
ISO 27001 Zertifizierung auf Basis von IT-Grundschutz

Dr. Lydia Tsintsifa

Bundesamt für Sicherheit in der Informationstechnik
IT-Sicherheitsmanagement, IT-Grundschutz

BITKOM KB Sicherheit

Berlin, 26.01.2006

Agenda

- ❑ Die neuen BSI-Standards
- ❑ BSI-Standard 100-2: Vorgehensweise nach IT-Grundschutz
- ❑ Die neue IT-Grundschutz Zertifizierung
- ❑ Materialien und Hilfsmittel

IT-Grundschutz

Aktuelle Entwicklungen

- ❑ IT-Grundschutz in eine Linie mit ISO 27001 bringen
 - ❑ Ergänzung und Anpassung von Maßnahmen
 - ❑ Anpassung der IT-Grundschutz Zertifizierung

- ❑ Trennung von Methode und konkreten Anforderungen
 - ❑ BSI-Standards und IT-Grundschutz-Kataloge

- ❑ Neues Schema für Prüfung und Lizenzierung

BSI-Standards zur IT-Sicherheit

- Bereich IT-Sicherheitsmanagement -

BSI Standard 100-1:

ISMS: Managementsysteme für
Informationssicherheit

BSI Standard 100-2:

IT-Grundschutz-Vorgehensweise

BSI Standard 100-3:

Risikoanalyse auf der Basis von IT-
Grundschutz

Zertifizierung nach ISO 27001 auf der
Basis von IT-Grundschutz

IT-Grundschutz-Kataloge

Kapitel 1: Einleitung

Kapitel 2: Schichtenmodell und Modellierung

Kapitel 3: Glossar

Kapitel 4: Rollen

- **Bausteinkataloge**

- Kapitel B1 „Übergreifende Aspekte“,
-B 1.0 IT-Sicherheitsmanagement

-...

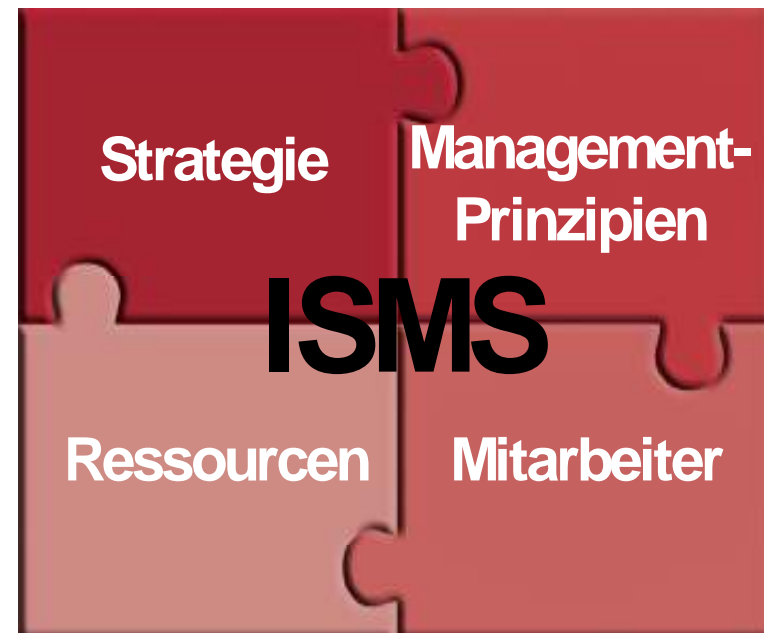
- Kapitel B2 „Infrastruktur“
- Kapitel B3 „IT-Systeme“
- Kapitel B4 „Netze“
- Kapitel B5 „IT-Anwendungen“

- **Gefährdungskataloge**

- **Maßnahmenkataloge**

Managementsysteme für Informationssicherheit

- Zielgruppe: Management
- Kompatibel mit ISO/IEC 27001
- Interpretation der Norm
- allgemeine Anforderungen an ein ISMS

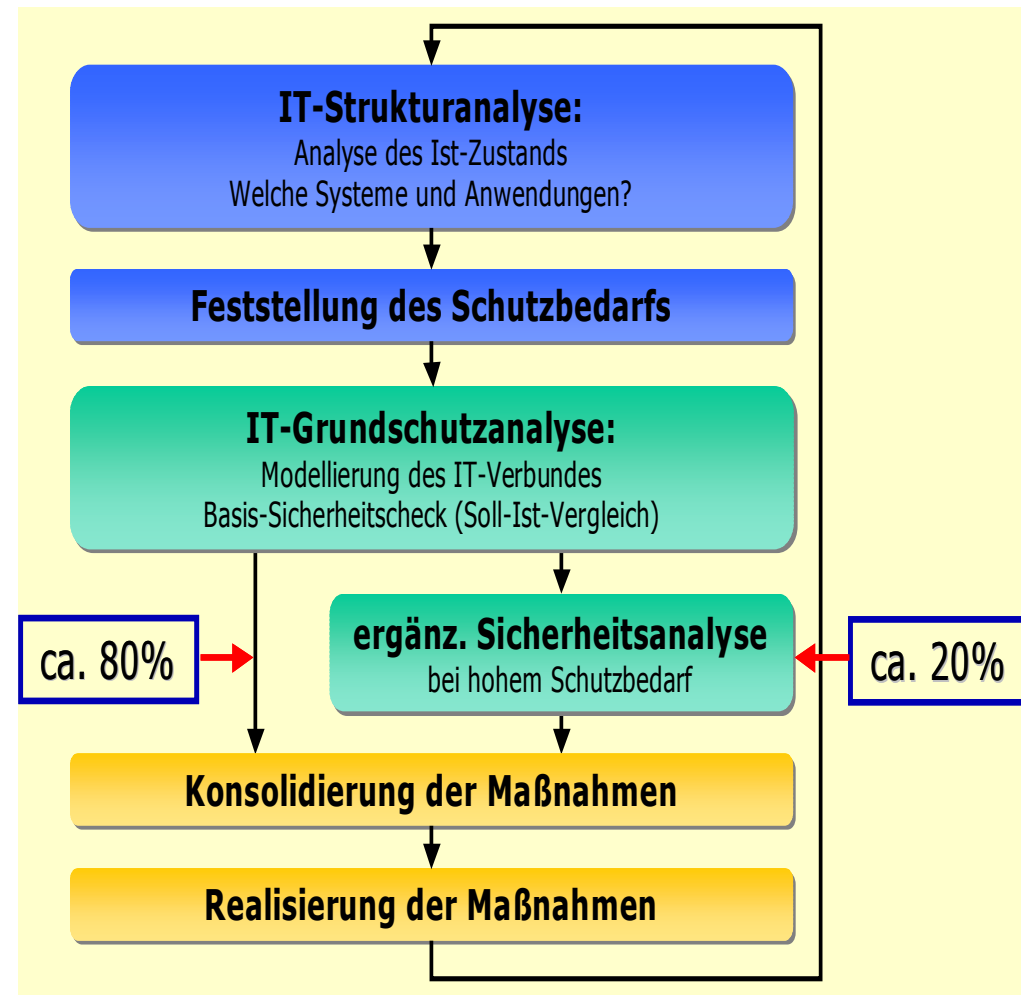


- ❑ Überblick über Standards
- ❑ ISMS-Definition und Prozessbeschreibung
- ❑ Management-Prinzipien
 - ❑ Aufgaben, Aufrechterhaltung, Kommunikation
- ❑ Ressourcen für IT-Betrieb und IT-Sicherheit
- ❑ Einbindung der Mitarbeiter in den IT-Sicherheitsprozess
- ❑ Der IT-Sicherheitsprozess
 - ❑ Planung, IT-Sicherheitsleitlinie, Erfolgskontrolle
- ❑ IT-Sicherheitskonzept
 - ❑ Erstellung, Umsetzung, Erfolgskontrolle und Verbesserung
- ❑ Das ISMS des BSI: IT-Grundschutz

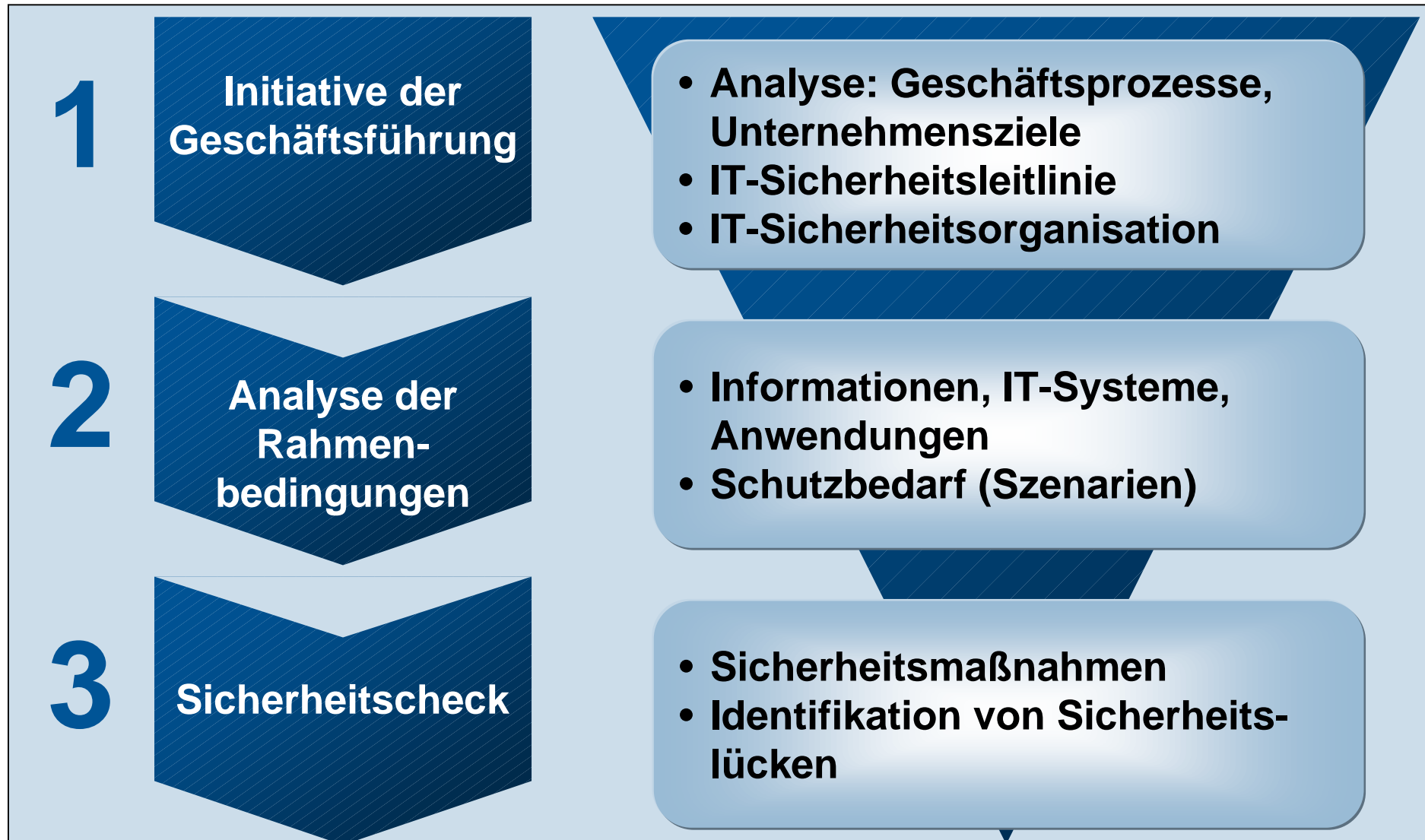
IT-Grundschutz Vorgehensweise

- ❑ ersetzt Kapitel 2 vom GS HB
- ❑ beschreibt die Methodik
- ❑ fokussiert auf
Managementaspekte

Integration einer Methode zur
Risikobetrachtung für hohen und
sehr hohen Schutzbedarf



Übersicht über den IT-Sicherheitsprozess



Übersicht über den IT-Sicherheitsprozess



IT-Sicherheitsmanagement

Verantwortung der Leitung

Ziele:

- Früherkennung und Minimierung von möglichen Risiken (KonTraG, Basel II, ...)
- Gewährleistung von vertraglichen IT-Sicherheitsanforderungen
- Orientierung an Standard-Vorgehensweisen

Vorgehen:

- Festlegung der IT-Sicherheitsziele
- Definition von Zuständigkeiten
- IT-Sicherheit integrieren
- Vorbild-Funktion der Leitung
- Kommunikation und Wissen
- Lenkung, Kontrolle und kontinuierliche Verbesserung

IT-Sicherheitsorganisation

IT-Sicherheitsorganisation

- ❑ Festlegung von Verantwortlichkeiten
- ❑ Planung und Überwachung der Umsetzung
- ❑ Kommunikationskanal im IT-Sicherheitsprozess

IT-Sicherheitsbeauftragter

- ❑ zentraler Ansprechpartner für Belange der IT-Sicherheit

→ Rückendeckung durch die Geschäftsleitung

IT-Sicherheitsleitlinie

- ❑ Bedeutung der IT und IT-Sicherheit für die Aufgabenerfüllung
- ❑ Festlegung der IT-Sicherheitsziele und -strategie
- ❑ Definition einer Organisationsstruktur für die IT-Sicherheit

→ Geschäftsleitung muss die IT-Sicherheitsleitlinie tragen!

→ IT-Sicherheitsleitlinie muss aktuell gehalten werden

IT-Sicherheitsmanagement

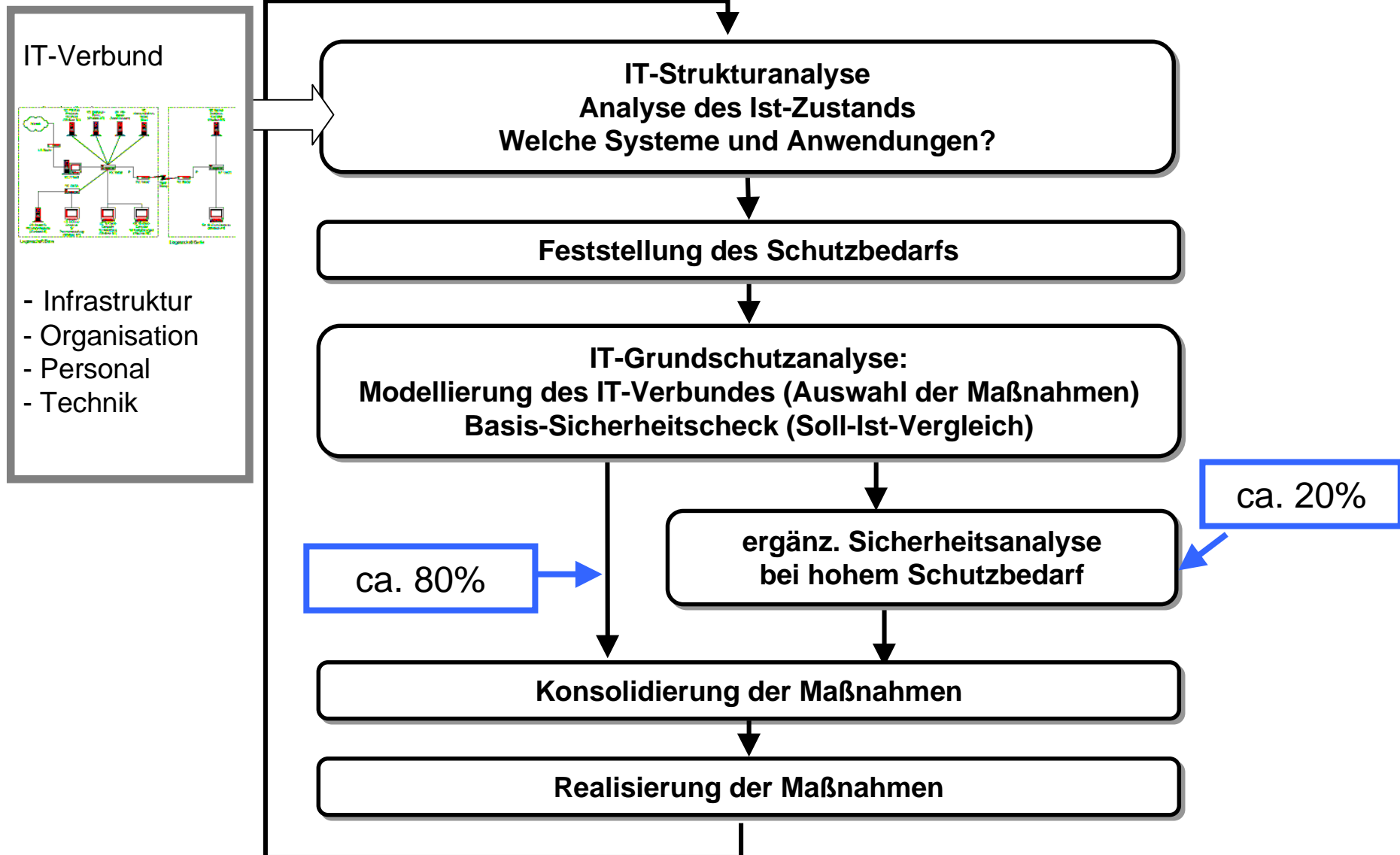
Ressourcen-Management

- Ressourcen für
 - den IT-Betrieb
 - die IT-Sicherheit
 - die Überprüfung der IT-Sicherheit

- Zugriff auf externe Ressourcen

- Wirtschaftlichkeitsaspekte in der IT-Sicherheitsstrategie

IT-Sicherheitskonzeption



IT-Verbund Definition

Ein **IT-Verbund** ist die Gesamtheit von

- ❑ infrastrukturellen,
- ❑ organisatorischen,
- ❑ personellen und
- ❑ technischen Komponenten,

die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

Ein **IT-Verbund** kann umfassen:

- ❑ die gesamte IT einer Institution
- ❑ einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z. B. Personal-Informationssystem) gegliedert sind
- ❑ Geschäftsprozesse

IT-Strukturanalyse: Analyse des Ist-Zustandes

Teilaufgaben

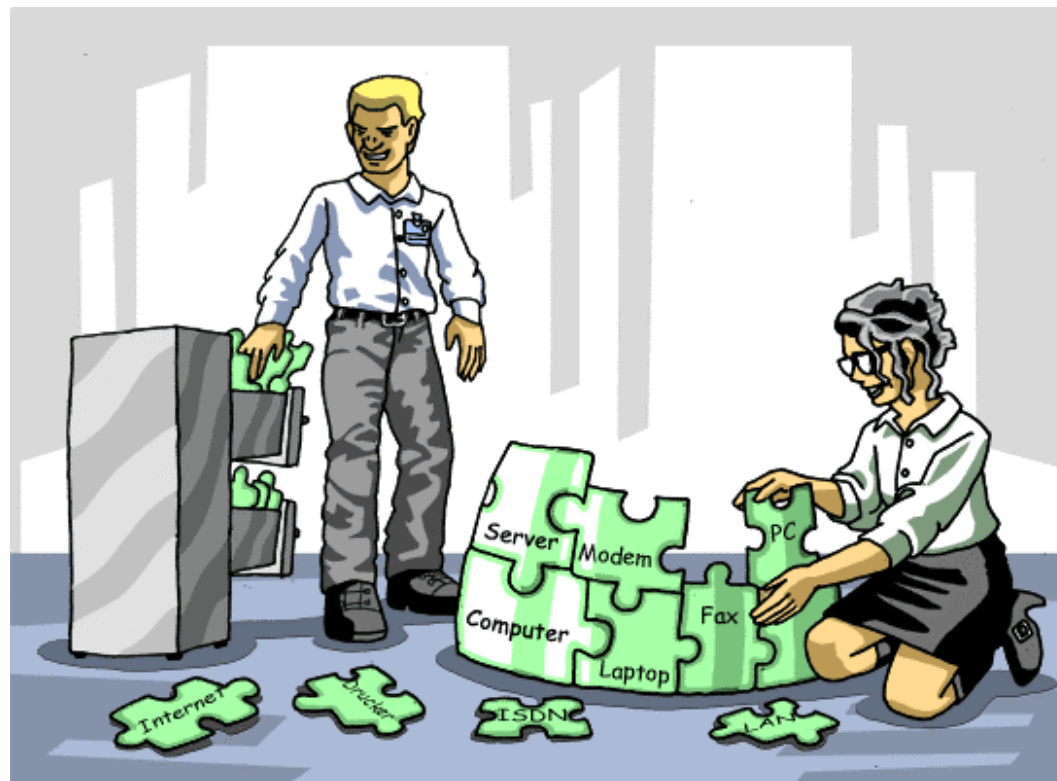
- ❑ Erstellung bzw. Aktualisierung eines Netzplans
(grafische Übersicht)
 - ❑ Erhebung der IT-Systeme (Tabelle)
 - ❑ Erfassung der IT-Anwendungen und der zugehörigen Informationen
(Tabelle)
 - ❑ Erhebung der IT-Räume
- ➔ Komplexitätsreduktion durch Gruppenbildung

Schutzbedarfsfeststellung

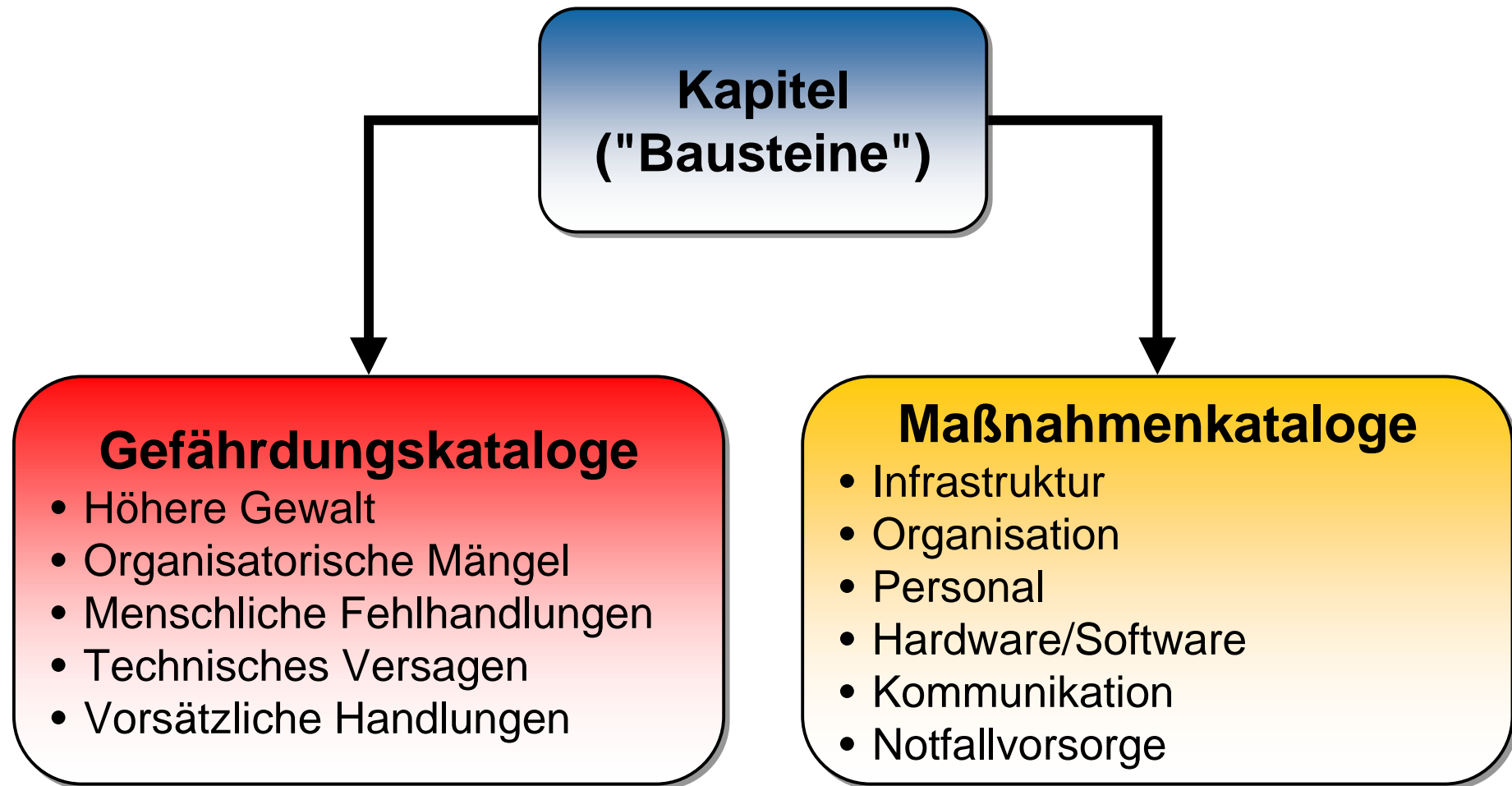
Schadensszenarien

- ❑ Schutzbedarfsfeststellung erfolgt immer bezüglich der Grundwerte **Vertraulichkeit, Integrität und Verfügbarkeit**.
- ❑ Betrachtung von **typischen Schadensszenarien** aus Sicht der Anwender ("Was wäre, wenn... ?")
 - ❑ Verstoß gegen Gesetze, Vorschriften, Verträge
 - ❑ Beeinträchtigung des informationellen Selbstbestimmungsrechts
 - ❑ Beeinträchtigung der persönlichen Unversehrtheit
 - ❑ Beeinträchtigung der Aufgabenerfüllung
 - ❑ negative Außenwirkung
 - ❑ finanzielle Auswirkungen
- ❑ **Individualisierung** der Zuordnungstabelle!

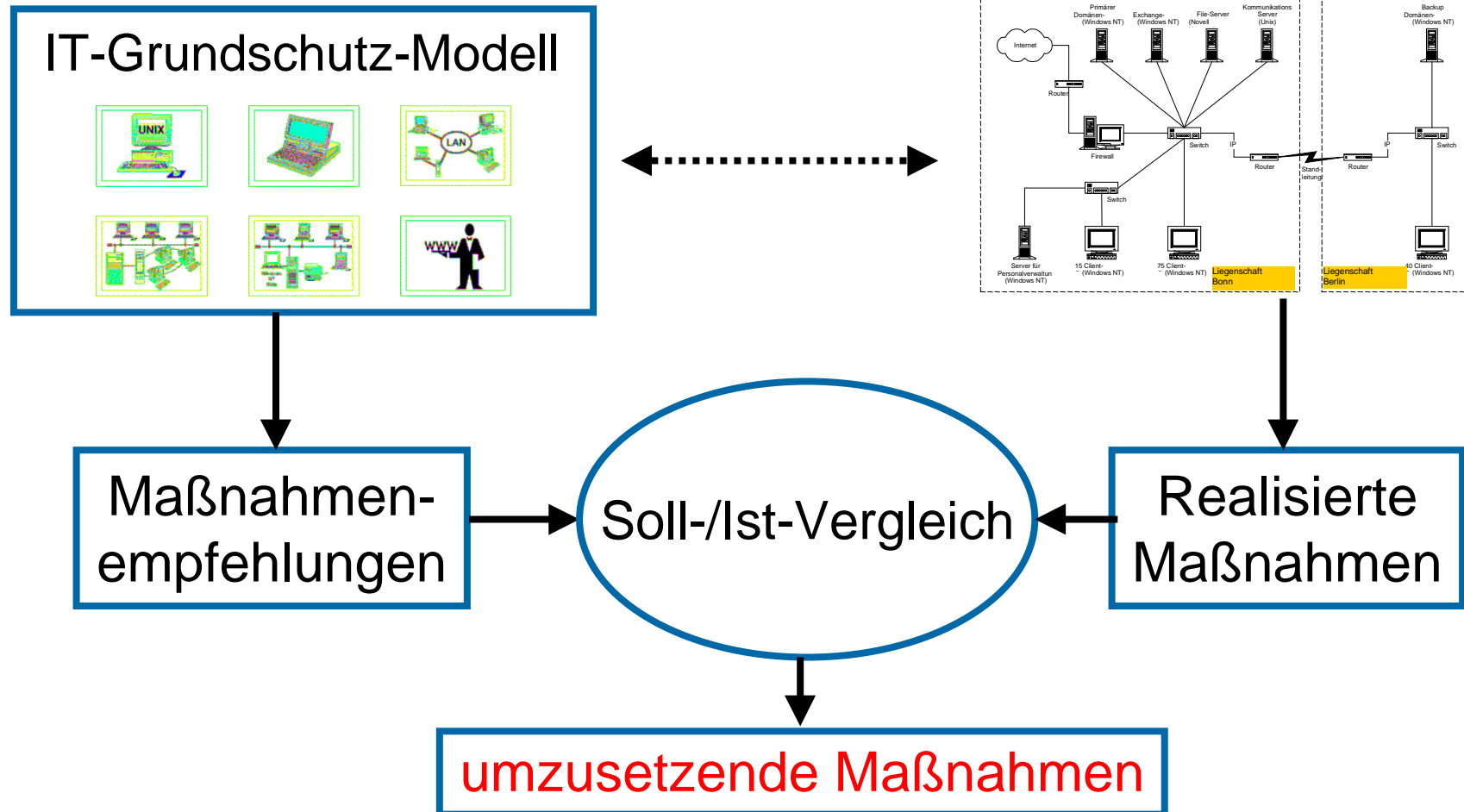
Nachbildung des IT-Verbunds durch Bausteine des IT-Grundschutzhandbuchs



IT-Grundschutz Bausteine Struktur

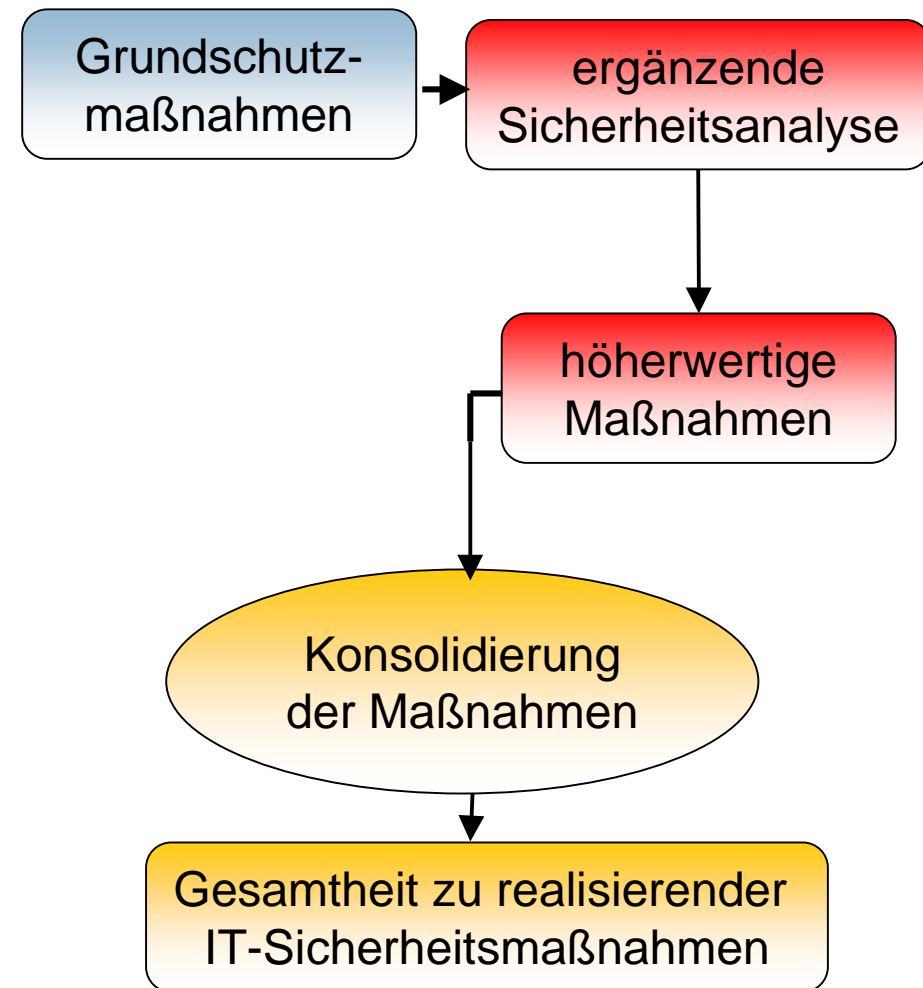


Basis-Sicherheitscheck



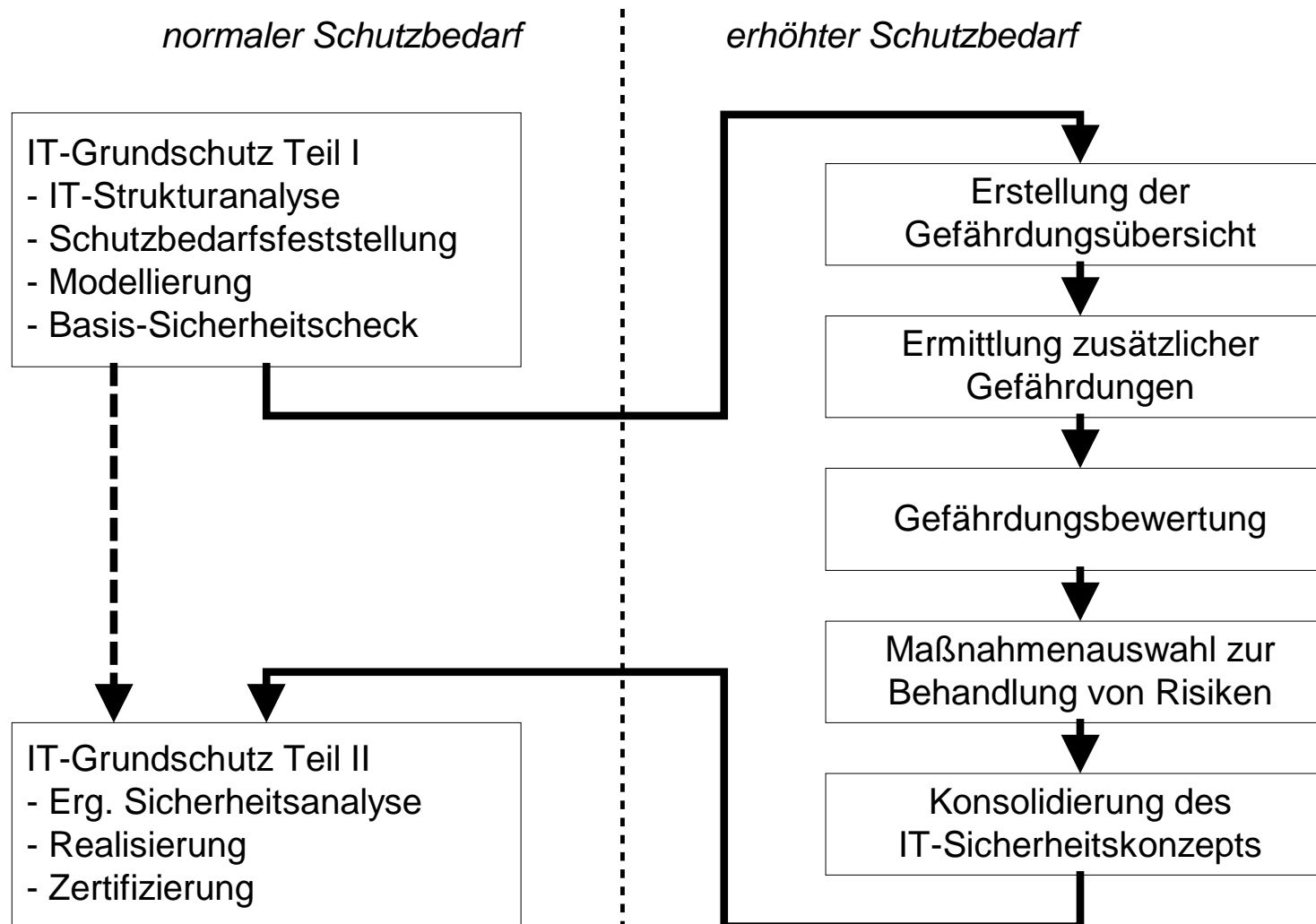
Ergänzende Sicherheitsanalyse

- ❑ hoher oder sehr hoher Schutzbedarf
- ❑ zusätzlicher Analysebedarf
- ❑ Kein geeigneter IT-Grundschatz Baustein für bestimmte Aspekte



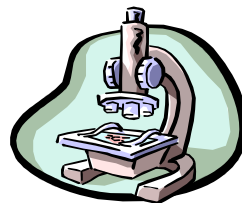
<http://www.bsi.bund.de/gshb/risikoanalyse>

Risikoanalyse auf der Basis von IT-Grundschutz



Konsolidierung des IT-Sicherheitskonzepts

- ❑ Sind die IT-Sicherheitsmaßnahmen zur Abwehr der jeweiligen Gefährdungen **geeignet**?
- ❑ **Wirken** die IT-Sicherheitsmaßnahmen sinnvoll **zusammen**?
- ❑ Sind die IT-Sicherheitsmaßnahmen **benutzerfreundlich**?
- ❑ Sind die IT-Sicherheitsmaßnahmen **angemessen**?



IT-Sicherheitsprozess

Aufrechterhaltung und Verbesserung (1)

- ❑ Regelmäßige Prüfungen

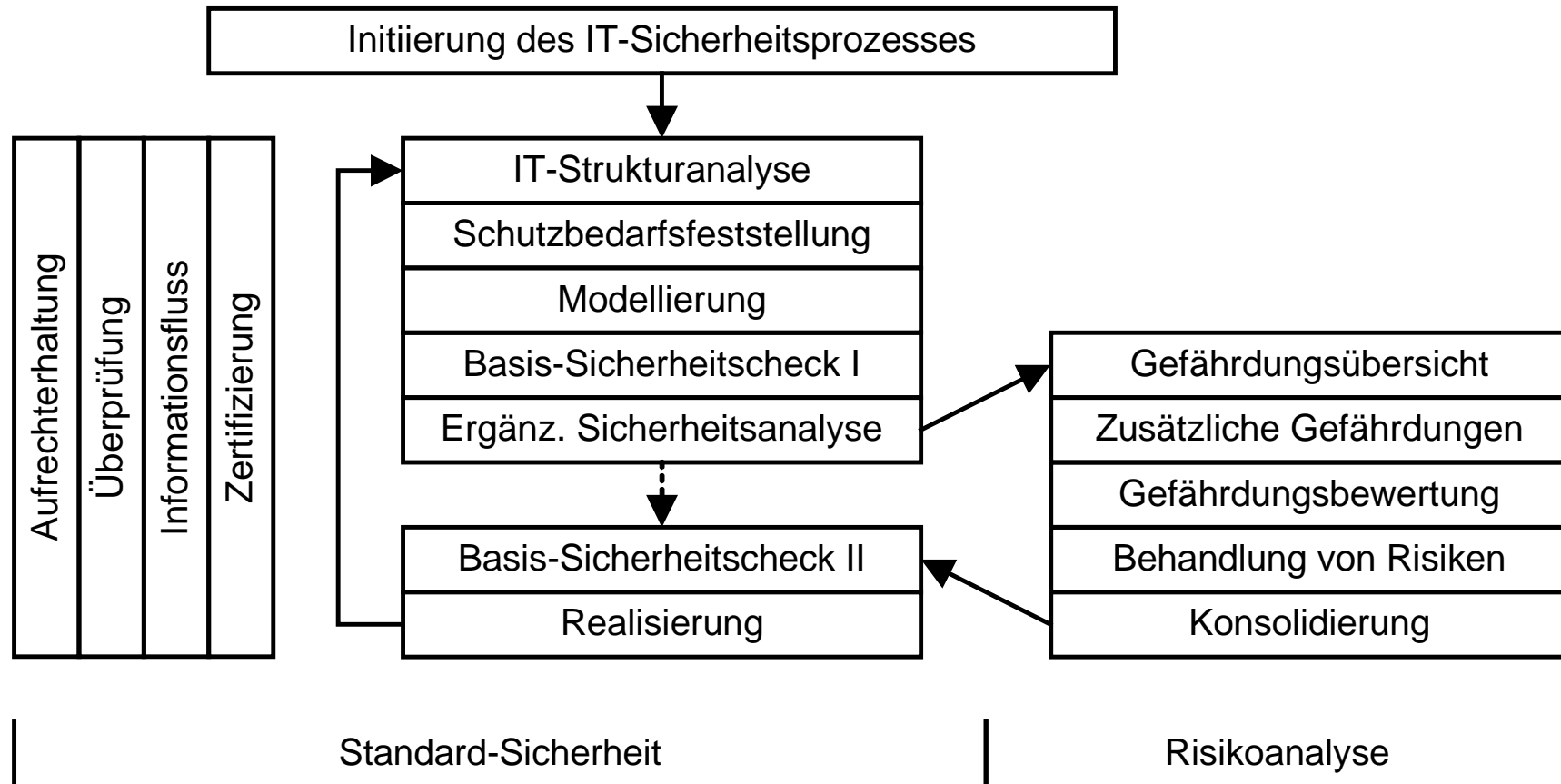
- ❑ Anlassbezogene Prüfungen
 - ❑ neue IT-Komponenten oder Prozesse
 - ❑ größere Änderungen der Infrastruktur (z. B. Umzug),
 - ❑ größere organisatorischen Änderungen (z. B. Outsourcing),
 - ❑ Veränderung der Gefährdungslage
 - ❑ Bekanntwerden von gravierenden Schwachstellen
oder Schadensfällen

IT-Sicherheitsprozess

Aufrechterhaltung und Verbesserung (2)

- ❑ Prüfung von
 - ❑ Einhaltung
 - ❑ Wirksamkeit
 - ❑ Effizienz
- der Sicherheitskonzeption
- ❑ Gegenmaßnahmen bei Feststellung von Abweichungen
 - ❑ Einbeziehung des verantwortlichen Vorgesetzten (bis hin zur Leitungsebene)
 - ❑ Managementreports (regelmäßig und anlassbezogen)

Vorgehensweise im Überblick



Weiterentwicklung der IT-Grundschutz-Zertifizierung 2005/2006

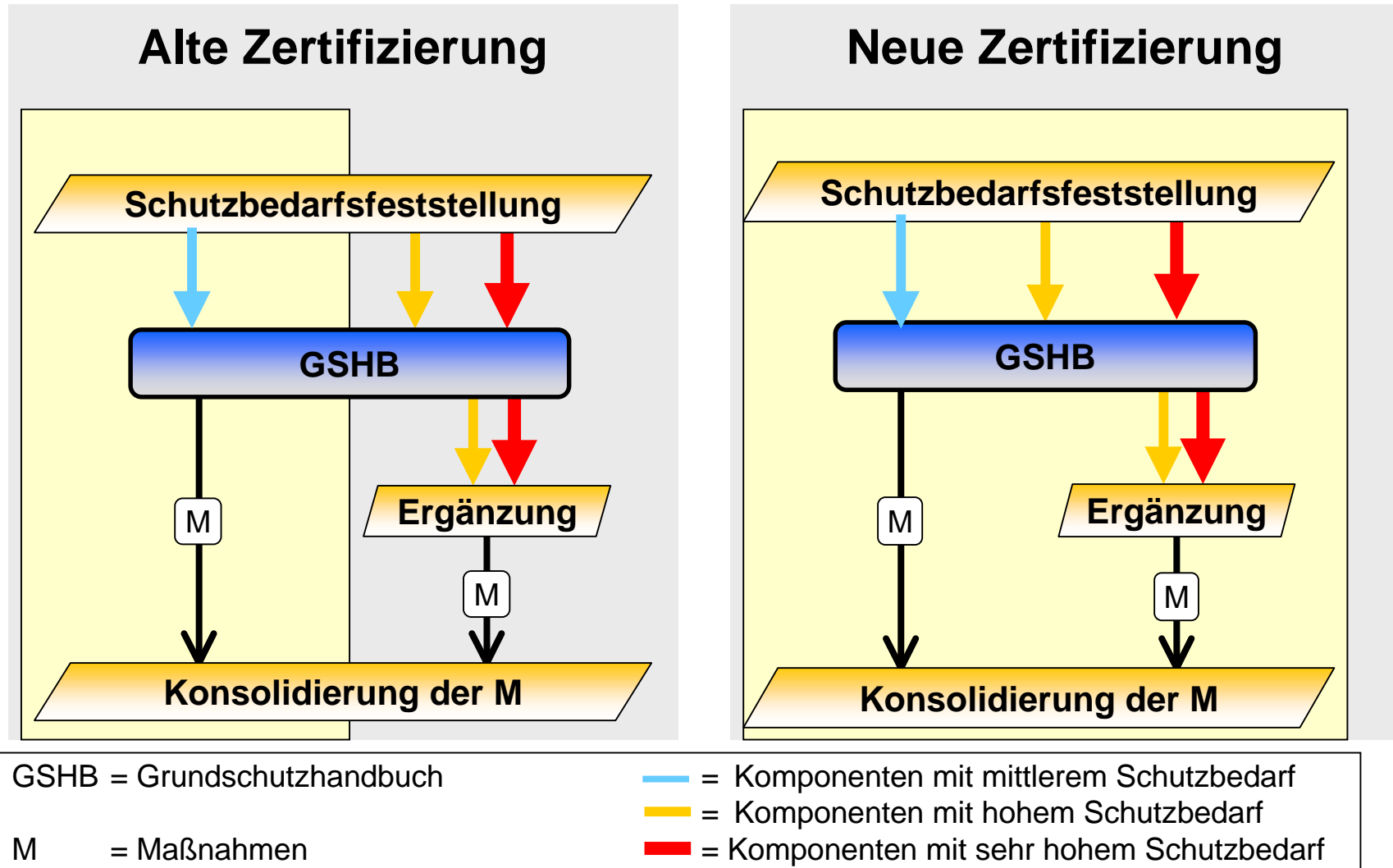
Eine BSI-Zertifizierung...

- ❑ umfaßt sowohl eine Prüfung des ISMS als auch der konkreten IT-Sicherheitsmaßnahmen auf Basis von IT-Grundschutz,
- ❑ beinhaltet **immer** eine offizielle ISO-Zertifizierung nach ISO 27001,
- ❑ ist aber aufgrund der zusätzlich geprüften technischen Aspekte wesentlich **aussagekräftiger** als eine reine ISO-Zertifizierung.

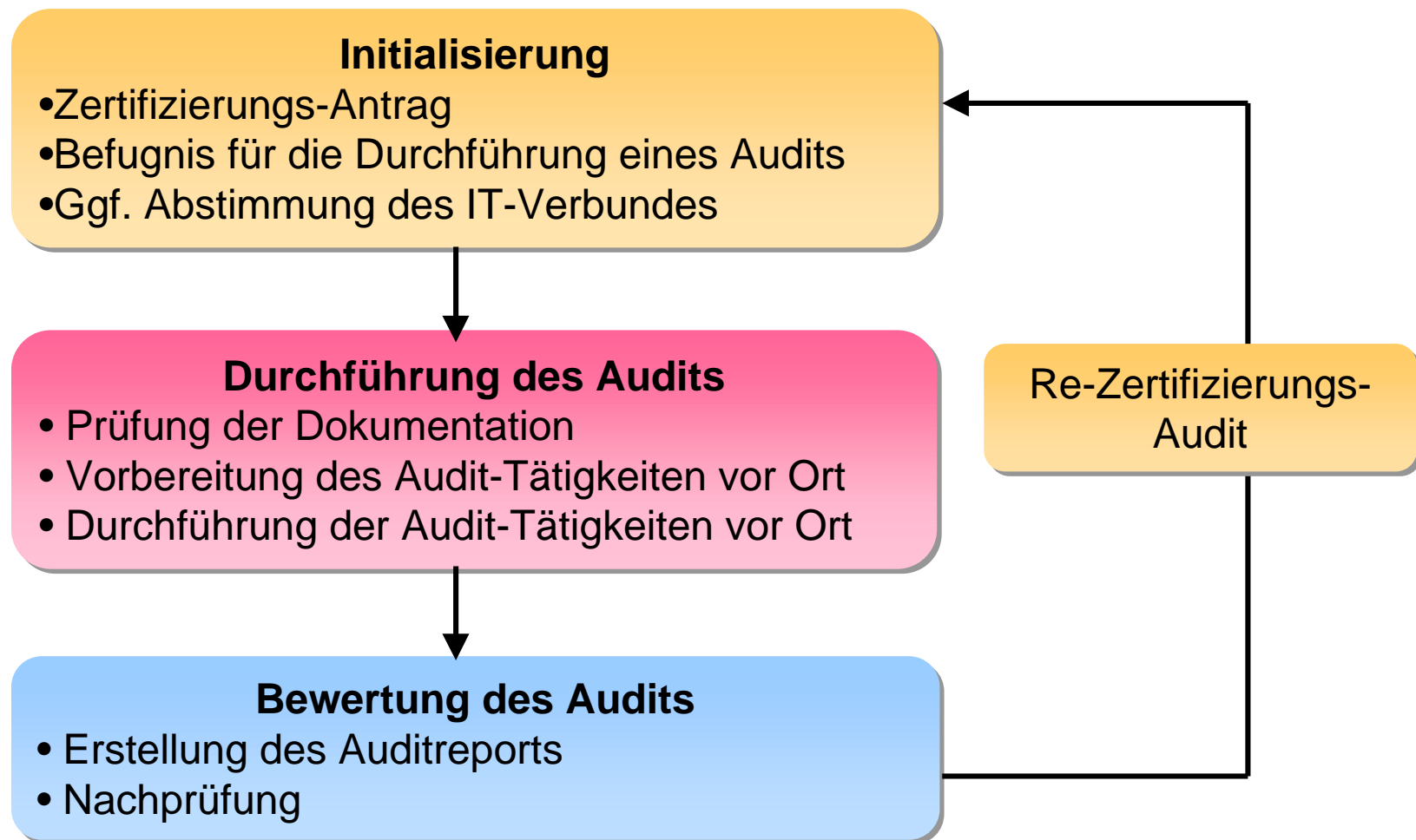
Vom BSI lizenzierte Auditoren...

- ❑ erfüllen alle Anforderungen, die die ISO an Auditoren für ein ISMS stellt (EA -7/03)

ISO-27001 Zertifizierung auf der Basis von IT-Grundschutz



Phasen der ISO 27001-Zertifizierung

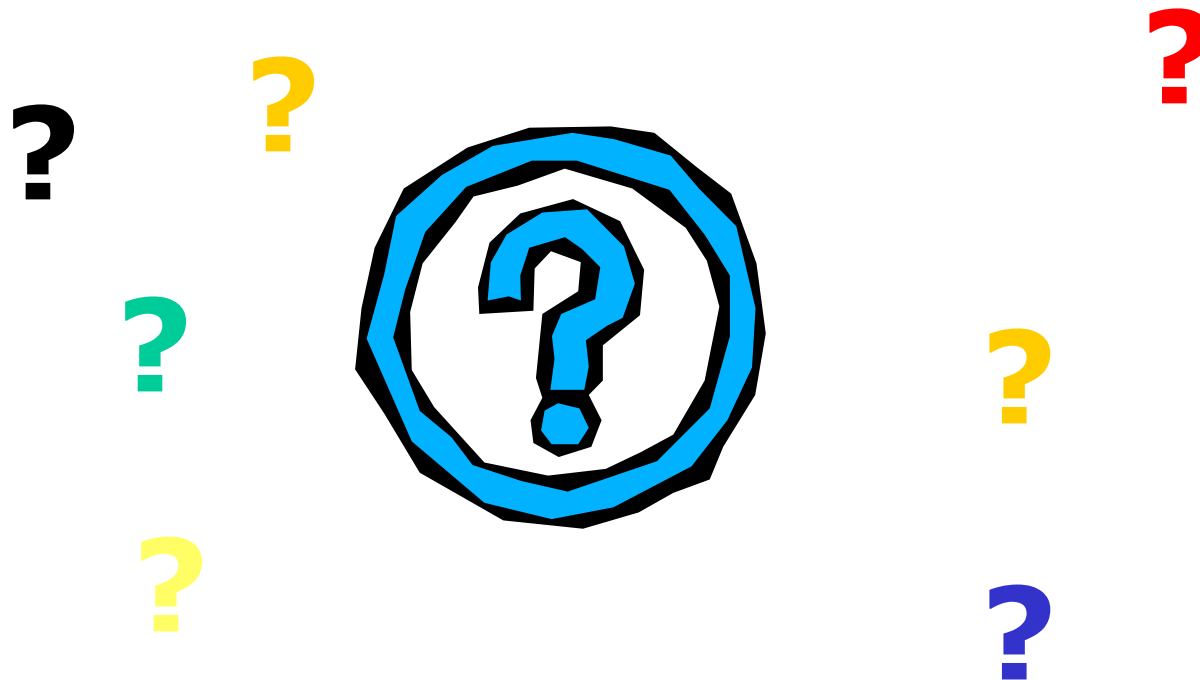


Materialien und Tools rund um den IT-Grundschutz

- Leitfaden IT-Sicherheit
- Musterrichtlinien
- Beispiel-Profile für den IT-Grundschutz
- Webkurs IT-Grundschutz
- GSTOOL
- Webkurs GSTOOL
- Kreuzreferenztabellen
- ...

- www.bsi.de

IT Grundschutz Fragen?



Kontakt



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Dr. Lydia Tsintsifa
Godesberger Allee 185-189
53175 Bonn

lydia.tsintsifa@bsi.bund.de
Tel: +49 (0)1888-9582-240
Fax: +49 (0)1888-9582-90240

GSHB Hotline:
gshb@bsi.bund.de
Tel: +49 (0)1888-9582-369

www.bsi.de