Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision

- Einleitung
- Maßnahmen
  - Maßnahmen zum Baustein DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision
- Weiterführende Informationen
  - Wissenswertes
  - Quellenverweise

1. Einleitung

Eine besondere Form der Revision ist die Informationssicherheitsrevision (IS-Revision) auf Basis des Leitfadens für IS-Revision. Der Leitfaden für IS-Revision (siehe [BSI_REVISION]) ist ein vom BSI erstelltes Dokument, das verschiedene Arten der IS-Revision beschreibt. Bundesbehörden sind durch den "Umsetzungsplan Bund 2017, Leitlinie für Informationssicherheit in der Bundesverwaltung" (siehe [UPB]) verpflichtet, IS-Revisionen auf Basis des Leitfadens durchzuführen. Andere Institutionen können, anstelle einer gewöhnlichen IT-Revision, ebenfalls IS-Revisionen zur Überprüfung ihres ISMS durchführen.

Die IS-Revision auf Basis des Leitfadens für IS-Revision zeichnet sich besonders durch ihren ganzheitlichen Ansatz aus. Das bedeutet, dass vom Aufbau einer Informationssicherheitsorganisation über Personalaspekte bis hin zur Konfiguration von IT-Systemen und Anwendungen alle Ebenen eines ISMS geprüft werden. Dabei werden die Wirtschaftlichkeit und Ordnungsmäßigkeit, die bei klassischen IT-Revisionen im Vordergrund stehen, nur nachrangig betrachtet. Die Informationssicherheit, einschließlich der Angemessenheit der Sicherheitsmaßnahmen, ist somit das wesentliche Kriterium, dessen Prüfung im Leitfaden für IS-Revision beschrieben wird.

Die Hauptaufgabe der IS-Revision ist es, die Leitung der Institution, das IS-Management-Team und insbesondere den Informationssicherheitsbeauftragten (ISB) dabei zu unterstützen, die Informationssicherheit umzusetzen und zu optimieren.

Der Leitfaden für IS-Revision unterscheidet zwischen IS-Kurzrevision, IS-Querschnittsrevision und IT-Partialrevision:

- Die IS-Kurzrevision ist der Einstieg in das regelmäßige Revisionsverfahren und kann bereits am Anfang des Sicherheitsprozesses durchgeführt werden. Es bestehen keine Voraussetzungen für die geprüfte Institution.
- Ist der Sicherheitsprozess weiter fortgeschritten und sind die meisten IT-Grundschutz-Anforderungen erfüllt, kann eine IS-Querschnittsrevision durchgeführt werden. Die IS-Querschnittsrevision hat einen ganzheitlichen Ansatz und ein breites Prüfspektrum. Bei einer IS-Querschnittsrevision werden alle Schichten des IT-Grundschutzes anhand von Stichproben geprüft. Prüfgegenstand ist immer die gesamte Institution.
- Eine IS-Partialrevision beschränkt sich auf einen speziellen Ausschnitt der Institution und wird bei Bedarf zum Beispiel durch das IS-Management-Team angestoßen. Die Prüftiefe kann hier wesentlich größer sein als bei der IS-Querschnittsrevision.

Hinweis: Die Vorschriften des Geheimschutzes und der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA, siehe [VSA]) bleiben unberührt und gelten unabhängig von den Anforderungen dieses Bausteins.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision

DER.3.2.M1 Benennung von Verantwortlichen für die IS-Revision (B)

Die Institution muss einen Verantwortlichen für die IS-Revision benennen. Umsetzungshinweise, die beschreiben, worauf bei der Auswahl geachtet werden sollte, sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 3.1) beschrieben.

DER.3.2.M2 Erstellung eines IS-Revisionshandbuches (B)

Worauf beim Erstellen eines IS-Revisionshandbuches zu achten ist, wird in den Umsetzungshinweisen im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 3.1) beschrieben.

DER.3.2.M3 Definition der Prüfungsgrundlage (B)

Für Bundesbehörden sind als zusätzliche Prüfungsgrundlagen die Aussagen des UP Bund 2017 verbindlich (siehe [UPB], Kapitel 2 - Grundsätze). Es sollte mit den Prüfungsgrundlagen auch ein einheitliches Bewertungsschema festgelegt werden. Nähere Gestaltungsmöglichkeiten sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.1 und 4.4.1) beschrieben.

DER.3.2.M4 Erstellung einer Planung für die IS-Revision (B)

IS-Revisionen müssen regelmäßig und geplant durchgeführt werden. Umsetzungshinweise zur Planung von IS-Revisionen sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 3.2) beschrieben.

DER.3.2.M5 Auswahl eines geeigneten IS-Revisionsteams (B)

Ein IS-Revisionsteam muss unabhängig und objektiv sein. Außerdem müssen seine Mitglieder fachlich geeignet sein, um Sicherheitsanforderungen angemessen zu prüfen. Umsetzungshinweise, die beschreiben, wie ein IS-Revisionsteam ausgewählt werden kann, sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 2.4, 2.5 und 3.3) zu finden.

DER.3.2.M6 Vorbereitung einer IS-Revision (B)

Eine IS-Revision muss von der Leitung der Institution initiiert werden. Bei der anschließenden Vorbereitung sind eine Reihe von Dokumenten bereitzustellen. Nähere Angaben sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.2) zu finden.

DER.3.2.M7 Durchführung einer IS-Revision (B)

Bei einer IS-Revision wird sowohl eine Dokumentenprüfung als auch eine Vor-Ort-Prüfung durchgeführt. Umsetzungshinweise zur Durchführung einer IS-Revision sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.1.1 und 4.4.2) beschrieben.

DER.3.2.M8 Aufbewahrung von IS-Revisionsberichten (B)

Der Umgang mit IS-Revisionsberichten und die Aufbewahrung von IS-Revisionsberichten sind in den Umsetzungshinweisen im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.5) beschrieben.

DER.3.2.M9 Integration in den Informationssicherheitsprozess (S)

IS-Revisionen sollten fest im ISMS verankert sein. Wie dies sichergestellt werden kann, ist in den Umsetzungshinweisen im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 2.2) ausgeführt.

DER.3.2.M10 Kommunikationsabsprache (S)

Der Schutz von ausgetauschten Informationen zwischen der Institution und dem IS-Revisionsteam ist von elementarer Bedeutung. Wie dieser Schutz sichergestellt werden kann, kann den Umsetzungshinweisen im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.5, Abschnitt Eröffnungsgespräch) entnommen werden.

DER.3.2.M11 Durchführung eines Auftaktgesprächs für eine IS-Querschnittsrevision (S)

Zu Beginn des Verfahrens werden in einem Auftaktgespräch wesentliche Rahmenbedingungen der IS-Revision zwischen Institution und IS-Revisionsteam abgestimmt. Umsetzungshinweise, aus denen hervorgeht, wie ein solches Auftaktgespräch geführt werden kann, sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.2) beschrieben.

DER.3.2.M12 Erstellung eines Prüfplans (S)

Im Prüfplan wird festgehalten, welche IT-Grundschutz-Anforderungen während der IS-Revision geprüft werden. Das BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.3) beschreibt, wie ein Prüfplan erstellt werden kann.

DER.3.2.M13 Sichtung und Prüfung der Dokumente (S)

Die Dokumentenprüfung ist fester Bestandteil jeder IS-Revision. Worauf bei der Dokumentenprüfung geachtet werden sollte, ist im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.3 und 4.2.4) beschrieben.

DER.3.2.M14 Auswahl der Zielobjekte und der zu prüfenden Anforderungen (S)

Bei den anforderungsbasierten IS-Revisionsarten ist die Auswahl der zu prüfenden Anforderungen ein zentraler Punkt der IS-Revision. Die genaue Vorgehensweise bei der Auswahl zu prüfender Anforderungen ist im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.3) beschrieben.

DER.3.2.M15 Auswahl von geeigneten Prüfmethoden (S)

Es existieren verschiedene Methoden, um zu prüfen, ob Anforderungen des IT-Grundschutzes erfüllt werden. Einige Beispiele, sowie deren mögliche Anwendungsfälle, sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.1.2) beschrieben.

DER.3.2.M16 Erstellung eines Ablaufplans für die Vor-Ort-Prüfung (S)

Die zeitliche und inhaltliche Reihenfolge der Vor-Ort-Prüfung wird in einem Ablaufplan festgehalten. Umsetzungshinweise zur Erstellung eines solchen Ablaufplans sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.4 und 4.4.2 Abschnitt *Schritt 3*) zu finden.

DER.3.2.M17 Durchführung der Vor-Ort-Prüfung (S)

Die Vor-Ort-Prüfung bildet den am deutlichsten sichtbaren und am meisten beachteten Teil einer IS-Revision. In den Umsetzungshinweisen im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.5 und 4.4.2 Abschnitt *Schritt 4*) ist beschrieben, worauf besonderer Wert gelegt werden sollte.

DER.3.2.M18 Durchführung von Interviews (S)

Zur Feststellung einzelner Sachverhalte werden häufig Interviews eingesetzt. Wie solche Interviews gestaltet werden können, ist im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.5, Abschnitt *Vorgehensweise bei der IS-Revision vor Ort*) beschrieben.

DER.3.2.M19 Überprüfung der gewählten Risikobehandlungsoptionen (S)

Der Risikobehandlungsplan ist ebenfalls bei einer IS-Revision zu prüfen. Welche Optionen hierbei möglich sind, ist im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.4) beschrieben.

DER.3.2.M20 Nachbereitung der Vor-Ort-Prüfung (S)

Die Vor-Ort-Prüfungen werden mit einer Nachbearbeitung abgeschlossen. Es sollte der geprüften Institution ausreichend Zeit gewährt werden, um nachgeforderte Dokumentationen einzureichen. Dokumente, die bis zum vereinbarten Enddatum nicht eingegangen sind, sollten als nicht existent gewertet werden.

Weitere Hinweise zur Auswertung und Konsolidierung der Ergebnisse werden im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.6) beschrieben.

DER.3.2.M21 Erstellung eines IS-Revisionsberichts (S)

Im IS-Revisionsbericht werden alle Ergebnisse aufbereitet und zusammengefasst. Der Prozess, einschließlich der Qualitätssicherung bis zum fertigen IS-Revisionsbericht, wird im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 4.2.7 und 4.4.2, Abschnitt *Schritt 5*) beschrieben.

DER.3.2.M22 Nachbereitung einer IS-Revision (S)

Umsetzungshinweise zum Nachbereiten einer IS-Revision und zum Einleiten eines Follow-up sind im BSI-Dokument "Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz" (siehe [BSI_REVISION], Kapitel 3.5) beschrieben.

DER.3.2.M23 ENTFALLEN (H)

Die zugehörige Anforderung ist entfallen.

3. Weiterführende Informationen

3.1. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2. Quellenverweise

[BSI_REVISION] Informationssicherheitsrevision: Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz,: Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 3.0, März 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v3.pdf , zuletzt abgerufen am 22.02.2021

[UPB] Umsetzungsplan Bund 2017 - Leitlinie für Informationssicherheit in der Bundesverwaltung,: Bundesministerium des Innern (BMI), 21.07.2017, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.pdf, zuletzt abgerufen am 22.02.2021

[VSA] Allgemeine Verwaltungsvorschrift des Bundesministerium des Inneren zum materiellen und organisatorischen Schutz von Verschlußsachen (VS-Anweisung - VSA): Bundesministerium des Innern (BMI), 01.09.2018, http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm, zuletzt abgerufen am 22.02.2021