IT-Compliance

31.10.06

Referent: Frank Bitzer

bitzer digital-media consulting

Vorstand Zentrum interaktive Medien ZIM e.V.

E-Mail: fb@bdcon.de

Web : www.bdcon.de

Portal: www.one.de

Intro

Frank Bitzer

- **Inhaber der bitzer digital-media consulting (BDCON.de)**
  Beratung für digitale Geschäftsprozesse und e-Business
- Vorstandsvorsitzender des Zentrums für interaktive Medien, ZIM e.V.
- EDV Projekte und IT-Erfahrung seit 1980
- Gründer von OpenImmo, dem Datenstandard in der Immobilienwirtschaft
- **Compliance Erfahrung u.a. in**
  - Entwicklung von Software für Banken
  - Zahlreiche Software- und Beratungsprojekte in unterschiedlichen Branchen
  - e-Procurement Planung
  - Seminaren zu Internet Sicherheit
- **Autor:**
  Die digitale Signatur, 1999 (Mit K. Brisch) und XML im Unternehmen, 2003

Das Thema

- IT-Compliance ist ein Teil der gesamten Corporate Covernance
- Wie kann dieses Vorhaben angegangen werden
- **Aufzeigen der organisatorischen Schritte**
  Nicht: Konfigurieren einer Firewall
- **Wir betrachten die Unternehmens Architektur**
  Personen, Geschäftsprozesse, Software Anwendungen
- Umfeld des IT Service Managements

--> Der Inhalt

Der Inhalt

5 1/2 d.h. 5 Fragen beantworten und einen Ausblick geben

- **1. Warum: Bedarf ermitteln**
  Muss ich mich da wirklich drum kümmern?
- **2. Wer: Planung.**
  Wer kümmert sich um das Thema.
- **3. Wo und Was:**
  Analyse der Schwachstellen, ermitteln der Aufgaben. Dokumentieren
- **4. Wie: Die Form der Umsetzung**
  Methoden, Standards und Werkzeuge
- **5. Wann:Das Review,**
  Regelmäßiges Update und Audit.
- **5 1/2 Was: Was bringt es zusätzlich**
  oder in Köln: Watt kost dat, watt bringt dat ?
- Tenor: Pargmatisches Vorgehen
- In der Literatur auch: Plan, Document, Act, Check

--> Kapitel:Schritt 1: Der Bedarf (Warum)

Schnelltest zum Bedarf

- **Organisation**
  - Software Lizenzen vs. Mitarbeiterzahl
  - Umgang mit privater E-Mail
    insbesondere nach Ausscheiden aus Unternehmen
- **Buchhaltung**
  - Können Sie nachweisen wer wann, was, wo gebucht hat
    Unter Wahrung der persönlichen Daten
- **IT-Sicherheit**
  - Passwörter auf Spickzettel
  - "Offene" PC's in der Mittagspause
  - Ungesicherte Laptops, PDA's und Handys
- **Internet**
  - Wer hat Zugang zu den Daten auf ihrer WebSite
- **ERGEBNIS:**
  Wenn nicht alle Risiken ausgeschlossen werden können, besteht Handlungsbedarf

--> Kapitel:Schritt 2: Die Planung (Wer)

Schritt 2: Die Planung (Wer)

Organisation

- **Ernennung eines Compliance Beauftragten**
  CCO Chief Compliance Officer. Klingt gut!
- **Wer kann das sein:**
  - IT-Leiter: Müsste sich selbst kontrollieren. Das ist problematisch
  - Datenschutz Beauftragter. Siehe IT-Leiter
  - Personal / Orga / Innendienst Personen
- **Separate Stelle bzw. Person**
  - Stabs Funktion, da für alle Abteilungen zuständig.
- Benötigte Vorkenntnis: Technik, Jura, Organisation
- **Externe Berater für den Projekt Start und die Begleitung**
  Als neutraler Moderator zwischen den Abteilungen

--> Technik

Technische Resourcen

- Im einfachsten Fall eine Textverarbeitung für die Dokumentation
- Besser ist natürlich eine Datenbank zur Speicherung und Auswertung
- Am Besten. Spezielle Tools mit Unterstützungsfunktionen
- BDCON verwendet "Compliance-WorX". Rund 50 Fragen mit Auswertung der Risiko Analyse
- Intranet für Datenerfassung, Anzeige und Information
- Frage klären: Make oder Buy
- Ausrichtung an Standards von BSI, ITIL und anderen

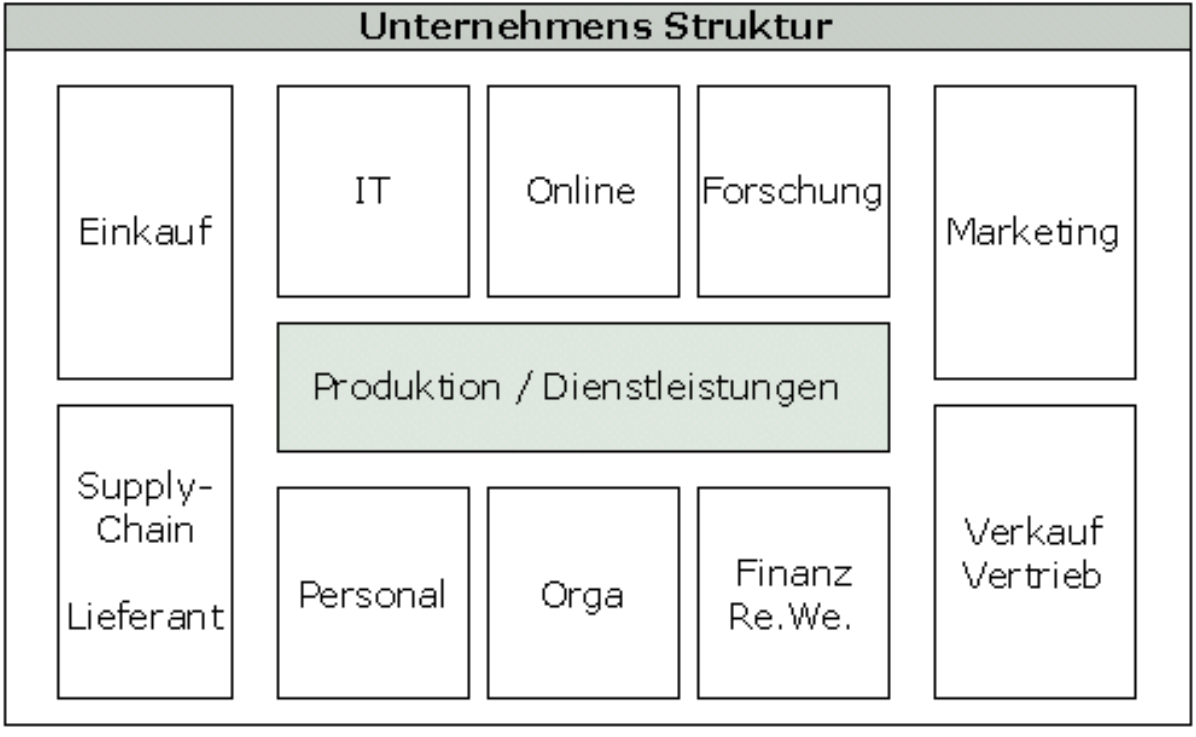
Ablauf

- Nicht kurzes Projekt und dann vergessen ..
- sondern ein dauerhafter Prozess
- Priorisierung der Arbeiten
- Budget und Zeitplanung
- Regelmäßiges Review einplanen
- Beginnen wir mit der Analyse des Unternehmens ...

--> Kapitel:Schritt 3: Die Analyse (Was und Wo)

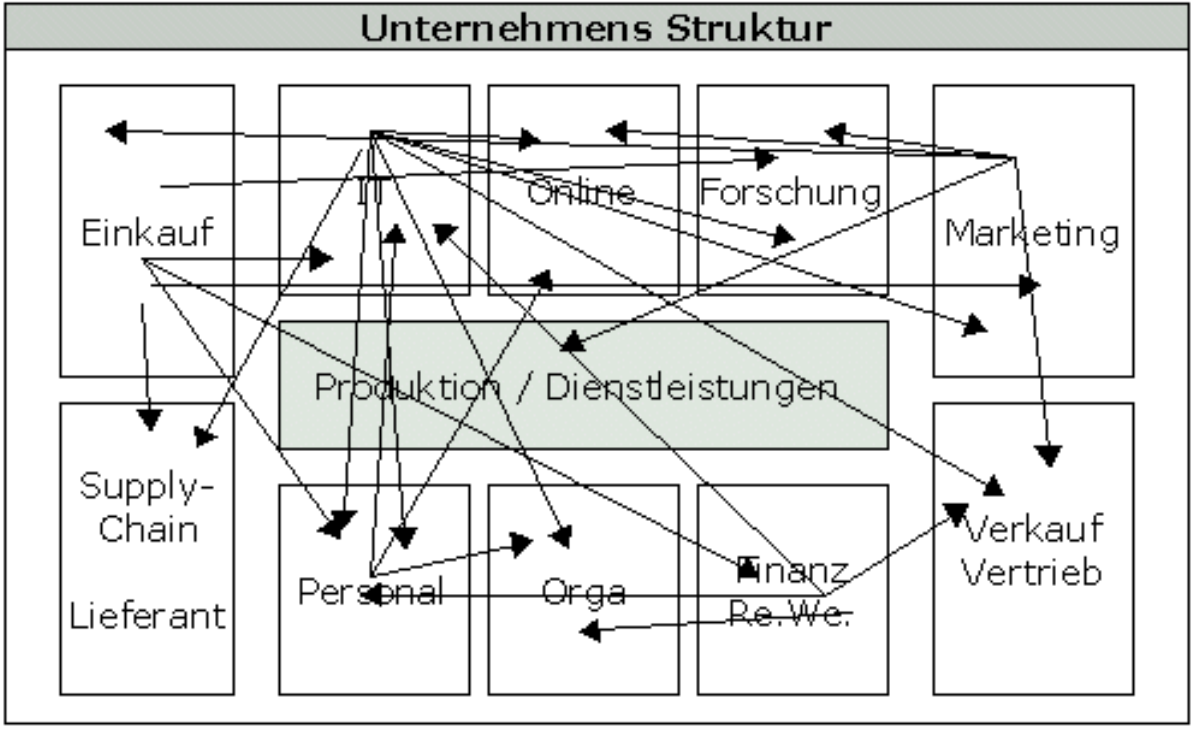
Schritt 3: Die Analyse (Was und Wo)

Ein Unternehmen und seine Abteilungen



--> Unternehmens Datenfluss

Der Datenfluss im Unternehmen



Was ist zu betrachten

- Geschäftsprozesse mit Ablauf und Auswirkung
- Personen und Ihre Aktivitäten
- Rollen und Rechte
- Technik und Infrastruktur
- Daten und deren Verwendung
- **Informationen auf externen Plattformen: Webserver, Outsourcing**

Was ist zu berücksichtigen?

- **Der BSI Grundschutzkatalog für IT Sicherheit (Über 3000 Seiten)**
  Zeigt ca. 900 Massnahmen in den Bereichen:
  Infrastruktur (Gebäude), Organisation, Personal,
  Hardware und Software, Kommunikation, Notfallvorsorge
  - Beispiele für die Massnahmen:
    - M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz
    - M 3.45 Planung von Schulungsinhalten zur IT-Sicherheit
    - M 6.22 Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen
- **Die gesetzlichen Regelungen bestimmen weitere Felder:**
  Basel II, KontraG, GdpdU, BDSG, TKG, SOX?
- **Eigene Firmen Angaben**
  - Organigramm der Abteilungen
  - Verzeichnis der IT Hardware und Software
  - Liste der Computer mit Internet Zugang
  - Verzeichnis der "Datenbanken"

--> Beispiele 1

Beispiele 1

- **IT-Sicherheit:**
  - Backup und ! Recovery. Datensicherung auch außerhalb des Betriebs
  - Personal Anweisungen für geschäftliche / privat E-Mail
  - Sicherung Mobiler Geräte (Laptop, PDA, Telefon)
  - Voice -over-IP Telefonie, WLAN Sicherung
- **ILM Information Lifecyle Management:**
  oder einfach: Was passiert mit alten Daten
  - Wechsel von Betriebssystem z.B. DOS Warenwirtschaft auf dBase ? (GdpdU)
  - Wechsel einer Software z.B. von Outlook zu Notes
  - DMS Dokumenten Management. Dateiformate wie z.B. PDF/A
- **Outsourcing**
  - Vereinbarung über Datenschutz
- **Online Präsenz**
  - Einfache Websites. Impressum, Copyrights
  - Online Shop / e-Procurement: eCommerce Richtlinie

--> Beispiele 2

Beispiele 2

- **IT-Organisation:**
  - Software Lizenz Management
  - Einhaltung der Lizenz Vorschriften (z.B. Open Source)
    Besonders bei Änderung und Erweiterung
  - Authentifizieren, Autorisieren. Wer arbeitet wann an welchen Daten
  - Identity Management
- **In den Fachabteilungen:**
  - Datenbasis auf Redundanz untersuchen
  - Zugänge und Nutzung von Anwendungen: Rollen und Rechte Konzept
  - Gibt es "private" Lösungen (z.B. 10 verschiedene Tabellen mit Kundendaten ..)
- **Finanzen**
  - GdpdU: Ausgabe von Daten im IDEA Format
  - Wer arbeiten an der Bilanz mit

--> Kapitel:Schritt 4: Die Umsetzung (Wie)

Datenerhebung auf Basis der Analyse

- **Strukturieren der Daten nach**
  Unternehmensbereichen, Anwendungen, Prozessen, Allg. IT Sicherheit
  evlt. in Kombination mit Directorys wie LDAP u.a.
- **Erfassen der "Objekte" mit**
  - Gefährdungspunkten, Rechtlicher Bezug, Maßnahmen zur Behebung
  - dem aktuellen Staus: Nicht erfüllt, Teils erfüllt oder Voll erfüllt
- **Laufende Daten der Erhebung**
  Personen, Zeiten, Status. Wichtig auch für Review

--> BSI-Beispiel

BSI Grundschutz: B 3.402 Faxgerät (Ein Auszug)

- **Gefährdungslage**
  Für den IT-Grundschutz werden bei der Informationsübermittlung per Fax folgende typische Gefährdungen angenommen:
  - Menschliche Fehlhandlungen:
  - G 3.14 Fehleinschätzung der Rechtsverbindlichkeit eines Fax
  - Technisches Versagen:
  - G 4.14 Verblassen spezieller Faxpapiere
  - Vorsätzliche Handlungen:
  - G 5.7 Abhören von Leitungen
- **Maßnahmenempfehlungen**
  - Umsetzung:
    - M 1.37 (A) Geeignete Aufstellung eines Faxgerätes
    - M 2.47 (B) Ernennung eines Fax-Verantwortlichen
    - M 3.15 (A) Informationen für alle Mitarbeiter über die Faxnutzung

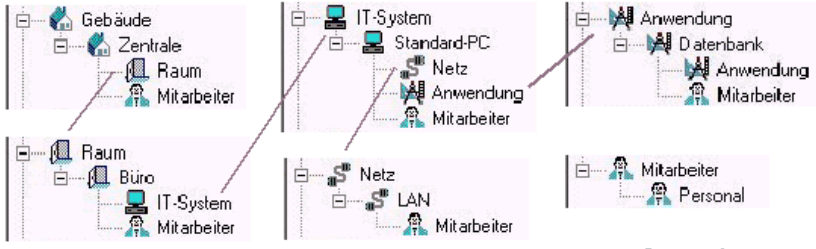
Werkzeuge

- Dazu gibt es Vorlagen und Schablonen
- GS Tool für die Erfassung und Auswertung nach BSI Grundschutz Katalog
- BITKOM, IT-Compliance beim Outsourcing
- Analyse und Dokumentations-Werkzeuge für Basel II, CObit u.a.
- **Unterschiedliche Software Tools von**
  IBM, Oracle, SAP, FoxT u.a.
  für einzelne Bereiche wie das Identity Management

--> Beispiel BSI-GSTool

Datenerfassung mit BSI GS-Tool 4.0

Strukturierung



Stammdaten

Name	Typ	Subtyp	Erfasst durch	Erfasst am	Rechte	ID
Anwendung 1	Anwendung	[allgemeine Anwendung]	DOMAENE-B\	09.02.2005 16:49:57	lesen / schreiben	10C38
BSI	übergreifende Aspekte	[allgemeiner IT-Verbund]	dbo	31.01.2006 08:48:29	lesen / schreiben	1
Haus 1	Gebäude	[allgemeines Gebäude]	DOMAENE-B\	31.01.2005 12:17:52	lesen / schreiben	10C09
Mitarbeiter 1	Mitarbeiter	[Mitarbeiterin/Mitarbeiter]	sa	01.02.2005 06:56:50	lesen / schreiben	10C11
Mitarbeiter 2	Mitarbeiter	[Mitarbeiterin/Mitarbeiter]	DOMAENE-B\	01.02.2005 08:14:51	lesen / schreiben	10C14
Netz 1	Netz	heterogenes Netz	DOMAENE-B\	09.02.2005 16:49:40	lesen / schreiben	10C37
Raum 1	Raum	Büroraum	sa	01.02.2005 07:59:26	lesen / schreiben	10C13
System 1	IT-System	[allgemeiner Client/PC]	DOMAENE-B\	09.02.2005 16:50:13	lesen / schreiben	10C39
Verbund 2	übergreifende Aspekte	[allgemeiner IT-Verbund]	DOMAENE-B\	10.02.2005 10:36:38	lesen / schreiben	10C43

Laufender Betrieb

- Lösung der Probleme nach Prioritäten
- **Kommunikation**
  - Information an die Mitarbeiter schon zu Beginn
  - Betriebsrat / Personalrat wenn vorhanden einbinden
  - Schulung im Umgang mit Sicherheitsthemen
    "Compliance beginnt in den Köpfen der Mitarbeiter"
  - Newsletter / Intranet für die laufende Information

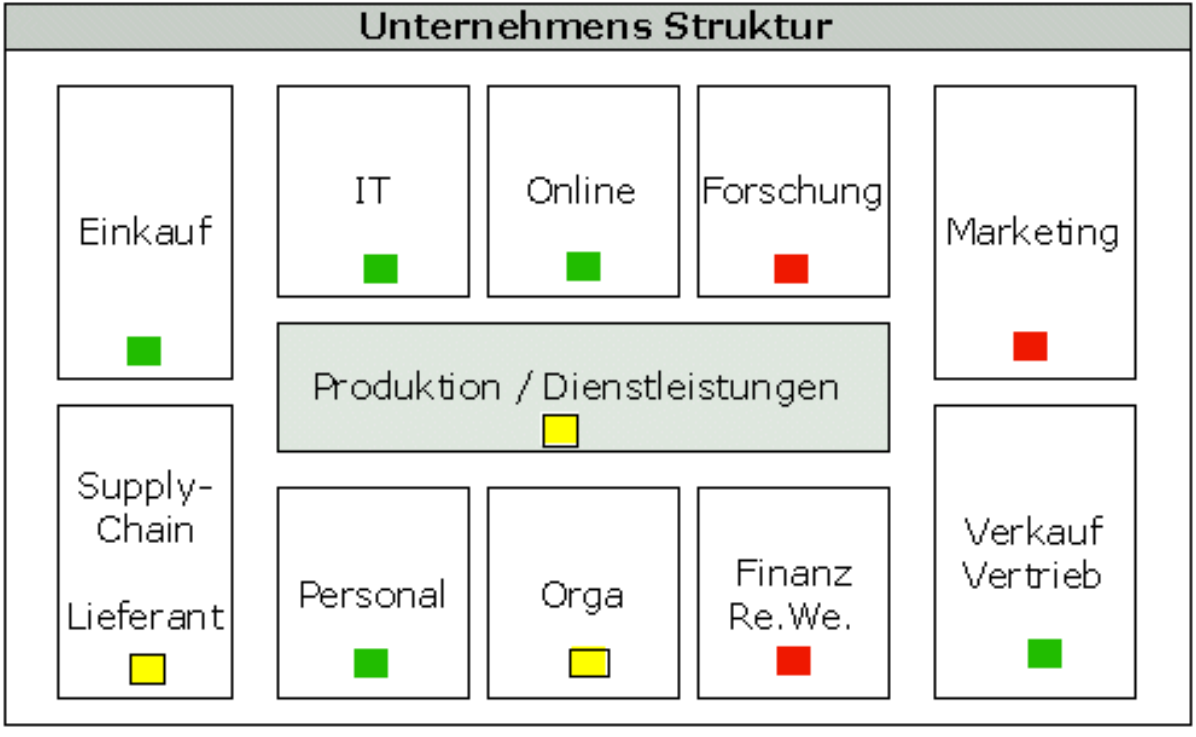
--> Datenauswertung

Ein permanenter Status

- **Dokumentation mit den**
  - Bereichen und ihrem Compliance Status
  - Weitere ToDos
  - Review Planung
- **In Kombination mit Software für**
  - Projekt Planung
  - Budget Planung

Unternehmen aktuell

Der aktuelle Status



--> Kapitel:Schritt 5: Das Review (Wann)

Schritt 5: Das Review (Wann)

Zeit und Umfang

- **Regelmäßige Überprüfung**
  - bei Personalwechsel
  - (Halb) Jährlich
  - bei neuen Gesetzen und Regeln
- Intranet für die Checkliste der Mitarbeiter
- Handlungsplan für die Compliance Beauftragten
- **Erinnerungsfunktion für Review**

--> Kapitel:Schritt 5-1/2: Das ROI

Schritt 5-1/2: Das ROI

Kosteneinsparung

- **Redundante Datenhaltung wird aufgedeckt**
  Dadurch weniger Reibungsverluste beim Kundenkontakt
- Nicht genutzte Alt-Lizenzen werden gefunden
- Status über Wartungsverträge für die Budgetierung
- **Asset Management und Lizenzmanagement**
  erspart das Turnschuh-Netzwerk und erleichtert Inventur
- **Gemäß Gartner: 80 % der IT Kosten durch laufenden Betrieb**
  - Reduzierung der Kosten im Helpdesk für vergessene Passworte
- Der immer aktuelle Überblick erspart Kosten für ad-hock Berichte

--> Vorteile und Perspektiven

Vorteile und Perspektiven

- **IT Welt**
  - Entwicklung eines effiziente IT Service Management
  - Ausrichtung an ITIL (Information Technology Infrastructure Library)
    IT Abteilung als Dienstleister für IT Services
- **Finanzwelt**
  - Besseres Rating für Basel II
  - Rabatte bei Versicherung
- **Prozess Optitmierung**
  - Die Analyse der Unternehmens Architektur visualisiert die Umsetzung der Geschäftsprozesse
  - Dies ist die optimale Basis für eine nachfolgende Optimierung
  - Hervorragende Basis für die EInführung einer SOA Service Orientierten Architektur

--> Kapitel:Fazit

Fazit

Ziel erreicht

IT-Compliance

- Es geht kein Weg dran vorbei
- Die Kosten sind überschaubar
- Der Nutzen ist darstellbar
- Machen Sie die Notwendigkeit zur Chance

- Danke für die Aufmerksamkeit
- **Weiterführende Informationen auch unter** www.zim.de und www.compliance.one.de
- Fragen gerne an fb@bdcon.de
- Start der Diskussionsrunde