

# IS-Revision in der Verwaltung

Dr. Gerhard Weck  
INFODAS GmbH, Köln  
27. November 2009

## Inhalt

- Nationaler Plan zur Sicherung der Informationsinfrastrukturen (NPSI)
  - Umsetzungsplan KRITIS
  - Umsetzungsplan Bund
- Grundlagen der IS-Revision
  - Integration in den ISMS-Prozess
  - Leitfaden IS-Revision
  - Arten der IS-Revision
  - Ablauf der IS-Revision
  - Umfang einer IS-Revision
  - Prüfmethoden
- 27001- Audit versus IS-Revision



■ Adressat:

- Bundesverwaltung

■ Adressaten:

- Energie
- Transport / Verkehr
- Finanzwesen
- Behörden, Justiz, Verwaltung

■ Strategische Ziele zum Schutz der Informationsinfrastrukturen:

- **Prävention** – Informationsinfrastrukturen angemessen schützen
- **Reaktion** – Wirkungsvoll bei IT-Sicherheitsvorfällen handeln
- **Nachhaltigkeit** – Deutsche IT-Sicherheitskompetenz stärken – international Standards setzen

■ Realisierung in Kooperation zwischen Bund und Wirtschaft

■ Konkretisierung durch vorgegebene Umsetzungspläne

- UP KRITIS: Vorgaben für den Schutz kritischer Infrastrukturen, deren Funktionieren von IT abhängt
- UP Bund (VS-NfD): Vorgaben für die Etablierung von Mindeststandards zur IT-Sicherheit in der Bundesverwaltung

## Prävention – Aufbau angemessenen Schutzes

- Ziel 1: Bewusstsein schärfen über Risiken der IT-Nutzung
  - Sensibilisierung für und die Aufklärung über IT-Risiken
- Ziel 2: Einsatz sicherer IT-Produkte und –Systeme
  - Zertifizierung durch das BSI
  - Produktempfehlungen und technische Richtlinien zum Einsatz
- Ziel 3: Vertraulichkeit wahren
  - Verfügbarkeit innovativer, vertrauenswürdiger Kryptoprodukte
- Ziel 4: Gewährleisten umfassender Schutzvorkehrungen
  - Aktualität und wirksame Umsetzung der IT-Sicherheitskonzepte

## Prävention – Aufbau angemessenen Schutzes

- Ziel 5: Vorgabe von Rahmenbedingungen und Richtlinien
  - Empfehlungen und Leitfäden zur IT-Sicherheit
  - Leitlinien für Bereiche der Wirtschaft mit Anforderungen an ein besonderes Sicherheitsniveau
- Ziel 6: Abgestimmte Sicherheitsstrategien
  - Definition gemeinsamer Standards und abgestimmter Nutzungskonzepte
- Ziel 7: Nationale und internationale Gestaltung politischer Willensbildung
  - Zusammenarbeit auf nationaler und internationaler Ebene
  - Kooperation mit der europäischen IT-Sicherheitsbehörde ENISA), der NATO, der OECD, den UN, den G8 und auf internationaler Ebene

## Reaktion auf IT-Sicherheitsvorfälle – Wirksames und schnelles Handeln

- Ziel 8: Erkennen, Erfassen und Bewerten von Vorfällen
  - Krisenreaktionszentrum IT des Bundes im BSI
    - nationales Lage- und Analysezentrum
    - Sensornetz für IT-Sicherheitsvorfälle
    - Mitwirkung im internationalen „Watch-and-Warning“-Netzwerk
- Ziel 9: Informieren, Alarmieren und Warnen
  - zielgruppengerechte Informationen zu Bedrohungen und Risiken
  - Alarmierungs- und Warnsystem für IT-Krisenmanagement
- Ziel 10: Reagieren bei IT-Sicherheitsvorfällen
  - schnelle Reaktion auf schwerwiegende Vorfälle durch das Krisenreaktionszentrum IT des Bundes
  - vorbereitete Notfallpläne und klare Vorgehensweisen für die Bewältigung von IT-Sicherheitsvorfällen

## Nachhaltigkeit – IT-Sicherheits- kompetenz und Standards

- Ziel 11: Fördern vertrauenswürdiger und verlässlicher Informationstechnik
- Ziel 12: Ausbau nationaler IT-Sicherheitskompetenz
  - Förderung des Know-hows der deutschen IT-Sicherheitsdienstleistungsunternehmen
  - Erweiterung der Kompetenzen und Aufgaben des BSI
- Ziel 13: IT-Sicherheitskompetenz in Schule und Ausbildung
  - Entwicklung neuer Berufsbilder und neuer Ausbildungsgänge
- Ziel 14: Fördern von Forschung und Entwicklung
  - vor allem bzgl. des 7. Europäischen Forschungsrahmenprogramms
- Ziel 15: Internationale Kooperationen ausbauen und Standards setzen

- Aufgabe aller Bundesbehörden
  - Vorgaben für die Organisation
  - Erstellung IT-Sicherheitskonzepte
  - Umsetzung IT-Grundschutz
  - Regelmäßige Durchführung von IS-Revisionen
  - Fortbildung zur IT-Sicherheit
- Aufgabe des BSI
  - Erstellung eines Leitfadens zur IS-Revision
  - Festlegung eines einheitlichen Verfahrens
  - Dienstleistung „Durchführung von IS-Revisionen“, vorrangig für Sicherheitsbehörden
  - Dienstleistung „Kurzrevision“ für Behörden / Sicherheitsdienstleister

- Flächendeckender Mindeststandard für IT-Sicherheit in der Bundesverwaltung: IT-Grundschutz
  - BSI-Standards 100-1 und 100-2 sind Mindeststandard
  - BSI-Standard 100-3 gilt zusätzlich bei erhöhten Anforderungen
- Sicherheitsprozess erfordert regelmäßige Überprüfung der erreichten Sicherheit
  - Überprüfung der Maßnahmen der Informationssicherheit auf
    - wirksame Umsetzung
    - Vollständigkeit
    - Aktualität
    - Angemessenheit
  - Ziel ist die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit

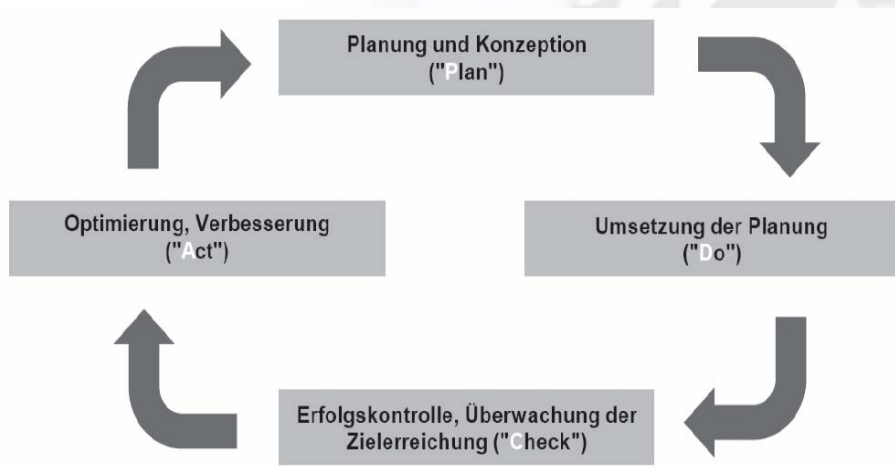
- Bestellung der Ressort-IT-Sicherheitsbeauftragten und der IT-Sicherheitsbeauftragten
- Anwendung der BSI-Standards 100-1 und 100-2
- Entwicklung und Fortschreibung eines dem jeweiligen Schutzbedarf angemessenen IT-Sicherheitskonzepts
- Regelmäßige IT-Sicherheitsrevisionen (alle 3 Jahre)
- Ziel: Nachweis des erreichten Sicherheitsniveaus durch ein ISO 27001 Zertifikat auf der Basis von IT-Grundschutz

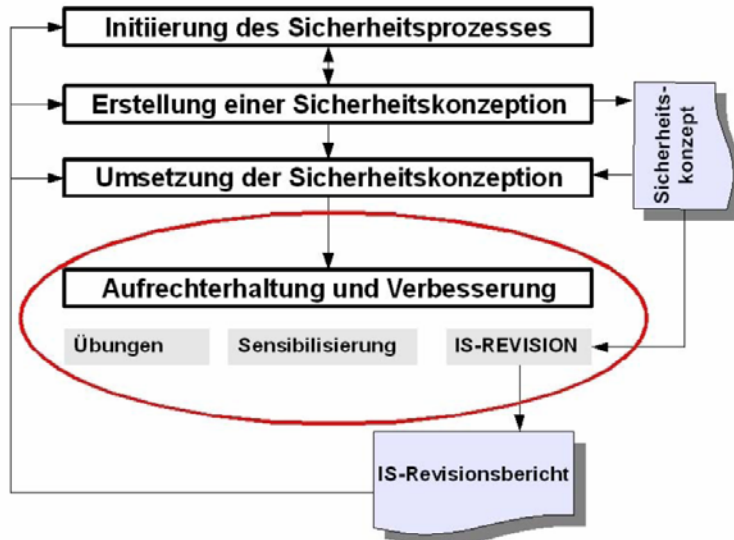
- Überprüfung
  - des IS-Prozesses
  - des Sicherheitskonzepts
  - der ergriffenen Maßnahmen
- Ergebnis
  - Übersicht über aktuelles Sicherheitsniveau
  - Hinweise auf Sicherheitsmängel / Verbesserungspotential
  - Hinweise auf Angemessenheit und Praxistauglichkeit der umgesetzten Maßnahmen
- Ziel
  - Optimierung des Sicherheitsprozesses
  - Steigerung der Informationssicherheit durch Behebung von Schwachstellen

# Grundlagen der IS-Revision



# Integration in den ISMS-Prozess





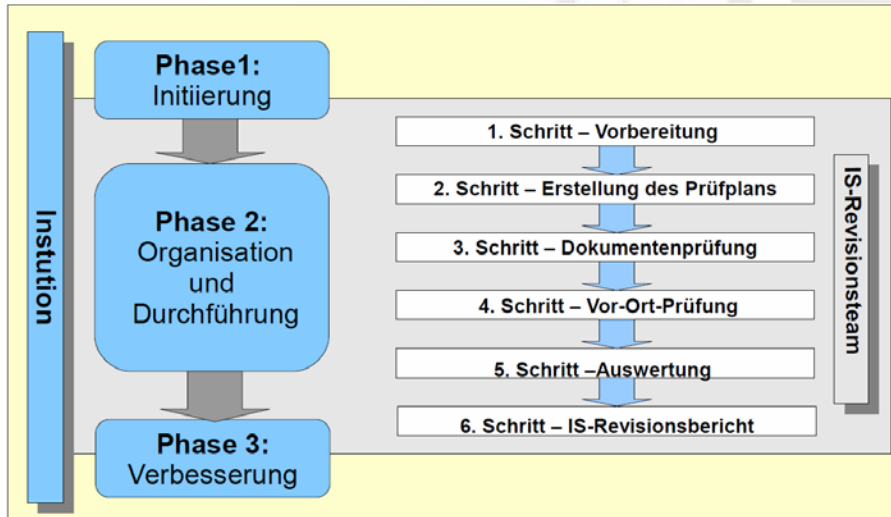
- Kapitel 1: Einleitung
- Kapitel 2: Einführung in die IS-Revision
- Kapitel 3: IS-Revision in der Institution
- Kapitel 4: Durchführung einer IS-Revision
- Kapitel 5: Hilfsmittel

[https://www.bsi.bund.de/DE/Themen/weitereThemen/ISRevision/Leitfaden/leitfaden\\_node.html](https://www.bsi.bund.de/DE/Themen/weitereThemen/ISRevision/Leitfaden/leitfaden_node.html)

oder unter „Sicherheitsberatung“

[https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/sicherheitsberatung\\_node.html](https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/sicherheitsberatung_node.html)

## Überblick über die IS-Revision



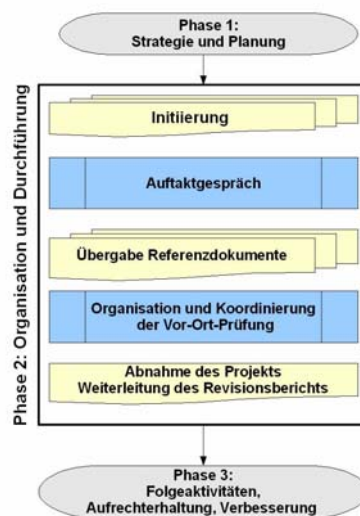
## Arten der IS-Revision

- IS-Querschnittsrevision
  - Pflicht nach UP Bund
  - IS-Basisrevision als Rückfallposition
    - kann durchgeführt werden, wenn Kriterien für IS-Querschnittsrevision nur z.T. erfüllt werden (z.B. fehlende Schutzbedarfsfeststellung / Modellierung)
- IS-Partialrevision
  - bei organisatorischen oder wesentlichen technischen Änderungen
- IS-Kurzrevision
  - Dienstleistung des BSI
  - z.B. bei Akkreditierung von IT-Sicherheitsdienstleistern

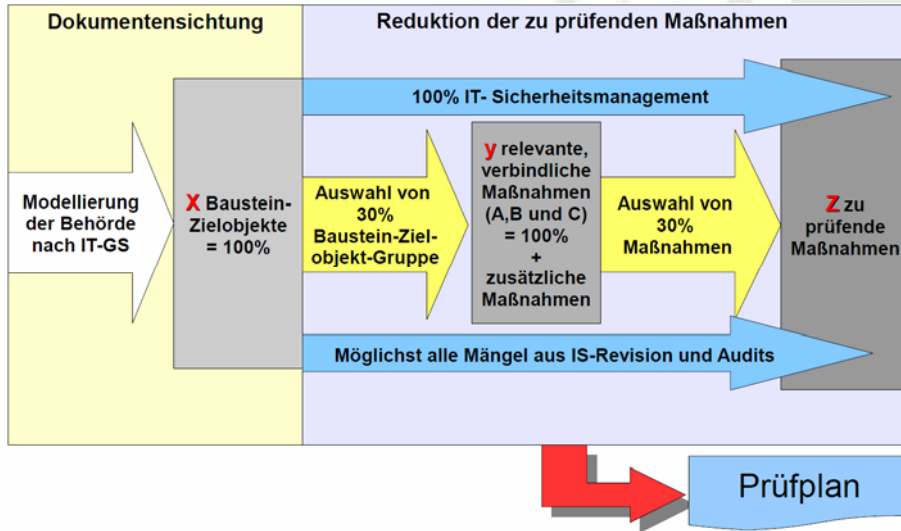
## Arten der IS-Revision

- IS-Querschnittsrevision – mindestens alle 3 Jahre
  - Prüfung nach UP Bund
  - Ganzheitlicher Ansatz, breites Prüfspektrum (alle Schichten des IT-Grundschutzes)
  - Gesamte Institution
  - stichprobenbasierte Prüfung
  - Voraussetzung: Netzplan und IT-Strukturanalyse nach Std. 100-2
- IS-Partialrevision – für kritische Geschäftsprozesse
  - Ggf. anlassbezogene Prüfung
  - Ganzheitlicher Ansatz, tiefes Prüfspektrum (nur von Änderungen betroffene Schichten)
  - Teil(e) einer Institution (IT-System, Abteilung, Verfahren, ...)
  - Vollständige oder stichprobenbasierte Prüfung

## Ablauf der IS-Revision



## Umfang einer IS-Revision



## Zu erwartender Aufwand

Aufwand in Personentagen		Größe der Institution		
		klein (bis 100 MA)	mittel (bis 500 MA)	groß (über 500 MA)
Komplexität	normal	30	50	60
	hoch	50	65	80
	sehr hoch	60	80	100

## Verteilung des Aufwands

Phase	Tätigkeit	Zeitanteile
Schritt 1	Vorbereitung der IS-Revision	5 %
Schritt 2	Erstellung des IS-Prüfplans	15 %
Schritt 3	Dokumentenprüfung	20 %
Schritt 4	Vor-Ort-Prüfung	35 %
Schritt 5	Nachbereitung der Vor-Ort-Prüfung	5 %
Schritt 6	Erstellung des IS-Revisionsberichts	20 %

## Prüfmethoden

- Mündliche Befragung (Interview)
- Inaugenscheinnahme von Systemen, Orten, Räumlichkeiten und Gegenständen
- Beobachtung (z. B. zufällige Wahrnehmungen im Rahmen der Vor-Ort-Prüfung)
- Aktenanalyse (hierzu gehören auch elektronische Daten)
- Technische Prüfung (z. B. Überprüfung von Alarmanlagen, Zutrittskontrollen, Anwendungen)
- Datenanalyse (z.B. Log-Files, Datenbank-Auswertung, etc.)
- Schriftliche Befragung (z.B. Fragebogen).

## Bewertung der Prüfergebnisse

Bewertung – Umsetzungsstatus (Schritt 1)	Bewertung – Sicherheitsmangel (Schritt 2)
Maßnahme ist nicht umgesetzt	Sicherheitsmangel oder schwerwiegender Sicherheitsmangel
Maßnahme ist teilweise umgesetzt	Sicherheitsmangel oder schwerwiegender Sicherheitsmangel
Maßnahme ist umgesetzt	Kein Sicherheitsmangel oder Sicherheitsempfehlung
Maßnahme ist entbehrlich	Kein Sicherheitsmangel

## Aufbewahrung und Archivierung der Prüfergebnisse

- IS-Revisionsbericht und zugrunde liegende Referenzdokumente müssen mindestens für die Dauer von 10 Jahren revisionssicher aufbewahrt werden
- Anforderungen an revisionssichere Archivierung:
  - Ordnungsmäßigkeit,
  - Vollständigkeit,
  - Schutz vor Veränderung und Verfälschung,
  - Sicherung vor Verlust,
  - Nutzung nur durch Berechtigte,
  - Einhaltung der Aufbewahrungsfristen,
  - Dokumentation des Verfahrens,
  - Prüfbarkeit sowie
  - Nachvollziehbarkeit

Muster für:

- ein IS-Revisionshandbuch
- einen IS-Prüfplan
- einen IS-Revisionsbericht
- usw.

[https://www.bsi.bund.de/DE/Themen/weitereThemen/ISRevision/Hilfsmittel/hilfsmittel\\_node.html](https://www.bsi.bund.de/DE/Themen/weitereThemen/ISRevision/Hilfsmittel/hilfsmittel_node.html)

## [B]-PRÜFUNGSRELEVANTE BAUSTEIN-ZIELOBEKTE

SCHICHT	BAUSTEIN	ZIELOBEKTE	BEGRÜNDUNG DER PRÜFUNGSRELEVANZ
Schicht 1:Übergeordnete Aspekte	B 1.0 IT-Sicherheitsmanagement	Gesamte Institution	Obligatorisch
	B 1.3 Notfallvorsorge-Konzept	Gesamte Institution	Hoher Schutzbedarf im Schutzziel Verfügbarkeit bei mehreren Verfahren
Schicht 2:Infrastruktur	B 2.1 Gebäude	GEB	Gebäude in dem sich S-RAUM-1 und Hauptverteiler befinden
	B 2.4 Serverraum	S-RAUM-1	Serverraum in dem die Verfahren mit dem höchsten Schutzbedarf betrieben werden
Schicht 3:IT-Systeme	B 3.101 Allgemeiner Server	IS	IS, AP und FILE sind Single Point of Failures (SPOF's) in Verfahren mit hohem Schutzbedarf
		AP	
	B 3.108 Windows Server 2003	IS	IS, AP und FILE sind SPOF's in Verfahren mit hohem Schutzbedarf
		AP	
B 3.201 Allgemeiner Client	WS	Standard-Client zur Bürokommunikation	
B 3.207 Client unter W2K	WS	Standard-Client zur Bürokommunikation	
Schicht 4:Netze	B 4.1 Heterogene Netze	NET-PROD	Produktionsnetz
Schicht 5:Anwendungen	B 5.2 Datenträgeraustausch	Gesamte Institution	Austausch von Datenbeständen aus Verfahren mit hohem Schutzbedarf im Schutzziel Vertraulichkeit (Organisationsuntersuchungen von Sicherheitsbehörden des Bundes) erfolgt teilweise über Datenträger

Anzahl Prüfungsrelevante Baustein-Zielobjekte:13 (ohne B 1.0)  
(42% der Baustein-Zielobjekte nach Modellierung)

# Prüfplan (Beispiel Maßnahmenauswahl)

## [C.2]-SCHICHT 2-INFRASTRUKTUR

### Begründung der Maßnahmenauswahl:

Bei der Auswahl der prüfungsrelevanten Maßnahmen der Bausteine in Schicht 2 (Infrastruktur) wurde ein besonderer Fokus auf Maßnahmen aus den Themenbereichen Brandschutz und Zutrittskontrolle gelegt, da im Jahr 2007 ein Brand im Lager (Raum E.05) des Hauptgebüdes (GEB) zu erheblichem Sachschaden führte und in den letzten Monaten vermehrt Diebstähle von Gegenständen in Büros durch die Mitarbeiter festgestellt wurden.

BAUSTEIN	ZIELOBJEKT	MASSNAHME
B 2.1 Gebäude (-15- A/B/C Maßnahmen)	GEB	M 1.3 – Angepasste Aufteilung der Stromkreise
		M 1.7 – Handfeuerlöscher
		M 1.8 – Raumbelegung unter Berücksichtigung von Brandlasten
		M 2.14 – Schlüsselverwaltung
		M 2.17 – Zutrittsregelung und -Kontrolle
B 2.4 Serverraum	S-RAUM-1	M 1.27 – Klimatisierung [Sicherheitsmangel IS-Revision 2007]

Anzahl Prüfungsrelevante Maßnahmen: 6  
(40% der A/B/C Maßnahmen des Baustein-Zielobjektes)

# Prüfplan (Beispiel Maßnahmenprüfung)

## [D.2]-SCHICHT 2-INFRASTRUKTUR

DATE: 01.12.2008 UHRZEIT: 1300-1600 Uhr  
REVISOR: Frau Musterfrau, Herr Mustermann/ANSPRECHPARTNER: Herr Raumbucher

BAUSTEIN	MASSNAHME	PRÜFMETHODE	STICHPROBE	UMSETZUNGS STATUS	ANMERKUNG
B 2.1 Gebäude	M 1.3 – Angepasste Aufteilung der Stromkreise	DOK / IAN	GEB [E.08]	Umgesetzt	Schriftlich in Sicherheitskonzept (SiKo) geregelt Stichprobe i.O. (Nutzlasten wurden angepasst)
	M 1.7 – Handfeuerlöscher	DOK / IAN	GEB [U.01]	Umgesetzt	Schriftlich in SiKo geregelt Stichprobe i.O.
	M 1.8 – Raumbelegung unter Berücksichtigung von Brandlasten	DOK / IAN	GEB [E.05 / E.06]	Umgesetzt	Wareneingangs- und Kartongelager in eigenem Brandabschnitt Stichprobe i.O.
	M 2.14 – Schlüsselverwaltung	DOK / IAN	GEB [Poststelle]	Umgesetzt	Schriftlich in Objektschutzkonzept geregelt Stichprobe i.O.
	M 2.17 – Zutrittsregelung und -Kontrolle	DOK / IAN	GEB	Teilweise umgesetzt	Schriftlich in Objektschutzkonzept geregelt Kontrolle erfolgt faktisch nicht, da Pförtner dauerhaft erkrankt ist und keine Vertretung
B 2.4 Serverraum	M 1.27 – Klimatisierung	IAN	S-RAUM-1	Teilweise umgesetzt	Regelungen existieren, werden gelebt, sind aber nicht dokumentiert  <i>Klimatisierung ist tatsächlicher Wärmelast im Raum plus Toleranzreserve angepasst. In Sommermonaten nun keine zusätzliche Klimatisierung über mobile Klimageräte mehr notwendig.</i>

## 27001- Audit versus IS-Revision

### 27001-Audit

- IT-Grundschutz umgesetzt
- definierter Informationsverbund
- 27001 Auditoren auf der Basis von IT-Grundschutz
- festgelegtes Prüfschema stichprobenartig die vollständige Umsetzung der Maßnahmen überprüfen
- „K.O.-Prüfung“
- Erteilung 27001-Zertifikat

### IS-Revision

- In der Umsetzungsphase IT-Grundschutz
- ganze Behörde
- unabhängige Revisoren (anerkannte Dienstleister)
- risikoorientierter Prüfauftrag
- Optimierung der Informationssicherheit, Hinweise für die Verbesserung

## IS-Revision in der Verwaltung

Dr. Gerhard Weck  
INFODAS GmbH, Köln  
27. November 2009