Hamburger Compliance-Zertifikat

++++

Handbuch

- Stand 2024 -

Inhalt

1. Teil: Das Zertifizierungsverfahren
I. Einleitung
II. Gesamtablauf des Zertifizierungsverfahrens
1. Präqualifizierungsphase
2. Auditierung
3. Erteilung des *Hamburger Compliance-Zertifikats*
4. Rezertifizierung
5. Entzug des *Hamburger Compliance-Zertifikats*

2. Teil: Auditierung
I. Elemente und Ablauf des Auditierungsverfahrens
II. Maßstab der Auditierung

3. Teil: Der Hamburger Compliance-Standard
I. Grundmodul: Allgemeines Compliance-Verständnis sowie Korruptions- und sonstige Kriminalitätsprävention
1. Compliance-Grundstruktur
2. Richtlinien
3. Allgemeine Organisatorische Maßnahmen
4. Korruptionsprävention
5. Unternehmenssicherheit
6. Zahlungsverkehr und Rechnungswesen
II. Modul 2: Vergabeverfahren
III. Modul 3: Kartellrecht
IV. Modul 4: Datenschutz und Datensicherheit
V. Modul 5: Gesundheitswirtschaft
VI. Modul 6: Lieferkette

4. Teil: Gebühren

1. Teil: Das Zertifizierungsverfahren

I. Einleitung

Das *Hamburger Compliance-Zertifikat* richtet sich vor allem an mittelständische Unternehmen und Familienunternehmen, die einen hohen Anspruch an unternehmerische und ethische Werte haben und sich insoweit von den Wettbewerbern positiv abheben möchten.

Das *Hamburger Compliance-Zertifikat* dient als Nachweis, dass ein Unternehmen über eine funktionierende und angemessene Compliance-Organisation verfügt. So können redliche Unternehmen nach dem Grundsatz „*Tue Gutes und rede darüber*" Gesetzestreue als Wettbewerbsvorteil nutzen. Im Bereich der öffentlichen Aufträge und im internationalen Geschäftsverkehr können Compliance-Zertifikate schon heute auch formal zu spürbaren Erleichterungen führen. Dieser gesetzgeberische Trend wird sich wahrscheinlich schnell fortsetzen.

Mit dem *Hamburger Compliance-Zertifikat* wird durch die Handelskammer Hamburg bescheinigt, dass das Unternehmen über eine Compliance-Organisation verfügt, die geeignet ist, die unternehmensspezifischen Risikofelder effektiv und angemessen zu kontrollieren. Dies umfasst

- die Konzeption und grundsätzliche Eignung der Compliance-Organisation,
- die Berücksichtigung der Anforderungen des Hinweisgeberschutzgesetz (HinSchG)
- die Angemessenheit im Hinblick auf Risikofelder, Geschäftsbereiche und interne Prozesse sowie
- die Effektivität in der Praxis, also die Geeignetheit, korrigierende Maßnahmen durchzuführen und präventive Maßnahmen umzusetzen.

Gegenstand der Zertifizierung sind die unternehmensinternen Prozesse. Gegenstand der Zertifizierung ist *nicht* die Frage der Gesetztestreue des Unternehmens und seiner Mitarbeiter in der Vergangenheit. Die Compliance-Organisation und das *Hamburger Compliance-Zertifikat* dienen auch dazu, das Risiko von Sanktionen gegen Unternehmen und Geschäftsleitung zu reduzieren. Denn durch die Zertifizierung wird dokumentiert, dass strukturell Vorsorge gegen Korruption und andere Gesetzesverstöße getroffen worden ist. Die Zertifizierung führt aber nicht dazu, dass die Geschäftsleitung von den Aufsichts- und Überwachungspflichten entbunden wird. Compliance-Verstöße können von der Handelskammer durch Abmahnung oder in schweren Fällen mit dem Entzug des Zertifikats geahndet werden.

Die Zertifizierung hat folgenden Nutzen für Unternehmen und handelnde Personen:

- Schutz und Stärkung des Unternehmensimages
- Stärkung der strategischen Beziehungen zu Geschäftspartnern
- Schaffung von Vertrauen bei Marktteilnehmern und Behörden
- Stärkung der Wettbewerbsfähigkeit
- Stärkung der Unternehmenskultur und des unternehmenseigenen Wertesystems
- Verbesserung der Rechtssicherheit
- Nachweis über die Einrichtung einer Hinweisgeberstelle nach dem HinSchG
- Maßnahme gegen Vergabesperre & Verzicht auf Registerabfrage nach § 6 Abs. 3 Nr. 5, § 7 GRfW
- Auskunftsfähigkeit und Transparenz gegenüber Behörden und Geschäftspartnern
- Reduzierung des Haftungsrisikos (§§ 30, 130 OWiG, § 43 GmbHG, § 91 Abs. 2, 93 AktG
  - Nachweis der Erfüllung von Organisations- und Aufsichtspflichten, Mai-Urteil BGH vom 9.5.2017
  - Straf- oder bußgeldmindernd in UK und USA, (P) strafrechtliche Haftung
  - Beweislast! LG München I Siemens/Neubürger Entlastung der Unternehmensleitung bei Auseinandersetzung mit Gesellschaft

II. Gesamtablauf des Zertifizierungsverfahrens

1. Präqualifizierungsphase

Sofern das Unternehmen nicht bereits über eine Compliance-Organisation verfügt, kann es im Vorfeld der Zertifizierung – der Präqualifizierungsphase – bei der Einrichtung der Compliance-Organisation von Experten beraten und unterstützt werden. Werden in der Präqualifizierungsphase Unstimmigkeiten festgestellt, können diese beseitigt werden. In Abstimmung mit dem Unternehmen wird ein Bericht über die ordnungsgemäße Einrichtung der Compliance-Organisation erstellt. Sofern das Unternehmen bereits über eine ausreichende Compliance-Organisation verfügt, ist die Präqualifizierungsphase nicht erforderlich.

2. Auditierung

Voraussetzung für die Erlangung des *Hamburger Compliance-Zertifikat*s ist die Durchführung eines Compliance-Audits, vgl. dazu näher Teil 2. Maßstab ist der *Hamburger Compliance Standard*, vgl. Teil 3. Die Prüfung erfolgt durch externe Auditoren, die bei der Handelskammer Hamburg akkreditiert sein müssen. Die Auditoren müssen der Handelskammer einschlägige Kenntnisse nachweisen und werden vom Unternehmen für das jeweilige Verfahren ausge-

wählt. Auf Antrag des Unternehmens wird das Auditierungsverfahren eingeleitet und vom Auditor durchgeführt. Der Auditor erstellt einen Auditbericht und übergibt diesen an das Unternehmen und an Pro Honore e.V.
Pro Honore e.V. prüft, ob die Voraussetzungen für die Erteilung des *Hamburger Compliance-Zertifikat*s vorliegen, und gibt eine entsprechende Empfehlung an die Handelskammer Hamburg. Werden Schwachpunkte entdeckt, so kann die Empfehlung unter dem Vorbehalt erfolgen, dass das Unternehmen diese in einem festgesetzten Zeitraum vollständig beseitigt.

3. Erteilung des *Hamburger Compliance-Zertifikats*
Liegen alle Voraussetzungen vor, wird dem Unternehmen durch die Handelskammer Hamburg das *Hamburger Compliance-Zertifikat* für drei Jahre erteilt. Dem Unternehmen werden eine Urkunde und eine Grafikdatei zur Verfügung gestellt, damit das Unternehmen mit der Zertifizierung werben kann. Die Zertifizierung erfolgt auf der Basis eines zivilrechtlichen Vertragsverhältnisses.

Fehlen wesentliche Voraussetzungen für die Verleihung des *Hamburger Compliance-Zertifikats*, so wird das Unternehmen unverzüglich informiert und ihm Gelegenheit zu einer Stellungnahme und zur Abhilfe gewährt. Kann auch daraufhin den Bedenken nicht abgeholfen werden, wird die Erteilung des *Hamburger Compliance-Zertifikats* endgültig versagt. In Streitfällen kann ein Clearing Board eingeschaltet werden, das die verfahrensrechtliche Stellung eines Schiedsgerichts hat und abschließend rechtskräftig entscheidet.

4. Rezertifizierung
Wenn sich das Unternehmen weiterhin redlich verhält und die erforderlichen Verfahren aufrecht erhält, kann das *Hamburger Compliance-Zertifikat* auf Antrag des Unternehmens durch eine Rezertifizierung verlängert werden.

Das dazu erforderliche Audit kann in einem abgekürzten Verfahren durchgeführt werden, wenn das Unternehmen nachweist, dass während der vergangenen drei Jahre keine nachteiligen Veränderungen in der Compliance-Organisation vorgenommen worden sind. Der Nachweis kann durch eine entsprechende Erklärung der Geschäftsleitung und durch Vorlage der regelmäßigen Compliance-Berichte für den Audit-Zeitraum erbracht werden. Die Entscheidung, ob das Audit im abgekürzten Verfahren durchgeführt werden kann, obliegt der Handelskammer Hamburg auf Empfehlung von Pro Honore e.V.

Bei einer positiven Rezertifizierung gelten die Zertifikatsrechte für weitere drei Jahre.

Verläuft das Rezertifizierungsverfahren negativ, wird das Unternehmen unverzüglich informiert und ihm Gelegenheit zu einer Stellungnahme und zur Abhilfe gewährt. Kann auch daraufhin

den Bedenken nicht abgeholfen werden, wird die Nutzung des *Hamburger Compliance-Zertifikats* untersagt. Das Unternehmen hat dann sofort die Zertifizierungsurkunde, sämtliche Kopien der Urkunde und Dateien herauszugeben und in elektronischen Medien zu löschen. Ferner hat das Unternehmen die Verwendung des *Hamburger Compliance-Zertifikats* sowohl intern als auch extern zu unterlassen, alle Werbemittel oder Schriftstücke, die das Zertifikat tragen, zu vernichten und es darf keine Schriftstücke oder Werbemittel mit dem Verweis auf das *Hamburger Compliance-Zertifikat* mehr in den Umlauf geben. In Streitfällen kann das Clearing Board eingeschaltet werden.

5. Entzug des *Hamburger Compliance-Zertifikats*

Bei Verdacht auf Compliance-Verstöße durch das zertifizierte Unternehmen erfolgt zunächst eine Anhörung durch Pro Honore e.V. Pro Honore e.V. bewertet den Sachverhalt und gibt eine Empfehlung an die Handelskammer Hamburg ab. Die grundsätzlichen Handlungsoptionen sind Einstellung des Verfahrens, ggfs. nach Behebung eines Problems im Unternehmen, eine Abmahnung bei minder schweren Verstößen und der Entzug des Zertifikats in schweren Fällen. Die Entscheidung trifft die Handelskammer Hamburg als Zertifikatsgeberin. Das Unternehmen kann dagegen das Clearing Board anrufen. Wird das Recht zur Führung des *Hamburger Compliance-Zertifikats* aberkannt, hat das Unternehmen sofort die Zertifizierungsurkunde, sämtliche Kopien der Urkunde und Dateien herauszugeben und in elektronischen Medien zu löschen. Ferner hat das Unternehmen die Verwendung des *Hamburger Compliance-Zertifikats* sowohl intern als auch extern zu unterlassen, alle Werbemittel oder Schriftstücke, die das Zertifikat tragen, zu vernichten und es darf keine Schriftstücke oder Werbemittel mit dem Verweis auf das *Hamburger Compliance-Zertifikat* mehr in den Umlauf geben.

Abbildung 1. Zeitlicher Ablauf

Abbildung 2. Ablauf Zertifizierungsverfahren

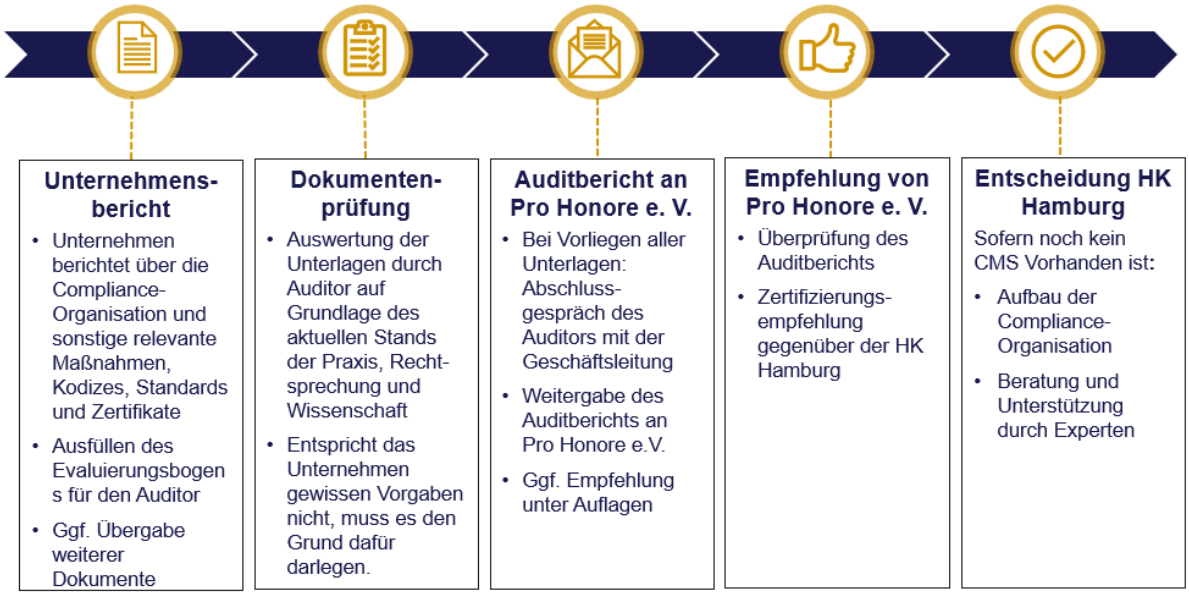
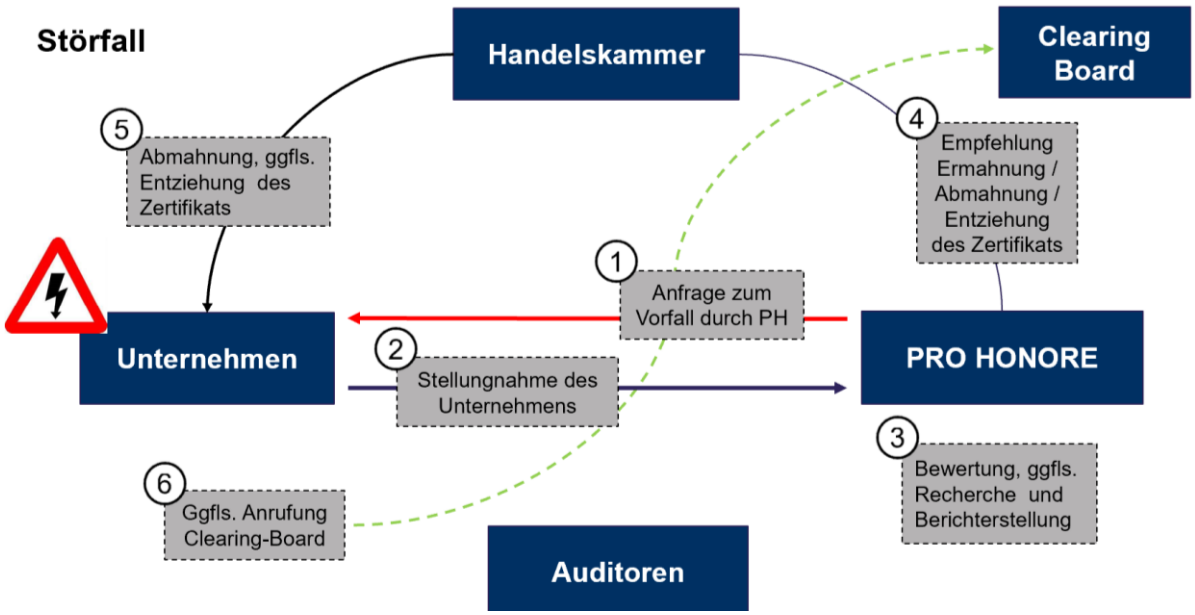


Abbildung 3. Vorgehen bei einem Störfall



2. Teil: Auditierung

Die Auditierung erfolgt auf der Grundlage des *Hamburger Compliance-Standards,* siehe hierzu näher Teil 3.

I. Elemente und Ablauf des Auditierungsverfahrens

Wesentliches Instrument für die Auditierung ist ein Evaluierungsbogen, der vom Unternehmen mit dem Auditor auszufüllen ist und durch entsprechende Unterlagen und Dokumente ergänzt wird. Solche sind insbesondere:

- Darstellung der Compliance-Organisation
- Fragebogen nach Hamburger Compliance Standard
- Darlegung der Einrichtung einer internen Meldestelle nach dem HinSchG
- Richtlinien und Arbeitsanweisungen und Prozessbeschreibungen
- Handbücher
- Rechtlich vorgeschriebene Dokumente
- Zertifikate oder Siegel dritter Institutionen.

Außerdem führt der Auditor Gespräche mit der Geschäftsleitung und mit Mitarbeitern.

Eingangs berichtet das Unternehmen selbständig über seine Compliance-Organisation und sonstige relevante Maßnahmen, Kodizes, Standards, Zertifikate o.ä. Nach der Ausfüllung des Evaluierungsbogens und der Übergabe der weiteren Dokumente wertet der Auditor diese Unterlagen und sonstige Informationen aus. Die Vorgaben des Evaluierungsbogens basieren auf dem aktuellen Stand in Praxis, Rechtsprechung und Wissenschaft. Sofern das Unternehmen bestimmten Vorgaben nicht entspricht, wird der Grund dafür dargelegt. Sachlich zweckmäßige Abweichungen stehen der Vergabe des Zertifikates nicht entgegen.

Sofern auf dieser Grundlage festgestellt wird, dass Fragen unbeantwortet geblieben sind, oder Dokumente fehlen, werden diese vom Auditor angefordert. Sollten danach noch Lücken vorhanden sein, wird das Unternehmen darauf hingewiesen und abgestimmt, ob und bis wann diese Lücken abschließend bearbeitet werden können.

Liegen alle Unterlagen vor und sind gegebenenfalls erforderliche Nachbesserungen erfolgt, führt der Auditor ein Abschlussgespräch mit der Geschäftsleitung. Daraufhin wird der abschließende Auditbericht fertiggestellt und an das Unternehmen und an Pro Honore e.V. übergeben. Gegebenenfalls kann der Auditor eine Empfehlung unter Auflagen aussprechen. In diesem Fall wird dem Unternehmen nochmals die Möglichkeit zur Behebung der Mängel gegeben.

Pro Honore e.V. überprüft den Auditbericht und spricht dann gegenüber der Handelskammer Hamburg eine Zertifizierungsempfehlung aus. Auf dieser Grundlage entscheidet die Handelskammer Hamburg über die Erteilung des Zertifikats.

Zusammengefasst verläuft das Auditierungsverfahren in folgenden wesentlichen Schritten:

1. Bericht des Unternehmens über die Compliance-Organisation und Bearbeitung des Evaluierungsbogens
2. Prüfung der Dokumente und weiterer Informationen durch den Auditor
3. Abschlussgespräch mit der Geschäftsführung
4. Auditbericht an Pro Honore e.V
5. Schlüssigkeitsprüfung durch Pro Honore e.V.
6. Empfehlung von Pro Honore e.V. an die Handelskammer Hamburg.

II. Maßstab der Auditierung

Grundlage der Auditierung sind die Anforderungen des *Hamburger Compliance-Standards,* siehe hierzu Teil 3. Der Evaluierungsbogen dient dazu, diese Inhalte systematisch abzuprüfen.

Bei der Auditierung sind immer die jeweiligen Umstände des Unternehmens zu berücksichtigen. Dies gilt insbesondere im Hinblick auf die mittelständische Struktur.

Der *Hamburger Compliance-Standard* zielt nicht auf die Einführung und Einhaltung rein formeller Regeln ab. Vielmehr ist zu gewährleisten, dass die Compliance-Maßnahmen im Unternehmen nachhaltig und effizient umgesetzt werden. Die Ausgestaltung im Einzelnen wird vom jeweiligen Unternehmen bestimmt. Maßgeblich sind dabei unter anderem die Struktur des Unternehmens, die Branche, die internationalen Ausrichtung, die Anzahl der Mitarbeiter und die Gesellschafterstruktur.

Sinn des Evaluierungsbogens ist es, die Anforderungen des *Hamburger Compliance Standards* in Gestalt von möglichst einfachen und auf Prozesse ausgerichteten Fragen abzuprüfen. Für mittelständische Unternehmen sind allerdings einheitliche Strukturen und Prozesse nicht immer zweckmäßig. Daher haben die Unternehmen die Möglichkeit, von den Vorgaben des Evaluierungsbogens abweichende unternehmensspezifische Besonderheiten zu erläutern.

Bei der Auditierung ist zu prüfen, ob und wie bestehende Zertifizierungen oder Siegel Dritter (beispielsweise aus den Bereichen Umweltschutz, Datenschutz, Produkthaftung oder ähnliches) eingebunden werden können.

3. Teil: Der Hamburger Compliance Standard

Für die Definition der Prüfkriterien ist zu berücksichtigen, dass eine Compliance-Organisation (oft auch als „Compliance Management System“ o.ä. bezeichnet) weder gesetzlich noch in der Rechtsprechung noch in der einschlägigen Literatur abschließend und eindeutig definiert ist. Aus den bestehenden rechtlichen Grundlagen können nur wenige konkrete Vorgaben zur Ausgestaltung einer Compliance-Organisation abgeleitet werden. Zentrale Bestandteile einer Compliance-Organisation haben sich jedoch in der Praxis herausgebildet. Sie werden auf Grundlage dieses Standards unter Einsatz des Evaluierungsbogens abgefragt.

Der Standard ist modular aufgebaut. Die Zertifizierung bezieht sich nur auf die Inhalte der vom Unternehmen jeweils ausgewählten Module. Die vertiefenden Module Vergabeverfahren, Kartellrecht, Datenschutz und Datensicherheit, Gesundheitswirtschaft bauen auf dem Grundmodul auf, so dass Doppelungen vermieden werden können.

I. Grundmodul: Allgemeines Compliance-Verständnis sowie Korruptions- und sonstige Kriminalitätsprävention

1. Compliance-Grundstruktur

1.1. Wesentliche Prüfpunkte

- Analyse der unternehmensspezifischen Compliance-Risiken
- Dokumentation der Compliance-Organisation und mindestens jährlicher Bericht über deren Arbeit
- Eindeutig bezeichneter Compliance-Verantwortlicher mit angemessener Schulung und angemessener hierarchischer Stellung
- Bestehen einer Hinweisgeberstelle nach HinSchG mit der Möglichkeit für die Mitarbeiter, zunächst vertraulich über compliance-relevante Sachverhalte zu berichten
- Schulungen und Erfa-Gruppen der Geschäftsleitung und der Mitarbeiter zur Verhinderung von Compliance-Verstößen

1.2. Erläuterungen

1.2.1. Risikoanalyse

Bei Aufbau und Ausgestaltung der Compliance-Organisation muss gewährleistet werden, dass diese zum einen den spezifischen Bedingungen des Unternehmens und zum anderen den individuellen Compliance-Risiken des Unternehmens gerecht wird. Dies erfolgt im Rahmen einer Risikoanalyse, die am Beginn des Aufbaus der Compliance-Organisation steht. Basis hierfür ist eine Erfassung der Unternehmensstruktur, die einen ausreichenden Eindruck des Unternehmens vermittelt. Die Risikoanalyse sollte laufend fortgeschrieben werden, um den veränderten Anforderungen an das Unternehmen einerseits und den getroffenen Compliance-Maßnahmen andererseits zu entsprechen.

Durch die Risikoanalyse müssen die spezifischen Risiken, die sich insbesondere aus der Struktur des Unternehmens, der Branche, der regionalen Ausrichtung, der Struktur des Vertriebes, sowie den Besonderheiten der Produkte ergeben, erfasst werden. Dabei sind die jeweils geltenden nationalen und internationalen gesetzlichen Anforderungen zu berücksichtigen.

Auf Grundlage dieser Risikoanalyse sind die erforderlichen Compliance-Maßnahmen auszuwählen und umzusetzen. Bei der regelmäßigen Fortschreibung der Risikoanalyse ist zu prüfen, inwieweit den ursprünglich erfassten Risiken wirksam begegnet worden ist, inwieweit sich neue Risikofelder eröffnet haben und wie mit diesen umgegangen werden kann.

Die Risikoanalyse ist zu dokumentieren. Über Ihre Fortschreibung ist in im Rahmen der jährlichen Berichterstattung (siehe unten Ziffer 1.2.2.) zu informieren.

1.2.2 Compliance-Organisation und deren Dokumentation

Bei der Erfassung und Darstellung der Compliance-Organisation des Unternehmens sind die Größe und Struktur des Unternehmens zu berücksichtigen, denn mittelständische Unternehmen verfügen in der Regel nicht über die finanziellen und personellen Ressourcen, wie dies bei einem großen Konzern der Fall sein mag. Gleichwohl kann dies, wie etwa aus dem HinSchG ersichtlich wird, keinen völligen Verzicht auf eine Compliance-Organisation bedeuten. Dies gilt auch im Hinblick auf die organisatorischen Dokumente wie etwa Handbücher, Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen oder die Beschreibung der gesamten Compliance-Organisation. Insbesondere die Dokumentation, also die Nachweise über die getroffenen Compliance-Maßnahmen im Einzelnen, sowie die Dokumentation von Lenkungsmaßnahmen hängt von der Größe und Struktur des jeweiligen Unternehmens ab. Die Dokumentation der Compliance-Maßnahmen dient ganz entscheidend der Minimierung des Haftungsrisikos der Geschäftsleitung. Gleichwohl muss dabei berücksichtigt werden, dass eine ausufernde Dokumentierung und Bürokratisierung nicht Sinn und Zweck einer Compliance-Organisation sein kann. Der Umfang der Dokumentation steht dabei im Spannungsfeld mit dem Haftungsrisiko der Geschäftsleitung. Die Schwerpunktsetzung steht im Ermessen des jeweiligen Unternehmens. Von besonderer Bedeutung ist jedoch eine regelmäßige, mindestens jährliche Berichterstattung über die Wirkung der Compliance-Organisation. Soweit es keine relevanten Vorfälle gegeben hat, kann dieser Bericht auch entsprechend kurz ausfallen.

1.2.3. Compliance-Verantwortlicher

Für die Umsetzung einer Compliance-Organisation ist es erforderlich, dass ein Compliance-Verantwortlicher benannt ist und über klar definierte Zuständigkeiten und Befugnisse verfügt. Bei größeren Unternehmen handelt es sich bei dem Compliance-Verantwortlichen (auch: Compliance-Officer) in der Regel um ein eigenständiges Ressort, das auf einer Ebene mit der Rechtsabteilung und der internen Revision oder Ähnlichem angesiedelt ist. Dies ist für mittelständische Unternehmen nicht zwingend erforderlich. Hier sind verschiedene Gestaltungen und Positionen denkbar. Selbstverständlich ist es auch möglich, dass die Aufgabe des Compliance-Verantwortlichen von der Geschäftsführung mit übernommen wird. An welcher Stelle

der Compliance-Verantwortliche im Unternehmen positioniert ist, hängt dabei von der Größe und Struktur des Unternehmens ab.

Entscheidend ist, dass der Compliance-Verantwortliche mit den für die Implementierung und Aufrechterhaltung der Compliance-Organisation erforderlichen Kenntnissen, Mitteln und Befugnissen ausgestattet ist, so dass er insbesondere

- gewährleisten kann, dass die erforderlichen Maßnahmen und Prozesse eingeführt und laufend umgesetzt werden,
- gewährleisten kann, dass die Compliance-Anforderungen und –Werte innerhalb des gesamten Unternehmens nachhaltig kommuniziert werden,
- Compliance-relevante Vorgänge und Verstöße erfassen und dokumentieren kann,
- laufend und uneingeschränkt an die Geschäftsleitung berichten kann.

Wesentlich ist, dass der Compliance-Verantwortliche bei der Wahrnehmung seiner Aufgaben unabhängig ist und keinen Weisungen unterliegt.

1.2.4. Hinweisgeberstelle

Zentrales Element einer Compliance-Organisation ist ein Hinweisgebersystem. Gesetzliche Grundlage ist hierfür das Hinweisgeberschutzgesetz (HinSchG). Hierbei handelt es sich um eine idealerweise externe Anlaufstelle (auch Ombudsmann, Whistleblower-Hotline, o.ä.), die es sowohl Mitarbeitern als auch externen Personen ermöglicht, compliance-relevante Hinweise mitzuteilen. Dabei ist es von entscheidender Bedeutung, dass der Hinweisgeber anonym bleiben und die den Hinweis aufnehmende Stelle sich auf eine berufsrechtliche Verschwiegenheitspflicht berufen kann. Um dies zu gewährleisten, sollte eine externe Stelle mit dieser Aufgabe betraut werden. Als externe Hinweisgeberstelle im Rahmen des Hamburger Compliance Modells fungiert Pro Honore e.V. und kann von Unternehmen beauftragt werden. Es können aber auch andere, gleichwertige Stellen eingeschaltet werden. Interne Lösungen sind grundsätzlich möglich, müssen aber besonders sorgfältig im Rahmen der Zertifizierung geprüft werden.

Für die Effizienz des Hinweisgebersystems ist es erforderlich, dass dessen Vorhandensein und Vertraulichkeit gegenüber den Mitarbeitern kommuniziert wird. Gegenüber den Mitarbeitern muss nach §§ 32 ff. HinSchG nachhaltig gewährleistet werden, dass die Meldung bei der Hinweisgeberstelle grundsätzlich nicht zu negativen arbeitsrechtlichen Konsequenzen führt.

1.2.5. Schulungen und Erfa-Gruppen

Straftaten werden nicht durch das Unternehmen, sondern durch die handelnden Mitarbeiter begangen. Zur Umsetzung und Durchsetzung des Compliance-Gedankens kommt es daher entscheidend auf die Wissensvermittlung bei den Mitarbeitern an. Ob dies durch Schulungen durch interne oder externe Personen und / oder durch andere Maßnahmen wie etwa Gruppengespräche zum Erfahrungsaustausch („Erfa-Gruppen) erfolgt, steht im Ermessen des Un-

ternehmens. Entscheidend ist jedoch, dass dies von einem nachhaltigen und dokumentierbaren Erfolg gekennzeichnet ist. Auch hier ist im Hinblick auf die Dokumentation zu beachten, dass dies für den Fall eines Compliance-Verstoßes der Haftungsreduzierung dienen kann.

2. Richtlinien

2.1. Wesentliche Prüfpunkte

- Allgemeiner und verbindlicher Verhaltenskodex, auch durch Einbezug anerkannter wirtschaftsethischer Leitbilder wie zum Beispiel das Leitbild der Versammlung Eines Ehrbaren Kaufmanns zu Hamburg e.V.
- Klare Zuständigkeitsregelungen
- Unterschriftenregelung, insbes. Vier-Augen-Prinzip bei wesentlichen Verfügungen
- Richtlinie für Geschenke, Bewirtungen und sonstige Zuwendungen bezogen auf Amtsträger und Geschäftspartner
- Richtlinie zur Nutzung der IT und des Internets durch die Mitarbeiter
- Sonderrichtlinien für besonders risikobehaftete, insbes. korruptionsgefährdete, Geschäftsbereiche, z.B. hinsichtlich der Auswahl von Lieferanten
- Arbeitsvertraglicher Einbezug dieser und sonstiger compliance-relevanter Richtlinien
- Regelmäßige Evaluation

2.2. Erläuterungen

2.2.1 Allgemeiner und verbindlicher Verhaltenskodex

Für den nachhaltigen Erfolg einer Compliance-Organisation ist es erforderlich, dass die Unternehmensleitung das Thema ernst nimmt und dahintersteht. Ob dies tatsächlich der Fall ist, kann nicht alleine mittels des Evaluierungsbogens geprüft werden. Vielmehr können auch z.B. die allgemeine Unternehmenskommunikation und Gespräche mit der Geschäftsleitung und den Mitarbeitern herangezogen werden.

Es kommt entscheidend darauf an, dass die Unternehmensleitung insgesamt nachhaltig zum Ausdruck bringt, dass von allen Mitarbeitern erwartet wird, dass die Compliance-Anforderungen eingehalten werden und Bestandteil der Ziele und Werte des Unternehmens sind.

Für die Inhalte des allgemeinen Verhaltenskodex kann das Leitbild der Versammlung eines Ehrbaren Kaufmanns zu Hamburg e.V. (VEEK) wertvolle Hinweise geben.

2.2.2 Weitere Richtlinien

Die Umsetzung, Gestaltung und Lenkung der compliance-relevanten Maßnahmen erfolgt im Wesentlichen auf der Basis von Richtlinien, Arbeitsanweisungen oder Prozessbeschreibungen. Wie diese gestaltet sind und welche Bereiche diese regeln, hängt von der Struktur des Unternehmens ab. Über alle Unternehmensstrukturen hinweg müssen jedoch die unter 2.1. genannten Themenfelder abgedeckt sein. Die Sonderrichtlinien für besonders risikobehaftete

Geschäftsbereiche müssen die Ergebnisse der Risikoanalyse wiederspiegeln und die dort definierten Bereiche abdecken. Die Richtlinien müssen arbeitsvertraglich für die Mitarbeiter verbindlich sein und regelmäßig evaluiert werden, zumindest im Rahmen des unter Ziffer 1 genannten Compliance-Berichts. Haben sich alle Richtlinien bewährt, kann der Berichtspunkt entsprechend kurz ausfallen.

3. Allgemeine Organisatorische Maßnahmen

3.1. Wesentliche Prüfpunkte

- Systematische Dokumentation aller wesentlichen Verträge
- Bei wesentlichen Verträgen Überprüfung neuer Geschäftspartner hinsichtlich Identität, Beteiligungsverhältnissen etc. („Business Partner Screening“)
- Systematische Überwachung laufender Verträge hinsichtlich der Leistungserbringung
- Systematische Dokumentation und regelmäßige Prüfung besonders risikobehafteter, korruptionsgefährdeter Vorgänge, z.B. Auswahl von Lieferanten
- Standardisierter Prozess zum Umgang mit Verdachts- und Verstoßfällen
- Systematische Erfassung und Dokumentation von versuchten Complianceverstößen durch Dritte, z.B. Schmiergeldangebote, versuchte Kartellabsprachen
- Funktionstrennung bei besonders sensiblen Vorgängen

3.2. Erläuterungen

Für die Umsetzung des Compliance-Gedankens sind verschiedene organisatorische Maßnahmen und Strukturen innerhalb des Unternehmens einzurichten.

Auch hier ist zu beachten, dass die Auswahl und Ausgestaltung der organisatorischen Maßnahmen im Einzelnen von der Unternehmensgröße und der Struktur abhängt. Eine pauschalierte Vorgabe ist gerade für mittelständische Unternehmen nicht möglich. Entscheidend kommt es darauf an, dass die Maßnahmen angemessen und effektiv sind. Die unter Ziffer 3.1. genannten Punkte sollten allerdings im Ergebnis umgesetzt sein. Generell wird bei sensiblen Positionen auch eine Job-Rotation empfohlen. Allerdings muss berücksichtigt werden, dass dies in kleineren Organisationen häufig nicht realisierbar ist.

4. Korruptionsprävention

4.1. Wesentliche Prüfpunkte

- Kontrolle der Einhaltung der Richtlinie für Geschenke, Bewirtungen und sonstige Zuwendungen gegenüber Amtsträgern und Geschäftspartnern
- Kontrolle der Geschäftskonten, insbes. im Ausland
- Kontrolle des Bargeldverkehrs
- Kontrolle der Gewährung von Sonderkonditionen, z.B. Rabatte, Gutschriften, Mehrlieferungen etc.
- Kontrolle der Vertragsgestaltung, Leistungserbringung und Abrechnung von Vermittlern, Agenten, Beratern

- Genehmigungspflicht von Nebentätigkeiten der Mitarbeiter
- Meldepflicht von privaten Beteiligungen der Mitarbeiter an Wettbewerbern und wesentlichen Geschäftspartnern

4.2. Erläuterungen

Die Maßnahmen zur Korruptionsprävention hängen stark von der Struktur des Unternehmens ab. Beispielsweise wird ein Unternehmen mit mehreren Beteiligungen / Tochtergesellschaften über zahlreiche Bankkonten verfügen, sodass sich allein hieraus ein erhöhtes Risiko der Bildung von Schwarzgeldkonten und unzulässigen Verfügungen ergeben kann. Die Maßnahmen zur Korruptionsprävention werden ausführlich und gesondert in die Prüfung einbezogen, da die Korruptionsprävention ein zentraler Gegenstand jeder Compliance-Organisation ist.

5. Unternehmenssicherheit

5.1. Wesentliche Prüfpunkte

- Schutz von Betriebsgeheimnissen, Richtlinie zum Umgang mit sensiblen Dokumenten und Daten
- IT-Sicherheit, insbes. regelmäßig wechselnde Zugangskennungen und Maßnahmen gegen Datenmanipulation
- Regelung zur Datenträgervernichtung
- Gebäudesicherheit
- Regelmäßige Erfassung der Lagerbestände zur Diebstahlsprävention und systematische Verfolgung von Fehlbeständen
- Jederzeit funktionsfähige Weisungskette, auch im Vertretungsfall

5.2. Erläuterungen

Klassischerweise umfasst die Compliance-Thematik solche Bereiche, bei denen das Risiko der Begehung von Straftaten aus dem Unternehmen heraus gegenüber Dritten besteht. Das Risiko von Straftaten gegenüber dem Unternehmen selbst wird dabei in der Regel ausgeklammert. Eine solche Trennung ist jedoch nicht effizient, da das entsprechende Wissen und die Strukturen in einer Compliance-Organisation ohnehin vorhanden sind. Vor allem kann durch die integrierte Betrachtung des Themas Unternehmenssicherheit innerhalb der Compliance-Organisation gerade für mittelständische Unternehmen ein erhebliches Risikopotential erfasst und mit abgedeckt werden.

Ein anderer wichtiger – und oft unterschätzter – Bereich ist der Bereich des Know-How-Schutzes und der IT-Sicherheit. Der Umgang mit Daten von Mitarbeitern und Geschäftspartnern und mit den eigenen Unternehmensdaten stellt in einer vernetzten Welt einen erheblichen Risikofaktor dar. Der Evaluierungsbogen erfasst bei der Prüfung der IT-Sicherheit auch die zentralen Aspekte des organisatorischen und technischen Datenschutzes, also insbesondere die Kontrolle von Zutritt, Zugang, Zugriff, sowie die Weitergabe, Verfügbarkeit und Eingabe von Daten und die Beauftragung Dritter mit EDV-Aufgaben.

Die hier zu treffenden Maßnahmen hängen wesentlich von dem Geschäftsmodell und der Struktur des Unternehmens ab.

6. Zahlungsverkehr und Rechnungswesen

6.1. Wesentliche Prüfpunkte

- Ordnungsgemäße Buchführung mit externer Gegenkontrolle durch Steuerberater oder Wirtschaftsprüfer
- Sicherstellung der Einhaltung von Vorschriften gegen Geldwäsche
- Standardisierte Prozesse zur Kontrolle und Freigabe von Rechnungen und Zahlungen, insbes. Vier-Augen-Prinzip
- Kassenordnung
- Regelung zum Scheckverkehr
- Regelmäßige Prüfung von Reisekosten- und Spesenabrechnungen
- Regelmäßige, unangemeldete Prüfungen der Kassen und des Scheckverkehrs

6.2. Erläuterungen

Die Bereiche Zahlungsverkehr und Rechnungswesen erfordern ein hohes Maß an Aufmerksamkeit, da hier korruptive Maßnahmen ermöglicht und verschleiert werden können. Daher liegt hier ein eigener Prüfungsschwerpunkt, wobei viele der genannten Maßnahmen auch aus anderen Gründen in den meisten Unternehmen regelmäßig eingeführt sind.

Von vielen Unternehmen wird häufig übersehen, dass sie Vorgaben zur Verhinderung von Geldwäsche beachten müssen. Diese Thematik ist insbesondere im internationalen Geschäfts- und Zahlungsverkehr besonders zu beachten.

II. Modul 2: Vergabeverfahren

1. Wesentliche Prüfpunkte

- Richtlinie zum Verhalten im Vergabeverfahren, insbes. Prävention von wettbewerbswidrigen Maßnahmen und sektorspezifische Aspekte (VOB, VOL etc.)
- Richtlinie für Geschenke, Bewirtungen und sonstige Zuwendungen gegenüber Amtsträgern mit besonderem Fokus auf die Akquisition öffentlicher Aufträge
- Effiziente Sicherungssysteme zur Vermeidung sonstiger, vergaberelevanter Verstöße im Sinne von § 2 des Hamburgischen Korruptionsregistergesetzes, insbes. Schwarzarbeit
- Abwesenheit von vergaberelevanten Sanktionen und Registereintragungen, sowohl des Unternehmens, der Geschäftsführung als auch der mit Vergabeverfahren betrauten Mitarbeiter
- Schulungen der Mitarbeiter zum Vergabeverfahren
- Systematische Dokumentation der Vergabeverfahren

2. Erläuterungen

Für das Modul Vergabeverfahren wird auf die Evaluierung des Grundlagen-Moduls aufgebaut. Der Fragenkatalog ist daher relativ überschaubar, da viele relevante Themen bereits mit dem Grundlagen-Modul abgefragt werden. Die hier aufgeführten Punkte sind als Vertiefung zu verstehen.

Für Unternehmen, die öffentliche Aufträge der Freien und Hansestadt Hamburg akquirieren, kommt es entscheidend auf das Vorliegen der Voraussetzungen nach dem Hamburger Korruptionsregistergesetz an. Der Einfachheit halber wird auf die dort unter § 2 abzufragenden Verstöße verwiesen. Die Sicherungssysteme gegen solche Verstöße sind daher gesondert zu erfassen. Soweit in anderen Bundesländern „Korruptionsregister“ eingeführt oder geplant sind, sind diese Themenfelder, soweit ersichtlich, ebenfalls relevant.

III. Modul 3: Kartellrecht

1. Wesentliche Prüfpunkte

- Stellung des Unternehmens zum Wettbewerb
- Vorliegen einer marktbeherrschenden Stellung
- Position zu Kunden und Lieferanten
- Vertriebsstrukturen
- Kooperationen
- Verbände
- Rabattstrukturen

2. Erläuterungen

Gerade von mittelständischen Unternehmen werden sowohl die Risiken von kartellrechtlichen Verstößen, als auch die eigene Positionierung im Wettbewerb oder gar das Vorliegen einer marktbeherrschenden Stellung unterschätzt. Kartellrechtliche Compliance ist daher für Unternehmen jeder Größe wichtig, da für die kartellrechtliche Bewertung nicht die Unternehmensgröße entscheidend ist, sondern die Positionierung auf nationalen oder internationalen Märkten. Es kommt daher im Modul Kartellrecht vornehmlich darauf an, das Bewusstsein hierfür zu schärfen und die Situation des Unternehmens zu erfassen um die kartellrechtlichen Risiken so gering wie möglich zu halten.

IV. Modul 4: Datenschutz und Datensicherheit

1. Wesentliche Prüfpunkte

- Datenschutzbeauftragter
- Auftragsverarbeitung
- Umgang mit Daten von Angestellten
- Umgang mit Daten von Geschäftspartnern

- Datenschutz und Internet
- Daten- und Unternehmenssicherheit
- Mobiles Arbeiten
- Überwachungsmaßnahmen
- Datenspeicherung und Umgang mit Anträgen von Betroffenen
- Erkennung, Prüfung und Meldung von Datenschutzverstößen

2. Erläuterungen

Verstöße gegen Datenschutzregelungen können nicht nur zu Bußgeldern – mit der DSGVO noch verschärft - und sogar strafrechtlicher Verfolgung führen, sondern auch ganz erhebliche Imageschäden hervorrufen. Das gilt nicht nur im Hinblick auf die Daten von Geschäftspartnern und Kunden. Auch die unternehmenseigenen Daten sind nicht immer optimal geschützt. Durch das umfangreiche Modul Datenschutz und Datensicherheit kann nachgewiesen werde, dass die Geschäftsführung die komplexen Anforderungen des Datenschutzes und der Datensicherheit erfüllt.

V. Modul 5: Gesundheitswirtschaft

1. Wesentliche Prüfpunkte

- Zusammenarbeit mit Fachkreisangehörigen und Patientenorganisationen
- Zuweisungen, Verordnungen, Empfehlungen und sonstige Leistungen gegen Entgelt
- Studien und Anwendungsbeobachtungen
- Drittmittel, Spenden & Sponsoring
- Zuwendungen, Fortbildungen, Einladungen, Geschenke und Bewirtung

2. Erläuterungen

Für die hoch regulierte Gesundheitswirtschaft die Beachtung von Compliance – insbesondere aufgrund der Neuregelung zur Bestechung Angehöriger eines Heilberufs nach § 299a StGB - ausgesprochen wichtig. Das Modul Gesundheitswirtschaft baut auf dem Grundmodul auf und vertieft die spezifische Problemstellung der Gesundheitswirtschaft insbesondere aus Sicht der Industrie, Kranken- und Pflegehäuser, Leistungserbringer und der übrigen Beteiligten der Gesundheitswirtschaft.

VI. Modul 6: Lieferkette und ESG

1. Wesentliche Prüfpunkte

- Existenz einer unternehmensinternen Lieferkettenstrategie und deren Implementierung
- Einrichtung und fortlaufende Überprüfung eines Risikomanagementsystems
- Erfassung von Daten im ESG-Bereich durch das Unternehmen
- Bewusstsein über Branchen-, Länder-, Produkt- und Lieferantenrisiken
- Detaillierte Risikoermittlung in den einschlägigen Bereichen

- Bewertung und Priorisierung der erfassten Risiken
- Durchführung risikospezifischer Abhilfemaßnahmen

2. Erläuterungen

Die Anforderungen an die Einhaltung gesetzlicher und bußgeldbewährter Verpflichtungen für den Bereich Lieferketten sind komplex und werden den kommenden Jahren mit der CSDDD auf europäischer Ebene verschärft. Insoweit praktisch relevant sind insbesondere Menschenrechts- und Umweltrisiken, die in vielen Facetten auftreten können. Beispielsweise ist die Verhinderung von Kinderarbeit und Sklaverei, die Einhaltung des Arbeitsschutzes, der Umgang mit Schadstoffen sowie eine kontrollierte Entsorgung von Abfallprodukten zu nennen. Aus wirtschaftlicher Sicht können Missachtungen in diesen Bereichen rasant medial verbreitet werden und zu einem erheblichen Umsatzrückgang und spürbar fortdauernden Imageschäden führen.

Dieses Modul soll auch solchen Unternehmen offenstehen, die nicht dem LkSG unterliegen und so die Möglichkeit geben, ihre Lieferkettenstrategie nach außen darzustellen.

4. Teil: Gebühren

		Kategorie 1	Kategorie 2	Kategorie 3	Kategorie 4
Zertifizierung	Grundmodul	900 €	2.700 €	5.400 €	n.V.
	Vergabeverfahren	300 €	900 €	1.800 €	33 % des Grundmoduls
	Kartellrecht	300 €	900 €	1.800 €	33 % des Grundmoduls
	Datenschutz und Datensicherheit	300 €	900 €	1.800 €	33 % des Grundmoduls
	Gesundheitswirtschaft	300 €	900 €	1.800 €	33 % des Grundmoduls
Nutzung des Zertifikats / p.a.	Grundmodul	150 €	450 €	900 €	15 % des Zertifizierungsentgelts
	Zusatzmodule	50 €	150 €	300 €	15 % des Zertifizierungsentgelts
Rezertifizierung	Grundmodul	450 €	1.350 €	2.700 €	50 % des Zertifizierungsentgelts
	Zusatzmodule	150 €	450 €	900 €	50 % des Zertifizierungsentgelts
Auditoren	Tagessatz (Richtwert)	1.600 - 2.000 €			

Unternehmenskategorien:	
1.	Weniger als 10 Mitarbeiter, Umsatz / Bilanzsumme max. 2 Mio. €
2.	10 bis 50 Mitarbeiter, Umsatz / Bilanzsumme max. 10 Mio. €
3.	51 bis 250 Mitarbeiter, Umsatz / Umsatz / Bilanzsumme max. 50 Mio. €
4.	Mehr als 250 Mitarbeiter, Bilanzsumme über 50 Mio. €

Richtwerte Kategorie 4 / Grundmodul	
Umsatz / Bilanzsumme bis 100 Mio. €, bis 300 Mitarbeiter	10.000 €
Umsatz / Bilanzsumme bis 200 Mio. €, bis 500 Mitarbeiter	15.000 €
Umsatz / Bilanzsumme über 500 Mio. €, über 500 Mitarbeiter	20.000 €