-Risiken und Lösungen im Netzwerk -

IT Security Checks und deren Relevanz bezüglich KonTraG, Basel II und ISO 9000:

Haftungsrisiken für EDV Leiter und Geschäftsführer

Referent:

Michael T. Wilczynska

Gliederung

- Einleitung
- Rechtliche Hintergründe und Normen
  - KonTraG
  - Basel II
  - ISO 9000
- Problemstellung
  - Gefahrenpotentiale
  - Haftungsrisiken für EDV- und Geschäftsleitung
- Lösung
  - Risikoanalyse und Risikomanagementsystem
- Fazit
- Zusammenfassung

Einleitung

Wichtige Hinweise für Beiträge mit juristischem Bezug:

Sowohl Referent als auch Provendo-Systems GmbH übernehmen keine Haftung für den Inhalt der rechtlichen Aspekte, insbesondere im Hinblick auf Richtigkeit, Aktualität und Vollständigkeit der zur Verfügung gestellten Informationen. Das Geltendmachen von Ansprüchen jeglicher Art ist ausgeschlossen.

Dieser Vortrag dient der allg. Bildung und Weiterbildung und nicht der Beratung im Falle eines individuellen rechtlichen Anliegens!

KonTraG

- bereits am 5. März 1998 vom Dt. Bundestag verabschiedet
- präzisiert und erweitert hauptsächlich HGB und AktG
- erweitert Haftung für Vorstand, Aufsichtsrat und Wirtschaftsprüfer
- Kern: Vorschrift, die Unternehmensleitungen zwingt ein unternehmensweites Früherkennungssystem für Risiken einzuführen u. zu betreiben

  - z.B. Auszug aus § 91, II AktG: {...} Vorschrift, nach der der Vorstand verpflichtet wird „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“.

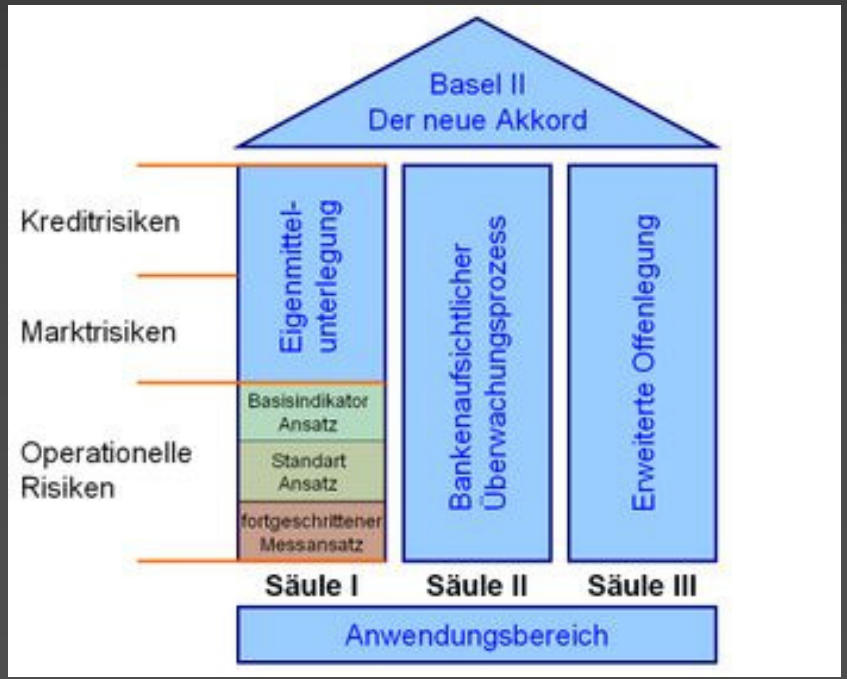
  - betrifft neben der **AG** auch **KGaA, GmbH** und hinsichtlich der Rechtsprechung zu Verantwortungsbereichen auch die KMUs

  - **Basel II**: zwingt Banken zum Rating und krit. Überprüfung der Einrichtung und des Betriebs eines **Risikomanagementsystems**

Referent: Michael T. Wilczynska

Basel II (1)

- Gesamtheit der EK-Vorschriften vom Baseler Ausschuss f. Bankenaufsicht
- Inkrafttreten innerhalb der Europ. Union Ende 2006
- Ziel: Sicherung EK-Ausstattung d. Banken + vereinheitl. Wettbewerbsbeding.
- Umsetzung in dt. Recht insbesondere über MaRisk in Bsl II Säule Nr. 2: „Bankaufsichtlicher Überprüfungsprozess“



Referent: Michael T. Wilczynska

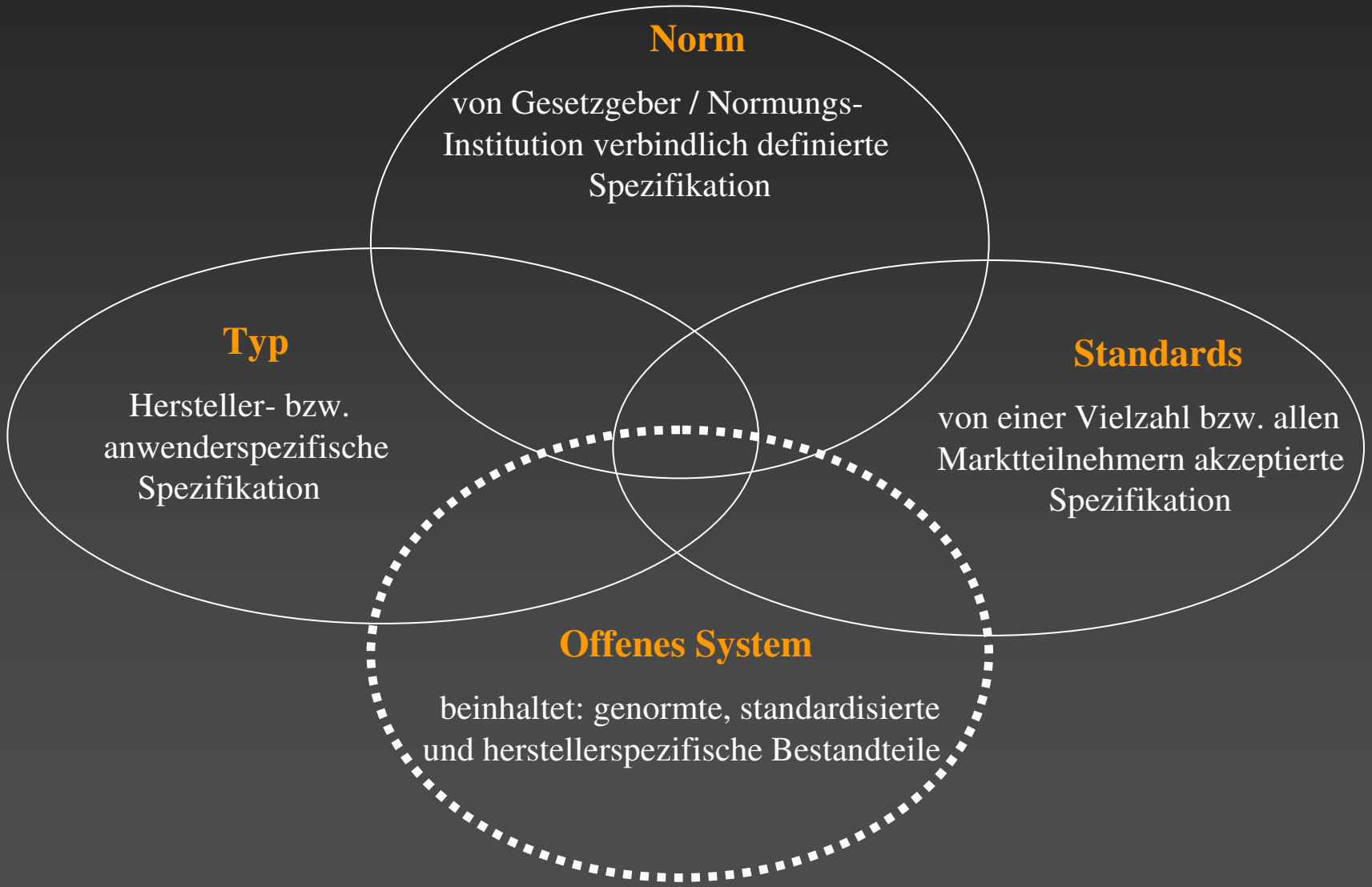
Basel II (2)

- NEU: Einbezug weiterer Risiken neben Marktpreisrisiko und Kreditrisiko: operationelle Risiken !!!

= Risiko direkter oder indirekter Verluste infolge **unzulänglicher oder ausfallender** interner **Verfahren, Mitarbeiter** und **Systeme**, oder infolge bankexterner Ereignisse

- Generell gilt: höhere Risiken - höhere Zinsen
- Einigung des Baseler Ausschusses: geringere EK-Unterlegung bei KMU; dennoch oft fehlende Vorbereitung auf Basel II (erforderliche Geschäftsprozesse und Dokumente)

Normen + Standards



ISO 9000

- normiert QM mittels Qualitätssicherungsnormen (inkl. ISO 9000 – 9004)
- beschreibt Anforderungen an Unternehmensleitung, um best. Anforderungen an QM zu entsprechen
- zur informativen unternehmensinternen Umsetzung oder Nachweis gegenüber Dritten
- beschreibt prozessorientierten QM Ansatz basierend auf 4 Hauptprozessen

1. Verantwortung der Leitung
2. Management von Ressourcen
3. Produktrealisierung
4. Messung, Analyse und Verbesserung

Referent: Michael T. Wilczynska

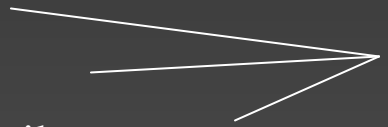
Problemstellung

Problem:

- Gefahrenpotentiale
- Haftungsrisiken für EDV- und Geschäftsleitung

Auftrag:

- Risikoanalyse
- Risikomanagement
- Minimieren der Haftungsrisiken



IT Sicherheit

Haftungsrisiken (1)

- Geschäftsführer: Grundsätze zur Arbeitnehmerhaftung regelmäßig nicht anwendbar
  - Grund: Sie sind Organe der Gesellschaft, nicht deren Angestellte
  - Tragen Verantwortung über Koordination u. Einsatz der Unt.-Ressourcen
    - Erfordert Verfolgung des gesellschaftl. Zwecks
    - Unterlassen aller Aktivitäten, die diesen Zweck vereiteln können
    - Überwachen der Mitarbeiter, die mit Durchführung der Aufgaben betraut
  - Sorgfalt eines ordentlichen Geschäftsmanns ist anzuwenden
- Mangelnder/unzureichender Katastrophenschutz durch EDV-Leiter:
  - Überarbeitungs- und Wartungspflichten für Katastrophenplan und Datensicherungskonzepte
  - Verantwortung für Ergreifung u. Aktualisierung von Schutzmaßnahmen gegen Schadsoftware (Viren, Trojaner, Würmer, Spyware, ...)
  - Verantwortung über Aufklärung der Mitarbeiter des Unternehmens

Haftungsrisiken (2)

Schutz des EDV-Leiters / Geschäftsführers vor möglicher Haftung:

- ✓ gewissenhafte Wahrnehmung der übertragenen Aufgaben
- ✓ informieren der Geschäftsleitung über mögl. Risiken
- ✓ Lösungsvorschläge für DV-Sicherheitsmängel erarbeiten und umsetzen
- ✓ Verweis auf Expertise eines qualifizierten Beraters möglich

Im Falle der Ablehnung der Lösungsvorschläge durch höhere Instanzen:

1. die Risiken erneut aufzeigen und das eigene Vorgehen protokollieren
2. eine schriftliche Ablehnung seiner Vorschläge verlangen
3. eine weitere Verantwortung ablehnen
4, in Form eines „ceterum censeo" auf die Gefahren hinweisen

Haftungsrisiken (3)

IT Sicherheit oft vernachlässigt trotz Schaden durch Datenverlust, Spionage, Imagebeeinträchtigung und strafrechtlicher Verantwortlichkeit der Geschäftsleitung:

Problem	Haftungsrisiko	Strafrahmen
Firewall unzureichend administriert; E-Mails nicht ausreichend verschlüsselt; CERT-Advisories nicht gelesen;	§ 17 UWG Verrat v. Betriebsgeheimnissen; § 203 StGB Verrat v. Amts-/Berufsgeheimn. § 43 BDSG Verstoß ggn. Datenschutzgesetz	3 Jahre 1 Jahr 1 Jahr
Mitarbeiter dürfen ohne Richtlinien eigene Software installieren, schleppen Viren oder Trojaner ein	§ 43 BDSG	1 Jahr
Mitarbeiter sendet strafbare Inhalte	§ 184, I StGB Verbreitung v. Pornographie § 86 StGB Verbreitung v. Propaganda verfassungswidriger Organisationen	1 – 5 Jahre
Mitarbeiter bricht in fremde Unternehmensnetze ein, installiert Trojaner, schießt Rechner ab	§ 202a StGB Ausspähen von Daten § 303a StGB Datenveränderung § 303b StGB Datensabotage	3 Jahre 2 Jahre 5 Jahre

Haftungsrisiken (4)

IT Sicherheit oft vernachlässigt trotz Schaden durch Datenverlust, Spionage, Imagebeeinträchtigung und strafrechtlicher Verantwortlichkeit der Geschäftsleitung:

Problem	Haftungsrisiko	Strafrahmen
Aufbewahrung v. Logfiles über Nutzung v. Telediensten nach Nutzungs-/Abrechnungsende	§ 43 BDSG	1 Jahr
Private Telefongespräche werden ohne besondere Vereinbarung kontrolliert	§ 43 BDSG § 206 StGB	1 Jahr 5 Jahre
Mitarbeiter nutzt kostenpflichtige Seiten kostenlos mit geknackten Passworten	§ 263a StGB Computerbetrug	5 Jahre
Private Mails von Mitarbeitern werden gelesen	§ 206 StGB § 202a StGB Ausspähen von Daten	5 Jahre 3 Jahre

Risikoanalyse

Stufenkonzept:

Risikoidentifizierung

Risikoanalyse

Stufenkonzept:

Risikoidentifizierung

Risikobewertung

Referent: Michael T. Wilczynska

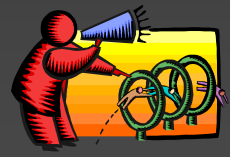
Risikoanalyse

Stufenkonzept:

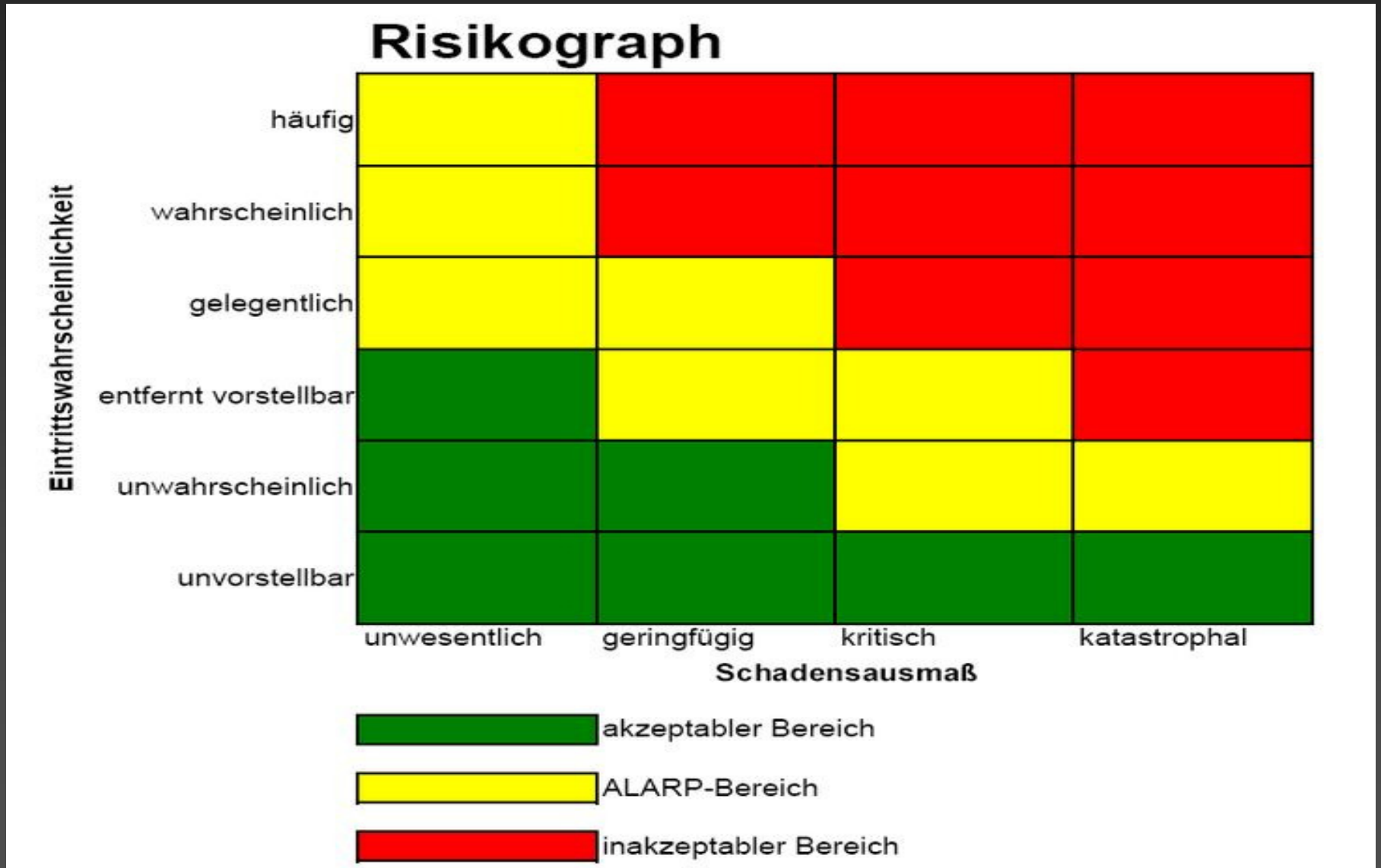
Risikoidentifizierung

Risikobewertung

Risikomanagement



Risikobewertung



Risikomanagement

Risikomanagement Systematik umfasst:

- Festlegungen von Zielen auf Basis der Organisationsstrategie
- Definition von Werttreibern oder krit. Erfolgsfaktoren zur Zielerreichung
- Festlegung einer Risikomanagement-Strategie
- Identifikation von Risiken (im Finanzrisikomanagement mit „Exposure-Ermittlung" bezeichnet)
- Bewertung/Messung von Risiken
- Bewältigung von Risiken
- Steuerung
- Monitoring zur Früherkennung

Fazit

- weitest möglicher Schutz gegen haftungsrechtliche Inanspruchnahme

Zusammenfassung

- ✓ Rechtliche Hintergründe
- ✓ Haftungsrisiken für EDV- und Geschäftsleitung
- ✓ Risikoanalyse und -management

➢ Provendo-Systems GmbH