auf die Belegschaft. Hinzu kommen die Berücksichtigung des aktuellen Arbeitsmarktes und auch ein Generationenwandel im Zugang zu Werten wie Integrität und Rechtstreue. Potenziellen Bewerber:innen ist es zunehmend wichtiger, in einem integren Unternehmen zu arbeiten, das sich an die Regeln hält sowie soziale und ökologische Verantwortung trägt.

1.2.9. Conclusio

Müssen wir Compliance also nun wirklich haben? Ja! Mag auch keine direkte gesetzliche Verpflichtung für Unternehmen außerhalb der Finanzwirtschaft bestehen, so spricht doch eine Reihe von Gründen dafür.

Es sollte alleine schon im eigenen Interesse der Geschäftsleitung liegen, ein CMS einzurichten, um eine **persönliche Haftung zu vermeiden**. Gesetzliche Regelungen sehen **Sorgfalts- und Überwachungspflichten** vor, denen nur durch ein wirksames CMS entsprochen werden kann. Compliance ist darüber hinaus ein wichtiger **Teil eines unternehmensweiten Risikomanagements**. Durch die strukturierte Erhebung und Bewältigung von Compliance-Risiken werden Verstöße gegen Gesetze und damit verbundene Sanktionen, die auch zur Existenzgefährdung führen können, vermieden.

Darüber hinaus werden durch Compliance laufend etwaige neue Regularien bzw gesetzliche Vorgaben, denen das Unternehmen unterliegt, identifiziert. Nicht zuletzt wird der Maßstab einer „Good Governance" in der Wirtschaft, aber auch in unserer Gesellschaft immer höher und für untätige Unternehmen nicht mehr erreichbar.

1.3. Was kostet Compliance?

„If you think compliance is expensive, try non-compliance."[20] Im Grunde ist damit alles gesagt. Dennoch stellt sich diese Frage verständlicherweise für die Geschäftsleitung bei der Entscheidung, ein CMS zu implementieren und damit auch eine Compliance-Organisation zu installieren.

Das **Gehalt** einer/s (Chief) Compliance Officer ist ein Kostenfaktor.[21] Die weitere Compliance-Organisation und damit verbundene Kosten hängen selbstverständlich von der Unternehmensgröße und -struktur ab. Weiters sind der **interne Aufwand** zu berücksichtigen, zum Beispiel die Teilnahme von Mitarbeiter:innen an einer Risikoanalyse oder an Schulungen. Hinzu können **Kosten für Tools** (zB Whistleblowing-System oder Geschenke- und Einladungsregister) kommen, die zugekauft werden, sowie gegebenenfalls **externe Beratungskosten**.

20 Dieses in der Compliance-Community wohl bekannteste Zitat stammt vom ehemaligen US Deputy Attorney General Paul McNulty.

21 Im Durchschnitt verdient ein Chief Compliance Officer jährlich je nach Erfahrung ungefähr zwischen EUR 70.000 und EUR 120.000.

2.6. Strategien der Risikobewältigung

Wenn einzelne Risiken identifiziert und bewertet worden sind, stellt sich im nächsten Schritt die Frage, wie diese gesteuert oder bewältigt werden sollen. Die Auswahl der geeigneten Risikobewältigungsstrategie hängt von der Art und dem Ausmaß des identifizierten Risikos sowie von den spezifischen Umständen des Unternehmens ab.

2.6.1. Risikovermeidung

Die Strategie der Risikovermeidung zielt darauf ab, potenzielle Risiken vollständig zu eliminieren, indem bestimmte risikobehaftete Tätigkeiten oder Geschäfte vermieden werden. Das ist besonders relevant, wenn das Risiko inakzeptabel hoch ist und keine effektiven Kontrollmaßnahmen vorhanden sind, um das Risiko zu mindern.

Beispiel

Ein Unternehmen entscheidet sich, fortan keine Geschäfte in einem bestimmten Land zu tätigen, weil die regulatorischen Anforderungen schwer zu erfüllen sind und das Risiko von Verstößen gegen Außenwirtschaftsgesetze hoch ist. Durch den Rückzug aus diesem Markt vermeidet das Unternehmen mögliche rechtliche und reputative Schäden.

2.6.2. Risikoverminderung

Bei der Risikoverminderung sind zwei Ansätze relevant. Abgeleitete Maßnahmen zielen entweder auf die Verminderung der Wahrscheinlichkeit des Eintretens eines Risikos oder auf die Reduzierung von dessen potenziellen Schäden ab. Diese Strategie beinhaltet die Implementierung von internen Kontrollen, die Erstellung und Kommunikation von klaren Verhaltensregeln oder die Definition von standardisierten Prozessen, um Compliance-Verstöße zu verhindern bzw ihre Auswirkungen zu begrenzen.

Beispiel

Ein Unternehmen führt regelmäßige Schulungen für seine Beschäftigten durch, um sie für das Thema Kartell- und Wettbewerbsrecht zu sensibilisieren und über die geltenden gesetzlichen Anforderungen aufzuklären. Durch diese Präventivmaßnahmen wird die Wahrscheinlichkeit von kartellrechtlichen Absprachen und den damit verbundenen Strafen erheblich reduziert. Zusätzlich kann die Durchführung von flächendeckenden und regelmäßigen Schulungen als Teil eines gesamthaften CMS im Fall eines dennoch eintretenden Anlassfalls bußgeldmindernd wirken.

2.6.3. Risikoübertragung

Bei der Risikoübertragung wird das Risiko auf eine dritte Partei transferiert. Dies kann typischerweise durch Abschluss von Versicherungen oder die Auslagerung von Tätigkeiten erfolgen.

Kund:innen eines Unternehmens, die Nutzer:innen der Unternehmenswebseite sowie die eigenen Mitarbeiter:innen.
- **Löschkonzept:** Erstellung eines Löschkonzepts, das für jede Datenkategorie die Aufbewahrungsdauer definiert. Nach Ablauf der Frist müssen die Daten entweder automatisiert gelöscht oder durch manuelle Schritte vernichtet werden.

2.7.8. Geheimhaltung und Know-how

Grundlagen

Ein des Öfteren unterschätztes Risikofeld betrifft einer der wichtigsten Güter eines Unternehmens: das Know-how und damit Geschäftsgeheimnisse. Mit der Richtlinie (EU) 2016/943[36] wurde im Hinblick auf den Schutz von Geschäftsgeheimnissen ein neuer Maßstab gesetzt. Kurz gesagt ist ein Geschäftsgeheimnis eine Information, die geheim, von wirtschaftlichem Wert und Gegenstand von entsprechenden Geheimhaltungsmaßnahmen ist. Es werden **konkrete Maßnahmen** verlangt, damit die für den geschäftlichen Erfolg wichtigen Geschäftsgeheimnisse nicht verloren gehen. Im gerichtlichen Anlassfall sind der wirtschaftliche Wert und die konkret getroffenen Geheimhaltungsmaßnahmen nachzuweisen, widrigenfalls der Schutz wegfällt.

Neben der Notwendigkeit von konkreten Maßnahmen und deren Umsetzung ist das Augenmerk aber auch auf das oft fahrlässige Verhalten von Menschen in Unternehmen zu richten. Es kann in diesem Zusammenhang nicht oft genug darauf hingewiesen werden, dass **öffentliche Orte** keine geeigneten Plätze darstellen, um vertrauliche Informationen zu besprechen oder auszutauschen. Es geht also nicht nur um konkret definierte Geschäftsgeheimnisse, sondern ganz allgemein um Vertraulichkeit und den Schutz sensibler Informationen und interner Prozessabläufe.

Typische Risikoszenarien

Zusammenarbeit mit externen Dienstleister:innen

Im Rahmen einer Zusammenarbeit werden zwischen Unternehmen oft auch geheime bzw vertrauliche Informationen ausgetauscht. Dies geschieht immer wieder auch im Vorfeld, bevor eine vertragliche Vereinbarung geschlossen wird. Erst im Zuge der Vertragserstellung kommt dann eine Geheimhaltungsvereinbarung ins Spiel.

Zug, Kaffeehaus oder Stadtpark

Das geöffnete Notebook im Zug mit vertraulichem Inhalt auf dem Monitor und für dahinter Sitzende gut lesbar, das offenherzige Gespräch mit Kolleg:innen im

36 In Österreich wurde die Richtlinie mit der UWG-Novelle 2018 umgesetzt. In Deutschland trat 2019 das Gesetz zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung in Kraft.

Fazit

Die enge Zusammenarbeit zwischen Compliance und den verschiedenen Schnittstellen innerhalb eines Unternehmens ist entscheidend für ein erfolgreiches CMS. Jede Abteilung bringt ihre spezifischen Funktionen und ihre Expertise ein, um die Einhaltung gesetzlicher sowie interner Anforderungen sicherzustellen. Es ist von großer Bedeutung, die konkreten Aufgaben der einzelnen Abteilungen klar zu definieren und für eine angemessene Abgrenzung zu sorgen, um Doppelgleisigkeiten und „blinde Flecken" zu vermeiden. Gerade im Hinblick auf die oft bestehenden Überschneidungen zwischen den Schnittstellen ist eine enge Zusammenarbeit unerlässlich. Zur Optimierung des Informationsaustauschs kann es sinnvoll sein, diese Schnittstellen in einem gemeinsamen Committee zusammenzufassen (siehe sogleich 3.4.), um einen effizienten und strukturierten Austausch von Informationen zu gewährleisten.

3.4. Compliance Committee

Das Compliance Committee ist ein permanentes bereichsübergreifendes Gremium. Dadurch werden wichtige Compliance-Aspekte nicht nur von einzelnen Personen beurteilt, sondern unter Einbeziehung weiterer unternehmensinterner Querschnitts- und Expertenfunktionen.

Die konkrete Ausgestaltung und die Aufgaben des Committee können je nach Unternehmensbedürfnissen und spezifischen Anforderungen variieren. Dabei sollten die folgenden Zielsetzungen in Betracht gezogen werden:

- **Erarbeitung von Vorschlägen und Weiterentwicklungsmaßnahmen des CMS:** Das Committee entwickelt konkrete Vorschläge zur Verbesserung und Weiterentwicklung des bestehenden CMS, um dessen Wirksamkeit kontinuierlich zu steigern.
- **Einbindung und Abstimmung bei der Ausgestaltung des CMS:** Das Committee bietet eine Plattform für den Austausch und die Abstimmung zu Fragen der CMS-Gestaltung, die durch die Compliance-Organisation vorangetrieben wird. Dies umfasst auch das Einholen von Feedback zu erstellten Unterlagen und Dokumentationen oder neuen Prozessen, die implementiert werden sollen.
- **Ableitung und Beratung von Maßnahmen aus den Ergebnissen von Compliance-Audits:** Nach Durchführung von Compliance-Audits analysiert das Committee die Ergebnisse und leitet daraus zur Verbesserung des CMS geeignete Maßnahmen ab.
- **Diskussions- und Entscheidungsgremium bei Compliance-Vorfällen:** Das Committee dient als Forum zur Diskussion und Entscheidungsfindung bei Compliance-Vorfällen und leitet notwendige Anpassungen des CMS basierend auf den Erkenntnissen von Compliance-Vorfällen ab.

volle Einblicke in mögliche Compliance-Risiken geben. Mitarbeiter:innen sollten die Gelegenheit erhalten, etwaige Verstöße oder Bedenken anzusprechen, die während ihrer Anstellung aufgetreten sind. Dieses Feedback kann genutzt werden, um das CMS kontinuierlich zu verbessern. Zugleich stärkt es auch die Beziehung und sorgt dafür, dass auch Menschen, die das Unternehmen verlassen, ernst genommen und wertgeschätzt werden.

4. Programm | CMS – der Name ist Programm

Ein zentrales Element eines wirksamen CMS ist das Compliance-Programm. Dieses umfasst sämtliche Dokumente und Maßnahmen, die die Organisation implementiert, um sicherzustellen, dass gesetzliche und interne Vorschriften eingehalten werden. Die Grundlage eines erfolgreichen Compliance-Programms bildet die Ableitung dieser Maßnahmen aus den Ergebnissen einer strukturierten Risikoanalyse (siehe 2.4.). Diese Analyse hilft, jene Risikobereiche zu identifizieren, auf die das Compliance-Programm ausgerichtet werden muss.

Im Mittelpunkt des Compliance-Programms stehen zentrale Dokumente wie der Verhaltenskodex, das CMS-Handbuch und Compliance-Richtlinien zu einzelnen Themenbereichen. Der Verhaltenskodex dient als grundlegende Orientierung für alle Mitarbeiter:innen und definiert die ethischen und rechtlichen Standards, die das Unternehmen verfolgt. Das CMS-Handbuch wiederum ist die Beschreibung des implementierten CMS und enthält eine detaillierte Erläuterung sämtlicher Prozesse und Maßnahmen. Schließlich legen spezifische Richtlinien klare Verhaltensweisen und Prozesse fest, um den Umgang mit verschiedenen Compliance-Risiken zu steuern.

Im Weiteren wird näher auf diese Schlüsseldokumente und deren konkrete Ausgestaltung eingegangen. Zum Programm selbst zählen aber nicht nur Compliance-Dokumente, sondern auch alle getroffenen Maßnahmen, die sicherstellen, dass die festgelegten Standards und Richtlinien in der Praxis gelebt werden. Das umfasst compliance-relevante Kontrollen und Prozesse, wie spezifische Genehmigungsverfahren oder Unterschriftenregelungen, aber auch Maßnahmen zur Vermittlung der Regeln und Grundsätze. Dabei ergeben sich wesentliche Überschneidungen zur Kommunikation und Schulung von Compliance (siehe dazu die Ausführungen unter 5.).

4.1. Der Verhaltenskodex

Der Verhaltenskodex (Code of Conduct) ist das Fundament eines jeden Compliance-Programms und spielt eine zentrale Rolle bei der Implementierung und Entwicklung eines CMS. Er stellt eine schriftliche Erklärung der wesentlichen Verhaltensgrundsätze dar, deren Einhaltung von allen erwartet wird. Zudem

Wichtig ist, dass die Entwicklung einer solchen Marke oder eines Logos nicht teuer sein muss. Oft können mit einfachen Mitteln große Wirkungen erzielt werden. Eine kreative Idee, die gut zum Unternehmen passt und konsequent umgesetzt wird, kann viel bewirken. Doch es braucht nicht nur Kreativität – ebenso entscheidend ist das Durchhaltevermögen. Es erfordert kontinuierliche Kommunikation, um Mitarbeiter:innen für Compliance zu gewinnen und die Marke zu verankern.

5.2. Schulungen und Trainings

Schulungen und Trainings sind entscheidende Werkzeuge, um die festgelegten Grundsätze und Regeln effektiv zu vermitteln. Sie sorgen dafür, dass Mitarbeiter:innen nicht nur die theoretischen Vorgaben kennen, sondern diese auch verstehen und in ihrem Arbeitsalltag anwenden können. Damit Schulungen ihre volle Wirkung entfalten, müssen sie auf die spezifischen Bedürfnisse der jeweiligen Zielgruppen zugeschnitten und regelmäßig durchgeführt werden. Ein gut durchdachtes Schulungskonzept ist daher unerlässlich, um sicherzustellen, dass alle relevanten Personen die erforderlichen Kenntnisse erwerben und das Wissen nachhaltig vermittelt wird.

5.2.1. Zielgruppen und Inhalte – Das Schulungskonzept

Ein definiertes **Schulungskonzept** spielt eine entscheidende Rolle bei der Implementierung und Aufrechterhaltung von Compliance-Richtlinien und -Prozessen. Ziel des Schulungskonzepts ist die Sicherstellung, dass alle Personen die für sie notwendigen Kenntnisse und Fähigkeiten besitzen, um compliance-konform im Arbeitsalltag zu handeln. Wesentlich für die Definition eines Schulungskonzepts sind dabei die relevanten Zielgruppen sowie die entsprechenden Inhalte (siehe Teil 2: 17. Schulungskonzept).

Zielgruppen sind definierte Personenkreise innerhalb (oder außerhalb) eines Unternehmens, die aufgrund ihrer Rolle, Funktion oder Verantwortung entsprechende Schulungsbedürfnisse haben. Die Definition der Zielgruppen ist wichtig, weil verschiedene Personenkreise unterschiedliche Anforderungen an Compliance-Wissen und -Training haben. Ein einheitlicher Schulungsansatz könnte entweder übermäßig komplex oder nicht detailliert genug sein, um den spezifischen Bedürfnissen jeder Gruppe gerecht zu werden. Bei der Definition der relevanten Zielgruppen sollten einige Überlegungen angestellt werden:

- **Funktion und Verantwortung:** Unterscheidung der Zielgruppen nach ihrer Funktion innerhalb des Unternehmens. Führungskräfte benötigen beispielsweise Schulungen, die sich auf strategische Entscheidungen, das Vorleben von Grundsätzen und ihre Verantwortung zB im Bereich der Antidiskriminierung konzentrieren. Mitarbeiter:innen in operativen Rollen hingegen benötigen

6. Überwachung und Verbesserung | Compliance ist ein Marathon

Compliance ist kein einmaliges Projekt, sondern ein fortlaufender Prozess, der kontinuierliche Aufmerksamkeit und Anpassung erfordert. In einem dynamischen, geschäftlichen und regulatorischen Umfeld ist es unerlässlich, dass das CMS nicht nur implementiert, sondern auch regelmäßig überwacht und verbessert wird. Gerade hier zeigen sich in der Praxis oft Schwierigkeiten und Herausforderungen für die Compliance-Verantwortlichen. Ein proaktiver Ansatz zur Verbesserung sorgt jedoch dafür, dass das CMS nicht nur reaktiv auf Veränderungen reagiert, sondern auch strategisch weiterentwickelt wird, um den sich wandelnden Anforderungen gerecht zu werden.

„Vertrauen ist gut, **Kontrolle** ist besser", sagt ein bekanntes Sprichwort. Für eine erfolgreiche Compliance-Kultur ist jedoch beides wichtig und sollten Vertrauen und Kontrolle nicht als Gegensätze verstanden werden. Durch ein gesamtheitliches CMS kann Compliance eine wichtige **Verteidigungslinie** und damit Schutzschild für das Unternehmen sein. Teil der Überwachung und Verbesserung ist die strukturierte **Berichterstattung**. Außerdem sollen **Kennzahlen** definiert und überwacht werden, mit denen die Wirksamkeit des CMS gemessen und bewertet wird. Auch die Klärung der Frage, wie auf konkrete Compliance-**Vorfälle** reagiert wird, ist unerlässlich, um sicherzustellen, dass etwaige Verstöße schnell identifiziert, angemessen adressiert und aus ihnen Lernprozesse für künftige Prävention abgeleitet werden. Die Durchführung von **Audits** spielt ebenfalls eine entscheidende Rolle in diesem Prozess, da sie eine unabhängige Bewertung der Effektivität des CMS bieten und Schwachstellen aufdecken können. Darüber hinaus kann eine formale **Zertifizierung** durch externe Prüfstellen bestätigen, dass das CMS den geltenden Standards entspricht.

6.1. Compliance – Kontrolle oder Vertrauen?

Compliance ist in hohem Maße Beziehungsarbeit, die auf Vertrauen und Eigenverantwortung der Mitarbeitenden basiert. Ein solcher Vertrauensaufbau ist essenziell, um ein Arbeitsumfeld zu schaffen, in dem sich alle Beteiligten ihrer ethischen Verantwortung bewusst sind und diese ernst nehmen. Die Implementierung von Kontrollmaßnahmen kann deshalb als Einschränkung oder als Ausdruck von Misstrauen empfunden werden. Diese Wahrnehmung kann die Motivation und das Engagement beeinträchtigen, wodurch eine gute Compliance-Kultur gefährdet wird.

Gleichzeitig sind Kontrollmaßnahmen jedoch unerlässlich, um Risiken und potenzielle Verstöße zu minimieren. Das sogenannte **Fraud Triangle** , das in den 1950er von dem Kriminologen *Donald R. Cressey* entwickelt wurde,[55] verdeut-

55 *Cressey, D. R.*, The criminal violation of financial trust. American Sociological Review 15 (1950) 738–743.

5. Fragebogen Antidiskriminierung (Auszug)

Die Einleitung zum Fragebogen sollte in einer möglichst für alle Teilnehmenden verständlichen Sprache verfasst sein und motivieren, daran teilzunehmen. Weiters sollte die Sicherheit vermittelt werden, dass die Umfrage anonym erfolgt und keine Rückschlüsse auf die teilnehmenden Personen möglich sind.

Nachfolgender Fragenbogen versteht sich grundsätzlich als vollständig, kann aber selbstverständlich um weitere Themenbereiche und Fragen ergänzt werden. Die Erfahrung zeigt, dass ein „freies Textfeld" am Ende wichtig ist und von einigen Teilnehmenden auch genutzt wird. Gerade aus diesen Ergänzungen lassen sich oft wertvolle Erkenntnisse gewinnen. Siehe Teil 1: 2.7.1.

Sehr geehrte Mitarbeiter:innen,

liebe Kolleg:innen,

im Rahmen unserer ständigen Bemühungen um ein faires und respektvolles Arbeitsumfeld möchten wir eine **anonyme** Umfrage zum Thema Diskriminierung durchführen. Unser Ziel ist es, den aktuellen Status zu erheben und wertvolle Einblicke zu gewinnen. Diese sollen uns helfen, mögliche Handlungsfelder zu erkennen und gezielte Maßnahmen zur Verbesserung zu ergreifen.

Ihre Antworten helfen uns daher sehr, einen Beitrag zu einem guten Miteinander zu leisten. Berücksichtigen Sie bitte nicht nur Ihr unmittelbares Arbeitsumfeld, sondern das gesamte Unternehmen. Bitte bedenken Sie bei der Beantwortung der Fragen, dass die Umfrage selbstverständlich anonym ist und wir die Ergebnisse ausschließlich aggregiert auswerten. Ein Rückschluss auf Sie als Person ist nicht möglich. Vielen Dank für Ihre Teilnahme!

Ihr Compliance-Team

Frage 1: Haben Sie im Unternehmen Fälle von ***Diskriminierung*** mitbekommen oder waren Sie selbst schon einmal Opfer von Diskriminierung im Unternehmen?

- ☐ Ja *(weiter zu 2)*
- ☐ Nein *(weiter zu 5)*
- ☐ Keine Angabe *(weiter zu 5)*

15. Muster: CMS-Handbuch

Das CMS-Handbuch ist „die Betriebsanleitung des Compliance-Management-Systems" – als dessen unverzichtbarer Bestandteil gibt es einen detaillierten Überblick über die Elemente des CMS eines Unternehmens. Nachfolgendes Muster ist ausführlich, deckt die relevanten Standards ISO 37301 sowie IDW PS 980 ab und soll jedenfalls als dynamisches Dokument verstanden werden, das sich nach den ersten notwendigen unternehmensangepassten Ergänzungen laufend weiterentwickelt. Siehe Teil 1: 4.2.

Musterunternehmen | Adresse | 1234 Musterstadt

CMS-Handbuch

Beschreibung des Compliance Management Systems (CMS) von UNTERNEHMEN

Datum: [Datum]

Version 1.0

Inhaltsverzeichnis:

16. Muster: Richtlinie Antikorruption

Dieses Muster für eine Compliance-Richtlinie zum Thema „Antikorruption" dient als Vorlage und sollte entsprechend den spezifischen Anforderungen und Prozessen des Unternehmens angepasst werden. Siehe Teil 1: 4.3.

Musterunternehmen | Adresse | 1234 Musterstadt

Compliance-Richtlinie Antikorruption

Datum:	[Datum]
Zuständigkeit	[Abteilung/Name]
Freigegeben von	[Funktion/Name]
Version	1.0

Inhaltsverzeichnis:
