



## **Unsere IT ist doch sicher ! Wozu ISO 27001 ?**

RBP Seminar, LRZ München, 27.10.2011

Marc Heinzmann, plan42 GmbH  
ISO 27001 Auditor





# plan42 GmbH

- Wir sind ein Beratungsunternehmen ohne Produktvertrieb, unsere Beratung erfolgt produktneutral und herstellerunabhängig.
- Unsere Senior Consultants sind zertifizierte
  - IT Service Manager (ITIL)
  - ISO 20000 certified Consultants
  - Zertifizierte ISMS Berater
  - Zertifizierte IT-Revisoren
  - ISO 27001 Auditoren
- Wir verbinden technische Expertise aus den Bereichen Enterprise Computing und IT-Security mit praxisbewährten IT-Management Konzepten.

# Agenda

- Kurzüberblick ISO / IEC 27000
- Motivation
- Wozu ISO 27001? – Gründe für CISOs
- Wozu ISO 27001? – Gründe für CIOs
- Wozu ISO 27001? – Gründe für CEOs



# Kurzüberblick ISO / IEC 27000



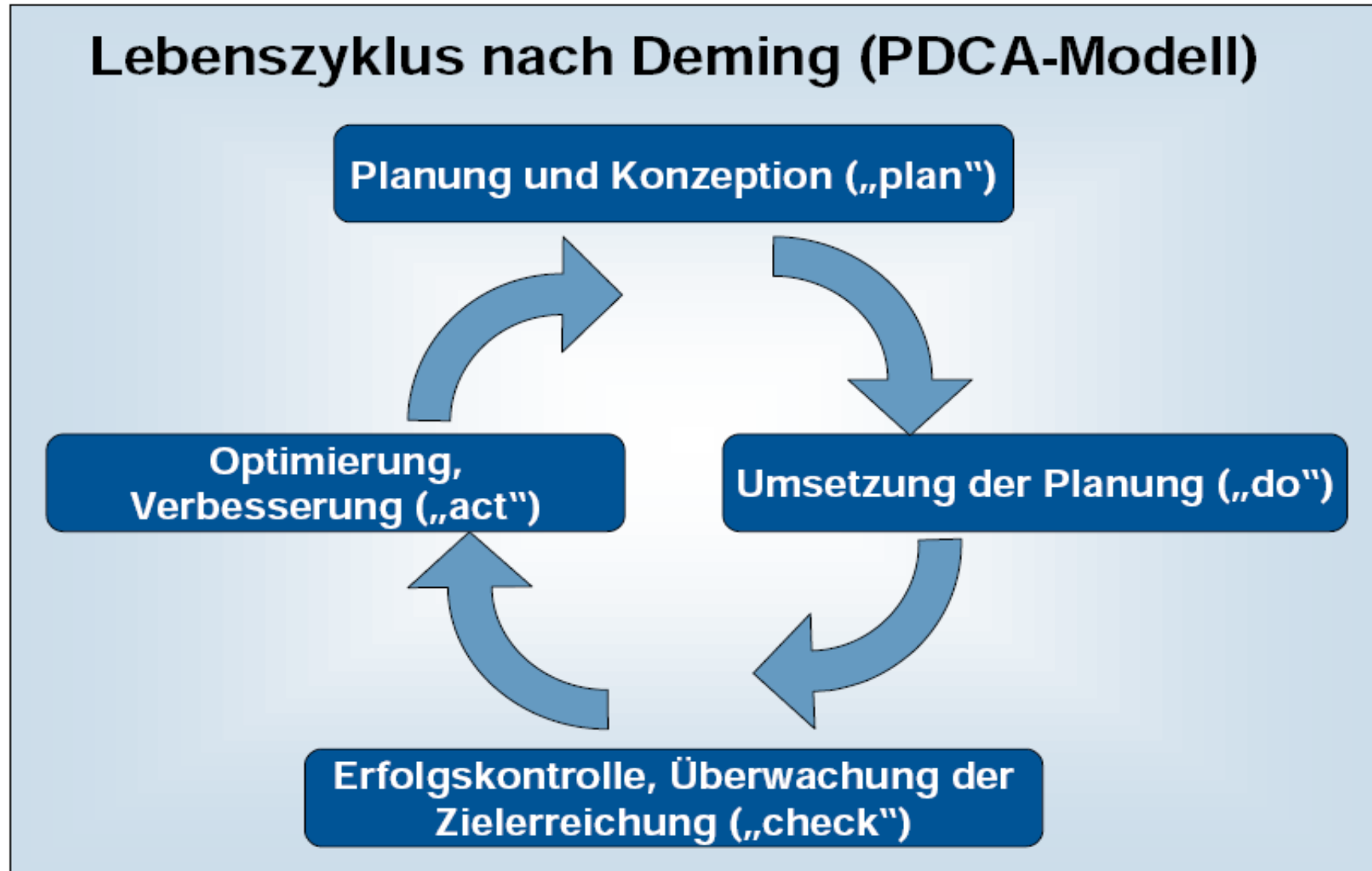
# Ziel

- Prozessbeschreibung (Management System) für den Schutz von Informationen
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
  
- Zusammenfassung aller Normen für den Bereich ISMS (Informationssicherheitsmanagementsystem) in der 27000'er Reihe
  
- Empfehlungen
  - Anforderungen an ein ISMS
  - Vorgehen zur Einführung eines ISMS
  - Risikomanagement
  - Maßnahmen
  
- International anerkannte und zertifizierbare Norm

# ISO / IEC 27000 Normen

- ISO / IEC 27000: “Grundlagen und Vokabular”
- ISO / IEC 27001: “ISMS Anforderungen”
- ISO / IEC 27002: “Maßnahmenkatalog”
- ISO / IEC 27003: “Leitfaden für die Umsetzung”
- ISO / IEC 27004: “Messbarkeit von ISMS”
- ISO / IEC 27005: “Risikomanagement für ISMS”
- ....
- Branchenspezifische Normen (z.B. Telekommunikation, Gesundheitswesen)

# Der ISMS Prozess nach ISO 27001





# Motivation

# Wozu ISO 27001? – Antworten von CIOs

Sicherheit kostet zu viel  
Zeit meiner ohnehin  
überarbeiteten Admins!

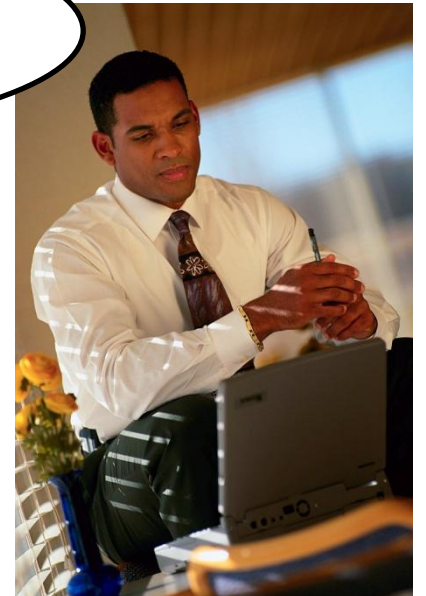
Wieso? Wir haben doch eine  
Firewall, Virenschutz und  
gehärtete Betriebssysteme!

Die von uns eingesetzten  
Sicherheitsfunktionen  
reichen vollkommen aus!

Unser IT-Budget reicht  
für so etwas nicht!

Sicherheit hemmt  
Investitionen in notwendige  
IT-Infrastruktur!

usw,  
usw,  
usw



# Wozu ISO 27001? – Antworten von CEOs

Sicherheit ist keiner unserer Erfolgsfaktoren! Welchen Mehrwert bietet IT-Sicherheit für unsere Geschäftsprozesse?

Unser Mitbewerb hat das auch nicht!

usw,  
usw,  
usw

Wir müssen wirtschaftlich arbeiten und brauchen keine weiteren Hemmschwellen!

Bisher ist doch nichts passiert!

Wir werden die IT ohnehin auslagern. Damit ist IT-Sicherheit ein Problem des Dienstleisters!

ISO 9000 hat uns schon viel zu viel Geld gekostet!





## Wozu ISO 27001? – Gründe für CISOs



# Strukturierter Ansatz

- Verbesserung der Informationssicherheit im Unternehmen
- Abarbeitung eines konkreten Vorgehensmodells
  - Es werden keine wichtigen Aspekte vergessen
  - Es werden Fehler vermieden

# Korrekte Wahrnehmung der IT-Sicherheit

- Nach ISO 27001 muss die Geschäftsleitung / Vorstand in den Prozess mit eingebunden werden → Unterstützung von der „obersten Leitungsebene“
- IT-Sicherheit ist ein Prozess und kein Projekt
- ISMS ist nicht der „Verhinderer / Bremser“ von Projekten
- IT-Sicherheit ist nicht nur IT-Technik
  - Personal
  - Organisation
  - Physische Infrastruktur
  - Risikomanagement
  - Ganzheitliche Sicht → Beteiligung in der frühen Projektplanung und Unternehmensstrategie

# Korrekte Wahrnehmung der CISO Rolle

- CISO kein Vorruehstandsposten → Manager direkt der GF / Vorstand unterstellt
- CISO ist ISMS Prozessverantwortlicher mit Schnittstellen zu
  - Geschäftsprozesse
  - Unternehmensstrategie
  - Risikomanagement
  - Datenschutz
  - Controlling
  - IT-Compliance / Governance Management
  - Rechtsabteilung / Juristen
  - IT-Organisation
  - IT-Technik
  - Werkschutz / physische Sicherheit



## Wozu ISO 27001? – Gründe für CIOs



# Bessere Wahrnehmung der IT

- Bezug Geschäftsprozesse zu IT
  - IT als „Business-Enabler“
  - IT wird transparenter für die GF / Vorstand gestaltet
  
- IT-Sicherheit ist gerade „in“
  - Ausnutzen der öffentlichen Diskussion zur besseren Darstellung & Optimierung der IT-Prozesse



# Ausnutzen der Synergieeffekte

- Erstellung einer aktuellen Ist-Aufnahme der IT-Infrastruktur (CMDB)
- Aktualisierung / Erstellung von Dokumentationen
  - Installationshandbücher
  - Betriebshandbücher
  - Notfallhandbücher
  - Physische Infrastruktur
  - Prozessbeschreibungen
- Schulungen
  - Administratoren
  - Benutzer

# Einführen geordneter Betriebsprozesse – 1

- Störungsmanagement
  - Service Desk zur Erfassung von Sicherheitsvorfällen
  
- Problemmanagement
  - Sicherheitsaudits ergeben meist „Problems“
  - Sicherheitslücken sind „Problems“
  
- Änderungsmanagement
  - Beheben von Sicherheitsproblemen
  - Beurteilung der Sicherheit von „Changes“
  
- Versionsmanagement
  - Prüfung neuer Komponentenversionen auf Sicherheit
  - Einführung von neuen Sicherheitslösungen

# Einführen geordneter Betriebsprozesse – 2

- Konfigurationsmanagement
  - CMDB (Vertraulichkeit, Verfügbarkeit und Integrität)
- Verfügbarkeitsmanagement
  - Verfügbarkeit ist ein Ziel des ISMS Prozesses
- Kapazitätsmanagement
  - Bereitstellung von Kapazitäten beeinflusst die Verfügbarkeit

# Kosteneinsparpotential

- Bessere Transparenz der Anforderungen → Passgenaue Investitionen in IT-Sicherheit
  - Abhängigkeit der Geschäftsprozesse von IT
  - Schutzbedarfsfeststellung
  - Risikomanagement
  
- Bessere Transparenz der IT
  - Schnellere Störungsbehebung → Bessere Unterstützung der Geschäftsprozesse
  
- Prozessoptimierung
  - Geregelt Schnittstellen zur IT
  - Schnellere Bearbeitung von Anfragen / Problemen
  - Weniger Belastung der Administratoren



## Wozu ISO 27001? – Gründe für CEOs



# Erfolgsfaktor für das Unternehmen

- Minimierung der Risiken
  - weniger Störungen, mehr Produktivität
  - Wahrscheinlichkeit eines Sicherheitsvorfalls wird reduziert
  
- Erhöhung der Transparenz
  - Bezug Geschäftsprozess zu IT
  - IT Reporting
  
- Kosteneinsparung
  - Effizienzsteigerung in der IT-Abteilung
  - Passgenaue Investitionen in IT, weniger Fehlinvestitionen

# Compliance Vorgaben

## ■ Rechtliche Vorgaben

- GmbHG, AktG, KonTraG
- BDSG
- GoBS
- ...

## ■ Branchenspezifische Vorgaben

- Banken
  - BASEL II, KWG, MaK, MaH, MaR
- Kreditkartenhersteller
  - MasterCard / Visa Requirements
- Merchants
  - PCI DSS
- Automobilindustrie
  - VDA Standards & Best Practices
- ...



# ISO 27001 Zertifikat

- Darstellung der Sorgfalt im Umgang mit Informationen
- Verkaufsargument
- Abhebung vom Wettbewerb
- Erleichterung von Audits

# Beim ISMS Prozess gibt es viele Gewinner!

- Unternehmensleitung
- IT-Abteilung
- IT-Anwender
- Kunden





# Kontakt

plan42 GmbH  
Bauerstr. 19  
80796 München

Tel.: 089 30765716

Web: <http://www.plan42.com>

Ansprechpartner Information Security:  
Marc Heinzmann  
[mh@plan42.com](mailto:mh@plan42.com)