Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

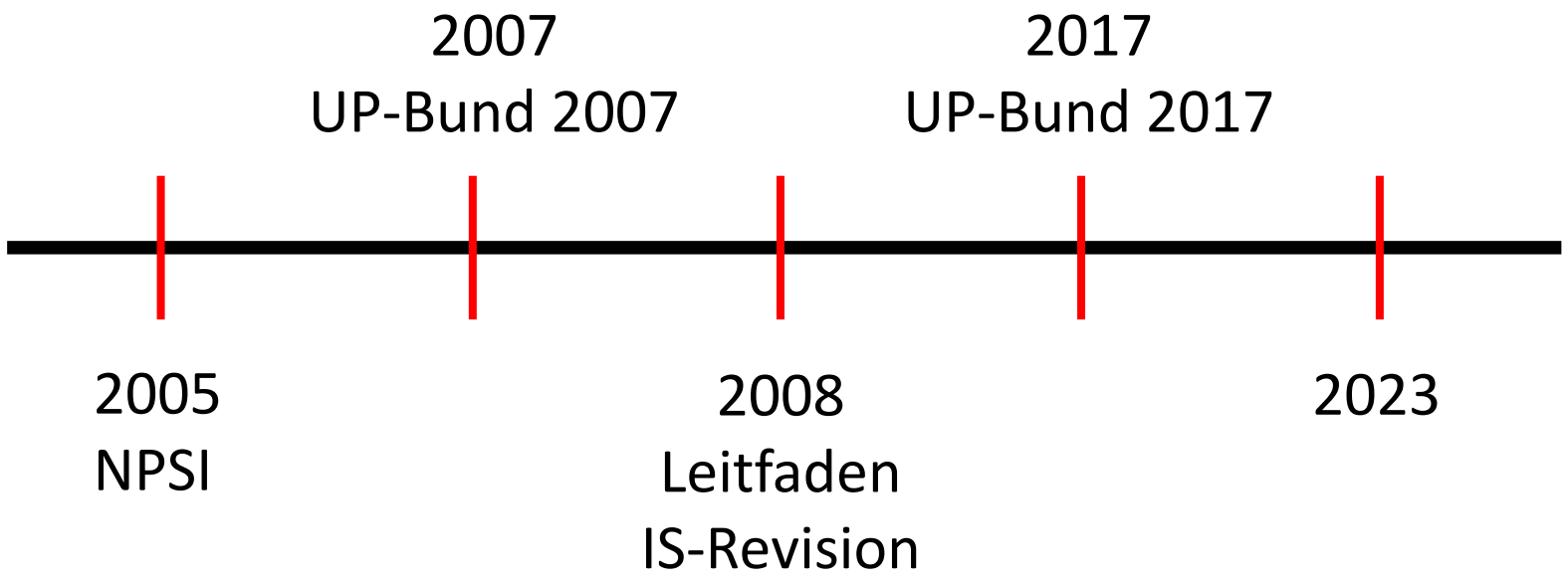
15 Jahre IS-Revision in der Bundesverwaltung

Erfahrungsbericht und Ausblick

Matthias Becker, Abteilung OC – Operative Cyber-Sicherheit

ISACA Focus Event 6.Juli 2023

Historie - Zeitstrahl



NPSI (2005)

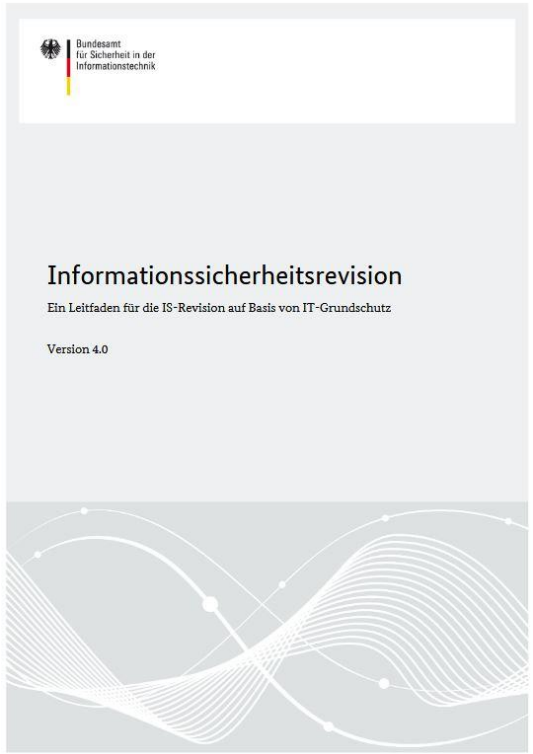

Nationaler Plan
zum Schutz der
Informationsinfrastrukturen
Nationaler Plan
Umsetzungsplan Bund
Nationaler Plan
Umsetzungsplan KRITIS

Umsetzungsplan Bund 2007 (VS-NfD eingestuft)

Auftrag an BSI zur Erarbeitung inhaltlicher und prozeduraler Empfehlungen zur Durchführung von regelmäßigen IT-Sicherheitsrevisionen.

Erstveröffentlichung im September 2008

Leitfaden IS-Revision



Festschreibung des Revisionszyklus auf **max. 3 Jahre**

Leitfaden und Hilfsmittel auf Webseite des BSI

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/ISRevision/Leitfaden/leitfaden_node.html

IT-Grundschutz Kompendium mit Grundschutzbaustein DER.3.2: “Revisionen auf Basis des Leitfadens IS-Revision”

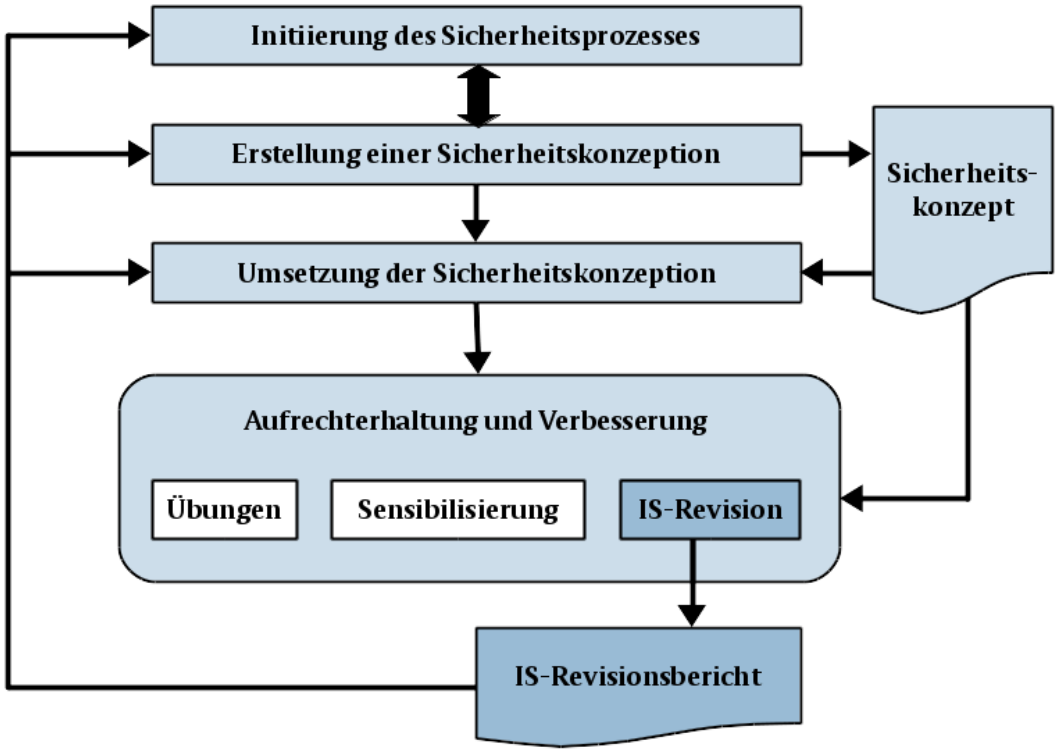
Umsetzungsplan Bund 2017

Evaluierung der Informationssicherheit

Zur Überprüfung der Informationssicherheitsmaßnahmen führen Einrichtungen in **regelmäßigen Abständen** sowie anlassbezogen geeignete Prüfungen z.B. in Form von Audits, Reifegradprüfungen, Revisionen oder Penetrationstests durch.

Bei der Durchführung von IS-Revisionen sind die Regelungen aus dem **Leitfaden des BSI für die IS-Revision** auf der Basis des IT-Grundschutzes zu beachten.

IS-Revision im Sicherheitsprozess



Revision vs. Audit

IS-Revision	ISO 27001-Audit
Bereits in Umsetzungsphase des IT-Grundschutzes möglich	IT-Grundschutz umgesetzt
ganze Behörde	definierter Informationsverbund
unabhängige Revisoren (anerkannte Dienstleister)	27001 Auditoren auf der Basis von IT-Grundschutz
risikoorientierter Prüfauftrag	festgelegtes Prüfschema, stichprobenartig, vollständige Umsetzung, „K.O.-Prüfung“
Optimierung der Informationssicherheit, Hinweise für die Verbesserung	Erteilung 27001-Zertifikat

Arten von IS-Revisionen

IS-Querschnittsrevision
das „Folgeverfahren“
Prüfung der gesamten Institution nach UP Bund 2017
auf Basis von IT-Grundschutz

IS-Partialrevision
für „Spezialfälle“
Vollständige oder stichprobenbasierte Prüfung
eines Teiles der Institution

IS-Kurzrevision
das etablierte „Einstiegsverfahren“
Überblick über den Sicherheitsstatus der Institution

Eckpunkte der IS-Kurzrevision

Ziel: Einschätzung

des Informationssicherheitsstatus

des Informationssicherheitsprozesses

Voraussetzungen

Keine

In jedem Stadium durchführbar

Wenig Aufwand

geringer Zeitaufwand

wenig Personal

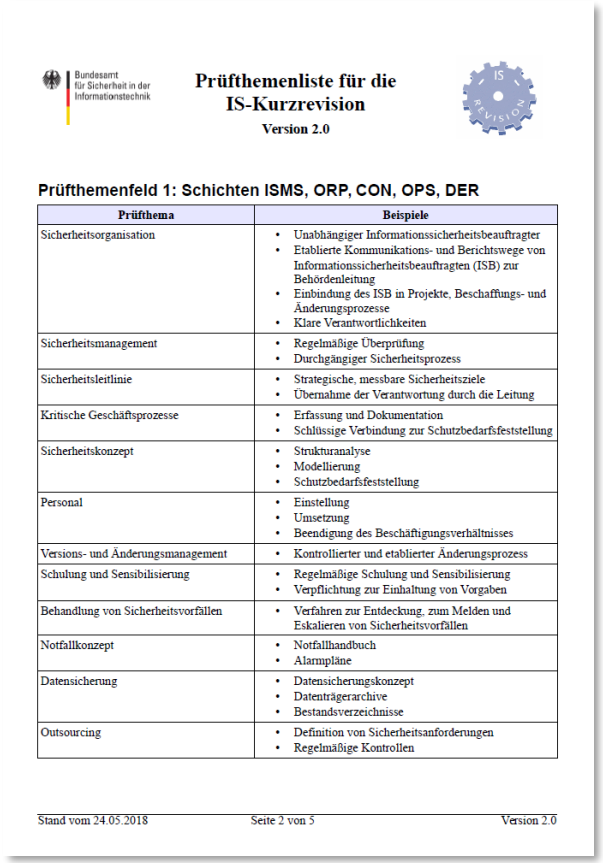
geringer Berichtsaufwand

Prüfinstrument

Prüfthemen (verbindliche Prüfthemenliste)

nicht anforderungsorientiert (und nicht maßnahmenorientiert)

Prüfthemenliste für die IS-Kurzrevision



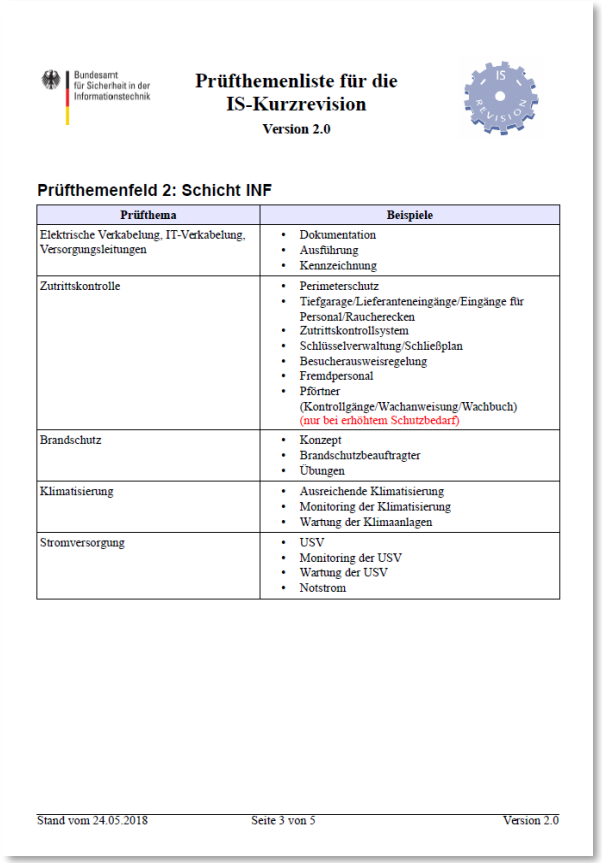
Bundesamt für Sicherheit in der Informationstechnik

Prüfthemenliste für die IS-Kurzrevision
Version 2.0

Prüfthemenfeld 1: Schichten ISMS, ORP, CON, OPS, DER

Prüfthema	Beispiele
Sicherheitsorganisation	• Unabhängiger Informationssicherheitsbeauftragter • Etablierte Kommunikations- und Berichtswege von Informationssicherheitsbeauftragten (ISB) zur Behördenleitung • Einbindung des ISB in Projekte, Beschaffungs- und Änderungsprozesse • Klare Verantwortlichkeiten
Sicherheitsmanagement	• Regelmäßige Überprüfung • Durchgängiger Sicherheitsprozess
Sicherheitsleitlinie	• Strategische, messbare Sicherheitsziele • Übernahme der Verantwortung durch die Leitung
Kritische Geschäftsprozesse	• Erfassung und Dokumentation • Schlüssige Verbindung zur Schutzbedarfsfeststellung
Sicherheitskonzept	• Strukturanalyse • Modellierung • Schutzbedarfsfeststellung
Personal	• Einstellung • Umsetzung • Beendigung des Beschäftigungsverhältnisses
Versions- und Änderungsmanagement	• Kontrollierter und etablierter Änderungsprozess
Schulung und Sensibilisierung	• Regelmäßige Schulung und Sensibilisierung • Verpflichtung zur Einhaltung von Vorgaben
Behandlung von Sicherheitsvorfällen	• Verfahren zur Entdeckung, zum Melden und Eskalieren von Sicherheitsvorfällen
Notfallkonzept	• Notfallhandbuch • Alarmpläne
Datensicherung	• Datensicherungskonzept • Datenträgerarchive • Bestandsverzeichnisse
Outsourcing	• Definition von Sicherheitsanforderungen • Regelmäßige Kontrollen

Stand vom 24.05.2018 Seite 2 von 5 Version 2.0



Bundesamt für Sicherheit in der Informationstechnik

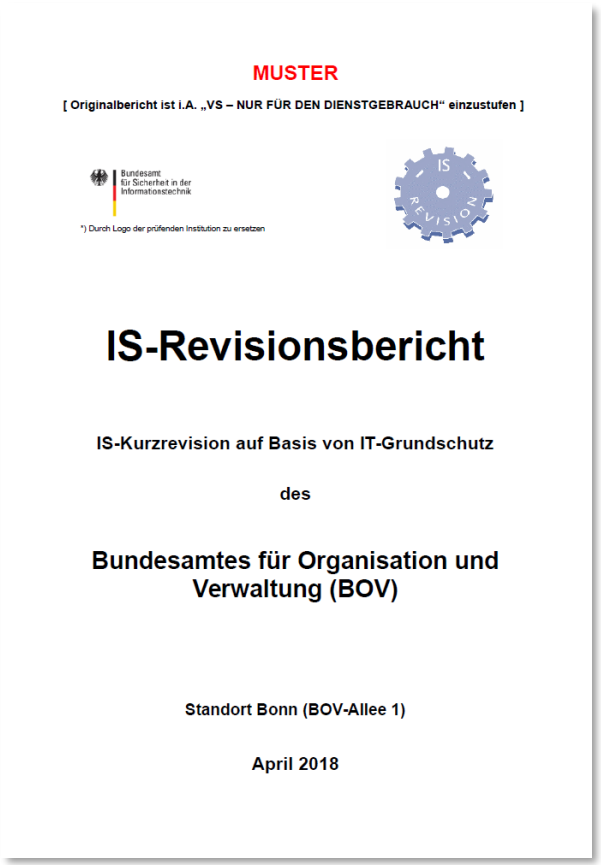
Prüfthemenliste für die IS-Kurzrevision
Version 2.0

Prüfthemenfeld 2: Schicht INF

Prüfthema	Beispiele
Elektrische Verkabelung, IT-Verkabelung, Versorgungsleitungen	• Dokumentation • Ausführung • Kennzeichnung
Zutrittskontrolle	• Perimeterschutz • Tiefgarage/Lieferanteneingänge/Eingänge für Personal/Raucherecken • Zutrittskontrollsystem • Schlüsselverwaltung/Schließplan • Besucherausweisregelung • Fremdpersonal • Pförtner (Kontrollgänge/Wachanweisung/Wachbuch) (nur bei erhöhtem Schutzbedarf)
Brandschutz	• Konzept • Brandschutzbeauftragter • Übungen
Klimatisierung	• Ausreichende Klimatisierung • Monitoring der Klimatisierung • Wartung der Klimaanlagen
Stromversorgung	• USV • Monitoring der USV • Wartung der USV • Notstrom

Stand vom 24.05.2018 Seite 3 von 5 Version 2.0

Berichtsformat für die IS-Kurzrevision



MUSTER

[Originalbericht ist i.A. „VS – NUR FÜR DEN DIENSTGEBRAUCH“ einzustufen]

Bundesamt für Sicherheit in der Informationstechnik

*) Durch Logo der prüfenden Institution zu ersetzen

IS-Revisionsbericht

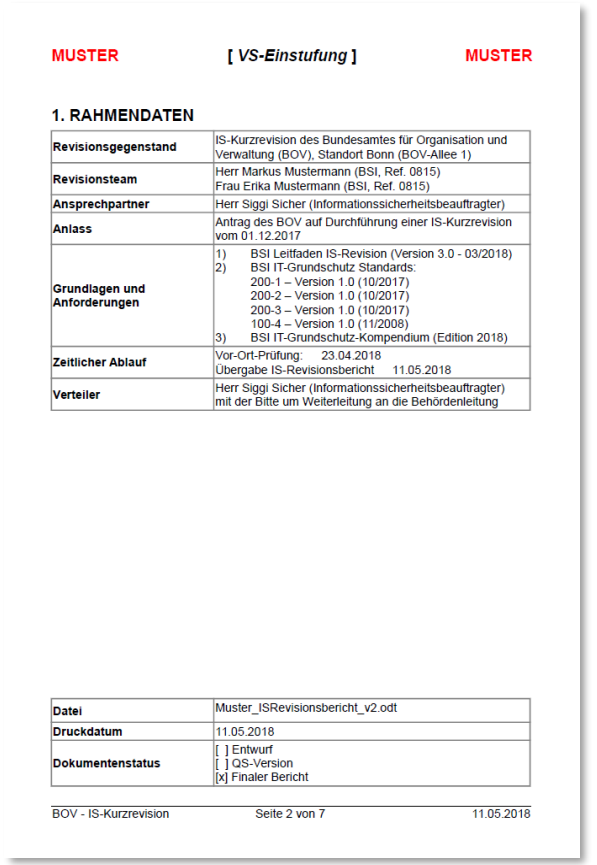
IS-Kurzrevision auf Basis von IT-Grundschutz

des

Bundesamtes für Organisation und Verwaltung (BOV)

Standort Bonn (BOV-Allee 1)

April 2018



MUSTER [*VS-Einstufung*] MUSTER

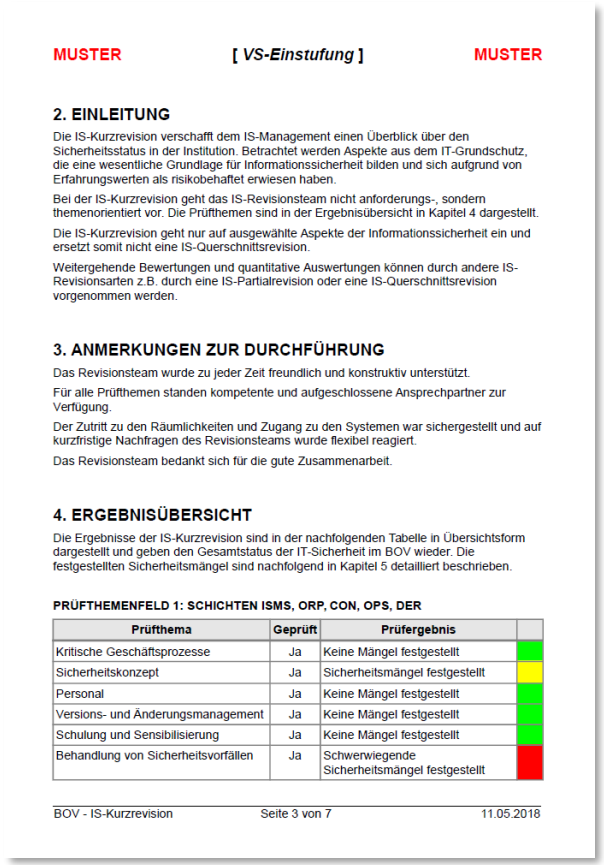
1. RAHMENDATEN

Revisionsgegenstand	IS-Kurzrevision des Bundesamtes für Organisation und Verwaltung (BOV), Standort Bonn (BOV-Allee 1)
Revisionsteam	Herr Markus Mustermann (BSI, Ref. 0815) Frau Erika Mustermann (BSI, Ref. 0815)
Ansprechpartner	Herr Siggi Sicher (Informationssicherheitsbeauftragter)
Anlass	Antrag des BOV auf Durchführung einer IS-Kurzrevision vom 01.12.2017
Grundlagen und Anforderungen	1) BSI Leitfaden IS-Revision (Version 3.0 - 03/2018) 2) BSI IT-Grundschutz Standards: 200-1 – Version 1.0 (10/2017) 200-2 – Version 1.0 (10/2017) 200-3 – Version 1.0 (10/2017) 100-4 – Version 1.0 (11/2008) 3) BSI IT-Grundschutz-Kompendium (Edition 2018)
Zeitlicher Ablauf	Vor-Ort-Prüfung: 23.04.2018 Übergabe IS-Revisionsbericht 11.05.2018
Verteiler	Herr Siggi Sicher (Informationssicherheitsbeauftragter) mit der Bitte um Weiterleitung an die Behördenleitung

Datei	Muster_ISRevisionsbericht_v2.odt
Druckdatum	11.05.2018
Dokumentenstatus	[ ] Entwurf [ ] QS-Version [x] Finaler Bericht

BOV - IS-Kurzrevision Seite 2 von 7 11.05.2018

Berichtsformat für die IS-Kurzrevision



MUSTER [*VS-Einstufung*] MUSTER

2. EINLEITUNG

Die IS-Kurzrevision verschafft dem IS-Management einen Überblick über den Sicherheitsstatus in der Institution. Betrachtet werden Aspekte aus dem IT-Grundschutz, die eine wesentliche Grundlage für Informationssicherheit bilden und sich aufgrund von Erfahrungswerten als risikobehaftet erwiesen haben.

Bei der IS-Kurzrevision geht das IS-Revisionsteam nicht anforderungs-, sondern themenorientiert vor. Die Prüfthemen sind in der Ergebnisübersicht in Kapitel 4 dargestellt.

Die IS-Kurzrevision geht nur auf ausgewählte Aspekte der Informationssicherheit ein und ersetzt somit nicht eine IS-Querschnittsrevision.

Weitergehende Bewertungen und quantitative Auswertungen können durch andere IS-Revisionsarten z.B. durch eine IS-Partialrevision oder eine IS-Querschnittsrevision vorgenommen werden.

3. ANMERKUNGEN ZUR DURCHFÜHRUNG

Das Revisionsteam wurde zu jeder Zeit freundlich und konstruktiv unterstützt.

Für alle Prüfthemen standen kompetente und aufgeschlossene Ansprechpartner zur Verfügung.

Der Zutritt zu den Räumlichkeiten und Zugang zu den Systemen war sichergestellt und auf kurzfristige Nachfragen des Revisionsteams wurde flexibel reagiert.

Das Revisionsteam bedankt sich für die gute Zusammenarbeit.

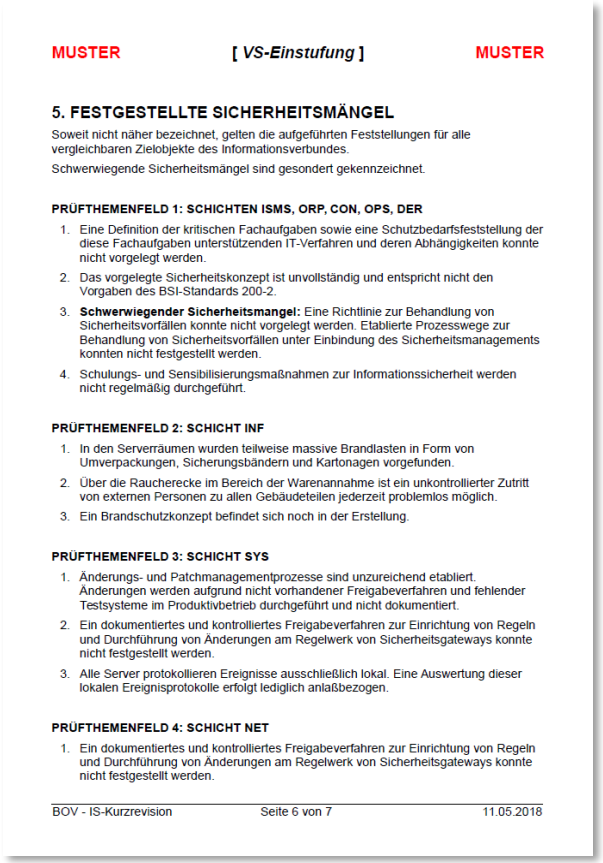
4. ERGEBNISÜBERSICHT

Die Ergebnisse der IS-Kurzrevision sind in der nachfolgenden Tabelle in Übersichtsform dargestellt und geben den Gesamtstatus der IT-Sicherheit im BOV wieder. Die festgestellten Sicherheitsmängel sind nachfolgend in Kapitel 5 detailliert beschrieben.

PRÜFTHEMENFELD 1: SCHICHTEN ISMS, ORP, CON, OPS, DER

Prüfthema	Geprüft	Prüfergebnis	
Kritische Geschäftsprozesse	Ja	Keine Mängel festgestellt	
Sicherheitskonzept	Ja	Sicherheitsmängel festgestellt	
Personal	Ja	Keine Mängel festgestellt	
Versions- und Änderungsmanagement	Ja	Keine Mängel festgestellt	
Schulung und Sensibilisierung	Ja	Keine Mängel festgestellt	
Behandlung von Sicherheitsvorfällen	Ja	Schwerwiegende Sicherheitsmängel festgestellt	

BOV - IS-Kurzrevision Seite 3 von 7 11.05.2018



MUSTER [*VS-Einstufung*] MUSTER

5. FESTGESTELLTE SICHERHEITSMÄNGEL

Soweit nicht näher bezeichnet, gelten die aufgeführten Feststellungen für alle vergleichbaren Zielobjekte des Informationsverbundes.

Schwerwiegende Sicherheitsmängel sind gesondert gekennzeichnet.

PRÜFTHEMENFELD 1: SCHICHTEN ISMS, ORP, CON, OPS, DER

1. Eine Definition der kritischen Fachaufgaben sowie eine Schutzbedarfsfeststellung der diese Fachaufgaben unterstützenden IT-Verfahren und deren Abhängigkeiten konnte nicht vorgelegt werden.
2. Das vorgelegte Sicherheitskonzept ist unvollständig und entspricht nicht den Vorgaben des BSI-Standards 200-2.
3. **Schwerwiegender Sicherheitsmangel:** Eine Richtlinie zur Behandlung von Sicherheitsvorfällen konnte nicht vorgelegt werden. Etablierte Prozesswege zur Behandlung von Sicherheitsvorfällen unter Einbindung des Sicherheitsmanagements konnten nicht festgestellt werden.
4. Schulungs- und Sensibilisierungsmaßnahmen zur Informationssicherheit werden nicht regelmäßig durchgeführt.

PRÜFTHEMENFELD 2: SCHICHT INF

1. In den Serverräumen wurden teilweise massive Brandlasten in Form von Umverpackungen, Sicherungsbändern und Kartonagen vorgefunden.
2. Über die Raucherecke im Bereich der Warenannahme ist ein unkontrollierter Zutritt von externen Personen zu allen Gebäudeteilen jederzeit problemlos möglich.
3. Ein Brandschutzkonzept befindet sich noch in der Erstellung.

PRÜFTHEMENFELD 3: SCHICHT SYS

1. Änderungs- und Patchmanagementprozesse sind unzureichend etabliert. Änderungen werden aufgrund nicht vorhandener Freigabeverfahren und fehlender Testsysteme im Produktivbetrieb durchgeführt und nicht dokumentiert.
2. Ein dokumentiertes und kontrolliertes Freigabeverfahren zur Einrichtung von Regeln und Durchführung von Änderungen am Regelwerk von Sicherheitsgateways konnte nicht festgestellt werden.
3. Alle Server protokollieren Ereignisse ausschließlich lokal. Eine Auswertung dieser lokalen Ereignisprotokolle erfolgt lediglich anlaßbezogen.

PRÜFTHEMENFELD 4: SCHICHT NET

1. Ein dokumentiertes und kontrolliertes Freigabeverfahren zur Einrichtung von Regeln und Durchführung von Änderungen am Regelwerk von Sicherheitsgateways konnte nicht festgestellt werden.

BOV - IS-Kurzrevision Seite 6 von 7 11.05.2018

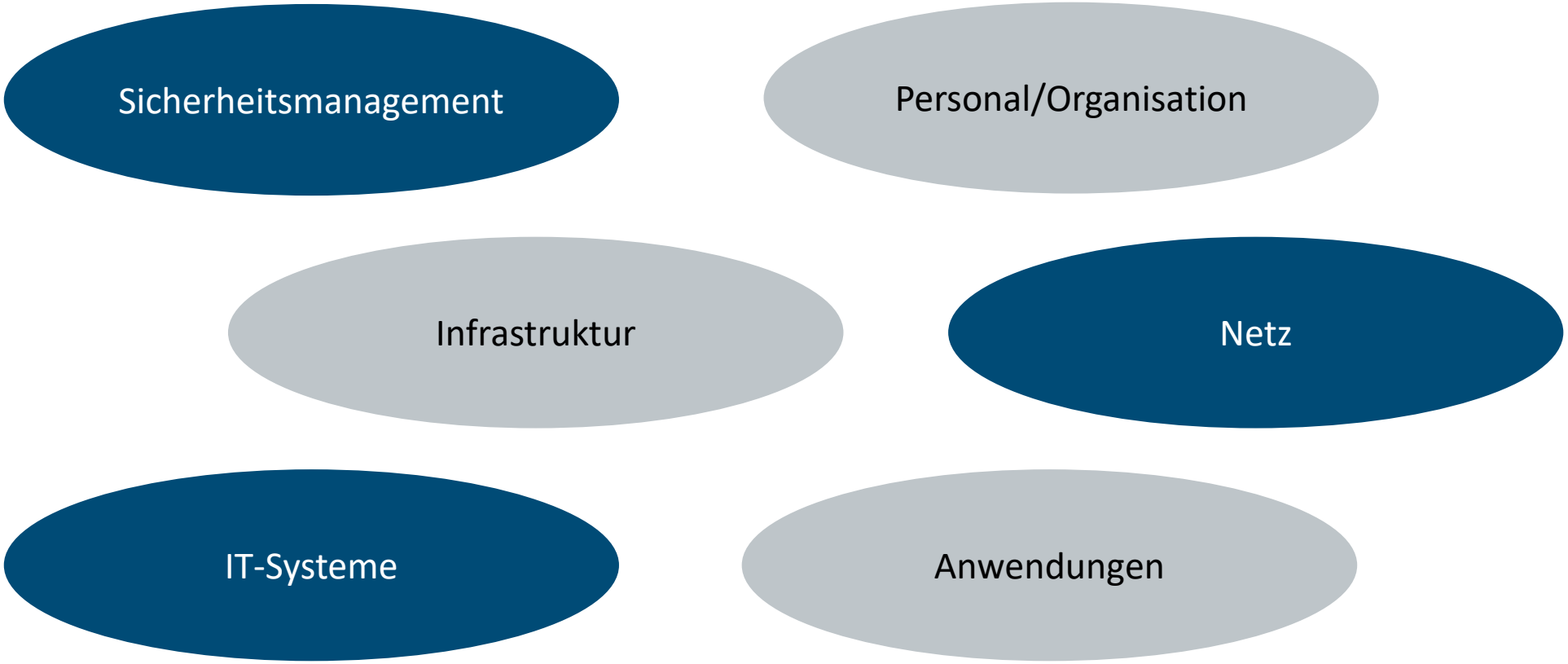
Erfahrungen bei der Vorbereitung

- ✓Gesamte Institution im Fokus behalten
- ✓Vorbereitungszeit maximal ein Tag (2 Personen)
- ✓Alle verfügbaren Unterlagen (kurz) sichten
- ✓Ablaufplan muss vor der Durchführung abgestimmt sein
- ✓Auftrag zur IS-Kurzrevision unbedingt aus Leitungsebene
- ✓Einbindung Personalrat/Betriebsrat/bDSB beachten

Erfahrungen bei der Durchführung

- ✓ Ablauf der Prüfung erläutern, Prinzip des „Hands Off“ erläutern
- ✓ Ablaufplan den aktuellen Gegebenheiten anpassen (stehen alle Ansprechpartner zur Verfügung?)
- ✓ Rückblick auf den Ablauf der Vor-Ort-Prüfung (Behinderungen?)
- ✓ Schwerwiegende Mängel erläutern (sofort abzustellen)
- ✓ Ansprechpartner auf reinen Mängelbericht vorbereiten
- ✓ Erläuterung des weiteren Ablaufs der Berichterstellung (QS-Version, Abstimmung Übertragungsweg)

Häufig festgestellte Mängel



Erfahrungen der letzten 15 Jahre - Zusammenfassung

- ✓IS-Kurzrevision hat sich als mittlerweile alleinige Prüfungsart etabliert
- ✓Prüfumfang, Prüftiefe und Prüfmethodik haben sich bewährt
- ✓IS-Kurzrevision wird auch bei Zertifizierung/Re-Zertifizierung von IT-Sicherheitsdienstleistern genutzt
- ✓Vorgehensweise der IS-Kurzrevision auf Überwachungsaudits im Rahmen von Zertifizierungen von ISO27001 auf der Basis von IT-Grundschutz übertragen
- ✓Vorgehensweise der IS-Kurzrevision auf §8a Prüfungen nach IT-SiG übertragen
- ✓Während Corona erfolgreiche Portierung der IS-Kurzrevision auf Online-Format

BSI-Gesetz – IT-SiG 2.0 (Mai, 2021)

Ausblick

„ (1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren“ .

Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI•

Kontakt

Matthias Becker

Referat OC34 – Penetrationstests und IS-Revision

matthias.becker@bsi.bund.de

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Godesberger Allee 185-189

53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik