Erfahrungen aus einer Zertifizierung nach ISO 27001 und nach BSI-Grundschutz

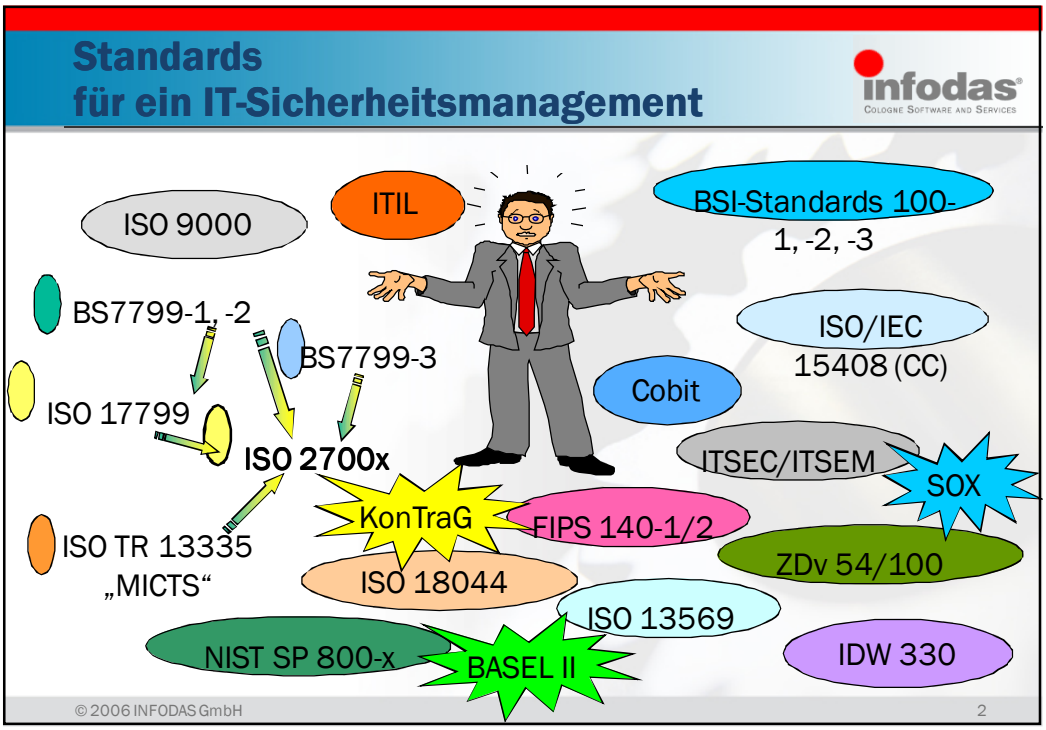
Dr. G. Weck, INFODAS GmbH, Köln
DECUS IT-Symposium, Nürnberg
Vortrag 2K04

Inhalt

- Kontext und Phasen der Zertifizierung
  - Schritte zur Durchführung eines Audits zur Zertifizierung
  - Das Zwei-Auditoren-Prinzip
- IT-Grundschutz-Methodik
  - IT-Strukturanalyse und Schutzbedarfsfeststellung
  - Modellierung / Basis-Sicherheitscheck
  - Ergänzende Sicherheitsanalyse
  - Risikoanalyse nach Grundschutz und Rückführung in den Prozess
- ISO 27001-Zertifizierung
  - Beteiligte Stellen / Phasen der Zertifizierung
  - Prüfschema für ISO 27001-Audits auf der Basis von IT-Grundschutz
  - Das Zertifizierungs-Audit
  - Erfolgsfaktoren für die Durchführung / Nutzen für den Kunden

© 2006 INFODAS GmbH 1

Standards für ein IT-Sicherheitsmanagement



© 2006 INFODAS GmbH 2

IT-Grundschutzhandbuch

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

www.bsi.bund.de/gshb

IT-Grundschutzhandbuch 2006
- 69 Bausteine
- 425 Gefährdungen
- 1057 Maßnahmen
- 3746 Seiten (incl. Standards)

Bundesamt für Sicherheit in der Informationstechnik

© 2006 INFODAS GmbH 3

ISO 27001 auf der Basis von IT-Grundschutz

- Neue Ausrichtung des Grundschutzes seit 01.01.2006
  - stärkere Hervorhebung der Methodik
  - **geschäftsprozessorientiert**
- Vorgehensweise gemäß IT-Grundschutz im neuen BSI-Standard 100-2 festgelegt
- Konform zu den Managementanforderungen der ISO 27001 für ISMS
  - Schwerpunkte:
    - Verantwortung der Leitung
    - Aufrechterhaltung des Sicherheitsprozesses
    - Abdeckung des Risikomanagements

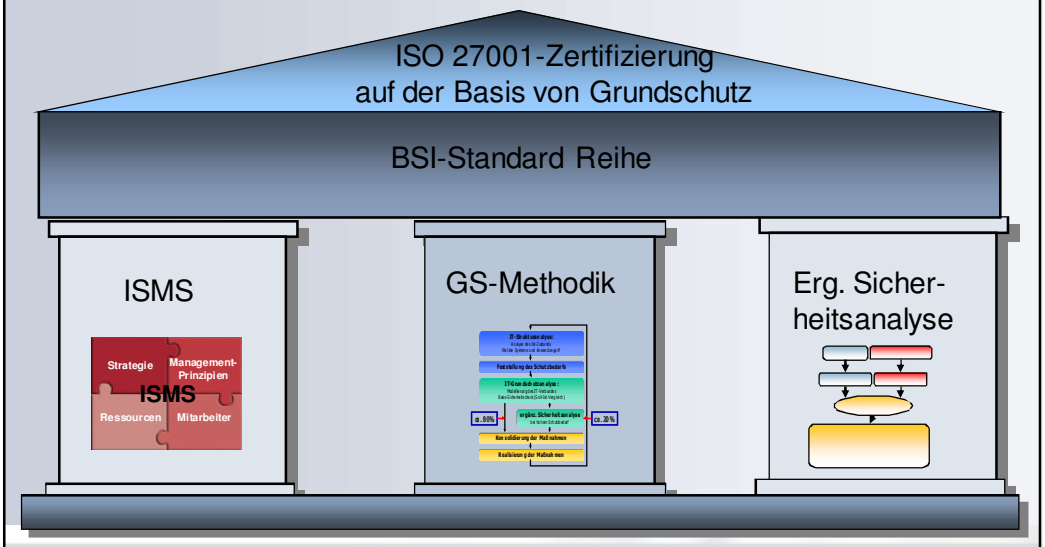
© 2006 INFODAS GmbH 4

ISO 27001 Zertifikat auf der Basis von IT-Grundschutz

- BSI zertifiziert nach deutschen und nach internationalen Standards
  - seit Anfang 2006 stellt das BSI „ISO 27001-Zertifikate auf der Basis von IT-Grundschutz“ aus, und realisiert eine Nationale Ausprägung der ISO 27001
- Eine BSI-Zertifizierung...
  - umfasst sowohl eine Prüfung des ISMS als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz
  - beinhaltet eine offizielle ISO-Zertifizierung nach ISO 27001
  - ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich aussagekräftiger als eine reine ISO-Zertifizierung
- Vom BSI lizenzierte Auditoren...
  - erfüllen alle Anforderungen, die die ISO an Auditoren für ein ISMS stellt

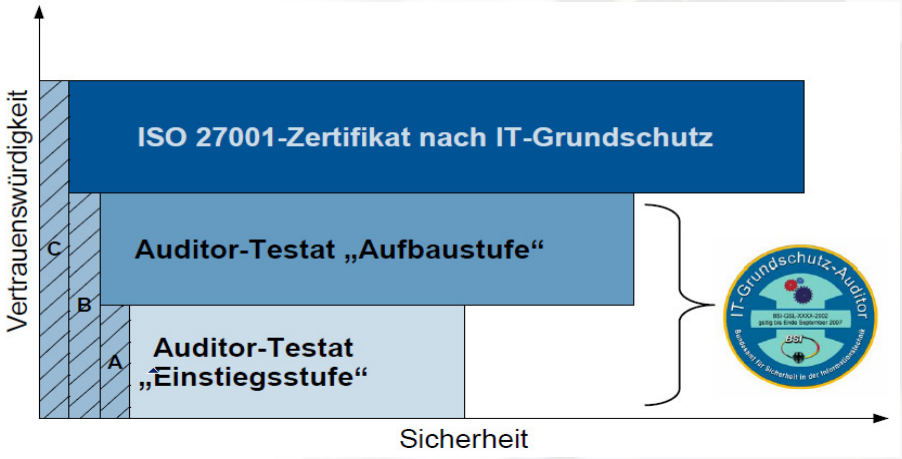
© 2006 INFODAS GmbH 5

Internationale GS-Zertifizierung



© 2006 INFODAS GmbH Quelle: BSI, 2005 6

Stufenkonzept



© 2006 INFODAS GmbH Quelle: BSI 7

Kontext der Zertifizierung

- Auftraggeber: SAP System Integration AG, Dresden
- IT-Verbund: Geschäftsbereich Hosting
  - Outsourcing Netzwerk mit der gesamten Netzwerktechnik
  - über 500 Windows- und UNIX-basierte Kundenserver zum Hosten der SAP/R3- und mySAP-Anwendungen
  - drei hochverfügbare Serverzentren
  - Firewall-Systeme, Backbone Switches bis zu den Kundenschnittstellen (Routern)
- Zertifizierung nach IT-Grundschutz in 2004 erfolgreich durchgeführt
- Re-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

© 2006 INFODAS GmbH 8

Phasen der Zertifizierung

- Zertifizierung nach IT-Grundschutz
  - Basis-Sicherheitscheck durch F. Reiländer (BSI-GSL-0059-2003)
  - Zertifizierungs-Audit durch G. Weck (BSI-GSL-0021-2002)
    - Grundschutz-Handbuch Version 05/2002
    - Prüfschema Stand 01.12.2003
    - Durchführung: 26.01.2004 – 06.02.2004 (4 + 5 PT)
  - Zertifikat Nr. BSI-GSZ-0006-2004
- Re-Zertifizierung
  - Basis-Sicherheitscheck durch D. Loß (BSI-GSL-0165-2005)
  - Zertifizierungs-Audit durch G. Weck (BSI-IGL-0063-2006)
    - Grundschutz-Handbuch Version 2005
    - Prüfschema Stand 01.02.2006
    - Durchführung 03.04.2006 – 08.05.2006 (3 + 5 PT)
  - Zertifikat Nr. BSI-IGZ-0004-2006

© 2006 INFODAS GmbH 9

Schritte zur Durchführung eines Audits zur Zertifizierung

- Vorbereitungsaudit
  - Durchlaufen aller notwendigen Schritte des Grundschutz-/ISO 27001-Verfahrens unter Berücksichtigung des Prüfschemas
    - IT-Strukturanalyse / Schutzbedarfsfeststellung für den IT-Verbund
    - Modellierung / vollständiger Basis-Sicherheitscheck
    - ergänzende Sicherheitsanalyse / Risikoanalyse
  - Ergebnis ist eine Liste aller Mängel, die einer Zertifizierung entgegenstehen
- Umsetzung der fehlenden Schutzmaßnahmen
- Zertifizierungsaudit
  - Anwendung des Prüfschemas unter Zertifizierungsbedingungen
  - Vorstufen stellen Erfüllbarkeit des Prüfschemas sicher

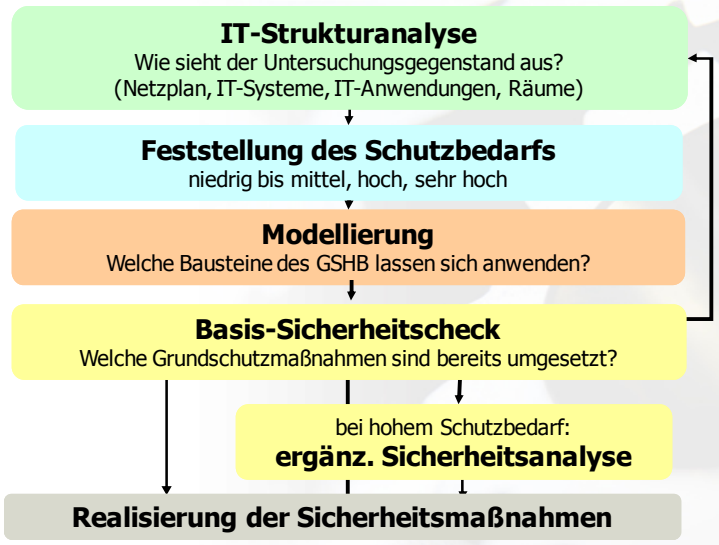
© 2006 INFODAS GmbH 10

Das Zwei-Auditoren-Prinzip

- Vorbereitung des Audits (Auditor 1)
  - Beratung bei der Abgrenzung des IT-Verbunds
  - Erfahrene Überprüfung/**Durchführung Basis-Sicherheitscheck**
  - **„Generalprobe“** unter Echtbedingungen
  - Unterstützung bei der Umsetzung defizitärer Maßnahmen
  - Durchführung der ergänzenden Sicherheitsanalyse / Risikoanalyse
- Anmeldung des Audits durch auditierte Institution
- Zertifizierungsaudit (Auditor 2)
  - Sichten der Referenzdokumente
  - Inspektion vor Ort
  - Erstellen des Auditreports

© 2006 INFODAS GmbH 11

IT-Grundschutz-Methodik



© 2006 INFODAS GmbH Quelle: BSI 12

IT-Strukturanalyse und Schutzbedarfsfeststellung

- IT-Strukturanalyse konnte von der Erst-Zertifizierung weitgehend übernommen werden
  - keine gravierenden strukturellen Änderungen
  - Netzplan wurde vor dem Audit neu gezeichnet, um verständlicher zu werden (keine inhaltliche Änderung)
- Schutzbedarf konnte ebenfalls übernommen werden
- Starke Reduzierung des Umfangs durch Gruppierung
  - nur wenige Server-Typen (Unix/Windows, hoher/normaler Schutz)
  - einheitliche, zentralisierte Verwaltung aller IT über virtuelle Management-Konsole
  - Dokumentation zur IT und zur Sicherheit zentral zugreifbar
  - 3 identisch verwaltete Serverzentren → Gruppierung der RZ !!!

© 2006 INFODAS GmbH 13

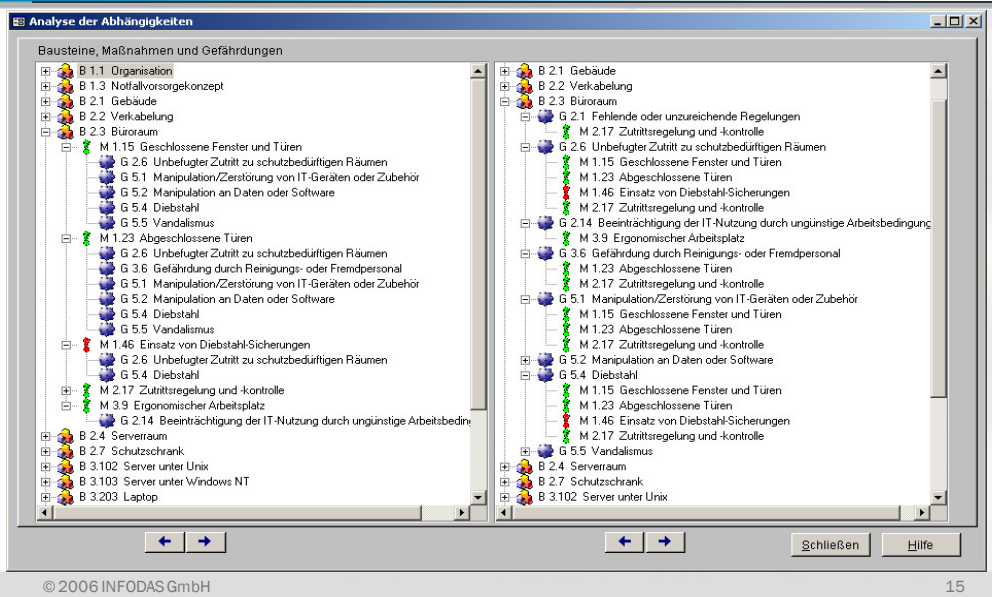
Modellierung

- B 1.0 IT-Sicherheitsmanagement
- B 1.1 Organisation
- B 1.2 Personal
- B 1.3 Notfallvorsorgekonzept
- B 1.4 Datensicherungskonzept
- B 1.6 Computer-Virenschutzkonzept
- B 1.7 Kryptokonzept
- B 1.8 Behandlung von Sicherheitsvorfällen
- B 1.9 Hard- und Software-Management
- B 1.10 Standardsoftware
- B 1.13 IT-Sicherheitssensibilisierung und -schulung
- B 2.1 Gebäude
- B 2.2 Verkabelung
- B 2.3 Büroraum
- B 2.5 Datenträgerarchiv
- B 2.6 Raum für technische Infrastruktur
- B 2.9 Rechenzentrum
- B 3.101 Allgemeiner Server
- B 3.102 Server unter Unix
- B 3.106 Server unter Windows 2000
- B 3.201 Allgemeiner Client
- B 3.203 Laptop
- B 3.209 Client unter Windows XP
- B 3.301 Sicherheitsgateway (Firewall)
- B 3.302 Router und Switches
- B 4.1 Heterogene Netze
- B 4.2 Netz- und Systemmanagement
- B 4.4 Remote Access
- B 4.5 LAN-Anbindung eines IT-Systems über ISDN
- B 5.2 Datenträgeraustausch
- B 5.3 E-Mail
- B 5.7 Datenbanken
- Bs5.13 SAP System

Vorabversion des Bausteins

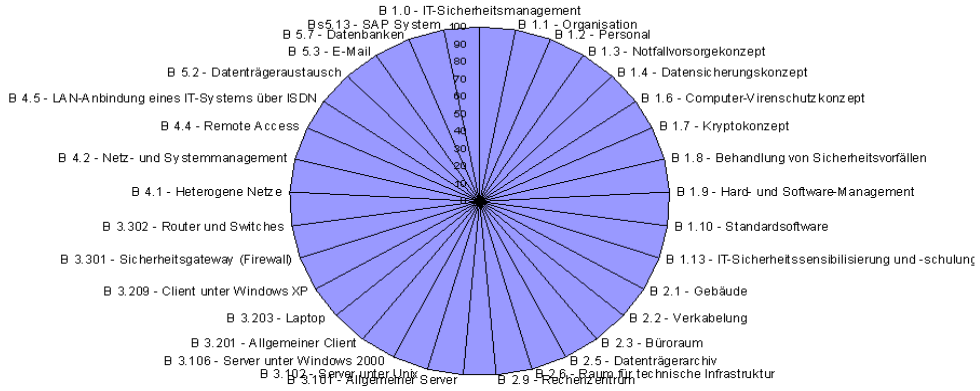
© 2006 INFODAS GmbH 14

Graphische Analyse der Maßnahmenumsetzung



© 2006 INFODAS GmbH 15

Ergebnis des Basis-Sicherheitschecks



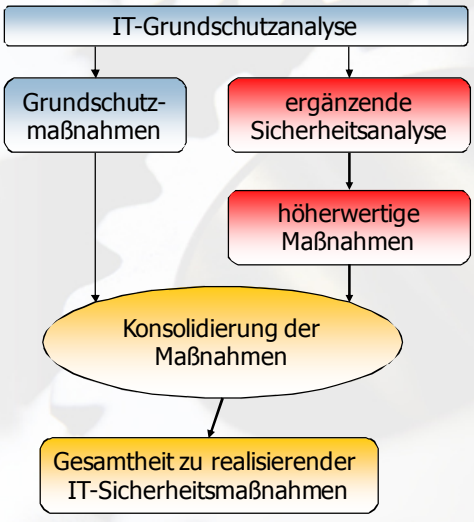
- volle Konformität zu den Anforderungen des Grundschutzes
- Zertifizierung hat Aussicht auf Erfolg

© 2006 INFODAS GmbH 16

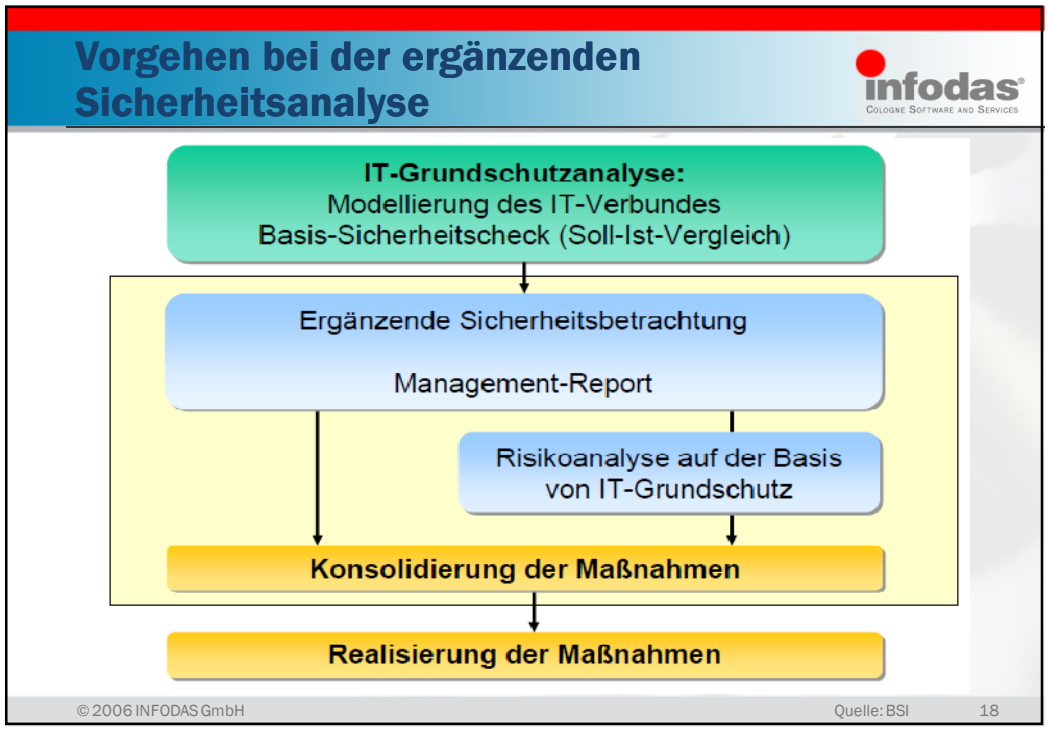
Ergänzende Sicherheitsanalyse

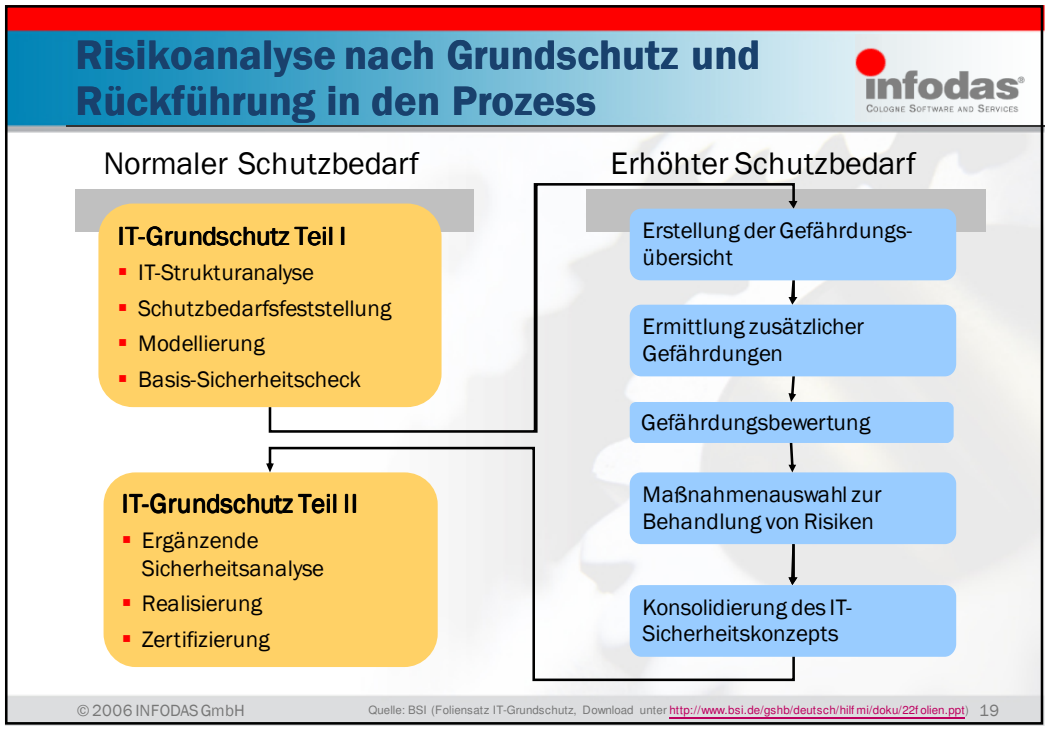
Eine ergänzende Sicherheits-analyse ist durchzuführen, wenn

- hoher oder sehr hoher Schutzbedarf vorliegt,
- zusätzlicher Analysebedarf besteht oder
- für bestimmte Aspekte kein geeigneter Baustein im IT-Grundschutzhandbuch existiert.



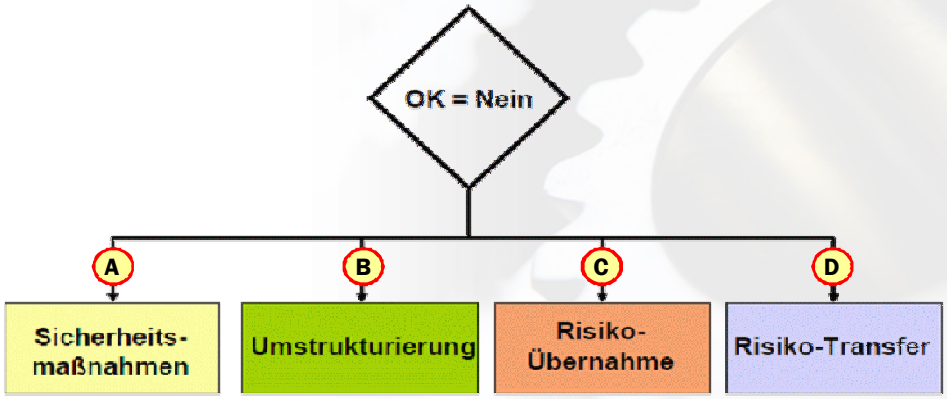
© 2006 INFODAS GmbH Quelle: BSI 17


Vorgehen bei der ergänzenden Sicherheitsanalyse
infodas
COLOGNE SOFTWARE AND SERVICES
IT-Grundschutzanalyse:
Modellierung des IT-Verbundes
Basis-Sicherheitscheck (Soll-Ist-Vergleich)
Ergänzende Sicherheitsbetrachtung
Management-Report
Risikoanalyse auf der Basis von IT-Grundschutz
Konsolidierung der Maßnahmen
Realisierung der Maßnahmen
© 2006 INFODAS GmbH
Quelle: BSI
18


Risikoanalyse nach Grundschutz und Rückführung in den Prozess
infodas
COLOGNE SOFTWARE AND SERVICES
Normaler Schutzbedarf
Erhöhter Schutzbedarf
IT-Grundschutz Teil I
IT-Strukturanalyse
Schutzbedarfsfeststellung
Modellierung
Basis-Sicherheitscheck
IT-Grundschutz Teil II
Ergänzende Sicherheitsanalyse
Realisierung
Zertifizierung
Erstellung der Gefährdungs-übersicht
Ermittlung zusätzlicher Gefährdungen
Gefährdungsbewertung
Maßnahmenauswahl zur Behandlung von Risiken
Konsolidierung des IT-Sicherheitskonzepts
© 2006 INFODAS GmbH
Quelle: BSI (Foliensatz IT-Grundschutz, Download unter http://www.bsi.de/gshb/deutsch/hilfmi/doku/22folien.ppt)
19

Behandlung verbleibender Risiken

- Prüfung der identifizierten Risiken:
  - Vollständigkeit der Umsetzung der zugeordneten Maßnahmen
  - ausreichende Abdeckung durch diese Maßnahmen



© 2006 INFODAS GmbH Vorgehen gemäß BSI-Standard 100-3, Kap. 6, Download unter http://www.bsi.de/literat/bsi_standard/standard_1003.pdf 20

Behandlung von Risiken

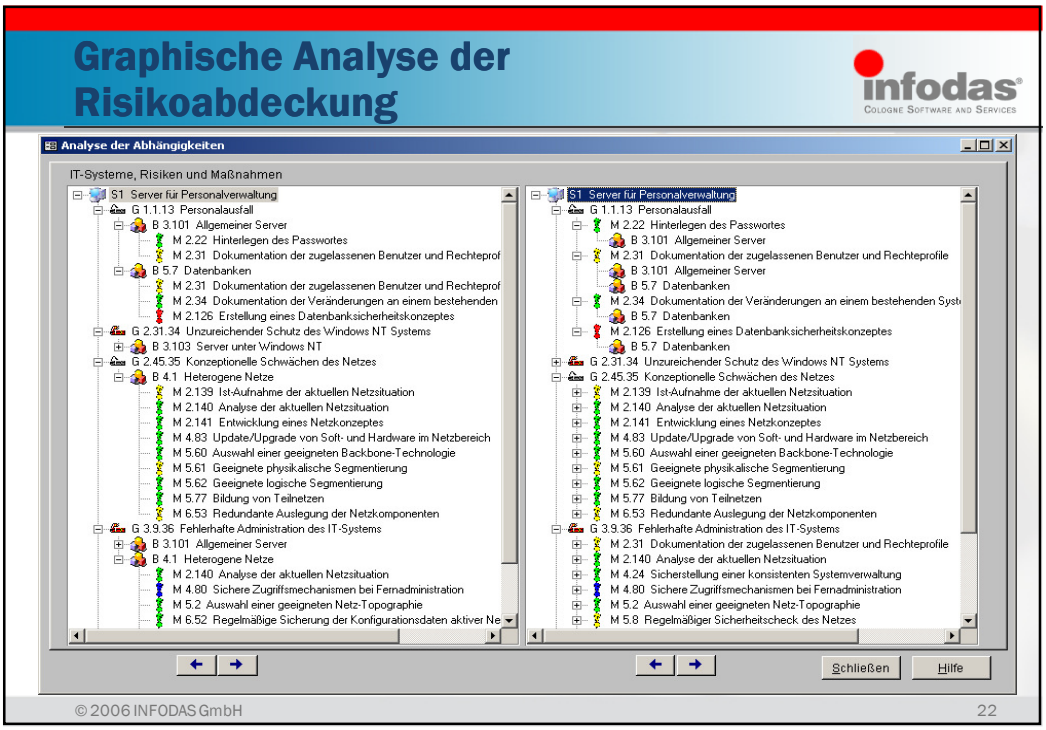
A Risiko-Reduktion durch weitere Sicherheitsmaßnahmen:
- Die verbleibende Gefährdung wird beseitigt, indem eine oder mehrere zusätzliche IT-Sicherheitsmaßnahmen erarbeitet und um-gesetzt werden, die der Gefährdung hinreichend entgegenwirken.

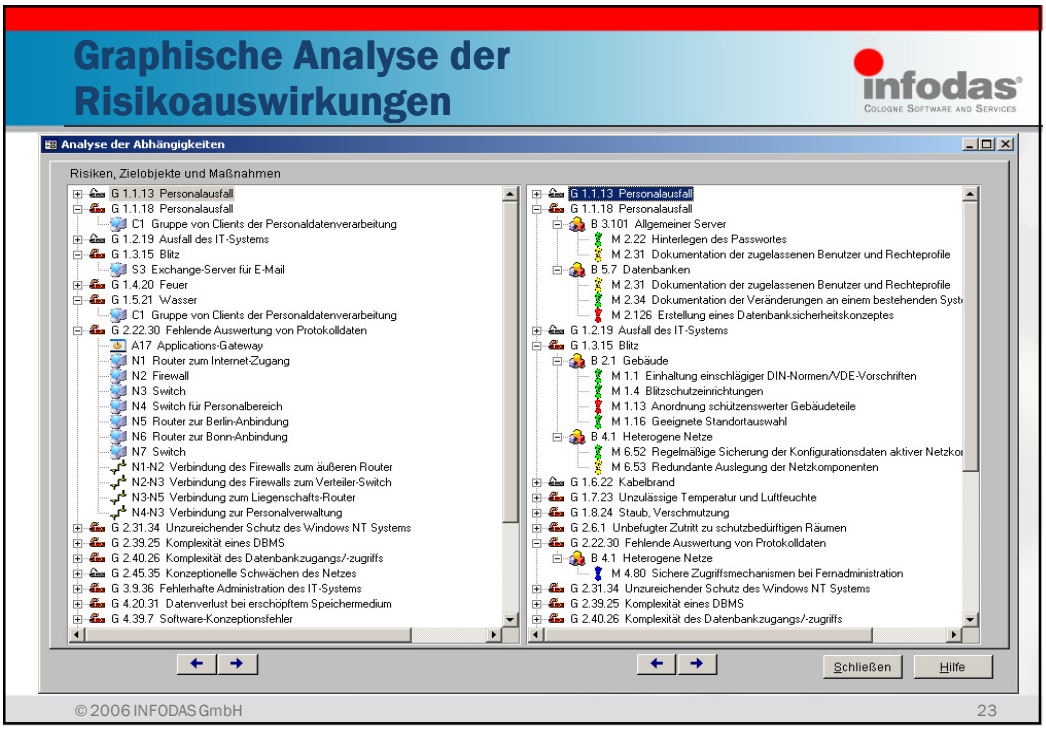
B Risiko-Reduktion durch Umstrukturierung:
- Die verbleibende Gefährdung wird beseitigt, indem der Geschäftsprozess oder der IT-Verbund umstrukturiert wird.

C Risiko-Übernahme:
- Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird akzeptiert.

D Risiko-Transfer:
- Das Risiko, das sich durch die verbleibende Gefährdung ergibt, wird an eine andere Institution übertragen, zum Beispiel durch Abschluss eines Versicherungsvertrags oder durch Outsourcing.

© 2006 INFODAS GmbH 21

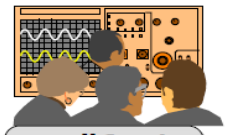

Graphische Analyse der Risikoabdeckung
infodas
COLOGNE SOFTWARE AND SERVICES
Analyse der Abhängigkeiten
IT-Systeme, Risiken und Maßnahmen
S1 Server für Personalverwaltung
G 1.1.13 Personalausfall
B 3.101 Allgemeiner Server
M 2.22 Hinterlegen des Passwortes
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprof
B 5.7 Datenbanken
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprof
M 2.34 Dokumentation der Veränderungen an einem bestehenden
M 2.126 Erstellung eines Datenbanksicherheitskonzeptes
G 2.31.34 Unzureichender Schutz des Windows NT Systems
B 3.103 Server unter Windows NT
G 2.45.35 Konzeptionelle Schwächen des Netzes
B 4.1 Heterogene Netze
M 2.139 Ist-Aufnahme der aktuellen Netzsituation
M 2.140 Analyse der aktuellen Netzsituation
M 2.141 Entwicklung eines Netzkonzeptes
M 4.83 Update/Upgrade von Soft- und Hardware im Netzbereich
M 5.60 Auswahl einer geeigneten Backbone-Technologie
M 5.61 Geeignete physikalische Segmentierung
M 5.62 Geeignete logische Segmentierung
M 5.77 Bildung von Teilnetzen
M 6.53 Redundante Auslegung der Netzkomponenten
G 3.9.36 Fehlerhafte Administration des IT-Systems
B 3.101 Allgemeiner Server
B 4.1 Heterogene Netze
M 2.140 Analyse der aktuellen Netzsituation
M 4.80 Sichere Zugriffsmechanismen bei Fernadministration
M 5.2 Auswahl einer geeigneten Netz-Topographie
M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Ne
S1 Server für Personalverwaltung
G 1.1.13 Personalausfall
M 2.22 Hinterlegen des Passwortes
B 3.101 Allgemeiner Server
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile
B 3.101 Allgemeiner Server
B 5.7 Datenbanken
M 2.34 Dokumentation der Veränderungen an einem bestehenden Syst
B 5.7 Datenbanken
M 2.126 Erstellung eines Datenbanksicherheitskonzeptes
B 5.7 Datenbanken
G 2.31.34 Unzureichender Schutz des Windows NT Systems
G 2.45.35 Konzeptionelle Schwächen des Netzes
M 2.139 Ist-Aufnahme der aktuellen Netzsituation
M 2.140 Analyse der aktuellen Netzsituation
M 2.141 Entwicklung eines Netzkonzeptes
M 4.83 Update/Upgrade von Soft- und Hardware im Netzbereich
M 5.60 Auswahl einer geeigneten Backbone-Technologie
M 5.61 Geeignete physikalische Segmentierung
M 5.62 Geeignete logische Segmentierung
M 5.77 Bildung von Teilnetzen
M 6.53 Redundante Auslegung der Netzkomponenten
G 3.9.36 Fehlerhafte Administration des IT-Systems
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile
M 2.140 Analyse der aktuellen Netzsituation
M 4.24 Sicherstellung einer konsistenten Systemverwaltung
M 4.80 Sichere Zugriffsmechanismen bei Fernadministration
M 5.2 Auswahl einer geeigneten Netz-Topographie
M 5.8 Regelmäßiger Sicherheitscheck des Netzes
Schließen
Hilfe
© 2006 INFODAS GmbH
22


Graphische Analyse der Risikoauswirkungen
infodas
COLOGNE SOFTWARE AND SERVICES
Analyse der Abhängigkeiten
Risiken, Zielobjekte und Maßnahmen
G 1.1.13 Personalausfall
G 1.1.18 Personalausfall
C1 Gruppe von Clients der Personaldatenverarbeitung
G 1.2.19 Ausfall des IT-Systems
G 1.3.15 Blitz
S3 Exchange-Server für E-Mail
G 1.4.20 Feuer
G 1.5.21 Wasser
C1 Gruppe von Clients der Personaldatenverarbeitung
G 2.22.30 Fehlende Auswertung von Protokolldaten
A17 Applications-Gateway
N1 Router zum Internet-Zugang
N2 Firewall
N3 Switch
N4 Switch für Personalbereich
N5 Router zur Berlin-Anbindung
N6 Router zur Bonn-Anbindung
N7 Switch
N1-N2 Verbindung des Firewalls zum äußeren Router
N2-N3 Verbindung des Firewalls zum Verteiler-Switch
N3-N5 Verbindung zum Liegenschafts-Router
N4-N3 Verbindung zur Personalverwaltung
G 2.31.34 Unzureichender Schutz des Windows NT Systems
G 2.39.25 Komplexität eines DBMS
G 2.40.26 Komplexität des Datenbankzugangs/-zugriffs
G 2.45.35 Konzeptionelle Schwächen des Netzes
G 3.9.36 Fehlerhafte Administration des IT-Systems
G 4.20.31 Datenverlust bei erschöpftem Speichermedium
G 4.39.7 Software-Konzeptionsfehler
G 1.1.13 Personalausfall
G 1.1.18 Personalausfall
B 3.101 Allgemeiner Server
M 2.22 Hinterlegen des Passwortes
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile
B 5.7 Datenbanken
M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile
M 2.34 Dokumentation der Veränderungen an einem bestehenden Syst
M 2.126 Erstellung eines Datenbanksicherheitskonzeptes
G 1.2.19 Ausfall des IT-Systems
G 1.3.15 Blitz
B 2.1 Gebäude
M 1.1 Einhaltung einschlägiger DIN-Normen/VDE-Vorschriften
M 1.4 Blitzschutzeinrichtungen
M 1.13 Anordnung schützenswerter Gebäudeteile
M 1.16 Geeignete Standortauswahl
B 4.1 Heterogene Netze
M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzko
M 6.53 Redundante Auslegung der Netzkomponenten
G 1.6.22 Kabelbrand
G 1.7.23 Unzulässige Temperatur und Luftfeuchte
G 1.8.24 Staub, Verschmutzung
G 2.6.1 Unbefugter Zutritt zu schutzbedürftigen Räumen
G 2.22.30 Fehlende Auswertung von Protokolldaten
B 4.1 Heterogene Netze
M 4.80 Sichere Zugriffsmechanismen bei Fernadministration
G 2.31.34 Unzureichender Schutz des Windows NT Systems
G 2.39.25 Komplexität eines DBMS
G 2.40.26 Komplexität des Datenbankzugangs/-zugriffs
Schließen
Hilfe
© 2006 INFODAS GmbH
23

Zertifizierung: Beteiligte Stellen

Antragsteller

- Umsetzung von IT-Grundschutz



Prüfer/ Auditor

- Prüfung des IT-Verbunds
- Erstellung eines Auditreports

Zertifizierungs-stelle

- Anforderungen an Prüfer/ Auditoren
- Lizenzierung von Auditoren
- Prüfschema
- Prüfung des Auditreports
- Veröffentlichung

© 2006 INFODAS GmbH Quelle: BSI 24

Phasen der ISO 27001-Zertifizierung

Initialisierung
- Zertifizierungs-Antrag
- Befugnis für die Durchführung eines Audits
- Ggf. Abstimmung des IT-Verbundes

Durchführung des Audits
- Prüfung der Dokumentation
- Vorbereitung des Audit-Tätigkeiten vor Ort
- Durchführung der Audit-Tätigkeiten vor Ort

Bewertung des Audits
- Erstellung des Auditreports
- Nachprüfung

Re-Zertifizierungs-Audit

© 2006 INFODAS GmbH Quelle: BSI 25

Prüfschema für ISO 27001-Audits auf der Basis von IT-Grundschutz

- IT-Grundschutz-Analyse als Voraussetzung
  - Auf Basis der aktuellen IT-GSK oder direkter Vorgängerversion
  - Basis-Sicherheitsüberprüfung
  - Ergänzende Sicherheitsanalyse
- Beschreibung sämtlicher Ablaufschritte in einem transparenten Prüfplan
  - Beantragung des Zertifikats
  - Dokumentenprüfung
  - Inspektion vor Ort
  - Bewertung und Nachvollziehbarkeit
  - Erstellen des Auditreports


Bundesamt für Sicherheit in der Informationstechnik

Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Prüfschema für ISO 27001-Audits

Stand: 1. Februar 2006

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik

© 2006 INFODAS GmbH
Download: http://www.bsi.de/gshb/zert/ISO27001/Pruefschema06.pdf 26

Vorgehen zur Zertifizierung

- Identifikation des Untersuchungsgegenstands
  - Geschäftsbereich Hosting der SAP Systems Integration AG
- Abgrenzung des IT-Verbunds
  - Router stellen die Schnittstelle zum Kunden dar
  - Kundensysteme sind gegeneinander isoliert
  - eventuelle Sicherheitslücken bei einem Kunden beeinflussen das SAP SI Netz und Systeme anderer Kunden nicht
- Abstimmung mit dem BSI hinsichtlich einer Zertifizierung
  - Prüfung des bereinigten Netzplans
  - Prüfung, ob alle relevanten Grundschutzbausteine betrachtet wurden
- Durchführung des Audits (ISO 27001-Auditor)
- Erstellung des Auditreports
- Prüfung durch die Zertifizierungsstelle

© 2006 INFODAS GmbH 27

Das Zertifizierungs-Audit

- Anforderungen ergeben sich aus dem Prüfschema für Auditoren
- Prüfung kann relativ schnell erfolgen, wenn
  - die Vorprüfung sorgfältig durchgeführt wurde
  - alle Ergebnisse der Vorprüfung sauber dokumentiert sind
  - die Dokumentation der Vorprüfung in einer direkt für die Zertifizierung nutzbaren Form erfolgt ist
  - der IT-Verbund nach der Vorprüfung nicht mehr verändert wurde
    - Zertifizierungs-Audit sollte zeitnah nach der Vorprüfung erfolgen
    - Zeitraum für die Nachbesserungen wird hierdurch eingeschränkt
- Vollständigkeit der Dokumente muss gegeben sein
- Verifikation beschränkt sich auf Stichproben

© 2006 INFODAS GmbH 28

Ergebnisse des Zertifizierungs-Audits

- Sichtung der Referenzdokumente
  - ✓ A1 IT-Strukturanalyse
  - ✓ A2 Schutzbedarfsfeststellung
  - ✓ A3 Modellierung des IT-Verbunds
    - Anwendbarkeit der Grundschutz-Methodik: durch Verwendung des SAP-Bausteins sichergestellt
    - Korrektheit der Gruppenbildung: durch zentrale Verwaltung des IT-Verbunds gewährleistet
  - ✓ A4 Basis-Sicherheitscheck
    - Konsistenz durch Werkzeugeinsatz
  - ✓ A5/6 Ergänzende Sicherheitsanalyse und Risikoanalyse
    - Probleme wurden im Projekt erkannt und gelöst

© 2006 INFODAS GmbH 29

Ergebnisse des Zertifizierungs-Audits

- Inspektion vor Ort
  - ✓ B1 Verifikation des Netzplans
    - Vergleich des virtuellen RZ mit dem realen
      → alle Komponenten waren aufzufinden
  - ✓ B2 Verifikation der Liste der IT-Systeme
  - ✓ B3 Verifikation des Basis-Sicherheitschecks
    - Auswahl der zu prüfenden Bausteine
    - Prüfung der Maßnahmenumsetzung
    - Dokumentation der Abweichungen
      nur Verbesserungen – keine Lücken festgestellt
- Keine Nachbesserungen erforderlich

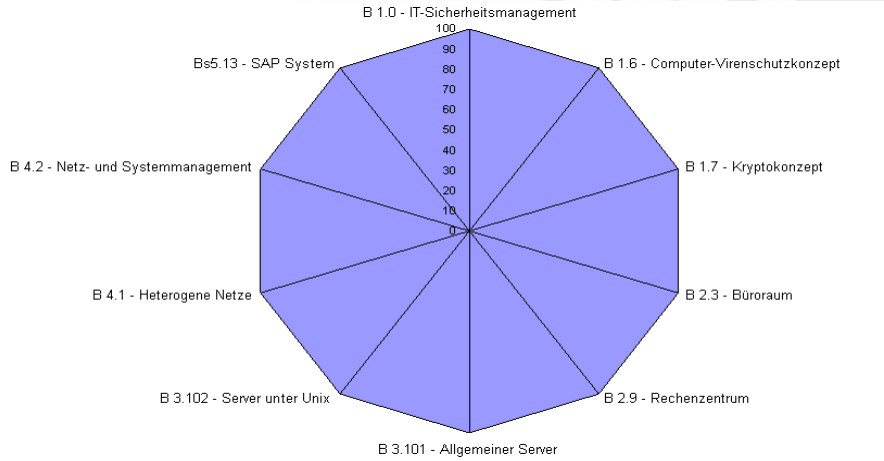
© 2006 INFODAS GmbH 30

Bausteine für die Verifikation des Basis-Sicherheitschecks

- Pflichtbaustein:
  - B 1.0 IT-Sicherheitsmanagement
- Zufällig ausgewählte Bausteine:
  - B 1.7 Kryptokonzept
  - B 2.3 Büroraum
  - B 3.102 Server unter Unix
  - B 4.1 Heterogene Netze
  - Bs5.13 SAP System
- Gezielt ausgewählte Bausteine:
  - B 1.6 Computer-Virenschutzkonzept
  - B 2.9 Rechenzentrum
  - B 3.101 Allgemeiner Server
  - B 4.2 Netz- und Systemmanagement

© 2006 INFODAS GmbH 31

Ergebnis der Verifikation



- nicht überraschend ...

© 2006 INFODAS GmbH 32

Beispiel: Verifikationsbericht

324 Verifikation des Basis-Sicherheitschecks

Bundesamt für Organisation und Verwaltung (BOV)
Daten für Zertifikats-Audit

B 1.1 Organisation

Zugeordnete Komponenten:	übergeordnet
Standort:	Hauptgebäude
Durchführung der Überprüfung:	16.03.2005
Durchführende(r) Auditor(en):	Wk
Befragte Mitarbeiter der Institution:	Geschäftsleitung
Referenz:	Standort Bonn

M 2.1 Festlegung von Verantwortlichkeiten und Regelungen für den IT-Einsatz

Stufe: Einstieg

Ergebnis des Basis-Sicherheitschecks: **Status:** Die Maßnahme ist teilweise umgesetzt.
Die Regelungen sind im Bereich RZ nicht vollständig dokumentiert.

Ergebnis des Zertifikats-Audits: **Status:** Die Maßnahme ist vollständig umgesetzt.
Die notwendigen Regelungen wurden inzwischen schriftlich formuliert und sind verabschiedet. Eine stichprobenhafte Überprüfung zeigte, dass die Regelungen sinnvoll und auch den Mitarbeitern bekannt sind.

Votum: Die Anforderungen dieser Maßnahme werden erfüllt.

© 2006 INFODAS GmbH 33

Audit-Bericht

Auditierung der SAP SI AG
Geschäftsbereich Hosting
zur Erlangung eines IT-Grundschutz-Zertifikats

Version V2.2
Stand: 23.06.2006
Auditor: Dr. Gerhard Weck
BSI-IGL-0063-2006

© 2006 INFODAS GmbH 34

Erfolgsfaktoren

- Enge Verbindung von IT-Sicherheit und QM beim AG
  - IT-Sicherheit wird als Qualitätsmerkmal behandelt
  - Sicherheitsanforderungen sind in SLAs der Kunden festgelegt
  - vollständige und aktuelle Dokumentation erlaubt einfachen Vergleich mit den Ergebnissen des früheren Audits
- Nutzung eines geeigneten Werkzeugs: SAVe®
  - erleichtert Vergleich zwischen erstem und zweitem Audit
  - erlaubt detaillierte Konsistenz- und Vollständigkeitskontrolle
  - Verfolgung der Querbeziehungen zwischen Risiken und Maßnahmen
- Gute und enge Zusammenarbeit mit dem BSI
  - schnelle und unbürokratische Klärung offener Fragen
  - Feedback über die Anwendung der Risikoanalyse nach Std. 100-3

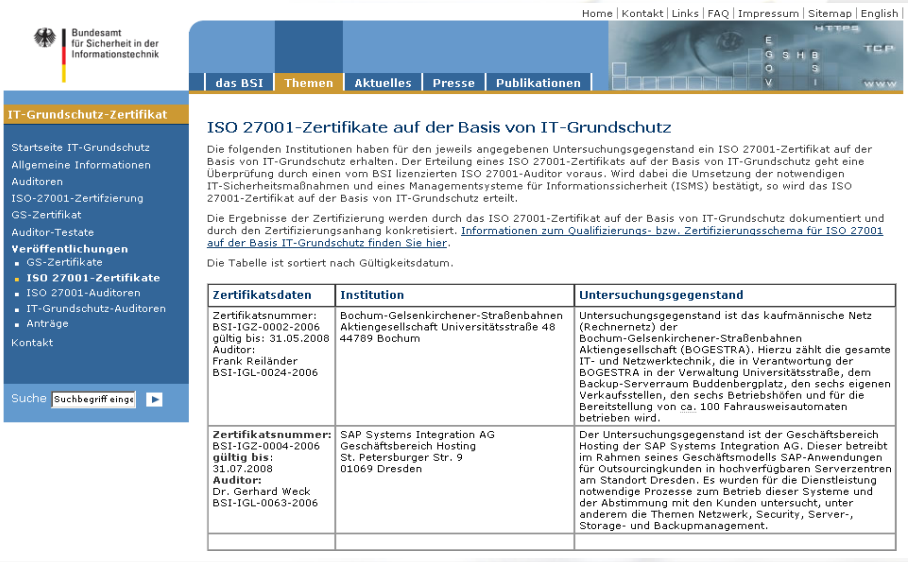
© 2006 INFODAS GmbH 35

Der Nachweis von IT-Sicherheit kann sich lohnen...

- Kenntnis und Optimierung der internen Prozesse führt zu einem geordneten, effektiven und effizienten IT-Betrieb
  - mittelfristige Kosteneinsparungen
- Das IT-Sicherheitsniveau wird messbar
- IT-Sicherheit als Qualitätsmerkmal
  - Erhöhung der Attraktivität für Kunden und Geschäftspartner mit hohen Sicherheitsanforderungen
  - Mitarbeiter und Unternehmensleitung identifizieren sich mit IT-Sicherheitszielen und sind stolz auf das Erreichte.
  - Versicherungen honorieren zunehmend IT-Sicherheit.

© 2006 INFODAS GmbH 36

Veröffentlichung der ISO 27001 Zertifikate



© 2006 INFODAS GmbH Quelle: http://www.bsi.de/gshb/zert/veroeffentl/iso27001_zertifikate.htm - Stand:26.10.2006 37

infodas
COLOGNE SOFTWARE AND SERVICES

Danke für Ihre Aufmerksamkeit!

Dr. Gerhard Weck, Leiter IT Security Consulting
INFODAS GmbH, Rhonestraße 2, 50765 Köln
☎ (0221) 70912-52 * 🖷 (0221) 70912-55
g.weck@infodas.de www.infodas.de