



UIMC[®]

DR. VOSSBEIN
GmbH & Co KG

**Unternehmens- und
Informations- Management
Consultants**

Informationssicherheit, Datenschutz und Compliance als integrierte Aufgabe

ISO 27001 - Umsetzungshilfe mit Best Practice

Referent: Tim Hoffmann

Internet: www.UIMC.de
E-Mail: consultants@UIMC.de

Nützenberger Straße 119
42115 Wuppertal

Telefon: 0202 - 265 74 - 0
Telefax: 0202 - 265 74 - 19

Tim Hoffmann (Dipl.-Kfm.)

- ➔ Wirtschaftswissenschaften an der Universität-GH Essen
- ➔ Studien-Schwerpunkte; u. a.
 - » Organisation
 - » Informationsmanagement
- ➔ Seit 2002 als Berater bei der **UIMC**[®]
- ➔ Schwerpunkte:
 - » Datenschutz und IT-Sicherheit
 - » insbesondere für KMU
- ➔ Datenschutzbeauftragter
- ➔ Leiter Arbeitskreis „ISO 27001“ (ruhr networker)



66,7 %



**Akkreditiert u. a. für ISO 27001
(inkl. Prototypenschutz)!**

**auch speziell für KMU:
Low-Budget-Konzept**

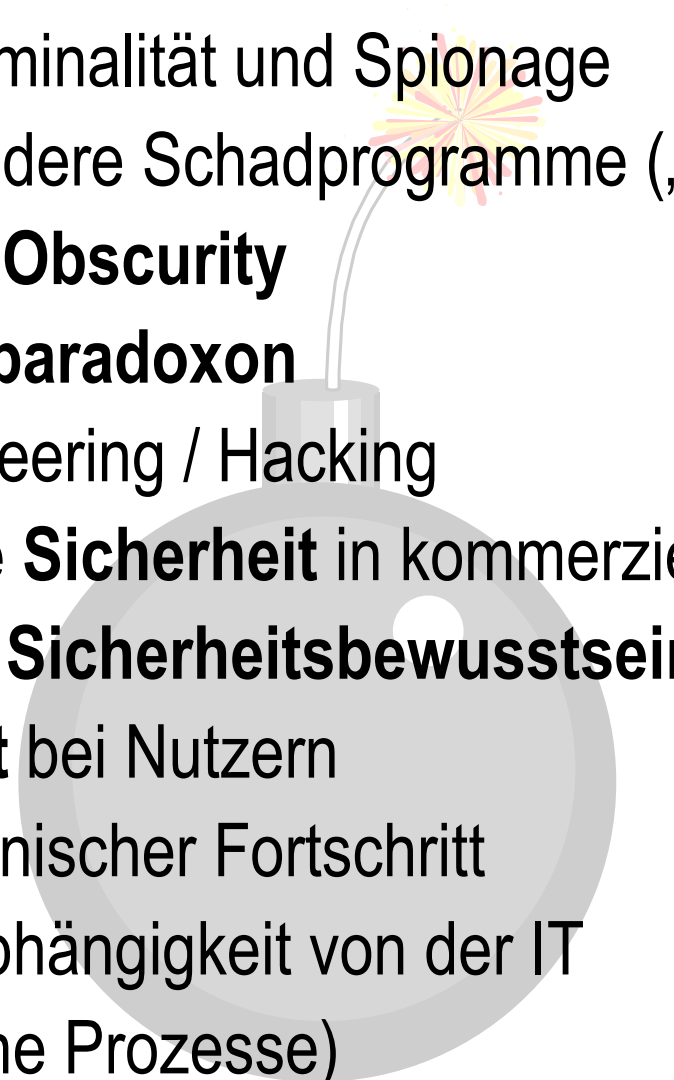
Individuelle Beratungen und Konzeptionen Unternehmensmanagement	Standardisierte Beratungen und Konzeptionen	Individuelle Beratungen und Konzeptionen IT-Management	Betriebliche und außerbetriebliche Fort- und Weiterbildung
Unternehmensführung	UMC - Unternehmens- und Management-Checkup	IT-Sicherheit	Unternehmensorganisation
Controlling		IT-Revision (Auditing)	Unternehmensplanung und -budgetierung
Aufbau- und Ablauforganisation	Sicherheits-Schwachstellenanalyse (Si-SSA) gem. ISO 17799/27001	Datenschutzberatung	IT-Systemplanung
Planung und Budgetierung		Externe Datenschutzbeauftragung	IT-Controlling
Informationssystemmanagement	Datenschutz-Checkup gem. BDSG und IuKDG	Datenschutz- und -sicherheit im Gesundheitssektor	Datenschutz
Marketing		Erstellen und Überprüfen von Pflichtenheften	Sicherheitskonzeptionen
	Organisationsmittel		Arbeitsplatzsicherheit
			ISO 27001
SW-Lösungen für interne und externe Beratungs- und Auditierungsprojekte			

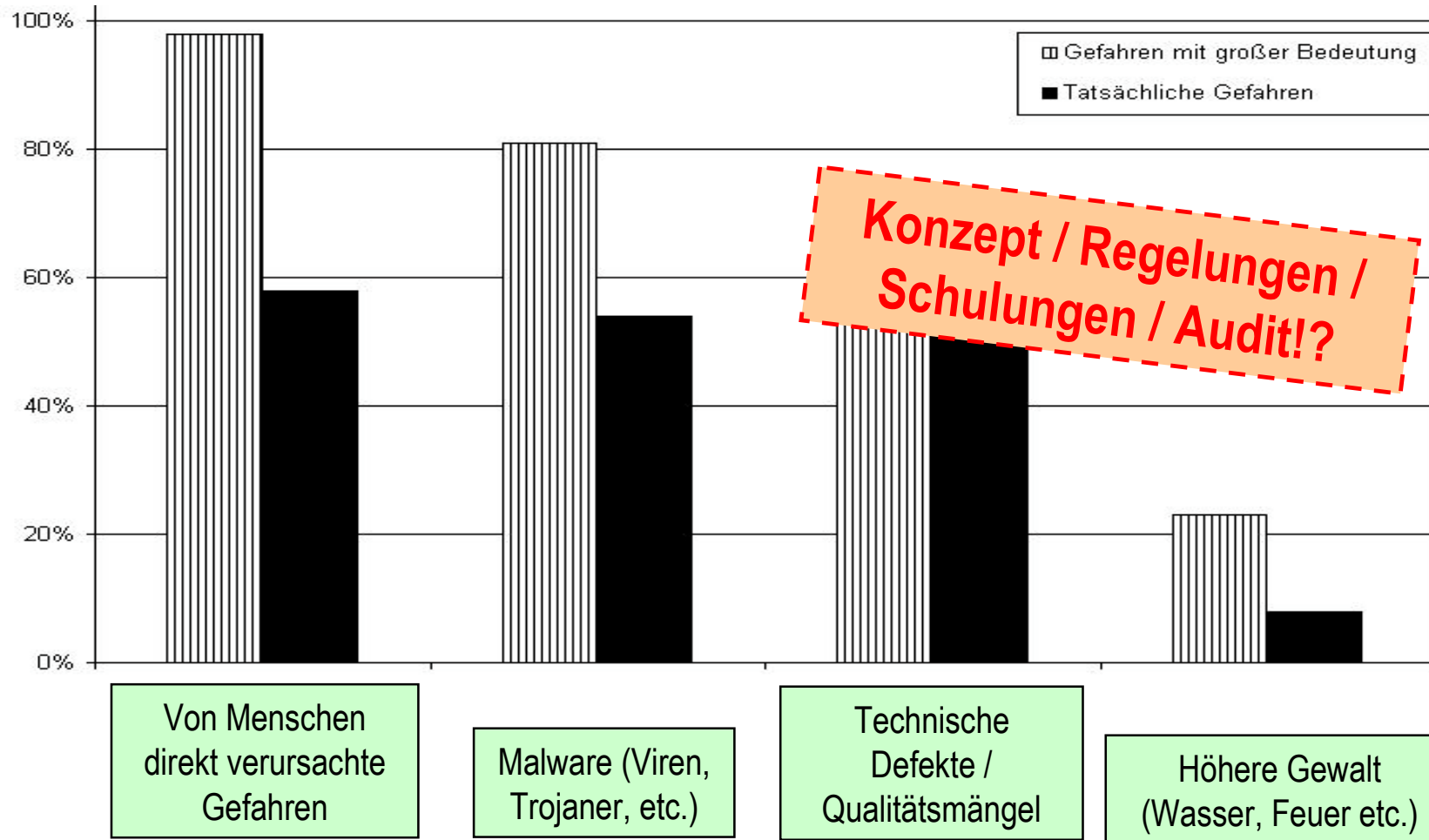
- 1 IT - Faktor für den Unternehmenserfolg**
- 2 Compliance: Worthülse oder Managementaufgabe?
- 3 ISO 27001 als Best-Practice-Norm
- 4 Fazit und Ausblick

Können Sie sich Ihr Geschäft noch so vorstellen?

- ➔ ohne Personal Computer und Netzwerk
 - ➔ ohne E-Mail-Korrespondenz
 - ➔ ohne elektronische Termin- und Adressverwaltung
 - ➔ ohne „CRM“-System
 - ➔ ohne Internetpräsenz
- oder (bald)
- ➔ ohne Handy / Smartphone / Blackberry
 - ➔ ohne W-LAN / VPN
 - ➔ ohne Laptop



- 
- ➔ Computerkriminalität und Spionage
 - ➔ Viren und andere Schadprogramme („**Malware**“)
 - ➔ **Security by Obscurity**
 - ➔ **Sicherheitsparadoxon**
 - ➔ Social Engineering / Hacking
 - ➔ **Trügerische Sicherheit** in kommerziellen Produkten
 - ➔ Mangelndes **Sicherheitsbewusstsein**
 - ➔ **Arglosigkeit** bei Nutzern
 - ➔ **Blinder** technischer Fortschritt
 - ➔ steigende Abhängigkeit von der IT
(insb. kritische Prozesse)



Quelle: KES Sicherheitsstudie 2004

„IT-Sicherheit ist ein lästiges Übel!“
(KES-Studie 2004)

Auswirkungen der Krise in den letzten neun Monaten

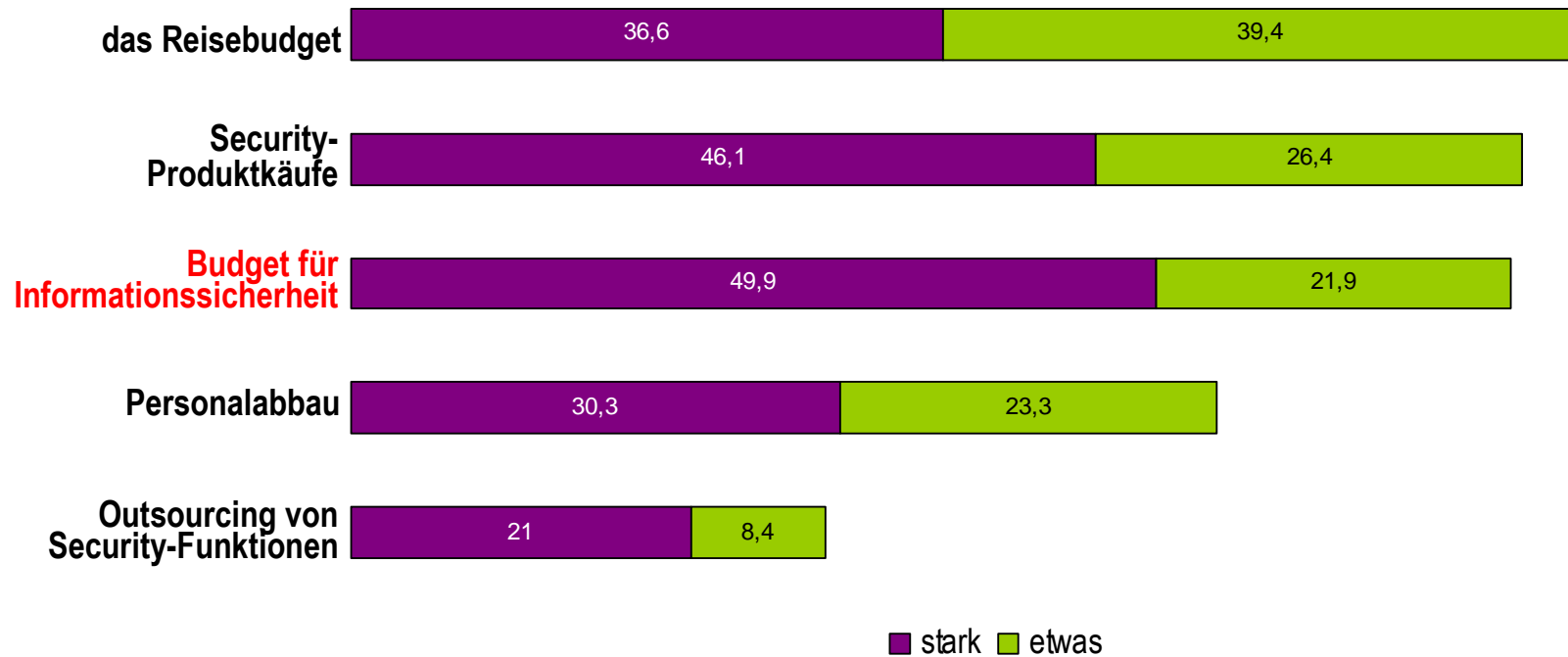


Abb.: Computer Zeitung Ausg. vom 15.06.09, Artikel "Blindes sparen gefährdet Schutz".

- » Ja klar! Wir haben eine Pflichtentrennung bei der Rechtebeantragung: Der Mitarbeiter beantragt und ich pflege dies in die Active Directory ein.“
(Administrator eines QM-zertifizierten Mittelständlers)
- » „Ich habe keinerlei wichtige Unterlagen; die können durchaus allen zur Einsicht gegeben werden.“
(Gruppenleitung in einer Behindertenwerkstatt mit Zugriff auf Gesundheitsdaten von Behinderten)
- » „Natürlich haben wir eine Alarmanlage! Wenn jemand eine Scheibe einwirft, dann werden die Nachbarn das schon melden!“ *(EDV-Leitung einer Sparkasse)*

- 1 IT - Faktor für den Unternehmenserfolg
- 2 Compliance: Worthülse oder Managementaufgabe?**
- 3 ISO 27001 als Best-Practice-Norm
- 4 Fazit und Ausblick

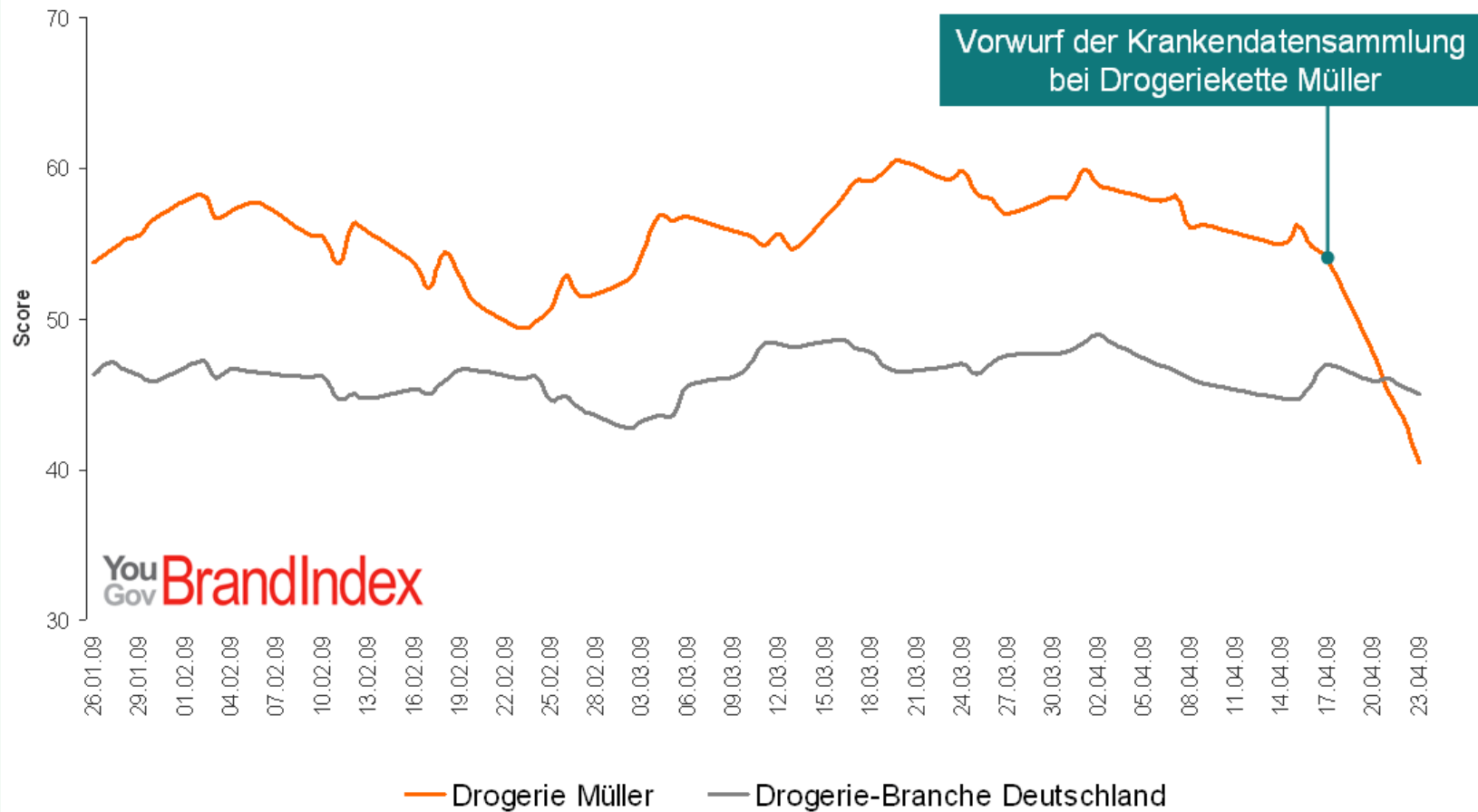
Was sagt Wikipedia?

- ➔ Das Wort Compliance (englisch Befolgung) bezeichnet die **Einhaltung** von Verhaltensmaßregeln, Gesetzen und Richtlinien (**Ordnungsmäßigkeit**).
- ➔ Compliance-Anforderungen in der IT: insb. Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz
 - » datenschutzrechtlich: BDSG, TKG, TMG etc.
 - » handelsrechtlich: GmbHG, GoDV, HGB etc.
 - » urheberrechtlich: UrhG, KunstUrhG
 - » risiko-orientiert: KonTraG etc.
 - » sonstiges: AGG, BetrVG, SigG, EnwVG etc.
 - » Neue Problemfelder durch „Globalisierung“: Sarbanes Oxley Act oder internationaler Datentransfer ins Ausland

Der Vorstand hat **geeignete Maßnahmen** zu treffen, insbesondere ein **Überwachungssystem** einzurichten, damit den Fortbestand der Gesellschaft **gefährdende Entwicklungen** früh erkannt werden (§ 91 AktG als Beispiel)

- ➔ Bestellung eines Datenschutzbeauftragten
 - » Zuverlässigkeit und Fachkunde
- ➔ Prüfung der Zulässigkeit
- ➔ Führung der Verfahrensübersicht;
- ➔ Vertragsgestaltung mit Dienstleistern;
- ➔ Vorabkontrolle neuer Systeme;
- ➔ Umsetzung von technisch-organisatorischen Maßnahmen
 - » angemessene Schutzmaßnahmen
 - » „Anforderungskatalog“ in Anlage zu § 9 BDSG
- ➔ Schulung und Verpflichtung der Mitarbeiter;
- ➔ etc.

Mit dem Datenskandal fällt Müller erstmals unter den Branchendurchschnitt



Neben der „bloßen“ gesetzlichen Forderung:

- ➔ (persönliche) Haftungsrisiken für Geschäftsführung;
- ➔ Rechtsunsicherheit und somit Risiken für System-Administratoren;
- ➔ nachteilige Auswirkungen bei arbeitsrechtlichen Auseinandersetzungen;
- ➔ evtl. problematische Mitbestimmungsprozesse;
- ➔ externe „Prüfungen“: Wirtschaftsprüfer, Kunden etc.
- ➔ mögliche Schadensersatzansprüche von Betroffenen;
- ➔ etc.



DATENSCHUTZ

Spitzel am Arbeitsplatz

VON KAI BIERMANN UND KARSTEN ... NEWSKI | © ZEIT online
27.3.2008 - 06:10 Uhr

Q: Zeit-online; 27.03.2008



21.10.2008

Drucken | Senden | Bookmark | Feedback | M

NACH PANNENSERIE

Schrift:

Telekom beruft neuen Datenschutz-Vorstand

Die Datenpannen bei der Telekom haben Konsequenzen: Nach langen Debatten hat der Konzern nun einen Datenschutz-Vorstand bestellt: Den bisherigen Chefjustiziar Manfred Balz.

Q: spiegel-online; 21.10.2008

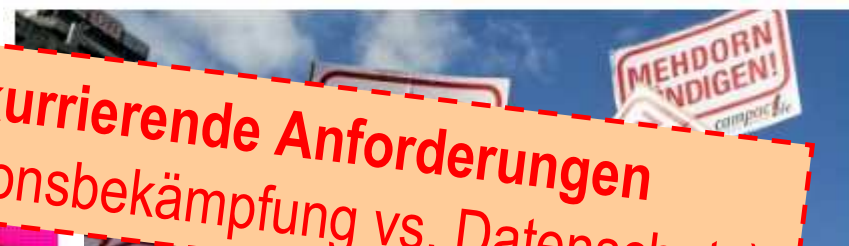
AUFKLÄRUNG

Bahn gibt Ermittlungen in Datenschutz-Affäre ab

18. Februar 2009, 20:51 Uhr

Nach immer neuen Enthüllungen in der Datenschutz-Affäre werden dem Vorstand der Deutschen Bahn die Ermittlungen aus der Hand genommen. Stattdessen soll im Auftrag des Aufsichtsrats ein unabhängiges Gremium die Affäre aufklären. Wer zu den Ermittlern gehören wird, ist auch schon klar.

**z. T. konkurrierende Anforderungen
(bspw. Korruptionsbekämpfung vs. Datenschutz)**



Vaduz ermittelt gegen BND-Informanten

Die Staatsanwaltschaft in Vaduz hat Ermittlungen gegen den mutmaßlichen Informanten des Bundesnachrichtendienstes BND eingeleitet. International zieht der Steuerskandal derweil immer weitere Kreise.

Q: fokus-online;
27.02.2008



Wesentliche Änderungen durch BDSG-Novelle 2009/2010

- ➔ Präzisierung von Kündigungsschutz und Fortbildungsanspruch des **Datenschutzbeauftragten**
- ➔ **Auftrags-Datenverarbeitung**
 - » Kontrollverpflichtung bei Dienstleister
 - » Anforderung an Vertragsgestaltung umfangreicher
- ➔ **Meldepflicht** an Aufsichtsbehörde und Betroffenen selbst bei „Datenpannen“
- ➔ Änderung bei Datennutzung für **Werbezwecke**, bei Scoring, bei automatisierter Einzelentscheidung etc.
- ➔ **Beschäftigten-Datenschutz**

Die Bestellung eines betrieblichen Datenschutzbeauftragten bereitet oftmals „praktische Schwierigkeiten“

*Landesbeauftragte für Datenschutz und Informationsfreiheit NRW
in ihrem 17. Datenschutzbericht formulierte.*

Grundsätzlich ist die Möglichkeit für die Bestellung
externer Beauftragter... oft eine praktikable Lösung, da
sie... kostengünstiger und fachlich qualifizierter arbeiten.

Oder: Warum Gesetze alleine nicht helfen!?

➔ Bewusstseinsprobleme

» kein Unrechtsbewusstsein

» mangelnde Schulung / Sensibilisierung

➔ Einstellungsprobleme

*Siehe auch Datenschutz-
Studie der UIMCert*

Und was hilft weiter?

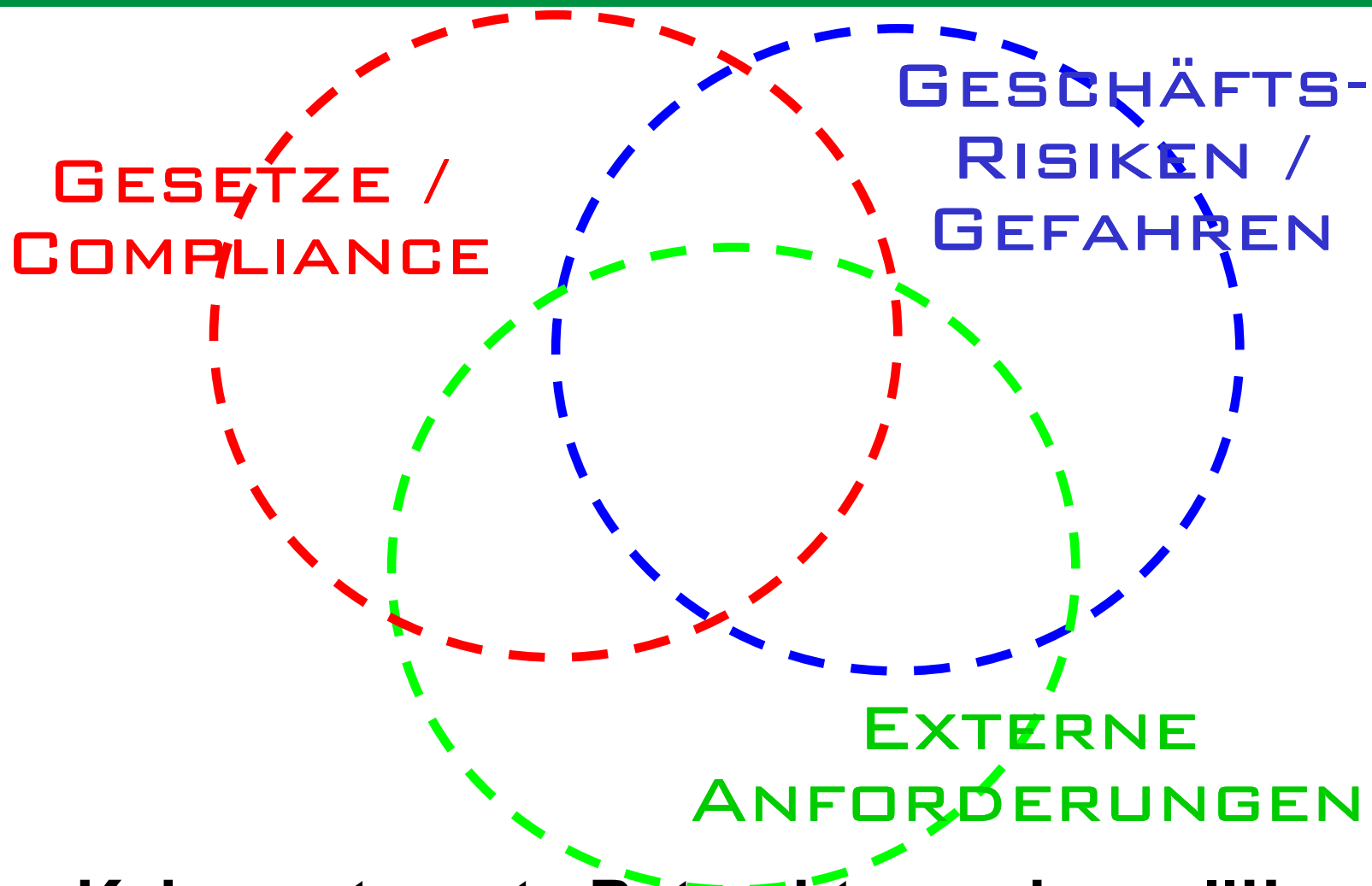
➔ Umsetzung von Standards und Normen

➔ Nutzung von PETs beim Datenschutz

➔ Gutes organisatorisches Informationssicherheitsmanagement

Kunden (B2B / B2C) fordern von ihren Lieferanten zunehmend Zusicherungen einer sicheren EDV!

z. B. fordern einige Automobilhersteller von ihren Zulieferern ein ISO 27001-Zertifikat



Keine getrennte Betrachtung sinnvoll!!

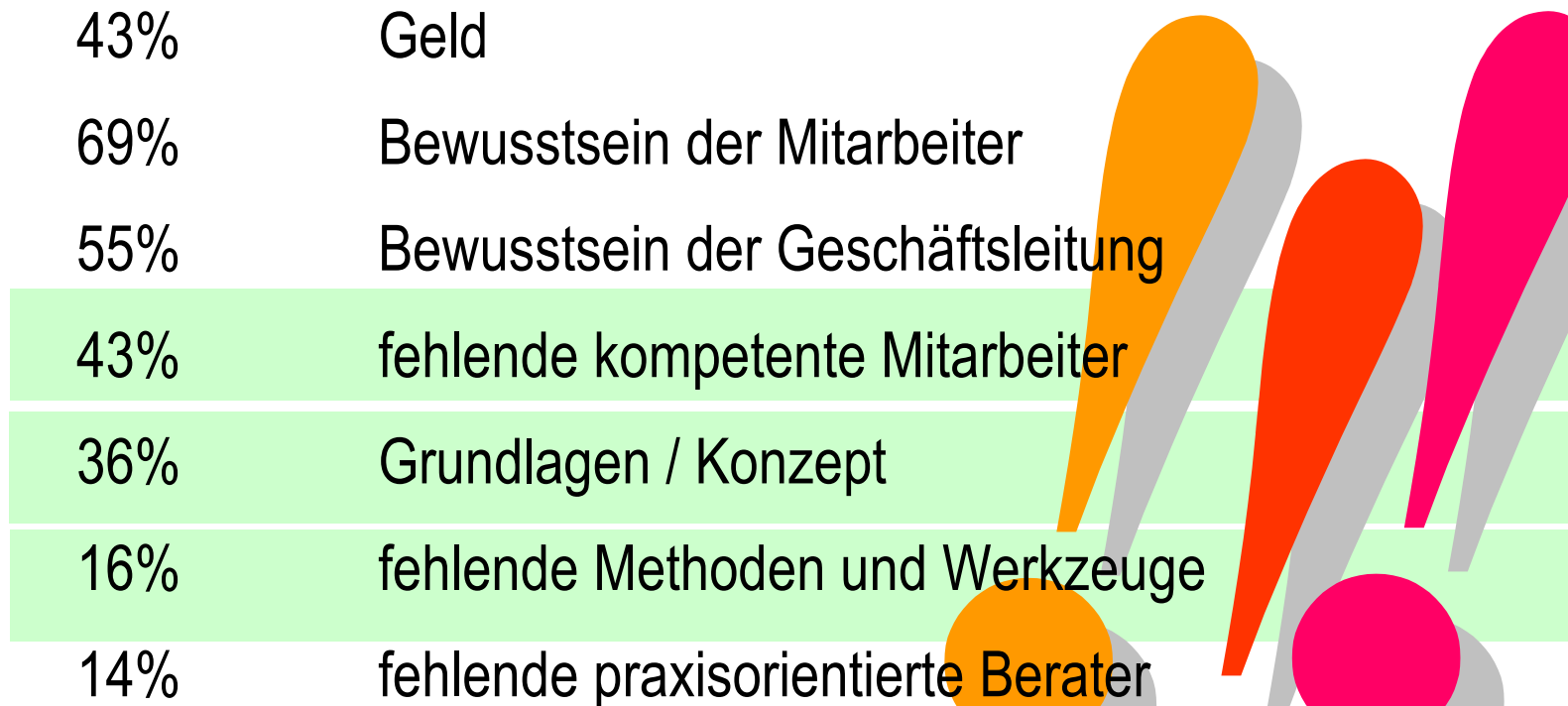
- 1 IT - Faktor für den Unternehmenserfolg
- 2 Compliance: Worthülse oder Managementaufgabe?
- 3 ISO 27001 als Best-Practice-Norm**
- 4 Fazit und Ausblick

Was sagt Wikipedia?

- ➔ Das Managementsystem für Informationssicherheit (engl.: Information Security Management System, ISMS) ist eine Aufstellung von **Verfahren und Regeln** innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit **dauerhaft**
 - » zu definieren,
 - » zu steuern,
 - » zu kontrollieren,
 - » aufrecht zu erhalten und
 - » fortlaufend zu verbessern.

- ➔ Aufbau ist unumgänglich
 - » formale Vorgaben
 - » Risiko-Reduktion im Rahmen des Geschäfts
- ➔ systematische Betrachtung sinnvoll
 - » Schonung der Ressourcen
 - » Verbesserung der Akzeptanz
- ➔ Nutzung von Normen / Checklisten naheliegend („Warum das Rad neu erfinden?“)
 - » ISO 27001
 - » Anlage zu § 9 BDSG
 - » etc.

Behinderung der Verbesserung der Lage



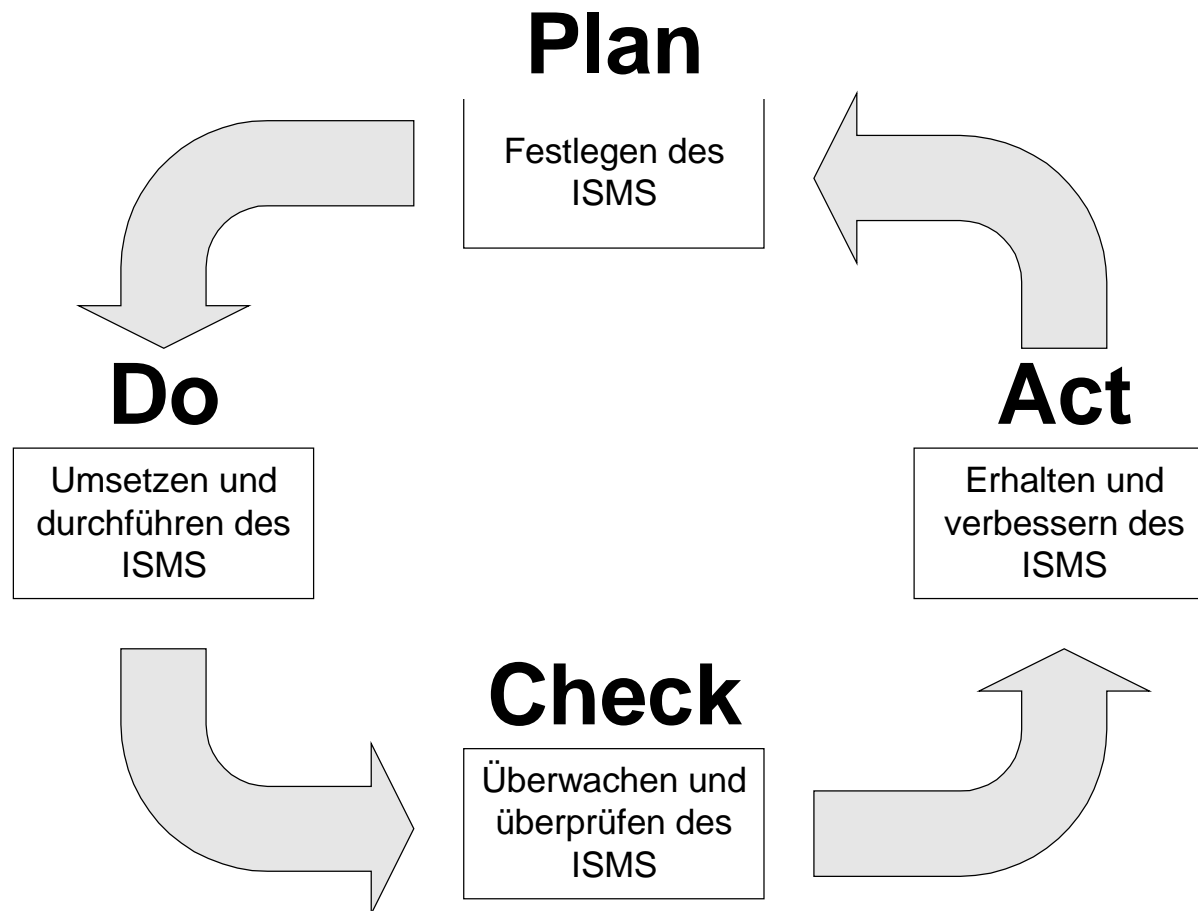
Quelle: KES-Studie 2008



**„Wie kann ich systematisch an
das Thema herangehen?“**

- ➔ internationale Norm
- ➔ als „code of practice“ in der IT-Sicherheit etabliert
- ➔ spezifiziert Anforderungen an ISMS
- ➔ anwendbar in Organisationen jeglicher Art, Ausprägung und Größe
- ➔ mögliche Grundlage für Vertragsbeziehungen zwischen Organisationen
- ➔ Implementierung und den Betrieb von integrierten Managementsystemen für
 - » Qualität (ISO 9001)
 - » Umwelt (ISO 14001)
 - » VDA Prototypenschutz-Katalog

Sicherheitspolitik	Kapitel 3
Organisation der Sicherheit	Kapitel 4
Einstufung und Kontrolle der Werte	Kapitel 5
Personelle Sicherheit	Kapitel 6
Physische und umgebungsbezogene Sicherheit	Kapitel 7
Management der Kommunikation und des Betriebs	Kapitel 8
Zugangskontrolle	Kapitel 9
Systementwicklung und -wartung	Kapitel 10
Management des kontinuierlichen Geschäftsbetriebs	Kapitel 11
Einhaltung der Verpflichtungen	Kapitel 12



Anders als z. B. beim BSI Grundschutz wird nicht jede einzelne Anwendung, jedes einzelne Subsystem oder jede Datei auf das spezifische Risiko untersucht

6 Schritte des Risikomanagements

- ➔ Risikoidentifikation
- ➔ Risikobewertung
- ➔ Identifikation und Bewertung der Möglichkeiten, mit Risiken umzugehen
- ➔ Auswahl von Maßnahmenzielen und Maßnahmen
- ➔ Erstellen eines Eignungsberichts
- ➔ Managementfreigabe

Umsetzung der Planung

- ➔ Management der Plan-Umsetzung
- ➔ Ressourcenmanagement
- ➔ Zeitmanagement
- ➔ Schulungsmanagement

Überwachung und Überprüfung des ISMS (Check)

➔ Überwachung

- » Kontrolle des laufenden Betriebs des ISMS

➔ Überprüfung

- » Kontrolle der Effektivität des ISMS im Rahmen eines Reviews

➔ Restrisiko

- » (regelmäßige) Kontrolle des verbleibenden und akzeptierten Restrisikos

Phase der Verbesserung (Act)

ISO 27001-02

- ➔ international geprägt und anerkannt
- ➔ Orientierung am allgemeinen Normenaufbau
- ➔ Risiko-Orientierung (inkl. Wahrscheinlichkeit)
- ➔ PDCA für gesamtes Managementsystem
- ➔ Orientierung an kritischen Geschäftsprozessen

BSI Grundschatz

- ➔ nationale Prägung und Anerkennung
- ➔ stark von allgemeinen ISO-Normen abweichend
- ➔ einfache Betrachtung der Gefährdungen
- ➔ PDCA nur für das IT-Sicherheitskonzept
- ➔ Basis: GS-Kataloge und Schichtenmodell

- ➔ Mühselige Erarbeitung einer umfassenden Checkliste
- ➔ Unangemessenheit in der Status-Quo-Feststellung
- ➔ Gefahr der Betriebsblindheit
- ➔ Ineffizienz während des Erhebungsprozesses
- ➔ Unrationelle Auswertung
 - » schwerfällige Berichterstellung
 - » wenig transparente Darstellungsform
 - » problematische Ableitung von Maßnahmen zur Kompensation der Schwachstellen

**„Mancher ertrinkt lieber,
als daß er um Hilfe ruft!“**

(Wilhelm Busch)

➔ Rationalisierung durch Computerunterstützung

- » Erhebung des Status quo
- » Auswertung
- » Berichterstellung
- » Ableitung von Maßnahmen zur Kompensation

7.1.2. Physische Zutrittskontrollen zur Sicherheitszone

1. Wird der Zutritt zu Sicherheitszonen durch Kontrollen überwacht?

Ja

Nein

➔ Quantifizierbarkeit

- » Schaffung von Transparenz durch graphische Darstellung
- » Vergleichbarkeit der Ergebnisse
- » verbesserte Promotion

➔ auch als (regelmäßiger) Selbst-Checkup

- 1 IT - Faktor für den Unternehmenserfolg
- 2 Compliance: Worthülse oder Managementaufgabe?
- 3 ISO 27001 als Best-Practice-Norm
- 4 Fazit und Ausblick**

Gründe für ein ISMS nach ISO 27001-02

- ➔ Reduzierung der Haftungsrisiken
- ➔ Benchmark zur „State of the art“
- ➔ Gedanke des Qualitätsmanagement
 - » „Wer schreibt, der bleibt!“
- ➔ Verbesserung der Compliance-Situation
 - » Sicherstellung der Einhaltung von rechtlichen Vorgaben
 - » Erfüllung von vertraglichen Vorgaben von Kunden
- ➔ Last, but not least:
 - » Sicherung des Geschäfts

Gute Gründe für ein Audit / Checkup / Zertifizierung

- ➔ Vollständige Prüfung des Status quo in der IT-Sicherheit
- ➔ **Dokumentation**
 - » der Bemühungen durch anerkannte Norm
 - » der Ordnungsmäßigkeit des IT-Systems
- ➔ Zugriff auf ein **praxisbewährtes** Instrumentarium
- ➔ **Neutrale Bewertung**
- ➔ **Strukturierung** der Maßnahmenplanung durch Priorisierung
- ➔ Interne **Promotion** des IT-Sicherheitsgedankens durch quantitative Auswertung



Fragen?

Aufmerksamkeit!

Diese und zusätzliche
Folien im Downloadbereich!

UIMC[®]

DR. VOSSBEIN
GmbH & Co KG

UIMC Dr. Vossbein GmbH & Co. KG

Nützenberger Straße 119

42115 Wuppertal

Telefon: (0202) 265 74 - 0

Telefax: (0202) 265 74 - 19

E-Mail: consultants@uimc.de

URL: www.UIMC.de

Neu!
UIMCollege[®]

UIMCert[®]
GMBH

UIMCert GmbH

Moltkestraße 19

42115 Wuppertal

Telefon: (0202) 3 09 87 39

Telefax: (0202) 3 09 87 49

E-Mail: certification@uimcert.de

URL: www.UIMCert.de

WANTED



erfahrene Datenschützer und IT-Sicherheitsfachleute!

Die Gesuchten sind bewaffnet mit:

- Analyse-Instrumenten (z. B. Datenschutz-Checkup),
- praxiserprobten Organisationsmitteln,
- computergestütztem Verfahrensverzeichnis,
- multimedialer Lern-CD,
- und einigem mehr...

Den Gesuchten wird vorgeworfen:
- jahrelange Erfahrungen im Datenschutz-
und IT-Sicherheitssektor,

- Beratungserfolge in einer Vielzahl von
Institutionen,
- effiziente und effektive Vorgehensweisen
bei Ihren Taten ...

Vorsicht:
Die Gesuchten sind erfahren in dem, was
sie tun und haben Komplizen in der UIMC!

UIMC®

DR. VOSSBEIN
GmbH & Co KG

**SACHDIENLICHE ANFRAGEN
WERDEN MIT UNVERBINDLICHEN
INFORMATIONEN BELOHNT!**

UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (0202) 265 74 - 0
Fax: (0202) 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

+++ Datenschutz +++ IT-Sicherheit +++ Business Continuity +++ Management +++ Zertifizierungen +++
++ Beratung ++ Seminare ++ Auditierung ++ Lern-Software ++ Analyse-Tools ++ Coaching ++ Beratung

UIMC[®]

DR. VOSSBEIN
GmbH & Co KG

**Unternehmens- und
Informations- Management
Consultants**

Die UIMC-Gruppe

*Eine starkes Team bei Beratung,
Audierung, Zertizierung und Schulung*

Internet: www.UIMC.de
E-Mail: consultants@UIMC.de

Nützenberger Straße 119
42115 Wuppertal

Telefon: 0202 - 265 74 - 0
Telefax: 0202 - 265 74 - 19



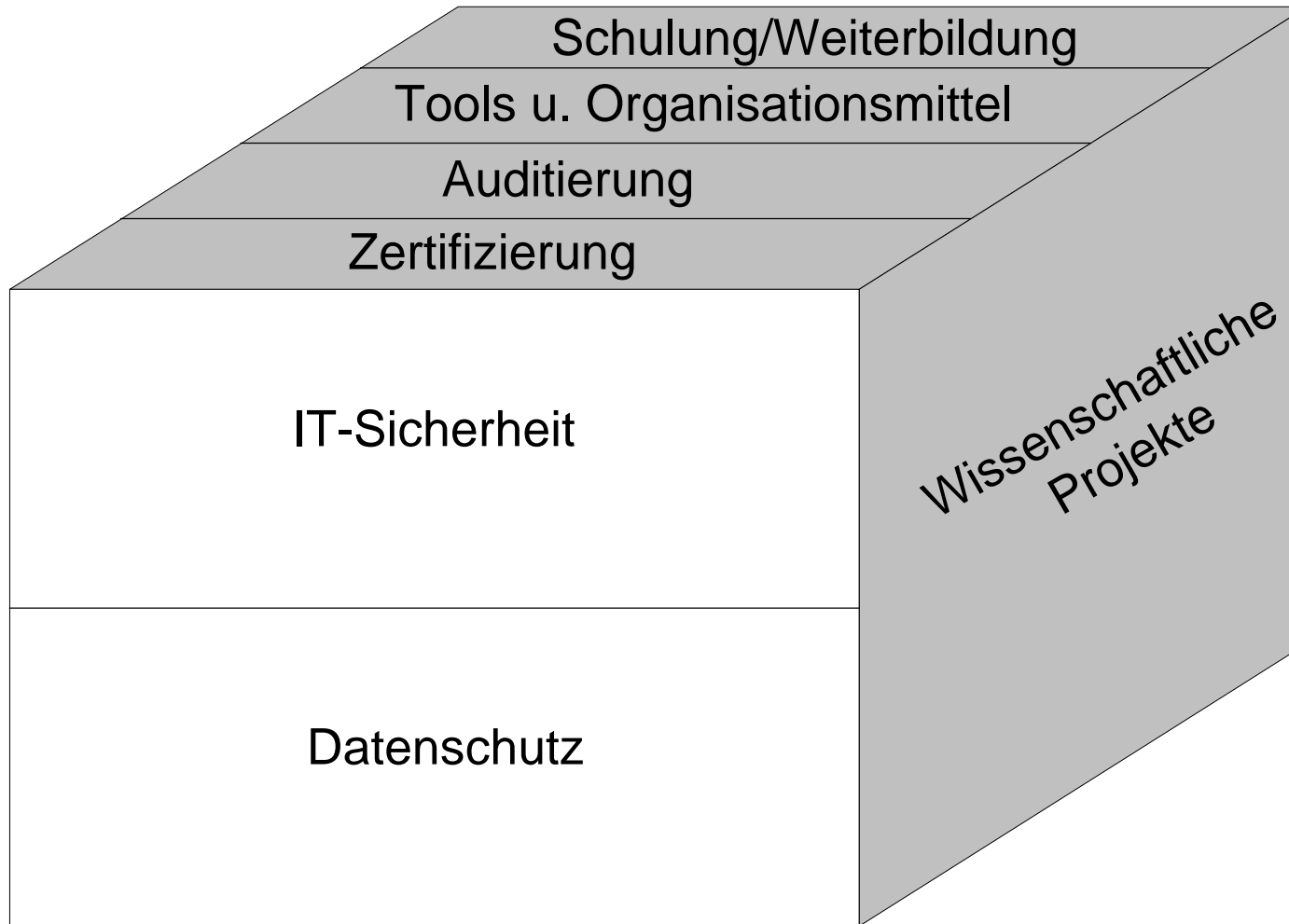
66,7 %



**Akkreditiert u. a. für ISO 27001
(inkl. Prototypenschutz)!**

**auch speziell für KMU:
Low-Budget-Konzept**

Individuelle Beratungen und Konzeptionen Unternehmensmanagement	Standardisierte Beratungen und Konzeptionen	Individuelle Beratungen und Konzeptionen IT-Management	Betriebliche und außerbetriebliche Fort- und Weiterbildung
Unternehmensführung	UMC - Unternehmens- und Management-Checkup	IT-Sicherheit	Unternehmensorganisation
Controlling		IT-Revision (Auditing)	Unternehmensplanung und -budgetierung
Aufbau- und Ablauforganisation	Sicherheits-Schwachstellen-analyse (Si-SSA) gem. ISO 17799/27001	Datenschutzberatung	IT-Systemplanung
Planung und Budgetierung		Externe Datenschutz-beauftragung	IT-Controlling
Informationssystem-management	Datenschutz-Checkup gem. BDSG und IuKDG	Datenschutz- und -sicherheit im Gesundheitssektor	Datenschutz
Marketing		Erstellen und Überprüfen von Pflichtenheften	Sicherheitskonzeptionen
	Organisationsmittel		Arbeitsplatzsicherheit
			ISO 27001
SW-Lösungen für interne und externe Beratungs- und Auditierungsprojekte			



- ➔ ... ist ein mittelständiges Beratungsunternehmen
- ➔ ... wurde durch Prof. Reinhard Voßbein und Dr. Jörn Voßbein im Jahre 1997 gegründet
- ➔ ... hat seinen Sitz in Wuppertal
- ➔ ... verfügt über ein breites Dienstleistungsangebot:
 - » Datenschutz;
 - » IT-Sicherheit;
 - » Notfallmanagement;
 - » Penetrationstest;
 - » Organisation/Management;
 - » Auditierung/Zertifizierungsvorbereitung;
 - » etc.

- ➔ ... ist führend auf den Gebieten der IT-Sicherheit und des Datenschutzes
 - » Auditierung
 - » Testierung
 - » Zertifizierung
- ➔ ... hat seit 1999 Vielzahl an Referenzen aufzuweisen
- ➔ ... hat seinen Sitz in Wuppertal
- ➔ ... verfügt über ein breites Angebot:
 - » ISO 27001
 - » Datenschutz-Produkt- und Verfahrens-Audit gemäß LDSG SH
 - » IDW-PS 330/331
 - » IDW PS 880

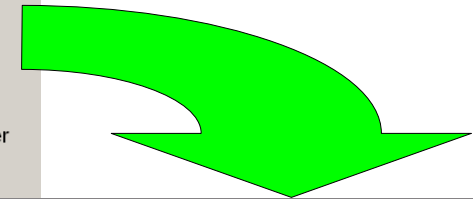
UIMC One Purpose Tool MultiDB - 4.Sonderformen der Datenverarbeitung (Frage im aktuellen Kapitel: 1 von 7 insgesamt 266)

Datel Frage Extras Hilfe

1

4.3. Mobile personenbezogene Speicher- und Verarbeitungsmedien gem. § 6c BDSG

1. Werden mobile personenbezogene Speicher- und Verarbeitungsmedien eingesetzt bzw. ist der Einsatz geplant?



2. Unternehmens- und Informations-Management Consultants UIMC[®]

Datenschutz-Schwachstellenbericht

...ung kommen, grundsätzlich unterschrieben worden.

Es wird vor der Verpflichtungserklärung bezüglich des Datengeheimnisses keine von den betroffenen Mitarbeitern schriftlich bestätigte Datenschutzunterweisung vorgenommen.

1.10 DV-Systeme

Es ist nicht durch schriftliche Anweisungen gewährleistet, dass sich die Gestaltung und Auswahl von DV-Systemen an dem Ziel ausrichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

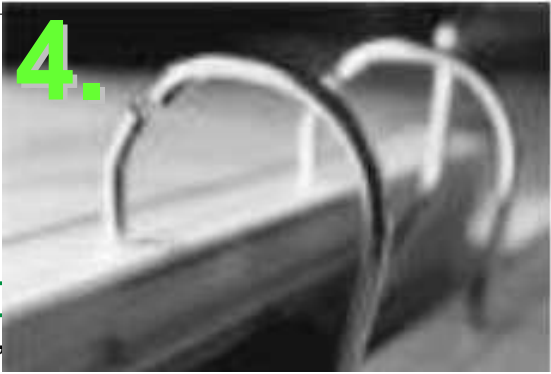
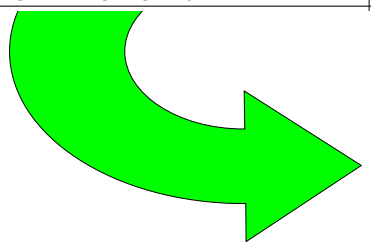
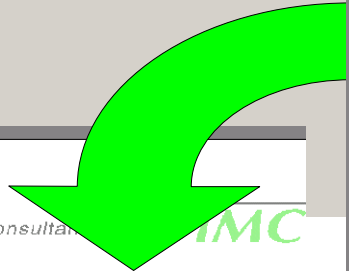
Es ist nicht gewährleistet, dass die Verarbeitung personenbezogener Daten...

Der Einsatz datenschutz-zert...
Die DV-Anlagen (PC, Druck...
zung zur Verfügung gestellt

3. Unternehmens- und Informations-Management Consultants UIMC[®]

Strukturierter Maßnahmenkatalog

Kapitel/Maßnahme	Prio.	Verantw.	Datum	Bemerkung
3 Technische und organisatorische Maßnahmen				
Es ist systemtechnisch sicherzustellen, dass der Nutzer sein Passwort bei Bedarf ändern kann.	1	EDV		Siehe Datenschutzhandbuch (Kapitel 5.4)
Die Passwortlänge ist systemtechnisch auf mindestens acht Zeichen festzulegen.	1	EDV		Siehe Datenschutzhandbuch (Kapitel 5.4)
Es ist sicherzustellen, dass eine Passworthistory verwendet wird. Ferner ist sicherzustellen, dass die Verwendung des alten Passwortes systemtechnisch unterdrückt wird, wenn das alte Passwort ein zweites Mal verwendet werden soll.	1	EDV		Siehe Datenschutzhandbuch (Kapitel 5.4)
Es sind für Anwender- und Systempasswörter Passwortwechsellhythmen festzulegen. Die Anwenderpasswörter sind alle sechs Wochen, die Systempasswörter sind monatlich zu wechseln.	1	EDV		Siehe Datenschutzhandbuch (Kapitel 5.4)
Den Systemverwaltern sind Anweisungen zu erteilen, dass das System so zu konfigurieren ist, dass keine Möglichkeit zur Eingabe sog. Trivialpasswörter besteht.	1	EDV		Siehe Datenschutzhandbuch



5. Betrieblicher Datenschutz UIMC[®]

Spezielle Problemfelder im Arbeitnehmerdatenschutz

Veröffentlichungen im Internet

- sofern das Bild eines Mitarbeiters im Internet veröffentlicht werden soll, so ist dies gemäß § 22 Kunsturhebergesetz **nur mit Einwilligung** des Abgebildeten gestattet.

private E-Mail- und Internetnutzung

- Diese sollte generell, idealerweise verboten werden. Sofern die E-Mail- und Internetnutzung zu privaten Zwecken zur Verfügung gestellt würde (oder nicht explizit verboten wird, sind die Regelungen des TKG, TDG und TDDSG zu beachten, die eine Einschränkung der Datenverbreiten (E-Mails oder Protokollidale) und spezielle Schutzmaßnahmen fordern.

Leistungs- und Verhaltenskontrolle

- sofern Protokolldaten erstellt werden (bspw. zur Datenschutzkontrolle oder zur Sicherstellung des ordnungsgemäßen Betriebs der EDV), dürfen diese Daten aufgrund der „besonderen Zweckbindung“ (§31 BDSG) **nicht** zur Leistungs- und Verhaltenskontrolle herangezogen werden.



Informationssicherheit,

Managementaufgabe

ZURÜCK

7.1.2. Physische Zutrittskontrollen zur Sicherheitszone

1. Wird der Zutritt zu Sicherheitszonen durch Kontrollen überwacht?

**Vorstrukturierte
Fragen**

Ja

Nein

Individualisierungsmöglichkeit



ZURÜCK

2. Beschreibung des IT-Systems

6. Treffen folgende Aspekte auf Ihr Unternehmen zu?

- interne Entwicklung von Software / Einsatz von Open-Source-Software
- Mobile Computing (z. B. Nutzung von Laptops, PDAs)
- Teleheimarbeit (z. B. Arbeiten in der Wohnung des Mitarbeiters)
- Externe Wartung der EDV/IT durch einen Dienstleister

- 9.4 Netzzugriffskontrolle
- 9.5 Kontrolle des Betriebssystemzugriffs
- 9.6 Zugriffskontrolle für Anwendungen
- 9.7 Überwachung des Systemzugriffs und der Systembenutzung
- 9.8 Mobile Computing und Telearbeit
 - 9.8.1 Mobile Computing
 - 9.8.2 Telearbeit

ZURÜCK

Qualitative Auswertung:

Es wird ein rtf-Dokument erzeugt, welches positive und negative Befunde enthält, aber auch Maßnahmenempfehlungen zur Beseitigung etwaiger Schwachstellen



Quantitative Auswertung:

Alle Fragen / Kapitel sind quantifiziert und gewichtet; durch den Export in xls ist eine problemlose, beliebige Auswertung der Ergebnisse möglich (inkl. Benchmarking)

Unternehmens- und Informations-Management Consultants



3 Technische und organisatorische Maßnahmen

3.1 Zutrittskontrolle

Es bestehen nur teilweise spezielle Richtlinien, die den Zutritt zu IT-Systemen regeln: Der Zutritt ins Gebäude ist geregelt, der Zutritt zu den Büros aber nicht.

Es sind Sicherheitszonen definiert.

Das Betreten und Verlassen der Sicherheitszonen wird restriktive Schlüsselvergabe vorgenommen. Für die Zutritte...

Das Betreten und Verlassen der Sicherheitszonen wird protokolliert. In Zukunft soll dies aber gew...

Dem Wartungs- und Reinigungspersonal ist der Zutritt durch autorisiertes Personal möglich.

Es ist nicht sichergestellt, dass sich nie weniger als zwei Personen in den Sicherheitszonen aufhalten.

3.2 Zugangskontrolle

Spezielle Richtlinien, die den Zugang zu IT-Systemen regeln. Beispielsweise Richtlinien dahingehend, dass Büroräume oder Unterlagen/Schränke beim Verlassen zu verschließen sind.

Es ist sicherzustellen, dass das Betreten und Verlassen der Sicherheitszonen für jede einzelne Person mit Namen und Zeiten ständig protokolliert wird.

Es ist durch Anweisung sicherzustellen, dass sich stets mindestens zwei Personen in den Sicherheitszonen aufhalten.

3.2 Zugangskontrolle

Es sind alle identifikations-/authentifizierungspflichtigen IT-Komponenten vollständig festzulegen.

Die Bedingungen und Formen der Identifikation/Authentifizierung sind schriftlich festzulegen.

Es sind Anweisungen zu erteilen, dass die Zugangsberechtigungen zeitlich begrenzt zu vergeben sind.

Es sind Anweisungen zu erteilen, dass die zuständige Person alle Zugriffsrechte immer an veränderte Aufgabenstellungen anzupassen und zu dokumentieren hat.

Es sind Anweisungen zu erteilen, dass alle Zugriffsrechte immer auf Richtigkeit und Gültigkeit durch die zuständige Person zu überprüfen und ggf. zu aktualisieren sind.

Es sind Richtlinien, die die Wartung/Fernwartung regeln, herauszugeben. Es ist u. a. festzulegen, dass den Servicekräften zeitlich eingeschränkte Zutritts-, Zugangs- oder Zugriffsrechte zu gewährleisten sind. Die erteilten Zutritts-, Zugangs- oder Zugriffsrechte sind nach Beendigung der Wartungsarbeiten zu löschen.

Unternehmens- und Informations-Management Consultants



Kapitel/Maßnahme	Prio.	Verantw.	Datum	Bemerkung
3 Technische und organisatorische Maßnahmen				
3.1 Zutrittskontrolle				
Es sind spezielle Richtlinien herauszugeben, die den Zutritt zu IT-Systemen regeln. Beispielsweise Richtlinien dahingehend, dass Büroräume oder Unterlagen/Schränke beim Verlassen zu verschließen sind.	1	GL/DSB		Siehe Datenschutzhandbuch (Kapitel 5.1)
Es ist sicherzustellen, dass das Betreten und Verlassen der Sicherheitszonen für jeden Einzelnen ständig kontrolliert wird.	1	EDV		Siehe Datenschutzhandbuch (Kapitel 5.5)
Es ist sicherzustellen, dass das Betreten und Verlassen der Sicherheitszonen für jede einzelne Person mit Namen und Zeiten ständig protokolliert wird.	3	EDV		Siehe Datenschutzhandbuch (Kapitel 5.5)
Es ist durch Anweisung sicherzustellen, dass sich stets mindestens zwei Personen in den Sicherheitszonen aufhalten.	2	GL/EDV		Siehe Datenschutzhandbuch (Kapitel 5.5)
3.2 Zugangskontrolle				
Es sind alle identifikations-/authentifizierungspflichtigen IT-Komponenten vollständig festzulegen.	3	GL/EDV		Siehe Datenschutzhandbuch (Kapitel 5.2)
Die Bedingungen und Formen der Identifikation/Authentifizierung sind schriftlich festzulegen.	1	AL/DSB		Siehe Datenschutzhandbuch (Kapitel 5.2)
Es sind Anweisungen zu erteilen, dass die Zugangsberechtigungen zeitlich begrenzt zu vergeben sind.	2	AL/DSB		Siehe Datenschutzhandbuch (Kapitel 5.2)
3.3 Zugriffskontrolle				
Es sind Anweisungen zu erteilen, dass die zuständige Person alle Zugriffsrechte immer an veränderte Aufgabenstellungen anzupassen und zu dokumentieren hat.	2	AL/DSB		Siehe Datenschutzhandbuch (Kapitel 5.3)
Es sind Anweisungen zu erteilen, dass alle Zugriffsrechte immer auf Richtigkeit und Gültigkeit durch die zuständige Person zu überprüfen und ggf. zu aktualisieren sind.	2	AL/DSB		Siehe Datenschutzhandbuch (Kapitel 5.3)
Es sind Richtlinien, die die Wartung/Fernwartung regeln, herauszugeben. Es ist u. a. festzulegen, dass den Servicekräften zeitlich eingeschränkte Zutritts-, Zugangs- oder Zugriffsrechte zu gewährleisten sind. Die erteilten Zutritts-, Zugangs- oder Zugriffsrechte sind nach Beendigung der Wartungsarbeiten zu löschen.	2	GL/DSB		Siehe Datenschutzhandbuch (Kapitel 4.3 und 5.8)
Es ist sicherzustellen, dass Remote-Wartung durch externe Firmen in Anwesenheit...	2	EDV		Siehe Datenschutzhandbuch

ZURÜCK

Executive Information System

- 4 Organisation der Sicherheit
- 5 Einstufung und Kontrolle der Werte
 - 5.1 Zurechenbarkeit für Werte
 - 5.2 Einstufung von Informationen
- 6 Personelle Sicherheit
- 7 Physische und umgebungsbezogene Sicherheit
 - 7.1 Sicherheitszonen
 - 7.1.1 Physische Sicherheitsgrenze
 - 7.1.2 Physische Zutrittskontrollen
 - 7.1.3 Sicherung von Geschäftsräumen und Gerät
 - 7.1.4 Arbeiten in Sicherheitszonen
 - 7.1.5 Separate Liefer- und Ladebereiche
 - 7.2 Sicherheit der Geräte
 - 7.3 Allgemeine Maßnahmen
- 8 Management der Kommunikation und des Betriebs

Legende

Kapitelebene	Fragenebene
Guter Wert	Guter Wert
Ausreichender Wert	Ausreichender Wert
Ungenügender Wert	Ungenügender Wert
Kapitel beinhaltet keine quantitative auswertbaren Fragen	Frage nicht von quantitativer Art
(Unter)Kapitel beinhaltet kritische Frage	Frage wurde nicht beantwortet
	Kritische Frage

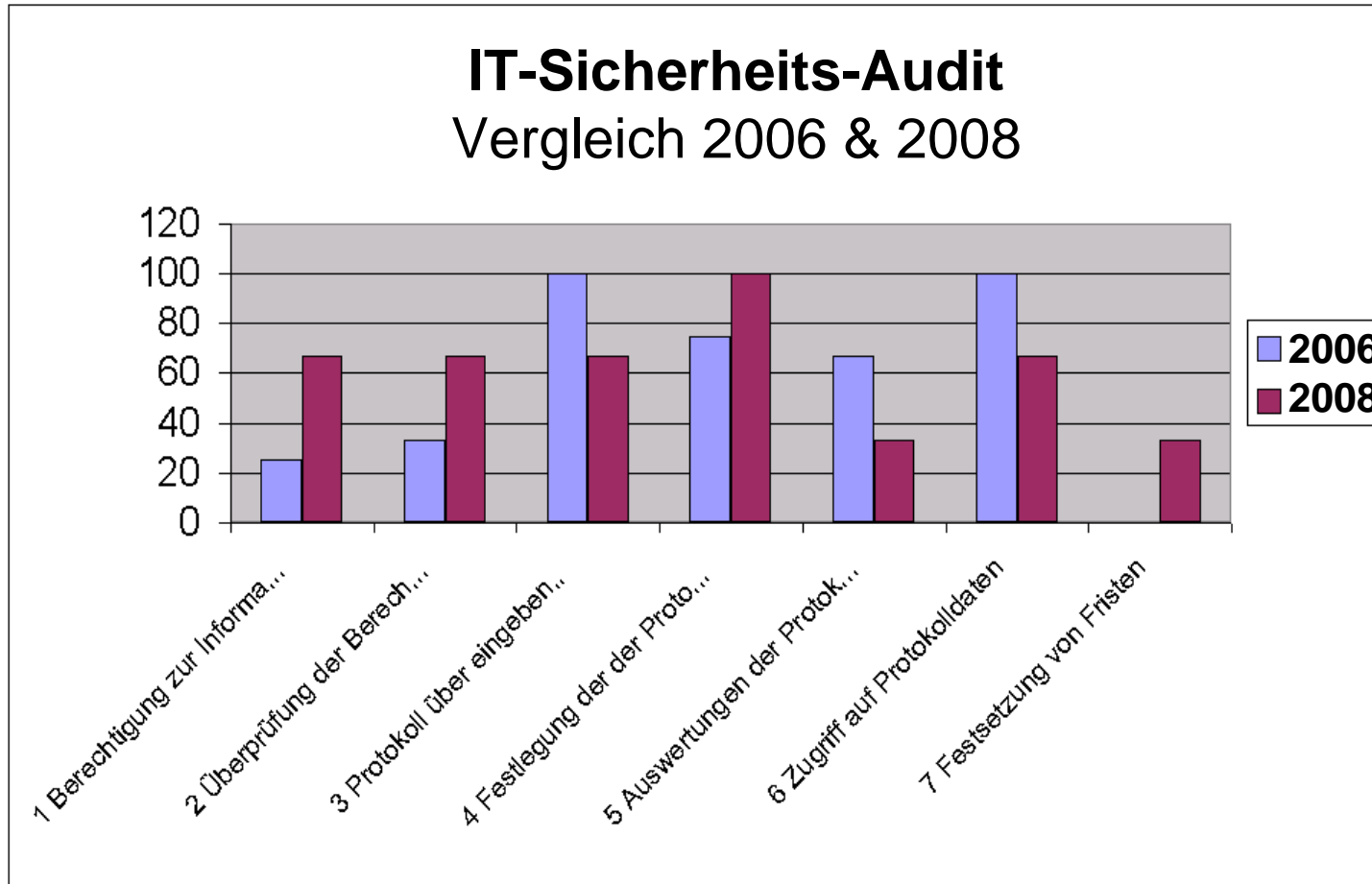
7.1.1 Physische Sicherheitsgrenze
Wert: **82 %**

33 66

Relatives Gewicht von 25 % innerhalb Kapitel "7.1 Sicherheitszonen"
Es wurde ein beantwortetes Kapitel ausgewählt

ZURÜCK

IT-Sicherheits-Audit Vergleich 2006 & 2008



ZURÜCK