



DR. VOSSBEIN
GmbH & Co KG

**Unternehmens- und
Informations- Management
Consultants**

Informationssicherheit und Compliance beim Outsourcing

Neue Herausforderungen durch die BDSG-Novelle

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

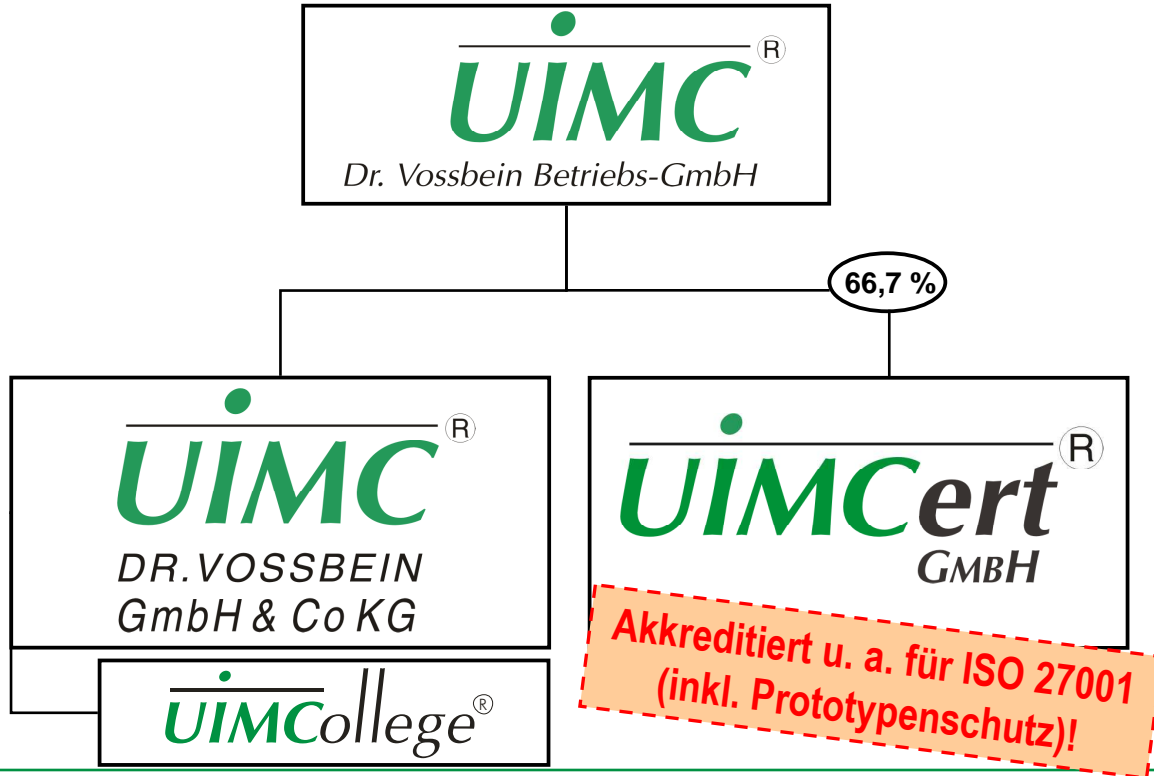


Referent



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
- ➔ Besteller Datenschutzbeauftragter
- ➔ Leiter Arbeitskreis „ISO 27001“ (ruhr networker)



Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing

3

- 1 Outsourcing im Mittelstand / bei KMU
- 2 BDSG-Novelle 2009
- 3 Anforderungen und deren Umsetzung
- 4 Fazit und Ausblick

Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing

4

- ➔ 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)

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

Auswirkungen der Krise in den letzten neun Monaten

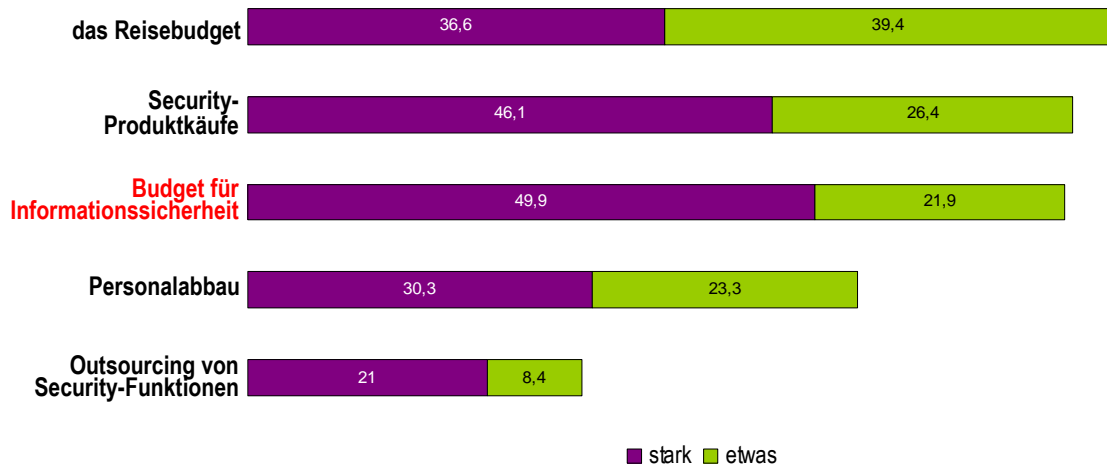


Abb.: Computer Zeitung Ausg. vom 15.06.09, Artikel "Blindes sparen gefährdet Schutz".

Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing

7 7

- » 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)
- » „Bei uns werden alle Berechtigungen zeitlich begrenzt vergeben!“
[beachte: Ablaufdatum laut AD: 31.12.2099]
(EDV-Leitung einer größeren Universitätsklinik)

Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing

8



„Wie kann ich systematisch an das Thema herangehen?“

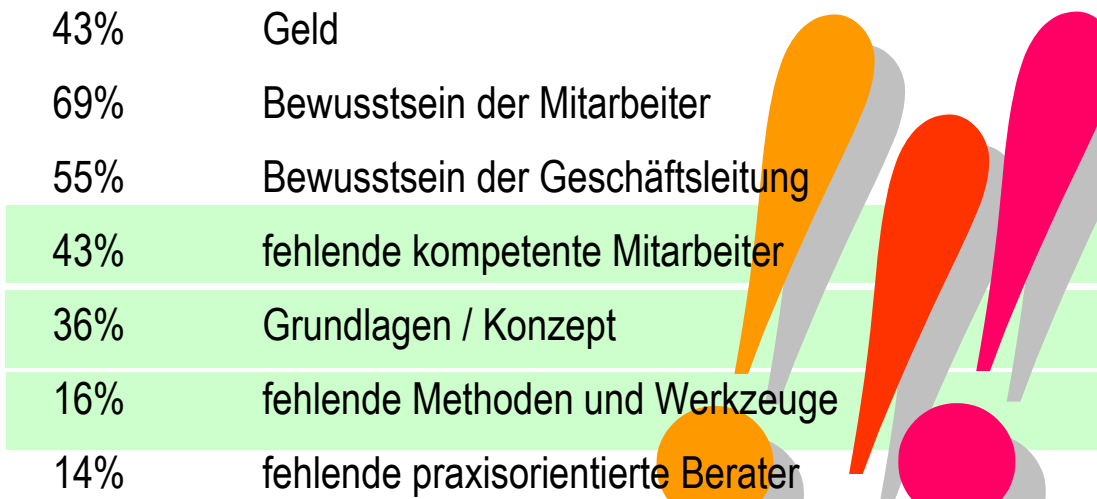
Was sagt Wikipedia?

- ➔ 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.

- ➔ 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

Behinderung der Verbesserung der Lage



Quelle: KES-Studie 2008

Lösungsansatz im Mittelstand/bei KMU!?

*Outsourcing von Diensten,
Service, Support etc.*

Lösungsansatz und neuer Lösungsbedarf!

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, EnWG 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)

➔ BDSG-Novelle II (seit 1.9.2009)

- » Arbeitnehmerdatenschutz
- » Auftragsdatenverarbeitung
- » Personalisierte Werbung
- » Informationspflicht über Datenpannen
- » Datenschutzbeauftragter und Aufsichtsbehörde
- » Bußgelder (Höhe und Tatbestände)
- » kleinere Änderungen (Wording etc.)

➔ Ausblick auf BDSG-Novelle I (ab 1.4.2010)

➔ Ausblick auf BDSG-Novelle III (ab 12.6.2010)

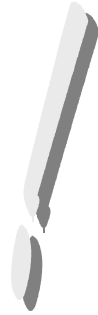
➔ Verantwortung im Datenschutz



„Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt **oder dies durch Andere im Auftrag vornehmen lässt.**“

... durch Andere:

- ➔ rechtlich selbstständig
- ➔ kein Konzern-Privileg:
auch Tochter-/Schwester-/Mutterfirmen
- ➔ Der Auftraggeber eines externen EDV-Dienstleisters bleibt für Ordnungsmäßigkeit verantwortlich!



Liegt auch vor „der Zugriff auf personenbezogene Daten nicht auszuschließen ist“!

Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei **insbesondere im Einzelnen festzulegen sind:**

- 1. der Gegenstand und die Dauer des Auftrags,**
- 2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,**
- 3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen**
- 4. die Berichtigung, Löschung und Sperrung von Daten,**
- 5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,**
- 6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,**
- 7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,**
- 8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,**
- 9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,**
- 10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.**

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich **vor Beginn der Datenverarbeitung und sodann regelmäßig** von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. **Das Ergebnis ist zu dokumentieren.**

Ordnungswidrigkeit nach § 43 Absatz 1 BDSG [Nr. 2b]:

- ➔ Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise **erteilt**
- ➔ nicht **vor Beginn** der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,
- ➔ „kurios“: nicht bußgeld-beweht
 - » kein regelmäßiges „Überzeugen“

- ➔ Existiert ein Überblick über DL-Verhältnisse?
- ➔ Klassifizierung und Priorisierung anhand
 - » Datenkategorien
 - » Dienstleistungsart
 - » grundsätzlich: Kritikalität
- ➔ Welche Änderungen sind in den Verträgen/
Vereinbarungen umzusetzen?
 - » Prüfung der bestehenden Verträge
 - » (sofern erforderlich) Nachverhandlung bei Dienstleister
- ➔ **Beachte:** Es existiert keine Übergangsfrist!

- ➔ Wie sieht das „Überzeugen“ aus?
 - » Vor-Ort-Überprüfung
 - » Audit (auf Basis eines Interviews und von Dokumenten)
 - » Beantwortung eines Fragebogen
 - » Testat eines „unabhängigen“ Sachverständigen
 - » Selbst-Auskunft des Dienstleisters
- ➔ Erarbeitung eines Konzepts („Wer schreibt, der bleibt“):
 - » Verfahren / Vorgehensweise
 - » Intervalle / Regelmäßigkeit
 - » Dokumentationsart
 - » Priorisierung / Umfang

- ➔ Erarbeitung eines Pflichtenhefts für Ausschreibung
 - » Abbildung der „sorgfältigen“ Auswahl
 - » Fokus auf TOMs nach § 9 BDSG
 - » insbesondere bei EDV-Dienstleistern ist ein ISMS nach ISO 27001 ebenfalls begrüßenswert
- ➔ Kombination mit Audit/Audit-Tool
 - » ggf. Quantifizierung: Erreichung eines Mindestmaßes in SLA
 - » aber: „A fool with a tool remains a fool“
- ➔ Erarbeitung eines (neuen) Vertragsmusters
 - » Mindest-Inhalte einen Dienstleister-Vertrag
 - » Integration des Datenschutzes in Beschaffungsprozesse

„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
- ➔ Quantifizierbarkeit
 - » Schaffung von Transparenz durch graphische Darstellung
 - » Vergleichbarkeit der Ergebnisse
 - » verbesserte Promotion
- ➔ auch als (regelmäßiger) Selbst-Checkup

7.1.2. Physische Zutrittskontrollen zur Sicherheitszone

1. Wird der Zutritt zu Sicherheitszonen durch Kontrollen überwacht?

Neu: Dienstleister-Audit-Tool

Ja

Gründe für ein (internes) 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

BDSG-Novelle fordert beim Outsourcing

- ➔ schriftliche Verträge mit konkreten Inhalten (§ 11 BDSG)
- ➔ Prüfung / Kontrolle des Dienstleisters
 - » vor Beginn der Datenverarbeitung „und sodann regelmäßig“
 - » Dokumentation der Kontrolle
- ➔ rechtlich eigene Prüfung vor Ort nicht zwingend erforderlich
 - » Auditierung / Testierung des Dienstleisters möglich
 - » ISO 27001 gute Voraussetzung, aber im konkreten Fall nicht ausreichend (Einzelfallprüfung!)
- ➔ Kontrolle aber auch aus „Eigennutz“ sinnvoll
 - » eigene Prüfung mittels Checkliste oder Audit-Tool



Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing



Vielen Dank für Ihre Aufmerksamkeit!

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

UIMCollege[®]

UIMC[®]cert
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

UIMC[®]

DR. VOSSBEIN
GmbH & Co KG

**Unternehmens- und
Informations- Management
Consultants**

Die UIMC-Gruppe
*Eine starkes Team bei Beratung,
Audierung, Zertifizierung 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

UIMCcert[®]
GMBH

Unternehmensgruppe

UIMC[®]

UIMC[®]

Dr. Vossbein Betriebs-GmbH

66,7 %

UIMC[®]

DR. VOSSBEIN
GmbH & Co KG

UIMCollege[®]

UIMCcert[®]
GMBH

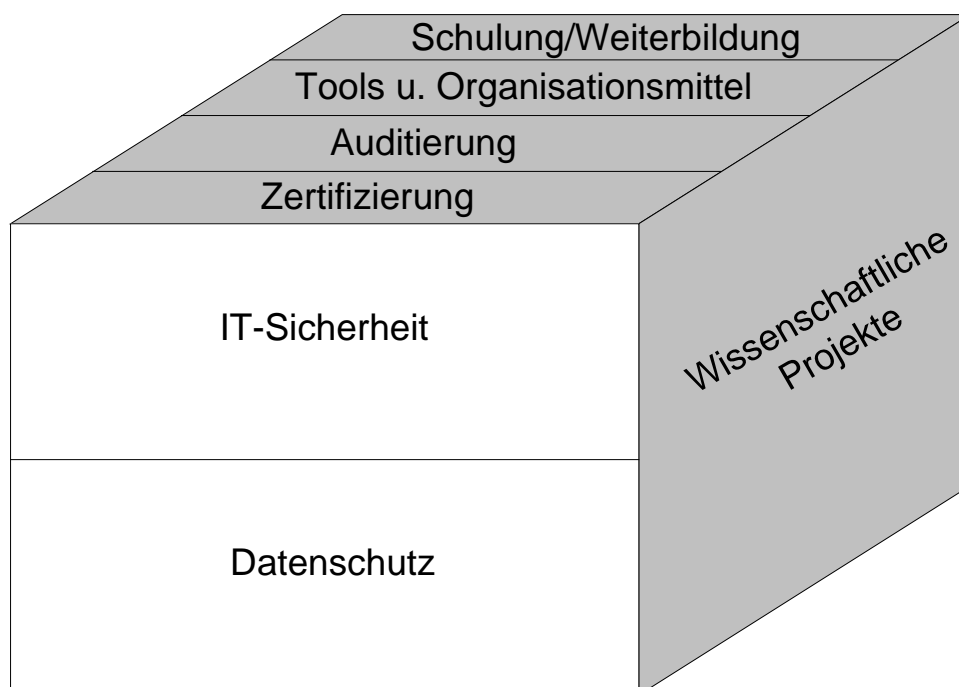
**Akkreditiert u. a. für ISO 27001
(inkl. Patentschutz)!**

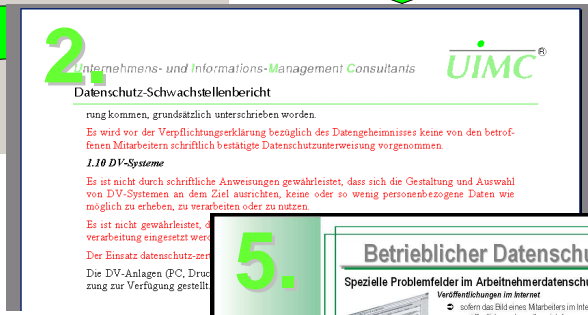
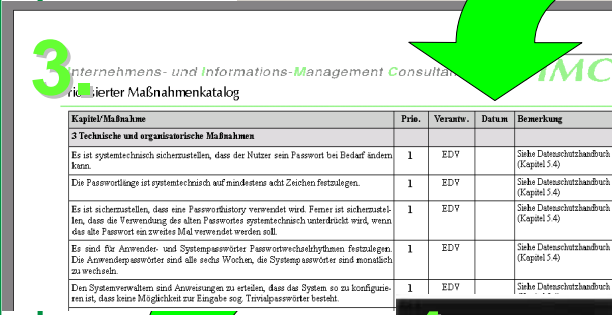
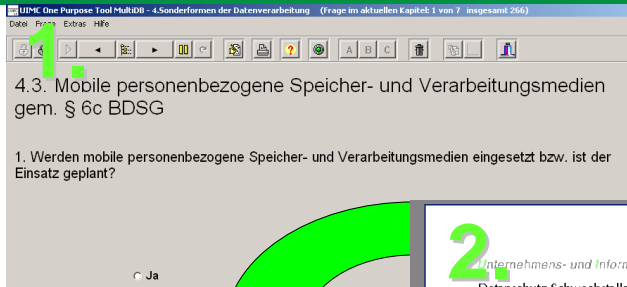
- ... ist ein mittelständiges Beratungsunternehmen
- ... wurde durch Prof. Reinhard Voßbein und Dr. Jörn Voßbein im Jahre 1997 gegründet
- ... hat seinen Sitz in Wuppertal
- ... verfügt über ein breites Dienstleistungsangebot:
 - » Datenschutz;
 - » IT-Sicherheit;
 - » Notfallmanagement;
 - » Penetrationstest;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

**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 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





Die neue § 11 BD

Outsourcing

UIMC-Tool zur Analyse und Berichterstellung

- ➔ **Datenschutz-Checkup**
 - » auch für KMU
 - » Bundes-/Landes-/Kirchenrecht
 - » branchenspezifische Lösungen
- ➔ **neu: Dienstleister-Checkup**
 - » Überprüfung eines Auftragnehmers bei einer Auftrags-Datenverarbeitung nach § 11 BDSG
- ➔ **IT-Sicherheits-Schwachstellenanalyse (SiSSA)**
 - » u. a. nach ISO 27001
- ➔ **Zertifizierungsvorbereitung, Re-Audits etc.**

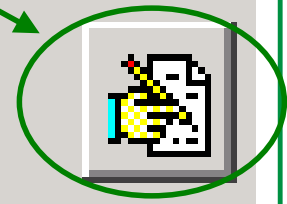
7.1.2. Physische Zutrittskontrollen zur Sicherheitszone

1. Wird der Zutritt zu Sicherheitszonen durch Kontrollen überwacht?

Vorstrukturierte Fragen

Ja Nein

Individualisierungsmöglichkeit



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

Überspringen nicht
notwendiger Fragen/Kapitel

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

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 restriktiv Schlüsselvergabe vorgenommen. Für die Z...

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

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

Es ist nicht sichergestellt, dass sich nie weniger als...

3.2 Zugangskontrolle

Spezielle Richtlinien, die den Zugang zu IT-Systemen...

Unbefugten wird der Zugang zu den Datenverarbeitung...

gene Daten verarbeitet werden, grundsätzlich verweh...

Vergabe, Änderung und Entzug von Zugangsrechte...

Person.

Der Zugang zum IT-System wird ständig kontrolliert.

Der Zugang zum IT-System wird ständig protokolliert.

Der Zugang zum IT-System wird ständig protokolliert.

Der Zugang zum IT-System wird ständig protokolliert.

Der Zugang zum IT-System wird ständig protokolliert.

Der Zugang zum IT-System wird ständig protokolliert.

Der Zugang zum IT-System wird ständig protokolliert.

Der Zugang zum IT-System wird ständig protokolliert.

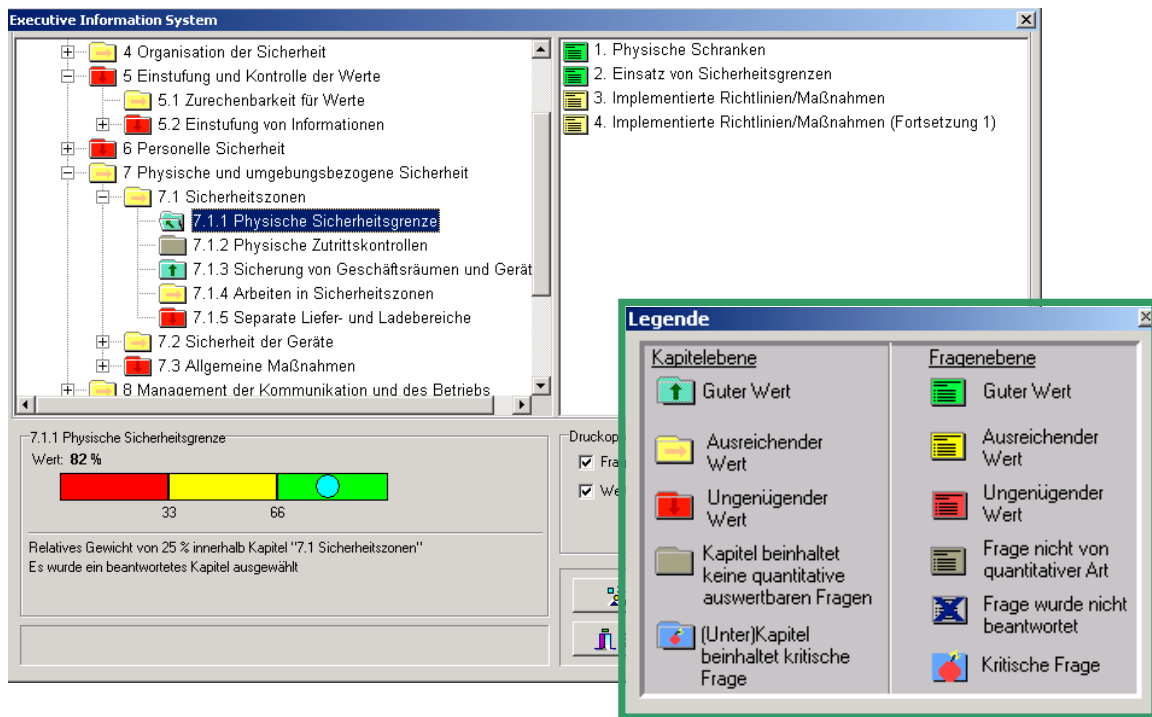
Status quo /
Schwachstellen

Maßnahmen zur
Verbesserung

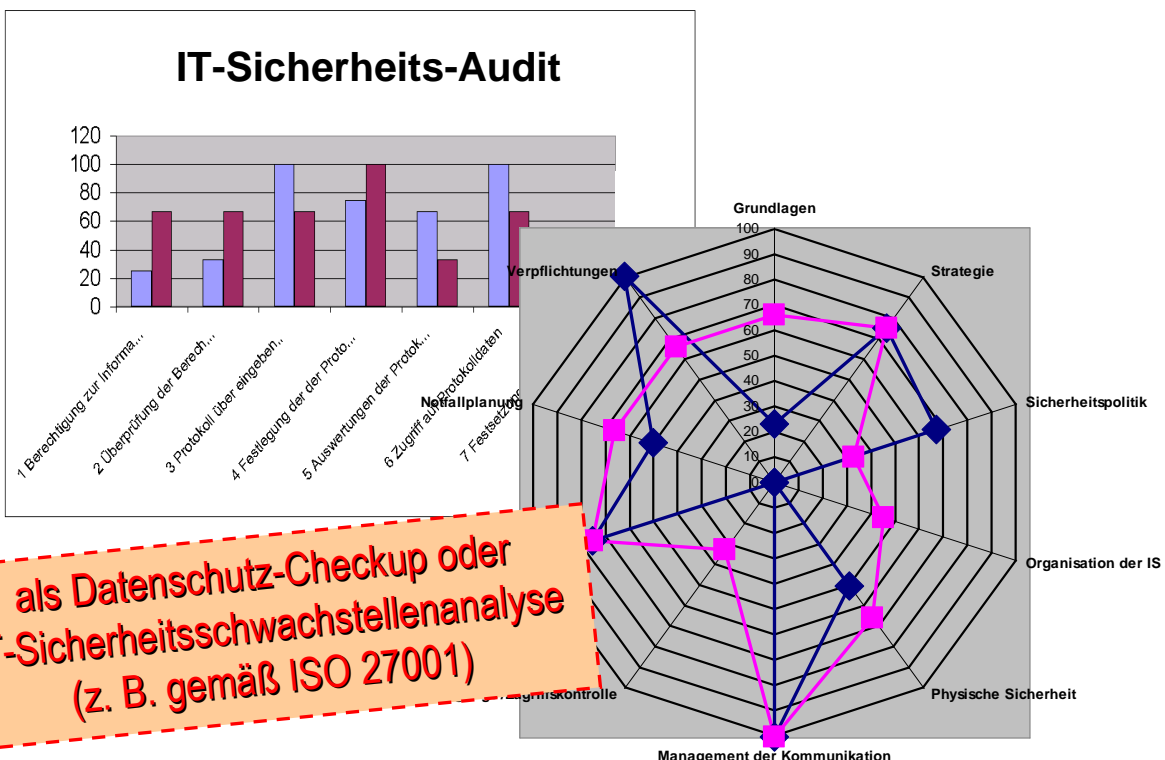
Unternehmens- und Informations-Management Consultants



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 Büroschlüssel oder Unterlagen/Schlüssel 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 Aufgabeneinstellungen 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/Fremdwartung 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 festzulegen, dass die Wartung/Wartungsmo...	3	EDV		Siehe Datenschutzhandbuch



Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing



als Datenschutz-Checkup oder
IT-Sicherheitsschwachstellenanalyse
(z. B. gemäß ISO 27001)

Die neue § 11 BDSG: Informationssicherheit und Compliance beim Outsourcing

Verbesserung der Funktionalitäten

- ➔ Effizienzgewinn bei Auswertung und Berichtserstellung
- ➔ schneller Überblick des Managements über die Prüfergebnisse
- ➔ Reduktion der Komplexität der Detaillergaben auf wesentliche Aussagen
- ➔ Darstellung der Sachverhalte zur Sensibilisierung des Managements

- ➔ **Verzahnung aller Tools**
- ➔ **UIMC-Tool für Analyse und Berichterstellung (UTAB)**
 - » z. B. als Datenschutz-Checkup
- ➔ **Organisationsmittel** wie z. B.
 - » Datenschutz-Handbuch (auch integriert mit IT-Sicherheit)
 - » Organisations-Kit
- ➔ **Schulungsunterstützung/-medien**
 - » multimediale Lern-CD
 - » Selbst-Lern-Kurs auf Powerpoint-Basis
- ➔ **computergestütztes Verzeichnis**