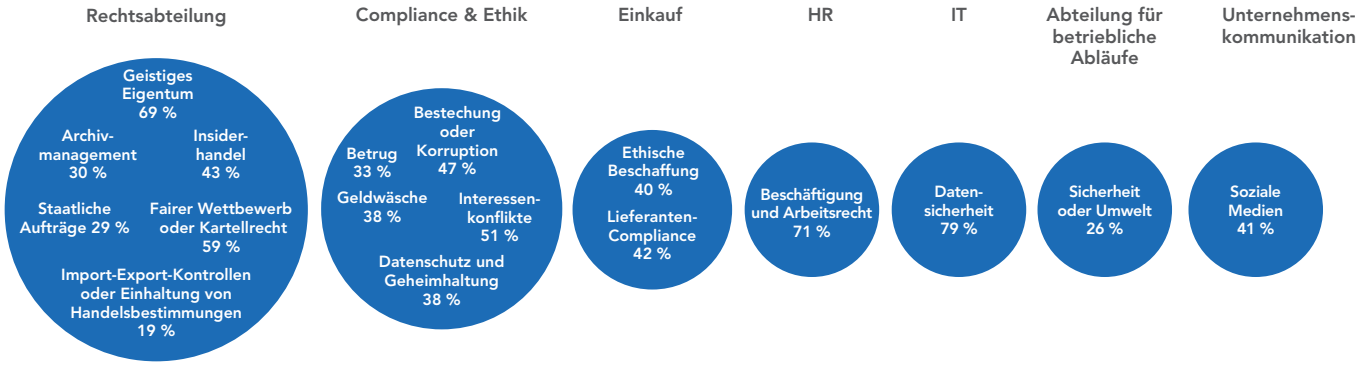
In den meisten Unternehmen werden viele der Compliance-Aufgaben ganz oder teilweise außerhalb der Corporate-Compliance-Funktion erledigt. Für andere Bereiche, wie z. B. das Management von Anti-Korruptions- und Whistleblowing-Hotlines, wird die Compliance-Funktion die Hauptverantwortung übernehmen. Operative Bereiche der Compliance - wie z. B. Datenschutz oder die Einhaltung von Handelsbestimmungen - werden eher direkt auf der Betriebsebene verwaltet, und die Compliance-Funktion bietet dabei lediglich Aufsicht und Unterstützung.

Viele Compliance-Bereiche erfordern die Zusammenarbeit zwischen mehreren Zuständigkeitsbereichen. Denken Sie beispielsweise an Risiken in der Lieferkette: Die Compliance-Funktion, der Einkauf, der Vertrieb und Lieferketten-Manager sollten zusammenarbeiten, um sicherzustellen, dass dieses kritische Risiko effektiv gemanagt wird.

Kommunizieren Sie Ihren Geltungsbereich an andere Risikoeigner, um ein gemeinsames Verständnis und eine klare Verantwortlichkeit für Compliance-Verpflichtungen in der gesamten Organisation zu schaffen. Denken Sie über die Einrichtung von Mechanismen nach, die die Zusammenarbeit und Koordination von Aktivitäten zwischen der Compliance-Funktion und anderen Einheiten erleichtern. Ihr Interagieren ist der Schlüssel zum Erfolg des Programms.

Wem „gehören" die Ethik- und Compliance-Risiken?

Dieses Diagramm veranschaulicht, welche Abteilung in einer Umfrage von PwC 2016 am häufigsten als „Eigentümer" von Compliance- und ethikbezogenen Risiken genannt wurde. Die angegebenen Zahlen zeigen den Prozentsatz der Befragten, die diese Abteilung als „Eigentümer" ausgewählt haben. Die Größe des Kreises hängt von der Anzahl der Risiken ab, die die Abteilung oder Funktion „besitzt" (und die am häufigsten als führend genannt werden).



Quelle: PWC-Studie zum Stand der Compliance 2016 ›››

Das richtige Team zusammenstellen

Die personelle Ausstattung Ihres Programms hängt von seinem Umfang und den Ressourcen ab, die der Organisation zur Verfügung stehen. Die Fähigkeiten, das Wissen und die Erfahrung der Compliance-Mitarbeiter sind entscheidende Faktoren für den Erfolg des Programms. Bei der Zusammenstellung Ihres Teams haben Sie eine große Auswahl: Rechtsanwälte, Wirtschaftsprüfer, Verhaltenspsychologen, Wirtschaftsethiker und Pädagogen, um nur einige zu nennen.

Eine Option, die von einigen Unternehmen gewählt wurde, ist die Einstellung ehemaliger Mitarbeiterinnen und Mitarbeiter der Aufsichtsbehörden ihrer Branche, die über umfassende Kenntnisse zu aufsichtsrechtlichen Fragen, Ermittlungspraktiken und Personal verfügen. Wenn Sie vor einer Personalentscheidung stehen, sollten Sie die folgenden Überlegungen anstellen:

Generalist vs. technischer Compliance-Beauftragter
Der Generalist konzentriert sich auf allgemeine Themen wie Ethik, Kultur, Schulung und Kommunikation. Ein technischer Compliance-Beauftragter hat ein Auge auf die Belange des technischen Regelwerks wie Compliance-Audits, Risikobewertungen und Monitoring.

Interne Position vs. externe Anstellung
Ein aktueller Mitarbeiter kennt das Unternehmen und seine inneren Abläufe möglicherweise sehr gut, während ein Externer neue Erfahrungen und Fachkenntnisse mitbringt.

Vollzeit- vs. Teilzeitmitarbeiter
Für viele Organisationen mit geografisch verstreuten Standorten (oder mit begrenzten Ressourcen) können Teilzeit-„Champions" für Ethik und Compliance die einzige praktikable Option sein. Diese „Champions" haben eine Vollzeitfunktion in ihrem Unternehmen, typischerweise im Finanz-, Personal- oder Beschaffungsbereich, tragen aber zusätzlich Compliance-Verantwortung. Zusätzlich zu ihren Management-Berichtslinien gibt es eine Dotted-Line-Berichterstattung an die Corporate Compliance-Funktion.

Chief Ethics and Compliance Officer: Wichtige Kompetenzen und Eigenschaften

Adaptiert von: A. Hayward und T. Osborn, The Business Guide to Effective Compliance and Ethics. Why Compliance isn't working - and how to fix it, 1. Auflage, Kogan Page, 2019.

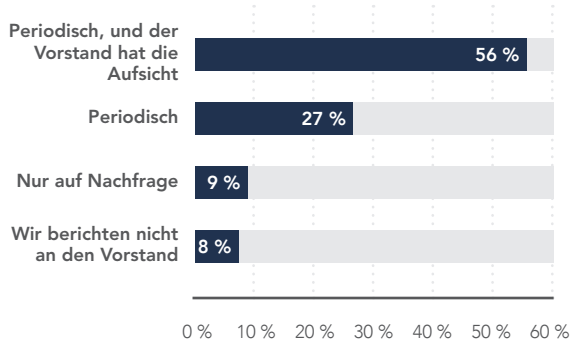
Das Programm koordinieren

Es ist wichtig sicherzustellen, dass die Programmkomponenten effektiv funktionieren, wenn sie zusammengefügt werden. Der Schlüssel dazu ist die Erstellung eines klaren Plans, wie das Programm koordiniert werden soll.

Die Rolle des Vorstands

Mit zunehmender Rechtsdurchsetzung stehen CEOs und Vorstandsmitglieder unter Druck, sowohl die Compliance- und Ethikaufsicht als auch die Verantwortung für die Unternehmensführung wahrzunehmen. Die Vorstände sind angehalten, dem Compliance-Beauftragten hierzu Zugang zu gewähren und die Umsetzung und Wirksamkeit des Programms zu überwachen - allerdings ohne die Vorstände zu Mikromanagern zu machen. Die Bedeutung eines regelmäßigen periodischen Austauschs mit dem Vorstand, und nicht nur nach Aufforderung, kann nicht genug betont werden. Eine erfolgreiche Zusammenarbeit mit dem Vorstand schafft Möglichkeiten für ein tieferes Engagement und Verbesserungen der Unternehmenskultur und kann dazu beitragen, das Vertrauen und den Respekt für die Leistungen des Ethik- und Compliance-Programms des Unternehmens zu stärken.

Wie oft tauschen sich die Compliance-Funktionen mit dem Vorstand aus?



	Reifegrad des Programms				
	Reaktiv	Einfach	Definierend	Reifend	Fortgeschritten
Periodisch, und der Vorstand hat die Aufsicht	26 %	43 %	56 %	78 %	86 %
Periodisch	29 %	33 %	29 %	19 %	12 %
Nur auf Nachfrage	24 %	12 %	7 %	2 %	1 %
Wir berichten nicht an den Vorstand	20 %	12 %	7 %	1 %	1 %

Basis: Alle Befragten ohne diejenigen, die „weiß nicht" antworteten. n=1.241

Quelle: NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020, page 48 >>>

Zusammenarbeit und Networking

Kommunikation und Zusammenarbeit sind der Schlüssel für ein effektives Risikomanagement - und für den Gesamterfolg Ihres Ethik- und Compliance-Programms.

Compliance-Ausschüsse sind ein beliebter Mechanismus für die formelle Koordinierung gemeinsamer Anstrengungen von Teams. Obwohl sie auf verschiedenen Organisationsebenen eingerichtet werden können, gehören ihnen typischerweise Vertreter der wichtigsten Geschäfts- oder Betriebseinheiten sowie der Funktionen Recht, Compliance, Audit, Risiko, Personal, Finanzen und Beschaffung an.

„Der Vorstand sollte eine aktive Rolle übernehmen bei der Gestaltung des Gesamtbildes von Ethik und Compliance im Unternehmen."

Carrie Penman, NAVEX Global

Aufbau interner Partnerschaften

Zusammenarbeit mit dem Vorstand
Stellen Sie auf der Grundlage der wichtigsten gesetzlichen Anforderungen und Best-Practice-Beispiele sicher, dass Sie die folgenden Punkte bei der Zusammenarbeit mit dem Vorstand abdecken:

- Stellen Sie sicher, dass alle Vorstandsmitglieder ihre Verantwortung in Bezug auf das Programm und die geltenden Vorschriften verstehen.
- Berichten Sie über den Inhalt und die Durchführung des Programms auf vierteljährlicher Basis.
- Reichen Sie das Compliance-Budget und den Personalbestand zur Überprüfung und Genehmigung ein.
- Etablieren Sie einen Eskalationsprozess, um die rechtzeitige Meldung und Lösung von Vorfällen sicherzustellen.
- Bieten Sie effektive und rollenrelevante Schulungen an.
- Machen Sie den Vorstand auf Risikobewertungen und vorstandsspezifische Risiken für das Unternehmen aufmerksam.
- Halten Sie die Vorstandsmitglieder über sich entwickelnde Trends und Themen von Interesse auf dem Laufenden.

Andere Teams einbinden
Um Verständnis und Partnerschaften über alle Ebenen des Unternehmens hinweg aufzubauen, sollten Sie die folgenden Taktiken in Betracht ziehen:

- Zeigen Sie die Relevanz von Ethik und Compliance für das Unternehmen: Gehen Sie auf die Mitarbeiter zu und erklären Sie, was Sie tun, wie Sie es tun und warum es wichtig ist.
- Zeigen Sie echtes Interesse: Sprechen Sie mit den Unternehmensfunktionen, um eine Vorstellung davon zu bekommen, was sie beschäftigt.
- Schaffen Sie informelle Kommunikationswege: Knüpfen Sie Kontakte und lernen Sie die Menschen kennen, mit denen Sie arbeiten.
- Bauen Sie ein Netzwerk von Unterstützern auf: Pflegen Sie Vertrauen, gegenseitigen Respekt und Verständnis in Ihren Interaktionen.

Eine Strategie entwickeln

Sobald die Struktur, die Meldewege und der Compliance-Bereich definiert und festgelegt sind, kann der Planungsprozess zur Strategieentwicklung übergehen.

Ein effektives Ethik- und Compliance-Programm muss ganzheitlich, risikobasiert und je nach Größe, geografischer Lage und Risikoprofil Ihres Unternehmens skalierbar sein. Berücksichtigen Sie bei der Konzeption und Planung des Programms die folgenden strategischen Überlegungen, um den Erfolg sicherzustellen.

Einbindung von Führung und Management

Führung wird traditionell mit der Fähigkeit in Verbindung gebracht, andere zu beeinflussen und zu motivieren, deshalb spielt sie eine wichtige Rolle in der Unternehmenskultur. Die erkennbare Unterstützung durch die oberste Führungsebene ist entscheidend für jedes Programm, das das Verhalten der Mitarbeiter beeinflussen oder verändern soll. Wenn ein Programm als unwichtig, lästig oder als Bedrohung für das Top-Management angesehen wird, werden die Mitarbeiter ihm nicht vertrauen und sich nicht darauf einlassen.

Die Vorstellung, dass die ethische Kultur einer Organisation allein durch die Botschaft des Vorstands und des CEOs geprägt wird, ist jedoch naiv. Obwohl es mit dem „Ton an der Spitze" beginnt, spielen die mittleren Führungskräfte und die fachlichen Vorgesetzten eine ebenso wichtige Rolle bei der Gestaltung eines Umfeldes, das ethisches Verhalten fördert und unterstützt. Durch ihre Handlungen beziehungsweise Untätigkeit, ihre Entscheidungen und die Verhaltensweisen, die sie belohnen, disziplinieren oder ignorieren, vermitteln Führungskräfte und Vorgesetzte eine starke Botschaft darüber, was wirklich geschätzt wird und was erforderlich ist, um beruflich zu überleben und erfolgreich zu sein.

Das Budget sichern

Compliance erfordert Investitionen. Aber selbst wenn die gesetzlichen Anforderungen steigen, erkennen viele Unternehmen nicht den Wert, den ein starkes Programm liefern kann. Grob gesagt lassen sich die Kostentreiber eines Ethik- und Compliance-Programms in drei Kategorien einteilen:

- Mitarbeiterzahl
- Verwaltungskosten (Büroräume, Ausrüstung, Verbrauchsmaterial, Reisen)
- Programmkosten (Compliance-bezogene Initiativen, Systeme und Tools, Beratungsgebühren, Konferenzen, Mitarbeiterschulungen usw.)

Es ist wichtig, dass Sie sich an Ihrer Budgetbehörde orientieren. Idealerweise sollte dies der Vorstand oder ein entsprechender Vorstandsausschuss sein. Aufsichtsbehörden und Strafverfolger erwarten, dass die Compliance-Funktionen mit angemessenen Ressourcen ausgestattet sind, um ihr Programm durchführen zu können. Aber wie definiert man „angemessen"?

Die beste Vorgehensweise besteht darin, das Budget und die Personalausstattung auf die identifizierten Ethik- und Compliance-Risiken abzustimmen, um sicherzustellen, dass diese effektiv gehandhabt werden. Als Teil der Aufsichtsfunktion des Vorstands muss dieser sicherstellen, dass das Programm vollständig ausgestattet ist, um die Herausforderungen in Bezug auf Personal und Ressourcen zu bewältigen.

Wie Sie Budget von Ihrem Vorstand bewilligt bekommen

Trotz der ständig zunehmenden gesetzlichen Anforderungen wird die Einhaltung von Vorschriften oft als Kostenfaktor und nicht als Geschäftsfaktor angesehen. Es liegt in der Verantwortung des CECO, den Wert der Compliance-Aktivitäten für das Unternehmen zu kommunizieren und den Vorstand davon zu überzeugen, in das Risikomanagement zu investieren. Erwägen Sie die folgenden Taktiken, um einen überzeugenden Businessplan für Ihren Budgetantrag zu erstellen:

Wählen Sie den richtigen Kommunikationsstil
Kennen Sie Ihre Zielgruppe und passen Sie Ihre Botschaft an deren Erwartungen an, z. B. in Bezug auf die Präsentation von Daten (Zahlen, Grafiken oder weiche Daten) und die Detailtiefe (ein Überblick auf hohem Niveau gegenüber einem tiefen Eintauchen in Fakten und Details).

Präsentieren Sie den Businessplan
Ihr Vorstand lebt nicht unbedingt in der Welt der Ethik und Compliance. Es ist daher Ihre Aufgabe, Argumente in der seinen vertrauten Terminologie vorzubereiten und zu entwickeln. Vergewissern Sie sich, dass Sie die übergeordneten Geschäftsziele des Unternehmens verstehen und erklären können, wie die Investition in Compliance das Unternehmen bei diesen Bemühungen unterstützt.

Gehen Sie proaktiv mit den Compliance-Kosten um
Fünfundvierzig Prozent der Unternehmen mit fortschrittlichen Ethik- und Compliance-Programmen geben mehr als ein Viertel ihres Budgets für Technologielösungen aus.[19] Angesichts steigender Compliance-Budgets besteht eine Möglichkeit, die wachsende Liste von Anforderungen zu bewältigen, darin, die Effizienz integrierter Risiko- und Compliance-Lösungen zu nutzen. Zeigen Sie dem Vorstand, dass Sie nicht nur um Geld bitten, sondern dass Sie die Berechnungen durchdacht haben. Legen Sie den Kostenunterschied zwischen der Einstellung von mehr Personal und dem Einsatz von Technologie dar. Zeigen Sie, dass Sie kostenbewusst sind und versuchen, das Geld der Organisation sinnvoll zu investieren.

[19] NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020, Seite 28 ›››

Überprüfen Sie Ihr regulatorisches Umfeld

Es gibt zwar keinen einzelnen eigenständigen Leitfaden, der für alle Situationen oder Organisationen geeignet ist, aber viele der wichtigsten Richtlinien und Rahmenwerke orientieren sich an ähnlichen Standards - wenn auch mit unterschiedlichem Augenmerk auf Programmkomponenten (wie z. B. der Bekämpfung von Bestechung und Korruption).

Bei der Gestaltung Ihres Ethik- und Compliance-Programms ist es vielleicht am sinnvollsten, mit diesen Leitmaßnahmen für ein abgerundetes Programm zu beginnen:

- **FSGO** 8B2.1
- **OECD** 13 Good Practices on Internal Controls, Ethics, and Compliance
- US **DOJ** Bewertung von Corporate Compliance-Programmen
- UK Ministry of Justice Leitfaden zum **UK Bribery Act**

Obwohl die meisten dieser Maßnahmen länderspezifisch sind, haben sie Auswirkungen auf die ganze Welt und sind Bestandteil der besten Compliance-Programme.

Vergleich der wichtigsten Themen in führenden Compliance-Frameworks

Ist das Compliance-Programm gut konzipiert?	UK Bribery Act	FSGO	OECD	DOJ
Risikobewertung	✓	✓	✓	✓
Standards, Richtlinien und Verfahren	✓	✓	✓	✓
Schulung und Kommunikation	✓	✓	✓	✓
Vertrauliche Meldestruktur	✗	✓	✓	✓
Untersuchung von Fehlverhalten	✗	✓	✓	✓
Verwaltung von Drittanbietern	✓	✗	✓	✓
Fusionen und Übernahmen	✗	✗	✗	✓
System der internen Kontrollen	✗	✗	✓	✓
Wird das Compliance-Programm effektiv umgesetzt?				
Engagement der Geschäftsleitung	✓	✓	✓	✓
Engagement des mittleren Managements	✗	✗	✓	✓
Eigenständigkeit und Ressourcen einer Compliance-Funktion	✗	✓	✓	✓
Due Diligence für Personal mit hoher Autorität	✗	✓	✗	✗
Anreize für Compliance	✗	✓	✓	✓
Disziplinarmaßnahmen bei Nichteinhaltung	✗	✓	✓	✓
Funktioniert das Compliance-Programm in der Praxis?				
Kontinuierliche Verbesserung, periodische Tests und Überprüfung	✓	✓	✓	✓
Kultur der Ethik und Einhaltung von Gesetzen	✗	✓	✗	✓
Analyse und Behebung des zugrunde liegenden Fehlverhaltens	✗	✓	✓	✓

Welche Gesetze und Normen könnten Ihr Unternehmen betreffen?

1. **Nationale Gesetze und Vorschriften** in Gerichtsbarkeiten, in denen Ihr Unternehmen geschäftlich tätig ist, einschließlich solcher, in denen Sie Dritte, Vertreter und Händler einsetzen.
2. **Branchenspezifische Vorschriften.** Diese sind besonders wichtig für Organisationen in stark regulierten Branchen wie dem Gesundheitswesen, Finanzdienstleistungen und Versicherungen.
3. **Gesetzgebung mit extraterritorialer Reichweite.** Zu den prominentesten Beispielen gehören der FCPA, der UK Bribery Act, das Gesetz Sapin II und die EU-DSGVO.
4. **Internationale Normen und Richtlinien**. Diese freiwilligen Initiativen fallen in die Kategorie des „Soft Law" und sind nicht direkt durchsetzbar, werden aber möglicherweise von einigen Kunden oder Partnern - oder innerhalb Ihrer Branche - erwartet. *Beispiel: ISO 37001:2016 Anti-Bribery Management Systems.*
5. **Ihre gesetzlichen oder vertraglichen Verpflichtungen.** Diese können sich auf Verhaltenskodizes für Lieferanten und Compliance-bezogene Klauseln in Verträgen beziehen, die Ihr Unternehmen unterzeichnet hat.

Einbindung der Stakeholder definieren

Zu den Stakeholdern des Programms sollten die Rechtsabteilung, das Risikomanagement, die Innenrevision, die Personalabteilung, der Einkauf, die Finanzabteilung, die Informationstechnologie, die soziale Verantwortung des Unternehmens und die Kommunikation gehören. Die Beteiligten sollten den Implementierungsplan, den Zeitrahmen, die Ressourcen und alle Verbesserungen, die das Programm wertvoller machen würden, diskutieren. Darüber hinaus muss der Vorstand den Implementierungsplan kennen und eventuell einige spezifische Anweisungen bezüglich des Betriebs geben wollen.

Stellen Sie sicher, dass jeder Beteiligte eine klar definierte Rolle im Programm hat. Wenn Sie den Umfang der Compliance-Funktion bereits definiert haben, haben Sie ein besseres Verständnis dafür, wer in Ihrer Organisation für die Risiken verantwortlich ist und welche Rolle er bei der Umsetzung des Programms spielen wird. Entwickeln und dokumentieren Sie einen Zeitplan für die Implementierung, der festlegt, wer den Prozess leitet, wer ihn koordiniert und wer Unterstützung leistet. Erstellen Sie eine formale Eskalationsrichtlinie, die detailliert festlegt, was die Geschäftsführung und der Vorstand wann wissen müssen.

Für bekannte Herausforderungen planen

Es gibt mehrere allgemeine organisatorische Herausforderungen, denen Sie bei der Implementierung eines Ethik- und Compliance-Programms begegnen können. Sie umfassen:

- Definition von Schlüsselpersonen und deren Rollen frühzeitig im Prozess.
- Effektive Kommunikation mit Implementierungsteams und Stakeholdern.
- Verstehen der bereits vorhandenen Prozesse, Verfahren, Daten, Systeme und Teams.
- Koordinierung von Teams, die durch geografische Grenzen getrennt sind.
- Gewinnung von Beteiligung und Input aus allen Ebenen des Managements.
- Regulatorische Änderungen verfolgen.
- Unzureichende oder stagnierende Budgets und begrenzte Programmressourcen.

Indem Sie frühzeitig Maßnahmen ergreifen, um diese Herausforderungen zu entschärfen, können Sie sicherstellen, dass Ihr Fortschritt nicht durch vermeidbare Rückschläge unterbrochen wird

Fokus auf Ethik

Viele Unternehmen haben Compliance-basierte Programme. Wie der Name schon sagt, konzentrieren sich diese Programme auf spezifische regulatorische Risiken, mit denen die Organisation konfrontiert ist, die ihrerseits komplex, vielschichtig und ständig im Wandel begriffen sein können.

Wertebasierte Programme betonen „das Richtige zu tun" und werden, wenig überraschend, als effektiver zur Abschreckung von unethischem Verhalten angesehen. Durch die Verankerung eines Verständnisses der allgemeinen ethischen Grundsätze, wie sie in Ihrem Verhaltenskodex niedergelegt sind, können Sie sicher sein, dass sich Ihre Mitarbeiter mit den Werten identifizieren können, zu deren Einhaltung Sie sie auffordern. Sie werden auch den Grund nachvollziehen können - im Gegensatz zu einer Reihe von technischen Regeln und Vorschriften.

Tappen Sie nicht in die Falle, Ethik als Compliance-Anforderung durch ständige Überwachung und strenge Kontrollen „aufzuzwingen". Mitarbeiter sollten ermutigt werden, die ethischen Implikationen einer Entscheidung zu bedenken, wenn sie sich in einem moralischen Dilemma befinden. Daher sollte die Ethik als Entscheidungsrahmen und nicht als fester Bezugspunkt kommuniziert und gefördert werden.

Effektiv umsetzen

Aufsichtsbehörden und Strafverfolger verlangen, dass jedes Unternehmen sein Programm auf seine eigenen Bedürfnisse, seine Größe, sein Geschäftsmodell, seine geografische Verteilung und sein Risikoprofil abstimmt. Es gibt keine einheitliche Lösung für alle. Wichtig ist, dass das Programm „in effektiver Weise umgesetzt, überprüft und ggf. überarbeitet wird"[20].

Aufsichtsbehörden haben oft ihre Frustration über die „Papierprogramme" zum Ausdruck gebracht, die man in der Geschäftswelt häufig antrifft. Die Richtlinien sind geschrieben, die Verfahren sind verabschiedet - aber was fehlt, ist vielleicht das wichtigste Element: die Umsetzung. Ihr Ethik- und Compliance-Programm sollte Substanz haben und in die täglichen Abläufe Ihres Unternehmens eingebettet sein.

[20] US-Justizministerium, 9-28.000 - Principles of Federal Prosecution of Business Organizations, Corporate Compliance Programs, Punkt B.

IMPLEMENTIEREN

EINRICHTEN DES ETHIK- UND COMPLIANCE-PROGRAMMS

Mit einer klar definierten Strategie und einem Budget sind Sie bereit, mit der Umsetzung Ihres Ethik- und Compliance-Programms zu beginnen. In diesem Abschnitt erfahren Sie, wie ein effektives Programm aufgebaut sein sollte, welche Elemente unerlässlich sind und wie sie auf die Branche, die Größe, die Historie und das Risikoprofil Ihres Unternehmens zugeschnitten werden müssen.

Best Practice: Die acht wesentlichen Elemente eines effektiven Programms

Aufsichtsbehörden und Strafverfolger weltweit erwarten von Unternehmen, dass sie unternehmerisches Fehlverhalten aufdecken und verhindern. Auch wenn die Leitlinien unterschiedlich sind, lassen sich die wichtigsten Anforderungen in acht wesentliche Elemente zusammenfassen, die ein starkes Compliance- und Ethikprogramm berücksichtigen muss. Wenn Sie diese Elemente erfolgreich in Ihr eigenes Programm integrieren, können Sie den Ruf Ihres Unternehmens schützen, das Engagement der Mitarbeiter fördern und die Unternehmenskultur verbessern.

Risikobewertung

Eine Risikobewertung ist der Schlüssel zur Entwicklung des Risikoprofils Ihrer Organisation. Sie sollte die fogenden Punkte identifizieren:

- Ethik-, Compliance- und Reputationsrisiken, denen Ihr Unternehmen aufgrund seiner Branche und Standorte ausgesetzt sein kann
- Risiken im Zusammenhang mit Ihrer Belegschaft
- Ihre aktuellen und geplanten Strategien zur Risikominderung, um das Risiko auf ein für Ihr Unternehmen akzeptables Niveau zu reduzieren

Risikobewertungen sollten auf dem neuesten Stand gehalten und regelmäßig überprüft werden, basierend auf dem kontinuierlichen Zugriff auf Betriebsdaten und Informationen aus dem gesamten Unternehmen.

Vergessen Sie nicht, dass es Dritte gibt.
Der Umfassende Leitfaden für das Management von durch Drittparteien verursachten Risiken von NAVEX Global hilft Ihnen bei der Navigation in diesem zunehmend wichtigen Bereich des Compliance-Risikos.

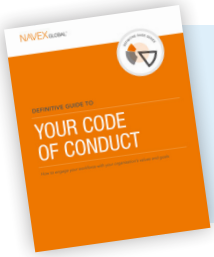
Aufsicht, Struktur und Führung

Ihr Programm benötigt sowohl eine angemessene Aufsicht (zum Schutz vor Risiken) als auch das Engagement der Führungsebene (um Verhalten und Kultur voranzutreiben). Diejenigen, die wichtige Aufsichtspflichten haben, einschließlich Ihres Vorstands, müssen über ihre Rollen informiert und geschult werden, um Ihrer Organisation zu einem effektiven Programm zu verhelfen.

„Selbst ein gut konzipiertes Compliance-Programm kann in der Praxis erfolglos sein, wenn die Umsetzung lax, mit zu wenig Ressourcen ausgestattet oder anderweitig ineffektiv ist."
US DOJ Criminal Division 'Bewertung von Compliance-Programmen in Unternehmen'

Normen, Richtlinien und Prozeduren

Bei der Entwicklung Ihres Programms werden Richtlinien und Verfahren eine entscheidende Rolle spielen. Ihr Verhaltenskodex sollte die Basisrichtlinie sein, unterstützt durch Standards und Verfahren, die die Einhaltung interner Werte sowie geltender Gesetze, Regeln und Vorschriften vorantreiben.



Der Umfassende Leitfaden für Ihren Verhaltenskodex von NAVEX Global erklärt, wie Sie Ihren Verhaltenskodex in eine ansprechende Mitarbeiter-ressource verwandeln können.

Über die Entwicklung dieser Richtlinien hinaus muss auch darüber nachgedacht werden, wie Sie diese verwalten und kommunizieren werden. Denken Sie daran, dass eine klare Kommunikation der Erwartungen an Ethik und Compliance ein grundlegender Schritt zur Schaffung einer Kultur ist, die ein effektives Programm unterstützt.

Der Umfassende Leitfaden für die Richtlinien- und Verfahrensverwaltung von NAVEX Global bietet eine Anleitung zur Optimierung Ihres Richtlinien- und Verfahrensmanagementprogramms.

Ausrichtung auf HR-Praktiken

Ein effektives Compliance-Programm hat viele Berührungspunkte und Überschneidungen mit der Personalabteilung eines Unternehmens. Zum Beispiel sendet die Auswahl der Personen, die ein Unternehmen einstellt und fördert, ein klares Signal über seine Ziele und Prioritäten. Achten Sie nicht nur auf eine sorgfältige Einstellungspraxis, sondern auch darauf, Leistungskennzahlen und Anreize mit ethischem und gesetzeskonformem Verhalten in Einklang zu bringen und eine konsequente Disziplinarpolitik anzuwenden. Die Entwicklung positiver Beziehungen zwischen Ethik und Compliance und der Personalabteilung ebnet den Weg für eine ethische Unternehmenskultur und sendet eine klare Botschaft, dass unethisches Verhalten nicht toleriert wird.

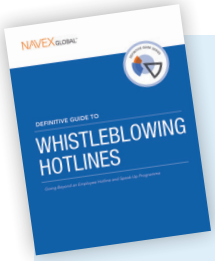
Kommunikation und Schulung

Die Aufsichtsbehörden erwarten von Organisationen, dass sie Standards und Verfahren an den Vorstand, hochrangige Mitarbeiter, Angestellte und (gegebenenfalls) Dritte weitergeben. Daher sollten die Richtlinien und Verfahren in Ihrem Ethik- und Compliance-Programm von einem strategischen Kommunikationsplan und einem Schulungsprogramm begleitet werden. Dadurch wird sichergestellt, dass die Mitarbeiter über die für sie geltenden Richtlinien informiert sind und diese auch einhalten. Ein regelmäßiger und effektiver Schulungsplan stellt sicher, dass die Mitarbeiter verstehen, was von ihnen erwartet wird. Er hilft außerdem Managern entscheiden, wie sie auf aufgeworfene Probleme reagieren sollen und stellt sicher, dass die gewonnenen Erkenntnisse konsequent zur Verbesserung der Unternehmenskultur genutzt werden.

Der Umfassende Leitfaden für das Ethik-& Compliance-Schulungsprogramm von NAVEX Global bietet eine Anleitung zur Verwaltung Ihres Mitarbeiterschulungsprogramms.

Melden und Reagieren

Der Meldeprozess ermöglicht es den Mitarbeitern, ihre Anliegen an Ihre Organisation heranzutragen. Jedes Ethik- und Compliance-Programm muss den Mitarbeitern Möglichkeiten bieten, Probleme einfach und bequem zu melden, ohne Angst vor Vergeltungsmaßnahmen. Es sollte auch gemessene Schritte enthalten, um auf diese Berichte zu reagieren und sie zu lösen, einschließlich Untersuchungen und Disziplinarverfahren.



Der Umfassende Leitfaden für Whistleblowing-Systeme von NAVEX Global bietet eine Anleitung, wie Sie Ihren Melde- und Reaktionsprozess verbessern können.

Überwachung und Bewertung

Die Messung und Überwachung Ihres Programms ist der einzige Weg, um zu wissen, ob es wirklich effektiv ist. Aufsichtsbehörden wie das DOJ erwarten von Unternehmen, dass sie „angemessene Schritte" unternehmen, um „sicherzustellen, dass das Compliance- und Ethikprogramm der Organisation befolgt wird, einschließlich der Überwachung und Prüfung zur Aufdeckung von kriminellem Verhalten", und „regelmäßig die Effektivität des Programms der Organisation bewerten "[21]. Sie müssen daher regelmäßig sinnvolle Maßnahmen ergreifen, um Ihr Ethik- und Compliance-Programm zu überprüfen und sicherzustellen, dass es sich im Laufe der Zeit weiterentwickelt.

Der Umfassende Leitfaden für die Beurteilung von Compliance-Programmen von NAVEX Global bietet eine Anleitung zur Bewertung und Verbesserung Ihres Compliance-Programms.

Kultur

Die Compliance-Vorschriften bekräftigen den Gedanken, dass Sie für ein effektives Programm eine Kultur pflegen müssen, die Compliance und Ethik fördert - nicht nur Regeln und zusätzliche Kontrollen. Erfolgreiche Programme sind integrierte Bemühungen, die finanzielle und Compliance-Anforderungen mit der Mission und den Werten einer Organisation in Einklang bringen. Vorausschauende Unternehmen bauen Kulturen auf, in denen die Mitarbeiter wissen, dass es erwartet wird, das Richtige zu tun. Sie verstehen die für sie geltenden Standards und glauben an die Integrität ihrer Führungskräfte. Dieselben Mitarbeiter sollten sich befähigt fühlen, Bedenken über Fehlverhalten vertrauensvoll und ohne Angst vor Vergeltungsmaßnahmen zu äußern.

Integrierte Ethik und Compliance

Auch wenn der primäre Fokus der Compliance-Beauftragten eher auf der Korruptionsbekämpfung liegt, kann das Rahmenwerk der acht Elemente auch in anderen Bereichen Ihres Ethik- und Compliance-Programms praktisch und effektiv angewendet werden, z. B:

- Handel
- Kartellrecht
- Interessenkonflikte
- Datenschutz
- Anti-Geldwäsche
- Anti-Diskriminierung
- Moderne Sklaverei
- sexuelle Belästigung
- IT-Sicherheit
- Betrug

[21] US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, Juni 2020, S. 3.

Vorbeugen - Erkennen - Reagieren

Ein Ethik- und Compliance-Management-System kann in drei Handlungsebenen unterteilt werden:

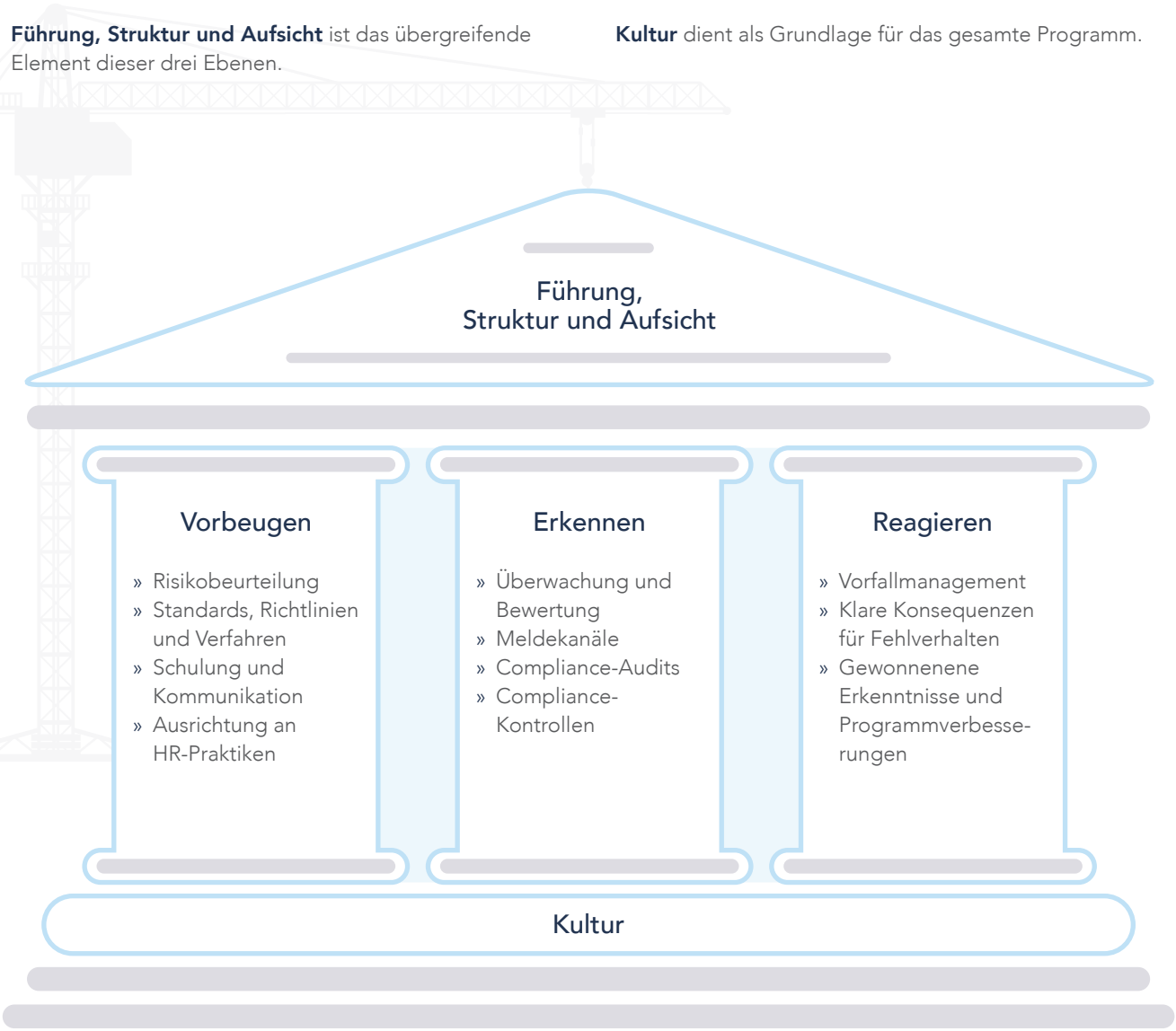
» **1. Vorbeugen:** Zu den Präventivmaßnahmen gehören Risikobewertungen, Richtlinien und Verfahren, Schulungen und Kommunikation sowie die Anpassung an die Personalpraxis.

» **2. Erkennen:** Überwachung und Bewertung, Meldewege und Vorfallsmanagementprozesse sind unverzichtbar, um Fehlverhalten zu erkennen.

» **3. Reagieren:** Klare Konsequenzen für Fehlverhalten sowie die daraus gezogenen Lehren und Programmverbesserungen bilden die Grundlage für eine effektive Reaktionsstrategie.

Führung, Struktur und Aufsicht ist das übergreifende Element dieser drei Ebenen.

Kultur dient als Grundlage für das gesamte Programm.



Ihr Programm anpassen

Der Kommentar zu den US Federal Sentencing Guidelines for Organizations (FSGO) besagt, dass ein effektives Ethik- und Compliance-Programm die Branche, die Größe und die Historie des Unternehmens berücksichtigt. Es ist daher ratsam, sich vor Beginn der Umsetzung Gedanken darüber zu machen, wie sich diese Parameter auf die Breite und Tiefe des eigenen Programms auswirken könnten.

Branchen-Praxis

Sie können Ihr Programm nach dem Vorbild anerkannter Branchenführer im Bereich Ethik und Compliance gestalten. Prüfen Sie die Verhaltenskodizes und Compliance-Richtlinien der Unternehmen und suchen Sie nach öffentlich zugänglichen Informationen über die Programme, die sie eingerichtet haben. Schauen Sie sich auch branchenspezifische Kodizes genau an - sie sind eine wertvolle Ressource, um Risiken und Praktiken zu identifizieren, mit denen Ihr Unternehmen und seine Mitbewerber konfrontiert sind. Wenn eine Organisation die anwendbaren Branchenpraktiken nicht einbezieht und befolgt, ist es weniger wahrscheinlich, dass ihr Programm von den Aufsichtsbehörden als effektiv angesehen wird.

Größe der Organisation

Aufsichts- und Vollzugsbehörden erwarten von großen Organisationen, dass sie mehr Ressourcen einsetzen und einen formaleren Ansatz für ihre Programme wählen. Im Gegensatz dazu können kleinere Organisationen einen verkürzten Ansatz wählen, vorausgesetzt, sie können „das gleiche Maß an Engagement für ethisches Verhalten und die Einhaltung der Gesetze wie große Organisationen nachweisen."[22] Beispiele für Informalität und den Einsatz von weniger Ressourcen sind:

- Schulungen können auf informellen Personalversammlungen stattfinden
- Überprüfung kann bei regelmäßigen „Rundgängen" durchgeführt werden
- verfügbares Personal kann für die Durchführung des Programms eingesetzt werden

Unternehmensgeschichte

Das erneute Auftreten von ähnlichem Fehlverhalten schafft ein zusätzliches Compliance-Risiko und lässt Zweifel an der Effektivität der Compliance-Bemühungen einer Organisation aufkommen. Eine Vorgeschichte von Compliance-Verstößen würde daher erfordern, dass mehr Ressourcen für das Ethik- und Compliance-Programm bereitgestellt werden.

[22] FSGO, §8B2.1, Kommentar 2(C) (Kap. 1, N. 24). .

Die Risikobewertung

Ein effektives Ethik- und Compliance-Programm sollte auf einem fundierten Verständnis der Risiken beruhen, mit denen das Unternehmen konfrontiert ist. Eine systematische Risikobeurteilung ist daher der wesentliche erste Schritt. Ohne sie könnten Sie Schwierigkeiten haben, zu erklären, warum Ihr Programm so gestaltet wurde, wie es gestaltet wurde, sollten Sie dazu aufgefordert werden.[23]

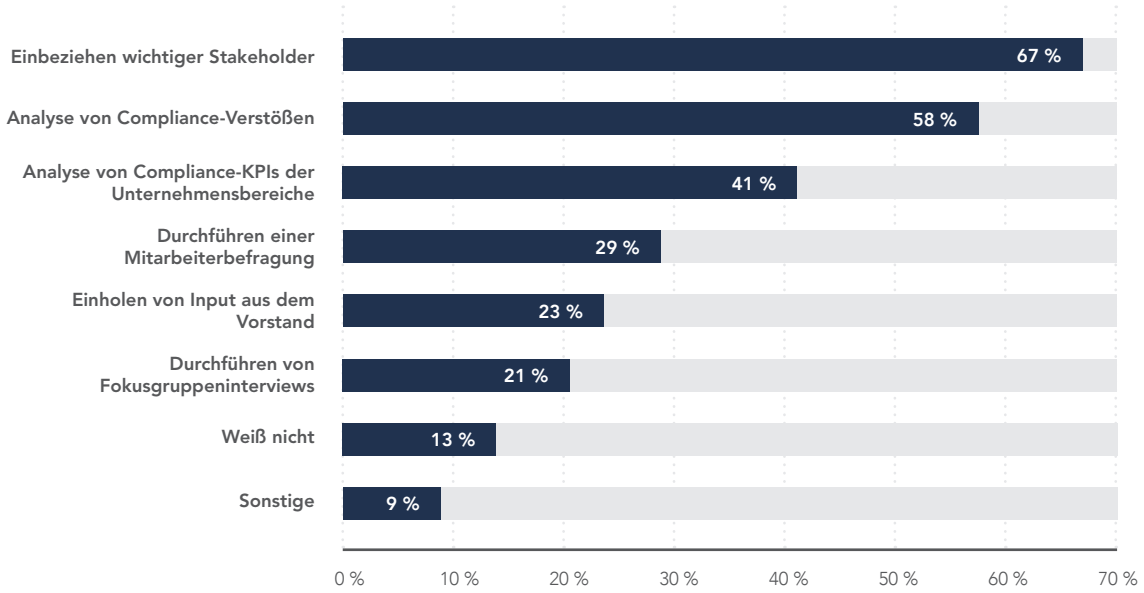
Ihr Risikoprofil ist eine Bewertung, die die einzigartigen Risiken identifiziert, denen Ihr Unternehmen angesichts seiner Branche, Geografie und Mitarbeiterpopulation ausgesetzt sein kann. In vielen Fällen sind Organisationen Vorschriften unterworfen und Risiken ausgesetzt, über die sie wenig wissen. Nach der Durchführung einer gründlichen Risikobeurteilung werden Sie wahrscheinlich Risiken entdecken, die neu sind, vorher nicht sichtbar waren oder die seit der letzten Beurteilung an Bedeutung gewonnen haben.

Laut dem 2020 NAVEX Global Definitive Risk & Compliance Benchmark Report hat die Risikobewertung bei den Befragten eine hohe Priorität. 46 % der Unternehmen planen in den nächsten 12 Monaten eine umfassende organisatorische Risikobewertung durchzuführen.[24]

Glossar

- **Risiko** ist definiert als „Auswirkung von Ungewissheit auf Ziele“[25] und wird meist in Form von Wahrscheinlichkeit und Auswirkung gemessen.
- **Eintrittswahrscheinlichkeit** ist die Wahrscheinlichkeit, mit der ein Risiko eintritt.
- **Auswirkung** sind die Kosten eines Risikos, wenn es eintritt.
- **Effektives Risikomanagement** beinhaltet „die systematische Anwendung von Managementrichtlinien, -verfahren und -praktiken auf die Aktivitäten der Kommunikation, Beratung, Festlegung des Kontextes und der Identifizierung, Analyse, Bewertung, Behandlung, Überwachung und Überprüfung von Risiken.“[26]
- **Eine Ethik- und Compliance-Risikobewertung** identifiziert die Ethik-, Compliance- und Reputationsrisiken der Organisation, die Belegschaft, die das Risiko verursacht, und die aktuellen und geplanten Strategien zur Risikominderung, um das Risiko auf ein für die Organisation akzeptables Niveau zu reduzieren.

Wie führt man eine Compliance-Risikobewertung durch?



Quelle: PWC State of Compliance survey 2015

[23] US DOJ, Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, S. 2 [24] NAVEX Global, The Definitive Risk & Compliance Benchmark Report, 2020 [25] ISO 31000:2018 Risk management – Guidelines, S. 3.1. [26] ISO 31000:2018 Risk management – Guidelines, S.4

Die 10 wichtigsten Schritte einer soliden Ethik- und Compliance-Risikobewertung

1. Die Führungsebene einbinden
Aktive und sichtbare Unterstützung durch die oberste Führungsebene und den Vorstand ist eine Schlüsselkomponente einer erfolgreichen Risikobewertung. Ohne sie können Risikobewertungen an Schwung verlieren, bestimmte Themen vermeiden oder unzureichend behandeln, oder ihre Qualität wird dadurch beeinträchtigt, dass andere Führungskräfte und Manager sich entscheiden, nicht teilzunehmen.

2. Rollen und Verantwortlichkeiten definieren
Legen Sie fest, wer für die Risikobeurteilung verantwortlich sein soll und wer beteiligt werden muss. Klar abgegrenzte Rollen und Verantwortlichkeiten sollten kommuniziert und verstanden werden.

Eine gut informierte Ethik- und Compliance-Risikobewertung berücksichtigt Folgendes:

- Das Geschäftsmodell des Unternehmens
- Den geografischen Standort seines Geschäftsmodells
- Den Industriesektor und die Wettbewerbsfähigkeit des Marktes
- Das regulatorische Umfeld
- Auftraggeber und Kunden
- Produkte und Dienstleistungen
- Lieferkette und Dritte
- Transaktionen und Projekte
- Die Arten, in denen sich Risiken manifestieren können

3. Angemessene Ressourcen sichern
Die Funktion, die die Risikobeurteilung leitet, sei es Compliance oder eine andere Abteilung, wird wahrscheinlich nicht in jedem Bereich über Fachwissen verfügen. Daher ist die Unterstützung durch andere Funktionen wie Recht, Risikomanagement, interne Revision, Vertrieb und Marketing, Beschaffung, Finanzen, Personalwesen, Lieferkette und Unternehmensangelegenheiten erforderlich (diese Liste ist erweiterbar). Die Beteiligten sollten den Implementierungsplan, den Zeitrahmen, die Ressourcen und alle Verbesserungen besprechen, die die Risikobewertung effektiver machen könnten.

4. Risikobereitschaft und Risikotoleranz festlegen
Bestimmen Sie die Risikobereitschaft und Risikotoleranz Ihres Unternehmens frühzeitig im Prozess der Risikobewertung. Risikobereitschaft ist das Ausmaß an Risiko, das eine Organisation bereit ist, zu akzeptieren oder zu behalten, und stellt eine breite Sichtweise des Risikos dar. Risikotoleranz bezieht sich auf bestimmte Risiken und Leistungsziele. Sie kann als Flexibilität der Organisation in Bezug auf bestimmte Risiken definiert werden.

5. Das eigene Arbeitsumfeld verstehen
Sie sollten ein klares Verständnis davon haben, wie Ihr Unternehmen funktioniert. Von einem Unternehmen wird erwartet, dass seine spezifischen Risiken im Kontext seiner Tätigkeit, seiner Standorte, seiner Branche, seiner Wettbewerber, der gesetzlichen Rahmenbedingungen, seiner Kunden und Geschäftspartner analysiert und behandelt. Indem Sie die Art der Betriebsabläufe und Standorte verstehen, können Sie die Arten von Risiken, die für Ihr Unternehmen spezifisch sind, sowie die möglichen Konsequenzen im Falle eines Verstoßes besser einschätzen.

6. Risikoindikatoren identifizieren
Risikoindikatoren sind Messgrößen, mit denen sich Risiken, die die Organisation betreffen, messen lassen. Sie können als Vorzeichen fungieren und frühzeitige Signale für zunehmende Risikobelastungen liefern. Die Analyse der Risikoindikatoren sollte ganzheitlich sein und sowohl interne als auch externe Ressourcen einbeziehen.

7. Daten erheben
Interviews, Umfragen, Selbstbeurteilungen und Brainstorming-Sitzungen sind verschiedene Methoden, um Daten und Informationen darüber zu sammeln, wie und warum Compliance-Risiken in der Organisation auftreten können. Machen Sie sich mit den Vor- und Nachteilen der einzelnen Methoden vertraut, bevor Sie sich für diejenige entscheiden, die für Ihre Ziele der Risikobewertung am besten geeignet ist.

8. Risiken identifizieren
Nachdem Sie den Geschäftsumfang und die Risikoindikatoren kennen, die für die Art der Geschäftstätigkeit und die Standorte spezifisch sind, sollten Sie die Risiken auf eine angemessene Detailebene herunterbrechen. Ziel der Risikoidentifikation ist es, eine umfassende Bestandsaufnahme der Compliance- und Ethik-Risiken zu erstellen, denen Ihr Unternehmen, Ihre Branche und Ihre Region ausgesetzt sind.

9. Wahrscheinlichkeit und Auswirkungen beurteilen
Bewerten Sie sowohl die Wahrscheinlichkeit, dass jedes Risiko eintreten könnte, als auch die entsprechenden potenziellen Auswirkungen dieses Eintretens. Das Ziel ist es, die Reaktionen auf die identifizierten Risiken in einem logischen Format zu priorisieren.

10. Einen Aktionsplan entwickeln
Sobald die Risikobeurteilung abgeschlossen ist, stellen Sie Ihre Ergebnisse und Empfehlungen in einem umfassenden Bericht zusammen, der dem Vorstand zur Überprüfung und Genehmigung vorgelegt wird. Der Prozess sollte jedoch nicht dort aufhören. Anschließend sollte ein Aktionsplan entwickelt werden, der die Empfehlungen aus der Risikobeurteilung priorisiert, um sicherzustellen, dass die notwendigen Verbesserungen umgesetzt werden.

„Obwohl es keine allgemein gültigen Regeln für die Risikobewertung gibt, sollte die Übung im Allgemeinen aus einer ganzheitlichen Überprüfung der Organisation von oben nach unten bestehen und ihre Berührungspunkte mit der Außenwelt bewerten."
OFAC-Leitfaden

MESSEN

ÜBERWACHEN, BEWERTEN UND VERBESSERN DER PROGRAMMEFFEKTIVITÄT

Ihr Ethik- und Compliance-Programm ist ein Ökosystem aus sich verändernden Komponenten. Neue Gesetze und Vorschriften, neue Geschäftszweige, neue Regionen sowie Fusionen und Übernahmen werden Teil eines wachsenden Unternehmens sein, das Ihr Compliance-Ökosystem unterstützen muss. Dies erfordert von den Verantwortlichen eine regelmäßige Überwachung und Bewertung der Risiken und Prioritäten, um notwendige Anpassungen vorzunehmen, die weiterhin ein effektives Programm ermöglichen.

Monitoring, Audits und Messungen

Monitoring, Audits und Messungen sind der Schlüssel zum Verständnis, ob Ihr Ethik- und Compliance-Programm angemessen konzipiert und implementiert ist und effektiv funktioniert. Die durch diese Analysen identifizierten Lücken sollten dann angegangen werden, um eine kontinuierliche Verbesserung zu gewährleisten.

Monitoring ist eine fortlaufende Echtzeit-Überwachung oder Aufsicht über Ihr Programm. Es ist wesentlich für die rechtzeitige Identifizierung von Mängeln der internen Kontrolle. Es beinhaltet die Prüfung der täglichen Geschäftsaktivitäten mit dem größten Fokus auf die Bereiche des Unternehmens, die den größten Risiken ausgesetzt sind.

Audits sind eine periodische, nicht fortlaufende, rückwirkende Übung. Obwohl die interne Revision sehr gut für die Durchführung von Compliance-Audits geeignet ist, benötigt der Vorstand von Zeit zu Zeit wahrscheinlich eine unabhängige Bestätigung. Externe Auditfirmen oder akkreditierte Berater können eine unabhängige Validierung Ihres Ethik- und Compliance-Programms vornehmen.

Messen und Bewerten ist eine umfassende Bewertung, wie Ihr Programm:

- Im Vergleich mit Unternehmen ähnlicher Größe, Branche und Ausprägung abschneidet
- Weltweit anerkannte oder in der Branche akzeptierte Standards erfüllt
- Hilft, Lücken in der Risikominderung zu schließen
- Verbesserungen in einer priorisierten Weise durch einen mehrjährigen Arbeitsplan definiert, um den gewünschten Programmreifegrad Ihres Unternehmens zu erreichen

Neben der Bewertung externer Faktoren muss ein robustes Programm auch eine wichtige interne Variable berücksichtigen - das menschliche Verhalten. Selbst wenn strenge Richtlinien und Compliance-Verfahren vorhanden sind, stellt das Verhalten der Mitarbeiter das größte Risiko für Ihr Ethik- und Compliance-Programm dar. Eine robuste Qualitätsbewertung hilft Ihnen, die Auswirkungen Ihres aktuellen Ethik- und Compliance-Programms auf die Mitarbeiter sowie die gesamte Unternehmenskultur zu verstehen.

Welche Metriken verwendet man, um die Effektivität des Compliance-Programms zu messen?

	Reifegrad des Programms			
	Reaktiv	Einfach	Reifend	Fortgeschritten
Mitarbeiterbefragungen und andere Unternehmenskulturbewertungen	10 %	35 %	58 %	81 %
Analyse der Ergebnisse der internen Revision	6 %	32 %	59 %	84 %
Verstöße gegen den Verhaltenskodex / interne Richtlinien	10 %	35 %	57 %	85 %
Durchführung von Kündigungsgesprächen und Messung der Mitarbeiterfluktuation	13 %	37 %	55 %	63 %
Verfolgung von Whistleblowing-Meldungen, Vergeltungsmaßnahmen und Quoten der erhärteten Verdachtsfälle	2 %	31 %	45 %	83 %
Quiz für Mitarbeiter zu Schulungen oder Richtlinien	9 %	29 %	47 %	60 %
Attestierungsraten für Schulungen und Richtlinienprogramme	10 %	22 %	39 %	72 %
Vergleiche mit Messungen oder Benchmarks von Dritten	1 %	12 %	26 %	66 %
Fallabschlusszeiten	4 %	13 %	21 %	57 %
Unabhängige Bewertungen durch externe Anwälte und / oder Berater	3 %	10 %	26 %	47 %
Beobachtung von Bewertungen auf 'Glassdoor' / Artikeln in sozialen Medien / Nachrichten	3 %	10 %	20 %	28 %
Reduzierung von behördlichen Geldstrafen oder Bußgeldern	3 %	7 %	15 %	40 %
Wir bewerten die Effektivität nicht formell	65 %	16 %	3 %	0 %

Quelle: NAVEX Global, The Definitive Corporate Compliance Benchmark Report, 2019, Seite 19 ›››

Eine Geschichte derWirksamkeit

Die Ergebnisse Ihrer Überwachungs-, Prüfungs- und Bewertungsaktivitäten sollten eine Geschichte erzählen, die die Effektivität Ihres Programms aufzeigt und wie es mit der Mission, den Werten und den strategischen Betriebsplänen Ihrer Organisation zusammenhängt.

Verwenden Sie die Daten, die Sie sammeln, um Ihre Geschichte in Beweisen zu verankern, während Sie die abstrakteren Beobachtungen und Einstellungen als kulturelle Manifestationen dieser Daten hinzufügen.

Ihre Effektivitätsgeschichte sollte einen konkreten Fahrplan enthalten, der veranschaulicht, wie Sie die Ergebnisse in Zukunft nutzen werden. Eines der wichtigsten Ergebnisse sollte die Entwicklung eines Ethik- und Compliance-Arbeitsplans sein, der Programmverbesserungen beinhaltet - und Programmlücken oder Ineffizienzen behebt. Zusammen mit den nächsten Schritten sollte Ihre Effektivitätsgeschichte auch geplante Termine für regelmäßige Überprüfungen und Kurskorrekturen der Programmanpassungen enthalten, die durch Ihre Überwachung, Prüfung und Bewertung ermittelt wurden.

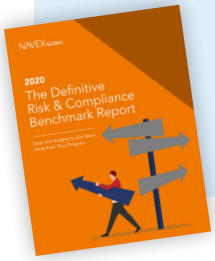
Beispiel: Vorlage zur Bewertung des Ethik- und Compliance-Programms

STANDARDS, RICHTLINIEN UND PROZEDUREN:	BENÖTIGT AUFMERKSAMKEIT	TEILWEISE ERFÜLLUNG DER BEST PRACTICE	BEST PRACTICE	AKTIONSPLAN	ZUSTÄNDIGER FÜR DEN AKTIONSPLAN	STATUS
UMFASSENDER VERHALTENSKODEX			X	*Keine Maßnahmen erforderlich, der Verhaltenskodex entspricht den Best Practices der Branche.*	*CECO*	*Vollständig*
RICHTLINIEN UND VERFAHREN IN BEREICHEN MIT HOHEM RISIKO		X		*Entwicklung, Adaption und Einführung der Richtlinie für Geschenke und Bewirtung. Die entsprechenden Mitarbeiter schulen.*	*CECO, mittlere Führungskräfte*	*In Bearbeitung*
RICHTLINIEN-MANAGEMENT-PROZESS: REGELMÄSSIGE UPDATES	X			*Entwerfen und implementieren eines Verfahrens zur regelmäßigen Überprüfung und Aktualisierung der Richtlinien und Verfahren auf der Grundlage der Risikobewertung.*	*CECO, Experten für Geschäftsprozesse*	*Offen*

Benchmarking Ihres Programms

Benchmarking ist ein wichtiger Teil des Bewertungsprozesses. Benchmarks können verwendet werden, um Ihr Budget oder andere Ressourcenanforderungen zu begründen, um eine priorisierte Liste von Verbesserungsmöglichkeiten zu erstellen und um den Zeitplan für die Einbeziehung dieser Verbesserungen zu überprüfen.

Am wichtigsten ist, dass Benchmarking Ihnen helfen kann, zu verstehen, ob Ihr Programm im normalen Bereich für die Größe Ihres Unternehmens und Ihrer Branche liegt - und wo das Programm als Ganzes (oder einzelne Elemente) auf dem Spektrum zwischen Substandard bis Best Practice landen könnte. Das Benchmarking dient nicht nur dazu, Ihr Programm mit anderen zu vergleichen, sondern ist auch ein wichtiger Schritt, um Ihr Programm so zu gestalten, dass es der Prüfung durch externe, staatliche oder regulatorische Stellen besser standhält.



Aktuelle Risiko- und Compliance-Benchmarking-Informationen finden Sie auf der NAVEX Global Website >>>

FAZIT

Ein effektives Ethik- und Compliance-Programm ist nie fertig. Stattdessen sollte sie sich kontinuierlich weiterentwickeln, um die unvermeidlichen regulatorischen, organisatorischen und externen Entwicklungen zu berücksichtigen, die ihren aktuellen Status und ihre zukünftige Ausrichtung beeinflussen.

Aufgrund des unerbittlichen Tempos solcher Veränderungen ist es wahrscheinlich, dass die Technologie für Ihren langfristigen Erfolg immer wichtiger wird. Die Vereinheitlichung Ihres Ethik- und Compliance-Programms innerhalb einer automatisierten, integrierten Lösung gibt Ihnen die Möglichkeit, mit neuen Entwicklungen Schritt zu halten, die Effektivität zu verbessern und Ihre Ethik- und Compliance-Risiken zu verwalten und zu mindern.

Über die Autorin

Vera Tscherepanowa
Ethics Advocate, Beraterin, Autorin
Studio Etica, Mailand (Italien) ›››

Vera Tscherepanowa ist eine ehemalige regionale Compliance-Beauftragte und Autorin des Buches „Compliance-Programm einer Organisation“. Vera hat vor Ort in Osteuropa, der GUS und Russland gearbeitet. Mit ihrer Erfahrung im Umgang mit den kulturübergreifenden Herausforderungen von Ethik und Compliance berät Vera derzeit internationale Konzerne, Non-Profit-Organisationen, Groß- und Einzelhandelsbetriebe sowie kleine bis große Unternehmen bei der Entwicklung von Ethik- und Compliance-Programmen. Vera spricht Russisch, Englisch, Französisch und Italienisch.

Weitere Ressourcen

Benchmarking und Markttrends

2020 The Definitive Risk & Compliance Benchmark Report ›››
2020 Third Party Risk Management Top Market Trends & Analysis ›››
2020 Risk & Compliance Hotline Benchmark Report ›››
Regionaler Benchmark-Bericht zur Whistleblowing-Hotline 2020 ›››

Behördliche und internationale Leitfäden zu Ethik- und Compliance-Programmen

US Department of Justice Evaluation of Corporate Compliance Programme ›››
2018 Federal Sentencing Guidelines Manual ›››
AFA Leitfaden zu SAPIN II Compliance (auf Französisch) ›››
UK Bribery Act Leitfaden von Transparency International (Englisch) ›››
FCPA Corporate Enforcement Policy ›››
ISO 19600:2014 Compliance Management Systems ›››
ISO 37001:2016 Anti-Bribery Management Systems ›››
ICC Ethics and Compliance Training Handbook ›››
UNODC Compliance Resources ›››
A Framework for OFAC Compliance Commitments ›››

Leitfäden zur Arbeit mit Vorständen

Key Elements for Effective Compliance Programme Board Reporting ›››
Four Key Board Responsibilities for Monitoring Risk and Compliance ›››

Leidfäden Risikobewertung

Risk Assessment Framework ›››
Sample Risk Prioritization Framework ›››
ISO 31000:2018 Risikomanagement – Richtlinien (Englisch) ›››

Umfassende Leitfäden für Compliance-Programme

Leitfaden für die Beurteilung von Compliance-Programmen ›››
Umfassender Leitfaden für das Management von durch Drittparteien verursachten Risiken ›››
Umfassender Leitfaden für Whistleblowing-Systeme ›››
Umfassender Leitfaden für Ihren Verhaltenskodex ›››
Leitfaden für die Richtlinien- und Verfahrensverwaltung ›››
Umfassender Leitfaden für das Ethik-& Compliance-Schulungsprogramm ›››

EMEA + APAC

Vantage London – 4th Floor
Great West Road, Brentford TW8 9AG, UK

www.navexglobal.com
+44 (0)20 8939 1650

Nord, Mittel- und Südamerika

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035, USA

www.navexglobal.com
+1 (866) 297 0224

BITTE RECYCLEN.

NAVEX GLOBAL®