IT-Compliance
aus Sicht des Wirtschaftsprüfers

19. November 2010

Karin Thelemann, Partnerin

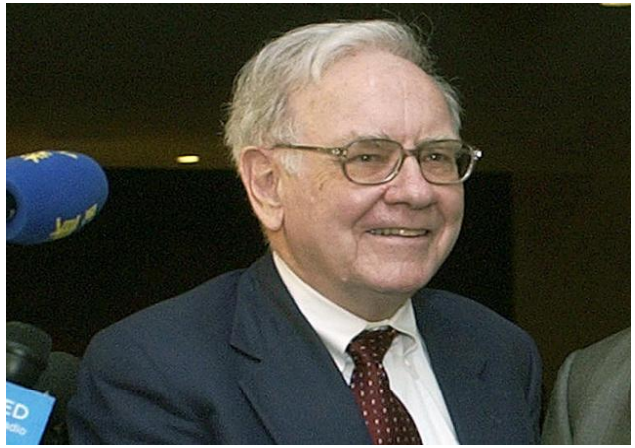
ERNST & YOUNG
Quality In Everything We Do

Rechnungswesen, IT und Compliance

- “It takes 20 years to build a reputation and five minutes to ruin it.”

  “If you think about it, you will do things differently”.

  (Warren Buffet)



Agenda

- **IT-Compliance**
- Aktuelle nationale und internationale Standards
- IT-Compliance und IT-Revision

IT-Compliance

IT-Compliance

- Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien aber auch freiwilligen Kodizes in Unternehmen **für den Bereich der Informationstechnologie** von Unternehmen/Organisationen
- Proaktive Vermeidung von Regelverstößen durch Sicherheits- und Risikomanagement der IT

- Compliance ist **NICHT** primär eine Frage von Ethik und Moral!

com·pli·ance [kəm'plaɪəns] *s.*
1. Einwilligung f, Erfüllung f; Befolgung f (with gen.): in compliance with gemäß;
2. Willfährigkeit f.

IT-Compliance

Compliance *von* IT

- Die im Unternehmen eingesetzten IT-Systeme müssen den Gesetzen, Richtlinien und anderen Verhaltensmaßregeln genügen, die für die Einrichtung und den Betrieb solcher Systeme gelten.

Compliance *durch* IT

- Viele Unternehmensfunktionen, für die Compliance-Anforderungen gelten, werden mit IT-Systemen abgebildet (z. B. Buchhaltung, Rechnungslegung, Aufbewahrungspflichten von Unterlagen).
- Mittelbare Compliance-Anforderungen nehmen stark zu, wie z. B. die Unverfälschbarkeit und die Revisionssicherheit von elektronischen Dokumenten, geordneter Archivierung (aus AO und konkretisiert durch GoBS und GdPDU) usw.

IT-Compliance

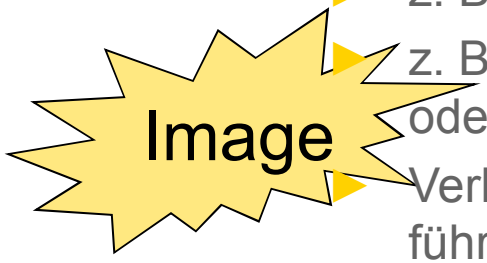
Warum eigentlich IT-Compliance?

- Persönliche Verantwortung der Geschäftsführungsorgane für gesetzeskonformes Verhalten des Unternehmens
  - Verantwortlichkeit und Haftungsrisiko von Geschäftsführungsorganen hat zugenommen, Beispiele sind:
    - KonTraG, 1998 (§ 91 Abs. 2 AktG: Einrichtung eines Risikomanagementsystems)
    - Corporate Governance Kodex und strengere Rechtssprechung
  - Schadensersatzpflicht nach § 93 Abs. 2 S. 2 AktG, § 43 GmbHG
  - § 91 Abs. 2 AktG: Pflicht der Unternehmensleitung, „geeignete Maßnahmen“ zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden
    - Querschnittsnorm, die allgemeine Pflichten einer Geschäftsleitung spezifiziert
    - Unternehmensleitung muss prüfen, ob ein mangelhaftes **IT-System** dem Unternehmen erhebliche wirtschaftliche Schäden zufügen kann, einschließlich Identifizierung „unternehmenskritischer Systeme“ (ERP, Risikomanagement)

IT-Compliance

Warum eigentlich IT-Compliance? (ff.)

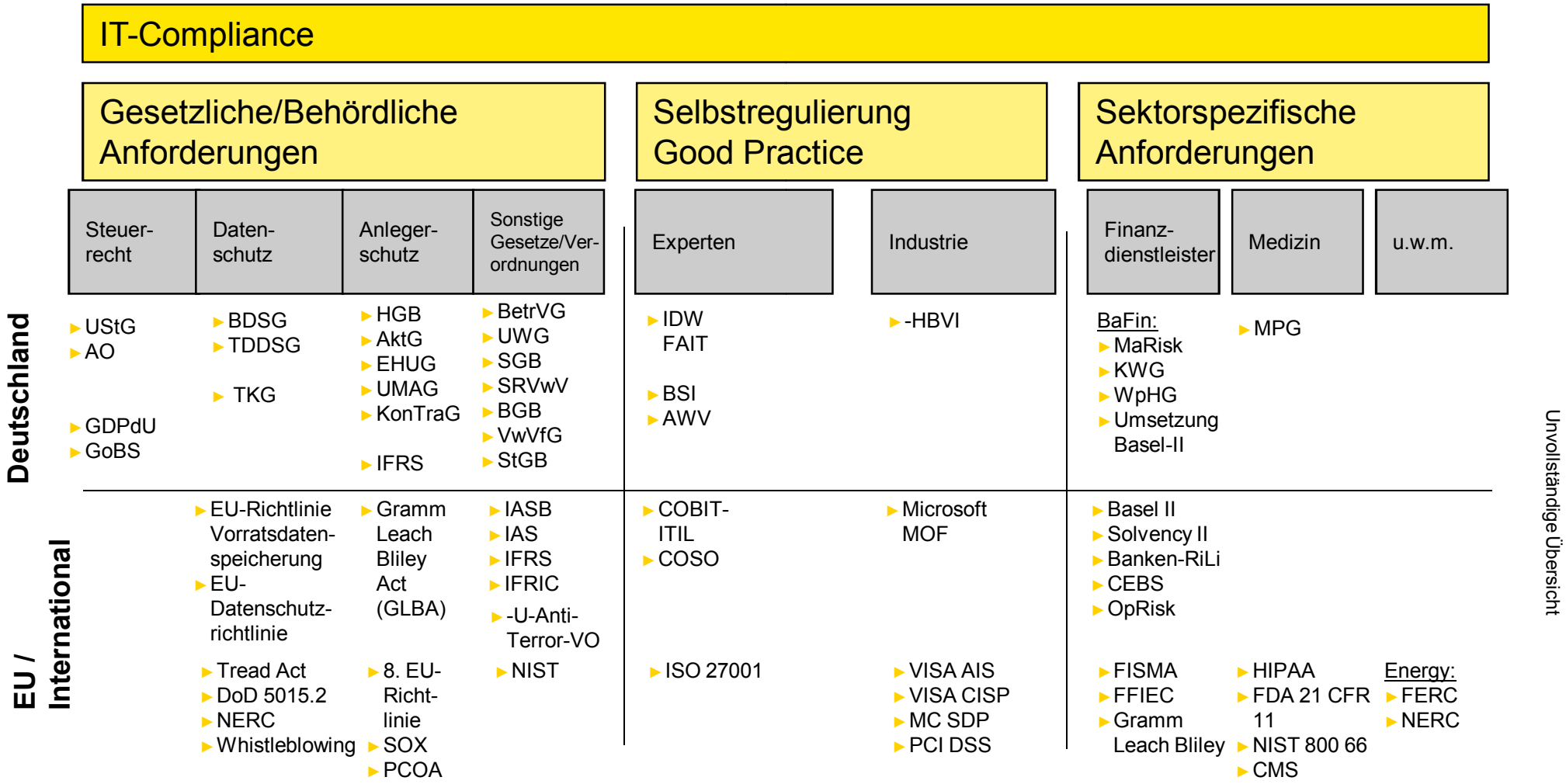
- Ausschluss von der Vergabe öffentlicher Aufträge
  - IT-Standards und entsprechende Zertifizierungen werden immer öfter als Wertungskriterien und Vertragsbestandteile verwendet; faktische Bindungswirkung für den Bieter (ITIL, COBIT)
- Wirtschaftsprüfertestat wird versagt
- Gesetzliche und vertragliche Obliegenheit
  - Nicht selbständig einklagbar, sondern bloße Verhaltensnorm, die bei Nichtbeachtung zum Rechtsverlust führen kann (§ 254 BGB)
    - Relevant im Versicherungsvertragsrecht/VVG
      - z. B. Pflicht, bedeutende Umstände anzuzeigen, § 16 VVG
      - z. B. Pflicht, keine Gefahrerhöhung nach Vertragsschluss vorzunehmen oder diese zuzulassen, Anzeigepflicht § 23 VVG
      - Verletzung von Obliegenheit kann zu Verlust von Versicherungsschutz führen



Agenda

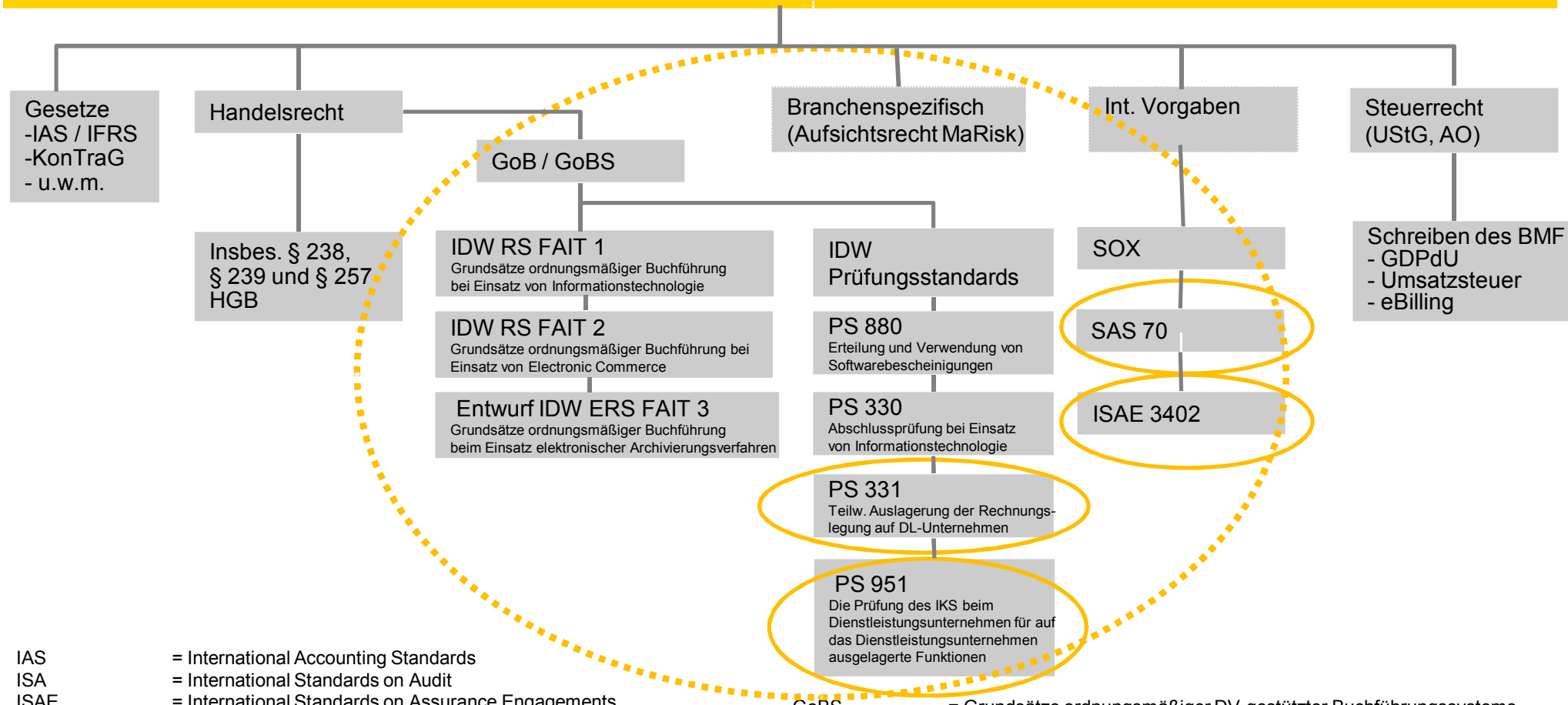
- IT-Compliance
- **Aktuelle nationale und internationale Standards**
- IT-Compliance und IT-Revision

Aktuelle nationale und internationale Standards



Aktuelle nationale und internationale Standards

Gesetzliche Rahmenbedingungen und Verlautbarungen



IAS	= International Accounting Standards
ISA	= International Standards on Audit
ISAE	= International Standards on Assurance Engagements
IFRS	= International Financial Reporting Standards
FAIT	= Fachausschuss für Informationstechnologie
GDPdU	= Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GoB	= Grundsätze ordnungsmäßiger Buchführung
GoBS	= Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme
HGB	= Handelsgesetzbuch
IdW	= Institut der Wirtschaftsprüfer
PS	= Prüfungsstandard
RS	= Stellungnahme zur Rechnungslegung

IDW PS 331 „Abschlussprüfung bei tlw. Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen“

- **Aktueller Stand 9. September 2010**
- **Neu TZ 26a**
- **Externe Dienstleister**
  - Sofern für das Rechnungswesen Informationstechnologie eingesetzt wird und diese ausgelagert wurde, ist grundsätzlich eine Prüfung und Beurteilung des rechnungslegungsbezogenen IT-Kontrollsystems des Dienstleistungsunternehmens notwendig.
  - Führt die Beurteilung zu dem Ergebnis, dass die Tätigkeit des Dienstleistungsunternehmens für das zu prüfende Unternehmen wichtig und für die Abschlussprüfung von Bedeutung ist, hat der Abschlussprüfer ausreichende Informationen einzuholen, um ein Verständnis für das interne Kontrollsystem des Dienstleistungsunternehmens zu entwickeln, um das Kontrollrisiko beurteilen zu können.
    - Externe Prüfungsberichte (Beschreibung und Beurteilung der Kontrollen)
    - Prüfung vor Ort (Prüfungsrecht!)

PS 951 „Die Prüfung des IKS beim Dienstleistungsunternehmen…“

IDW PS 591 „Prüfung des IKS beim Dienstleistungsuntern. für auf das Dienstleistungsunternehmen ausgelagerte Funktionen“

Das IDW formulierte den Prüfungsstandard IDW PS 951, um einen deutschen Standard zur Berichterstattung bezüglich des dienstleistungsbezogenen internen Kontrollsystems zu schaffen. (aktueller Stand 9. September 2010)

Sinn und Zweck:

- Unternehmen erbringt Dienstleistungen für Kunden;
- Eine Prüfung des rechnungslegungsbezogenen, an das Unternehmen ausgelagerten IKS ist für die Abschlussprüfer dieser Kunden notwendig;
- Der Abschlussprüfer des Kunden ist dabei angehalten Informationen zu Art, Umfang und Zeitbezug der Prüfungshandlungen auszuwerten, bevor er sich auf die Prüfungs-ergebnisse Dritter verlässt.

Bescheinigung **Typ A**: Prüfungsurteil zur Darstellung und Angemessenheit IKS

Bescheinigung **Typ B**: darüber hinaus ein Urteil zur Wirksamkeit des IKS

SAS 70 / ISAE 3402

- SAS 70 US Standard zur Kommunikation zwischen Prüfern
  - Beschreibung des IKS
  - Type 1 und Type 2

- The International Accounting and Auditing Standards Board (IAASB) of the International Federation of Accounting entwickelte den ISAE 3402 (International Standards on Assurance Engagements)

  - Release in Dezember 2009
  - Effektiv für Abschlüsse ab dem 15. Juni 2011

Agenda

- IT-Compliance
- Aktuelle nationale und internationale Standards
- **IT-Compliance und IT-Revision**

IT-Compliance und IT-Revision

Funktion der IT-Revision

- Die **IT-Revision als Teil der Internen Revision** unterstützt Sie bei der Überprüfung sämtlicher IT-Aspekte einer Unternehmung. Sie untersucht gezielt, ob die Grundsätze von Sicherheit und Ordnungsmäßigkeit sowie von Wirtschaftlichkeit und Zweckmäßigkeit beachtet werden.

Aufgaben der IT-Revision

- Die Prüfungstätigkeit der IT-Revision hat sich auf **alle Betriebs- und Geschäftsabläufe** der Gesellschaft zu erstrecken. Dabei sind **Umfang** und **Risikogehalt** der Betriebs- bzw. Geschäftstätigkeit zu berücksichtigen.
- Die Interne Revision erbringt unabhängige und objektive Prüfungs- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese zu verbessern hilft.

IT-Compliance und IT-Revision

- **Eine funktionsfähige IT-Revision unterstützt die Ziele der IT-Governance**
  - Nachweis der Wirksamkeit der Umsetzung der Unternehmensstrategie im Bereich der IT
  - Prüfung aller Elemente des IT-Systems
- **Die Funktionsfähigkeit der IT-Revision muss sichergestellt sein**
  - Nachweis über Qualitätssicherungs- und -verbesserungsmaßnahmen
  - Einhalten von **Good Practice-Empfehlungen** der Revisionsverbände
  - Bestätigung für externe Adressaten des Unternehmens

IT-Compliance und die Revision in der Zukunft

Zunehmendes Interesse des Top-Managements an der Arbeit und den Ergebnissen der IR

Interne Revision (heute)

1. Ausrichtung der Prüfungstätigkeit auf die aktuelle Risikosituation des Unternehmens
2. Unternehmerisches Denken
3. Wandlung weg vom Disziplinierungsinstrument hin zum Anbieter interner Informationen
4. Interne Revision als Teil der Wertschöpfungskette (Inhouse Consultant)

Interne Revision (zukünftig)

Ihr Ansprechpartner für Fragen und Anmerkungen

Karin Thelemann
Partnerin, Advisory, Financial Services

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft
Mergenthalerallee 3 - 5
65760 Eschborn
Telefon +49 6196 996 26488
Fax +49 6196 8024 26488
Mobil: +49 160 939 26488
Karin.Thelemann@de.ey.com

Herzlichen Dank
für Ihr Interesse!

ERNST & YOUNG
Quality In Everything We Do

Ernst & Young

Assurance | Tax | Transactions | Advisory

Die internationale Ernst & Young-Organisation im Überblick
Die internationale Ernst & Young-Organisation ist einer der Marktführer in der Wirtschaftsprüfung, Steuerberatung und Transaktionsberatung sowie in den Advisory Services. Rund 144.000 Mitarbeiter sind durch gemeinsame Werte und einen hohen Qualitätsanspruch verbunden. Das Ziel von Ernst & Young ist es, das Potenzial seiner Mitarbeiter und Mandanten zu erkennen und zu entfalten.

Die internationale Ernst & Young-Organisation besteht aus den Mitgliedsunternehmen von Ernst & Young Global Limited (EYG). Jedes EYG-Mitgliedsunternehmen ist rechtlich selbständig 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 Mandanten. Weitere Informationen finden Sie unter www.de.ey.com

In Deutschland ist Ernst & Young mit rund 7.100 Mitarbeitern an 22 Standorten präsent. „Ernst & Young“ und „wir“ beziehen sich in dieser Präsentation auf alle deutschen Mitgliedsunternehmen von Ernst & Young Global Limited.