

# Compliance Management

Eine anspruchsvolle Aufgabe:  
Von der Vermeidung von Haftungsfällen  
zu guter Unternehmensführung



# Inhaltsverzeichnis

Generelle Anforderungen .....	4
1. Entwicklung und Implementierung von Compliance- Management-Systemen (CMS).....	6
2. Prüfung von Compliance-Management-Systemen .....	8
3. Mitarbeiterschulungen .....	10
4. Compliance Audits .....	11
5. Compliance Due Diligence .....	12
6. Compliance Screenings .....	14
Kontakt .....	15

# Generelle Anforderungen

**Compliance bedeutet die Einhaltung von Gesetzen, regulatorischen Anforderungen, Organisationsgrundsätzen, internen Kodizes und Richtlinien durch das Unternehmen, seine Organe und Mitarbeiter.**

Verschärfte Rahmenbedingungen weltweit

Die Missachtung von Gesetzen, regulatorischen Anforderungen und der darauf abgestimmten internen Richtlinien kann gravierende Negative Auswirkungen auf Unternehmen haben und in Einzelfällen existenzbedrohend sein. Non-Compliance wird in aktuellen Umfragen als eines der Hauptrisiken für Unternehmen genannt. Die zahlreichen Unternehmensskandale der letzten Jahre aufgrund von Korruptions-, Betrugs-, Bilanzdelikten und Kartellverstößen haben weltweit eine Welle der Regulierung und der verschärften Durchsetzung bereits vorhandener Rechtsnormen ausgelöst. Unternehmen versuchen daher verstärkt, sich vor Haftungsfällen und damit einhergehenden Reputationsschäden zu schützen.

Haftung von Leitungs- und Aufsichtsorganen

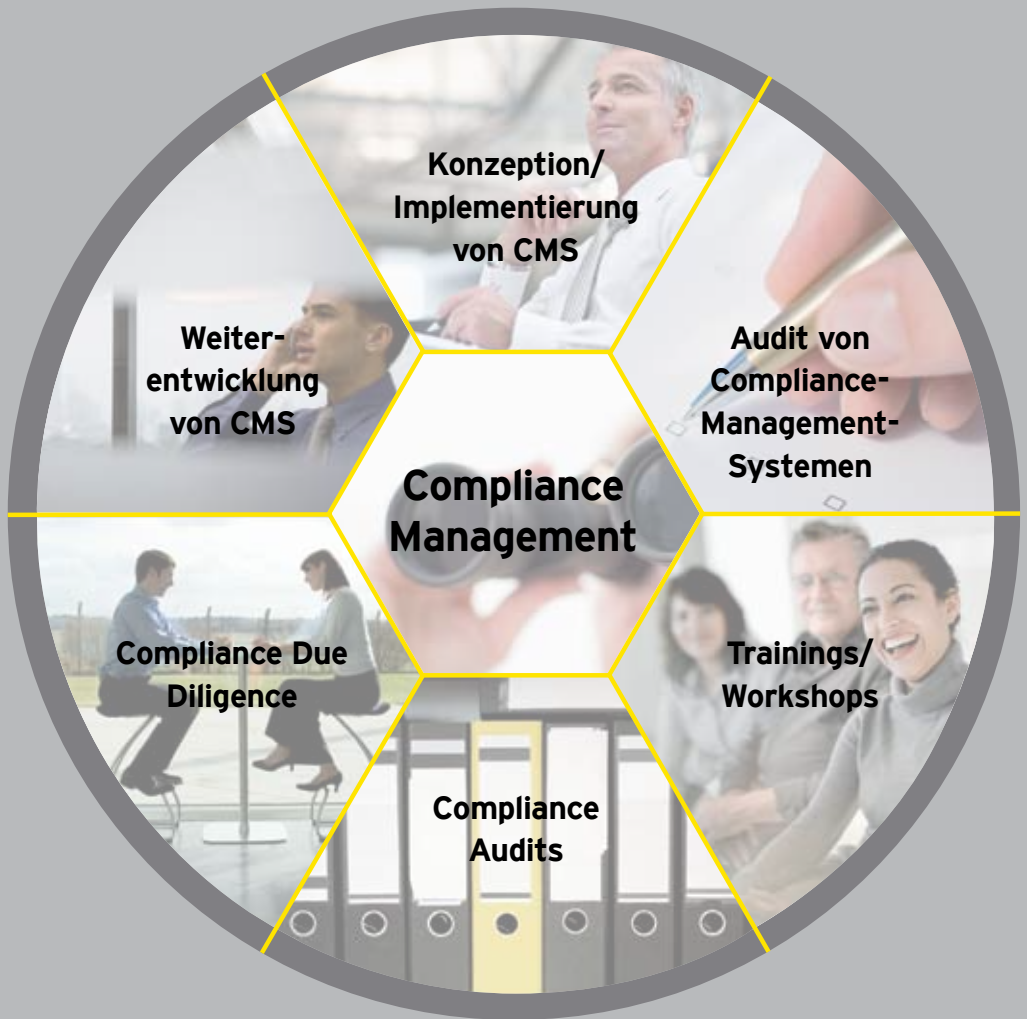
Seit den Unternehmensskandalen und der Kapitalmarkt-/Kreditkrise wird vermehrt der Ruf nach Inanspruchnahme der Verantwortlichen laut: Vorstände und Aufsichtsräte werden zunehmend für Pflichtverletzungen persönlich zur Verantwortung gezogen.

Gute Unternehmensführung als Erfolgsfaktor

Seit Veröffentlichung des Österreichischen Corporate Governance Kodex im Jahr 2002 gilt Compliance als ein wesentlicher Bestandteil guter Unternehmensführung (Corporate Governance). Mit dem Inkrafttreten des Unternehmensrechtsänderungsgesetz 2008 hat der Gesetzgeber die Aufsichtspflichten der Aufsichtsräte und des Managements von Aktiengesellschaften und kapitalmarktorientierten Unternehmen erweitert. Die Regelungsdichte im Bereich Corporate Governance/Compliance steigt weltweit und die Einhaltung wird zu einem Erfolgsfaktor für Unternehmen aller Größen und Branchen.

Vorkehrungen treffen

Compliance-Management-Systeme sind darauf ausgerichtet, den organisatorischen Rahmen hinsichtlich Aufbau und Ablauf zu schaffen, um Verstöße zu vermeiden. Dazu gehört eine auf die Organisation zugeschnittene Konzeption und Implementierung ebenso wie die effektive und effiziente Überwachung der Einhaltung von Gesetzen und internen Richtlinien durch die Organe und Mitarbeiter des Unternehmens.



CMS - Compliance-Management-Systeme

# 1. Entwicklung und Implementierung von Compliance-Management-Systemen (CMS)

Zur Vermeidung von Verstößen gegen Anti-Korruptions-, Kartell- oder auch Datenschutzgesetze und zur Vermeidung von wirtschaftskriminellen Handlungen werden unternehmensinternen Compliance-Management-Systeme installiert. Sie sollen Mitarbeitern und Stakeholdern einen Orientierungsrahmen bieten und präventiv Non-Compliance verhindern.

Die unternehmensspezifische Konzeption und Implementierung eines Compliance-Management-Systems ist eine Herausforderung für die Unternehmensleitung sowie die Aufsichtsgremien. Compliance selbst entwickelt sich hierbei auf Basis der jeweiligen Unternehmensgeschichte und damit verbundener Werte, an denen sich alle Mitarbeiter orientieren (Unternehmenswerte). Ebenso ist Compliance nicht mehr nur ein Steuerungs- und Kontrollelement, sondern vielmehr auch zu einem Instrument nachhaltiger Unternehmensführung geworden und bietet Hilfestellung für alle Stakeholder des Unternehmens.

Die Eingliederung von Compliance Management in die Unternehmenswerte und -kultur, die Geschäftsprozesse sowie in das Berichts- und Kontrollwesen ist eine elementare und schwierige Aufgabe für jedes Unternehmen. In der Praxis hat sich bei der Ausgestaltung von Compliance-Management-Systemen ein Drei-Säulen-Modell etabliert, das in der nachfolgenden Grafik dargestellt ist.



Compliance-Kultur, Compliance-Ziele, Compliance-Organisation		
Vermeidung	Früherkennung	Reaktion
Vorschriften und Verfahren	Risiko-Analyse	Sanktionen
Schulungen	Hinweisgeberstelle	Fallverfolgung
Beratung	Mitarbeiterbefragungen	Systemanpassungen
Anreizsystem	Compliance Audits	
Kommunikation		
Prüfung von CMS		

Compliance Management ist nicht zuletzt durch die Aufnahme in eine Vielzahl von nationalen und internationalen Standards und Gesetzen (z.B. Österreichischer Corporate Governance Kodex, US Federal Sentencing Guidelines, UK Bribery Act, etc.) sowie durch die Erwartungshaltung der Interessenvertreter an „Good Governance“ und „Zero Tolerance“ bei Verstößen gegen Gesetze oder Richtlinien zu einem wichtigen Element der guten Unternehmensführung geworden.

Folgende Schritte sollten bei der Konzeption und Implementierung eines Compliance-Management-Systems im Mittelpunkt stehen:

- ▶ Durchführung von Risikoanalysen und Erarbeitung von unternehmensspezifischen Compliance-Konzepten;
- ▶ Entwicklung von Organisationsstrukturen und Berichtswegen;
- ▶ Erstellung von Richtlinien, Arbeitshilfen, Schulungsunterlagen, Reporting-Lösungen und gegebenenfalls Einrichtung einer Whistleblower-Hotline;
- ▶ Erstellen von Roll-Out- und Implementierungskonzepten.

## 2. Prüfung von Compliance-Management-Systemen

Etablierte Compliance-Management-Systeme unterliegen einem ständigen Wandel. Nicht nur interne Strukturen und Prozesse verändern sich, sondern auch regulatorische Anforderungen sowie die Risiken, mit denen Ihr Unternehmen konfrontiert ist.

Eine unabhängige Prüfung des Compliance-Management-Systems durch Ernst & Young gibt Ihnen die Sicherheit, dass Sie gut aufgestellt sind und Ihr Compliance-Management-System allen Anforderungen gerecht wird. Sie können hierbei je nach Bedarf aus den folgenden Prüfungsdienstleistungen wählen:

### 1. Compliance-Quick-Check:

Kurzreview Ihrer Risikolandschaft und Ihres Compliance-Management-Systems;

### 2. Prüfung des Compliance-Management-Systems in Anlehnung an den deutschen Prüfungsstandard IDW PS 980:

Bei der Prüfung von Compliance-Management-Systemen ist zwischen den folgenden, aufeinander aufbauenden Arten zu unterscheiden:

#### ► **Konzeptionsprüfung:**

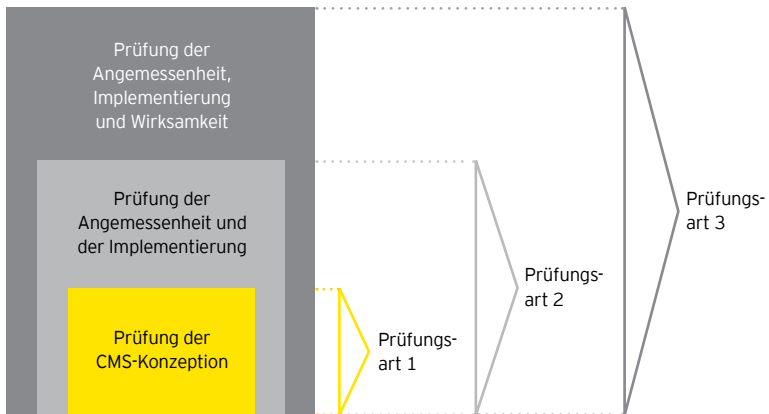
Prüfung der Konzeption des Compliance-Management-Systems unter Berücksichtigung der Risikosituation des Unternehmens;

#### ► **Angemessenheits- und Implementierungsprüfung:**

Prüfung der Angemessenheit sowie der zentralen und dezentralen Implementierung des Compliance-Management-Systems;

#### ► **Angemessenheits-, Implementierungs- und Wirksamkeitsprüfung:**

Prüfung der Angemessenheit, der zentralen und dezentralen Implementierung sowie der Wirksamkeit des Compliance-Management-Systems.



3. Überprüfung Ihres Compliance-Management-Systems in Anlehnung an weitere allgemein anerkannte Standards (z.B. US Federal Sentencing Guidelines) sowie in Bezug auf branchenspezifische Anforderungen.

**Nationale und internationale Standards geben dem Compliance-Management-System einen Rahmen, ohne die individuelle Ausgestaltung und Umsetzung einzuschränken.**



# 3. Mitarbeiterschulungen

Die Auslegung gesetzlicher oder regulatorischer Vorgaben für Compliance-relevante Themen kann nicht dem einzelnen Mitarbeiter überlassen werden. Um Missverständnisse zu vermeiden, ist es wichtig, sowohl die Compliance-relevanten Rahmenbedingungen praxisgerecht zu vermitteln, als auch die Komponenten der Compliance-Organisation vorzustellen. Mit strukturierten und umfassenden Schulungen zu Themenkomplexen wie Anti-Korruption, Datenschutz, Wettbewerbs- und Außenwirtschaftsrecht im Rahmen von Compliance-Trainings (national und international) können Mitarbeiter für diese Thematik sensibilisiert werden.

Zur Mitarbeiterschulung können entsprechende Zielgruppen definiert und ein teilnehmergerechtes Training mit Fallbeispielen, Übungen und der Möglichkeit zur Diskussion entwickelt werden.

Ziel ist es, den Mitarbeitern einen verlässlichen Handlungsrahmen insbesondere für konkrete Dilemma-Situationen in der Praxis zu vermitteln. Für Schulungen von Mitarbeitern in Landesgesellschaften können Seminarinhalte an die rechtlichen Rahmenbedingungen in den jeweiligen Ländern sowie die unternehmensindividuellen Dilemma-Situationen angepasst werden.

**Nutzen von Corporate Compliance**  
Funktionsfähiges Compliance Management hat Vorteile

- Höhere Rechtssicherheit für Unternehmen & Mitarbeiter und Mitarbeiter
- Senkung des Haftungsrisikos für Organmitglieder und Mitarbeiter
- Sicherung / Verbesserung der Unternehmensreputation und Geschäftsbeziehungen
- Präventive Wirkung gegen dolose Handlungen im Unternehmen (Vermögensschutz)
- Steigerung der Profitabilität
  - Senkung der internen und externen Transaktionskosten
  - Vermeidung von Risiken
  - Wettbewerbsvorteile durch Investition in Erfolgsfähigkeit
- Steigerung des Unternehmenswertes
- Verbesserung des Risikomanagements
- Informationsgewinnung und Auswertung

**Wettbewerbsvorteil**

**Typisches Täterprofil für alle (am Beispiel des Finanzsektors)**

- 90% männlich
- 40-45 Jahre alt
- Überdurchschnittlich gebildet

> 10 Jahre im Unternehmen, davon > 8 Jahre auf der gleichen Position

ca. 70% nicht aus dem Management, aber ca. 15 % aus dem Top-Management

**Compliance Kompaktseminar  
Compliance im Vertrieb**

25. Januar 2011, XY GmbH,

Ernst & Young Wirtschaftsprüfungsgesellschaft GmbH  
Fraud Investigation & Dispute Services /  
Corporate Compliance Services

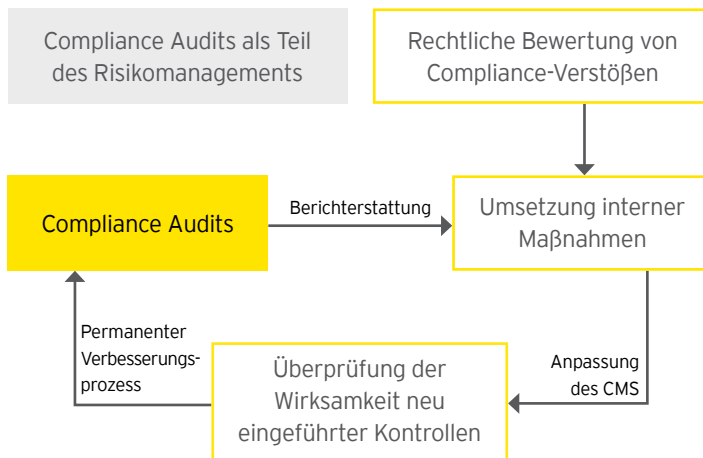
**ERNST & YOUNG**  
Quality in everything we do

## 4. Compliance Audits

Wesentlicher Bestandteil eines Compliance-Management-Systems ist die Überwachung der Einhaltung von gesetzlichen und regulatorischen Anforderungen sowie von entsprechenden internen Richtlinien.

Die Durchführung von nicht-anlassbezogenen und risikoorientierten Compliance Audits in Kooperation mit der Internen Revision/Compliance-Abteilung ist empfehlenswert.

Ziel der Compliance Audits ist es, Verstöße gegen Gesetze und interne Richtlinien aufzudecken. Zudem bieten Compliance-Audits wertvolle Einblicke in die tatsächlich gelebten Unternehmensprozesse und helfen dabei, ein besseres Verständnis für die Risikosituation des Unternehmens zu entwickeln.



In Zusammenhang mit Compliance-Audits sollten die folgenden wesentlichen Schritte beachtet werden:

- ▶ Erarbeitung eines Compliance-Audit-Ansatzes – zugeschnitten auf die Compliance-Risiken des Unternehmens oder bestimmte Unternehmensbereiche;
- ▶ Durchführung von nicht-anlassbezogenen Compliance Audits im In- und Ausland, um die Beachtung von Gesetzen und internen Richtlinien zu überwachen;
- ▶ Dokumentation bei Verstößen, um konkrete Maßnahmen zur Verbesserung des Compliance-Management-Systems einleiten zu können;
- ▶ Erarbeitung eines Maßnahmenkataloges, um auf Grundlage der Erkenntnisse aus den Compliance Audits das Kontrollumfeld des Unternehmens oder einzelner Bereiche nachhaltig zu verbessern.

# 5. Compliance Due Diligence

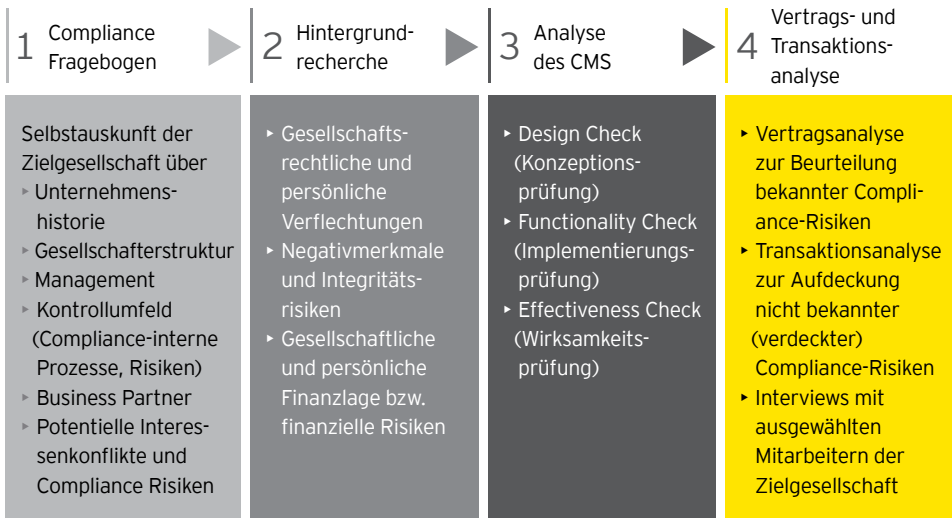
Aufstrebende und erfolgreiche Unternehmen wachsen häufig durch Zukäufe von anderen Gesellschaften. Was oftmals unterschätzt wird: Transaktionen dieser Art können erhebliche rechtliche, regulatorische und geschäftliche Risiken mit sich bringen. Sobald die erwerbende Gesellschaft die Kontrolle über die Zielgesellschaft übernimmt, kann der Käufer für Verstöße gegen Anti-Korruptions- und Kartellgesetze durch das erworbene Unternehmen oder dessen Mitarbeiter haftbar gemacht werden – auch wenn diese bereits vor der Übernahme erfolgt sind. Darüber hinaus kann das erwerbende Unternehmen auch für die markt- und reputationsbedingten Risiken zur Rechenschaft gezogen werden.

Um eine erste Einschätzung der vorhandenen Compliance-Risiken der Zielgesellschaft vornehmen zu können, sollte eine Compliance Due Diligence bei der Zielgesellschaft durchgeführt werden. Dabei sollte eine Auswertung der durch die Zielgesellschaft zugänglich gemachten Informationen und Daten vorgenommen werden. Darüber hinaus können öffentliche Quellen zur Verifizierung der Angaben herangezogen werden. Folgende Bereiche sollten bei der Compliance Due Diligence beachtet werden:

- ▶ Die Beschaffung und Auswertung von Hintergrundinformationen über das Unternehmen, das Management und relevante Geschäftspartner;
- ▶ Die Analyse und Einschätzung der Ausgestaltung und Effektivität des bestehenden Compliance-Management-Systems der Zielgesellschaft;
- ▶ Die Identifikation von Integritätsrisiken und Interessenskonflikten des Verkäufers;
- ▶ Die Untersuchung auf risikobehaftete Geschäftsbeziehungen und die Untersuchung ausgewählter Transaktionen.



Zur Durchführung der Compliance Due Diligence kann nach folgenden Arbeitsschritten vorgegangen werden, wobei die Arbeitsschritte 2 bis 4 auch unabhängig voneinander und separat durchgeführt werden können:



Mit den Ergebnissen der Compliance Due Diligence-Prüfung steht eine Einschätzung über mögliche Compliance-Risiken beim Zielunternehmen sowie eine Einschätzung der Integrität des Managements und dessen Geschäftsgebarens zur Verfügung. Ziel ist die Vermeidung von Image- und Reputationsschäden sowie von direkten finanziellen Verlusten aus Strafzahlungen, Schadensersatzleistungen und hohen internen Aufklärungskosten bei Verstößen, z.B. gegen Anti-Korruptionsgesetze.

## 6. Compliance Screenings

Das „Know Your Customer“ (KYC) -Prinzip, der Foreign Corrupt Practices Act (FCPA), die OECD Anti-Bribery Convention, der UK Bribery Act sowie eine Reihe anderer regulatorischer Anforderungen verlangen ein ausgewiesenes Wissen über die Hintergründe und die Reputation, letztlich also die Integrität des Gegenübers im Geschäftsverkehr. An dieser Stelle setzen Compliance Screenings an: Analog zu den Hintergrundrecherchen (siehe auch Compliance Due Diligence) handelt es sich hierbei um ein Verfahren systematisierter Primär- und Sekundärrechercheverfahren, mit dem Ziel, ein verlässliches Maß an Informationen zu gewinnen und diese hinsichtlich ihrer Validität und Glaubwürdigkeit zu bewerten. Dies erfordert neben dem Wissen über Zugänge zu weltweiten, öffentlich verfügbaren Datenquellen, proprietärer oder non-proprietärer Natur, auch die Fähigkeit eines international vernetzten Handelns.

Die Durchführung eines Compliance Screenings beinhaltet:

- ▶ Die Planung der Recherche und Bestimmung der integritätsrelevanten Indikatoren (z.B. Negativmeldungen in der Presse) bezogen auf das jeweilige Integritätsrisiko, der zu recherchierenden Gesellschaft/Person und der regionalen Besonderheiten (z.B. in asiatischen Ländern oder in Ländern des Nahen/Mittleren Ostens);
- ▶ Die Sammlung von integritätsrelevanten Aussagen im öffentlichen Raum bezogen auf die jeweilige Gesellschaft/Person (dies schließt z.B. auch die Nutzung internationaler Compliance-Datenbanken und damit die Analyse von weit über 300 internationalen Sanktionslisten mit ein);
- ▶ Die Produktion und Analyse der gesammelten Informationen vor dem Hintergrund der Recherchefragestellung;
- ▶ Die Übergabe in Form eines Berichts (dieser kann neben Integritätsaussagen z.B. auch analytische grafische Aufbereitungen beinhalten).

# Kontakt

Wir hoffen, dass Sie die Lektüre dieses Praxisleitfadens unterstützt, die wesentlichen Elemente des Compliance Management zu adressieren.

Für Fragen und weitere Auskünfte stehen Ihnen Ihre Ernst & Young Ansprechpartner gerne zur Verfügung.

---

**Mag. Gunther Reimoser**

Tel. +43 1 211 70 1032

gunther.reimoser@at.ey.com

**Dkfm. Jörg Johannsen**

Tel. +43 1 211 70 1052

joerg.johannsen@at.ey.com

**Benjamin Weissmann, BSc**

Tel. +43 1 211 70 1121

benjamin.weissmann@at.ey.com

**Mag. Markus Hölzl**

Tel. +43 1 211 70 1182

markus.hoelzl@at.ey.com

---

Ernst & Young

Assurance | Tax | Transactions | Advisory

#### Die globale Ernst & Young-Organisation im Überblick

Die globale Ernst & Young-Organisation ist einer der Marktführer in der Wirtschaftsprüfung, Steuerberatung und Transaktionsberatung sowie in der Risiko- und Managementberatung. Ihr Ziel ist es, das Potenzial ihrer Mitarbeiterinnen und Mitarbeiter und Klienten zu erkennen und zu entfalten. Die 152.000 Mitarbeiterinnen und Mitarbeiter sind durch gemeinsame Werte und einen hohen Qualitätsanspruch verbunden.

Die globale Ernst & Young-Organisation besteht aus den Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig und haftet nicht für das Handeln und Unterlassen der jeweils anderen Mitgliedsunternehmen. Ernst & Young Global Limited ist eine Gesellschaft mit beschränkter Haftung nach britischem Recht und erbringt keine Leistungen für Klienten. Weitere Informationen finden Sie unter [www.ey.com/austria](http://www.ey.com/austria)

In Österreich ist Ernst & Young mit rund 550 Mitarbeiterinnen und Mitarbeitern an vier Standorten präsent. „Ernst & Young“ und „wir“ beziehen sich in dieser Publikation auf alle österreichischen Mitgliedsunternehmen von Ernst & Young Global Limited.

© 2012 Ernst & Young

Wirtschaftsprüfungsgesellschaft m.b.H.  
All Rights Reserved.

Diese Publikation ist lediglich als allgemeine, unverbindliche Information gedacht und kann daher nicht als Ersatz für eine detaillierte Recherche oder eine fachkundige Beratung oder Auskunft dienen. Obwohl sie mit größtmöglicher Sorgfalt erstellt wurde, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität; insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalls Rechnung tragen. Eine Verwendung liegt damit in der eigenen Verantwortung des Lesers. Jegliche Haftung seitens der Ernst & Young Wirtschaftsprüfungsgesellschaft m.b.H. und/oder anderer Mitgliedsunternehmen der globalen Ernst & Young-Organisation wird ausgeschlossen. Bei jedem spezifischen Anliegen sollte ein geeigneter Berater zu Rate gezogen werden.

Bildrechte bis 6. Jänner 2013