GI FG SecMgt, Workshop 17.05.04, Darmstadt

IT-Grundschutz als Basis für ein Datenschutzaudit

Frank Reiländer, Berater IT-Sicherheit
- Lizenzierter IT-Grundschutz-Auditor des BSI -
Infodas GmbH, Rhonestr. 2, 50765 Köln
☎(0221) 70912-85 f.reilaender@infodas.de
www.save-infodas.de

SAVe® Security Services

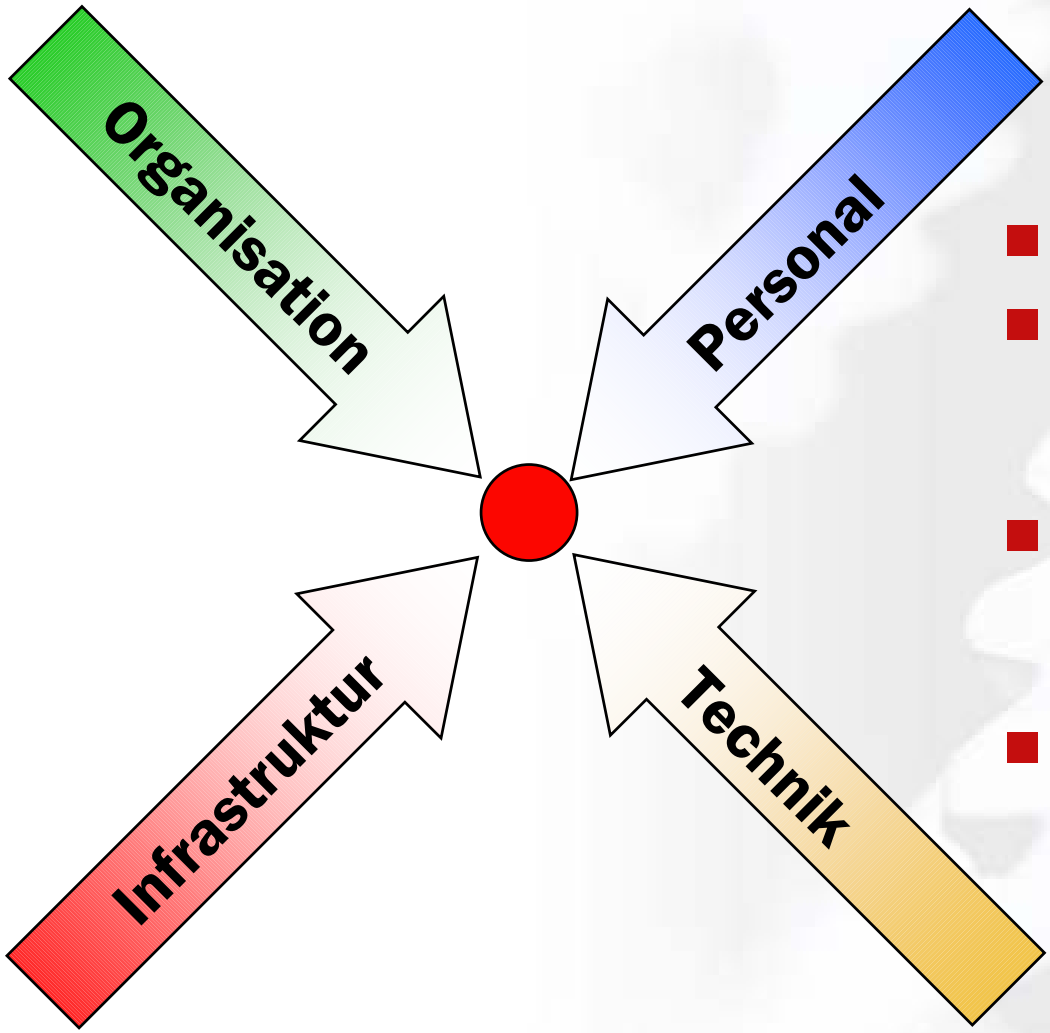
Innovative Beratung und Lösungen

- Security Management
- Security Policies
- Sicherheitskonzepte
- Datenschutzberatung
- Business Continuity Planning
- SAVe IT-Sicherheitsdatenbank
- Sicherheitszertifizierungen

IT-Grundschutz und Datenschutz

- Das IT-GSHB und die IT-Grundschutz-Methodik
- Ansätze für ein Datenschutzaudit
- Ableitungen aus der BDSG-Novelle 2001
- Sicherheits- und Kontrollziele der Datenschutzgesetzgebung
- Umsetzung der Methodik und Unterstützung der Erfassung

IT-Grundschutzes
Idee und Konzeption



- ganzheitlicher Ansatz
- Vorgehensbeschreibung zur Erstellung eines Sicherheitskonzeptes
- Standardsicherheits-Maßnahmen für typische IT-Systeme
- Referenz und Nachschlagewerk

Quelle: BSI

IT-Grundschutz ...die Anfänge 1995

Bundesanzeiger

ISSN 0720-6100 G 1990 A

Jahrgang 47 Ausgegeben am Sonnabend, dem 6. Mai 1995 Nummer 86 a

IT-Grundschutzhandbuch

Maßnahmenempfehlungen
für den mittleren Schutzbedarf

Schriftenreihe zur IT-Sicherheit

- Band 3 -

Stand: 1995

- komplette Erstellung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Beratungsauftrag des BSI für die Bundesbehörden
- kein integraler Sicherheitsprozess

IT-Grundschutzhandbuch 1995

- 18 Bausteine
- 200 Maßnahmen
- 150 Seiten

IT-Grundschutz
Standard für IT-Sicherheit

- Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten
- Standard für IT-Sicherheit
- Maßnahmensammlung
- Nachschlagewerk

- www.bsi.bund.de/gshb

IT-Grundschutzhandbuch 2003

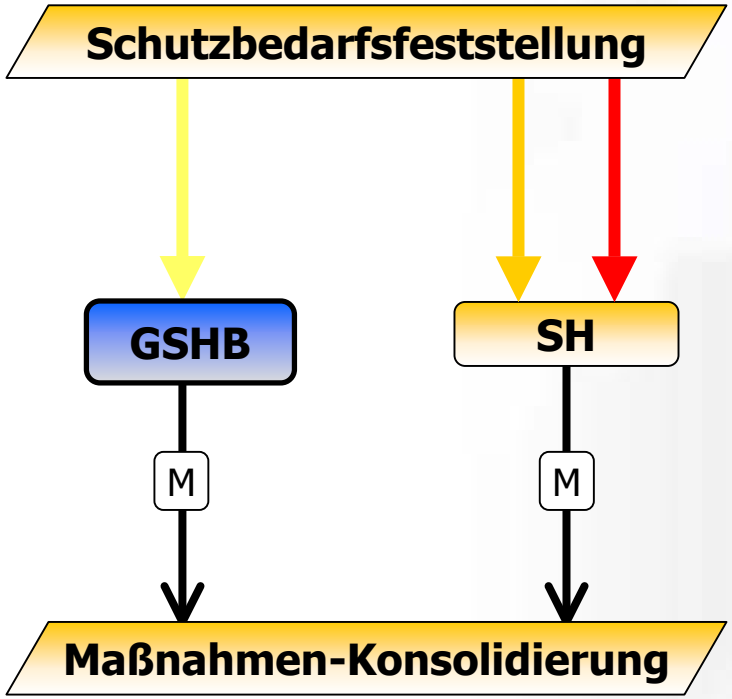
- 65 Bausteine
- 335 Gefährdungen
- 772 Maßnahmen
- 2525 Seiten

BSI Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz
Ablauf Basis-Sicherheitscheck

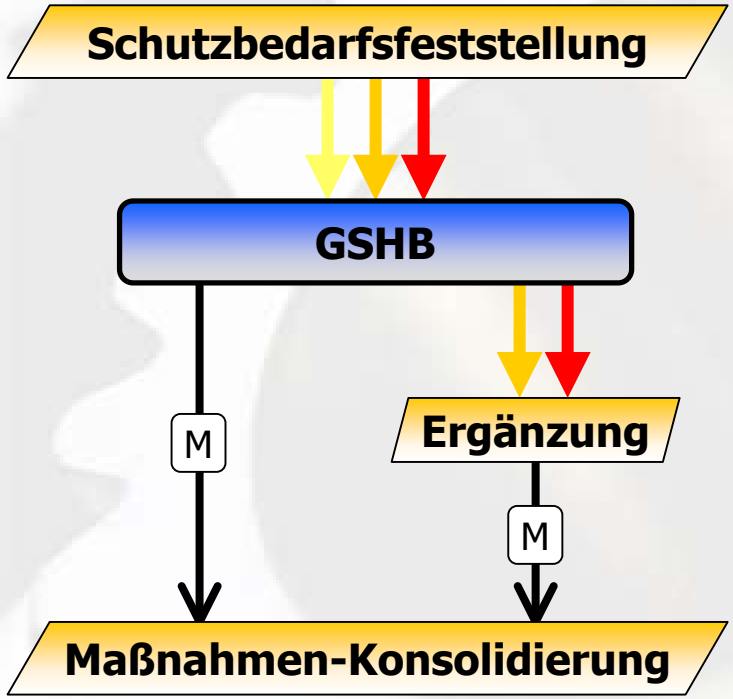
GSHB 1995

Zielgruppe: Behörden



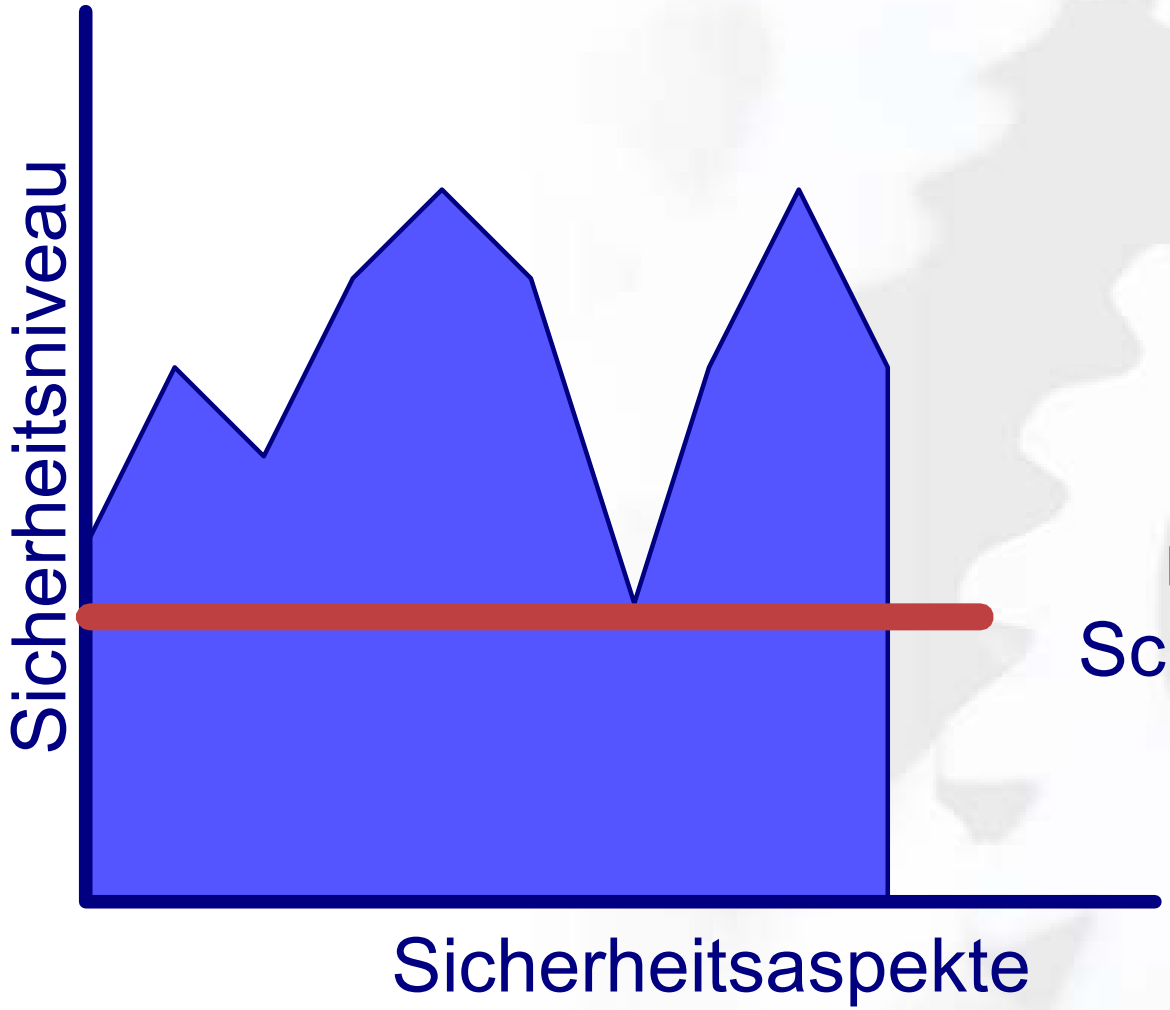
GSHB heute

Zielgruppe: Behörden, Unternehmen



GSHB	= Grundschutzhandbuch	=	Komponenten mit mittlerem Schutzbedarf
SH	= IT-Sicherheitshandbuch	=	Komponenten mit hohem Schutzbedarf
M	= Maßnahmen	=	Komponenten mit sehr hohem Schutzbedarf

IT-Grundschutz
Erreichbares Sicherheitsniveau



Methodik IT-Grundschutz

- Charakteristika (Auswahl)
  - Baukastenprinzip
  - Implizite Risikoanalyse
  - Konkrete standardisierte Maßnahmen
  - Fokussierung auf den Anwendungsbereich
  - Einheitliche Prüftiefe
  - Prozessunterstützung des IT-Sicherheitsmanagements
- Bewertung
  - Leichte Anwendbarkeit
  - Unterstützung bei Implementierung und Auditierung
  - Einheitliches Bewertungsschema (Kategorien)
  - Eignung zur standardisierten und Tool-unterstützten Erfassung

IT-Grundschutz und Datenschutz

- Das IT-GSHB und die IT-Grundschutz-Methodik
- Ansätze für ein Datenschutzaudit
- Ableitungen aus der BDSG-Novelle 2001
- Sicherheits- und Kontrollziele der Datenschutzgesetzgebung
- Umsetzung der Methodik und Unterstützung der Erfassung

Ziele eines Datenschutzaudits

- Marktgerechte Anreize zu einer Mobilisierung der Selbstverantwortung der verantwortlichen Stellen
- Freiwillige Überprüfung des Datenschutz-Managementsystems hinsichtlich seiner Eignung
- Kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit
- Verbesserungen des Datenschutzes und der Datensicherheit ohne Zwang
  - durch freiwillige Selbstregulation der Wirtschaftseinheiten
  - durch die Kräfte des Wettbewerbs

Prinzipien des modernen Datenschutzes

- Fokussierung auf elektronische Speicherung und Nutzung
- Aspekte der IT-gestützten Übermittlung
- Auftrags-DV und Outsourcing
  - technische/organisatorische Schutzmaßnahmen
- Prozesssicht
  - Dateiregister -> Verfahrensübersicht
- Systemdatenschutz
  - Datenvermeidung und -Sparsamkeit

Hilfe für den Datenschutzbeauftragten

- Unterstützung durch intensive Schulungen
- Methoden zur Bildung eines objektiven Urteils über den aktuellen Stand des Datenschutzes und der IT-Sicherheit im Unternehmen
- Datenschutzaudit zur Feststellung dieses Stands:
  - auf eine normierte Art
  - mit einem hohen Grad an Objektivität
- Kontrollinstrument zur nachhaltigen Verbesserung
  - des Datenschutzes
  - der zugrundeliegenden IT-Sicherheit

Argumente zum Datenschutzaudit

- Datenschutzaudit zur Stärkung der Selbstkontrolle des betrieblichen Datenschutzbeauftragten
- Effizientes, wettbewerbsgerechtes Verfahren statt staatlicher Kontrolle
- „Wildwuchs“ an Datenschutz-Gütesiegeln sollte verhindert werden

Grundschutz bietet den nötigen umfassenden Ansatz:

Etablierte Standards fördern Synergie-Effekte und eine schnelle Etablierung im Sinne eines Qualitätsmerkmals.

IT-Grundschutz und Datenschutz

- Das IT-GSHB und die IT-Grundschutz-Methodik
- Ansätze für ein Datenschutzaudit
- Ableitungen aus der BDSG-Novelle 2001
- Sicherheits- und Kontrollziele der Datenschutzgesetzgebung
- Umsetzung der Methodik und Unterstützung der Erfassung

Erweiterte Anforderungen des BDSG 2001

- Erweiterte Transparenz gegenüber dem Betroffenen
  - Erstellen einer öffentlichen Verfahrensübersicht
- Erweiterte Verarbeitungsbeschränkungen
  - Allgemeines Widerspruchsrecht
  - „Besondere Arten“ personenbezogener Daten
- Erweiterte Datenschutzkontrolle
  - Vorabkontrolle bei risikoreichen Verarbeitungen
- Einführung des Datenschutzaudits
  - Qualitätsmerkmal und –Kontrolle (freiwillig)

Stellenwert der IT-Sicherheits-Aspekte im Datenschutz

- Technische und organisatorische Maßnahmen (§9, Anlage zu §9 BDSG)
  - Datensicherungsmaßnahmen (BDSG 1990) -> Datensicherheitsmaßnahmen (BDSG 2001)
  - „Terminologie der IT-Sicherheit“ (Aussage BMI)
- Prozesssicht der Verarbeitung
  - Datei-Register -> Verfahrensübersicht
  - Widerspruchsrecht des Betroffenen
- Datenschutzkontrolle
  - Kontrolle der DV-Programme, Vorabkontrolle

Datenschutzaudit als Werkzeug zur Selbstkontrolle

- Novellierung des Datenschutzes vom Mai 2001:
  - stärkere Orientierung an den Kriterien der IT-Sicherheit
  - Empfehlung eines Datenschutzaudits als Qualitätskriterium

Zusammenwachsen von Datenschutz und IT-Sicherheit (nach einem Vierteljahrhundert!)

- Treibende Faktoren:
  - Umsetzung der EU-Vorgaben (Richtlinie 95/46/EG)
  - grundlegende Überlegungen für ein „modernes Datenschutzrecht“

Thesen zur Konvergenz von Datenschutz und IT-Sicherheit

- „Datenschutz stützt sich zu zwei Dritteln auf Datensicherheit“
  - allg. Betrachtung der Datenschutz-Fachpresse
- „Datensicherheit identifiziert sich mit den Grundwerten der IT-Sicherheit“
  - Kommentierung BDSG-Novelle
- Praxistest „Datenschutzaudit und IT-Gütesiegel“ des ULD, Schleswig-Holstein
  - Datenschutz und -sicherheit als Qualitätsmerkmal
  - Einführung datenschutzfreundlicher Technik

IT-Grundschutz und Datenschutz

- Das IT-GSHB und die IT-Grundschutz-Methodik
- Ansätze für ein Datenschutzaudit
- Ableitungen aus der BDSG-Novelle 2001
- Sicherheits- und Kontrollziele der Datenschutzgesetzgebung
- Umsetzung der Methodik und Unterstützung der Erfassung

BDSG 1990
„10 Gebote“ der Datensicherung

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übermittlungskontrolle
- Eingabekontrolle
- Auftragskontrolle
- Transportkontrolle
- Organisationskontrolle

BDSG 2001
Datensicherheitsziele

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle
- Organisationskontrolle

Landesdatenschutz
Sicherheitsziele (AK Technik)

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Revisionsfähigkeit
- Transparenz

- Verankert in den Datenschutzgesetzen in Berlin, Hamburg*, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Sachsen (Entwurf), Sachsen-Anhalt, Thüringen

IT-Grundschutz und Datenschutz

- Das IT-GSHB und die IT-Grundschutz-Methodik
- Ansätze für ein Datenschutzaudit
- Ableitungen aus der BDSG-Novelle 2001
- Sicherheits- und Kontrollziele der Datenschutzgesetzgebung
- Umsetzung der Methodik und Unterstützung der Erfassung

Inhalt des Datenschutzaudits

- Zwei Prüffelder sind abzudecken:
  - Einhaltung der juristischen Vorschriften
  - Gewährleistung der Einhaltung durch organisatorische und technische Maßnahmen
- Maßnahmenrahmen ist durch Anlage zum §9 gesetzt
  - Festlegung von 8 Geboten (Kontrollzielen)
  - Orientierung an Normen zur IT-Sicherheit

Folgerung:

IT-Grundschutz als „der“ deutsche **Standard** für IT-Sicherheit bietet ebenso eine solide Basis für die Umsetzung und Überprüfung von technischen und organisatorischen **Datensicherheitsmaßnahmen.**

Umsetzung der Methodik

- Prüfung der Datenschutz-Aspekte

  Prüfgegenstand:

  - Datenschutzorganisation und Aufgaben des betrieblichen Datenschutzbeauftragten
  - Prüfung der Datenschutzorganisation anhand der Maßnahmenempfehlungen des BfD

- Prüfung der Datensicherheits-Aspekte

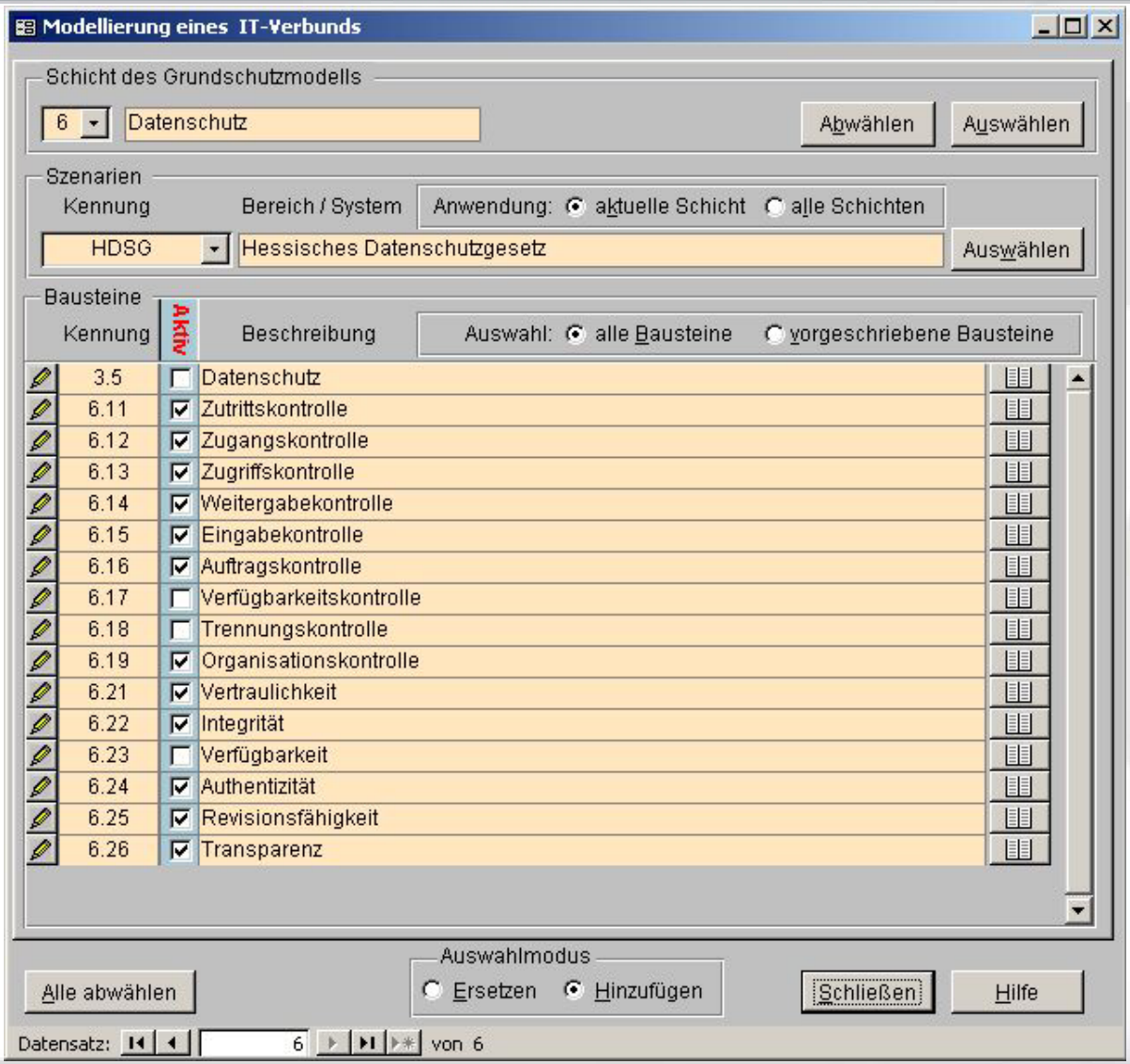
  Prüfgegenstand:

  - Umsetzung der technischen und organisatorischen Maßnahmen
  - Prüfung des Umsetzungsstands der Maßnahmen durch Abbildung auf relevante Grundschutz-Maßnahmen

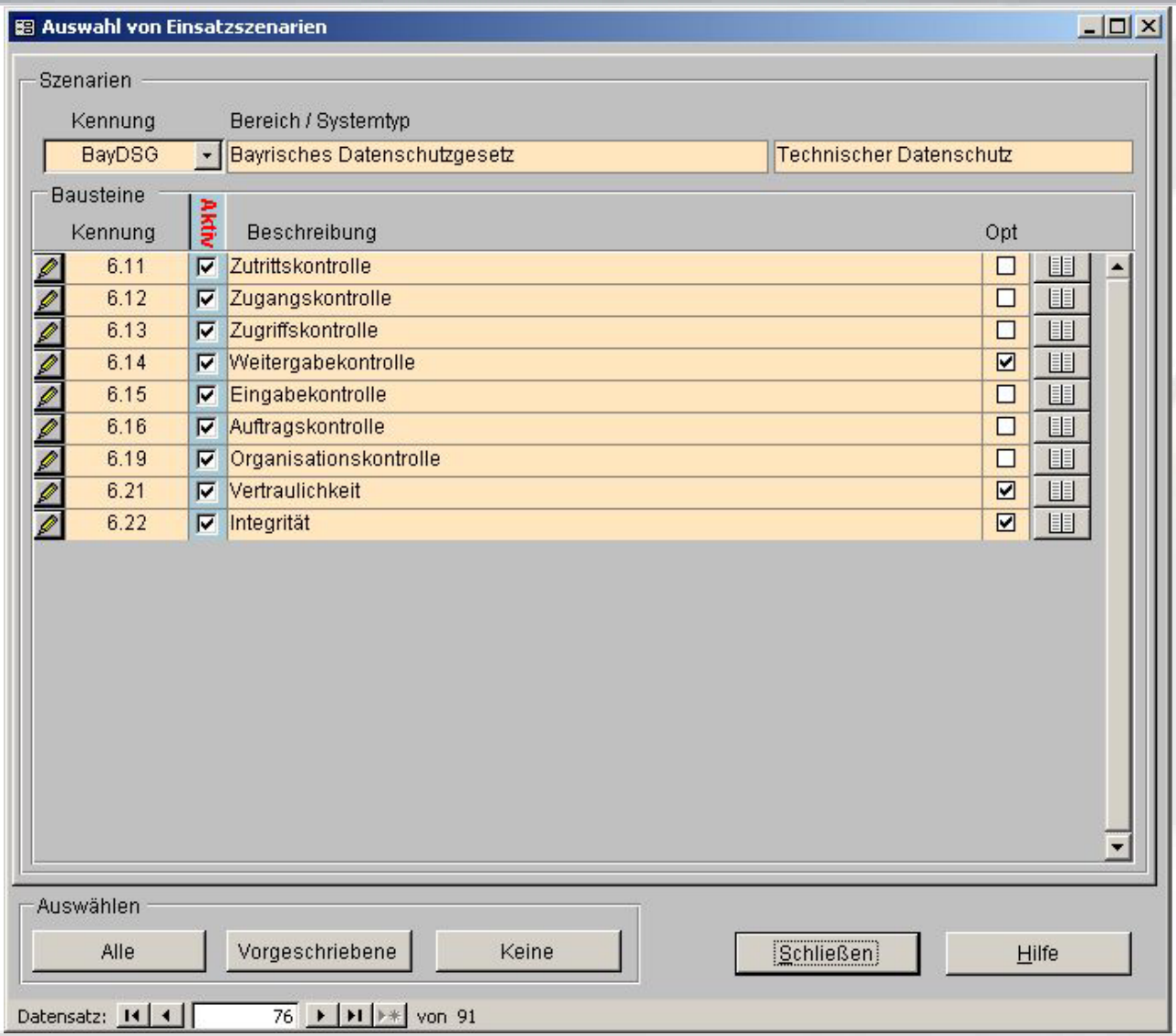
Datenschutz-Audit mit SAVe®
Methodischer Ansatz

- IT-Grundschutzhandbuch, Baustein 3.5
  - Bundesbeauftragter für den Datenschutz 1999, wurde nicht offiziell ins IT-GSHB übernommen
  - siehe www.bfd.bund.de/technik/DS-KAP/35.htm
- Zuordnungstabelle der „Gebote“ (Anl. zu §9 BDSG) – Grundschutzmaßnahmen
- Konsolidieren der Maßnahmen-Empfehlungen anhand aktueller Datenschutz-Ziele (Prüffragen)
- Aktualisierung der Datensicherheits-Maßnahmen gemäß BDSG 2001

Anwendungsbeispiel: Datenschutzziele Hessen



Anwendungsbeispiel: Datenschutzziele Bayern



Maßnahmen Datenschutz (Baustein 3.5 / 1999)

- Regelung der Verantwortlichkeiten im Bereich Datenschutz (M 7.0)
- Prüfung der Zulässigkeit der Datenverarbeitung (M 7.1)
- Prüfung der Erforderlichkeit (M 7.2)
- Prüfung der Verwendung von Daten hinsichtlich der Zweckbindung (M 7.3)
- Prüfung der Verwendung der Daten hinsichtlich der besonderen Zweckbindung (M 7.4)
- Bestellung eines Datenschutzbeauftragten (M 7.5)
- Verpflichtung/Unterrichtung der Mitarbeiter (M 7.6)
- Organisatorische Verfahren zur Sicherstellung der Rechte der Betroffenen (M 7.7)
- Führung von Dateien- und Geräteverzeichnissen und Erfüllung der Meldepflichten (M 7.8)

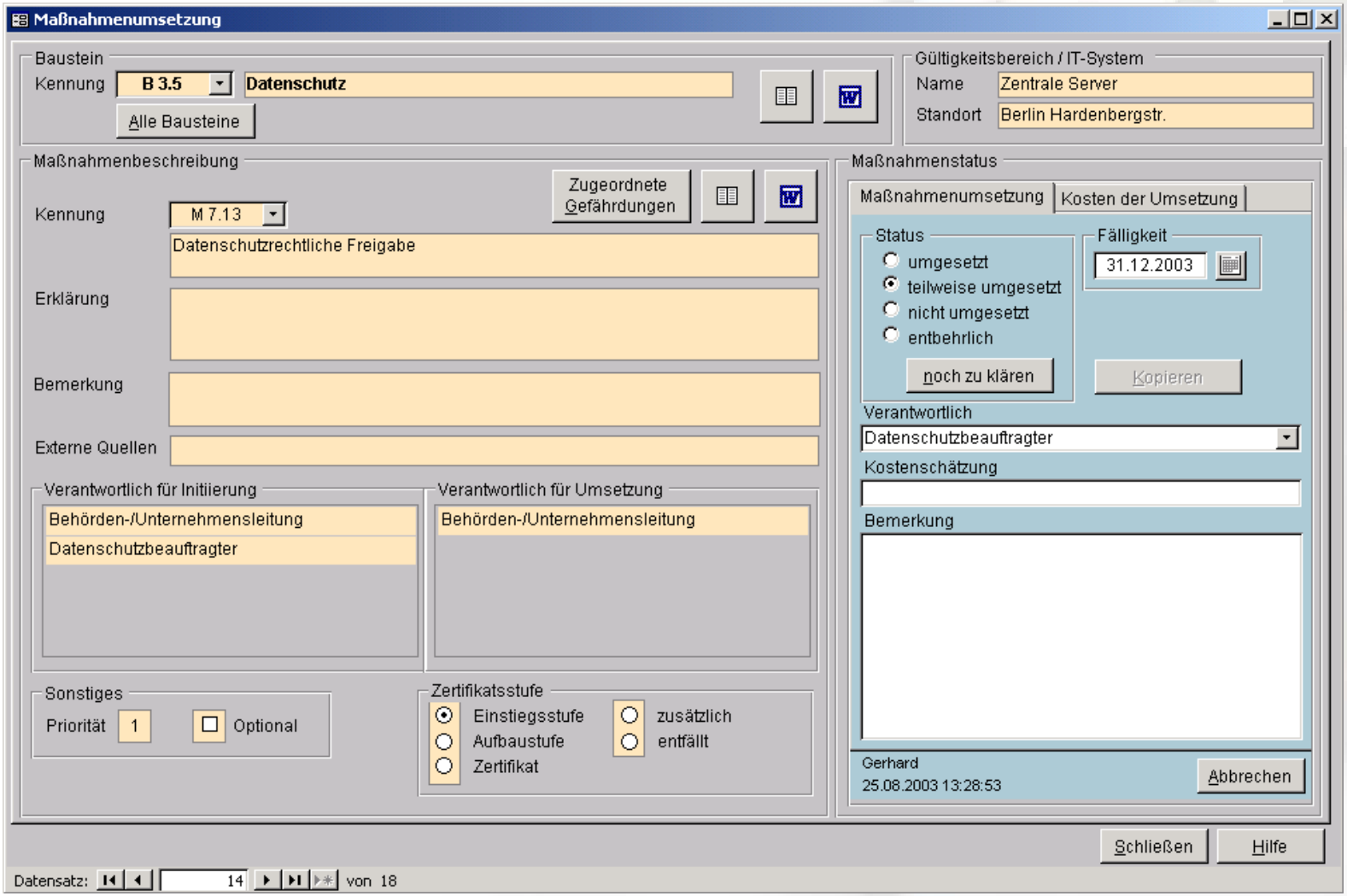
Maßnahmen Datenschutz (Baustein 3.5 / 1999)

- Ergreifen von technisch-organisatorischen Maßnahmen entsprechend dem Stand der Technik (M 7.9)
- Dokumentation der datenschutzrechtlichen Zulässigkeit (M 7.10)
- Datenschutzaspekte bei der Protokollierung (M 7.11)
- IT- und Datenschutz-Regelungen (M 7.12)
- Datenschutzrechtliche Freigabe (M 7.13)
- Meldung und Regelung von Abrufverfahren (M 7.14)
- Regelung der Auftragsdatenverarbeitung (M 7.15)
- Regelung der Verknüpfung und Verwendung von Daten (M 7.16)
- Einrichtung einer internen IT-Revision und Datenschutzkontrolle (M 7.17)

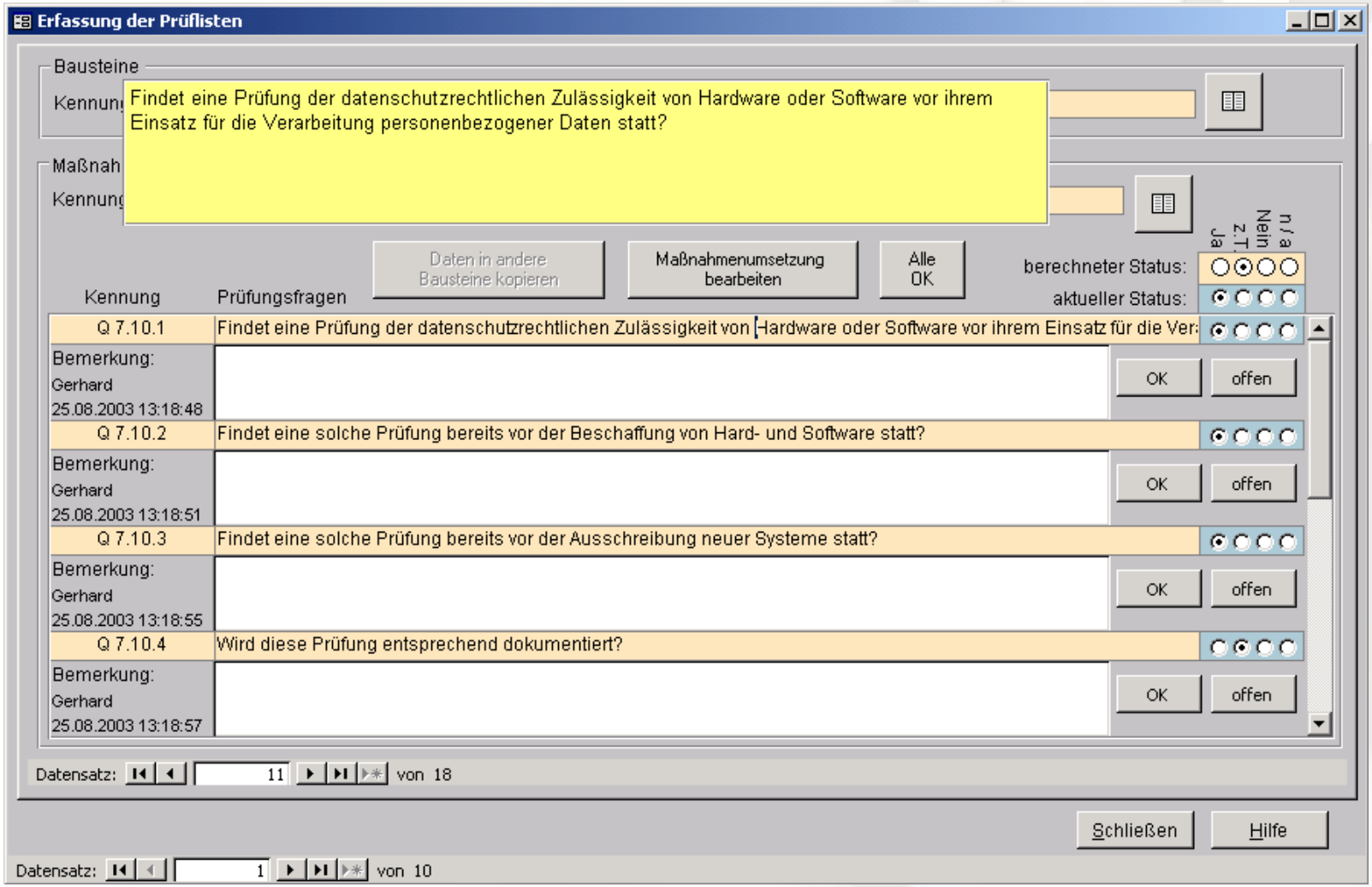
Maßnahmen Datenschutz (Baustein 1.5 / 2004 ???)

- Der Baustein 3.5 des BfD von 1999 berücksichtigt nicht die Neuerungen/Änderungen des BDSG 2001
- Eine Novelle des Bausteins 3.5 von 1999 ist zurzeit in Arbeit
- Erarbeitung unter Federführung des BfD
- Beteiligung des BSI
- Abstimmung mit dem „Düsseldorfer Kreis“
- Platzhalter (B 1.5) bleibt im IT-GSHB auch nach der Restrukturierung 2004 erhalten

Werkzeuggestützte Erfassung



Erfassung von Checklisten



Planung der Mängelbeseitigung

Realisierungsplanung offener Maßnahmen

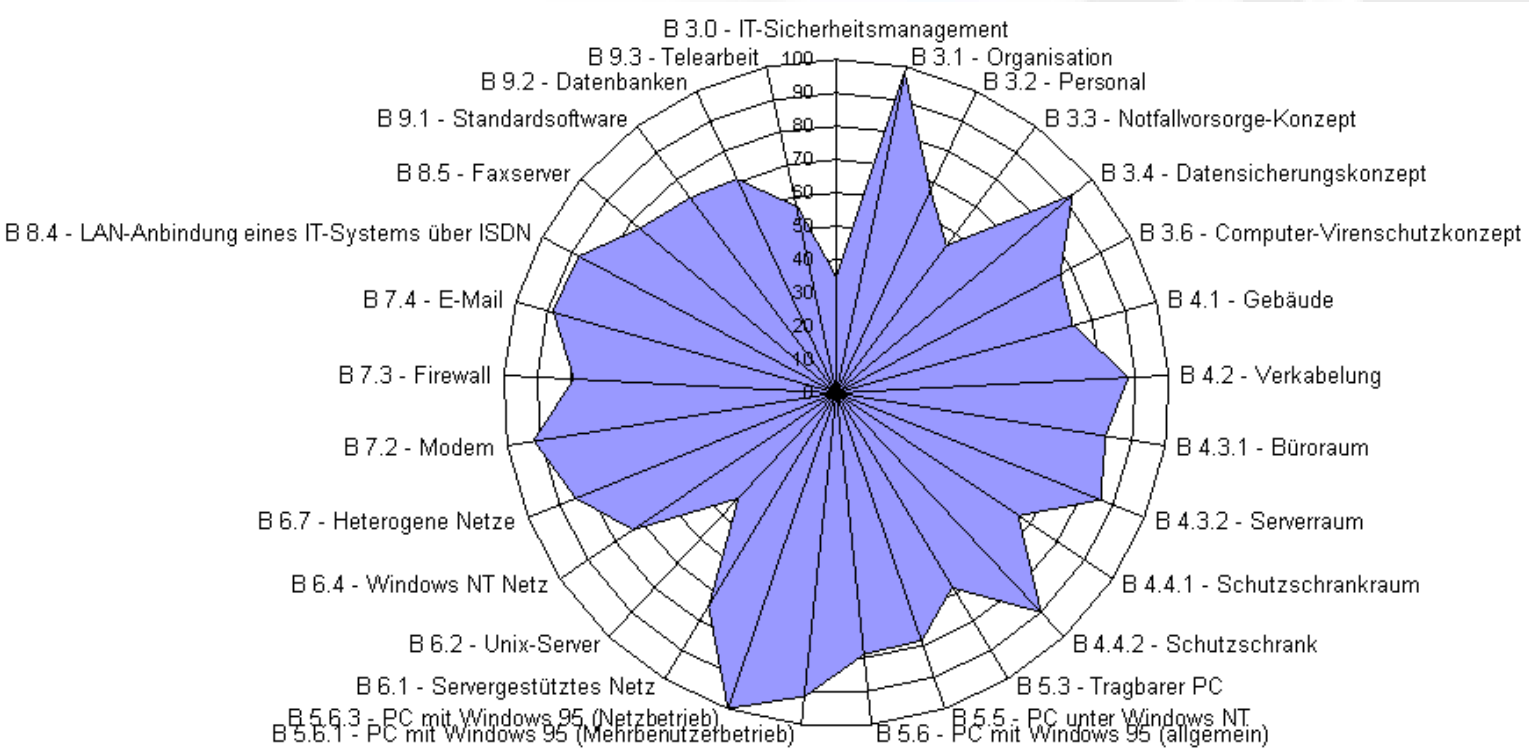
Datenbestand: Zentrale Server

Datenschutz Nr.	Beschreibung	Zertifikat	z.T.	Nein	fällig	verantwortlich	Bemerkungen	Kosten: Personalaufwand (PT) einmalig	Kosten: Personalaufwand (PT) pro Monat	Kosten: Sachkosten (€) einmalig	Kosten: Sachkosten (€) pro Monat
M 2.131	**Aufteilung von Administrationstätigkeiten bei Datenbanksystemen**										
B 3.5.8	Trennungsgebot (BDSG)	Zertifikat	◉	○	25.08.2003	IT-Sicherheitsmanagement					
B 3.5.9	Organisationskontrolle (BDSG)	Zertifikat	◉	○	25.08.2003	IT-Sicherheitsmanagement					
M 2.133	**Kontrolle der Protokolldateien eines Datenbanksystems**										
B 3.5.5	Eingabekontrolle (BDSG)	Einstieg	○	◉	31.12.2003	Revisor					
B 3.5.9	Organisationskontrolle (BDSG)	Einstieg	○	◉	31.12.2003	Revisor					
M 2.167	**Sicheres Löschen von Datenträgern**										
B 3.5.6	Auftragskontrolle (BDSG)	Aufbau	○	◉	31.08.2003	IT-Verfahrensverantwortlicher					
M 5.14	**Absicherung interner Remote-Zugänge**										
B 3.5.4	Weitergabekontrolle (BDSG)	Einstieg	○	◉	25.08.2003	Administrator					
B 3.5.9	Organisationskontrolle (BDSG)	Einstieg	○	◉	25.08.2003	Administrator					
M 7.13	**Datenschutzrechtliche Freigabe**										
B 3.5	Datenschutz	Einstieg	◉	○	31.12.2003	Datenschutzbeauftragter					

Eröffnen der Datensicherheits-Sicht auf den Grundschutz

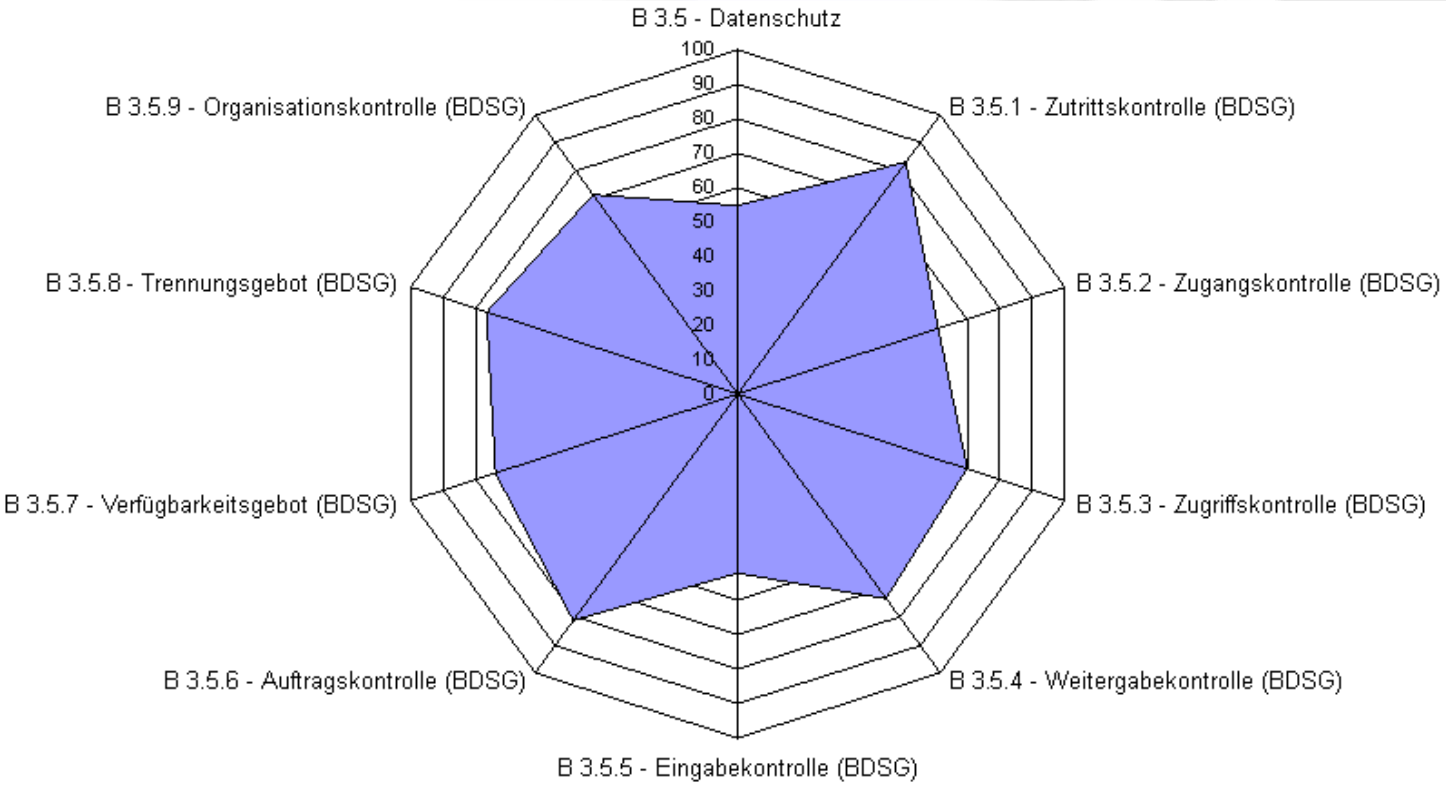
- Konsolidieren, Aktualisieren und Erweitern der Verknüpfungen
- Zuordnen der neuen Datensicherheits-„Gebote“
- Modellieren der Referenzbeziehungen in SAVe®
- Regelmäßiger Expertenworkshop zur Bewertung der Maßnahmen-Empfehlungen

Umsetzungsstand von IT-Grundschutzmaßnahmen



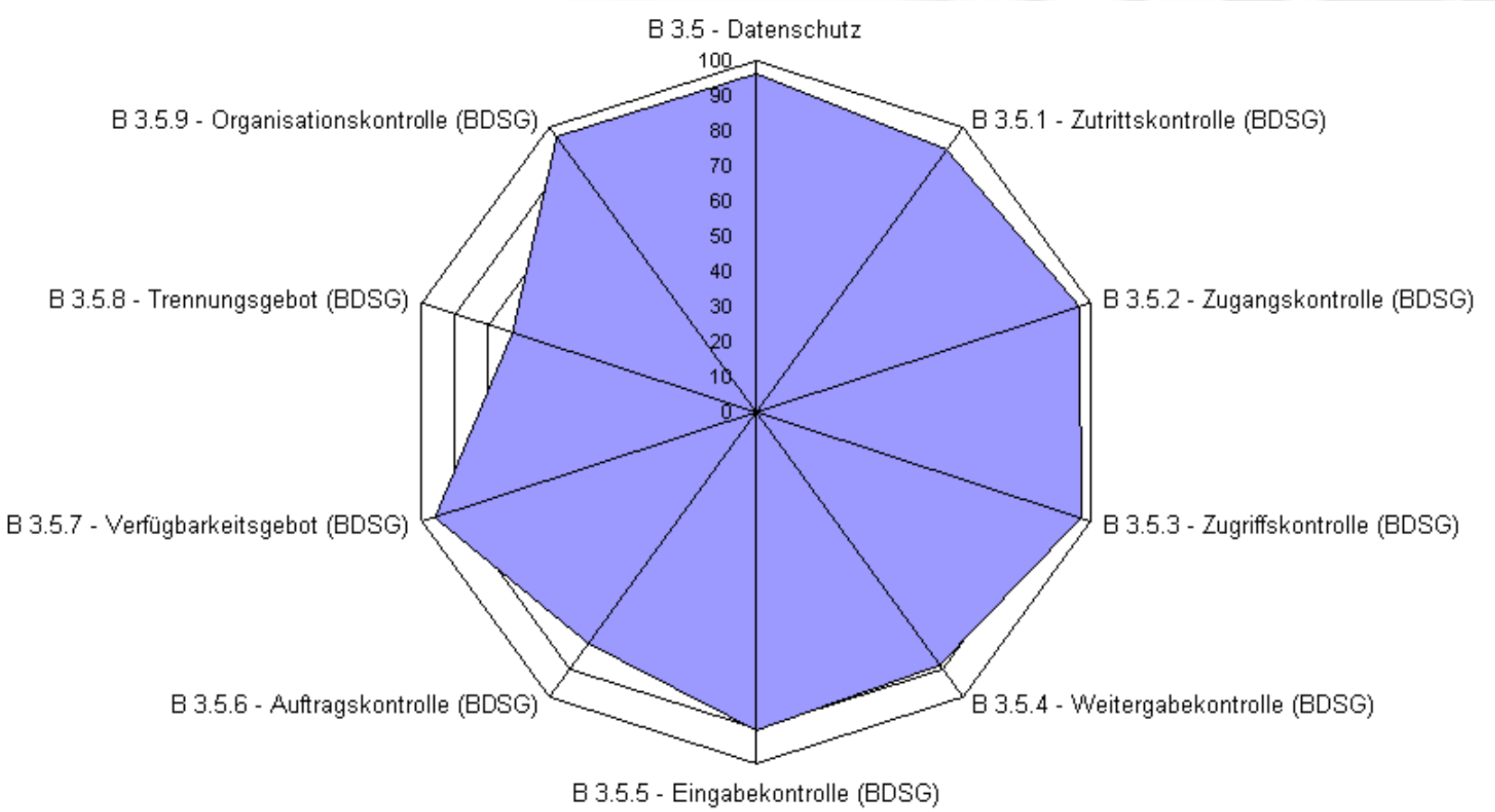
- Ergebnis eines Basis-Sicherheitschecks nach IT-Grundschutz-Handbuch (Praxisbeispiel)

Datenschutz-Audit – Ergänzung des Basis-Sicherheitschecks



- Datensicherheitssicht auf den den Ergebnisse dieser Grundschutzerhebung (Praxisbeispiel)

Weiteres Praxisbeispiel



Fazit

- IT-Sicherheit und Datenschutz ergänzen sich in vielen Aspekten
- Synergiepotential gemeinsamer Bearbeitung
  - führt zu einheitlichen Bewertungsmaßstäben
  - erlaubt die Nutzung einer Werkzeugunterstützung
- Vorgehen setzt die gesetzlichen Forderungen nach einem Datenschutzaudit sinnvoll in die Praxis um
- Der Ansatz berücksichtigt gleichzeitig
  - Selbstkontrolle
  - Effizienz
  - Wirtschaftlichkeit

IT-Grundschutz als Basis für ein Datenschutzaudit

Vielen Dank für Ihre Aufmerksamkeit!