

# COMPLIANCE

Dr. Christof Müller

- Einleitung
- Begriffserklärung und Grundlagendefinition „Compliance & Ethics“
- Strategie und Unternehmensführung & der Stellenwert von Compliance
- Tone from the Top – Bedeutung in der Praxis
- Grundsätze eines Compliance Management Systems (CMS)
- Welche Chancen bietet Compliance für ein Unternehmen?
- Rechtliche Grundlagen & Standards

COMPLIANCE FIRST!

# EINLEITUNG

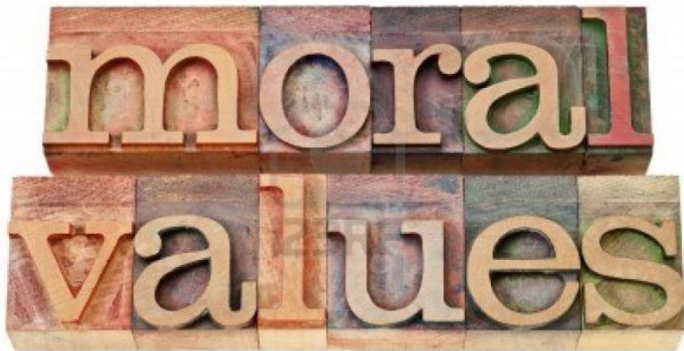
Warum stehlen Sie nicht im Supermarkt?

# EFFIZIENTES COMPLIANCE-PROGRAMM

## COMPLIANCE FIRST!

Was ist Compliance?

Eine Definition: Die Gesamtheit aller Maßnahmen in einem Unternehmen, um rechtmäßiges Verhalten der mit dem Unternehmen in Zusammenhang stehenden Personen zu gewährleisten.



# EFFIZIENTES COMPLIANCE-PROGRAMM

## COMPLIANCE FIRST!

Seit wann gibt es Compliance?

5. Mose, 16,19:

Du sollst das Recht nicht beugen,  
die Person nicht ansehen und  
kein Bestechungsgeschenk annehmen,  
denn Bestechung macht weise Leute blind  
und verdreht die Worte der Gerechten.



# EFFIZIENTES COMPLIANCE-PROGRAMM

## COMPLIANCE FIRST!

Was sind die (wechselwirkenden) **Grundsätze** eines Compliance Management Systems (CMS)?

**Kultur** --- tone from the top

**Ziele** --- Festlegung auf Grundlage der allgemeinen Unternehmensziele

**Organisation** --- Bestimmung der Struktur und der Verantwortlichkeiten

**Risiken** --- Identifikation und Einführung systematischer Verfahren

**Programm** --- Grundsätze & Maßnahmen zur Begrenzung/Vermeidung von Risiken und Verstößen

**Kommunikation** --- Information der Mitarbeiter und Festlegung der Berichtswege

**Monitoring** --- Überwachung, Dokumentation, Berichterstattung und Verbesserung

## COMPLIANCE FIRST!

Welche Chancen bietet Compliance?

- ✓ Vermeidung und Prävention von Straftaten und Fehlverhalten in der Organisation
- ✓ Rechtssicherheit für das Unternehmen und Handlungsorientierung für die Mitarbeiter
- ✓ Erwerb und Erhalt einer Reputation für Vertrauenswürdigkeit, Stabilität und Integrität
- ✓ Sicherung der Geschäftstätigkeit und des Vertrauens von Geschäftspartnern
- ✓ Wettbewerbsvorteil
- ✓ Wesentlicher Beitrag zur Organisationskultur

*...oder: „If you think compliance is expensive, try non-compliance.“*

# RECHTLICHE GRUNDLAGEN

Besteht in Österreich eine Verpflichtung  
zur Einführung von Compliance-Systemen?



## COMPLIANCE & RECHT

Die Beantwortung der Frage, ob eine **Verpflichtung zur Einführung** eines CMS besteht, hängt grundsätzlich vom Gesichtspunkt und von der Definition des Begriffes „Compliance“ ab.

Der **Spannungsbogen** reicht dabei von der Einhaltung der gesetzlichen Regelungen bis zur sozialen Verantwortlichkeit eines Unternehmens.

Zu den wichtigsten **internationalen Compliance-Regeln & Standards** zählen:

- Sarbanes-Oxley Act (SOX), Foreign Corrupt Practises Act (FCPA), USA
- UK Bribery Act 2010, Australian Standard on Compliance Programs
- ICC-Kodex, OECD-Leitfaden, IDW PS 980

## COMPLIANCE & RECHT

### Zur Situation in Österreich

Es gibt weder eine Legaldefinition des Begriffes „Compliance“ noch branchenübergreifende Regelwerke, die den Begriff verwenden. Auch in der Judikatur gibt es noch keine richtungsweisenden Entscheidungen.

Das Interesse von Vorstand/Geschäftsführung, eine Compliance-Organisation einzurichten, wird sich jedoch auch aus folgenden **Haftungsnormen** ableiten.

## COMPLIANCE & RECHT

### Zur Situation in Österreich

- § 82 AktG und § 22 Abs 1 GmbHG → „Dafür Sorge tragen, dass ein Rechnungswesen und ein internes Kontrollsystem geführt werden, entsprechend den Anforderungen des Unternehmens.“
- Verbandsverantwortlichkeitsgesetz (VbVG) → strafrechtliche Verantwortlichkeit von juristischen Personen und anderen Verbänden für Straftaten ihrer Entscheidungsträger und sonstigen Mitarbeiter. Aufsichtsversagen der Entscheidungsträger - § 3 VbVG?

## COMPLIANCE & RECHT

### Zur Situation in Österreich

- Österreichischer Corporate Governance Kodex → Dieser ist ein Ordnungsrahmen für österr. Aktiengesellschaften als wirksames Instrument zur Förderung des Vertrauens und damit ein Maßstab für gute Unternehmensführung und Unternehmenskontrolle am Kapitalmarkt → [www.corporate-governance.at](http://www.corporate-governance.at)
- Arbeitsrecht und Datenschutzrecht
- Strafrecht (u.a. §§ 304-309 StGB, § 153(a) StGB)

- 
- Compliance, IKS und Risikomanagement
- Risikoidentifikation und Risikobewertung
- Elemente eines Compliance-Programms im Überblick
- Der Verhaltenskodex und seine Bedeutung in der Praxis
- Geschenke & Einladungen Oder: Anti-Korruption&Bestechung

# Compliance, IKS und Risikomanagement

Grundsätze eines ordnungsgemäßen IKS

## ADRESSATENKREIS

→ Gesamtes Personal

- IKS betrifft ALLE Bereiche und ALLE Mitarbeiter im Unternehmen
- Interne Kontrollen (IK) hat es immer schon gegeben
- In vielen Bereichen fehlt nur noch das „S“ des IKS – die Systematik
- IKS bedeutet nicht, dass Vertrauen der Organisation in Mitarbeiter fehlt
- IKS soll vielmehr die Zielerreichung der Organisation unterstützen und Risiken in akzeptablen bzw. vordefinierten Grenzen zu halten

# EFFIZIENTES COMPLIANCE-PROGRAMM

## ZIELE DER POLICY

- Bereitstellung von Grundlagen für bestmögliche Erstellung von Prozessen in Bezug auf Kontrollen
- Unterstützung der Unternehmensfunktionen bei der Erreichung der internen Kontrollziele
- Aufbau und Weiterentwicklung eines Kontrollverständnisses
- **Interne Kontrolle wird direkt von allen Mitarbeitern bei der Ausführung ihrer tagtäglichen Arbeit wahrgenommen**
  
- Kontrollen sind
  - ein wirksamer und zuverlässiger Schutz vor Risiken bzw. Minimierung von Risiken
  - Bestandteil jedes Geschäftsprozesses
  - Verantwortung der Leiter der Organisationseinheiten (OE) / Führungskräfte
- Festlegung von Kontrollmechanismen für Prozesse in eigener OE und deren Durchführung gehört zur Aufgabe von Führungskräften
- Kontroll- und Risikomanagementmechanismen sollen wirksam, effizient und einwandfrei sein
- Ziel ist, das erwünschte Verhalten bzw. die erwünschten Ergebnisse des Prozesses zu erreichen



## DAS INTERNE KONTROLLSYSTEM (IKS)

- **Aufgabe des IKS** = Sicherstellung, dass
  - Geschäftsaktivitäten geltendem Recht sowie Vorschriften und Anordnungen entsprechen und
  - Geschäftsprozesse in Bezug auf ihre Ziele effizient und wirksam sind und
  - Rechnungslegungs- und Managementinformationen zuverlässig und vollständig sind.
- **Interne Kontrolle (IK)** = Instrumente, die dem Unternehmen dienen, seine Ziele zu erreichen (Geschäfts-, Finanzberichterstattungs- und Compliance-Ziele), wobei sich Bedeutung und Gestaltung von internen Kontrollen an identifiziertem Risiko und betrachtetem Prozess orientiert.
- **Kontrollumfeld** = wesentlicher Faktor, der zeigt, welche Bedeutung den internen Kontrollen beigemessen wird und wie sensibel das Personal der Notwendigkeit von Kontrolle gegenübersteht (Integrität, Werte).
- **Kontrollverständnis („Kontrollkultur“)** = den Mitarbeitern sind Wichtigkeit, Nutzen und Mehrwert der internen Kontrollen sowie die eigenen Aufgaben und Verantwortungen bewusst (Einbindung der Mitarbeiter in die auszuführenden Kontrollen).
- Aufgabenverständnis und Verantwortungsbewusstsein basiert auf Kenntnis, Befugnissen und Berichtswegen.

# EFFIZIENTES COMPLIANCE-PROGRAMM

## DIE WIRKSAMKEIT DES IKS

- **Wirksamkeit der Kontrollen** wird garantiert durch:
  - Überwachungs- und Kontrollaktivitäten
  - Berichtswege zur Meldung von Verstößen gegen Ethik Kodex
  - Berichtswege zur Meldung von (vermuteten) Fraud Fällen
- Festigung des Kontrollverständnisses auch durch das Bonifikationssystem
- Kontrollmechanismen sind in erster Linie im Interesse von Leitern der OEs
- IKS schließt alle Mitarbeiter in Kontrollaktivitäten ein

## GLIEDERUNG DES IKS

- **1st Level Kontrollen**  
**Kontrollen, die Aufgabe der OEs sind**  
Diese sind Bestandteil jedes Organisationsprozesses und Fundament des IKS
- **2nd Level Kontrollen**  
**Kontrollen, die von eigenen „Kontrollfunktionen“ durchgeführt werden**  
z. B. Risikomanagement-Funktion, Compliance-Funktion, Controlling, Fraud-Präventionsfunktion, andere notwendige Überwachungsfunktionen
- **3rd Level Kontrollen**  
**Interne Revision** bewertet unabhängig und objektiv die Qualität und die Wirksamkeit des IKS

# EFFIZIENTES COMPLIANCE-PROGRAMM

## VON ORGANISATIONSEINHEITEN DURCHGEFÜHRTE KONTROLLEN – KLASSIFIZIERUNG (I)

### VORBEUGENDE KONTROLLEN VERSUS AUFDECKENDE KONTROLLEN

- System muss gesamthaft hieb- und stichfest sein
- Aufdeckende Kontrollen müssen dort ausgeführt werden, wo Unregelmäßigkeiten durch das Netzwerk vorbeugender Kontrollen schlüpfen können
- Intensität und Ausmaß aufdeckender Kontrollen sind abhängig von der Wirksamkeit vorbeugender Kontrollen
- Je größer das abzuschwächende Risiko, desto wichtiger sind vorbeugende Kontrollen
- Kontrollaktivitäten müssen laufend gewährleistet werden
- Je komplexer und weniger standardisiert ein Prozess ist, desto konzentrierter müssen die Kontrollen sein

## VON ORGANISATIONSEINHEITEN DURCHGEFÜHRTE KONTROLLEN – KLASSIFIZIERUNG (II)

- Die Wirksamkeit eines IKS ist unabhängig von der Anzahl der Kontrollen, wichtiger sind: **Effizienz und Zusammenspiel!**
- Kontrollen verursachen Kosten (z. B. verwendete Ressourcen, Systeme)
- Ziel = Einrichtung notwendiger Kontrollen (Schlüsselkontrollen)

### **SCHLÜSSELKONTROLLEN**

Kontrollen, die ein größtes Maß an Gewissheit und Nachweis liefern, dass der gesamte (Teil)-Prozess richtig funktioniert.

- Eine gut konzipierte Schlüsselkontrolle kann eventuell mehrere Kontrollen anderer Art ersetzen
- Schlüsselkontrollen führen zu verbesserter Effizienz und Wirksamkeit

## VON ORGANISATIONSEINHEITEN DURCHGEFÜHRTE KONTROLLEN – KLASSIFIZIERUNG (III)

### **AUTOMATISCHE KONTROLLEN VERSUS MANUELLE KONTROLLEN**

- Die Wahl der Kontrolle ist abhängig von organisatorischen und geschäftsspezifischen Faktoren
- Automatische Kontrollen:
  - Zur Erhöhung von Effizienz und Verlässlichkeit
  - In Hinblick auf Vereinfachung und Wirtschaftlichkeit
  - Bei großer Anzahl sich wiederholender Transaktionen
  - Wenn ein Prozess anfällig für Versuche von Unterschlagung oder Veruntreuung ist
  - Wo menschliches Ermessen und Einschreiten in geringem Grad verlangt wird

### **NACHVOLLZIEHBARKEIT SICHERSTELLEN**

- Nachvollziehbarkeit bedeutet: Ein Dritter ist in der Lage, die Kontrolle zurückzuverfolgen und die korrekte Ausführung zu prüfen
- Der Nachweis der durchgeführten Kontrollen ist zu behalten, Dokumente sind zu kennzeichnen (paraphieren) und Kontrolllisten sind aufbewahren
- Für Entscheidungsfindungsprozesse sind Aktennotizen anzufertigen, aus denen entscheidungsrelevante Elemente hervorgehen

## KONTROLLMECHANISMEN

### **Organisatorische Kontrollmechanismen (in der Aufbauorganisation)**

- Im Zusammenhang mit Struktur
- Angemessene organisatorische Konzipierung soll ordnungsgemäße Ausführung der Geschäftstätigkeit sicherstellen und vor Hauptrisiken schützen.
- Verantwortlich: wer mit Konzipierung der Organisationsstruktur betraut ist

### **Operationale Kontrollmechanismen (in der Ablauforganisation)**

- Zur Vermeidung von Risiken und Verlusten aus Störungen und Fehlfunktionen von Prozessen, aus menschlichem Versagen oder Systemfehlern
- Verantwortlich: wer den (Teil)-Prozess ausführt

# EFFIZIENTES COMPLIANCE-PROGRAMM

## ORGANISATORISCHE KONTROLLMECHANISMEN IN DER AUFBAUORGANISATION

- Wesentliche Anforderung: wesentliche Unternehmensaktivitäten dürfen nicht in einer Funktion bzw. von einer Person ausgeführt werden
- Damit: Risikoverringung durch Einbeziehung größerer Anzahl von Mitarbeitern
- Erforderlich: Ordnungsgemäße Organisation von Prozessen und Geschäftstätigkeiten bzw. ordnungsgemäße Zuteilung von Aufgaben und Verantwortungen:
  - Funktionstrennung (zwischen OEs)
  - Arbeitsteilung (innerhalb OEs)
  - Befugnis- und Ermächtigungssystem (organisatorische Aspekte)
  - System unternehmensinterner Regeln und Vorschriften (organisatorische Aspekte)
  - Einrichtung spezifischer Kontrollfunktionen oder Kontrolleinheiten

## OPERATIONALE KONTROLLMECHANISMEN IN DER ABLAUFORGANISATION

- Vorhandensein unternehmensinterner Regeln und Vorschriften, z. B. Handbücher, Arbeitsanleitungen, Rundschreiben, Leitlinien
- Prozessbezogene Kontrollaktivitäten, z. B. Stichproben
- „Gebarenskontrolle“, z.B. Feedback, Personalmanagement



# EFFIZIENTES COMPLIANCE-PROGRAMM

## AUFBAU- UND ABLAUFORGANISATION MÜSSEN ZUSAMMENPASSEN

- Aufbauorganisation – Organigramme aus HR
  - Aktuell
  - Klare Zuständigkeiten, Kompetenzen und Transparenz
  - Dokumentation disziplinierte/fachliche Führung
- Ablauforganisation (z. B. Dokumentation, IT-Systeme)
  - Modellierte Prozesse bzw. Dokumentationen müssen der IST-Situation gemäß Kompetenzen laut Aufbauorganisation entsprechen
  - Vollständige Abbildung der Prozesse inklusive Kontrollen
  - Transparenz zu den Schnittstellen