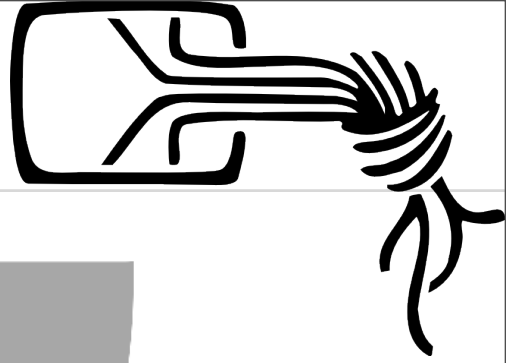
IT-Grundschutz

Manuel Atug & Daniel Jedecke

Chaos Computer Club Cologne (C4) e.V.

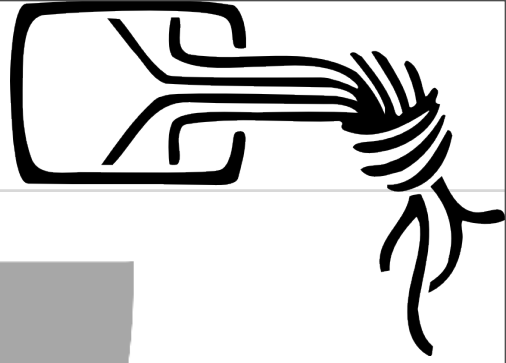
OpenChaos Januar 2007

IT-Grundschutzhandbuch



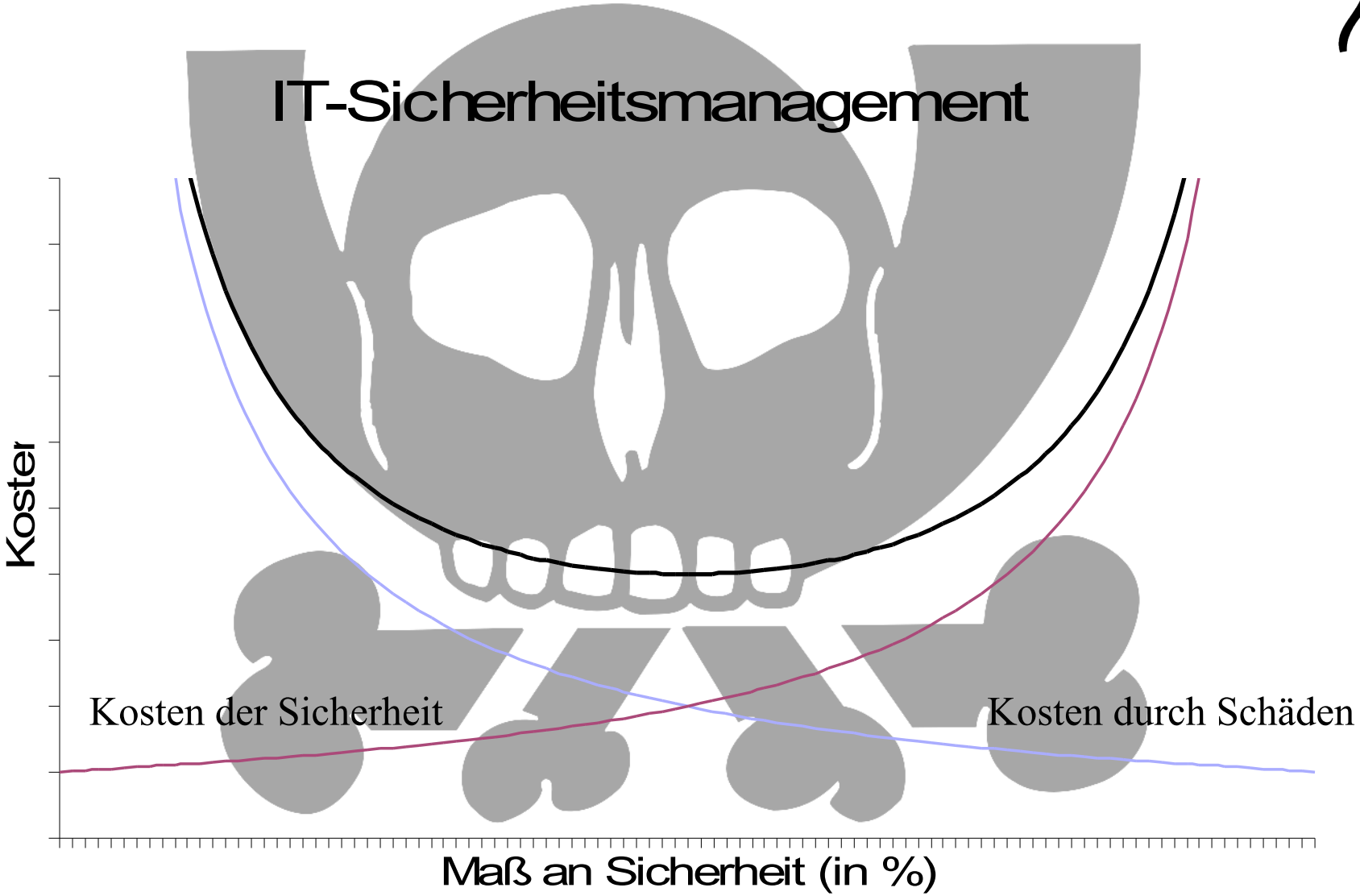
Agenda

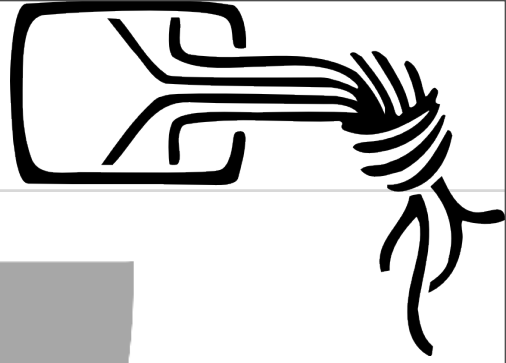
- Ziel der IT-Sicherheit
- Das IT-Grundschutzhandbuch
- Umsetzung des IT-Grundschutzhandbuchs
- Ausbaustufen und Zertifizierung



Ziel der IT-Sicherheit

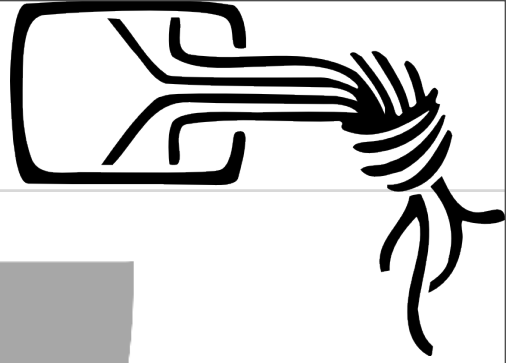
Ziel der IT-Sicherheit





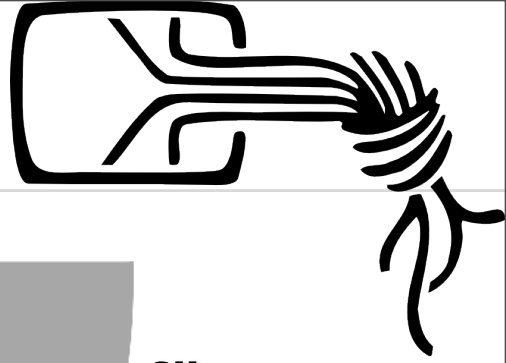
IT-Grundschutz

IT-Grundschutz



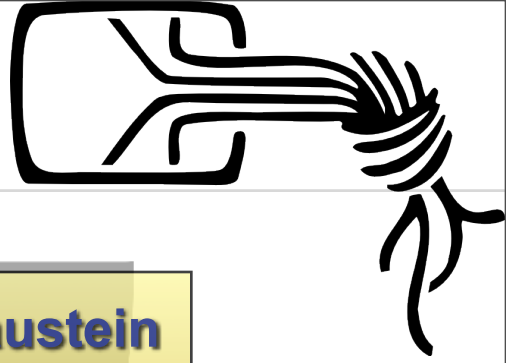
- **IT-Grundschutzhandbuch**
  - Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Standard-Sicherheitsmaßnahmen
    - Baukasten-Prinzip
  - Zertifizierbar mit IT-Grundschutz-Zertifikat des BSI
  - Quelle: http://www.bsi.de/gshb

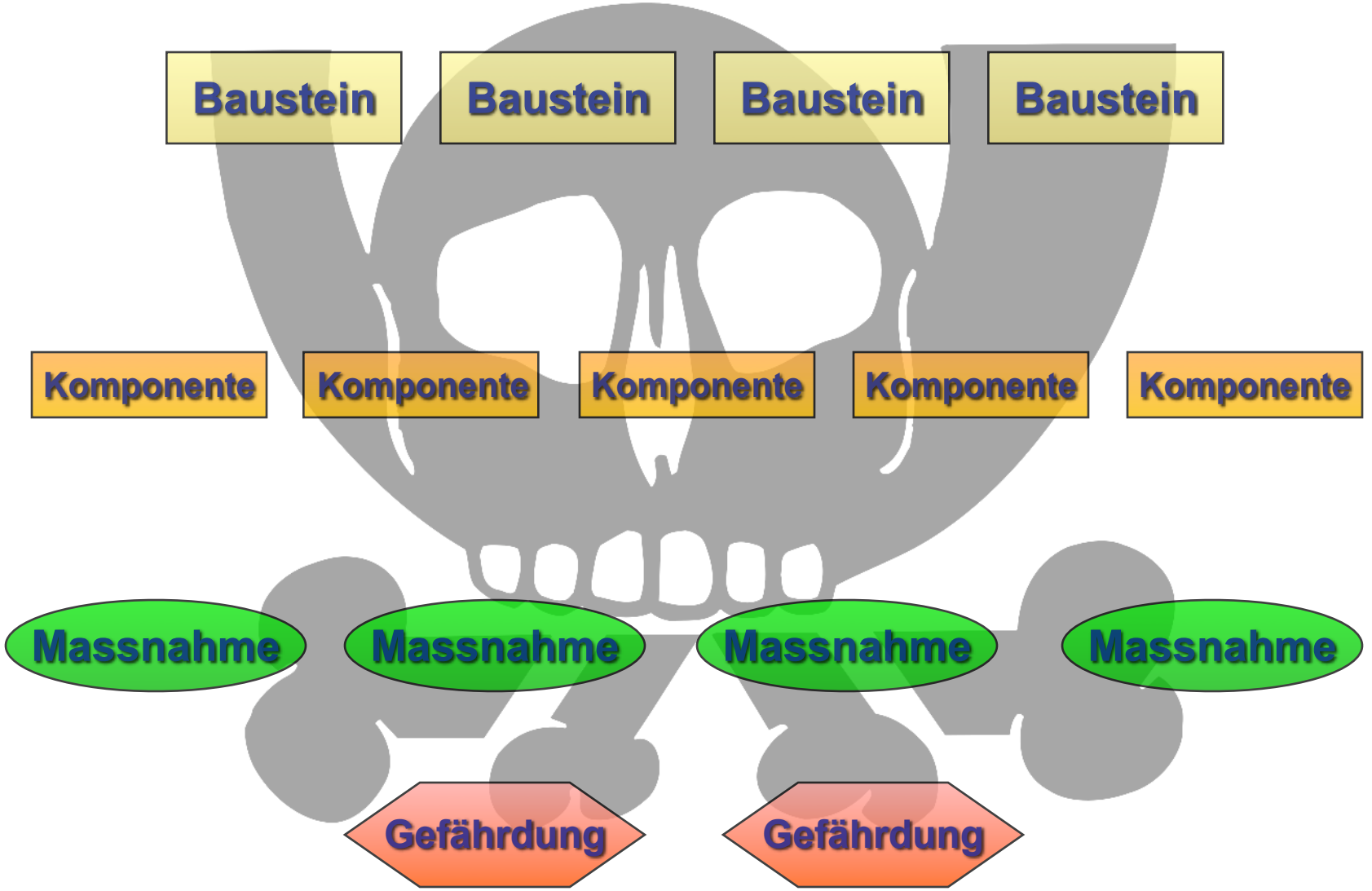
IT-Grundschutz



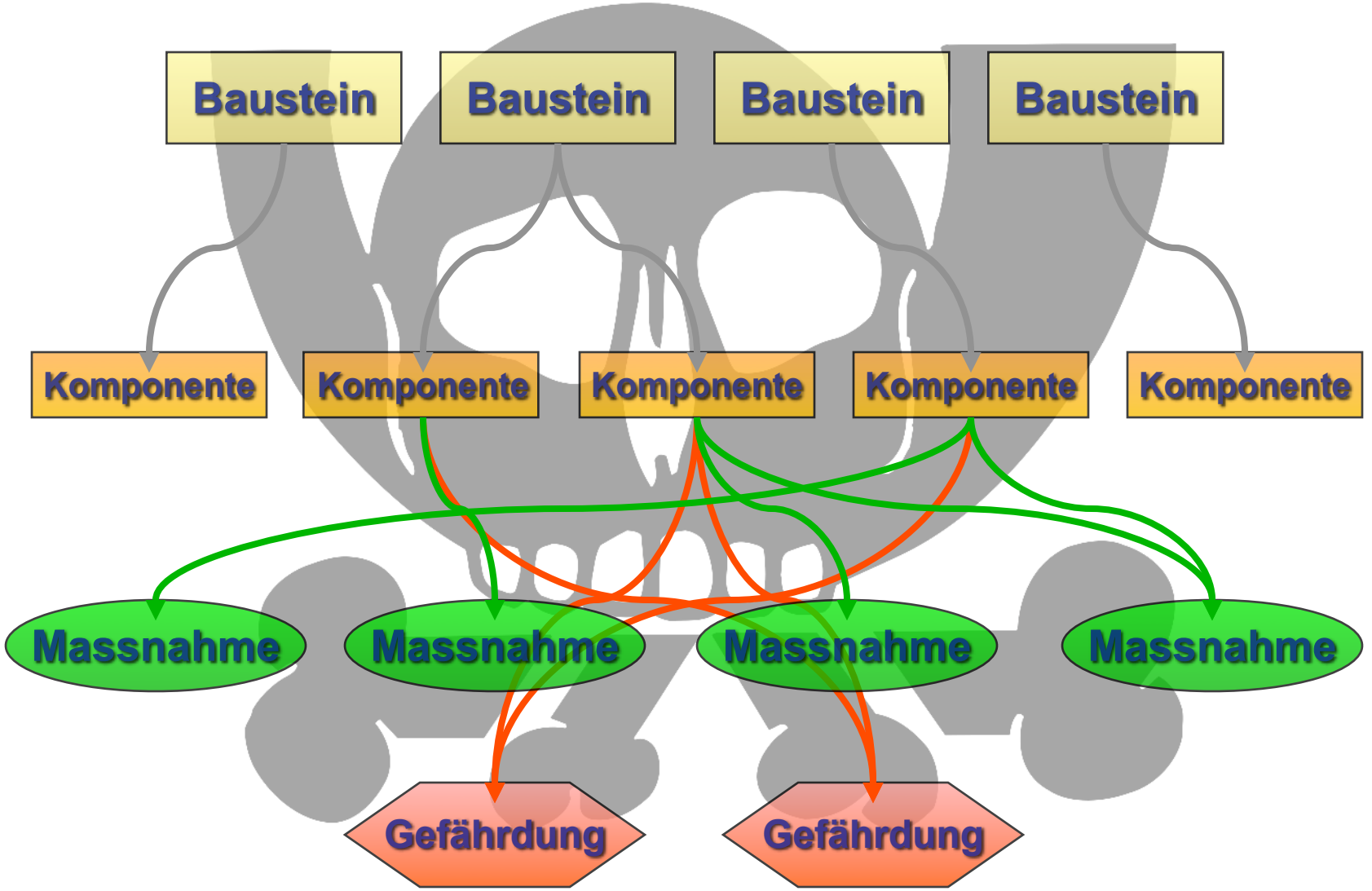
- BSI Standards
  - BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
  - BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
  - BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- IT-Grundschutzkataloge
  - 5 Bausteine
  - > 3000 Seiten

Das Grundschutzhandbuch im Detail

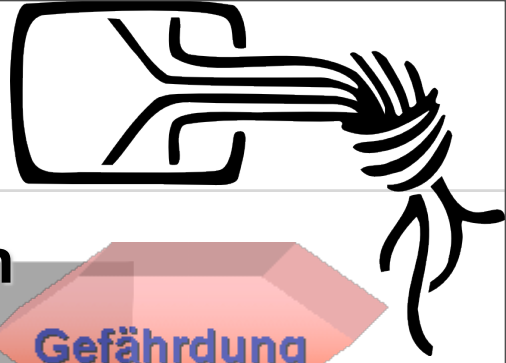




Das Grundschutzhandbuch im Detail



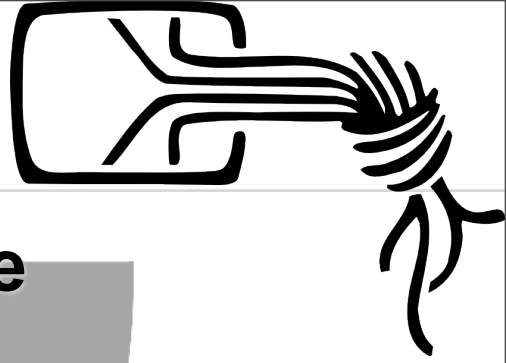
Das Grundschutzhandbuch im Detail



- **Gefährdungskataloge aus den Bereichen**
  - Höhere Gewalt
  - Organisatorische Mängel
  - Menschliche Fehlhandlungen
  - Technisches Versagen
  - Vorsätzliche Handlungen

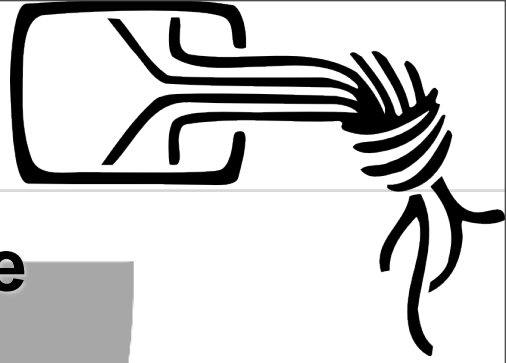
- **Maßnahmenkataloge aus den Bereichen**
  - Infrastruktur
  - Organisation
  - Personal
  - Hardware/Software
  - Notfallvorsorge

Bausteinkataloge



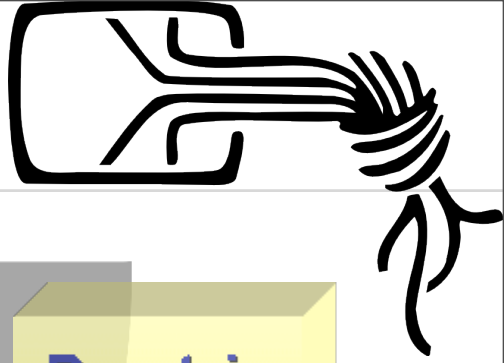
- Die Baussteinkataloge umfaßen die Bausteine
  - Übergreifende Aspekte (Kapitel 1)
  - Infrastruktur (Kapitel 2)
  - IT-Systeme (Kapitel 3)
  - Netze (Kapitel 4)
  - IT-Anwendungen (Kapitel 5)

Bausteinkataloge



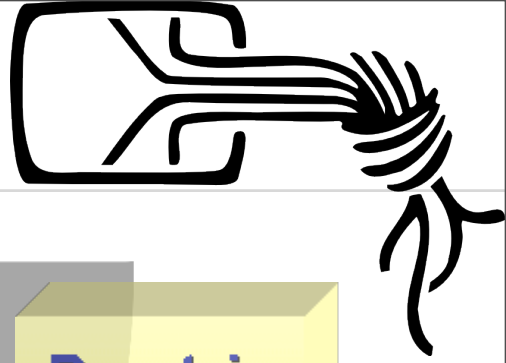
- Die Baussteinkataloge umfaßen die Bausteine
  - Übergreifende Aspekte (Kapitel 1)
  - Infrastruktur (Kapitel 2)
  - IT-Systeme (Kapitel 3)
  - Netze (Kapitel 4)
  - IT-Anwendungen (Kapitel 5)

Das Grundschutzhandbuch im Detail



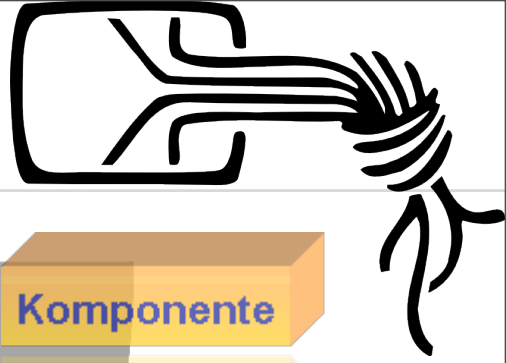
- Beispiel: **IT-Systeme**
  - **B 3.101 Allgemeiner Server**
  - **B 3.102 Server unter Unix**
  - **B 3.103 Server unter Windows NT**
  - **B 3.104 Server unter Novell Netware 3.x**
  - **B 3.105 Server unter Novell Netware Version 4.x**
  - **B 3.106 Server unter Windows 2000**
  - **B 3.107 S/390- und zSeries-Mainframe**
  - **B 3.201 Allgemeiner Client**
  - **B 3.202 Allgemeines nicht vernetztes IT-System**
  - **B 3.203 Laptop**
  - **...**

Das Grundschutzhandbuch im Detail



- Beispiel: **IT-Systeme**
  - **B 3.101 Allgemeiner Server**
  - **B 3.102 Server unter Unix**
  - **B 3.103 Server unter Windows NT**
  - **B 3.104 Server unter Novell Netware 3.x**
  - **B 3.105 Server unter Novell Netware Version 4.x**
  - **B 3.106 Server unter Windows 2000**
  - **B 3.107 S/390- und zSeries-Mainframe**
  - **B 3.201 Allgemeiner Client**
  - **B 3.202 Allgemeines nicht vernetztes IT-System**
  - **B 3.203 Laptop**
  - **...**

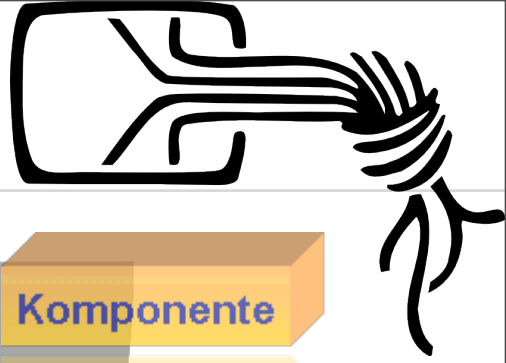
Das Grundschutzhandbuch im Detail



- Beispiel: **Allgemeiner Server**

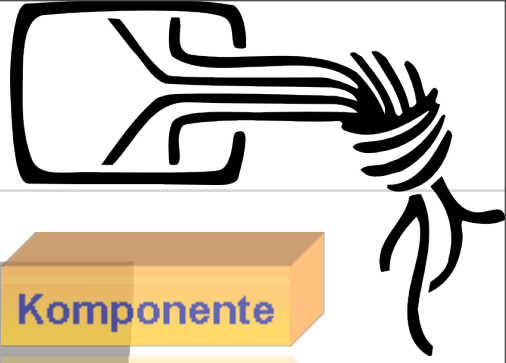
  - 33 Gefährdungen, z.b.
    - G 1.1 **Personalausfall**
    - G 2.7 **Unerlaubte Ausübung von Rechten**
    - G 3.6 **Gefährdung durch Reinigungs- oder Fremdpersonal**
    - G 4.6 **Spannungsschwankungen/...**
    - G 5.2 **Manipulation an Daten oder Software**
  - 31 Maßnahmen, z.b.
    - M 1.28 **Lokale unterbrechungsfreie Stromversorgung**
    - M 2.318 **Sichere Installation eines Servers**
    - M 4.238 **Einsatz eines lokalen Paketfilters**
    - M 6.69 **Notfallvorsorge für einen Server**

Das Grundschutzhandbuch im Detail



- Beispiel: **Allgemeiner Server**
  - 33 Gefährdungen, z.b.
    - G 1.1 **Personalausfall**
    - G 2.7 **Unerlaubte Ausübung von Rechten**
    - G 3.6 **Gefährdung durch Reinigungs- oder Fremdpersonal**
    - G 4.6 **Spannungsschwankungen/...**
    - G 5.2 **Manipulation an Daten oder Software**
  - 31 Maßnahmen, z.b.
    - M 1.28 **Lokale unterbrechungsfreie Stromversorgung**
    - M 2.318 **Sichere Installation eines Servers**
    - M 4.238 **Einsatz eines lokalen Paketfilters**
    - M 6.69 **Notfallvorsorge für einen Server**

Das Grundschutzhandbuch im Detail



- Beispiel: **Allgemeiner Server**
  - 33 Gefährdungen, z.b.
    - G 1.1 **Personalausfall**
    - G 2.7 **Unerlaubte Ausübung von Rechten**
    - G 3.6 **Gefährdung durch Reinigungs- oder Fremdpersonal**
    - G 4.6 **Spannungsschwankungen/...**
    - G 5.2 **Manipulation an Daten oder Software**
  - 31 Maßnahmen, z.b.
    - M 1.28 **Lokale unterbrechungsfreie Stromversorgung**
    - M 2.318 **Sichere Installation eines Servers**
    - M 4.238 **Einsatz eines lokalen Paketfilters**
    - M 6.69 **Notfallvorsorge für einen Server**

Komponente

Höhere Gewalt

Organisatorische Mängel

Menschliche Fehlhandlungen

Technisches Versagen

Vorsätzliche Handlungen

Infrastruktur

Organisation

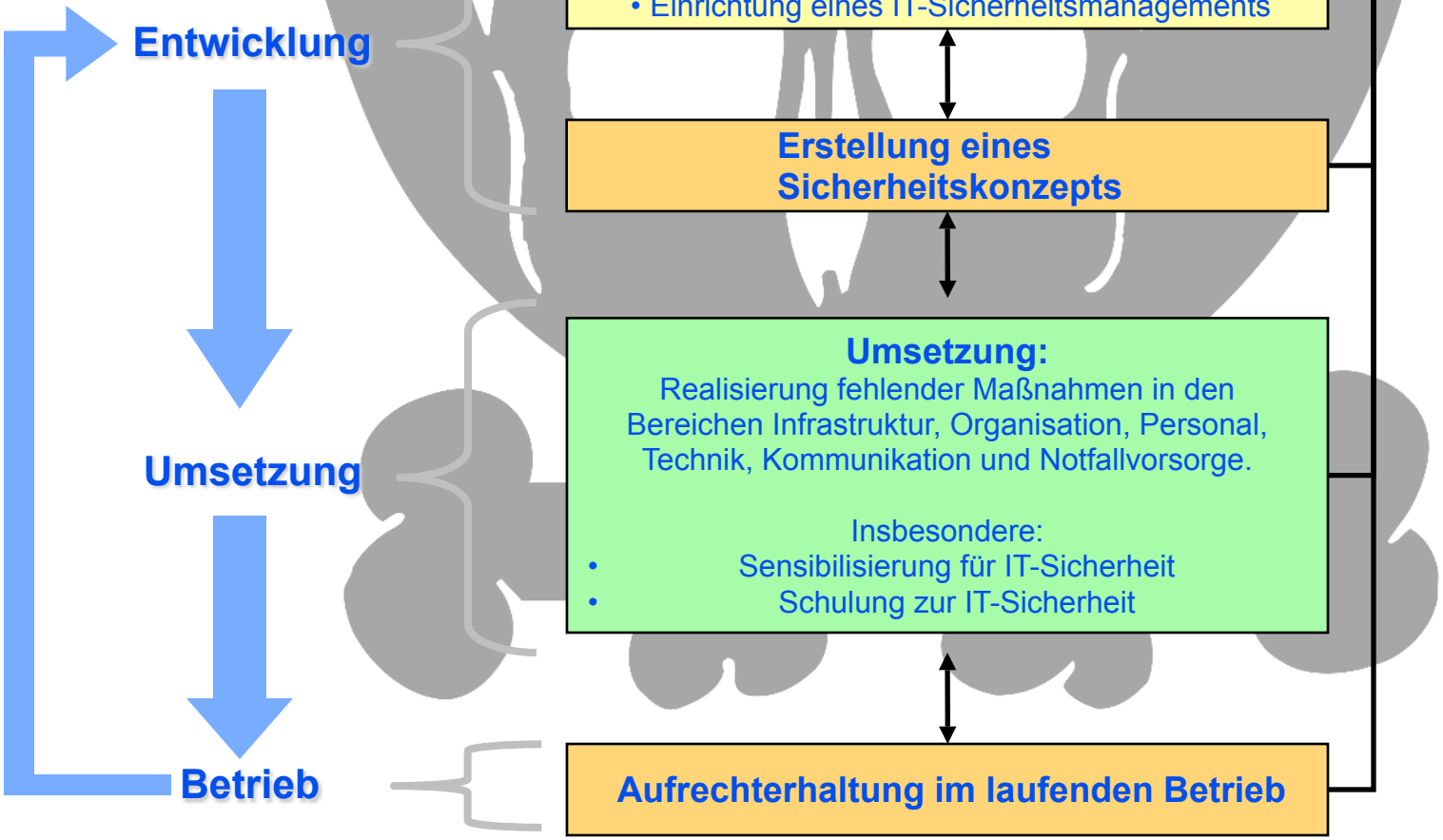
Hardware/-Software

Notfallvorsorge

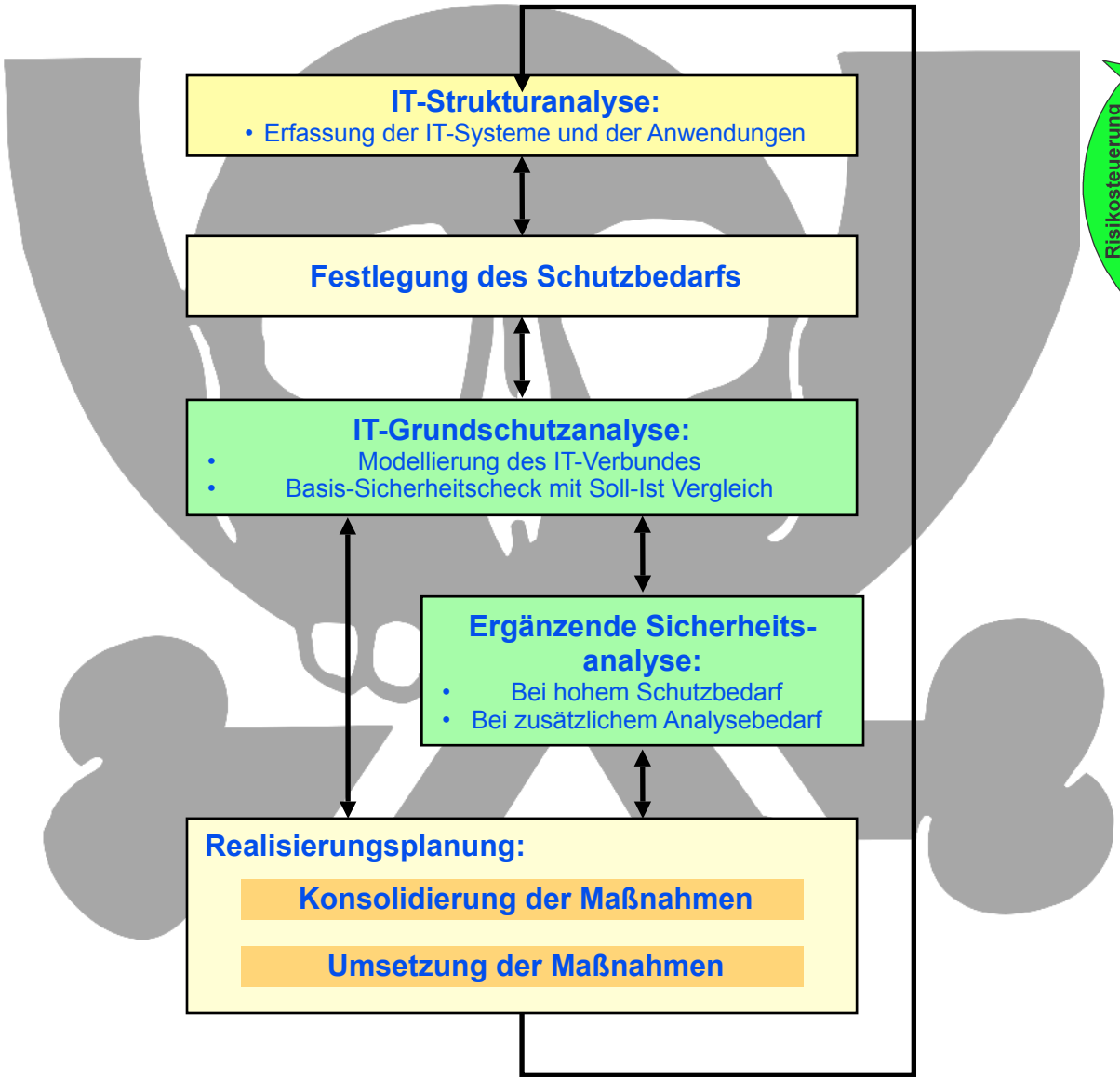
Umsetzung

Umsetzung

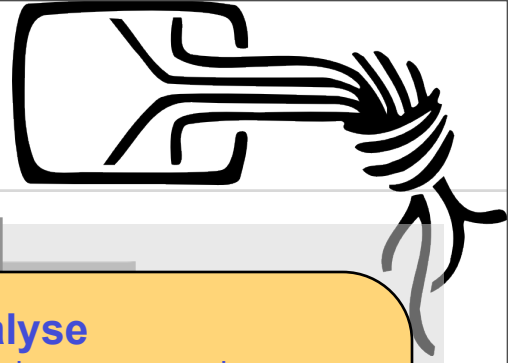
Vorgehensweise nach IT-Grunschutzhandbuch



Vorgehensweise (IT-Grundschutz-Modell)



Vorgehensweise (IT-Grundschutz-Modell)



Initiierung des Sicherheitsprozesses
- Erstellung einer IT-Sicherheitsleitlinie
- Einrichtung eines IT-Sicherheitsmanagements

IT-Strukturanalyse
- Erhebung der Geschäftsprozesse, der zugehörigen Dienstleister / Outsourcing-Partner, IT-Anwendungen und der zugehörigen Informationen sowie der IT-Systeme und Kommunikationsbeziehungen.

Schutzbedarfsanalyse
- Festlegung der Schutzbedarfskategorien (z.B. niedrig, mittel, hoch, sehr hoch)
- Zuordnung zu den Geschäftsprozessen, IT-Systemen, IT-Anwendungen, Daten und Kommunikationsbeziehungen.

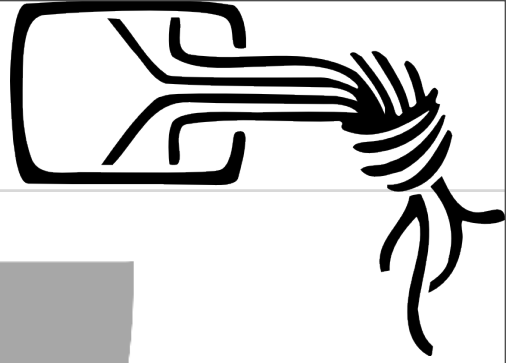
IT-Grundschutzanalyse
- Abbildung zwischen Anforderungen aus dem Grundschutzhandbuch und den hauseigenen Umsetzungen (Modellierung).
- Basis-Sicherheitscheck mit Soll-Ist Vergleich
- Erstellung spezifischer Berichte, z.B.
- ggf ergänzende Sicherheitsanalyse
  - bei hohem Schutzbedarf
  - bei zusätzlichem Analysebedarf

Realisierungsplan
- Konsolidierung der Maßnahmen
- Umsetzungsplan

Maßnahmenumsetzung
- Beseitigung der Defizite
- Umsetzung technischer, organisatorischer und konzeptioneller Maßnahmen

Zertifizierung

IT-Strukturanalyse



Netzplanerhebung

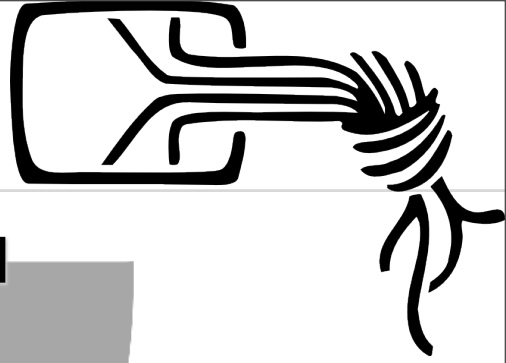
Auswertung eines Netzplans

- **IT-Systeme, z.B. Clients, Server, Netzkomponenten**
- **Netzverbindungen zwischen diesen Systemen**
- **Verbindungen nach außen, z. B. Einwahl oder Internet**

Aktualisierung des Netzplans

- **Netzplan ist meist nicht auf aktuellem Stand**
- **IT-Verantwortliche und Administratoren konsultieren**
- **ggf. Netz- und Systemmanagement heranziehen**

IT-Strukturanalyse

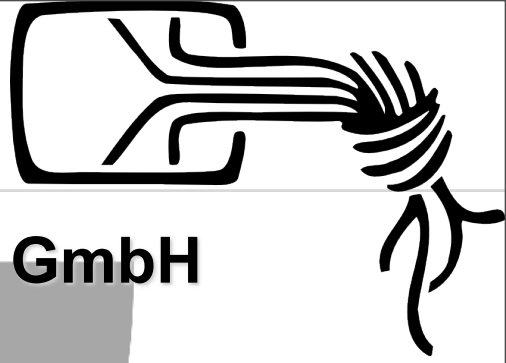


Erhebung der IT-Systeme der Chaos GmbH

Beispiel:

Nr.	Beschreibung	Plattform	Anz.	Ort	Status	Anwender/ Admin.
S1	Server für Personal-verwaltung	Windows NT Server	1	Bonn, R 1.01	in Betrieb	Personal-referat
S2	Primärer Domänen-Controller	Windows NT Server	1	Bonn, R 3.10	in Betrieb	alle IT-Anwender
C6	Gruppe der Laptops für den Standort Berlin	Laptop unter Windows 95	2	Berlin, R 2.01	in Betrieb	alle IT-Anwender in Berlin
N1	Router zum Internet-Zugang	Router	1	Bonn, R 3.09	in Betrieb	alle IT-Anwender
T1	TK-Anlage für Bonn	ISDN-TK-Anlage	1	Bonn, B.02	in Betrieb	alle Mitarb. in Bonn

IT-Strukturanalyse



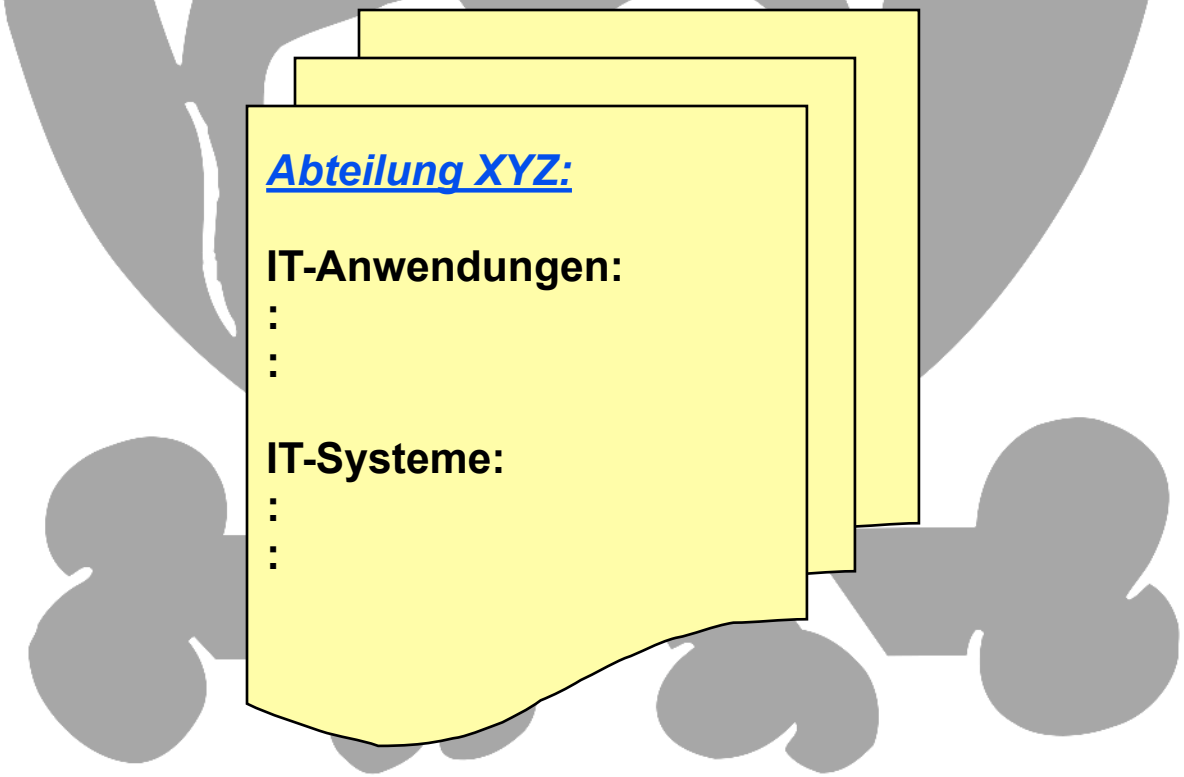
Erfassung der IT-Anwendungen der Chaos GmbH

Beispiel:

Beschreibung der IT-Anwendungen			IT-Systeme						
Anw.-Nr.	**IT-Anwendung/ Informationen**	**Pers.-bez. Daten**	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
A1	Personaldaten-verarbeitung	X	X						
A4	Benutzer-Authentisierung	X		X				X	
A5	Systemmanagement			X					
A7	zentrale Dokumentenverwaltung					X			

Erhebung der IT-Systeme und IT-Anwendungen

Beispiel:



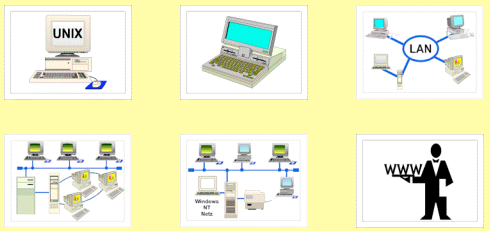
Schutzbedarfsfeststellung

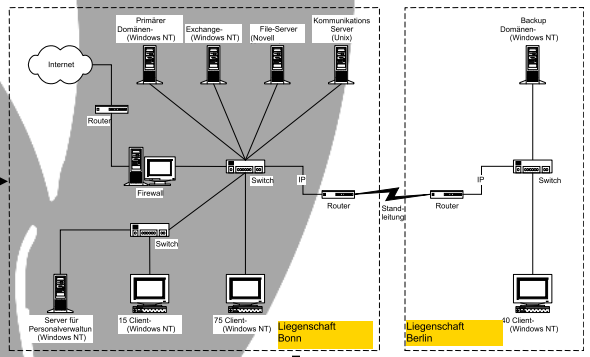
Unterschieden werden drei Schutzbedarfskategorien anhand der maximalen Schäden und Folgeschäden bei Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit:

Niedrig bis mittel	**Begrenzte und überschaubare Schäden**
Hoch	**Beträchtliche Schäden möglich**
Sehr hoch	**Existenziell bedrohliche, katastrophale Schäden möglich**

Soll-Ist Vergleich:

Grundschutzmodell





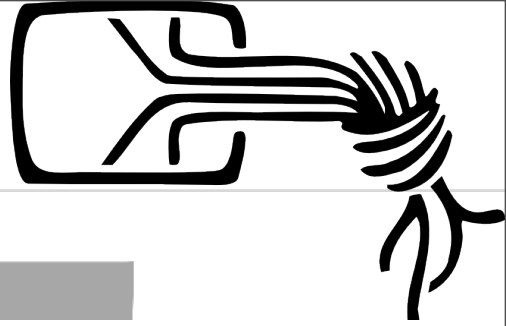
Maßnahmen-empfehlungen

Soll-Ist Vergleich

Realisierte Maßnahmen

IT-Sicherheitskonzept:
defizitäre Maßnahmen

Basis-Sicherheitscheck



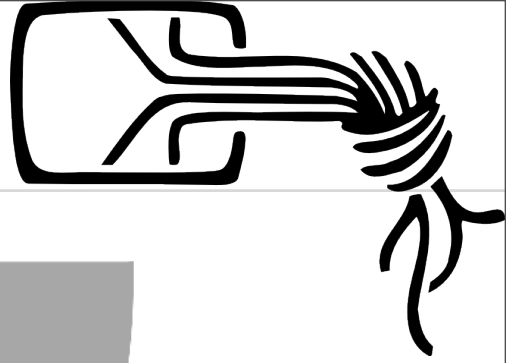
Ergebnisdarstellung:

GSHB-Erhebung: Formular zu Faxgerät

Nummer des IT-Systems: _____ erfasst am: _____ befragte Personen: _____
Bezeichnung: _____ erfasst durch: _____ - " - _____
Standort: _____ - " - _____
- " - _____
- " - _____

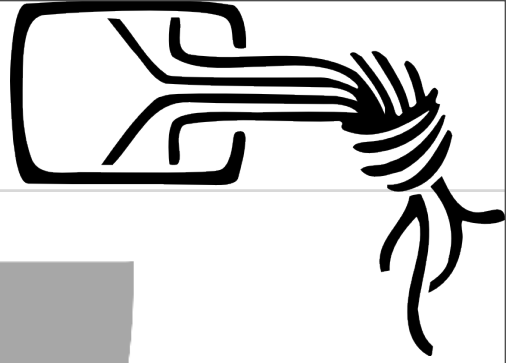
Maßnahme (Priorität)	Faxgerät	entbehrlich	Ja	teilweise	Nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
M 2.30 (2)	Regelung für die Einrichtung von Benutzern / Benutzergruppen								
M 2.64 (1)	Kontrolle der Protokolldateien								
M 2.178 (1)	Erstellung einer Sicherheitsleitlinie für die Faxnutzung								
M 2.179 (1)	Regelungen für den Faxserver-Einsatz								
M 2.180 (1)	Einrichten einer Fax-Poststelle								
M 2.181 (1)	Auswahl eines geeigneten Faxservers								
M 3.4 (1)	Schulung vor Programmnutzung								
M 3.5 (1)	Schulung zu IT-Sicherheitsmaßnahmen								

Ergänzende Sicherheitsanalyse



... ist durchzuführen, wenn

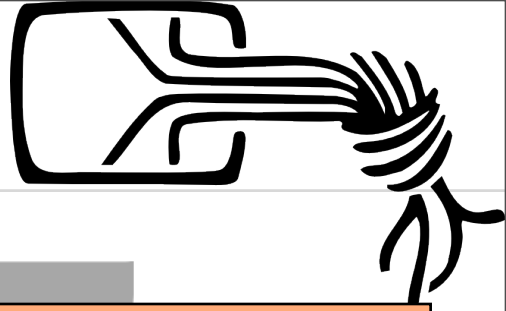
- Schutzbedarfskategorie "hoch" oder "sehr hoch„ in mindestens einem der drei Grundwerte vorliegt,
- zusätzlicher Analysebedarf besteht (z. B. bei besonderem Einsatzumfeld) oder
- für bestimmte Komponenten oder Aspekte keine Standardmaßnahmen vorhanden sind.

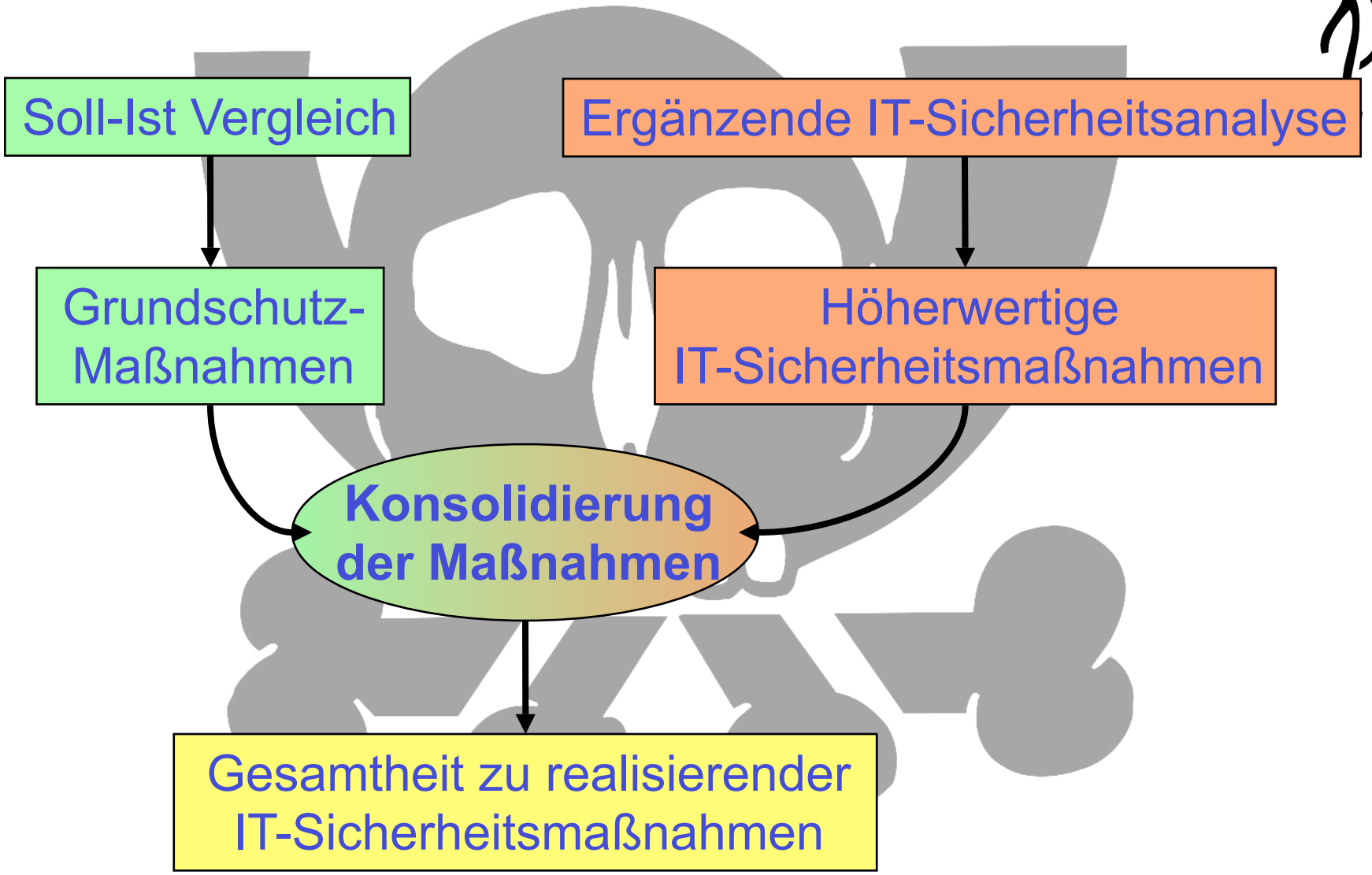


Mögliche Vorgehensweisen sind:

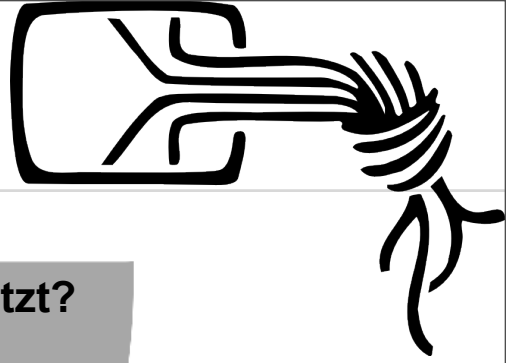
- **Risikoanalyse**
  - Gemäß „*BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*“
  - relevante Bedrohungen ermitteln
  - Eintrittswahrscheinlichkeiten schätzen
- **Penetrationstest**
  - Verhalten eines Angreifers simulieren
  - Blackbox- und Whitebox-Ansatz unterscheiden
- **Differenz-Sicherheitsanalyse**
  - höherwertige Maßnahmen identifizieren
  - Schutzklassenmodelle

Konsolidierung der Maßnahmen





Realisierung von IT-Sicherheitsmaßnahmen



Schritt 1: Sichtung der Untersuchungsergebnisse

Welche Maßnahmen sind nicht oder nur teilweise umgesetzt?

Schritt 2: Konsolidierung der Maßnahmen

Welche Maßnahmen werden durch höher- oder gleichwertige ersetzt?

Schritt 3: Kosten- und Aufwandsschätzung

Welche einmaligen/wiederkehrenden Kosten entstehen?

Schritt 4: Festlegung der Umsetzungsreihenfolge

Welche fehlenden Maßnahmen sollten zuerst umgesetzt werden?

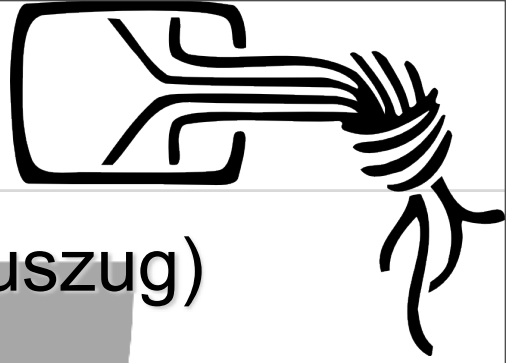
Schritt 5: Festlegung der Verantwortlichkeit

Wer setzt welche Maßnahme bis wann um?
Stehen die erforderlichen Ressourcen zur Verfügung?

Schritt 6: Realisierungsbegleitende Maßnahmen

Werden die Mitarbeiter geschult und sensibilisiert, so dass die IT-Sicherheitsmaßnahmen akzeptiert werden?

Realisierungsplan



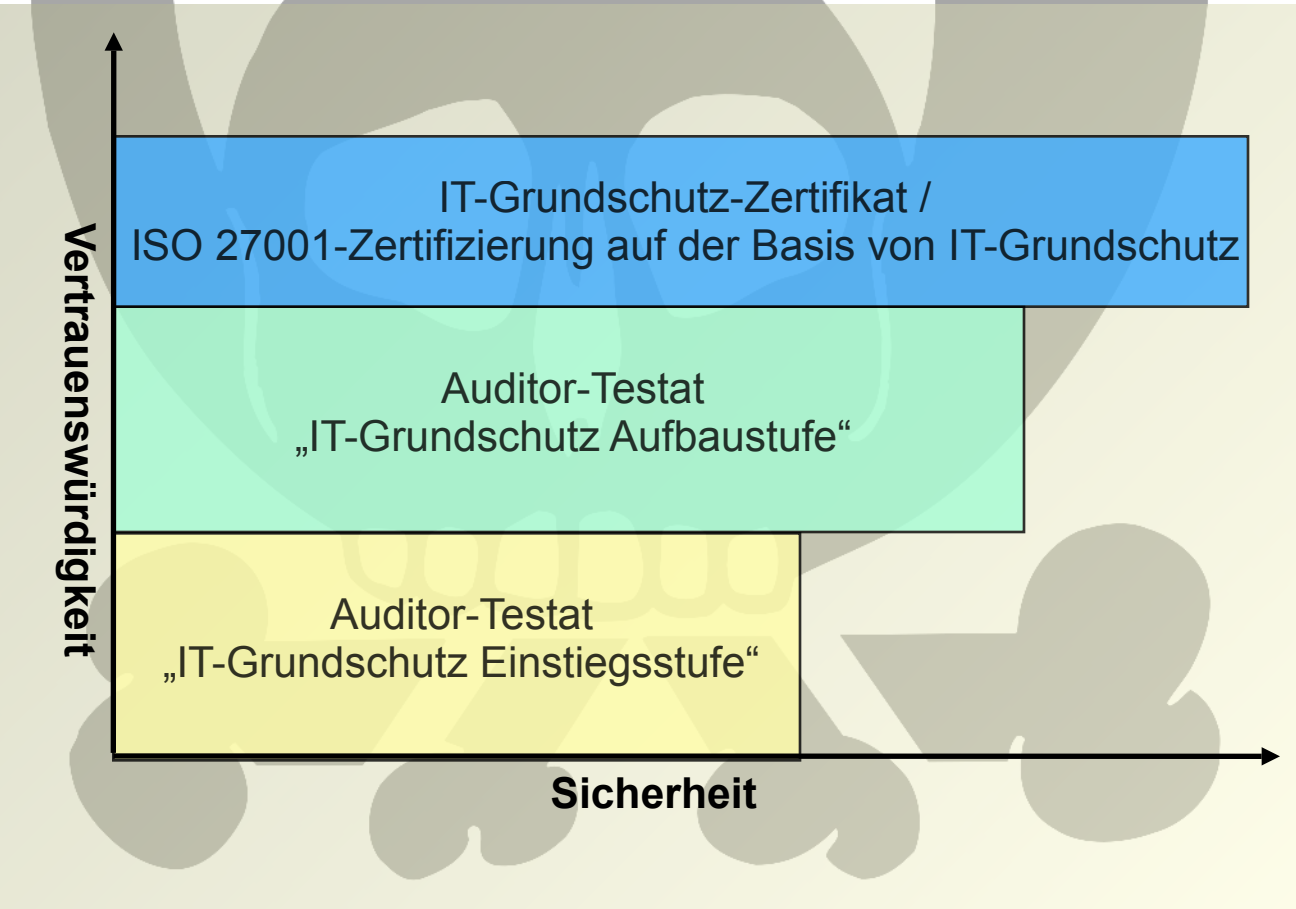
Beispiel für einen Realisierungsplan (Auszug)

Zielobjekt	Maßnahme	Umsetzung bis	Verantwortlich	Budgetrahmen	Bemerkung
Gesamte Institution	M 2.11 Regelung des Passwortgebrauchs	31.12.03	Umsetzung: Herr Müller Kontrolle: Frau Meier	einmalig 2 AT	
Gruppe Clients C1	Z 2 chipkartengestützte Authentisierung und lokale Verschlüsselung der Festplatten	31.12.03	Umsetzung: Herr Schulz Kontrolle: Frau Meier	einmalig 1400,- Euro + 2 AT wiederkehrend 2 AT/Jahr	
usw.					

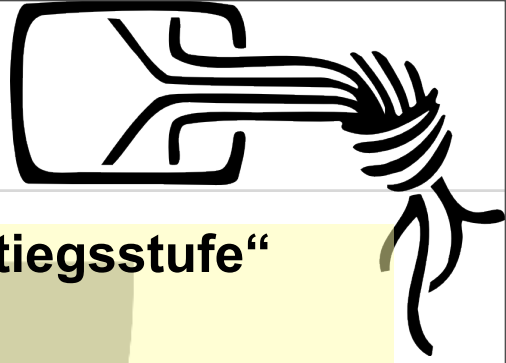
IT-Grundschutz-Zertifikat

Ausbaustufen

- **Die drei Stufen der Zertifizierung**



Ausbaustufen



- Stufe 1: **Auditor-Testat „IT-Grundschutz Einstiegsstufe“**

  Gültigkeit: **2 Jahre**

  Verlängerbar: **Nicht für denselben IT-Verbund**

- Stufe 2: **Auditor-Testat „IT-Grundschutz Aufbaustufe“**

  Gültigkeit: **2 Jahre**

  Verlängerbar: **Nicht für denselben IT-Verbund**

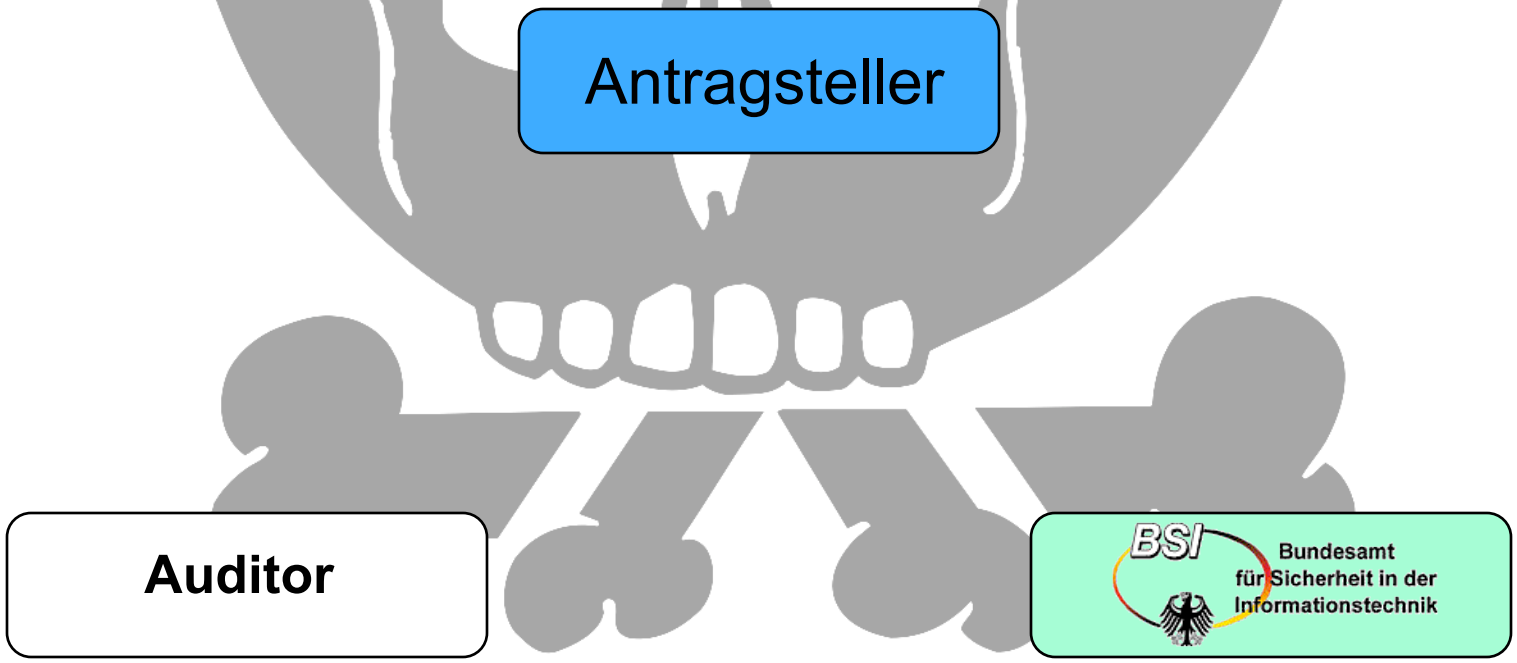
- Stufe 3: **IT-Grundschutz-Zertifikat / ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz**

  Gültigkeit: **2 Jahre**

  Verlängerbar: **Ja**

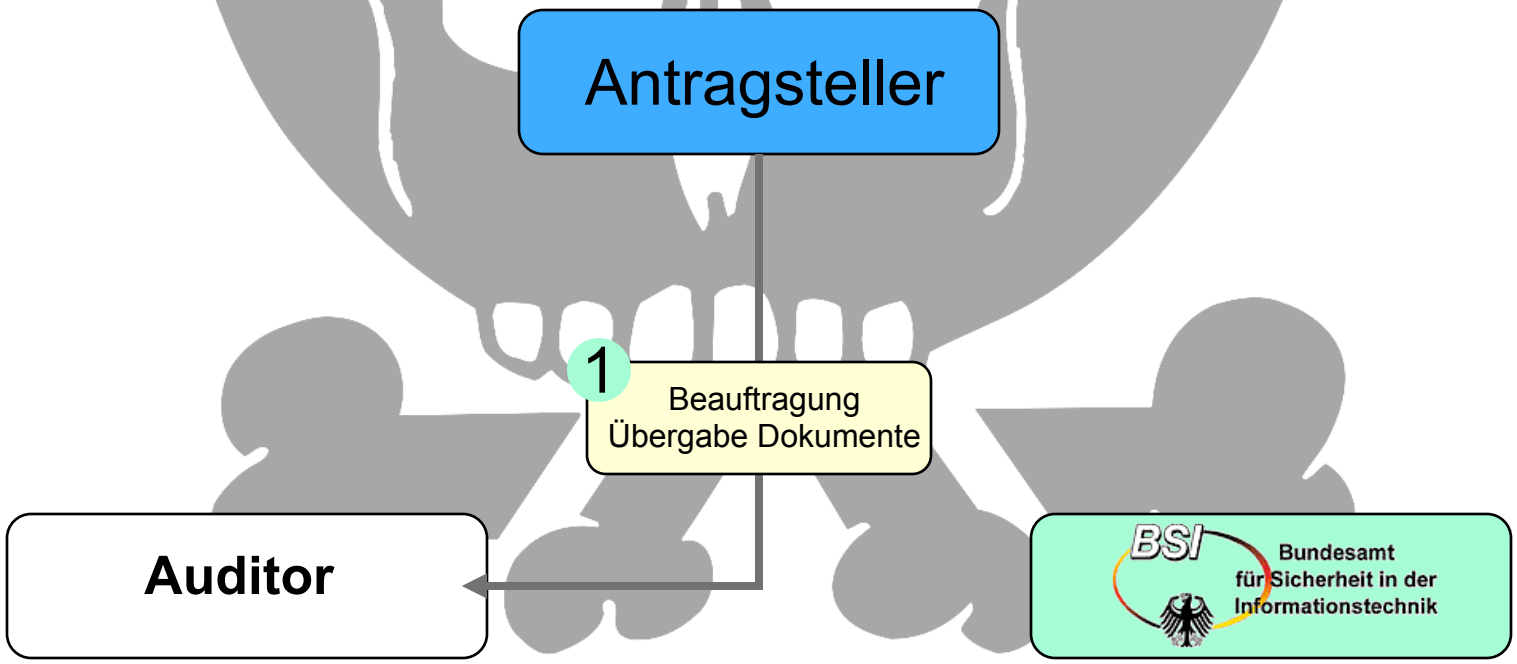
Ausbaustufen

- **Auditierung nach dem Zertifizierungsschema**



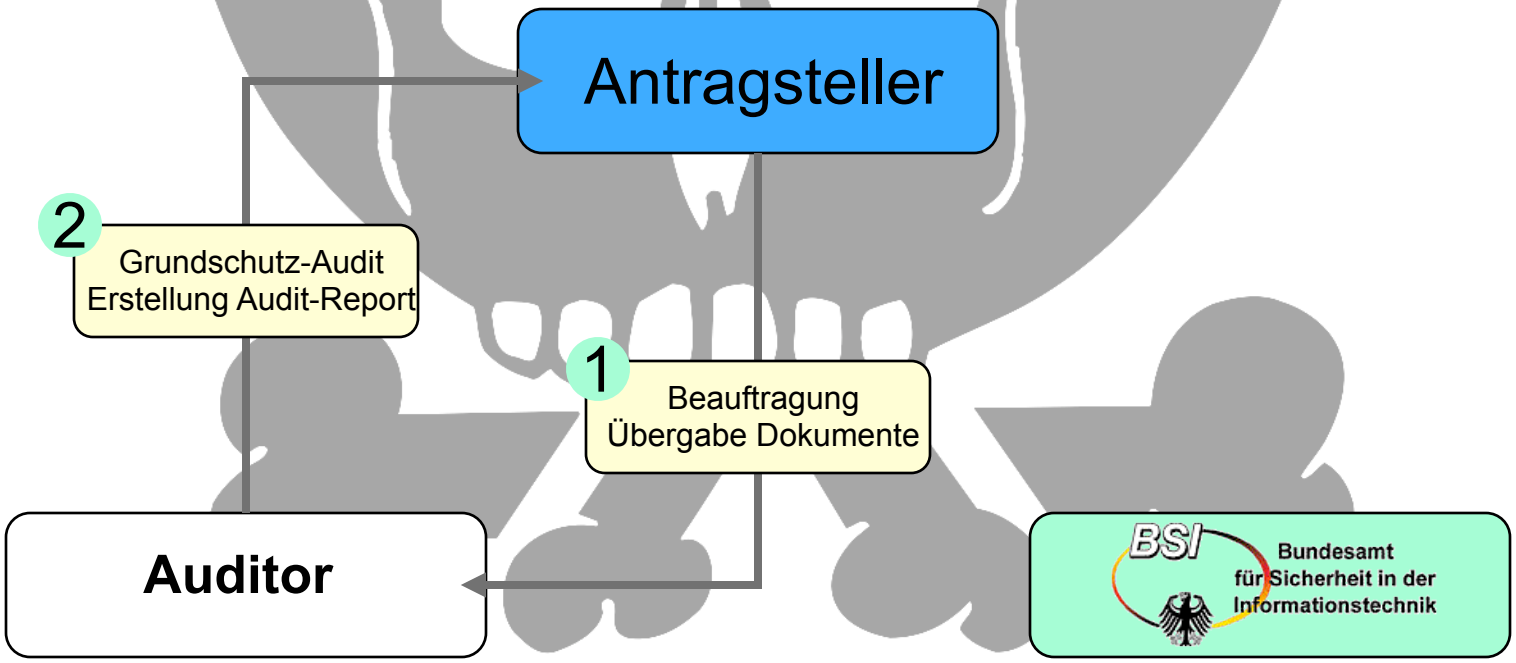
Ausbaustufen

- **Auditierung nach dem Zertifizierungsschema**



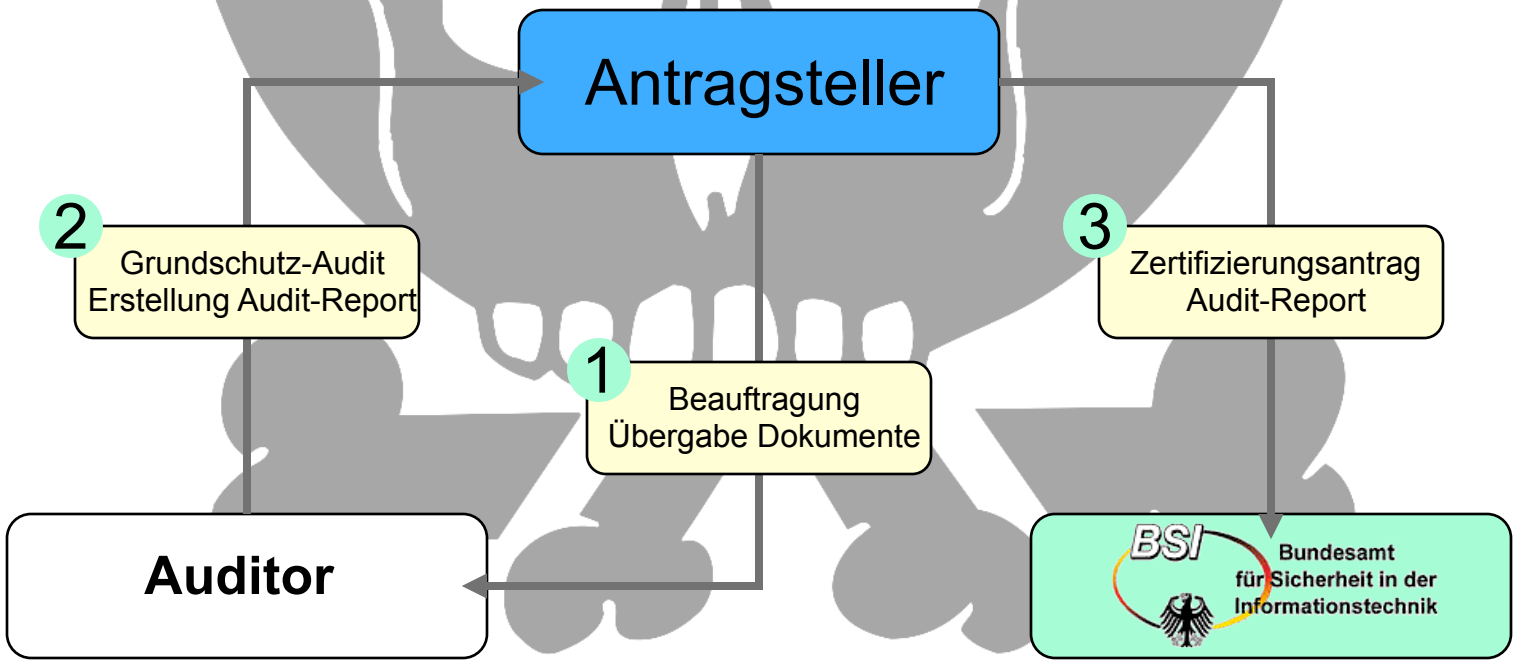
Ausbaustufen

- **Auditierung nach dem Zertifizierungsschema**



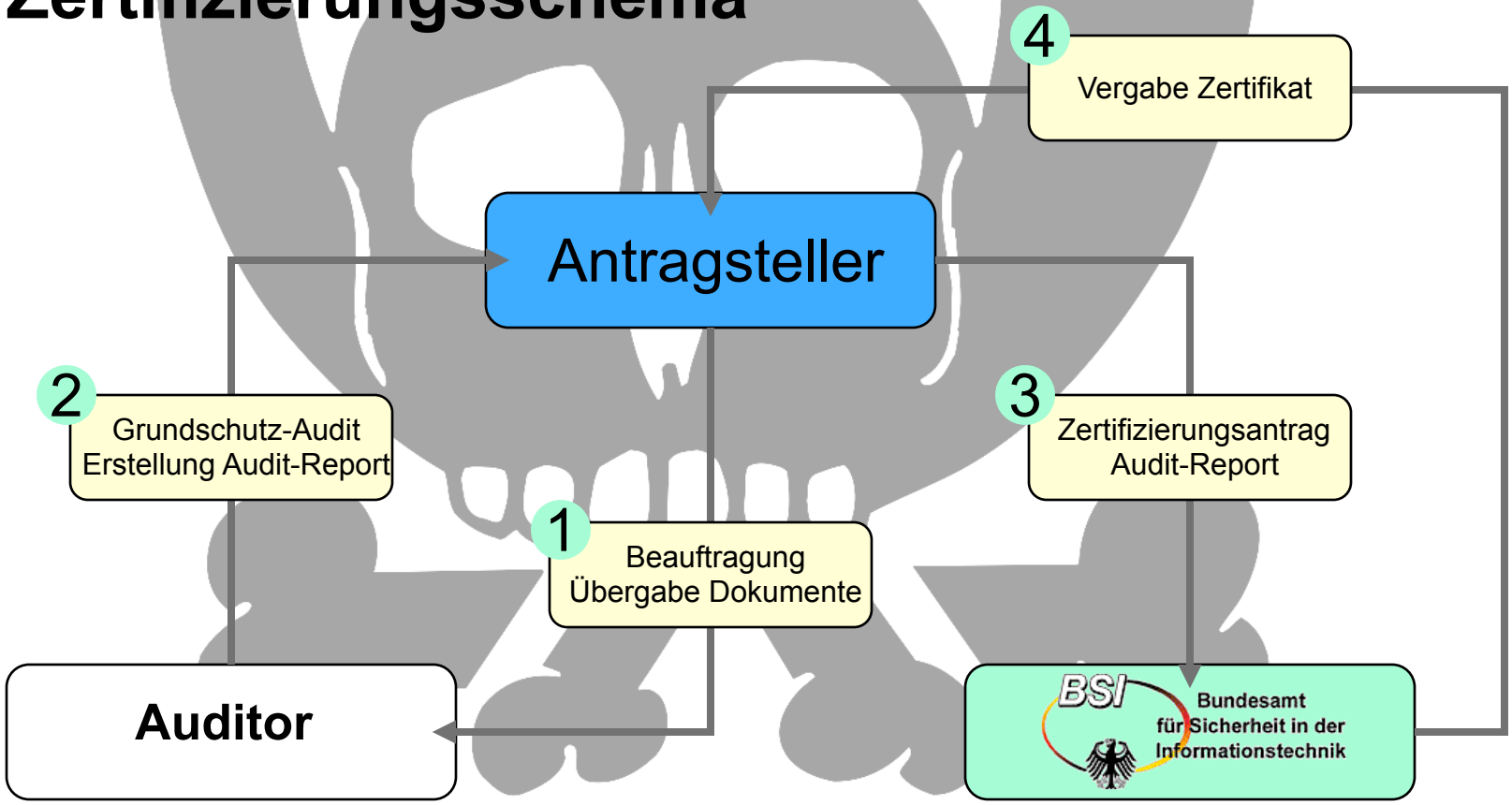
Ausbaustufen

- **Auditierung nach dem Zertifizierungsschema**



Ausbaustufen

- **Auditierung nach dem Zertifizierungsschema**



Rechtsverhältnisse

- **BSI Zertifizierungsschema**

(Auditor)

Rechtsverhältnisse

- **BSI Zertifizierungsschema**

(Antragsteller)

(Auditor)

Rechtsverhältnisse

- **BSI Zertifizierungsschema**

(Antragsteller)

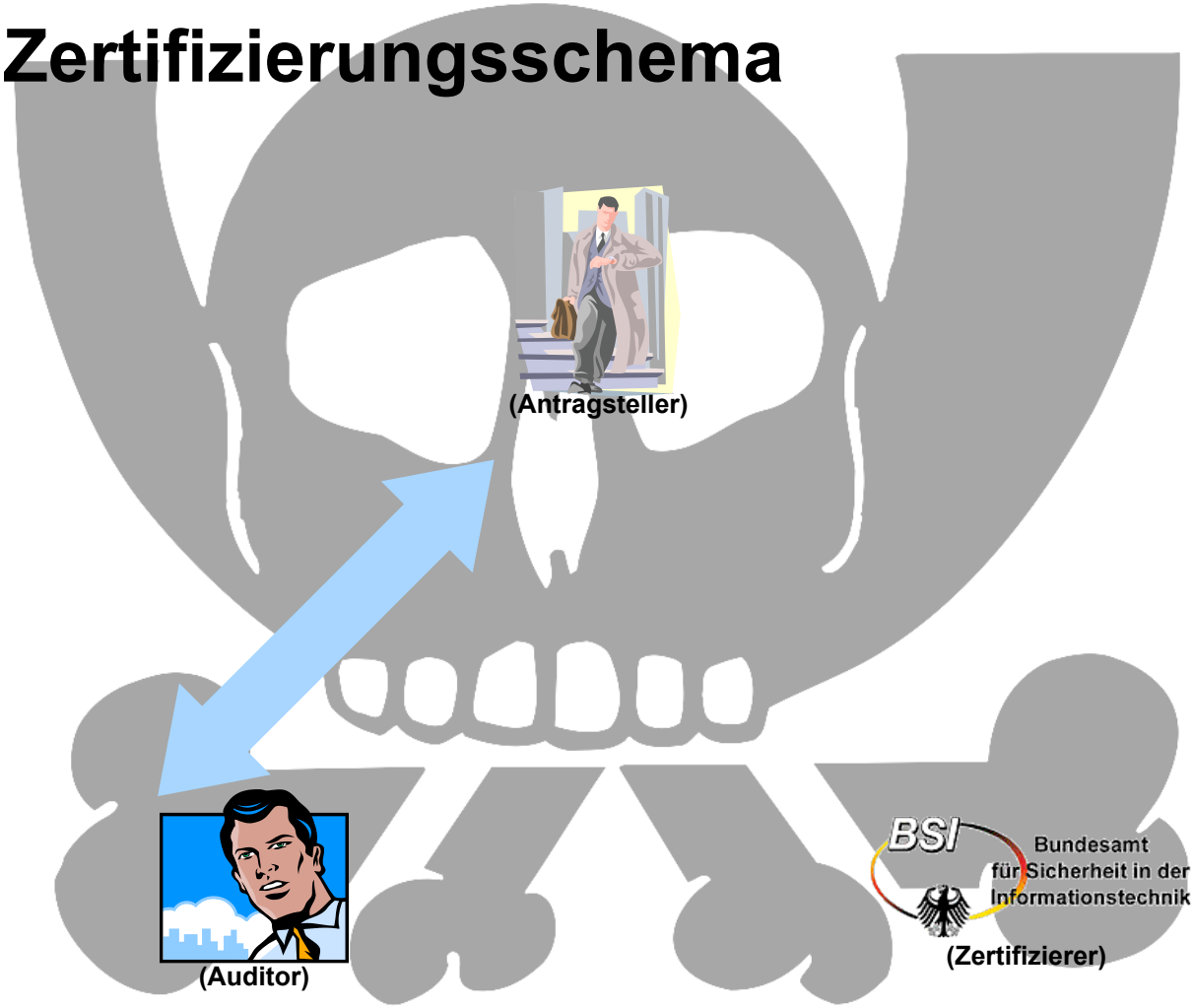
(Auditor)

BSI Bundesamt für Sicherheit in der Informationstechnik

(Zertifizierer)

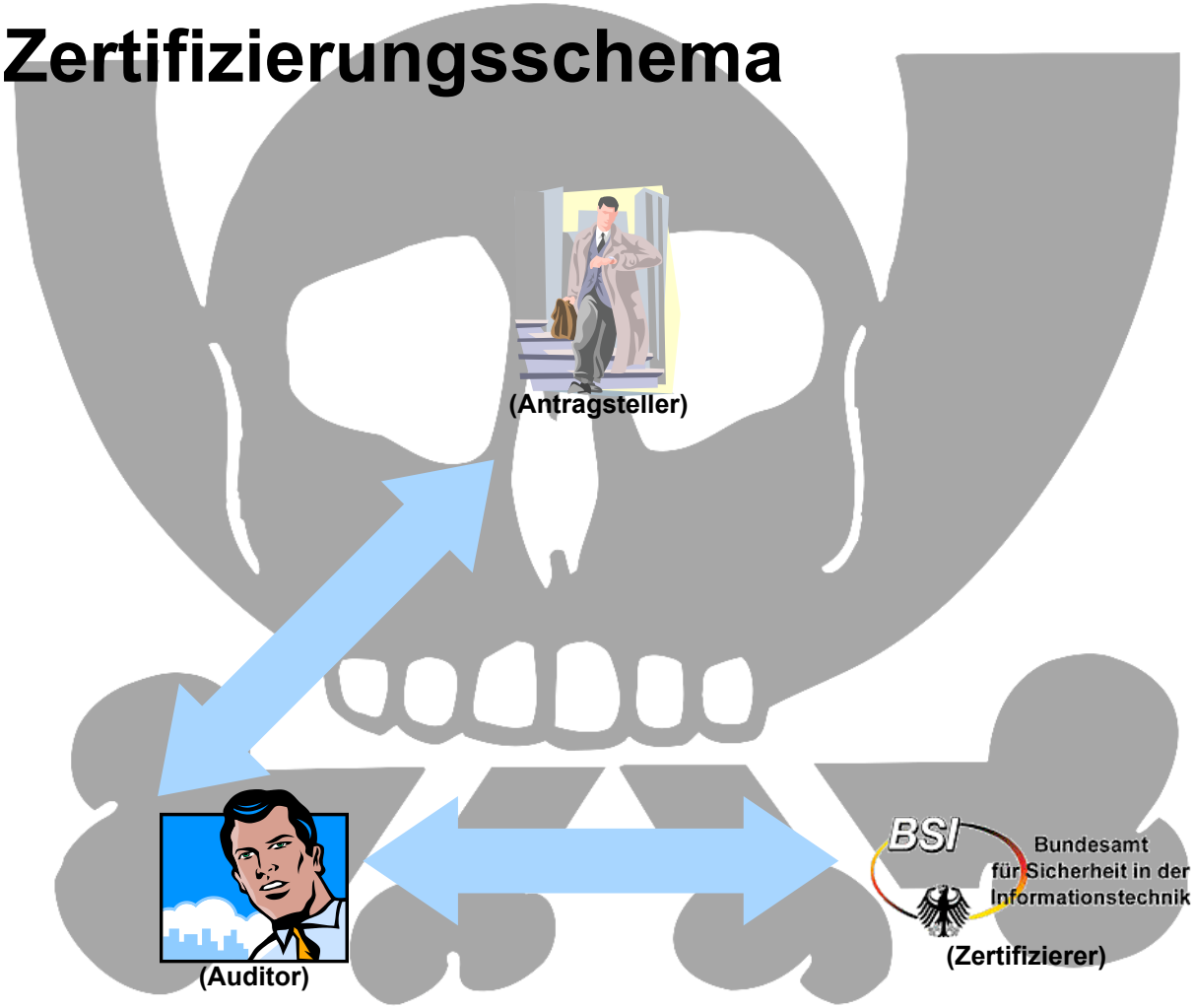
Rechtsverhältnisse

- **BSI Zertifizierungsschema**



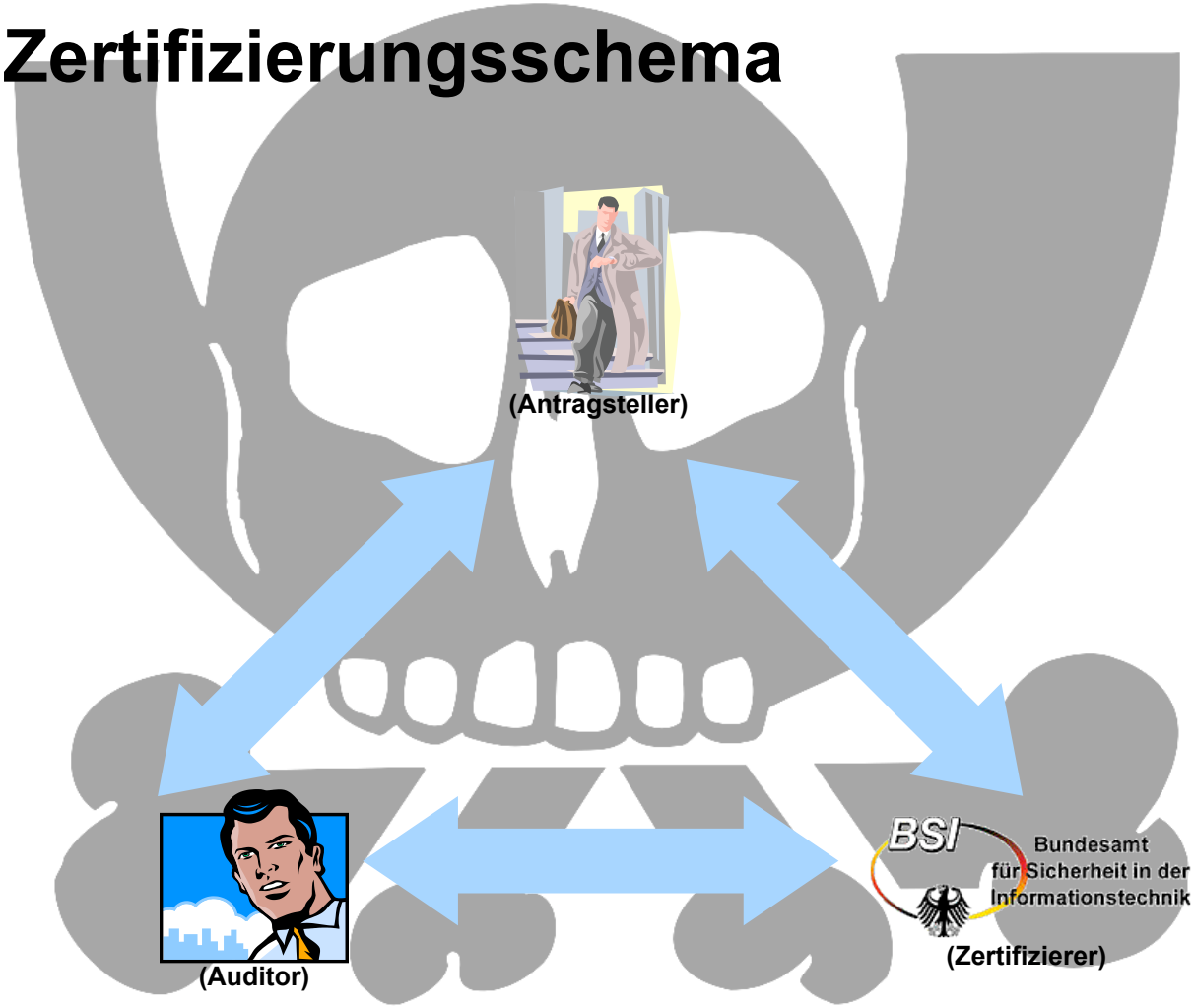
Rechtsverhältnisse

- **BSI Zertifizierungsschema**

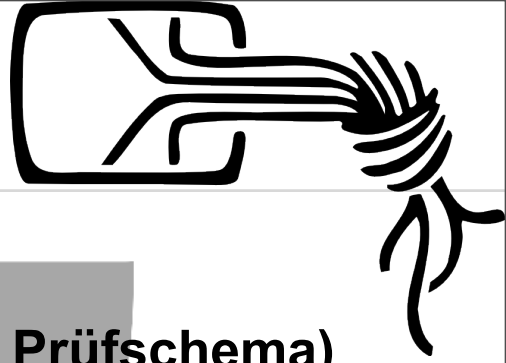


Rechtsverhältnisse

- **BSI Zertifizierungsschema**

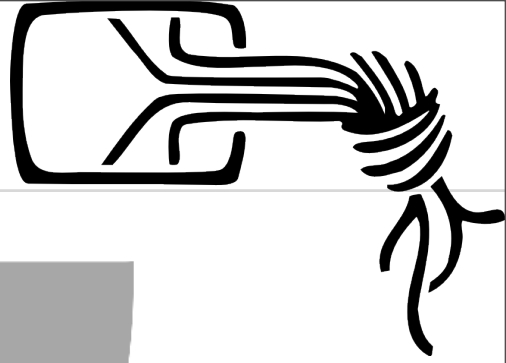


Vorgehensweise: Zertifizierung



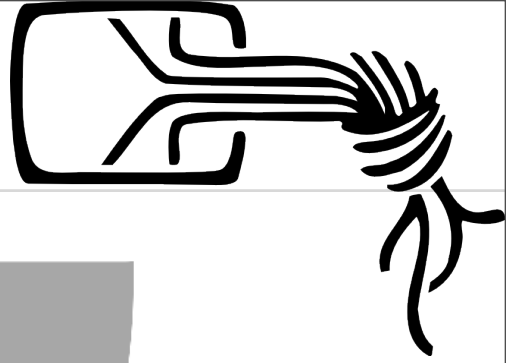
- **Aufgaben des Antragstellers:**
- **Erstellung erforderlicher Dokumente (vgl. Kap. 1 Prüfschema)**
  - **IT-Strukturanalyse**
    - **Definition Geltungsbereich**
    - **Bereinigter Netzplan**
    - **Liste der IT-Systeme**
    - **Liste der IT-Anwendungen**
  - **Schutzbedarfsfeststellung**
    - **Definition Schutzbedarfskategorien**
    - **Schutzbedarf IT-Anwendungen, IT-Systeme, Kommunikationsverbindungen und Räume**
  - **Modellierung IT-Verbund**
  - **Ergebnisse des Basis-Sicherheitschecks**

Vorgehensweise: Zertifizierung



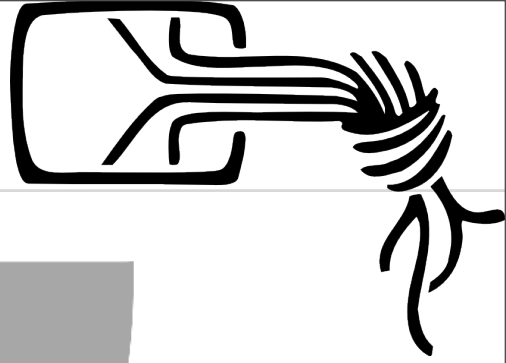
- Aufgaben des Auditors:
- Plausibilitätsprüfung
  - Sinnvolle Mindestgröße des IT-Verbunds
  - Plausibilität der Strukturanalyse
  - Korrektheit der Modellierung
  - Plausibilität des Basis-Sicherheitschecks
- Realisierungsprüfung
  - Stichprobenartige Ermittlung des im Basis-Sicherheitscheck dokumentierten Umsetzungsstatus
    - Baustein „IT-Sicherheitsmanagement“
    - jeweils einem Baustein der fünf Schichten
    - und vier weitere Bausteinen
- Erstellung des Audit-Reports (gem. Kapitel 7 Prüfschema)

Weitere Informationen zum Thema



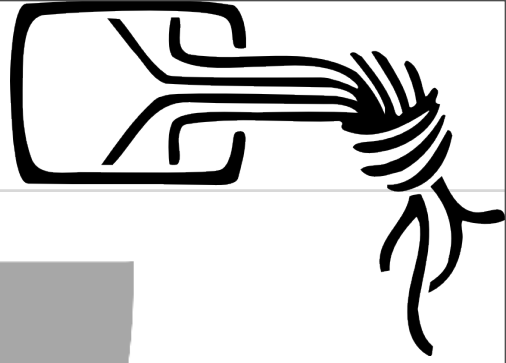
- IT-Grundschutz-Handbuch
  - http://www.bsi.bund.de/gshb
- Prüfschema für Auditoren
  - http://www.bsi.de/gshb/zert/schema.htm
- IT-Grundschutz-FAQ
  - http://www.bsi.de/gshb/zert/faq_zert.htm
- BSI Tool IT-Grundschutz (GSTOOL)
  - http://www.bsi.bund.de/gstool/

Weitere Informationen zum Thema



- IT-Grundschutz umsetzen mit GSTOOL
  - Frederik Humpert, ISBN 3-446-22984-1
- ISO 27001 sowie ISO 17799 und IT-Grundschutz
  - www.bsi.de/gshb/deutsch/hilfmi/Vergleich_ISO17799_GS.pdf
- Diplomarbeit zum Thema IT-Grundschutz und PCI DSS
  - www.daniel-jedecke.de/Privat/Diplom.html

Kontakt



- Manuel Atug (HonkHase)
- Mail: Manuel@atug.de
- Jabber: honkhase@jabber.ccc.de

- Daniel Jedecke (Jedi)
- Mail: diplom@daniel-jedecke.de
- Jabber: Jedi@jabber.daniel-jedecke.de