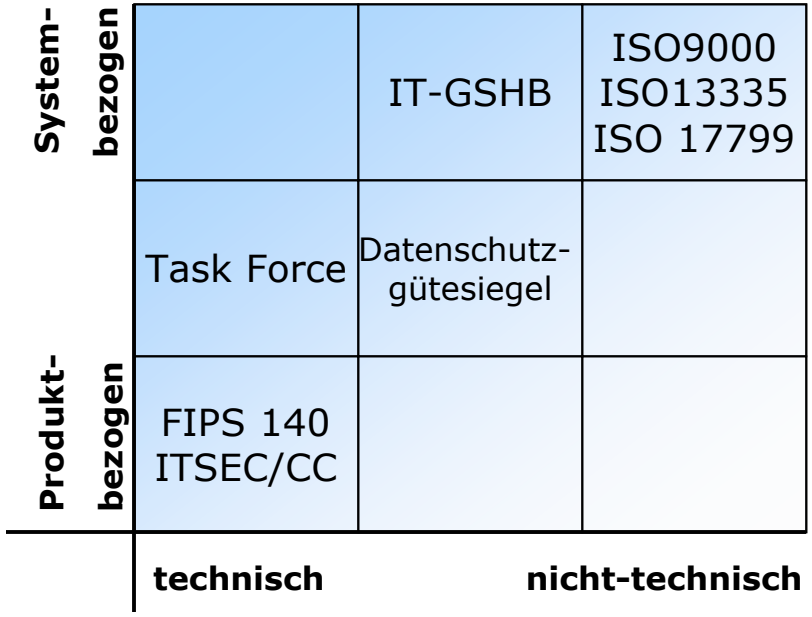
IT-Sicherheitsmanagement nach ISO 17799 und nach BSI-Grundschutzhandbuch — Eine vergleichende Betrachtung

Prof. Dr. Hannes Federrath
Universität Regensburg

http://www-sec.uni-regensburg.de

Kriterienlandschaft Sicherheitsmanagement

- Sicherheitsbezogene Standards existieren für
  - kryptographische Methoden
  - Hardwaresicherheit
  - Verfahren für Schlüssel- und Zertifikatsmanagement
  - ...
- teilweise sogar banchenspezifische Standards (z.B. Banking)



nach: Initiative D21: IT-Sicherheitskriterien im Vergleich. Leitfaden der Projektgruppe IT-Sicherheitskriterien und IT-Grundschutz-Zertifikat/Qualifizierung, Projekt der Arbeitsgruppe Sicherheit und Vertrauen im Internet, 20.12.2001.

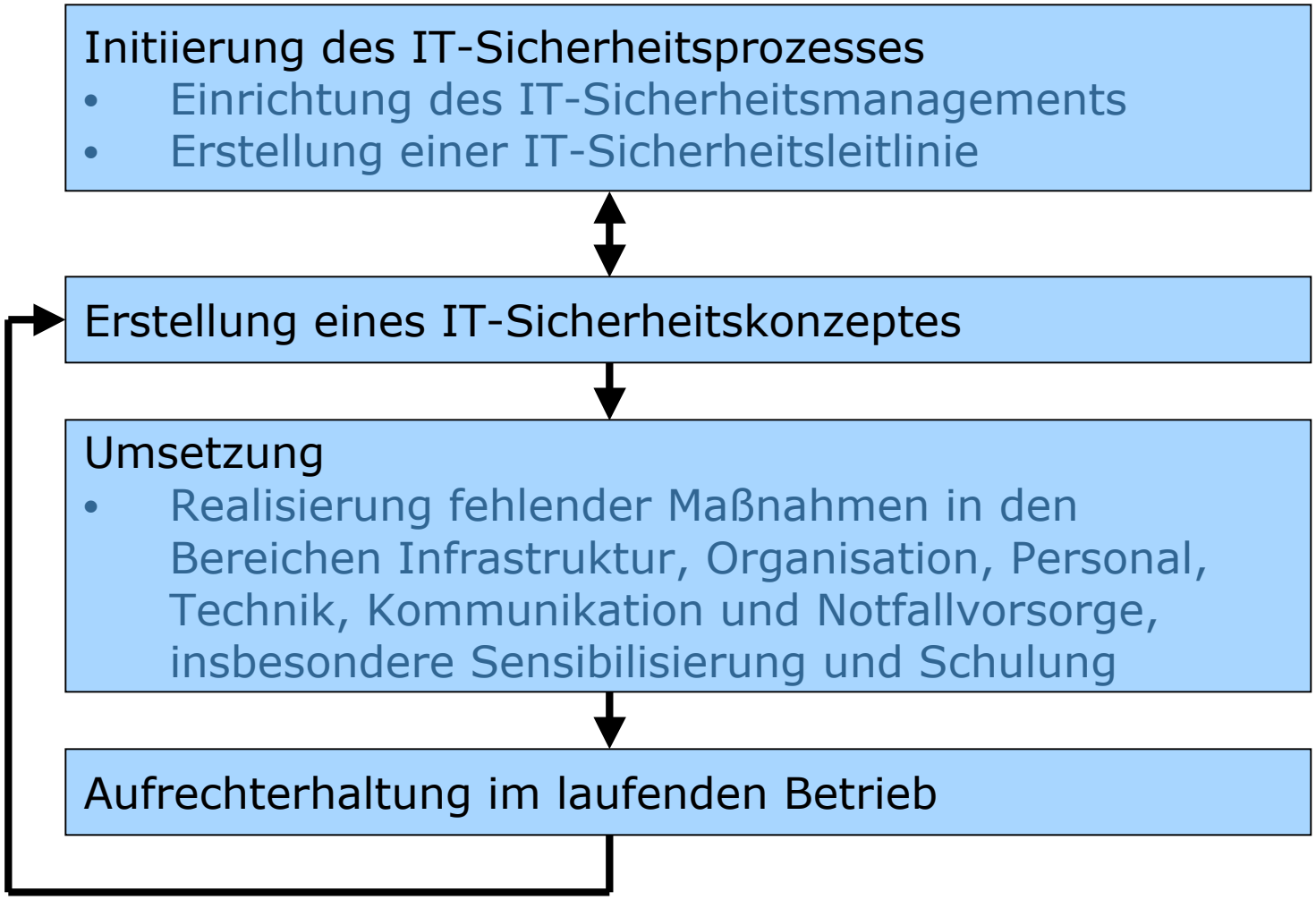
IT-Grundschutzhandbuch (GSHB)

- beschreibt Standardsicherheitsmaßnahmen für typische IT-Systeme mit "normalem" Schutzbedarf
  - Standard-Sicherheitsmaßnahmen aus den Bereichen Infrastruktur, Organisation, Personal, Technik und Notfallvorsorge
  - keine Maßnahmen für Individuallösungen

- vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) herausgegeben
  - etwa 2000 Seiten Papier, auch auf CD-ROM erhältlich
  - Online unter http://www.bsi.bund.de/gshb/
  - wird halbjährlich aktualisiert

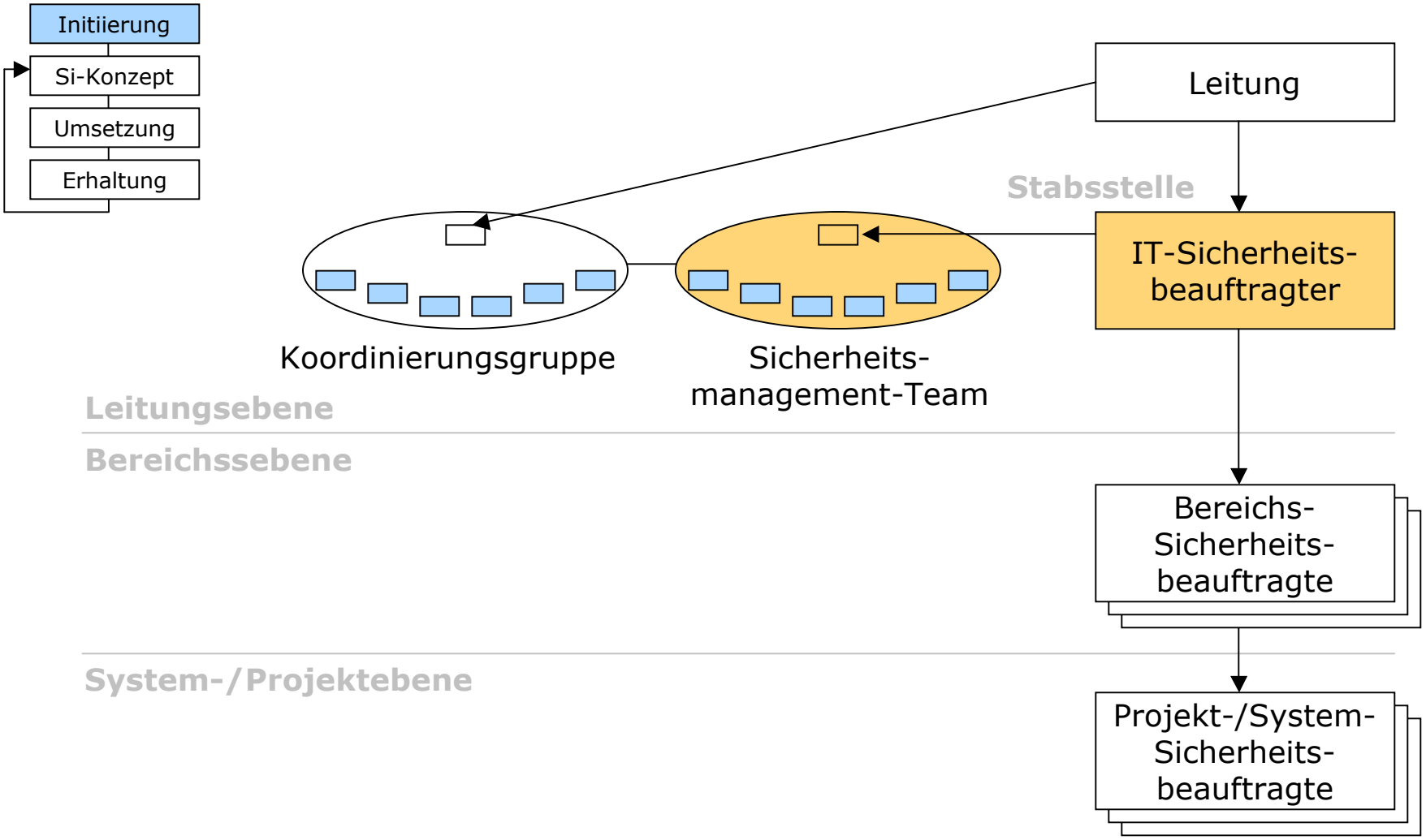
- keine traditionelle Risikoanalyse
  - stattdessen Soll-Ist-Vergleich zwischen empfohlenen und bereits realisierten Maßnahmen

Anwendung des IT-Grundschutzhandbuchs



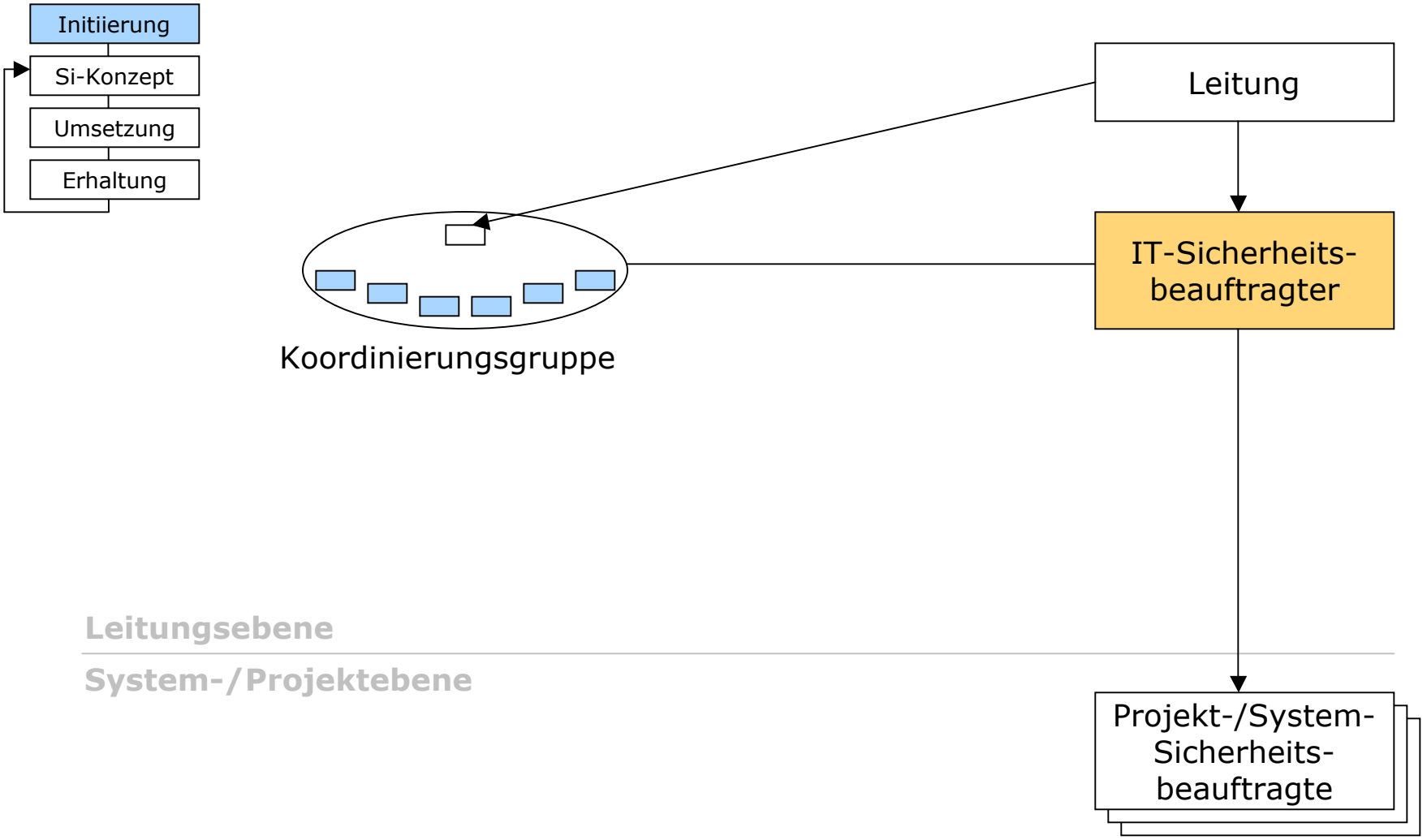
vgl. GSHB, M2.191

Organisationsstruktur für IT-Sicherheit: *Große Organisationen*



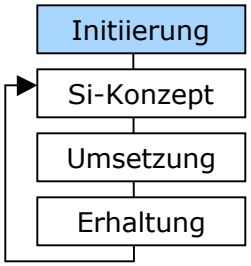
nach: GSHB, M2.193

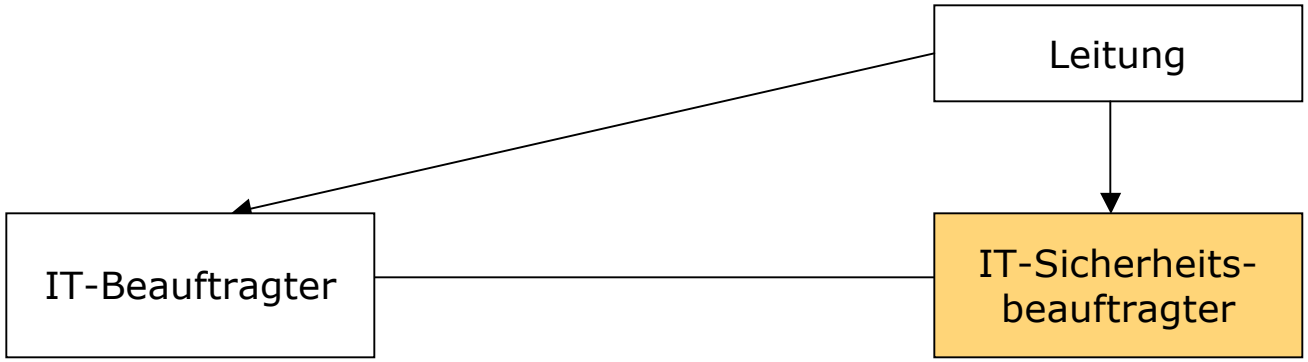
Organisationsstruktur für IT-Sicherheit: *Mittlere Organisationen*



nach: GSHB, M2.193

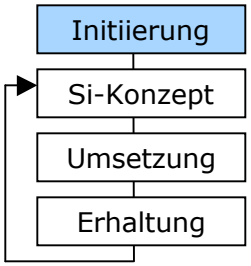
Organisationsstruktur für IT-Sicherheit: *Kleine Organisationen*





nach: GSHB, M2.193

Erstellung einer Sicherheitsleitlinie nach GSHB, M 2.192



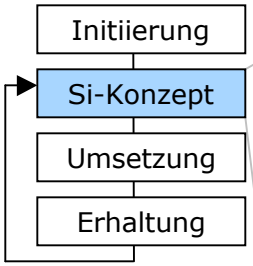
Inhalt der Sicherheitsleitlinie:

- Bedeutung der IT-Sicherheit
- Sicherheitsziele und Sicherheitsstrategie
- Verpflichtung des Managements
- Etablierte Organisationsstruktur

optional:

- Zuweisung von Verantwortlichkeiten
- Vorgehensweise bei Verstößen
- Überblick über die Dokumentationen
- Angaben zur periodischen Überprüfung
- Maßnahmen zur Schulung und Sensibilisierung

Erstellung eines IT-Sicherheitskonzepts



IT-Strukturanalyse
- Erfassung der IT und der IT-Anwendungen
- Gruppenbildung

Schutzbedarfsfeststellung

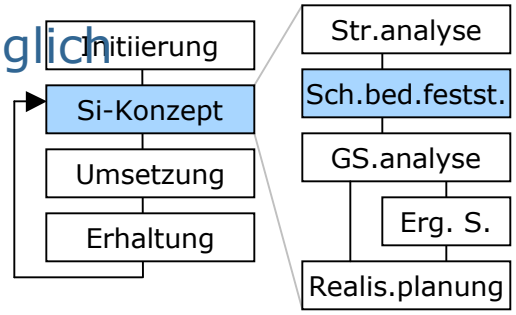
IT-Grundschutzanalyse
- Modellierung nach IT-Grundschutz
- Basis-Sicherheitscheck mit Soll-Ist-Vergleich

Ergänzende Sicherheitsanalyse
- bei hohem Schutzbedarf
- bei zusätzlichem Analysebedarf

Realisierungsplanung
- Konsolidierung der Maßnahmen
- Umsetzungsplan

vgl. GSHB, M2.195

Schutzbedarfsfeststellung

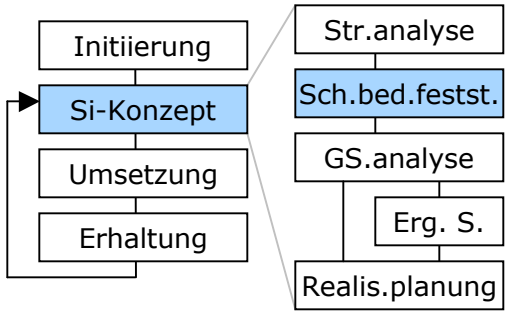


- Schutzbedarf der zuvor erfassten Systeme bezüglich
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

  ermitteln
- dabei Orientierung an den möglichen Schäden

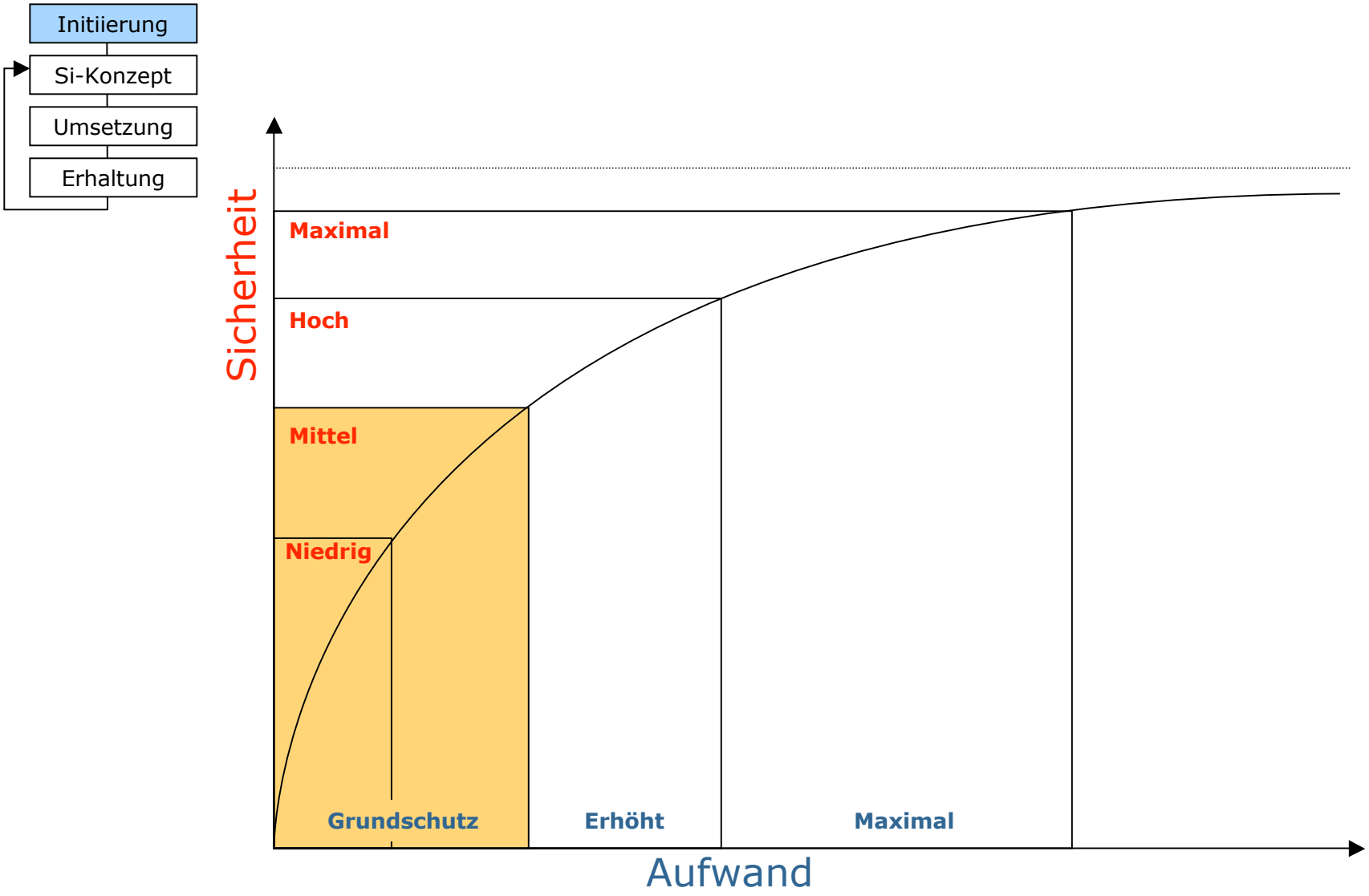
- Unterteilung des Schutzbedarfs in drei Kategorien:
  - "niedrig bis mittel"
    - Schadensauswirkungen sind begrenzt und überschaubar
  - "hoch"
    - Die Schadensauswirkungen können beträchtlich sein.
  - "sehr hoch"
    - Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Schutzbedarfsfeststellung



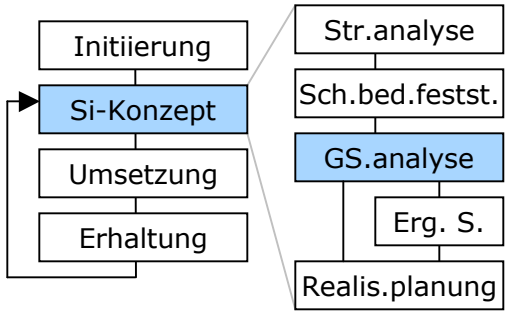
- Interpretation im Hinblick auf die Schutzwirkung des GSHB:
  - Schutzbedarfskategorie "niedrig bis mittel":
    - Standard-Sicherheitsmaßnahmen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
  - Schutzbedarfskategorie "hoch":
    - Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, sind aber u. U. alleine nicht ausreichend. Weitergehende Maßnahmen können auf Basis einer ergänzenden Sicherheitsanalyse ermittelt werden.
  - Schutzbedarfskategorie "sehr hoch":
    - Standard-Sicherheitsmaßnahmen nach IT-Grundschutz bilden einen Basisschutz, reichen aber alleine i. A. nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer ergänzenden Sicherheitsanalyse ermittelt werden.

Aufwand-Nutzen-Relation nach GSHB, M 2.192



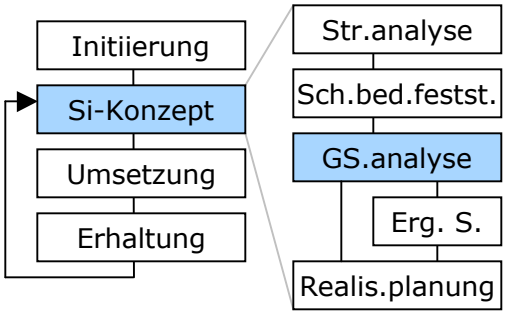
Modellierung nach IT-Grundschutz

- Bausteine in Schichten organisiert:
  1. Schicht: Übergreifende Aspekte
  2. Schicht: Infrastruktur
  3. Schicht: IT-Systeme
  4. Schicht: Netze
  5. Schicht: IT-Anwendungen



- Vorgehen
  1. Anfertigen einer Tabelle, die die Bausteine des GSHB den Zielobjekten zuordnet
  2. danach Überprüfung, ob alle IT-Komponenten abgedeckt sind.
     - falls kein passender Baustein im GSHB vorhanden:
       An ähnlichen Bausteinen orientieren und diese sinngemäß anwenden

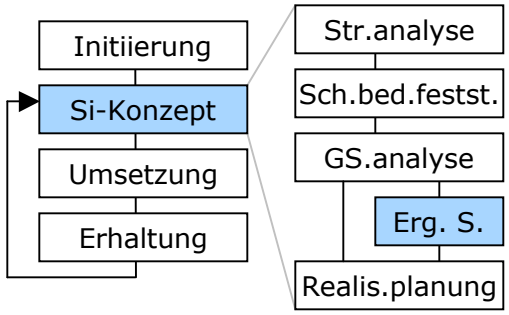
Basis-Sicherheitscheck mit Soll-Ist-Vergleich



- Methode
  - Durchführung von Interviews
- Ziel
  - Einteilung der Maßnahmenbeurteilungen in die Kategorien entbehrlich, ja, teilweise und nein
- Dokumentation der Ergebnisse
  - Standardisierte Dokumentation der Ergebnisse

Ergänzende Sicherheitsanalyse

- Ggf. notwendig für Systeme mit hohem bzw. sehr hohem Schutzbedarfsniveau

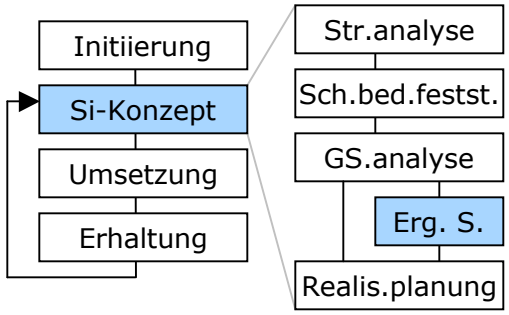


- Mögliche Methoden
  - Risikoanalyse
  - Penetrationstest
  - Differenz-Sicherheitsanalyse

- Risikoanalyse
  - Relevante Bedrohungen erkennen
  - Eintrittswahrscheinlichkeit und Schutzbedarf ermitteln
  - Geeignete Sicherheitsmaßnahmen auswählen, um die Eintrittswahrscheinlichkeit zu senken bzw. die Schadenshöhe zu reduzieren

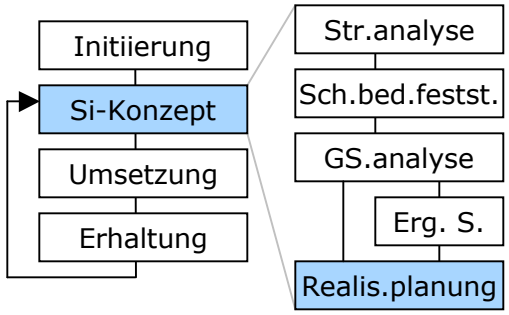
Ergänzende Sicherheitsanalyse

- Penetrationstest
  - Simulation möglicher Angriffe
  - Blackbox-Ansatz:
    - Angreifer besitzt keinerlei Informationen über IT-Verbund (Außentäter)
  - Whitebox-Ansatz:
    - Angreifer besitzt Kenntnisse über den internen Aufbau, Anwendungen und Dienste im IT-Verbund (Innentäter)



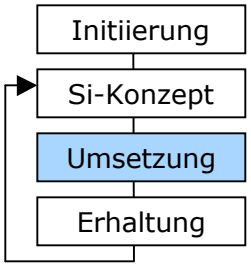
- Differenz-Sicherheitsanalyse
  - Feststellen, welche der Sicherheitsmaßnahmen über die Grundschutzmaßnahmen hinausgehend realisiert sind
  - Vergleich durchführen, ob die ergriffenen Maßnahmen den Musterlösungen entsprechen, die sich in der Praxis für hochschutzbedürftige IT-Bereiche etabliert haben

Realisierung von IT-Sicherheitsmaßnahmen



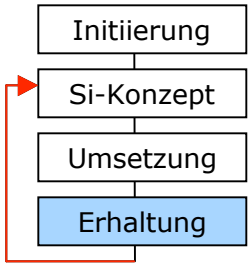
1. Sichtung der Untersuchungsergebnisse
2. Konsolidierung der Maßnahmen
   - nochmals Prüfung der Eignung der Maßnahmen und evtl. Anpassungen vornehmen und dokumentieren
3. Kosten- und Aufwandsschätzung und Wirtschaftlichkeitsabwägungen
4. Festlegung der Umsetzungsreihenfolge der Maßnahme
   - unter Berücksichtigung der Maßnahmenprioritäten und logischer Abhängigkeiten
5. Festlegung der Verantwortlichkeit
   - Wer muss bis wann welche Maßnahmen realisieren und wer muss sie überwachen?
6. Realisierungsbegleitende Maßnahmen
   - v. a. Schulung und Sensibilisierung der Mitarbeiter bzgl. der Maßnahmen

Umsetzung der IT-Sicherheitsmaßnahmen, M 2.196



- Realisierungsplan enthält Angaben zu
  - Verantwortlichkeiten
  - Priorität
  - Zeitpunkt
  - Ressourcen
- Begleitende Maßnahmen
  - Schulungskonzept erstellen: M 2.197
  - Sensibilisierung der Mitarbeiter: M 2.198
- Umsetzung
  - Gestaltung von technischen und organisatorischen Abläufen an den Arbeitsplätzen
  - Anpassung der Aufgabenbeschreibungen
  - Bereitstellung von Anleitungen und Informationen für Schulung und Sensibilisierung
  - Bereitstellung von Hilfsmitteln

Aufrechterhalten des sicheren Betriebs, M 2.199



- Regelmäßige und anlaßbezogene Prüfungen vornehmen
- Revision und Aktualisierung
  - Übereinstimmung mit Dokumentation
  - beabsichtigte Funktionsweise
  - Prüfung auf Aktualität
- Managementreport erstellen: M 2.200
  - regelmäßig und ggf. anlaßbezogen
  - Präsentation des Status, ggf. des Vorfalls
  - ggf. Entscheidungsvorlage erarbeiten
- ggf. Korrekturen vornehmen

ISO 17799

ISO 17799

- International Standard ISO/IEC 17799

  Information technology — Code of practice for information security management, 2000

- Zweck/eigener Anspruch
  - «A comprehensive set of controls comprising best practices in information security»
  - Internationaler «Code of practice» für das Management der Informationssicherheit

- Umfang
  - 71 Seiten, umfasst 10 Gliederungspunkte bzgl. Managementaufgaben

Gliederungspunkte

• Security policy	• *Sicherheitspolitik*
• Organizational security	• *Organisatorische Sicherheit*
• Asset classification and control	• *Einstufung und Kontrolle der Werte*
• Personnel security	• *personelle Sicherheit*
• Physical and environmental security	• *physische und umgebungsbezogene Sicherheit*
• Communications and operations management	• *Management der Kommunikation und des Betriebs*
• Access control	• *Zugriffskontrolle*
• Systems development and maintenance	• *Systementwicklung und -wartung*
• Business continuity management	• *Management des kontinuierlichen Geschäftsbetriebs*
• Compliance	• *Einhaltung der Verpflichtungen*

Organizational security

1. Infrastrukturmaßnahmen
   - Security Manager
   - Koordinationsgruppe
2. Zugriff auf Unternehmensdaten durch Dritte
   - Festlegen von Zugriffsarten (logischer, physischer) Zugriff
   - Beschreiben, für welche Aufgaben der Zugriff nötig ist
3. Outsourcing
   - Vertragliche Festlegung von Sicherheitsanforderungen, z.B.
     - Einhaltung gesetzlicher Vorschriften (z.B. Datenschutz)
     - Maßnahmen zur Einhaltung der Sicherheitsvorschriften auch durch «subcontractors»
     - Maßnahmen zur Erhaltung des Sicherheitsniveaus
     - Physische Sicherheitsmaßnahmen
     - Recht auf Überprüfung der Einhaltung der festgelegten Anforderungen

Asset classification and control

1. Führen einer «Inventarliste»
   - Information assets
   - Software assets
   - Physical assets
   - Services

2. Klassifikation
   - Festlegen des notwendigen Schutzgrades
     - von sensitiv/kritisch ····· unwichtig/egal

Personnel security

1. Sicherheit bei der Stellenbesetzung zur Vermeidung von menschlichem Versagen, Missbrauch, Diebstahl, Betrug
   - Sicherheitsüberprüfung der Mitarbeiter
   - Non-Disclosure-Agreements mit Externen
2. Trainingsmaßnahmen zur Verbesserung der «Awareness»
   - Schulung und Sensibilisierung im Umgang mit Informationen
3. Vorgehensweise bei Sicherheitsverletzungen und Fehlfunktionen
   - Berichtswesen und Vorgehen bei Entdecken von
     - Sicherheitsschwächen,
     - Sicherheitsverletzungen und
     - Fehlfunktionen
   - Disziplinarmaßnahmen

Physical and environmental security

1. Sicherheitsbereiche festlegen
   - Aufbau physischer Barrieren
   - Definition von Besucherrichtlinien
   - Zugangskontrollen an Gebäuden, Räumen und Systemen
   - Absicherung von Büros, Räumen und Einrichtungen
     - «Fenster schließen bei Verlassen der Büros»
2. Gerätesicherheit
   - Generelle Empfehlungen
     - «Nicht essen am Computer»
   - Geeignete Energieversorgung
     - UPS, Notstrom
   - Entsorgung von Geräten, Datenträgern
     - vorher Daten löschen/unkenntlich machen
3. Allgemeine Regeln am Arbeitsplatz

Erkennbares Problem: Es fehlt an einer «schönen» Systematik.
ISO 17799 ist eher eine Punktliste ohne tieferen Zusammenhang.

Communications and operations management

1. Zuständigkeiten für den sicheren Betrieb der Informationsverarbeitungseinrichtungen
2. Systemplanung
   - Ressourcenmanagement
   - Planung von Kapazitäten
   - Schaffung von Systemakzeptanz
3. Schutz vor fehlerhafter und böswilliger Software
4. «Housekeeping»
   - Backup
5. Netzmanagement
   - Verschlüsselung auf Übertragungsstrecken
   - Virtuelle Private Netze
6. Sicherer Umgang mit Medien
   - Löschung nicht mehr genutzter Medien (Wh. zu phys. Si.)
7. Informationsaustausch zwischen Unternehmen

Schlechte Struktur erkennbar:

einerseits sehr konkrete Empfehlungen, andererseits nur grobe Schlagworte

Access control

1. Access control policy
2. Mechanismen der Zugriffskontrolle
3. Verantwortlichkeiten der Nutzer
   - Passwortsicherheit
   - Verhalten beim Verlassen des Rechners
4. Entfernter Zugriff (über Rechnernetze)
5. Zugriffskontrolle auf Betriebssystemebene (eigentl. Zugangskontrolle)
6. Zugriffskontrolle auf Anwendungsebene
7. Protokollierung
8. Sicherheit beim mobile Computing und bei Telearbeit

Passt 8. zu den anderen 7 Abschnitten?
Standard zeigt hier seine eigenen Grenzen auf...

Systems development and maintenance

- Maßnahmen
  1. Definition von Sicherheitsanforderungen bereits beim Systemdesign
  2. Sicherheit in Anwendungssystemen
  3. Einsatz kryptographischer Verfahren
  4. Schutz von Systemdateien (z.B verwendete Bibliotheken)
  5. Sicherheit innerhalb des Entwicklungsprozesses

- adressiert die Entwicklung sicherer Systeme
  - betrifft lediglich Unternehmen, die selbst SW entwickeln
  - strukturierter SW-Entwicklungsprozess

Macht deutlich:
Sicherheit ist ein Querschnittsthema!

Business continuity management

- Verhindern von Unterbrechungen und Sicherstellung des laufenden Geschäftsbetriebs

  Maßnahmen

  1. Beschreibung des Prozesses
  2. Analyse
  3. Aufstellen eines business continuity plans
  4. Test

- Sicherheit wird nicht als Zustand, sondern als Prozess verstanden

Compliance

1. Übereinstimmung mit den gesetzlichen Rahmenbedingungen
   - Copyright, Softwarerecht
   - Datenschutz
   - Missbrauch, Strafverfolgung, ...

2. Prüfen, ob ergriffene Maßnahmen zur Informationssicherheit mit der Security Policy übereinstimmen
   - ggf. Änderungen vornehmen

3. Maßnahmen zur effektiven Systemüberprüfung
   - z.B. im Hinblick auf eine spätere Zertifizierung

Gliederungspunkte

1. Security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

Bewertung von ISO 17799

- Erreichbares Sicherheitsniveau
  - recht umfassender Maßnahmenkatalog
  - definiert größtenteils Standard-Sicherheitsmaßnahmen
  - für Hochsicherheit weiter gehende Maßnahmen erforderlich
  - jedoch: Management von Hochsicherheit wird durch Managementansatz unterstützt
- Aufwand für Umsetzung
  - hängt vom Organisationsgrad des Unternehmens ab
  - hoher Organisationsgrad — weniger Aufwand
  - Umsetzung der Maßnahmen kann durch Tools unterstützt werden

Vergleich GSHB — ISO 17799

	GSHB	ISO 17799
Einordnung	nicht-technisch bis technisch	nicht-technisch
Inhalt	Kataloge von Standardsicherheitsmaßnahmen für nahezu alle Bereiche des sicheren IT-Einsatzes	generische Sicherheitsmaßnahmen für nahezu alle Bereiche des sicheren IT-Einsatzes
Unternehmens-typen	Primär Serverbetreiber, Inhalteanbieter, Unternehmen als IT-Anwender	dito.
Unternehmens-größe	Behörden und Unternehmen aller Größen, sehr eingeschränkt Privatanwender	eher mittlere und größere Unternehmen

Vergleich GSHB — ISO 17799

	GSHB	ISO 17799
Ausführende Rollen im Unternehmen	Projektmanagement, Administratoren, IT-Leiter, IT-Sicherheitsbeauftragte	tendenziell höhere Management-Ebenen, aber auch IT-Sicherheitsbeauftragte und IT-Leiter
Aktualität	zweimal jährlich überarbeitet	vorgesehen
Ansatz	Bausteine beschreiben allgemeine und spezifische Maßnahmen	Top-Down, sehr generisch, daher wenig konkret
Erreichbares Sicherheits-niveau	Baseline Security (Grundschutz)	Grundschutz bis hin zur Unterstützung von Hochsicherheit

Vergleich GSHB — ISO 17799

	GSHB	ISO 17799
Umfang	ca. 2000 Seiten	71 Seiten
Aufwand und Kosten	mittel bis hoch	hoch bis sehr hoch
Zertifizierung	drei Stufen	möglich
Internationalität	engl. Version verfügbar, inzwischen auch Einsatz im Ausland	internationaler Standard

IT-Grundschutz-Zertifikat

- Seit 2002 in drei Ausbaustufen erhältlich
  - Stufe 1: IT-Grundschutz-Einstiegsstufe kann durch Selbsterklärung erfolgen
  - Stufe 2: IT-Grundschutz-Aufbaustufe ebenfalls durch Selbsterklärung erreichbar
  - Stufe 3: IT-Grundschutz-Zertifikat wird nur durch einen lizenzierten IT-Grundschutz-Auditor vergeben

    Mit jeder Stufe steigt die Zahl der Maßnahmen aus dem GSHB, die umgesetzt werden müssen, um die Stufe zu erreichen und damit auch der Grad der Sicherheit im Unternehmen.

  - Kann ergänzt werden um ISO 17799-Zertifikat