



# 3612 Seiten IT-Sicherheit - ISO 27001 auf der Basis von IT-Grundschutz

Institut für Informatik und Automation

Dipl.-Inf. Günther Diederich

- **In-Institut der Hochschule Bremen**
- **Seit 1997 aktiv**
- **35 Mitglieder**
- **Verbindung von Informatik und Automation mit Geschäftsabläufen**
  
- **Schwerpunkte der Gruppe um Prof. Sethmann**
  - **Rechnernetze**
  - **Sicherheit in Netzen**
  - **Mobile Netze**
- **Mitglied des Mobile Research Center Bremen**



---

## Ein Einblick in die Arbeit mit Standards am Beispiel ISO 27001 auf der Basis von IT-Grundschutz

- **Arbeiten mit Standards – Pro und Contra**
- **Zentrale Punkte in der Arbeit mit  
ISO 27001 auf der Basis von IT-Grundschutz**
- **Entstehung einer IT-Sicherheitsleitlinie**
- **Entwicklung des IT-Sicherheitskonzepts**
- **Aufbau eines IT-Grundschutz-Bausteins  
Beispiel: Baustein Router und Switches**

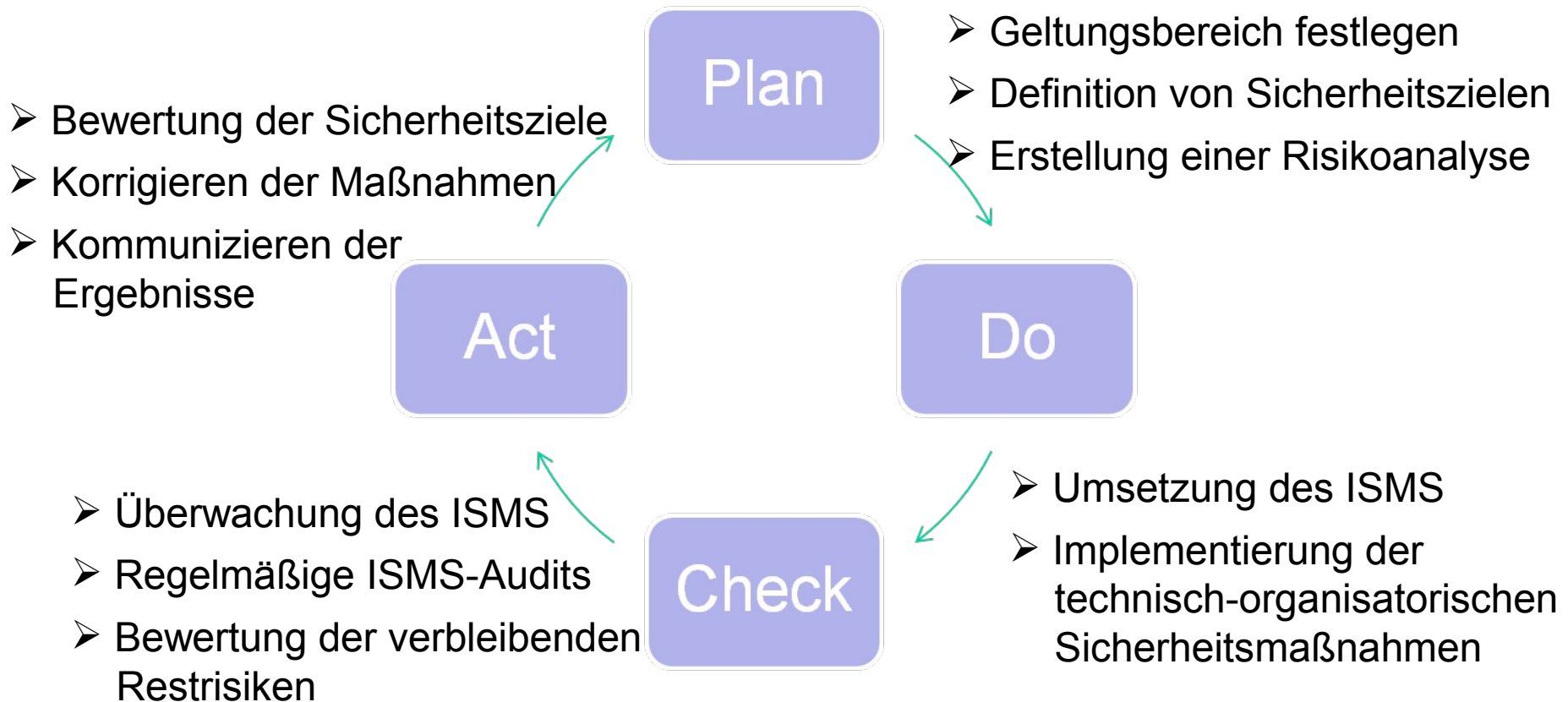
- **IT-Sicherheits- und Risikomanagement**
  - ISO 13335 (Management von Sicherheit der Informations- und Kommunikationstechnik (IuK))
  - ISO/IEC 27002 [zuvor 17799] (Leitfaden zum Informationssicherheitsmanagement)
- **Sicherheitsmaßnahmen und Monitoring**
  - ISO/IEC 18028 (IT-Netzwerksicherheit)
  - ISO/IEC TR 18044 (Management von Vorfällen in der IT-Sicherheit)
- **Standards mit IT-Sicherheitsaspekten**
  - Cobit (Control Objectives for Information and Related Technology)
  - ITIL (IT Infrastructure Library, Best Practice Referenzmodell für IT-Serviceprozesse, BS 15000 mittlerweile ISO 20000)
  - IDW PS 330 (Institut der Wirtschaftsprüfer in Deutschland e.V.: Abschlussprüfung bei Einsatz von Informationstechnologie“)
- **Vorschriften**
  - KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
  - SOX / EURO-SOX (SOX Sektion 404: Ordnungsmäßigkeit der Verarbeitung und die Integrität der verarbeiteten relevanten Finanzdaten ist jederzeit gewährleistet)
- **...und noch sehr viel mehr (Physische Sicherheit, Kryptographie,...)**

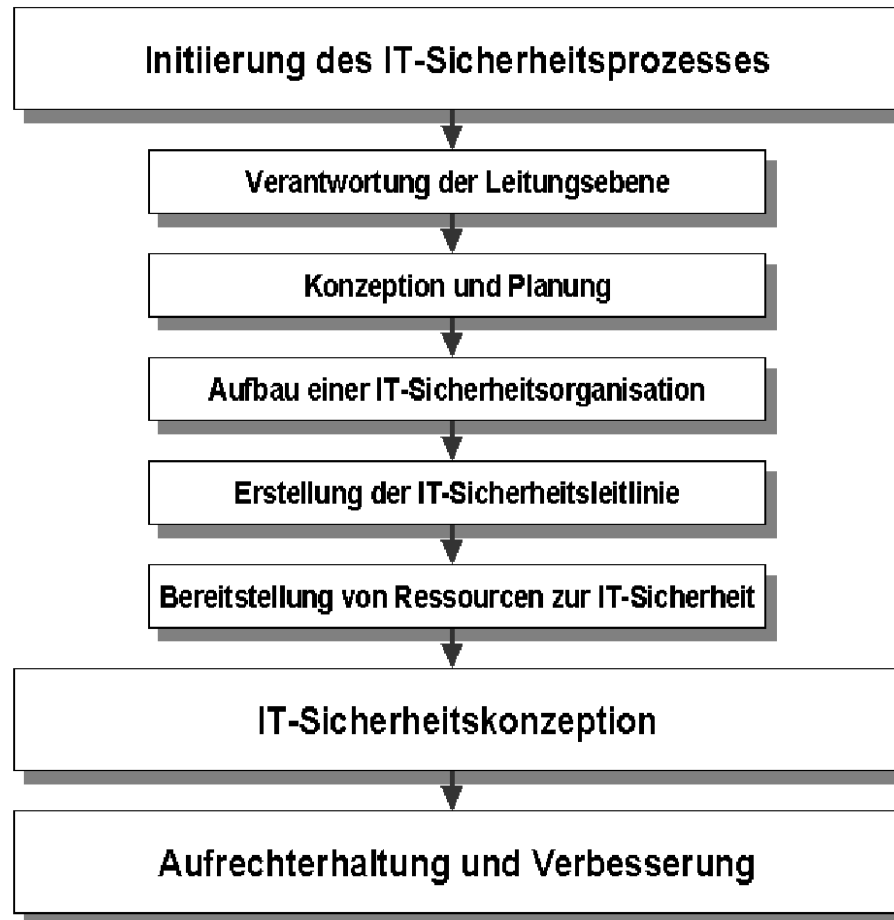
- ☹ **Braucht Zeit**
- ☹ **Viel Geld**  
**(Zertifizierung,  
Rezertifizierung)**
- ☹ **Mehr Personal**
- ☹ **Kompliziertere  
Arbeitsabläufe**
- ☹ **Verhindert  
Innovation**



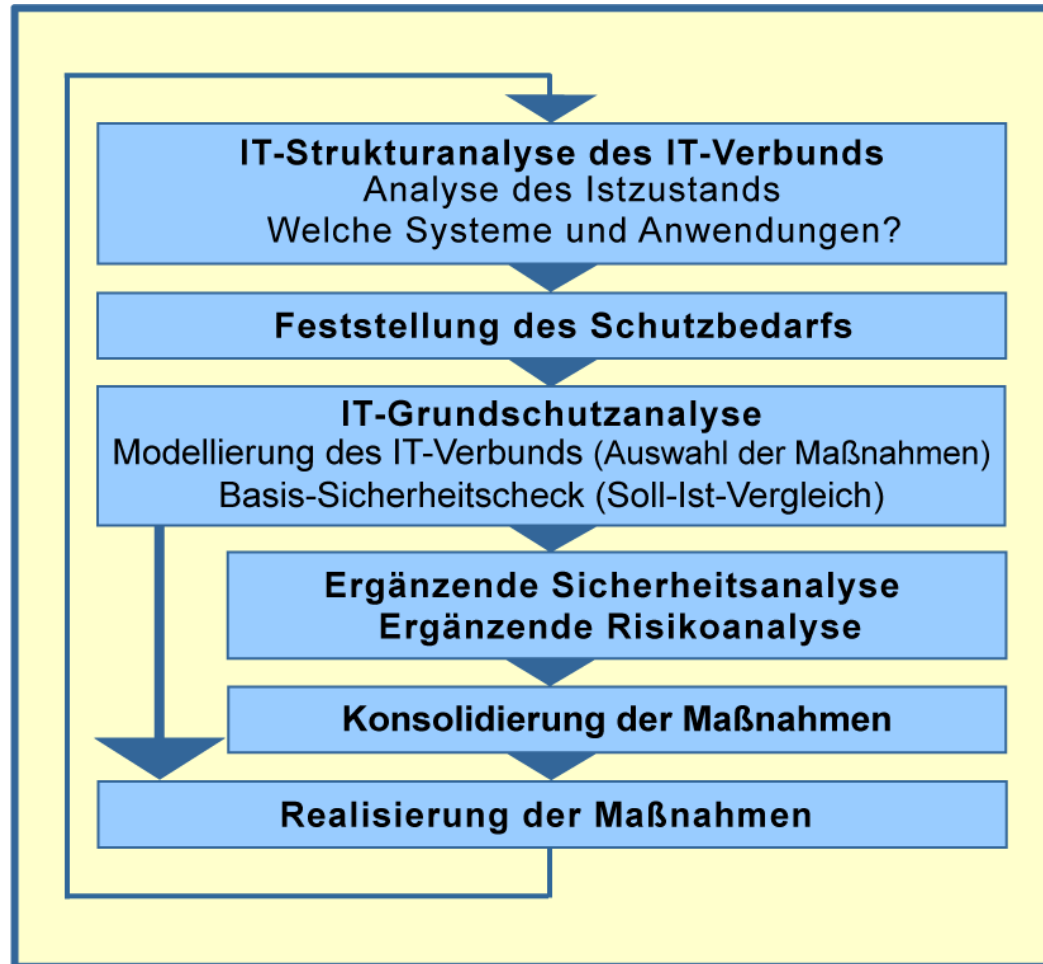
- ☺ **Methodisches Vorgehen / Soll-Ist-Vergleich**
- ☺ **Vollständige Abdeckung einer best. Menge von Gefährdungen**
- ☺ **Referenzierbare / übertragbare Konzepte oder Maßnahmen**
- ☺ **Praxiserprobte Maßnahmen (Best Practice)**
- ☺ **Optimierung interner Prozesse / klare Vorgaben**
- ☺ **Nachvollziehbare / quantifizierbare IT-Sicherheit**

# Methode Plan-Do-Check-Act





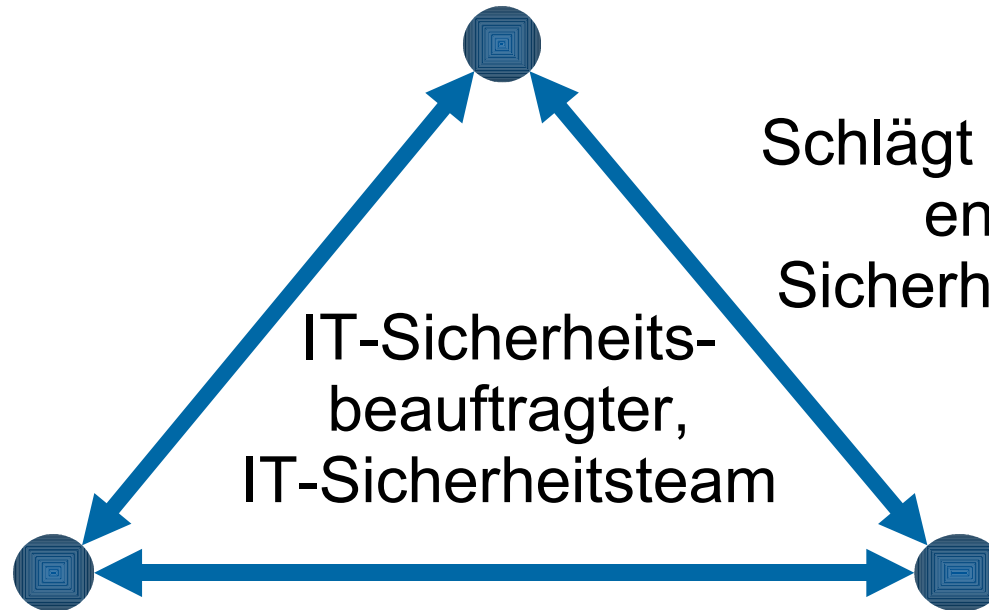
# Entwicklung eines IT-Sicherheitskonzepts



- **BSI Standards**
  - **BSI-Standard 100-1:**  
**Managementsysteme für Informationssicherheit**
  - **BSI-Standard 100-2:**  
**Vorgehensweise nach IT-Grundschutz**
  - **BSI-Standard 100-3:**  
**Risikoanalyse auf der Basis von IT-Grundschutz**
  - **BSI-Standard 100-4:**  
**Notfall-Management**
- **IT-Grundschutzkataloge**
  - **Loseblattsammlung**
  - **Themenorientierte Bausteine (z.B. Server unter Linux)**
  - **Gefährdungs- und Maßnahmenkataloge**
- **Ermöglicht Zertifizierung nach  
ISO 27001 auf der Basis von IT-Grundschutz**



Geschäftsführung:  
Setzt Ziele, bestimmt Vorgehensweisen



Schlägt Leitlinien vor,  
entwickelt  
Sicherheitskonzepte

IT-Sicherheits-  
beauftragter,  
IT-Sicherheitsteam

IT-Abteilung:  
Stellt Technik,  
entwickelt Lösungen

Finanzen:  
Liefert Kennzahlen,  
Qualitätsmerkmale

## Die Geschäftsführung hat festgelegt (BSI 100-1, BSI 100-2):

- Die Leitung verabschiedet hiermit folgende **IT-Sicherheitsleitlinie als Bestandteil ihrer Strategie**
- Unsere Daten und unsere IT-Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer **Verfügbarkeit** so gesichert, dass die **zu erwartenden Stillstandszeiten minimal sind**
- **Die Koordination der IT-Sicherheit gehört zu den Tätigkeiten der Administratoren**, ein externer Berater koordiniert den Aufbau der IT-Sicherheit
- **Für unsere Kunden** ist die Verfügbarkeit der durch uns betriebenen Serversysteme **wichtig**, da interne Prozesse des Kunden von der Verfügbarkeit abhängen. Durch die Umsetzung technischer und organisatorischer Maßnahmen gewährleisten wir, **dass alle Server hochverfügbar sind**.

## Rückmeldungen zur IT-Sicherheitsleitlinie:

- Die Leitung verabschiedet hiermit folgende IT-Sicherheitsleitlinie als Bestandteil ihrer Strategie
  - Alle Beteiligten: Die GF will IT-Sicherheit und beschreibt sie in dieser Leitlinie
- ...werden in ihrer **Verfügbarkeit** so gesichert, dass die **zu erwartenden Stillstandszeiten minimal sind**
  - IT: 24/7? Kein Problem, wir benötigen für alle Server und Router hot stand-by Ersatzgeräte und ...
  - Finanzen: Das ist teuer, muss es 24/7 sein? Wirklich für alle?
- **Die Koordination der IT-Sicherheit gehört zu den Tätigkeiten der Administratoren, ...**
  - IT: Die fortlaufenden Berichte verzögern unsere Arbeit
  - IT-Sicherheitskoordinator (Berater): Die Administratoren würden für ihre eigene Arbeit eine Qualitätssicherung durchführen

## Rückmeldungen zur IT-Sicherheitsleitlinie (fortgesetzt):

- Für unsere Kunden ist die Verfügbarkeit der durch uns betriebenen Serversysteme **wichtig**, da interne Prozesse des Kunden von der Verfügbarkeit abhängen. Durch die Umsetzung technischer und organisatorischer Maßnahmen gewährleisten wir, **dass alle Server hochverfügbar sind**.
  - IT: Alle Kundenserver sind durch ein Backup gesichert und stehen bereits am nächsten Werktag wieder zur Verfügung
  - Finanzen: Im QS-Prozess „Verkauf“ sind 3 Verträge mit unterschiedlichen Verfügbarkeiten vorgesehen, die sollten unterschiedlich abgerechnet werden
  - Finanzen: Wieso Werktag? In unseren Premium-Verträgen steht Kalendertag!
  - IT-Sicherheitskoordinator (Berater): Wo ist der Unterschied zwischen „hochverfügbar“ und „minimaler Stillstand?“

## Direkte Ergebnisse aus dem Teilschritt IT-Sicherheitsleitlinie:

- Sensibilisierung aller Beteiligten
- Gemeinsames Bild der IT-Sicherheit
- Einheitliche Begriffe vermeiden Missverständnisse
- Gewachsene Prozesse werden überprüft und ggf. wieder zusammengeführt

## Korrekturen an der IT-Sicherheitsleitlinie

- ...werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten tolerabel sind.
- ...dass die Verfügbarkeitsanforderungen unserer Kunden eingehalten werden.
- Es ist ein IT-Sicherheitsbeauftragter benannt worden.  
Der IT-Sicherheitsbeauftragte sorgt für...

# Kurz zurück zur Theorie – Zielsetzung IT-Grundschutz

---

- Den **Aufwand reduzieren**, d.h.
  - bekannte Vorgehensweisen bündeln
  - Bewährte Vorgehensweisen wiederverwenden
- ein IT-Sicherheitsniveau erreichen, das **einem normalen Schutzbedarf angemessen** ist, indem empfohlene
  - organisatorische,
  - personelle,
  - infrastrukturelle und
  - technische Standard-Sicherheitsmaßnahmen in geeigneter Weise angewendet werden
- Eine **Basis für hochschutzbedürftige Geschäftsprozesse schaffen**

- **Aufgabe „IT“: Ist-Zustand erfassen  
(IT-Strukturanalyse des IT-Verbunds)**
  - **Alle IT-Anwendungen und zugehörige Informationen**
  - **Alle IT-Systeme**
  - **Netzplan**
  - **Alle Räume und Gebäude**
  - **Erfassen des Personals (Zugang/Zugriff)**
- **Komponenten im Netzplan zusammenfassen, wenn:**
  - **Sie vom gleichen Typ sind**
  - **Gleiche oder nahezu gleiche Konfiguration haben**
  - **Gleiche oder nahezu gleiche Netzanbindung haben  
(z. B. Anschluss am gleichen Switch)**
  - **Gleichen Rahmenbedingungen unterliegen  
(z.B. Administration und Infrastruktur)**
  - **Gleiche Anwendungen auf den Systemen laufen**

## Mögliche Dienstleistungen eines Rechenzentrums (RZ):

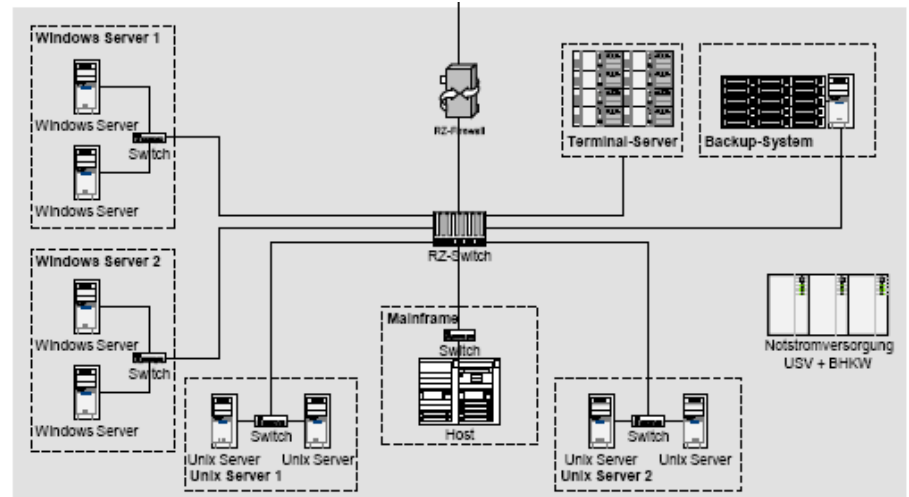
- **Housing**
  - RZ kontrolliert Gebäude, Räume, Personal
  - Kunde ist für Hardware, Betriebssystem, Anwendung und Daten verantwortlich
- **Root-Server**
  - RZ: Housing + Hardware
  - Kunde: Betriebssystem + Anwendung + Daten
- **Managed Server**
  - RZ: Root-Server + Betriebssystem
  - Kunde: Anwendung + Daten
- **Managed Application**
  - Managed Server + Anwendung
  - Kunde: Daten
- **Auftragsdatenverarbeitung durch das RZ**

# Was wäre wenn? Schutzbedarfsfeststellung

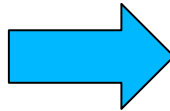
---

- Aufgabe „Finanzen“: **Schutzbedarf feststellen**
- Für die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität Schadensfälle beschreiben
- Betrachtung von **typischen Schadensszenarien** aus Sicht der Anwender ("**Was wäre, wenn... ?**"), z.B. bei:
  - Verstoß gegen Gesetze, Vorschriften, Verträge
  - Beeinträchtigung des informationellen Selbstbestimmungsrechts
  - Beeinträchtigung der persönlichen Unversehrtheit
  - Beeinträchtigung der Aufgabenerfüllung
  - negative Außenwirkung
  - finanzielle Auswirkungen
- **Schäden** quantifizieren oder qualitativ **beschreiben**, z.B. normal, mittel, hoch
- **Bestehende Dokumentationen prüfen & verwenden**

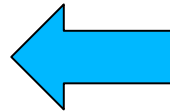
# Alles zusammen – IT-Sicherheitskonzept erstellen



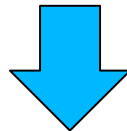
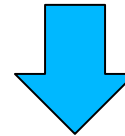
Prüfplan /  
Soll-Modell



**Basis-  
Sicherheitscheck**



Ist-Zustand



Handlungsbedarf ?

# Aufbau eines IT- Grundschutzbausteins

---

- **Beschreibung des Bausteins**
  - **Anwendbarkeit**
  - **Verweise auf andere Bausteine**
  - **Begriffsbestimmungen**
- **Typische Gefährdungen, z.B. für Router und Switche:**
  - **Fehlende Auswertung von Protokolldaten**
  - **Fehlerhafte Konfiguration von Routern und Switchen**
  - **Bekanntwerden von Softwareschwachstellen**
  - **Unberechtigter Anschluss von IT-Systemen an ein Netz**
- **Maßnahmeempfehlungen, z.B. für Router und Switche:**
  - **Gesicherte Aufstellung aktiver Netzkomponenten**
  - **Regelmäßige Kontrolle von Routern und Switches**
  - **Sichere Außerbetriebnahme von Routern und Switches**
  - **Software-Pflege auf Routern und Switches**

- **Erst Sicherheitsbedarf bestimmen**, dann geeigneten Standard (ggf. mehrere) suchen
- **Ausreichend Ressourcen einplanen**, insbesondere für die **Koordination** der verschiedenen Bereiche
- **Sicherheitsziele, Konzepte und Maßnahmen gut kommunizieren**
- **Sofort verwertbare Zwischenergebnisse nutzen**
- **Ergebnisse regelmäßig prüfen**
- **In jeder Phase gut dokumentieren**
- **Grenzen des Standards erkennen und ggf. ergänzen**
- **Hilfsmaterial verwenden, z.B.:**
  - **Webkurs IT-Grundschutz** (<http://www.bsi.de/gshb/webkurs/index.htm>)
  - **Checklisten, Formulare, Beispiele** (<http://www.bsi.de/gshb/deutsch/hilfmi/hilfmi.htm>)

- **IT-Sicherheitsniveau ist messbar / vergleichbar**
- **Bestätigung der IT-Sicherheit durch vertrauenswürdige Dritte für Kunden, Versicherungen, Banken...**
- **Unternehmensweit einheitliche Basis der IT-Sicherheit**
- **Optimierung der internen Prozesse**
- **Fundierte Fachkenntnis**
  - **Beispielkonzepte und Vorlagen**
  - **Maßnahmeempfehlungen**
  - **Studien und Dokumentationen**

# 3612 Seiten IT-Sicherheit – jeder Anfang ist schwer



Dipl.-Inf. Günther Diederich

Guenther.Diederich@hs-bremen.de

Tel: 0421 5905 5472

Fax: 0421 5905 5412

**Vielen Dank  
für Ihre  
Aufmerksamkeit!**

Quelle:failblog.wordpress.com

Akademietag 2008