

# DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision

## 1. Beschreibung

### 1.1. Einleitung

Eine besondere Form der Revision ist die Informationssicherheitsrevision (IS-Revision) auf Basis des Dokuments *Informationssicherheitsrevision - Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz* (kurz „Leitfaden IS-Revision“).

Der „Leitfaden IS-Revision“ ist ein vom BSI veröffentlichtes Dokument, das die Vorgehensweise der IS-Revision beschreibt. Bundesbehörden sind dazu verpflichtet, ihr Managementsystem für Informationssicherheit (ISMS) durch IS-Revisionen zu überprüfen. Andere Institutionen können, anstelle einer regulären IT-Revision, eine IS-Revision auf Basis des Leitfadens durchführen, wenn sie die Umsetzung ihres ISMS überprüfen wollen.

Die IS-Revision auf Basis des Leitfadens zeichnet sich durch einen 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 Prüfkriterium der IS-Revision.

Die IS-Revision ist ein wesentlicher Bestandteil eines erfolgreichen Informationssicherheitsmanagements. Denn nur wenn die etablierten Maßnahmen und die Prozesse zur Informationssicherheit regelmäßig überprüft werden, kann beurteilt werden, ob diese wirksam umgesetzt, vollständig, aktuell und angemessen sind. Die IS-Revision ist somit ein geeignetes Werkzeug, um ein angemessenes Sicherheitsniveau in einer Institution festzustellen, zu erreichen, zu erhalten und kontinuierlich zu verbessern.

Die Hauptaufgabe der IS-Revision ist es, die Leitung der Institution, das IS-Management-Team und insbesondere den oder die ISB so zu unterstützen und zu begleiten, dass diese ein möglichst hohes Niveau der Informationssicherheit in der Institution erreichen können.

## 1.2. Zielsetzung

Der Baustein definiert Anforderungen an eine IS-Revision mit dem Ziel, die Informationssicherheit in einer Institution zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Sicherheitsmaßnahmen und -prozesse zu optimieren.

## 1.3. Abgrenzung und Modellierung

Der Baustein ist immer dann anzuwenden, wenn eine Institution dazu verpflichtet ist, Revisionen auf Basis des „Leitfadens IS-Revision“ durchzuführen oder diese freiwillig durchführen will. Der Baustein ist auf den gesamten Informationsverbund anzuwenden.

Es wird nicht berücksichtigt, wie sich die IS-Revision in eine bereits bestehende, übergeordnete Prüforganisation einer Institution (z. B. interne Revision) integrieren lässt. Der Baustein DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision* ist eine konkrete Ausgestaltung der im Baustein DER.3.1 *Audits und Revisionen* allgemein beschriebenen Anforderungen. Institutionen, die den vorliegenden Baustein umsetzen, müssen den Baustein DER.3.1 *Audits und Revisionen* nicht mehr umsetzen, da dessen Anforderungen vollständig in diesem Baustein enthalten sind.

Die IS-Revision und die Zertifizierung eines ISMS nach ISO 27001 auf der Basis von IT-Grundschutz ergänzen sich gegenseitig. IS-Revisionen können den Weg zur Zertifizierung begleiten und im Gegensatz hierzu bereits bei der Initiierung des Sicherheitsprozesses in der Institution durchgeführt werden. Sie zeigen der Institution auf, wo dringender Handlungsbedarf besteht und welche Sicherheitsmängel vorrangig bearbeitet werden sollten. Sind einzelne Informationsverbünde der Institution nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert, sollten Re-Zertifizierung und IS-Revision für diese Informationsverbünde nach Möglichkeit zusammen durchgeführt werden. Erkenntnisse aus Überwachungsaudits oder den Zertifizierungsverfahren können für die IS-Revision genutzt werden.

Liegt für die gesamte Institution ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz vor, lösen die im Zertifizierungsverfahren geforderten Überwachungsaudits die IS-Revisionen ab.

Die Vorschriften des Geheimschutzes und der Verschlusssachenanweisung des Bundes (VSA) bleiben unberührt und gelten unabhängig von den Anforderungen dieses Bausteins.

## 2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein DER.3.2 *Revisionen auf Basis des Leitfadens* von besonderer Bedeutung.

### 2.1. Verstoß gegen die Vorgaben des UP Bund

Der „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund 2017) ist als Leitlinie für Informationssicherheit in der Bundesverwaltung festgelegt. Somit befinden sich Bundesbehörden in einem ressortübergreifenden Management für Informationssicherheit, bei dem jede Behörde dafür verantwortlich ist, ihr spezifisches Sicherheitskonzept zu erstellen und umzusetzen. Nicht nur die Behörden des Bundes, sondern auch andere Institutionen können durch gesetzliche, vertragliche oder anderweitige Regelungen verpflichtet sein, den UP Bund 2017 umzusetzen. Der UP Bund 2017 legt dabei ausdrücklich fest, dass die Standards des BSI zur Informationssicherheit und zum IT-Grundschutz sowie die darin beschriebene Vorgehensweise der Standard-Absicherung als Mindestanforderung umgesetzt werden müssen. Weiterhin legt der UP Bund 2017 verbindlich fest, dass alle verpflichteten Institutionen den Stand des eigenen ISMS, z. B. durch eine geeignete IS-Revision, regelmäßig überprüfen und dabei den „Leitfaden für die

Informationssicherheitsrevision“ anwenden müssen. Geschieht dies nicht, verstoßen diese Institutionen gegen die Vorgaben des UP Bund.

## **2.2. Aussetzen von Sicherheitsmaßnahmen**

Das Sicherheitsniveau von Institutionen wird davon beeinflusst, ob Sicherheitsmaßnahmen vollständig und korrekt umgesetzt werden. Insbesondere in der kritischen Phase von Projekten oder unter bestimmten Rahmenbedingungen werden Sicherheitsmaßnahmen häufig temporär ausgesetzt. Teilweise wird dann jedoch vergessen, sie wieder zu reaktivieren, sodass ein zu niedriges Sicherheitsniveau bestehen bleibt.

## **2.3. Wirkungslose oder nicht wirtschaftliche Umsetzung von Sicherheitsmaßnahmen**

Werden Sicherheitsmaßnahmen umgesetzt, ohne dabei vorhandene Praxisaspekte zu berücksichtigen, sind diese Maßnahmen unter Umständen wirkungslos. So ist es zum Beispiel sinnlos, einen Eingangsbereich mit Drehkreuzen abzusperren, wenn die Mitarbeitenden das Gebäude stattdessen durch einen offenen Seiteneingang betreten können.

Ebenso kann es passieren, dass Einzelmaßnahmen ergriffen werden, die wirtschaftlich nicht sinnvoll sind. So ist für den Schutz von Informationen mit einem normalen Schutzbedarf bezüglich der Vertraulichkeit ein angemessen implementiertes Rechte- und Rollenkonzept sinnvoller und wirtschaftlicher als der Aufbau einer komplexen, zertifikatsbasierten Verschlüsselung auf dem Fileserver.

## **2.4. Unzureichende Umsetzung des Managementsystems für Informationssicherheit**

In vielen Institutionen überprüft der oder die ISB selbst, ob Sicherheitsmaßnahmen umgesetzt werden. Oft wird in diesem Zusammenhang die Prüfung des eigentlichen ISMS vergessen, da der oder die ISB als Teil des ISMS nicht unparteilich ist. Folglich könnten die Prozesse eines ISMS ineffizient oder nicht angemessen umgesetzt worden sein, was zu einem ungewollt niedrigen Sicherheitsniveau der Institution geführt haben könnte.

## **2.5. Unzureichende Qualifikation des Prüfteams**

Ist das Prüfteam nicht ausreichend qualifiziert oder bereitet sich ungenügend auf die Prüfungen vor, kann es während einer IS-Revision eventuell den Sicherheitszustand einer Institution falsch einschätzen. Unter Umständen empfiehlt es dann in seinem Prüfbericht nicht die nötigen oder sogar die falschen Korrekturmaßnahmen. In diesem Fall kann es passieren, dass die Informationen unwirtschaftlich oder sehr risikobehaftet geschützt werden.

## **2.6. Befangenheit interner IS-Revisionsteams**

Innerhalb von Institutionen können IS-Revisionsteams aus internem Personal gebildet werden. Sind diese Teams nicht ausreichend von anderen Abläufen abgegrenzt, könnten sie beeinflusst oder befangen sein. Dies ist insbesondere dann der Fall, wenn Mitglieder des IS-Revisionsteams an der Planung oder Umsetzung des ISMS beteiligt sind oder waren.

## **2.7. Fehlende langfristige Planung**

Werden IS-Revisionen nicht langfristig und zentral geplant, kann es passieren, dass einzelne Organisationseinheiten einer Institution sehr häufig und andere überhaupt nicht geprüft werden.

Auch ist es möglich, dass Veränderungen am ISMS nicht ausreichend untersucht werden, wenn Prüfungen nur unregelmäßig durchgeführt werden. In diesem Fall ist es nur sehr schwer oder gar nicht möglich, den Sicherheitszustand des gesamten Informationsverbunds geeignet zu bewerten.

## 2.8. Mangelhafte Planung und Abstimmung bei der Durchführung von IS-Revisionen

Wenn eine IS-Revision mangelhaft geplant und nicht mit dem zuständigen Personal der Institution abgestimmt wurde, sind während der Vor-Ort-Prüfung eventuell nicht die richtigen Personen verfügbar. Folglich lassen sich möglicherweise einzelne Bereiche überhaupt nicht prüfen. Auch wenn die Termine für die Prüfung der einzelnen Bereiche zu eng gesetzt wurden und nicht genügend Zeit eingeplant wurde, könnte es passieren, dass die Institution nur oberflächlich geprüft wird.

## 2.9. Fehlende Abstimmung mit der Personalvertretung

Im Rahmen von IS-Revisionen können auch Aspekte geprüft werden, aus denen Rückschlüsse gezogen werden könnten, wie sich Personen bei ihrer Arbeit verhalten und wie leistungsfähig sie sind. Somit könnten diese Prüfungen als Verhaltens- und Leistungskontrolle gewertet werden. Wird die Personalvertretung nicht mit einbezogen, kann die Vor-Ort-Prüfung verzögert oder sogar abgebrochen werden.

## 2.10. Absichtliches Verschweigen von Abweichungen oder Problemen

Personen könnten befürchten, dass bei einer IS-Revision ihre eigenen Fehler aufgedeckt werden. Um dies zu vermeiden, könnten sie Sicherheitsprobleme kaschieren und so ein falsches Bild über den tatsächlichen Sicherheitsstand vermitteln. So blieben Sicherheitsmängel unentdeckt und könnten nicht korrigiert werden. Darüber hinaus könnte die Institutionsleitung das mit diesem Sicherheitsmangel einhergehende Risiko falsch einschätzen.

## 2.11. Vertraulichkeitsverlust von schützenswerten Informationen

Während einer IS-Revision werden vertrauliche Informationen (z. B. Schwachstellen und Angriffsmöglichkeiten) durch das IS-Revisionsteam erhoben. Auch werden gegebenenfalls Defizite in der Informationssicherheit der geprüften Institution benannt. Werden diese Mängel unberechtigten Dritten bekannt, könnten sie dazu benutzt werden, die Institution anzugreifen oder in einen schlechten Ruf zu bringen.

## 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.3.2 *Revisionen auf Basis des Leitfadens IS-Revision* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	IS-Revisionsteam, Institutionsleitung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig

zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

### **3.1. Basis-Anforderungen**

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

#### **DER.3.2.A1 Benennung von Verantwortlichen für die IS-Revision (B) [Institutionsleitung]**

Die Institution MUSS eine verantwortliche Person für die IS-Revision benennen. Diese MUSS die IS-Revisionen planen, initiieren und die Ergebnisse nachverfolgen.

#### **DER.3.2.A2 Erstellung eines IS-Revisionshandbuches (B)**

Für die IS-Revision MUSS ein IS-Revisionshandbuch erstellt werden, das die angestrebten Ziele, einzuhaltende gesetzliche Vorgaben, Informationen über die Organisation, die Ressourcen und die Rahmenbedingungen enthält. Außerdem MUSS darin die Archivierung der Dokumentation beschrieben sein. Das Handbuch MUSS von der Leitungsebene verabschiedet werden.

#### **DER.3.2.A3 Definition der Prüfungsgrundlage (B)**

Die BSI-Standards 200-1 bis 200-3 sowie das IT-Grundschutz-Kompendium MÜSSEN die Prüfungsgrundlagen für die IS-Revision sein. Dabei SOLLTE die Standard-Absicherung des IT-Grundschutzes verwendet werden. Diese Prüfungsgrundlagen MÜSSEN allen Beteiligten bekannt sein.

#### **DER.3.2.A4 Erstellung einer Planung für die IS-Revision (B)**

Wenn die Institution nicht nach ISO 27001 auf Basis von IT-Grundschutz zertifiziert ist, MUSS sichergestellt werden, dass mindestens alle drei Jahre eine IS-Kurz- oder Querschnitts-Revision durchgeführt wird. Darüber hinaus SOLLTEN weitere Revisionen eingeplant werden, falls der Informationsverbund wesentlich verändert wird.

Es SOLLTE eine mehrjährige Grobplanung für die Revisionsvorhaben erstellt werden. Diese SOLLTE dann durch eine jährliche Detailplanung konkretisiert werden.

#### **DER.3.2.A5 Auswahl eines geeigneten IS-Revisionsteams (B)**

Es MUSS ein aus mindestens zwei Personen bestehendes IS-Revisionsteam zusammengestellt oder beauftragt werden. Dem IS-Revisionsteam MUSS ein uneingeschränktes Informations- und Einsichtnahmerecht für seine Tätigkeit eingeräumt werden. Bei eigenen IS-Revisionsteams MÜSSEN die einzelnen Mitglieder unparteilich sein. Die Mitglieder eines IS-Revisionsteams DÜRFEN NICHT an der Planung oder Umsetzung des ISMS beteiligt sein oder gewesen sein.

#### **DER.3.2.A6 Vorbereitung einer IS-Revision (B) [IS-Revisionsteam]**

Es MUSS ein IS-Revisionsteam mit einer IS-Revision beauftragt werden. Das IS-Revisionsteam MUSS festlegen, welche Referenzdokumente für eine IS-Revision benötigt werden. Die zu prüfende Institution MUSS das Sicherheitskonzept und alle weiteren erforderlichen Dokumente an das IS-Revisionsteam übergeben.

#### **DER.3.2.A7 Durchführung einer IS-Revision (B) [IS-Revisionsteam]**

Im Rahmen einer IS-Revision MÜSSEN eine Dokumenten- und eine Vor-Ort-Prüfung durch das IS-Revisionsteam durchgeführt werden. Sämtliche Ergebnisse dieser beiden Prüfungen MÜSSEN dokumentiert und in einem IS-Revisionsbericht zusammengefasst werden.

Bevor erstmalig eine IS-Querschnittsrevision durchgeführt wird, MUSS als IS-Revisionsverfahren eine IS-Kurzrevision ausgewählt werden. Die IS-Kurzrevision MUSS mit positivem Votum abgeschlossen werden, bevor eine IS-Querschnittsrevision durchgeführt wird.

### **DER.3.2.A8 Aufbewahrung von IS-Revisionsberichten (B)**

Die Institution MUSS den IS-Revisionsbericht und die diesem zugrundeliegenden Referenzdokumente mindestens für zehn Jahre ab Zustellung des Berichts sicher aufbewahren, sofern keine anders lautenden Gesetze oder Verordnungen gelten. Die Institution MUSS sicherstellen, dass lediglich berechnete Personen auf die IS-Revisionsberichte und die Referenzdokumente zugreifen können.

## **3.2. Standard-Anforderungen**

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

### **DER.3.2.A9 Integration in den Informationssicherheitsprozess (S)**

Die Institution SOLLTE sicherstellen, dass IS-Revisionen ein Teil des Sicherheitsprozesses sind. Außerdem SOLLTEN die Ergebnisse von IS-Revisionen in das ISMS zurückfließen und zu dessen Verbesserung beitragen.

Weiter SOLLTEN die Ergebnisse der IS-Revisionen sowie die Aktivitäten, um Mängel zu beseitigen und um die Qualität zu verbessern, in den regelmäßigen Bericht des oder der ISB an die Institutionsleitung aufgenommen werden.

### **DER.3.2.A10 Kommunikationsabsprache (S)**

Es SOLLTE klar geregelt werden, wie Informationen zwischen dem IS-Revisionsteam und der zu prüfenden Institution auszutauschen sind. So SOLLTE sichergestellt werden, dass diese Informationen vertraulich und integer bleiben.

### **DER.3.2.A11 Durchführung eines Auftaktgesprächs für eine IS-Querschnittsrevision (S) [IS-Revisionsteam]**

Für eine IS-Querschnittsrevision SOLLTE ein Auftaktgespräch zwischen dem IS-Revisionsteam und der zu prüfenden Institution durchgeführt werden. Darin SOLLTEN folgende Inhalte besprochen werden:

- Die Erläuterung und Darstellung des IS-Revisionsverfahrens,
- die Vorstellung der Institution (Arbeitsschwerpunkte und Überblick der eingesetzten IT) sowie
- die Übergabe der Referenzdokumente an das IS-Revisionsteam.

### **DER.3.2.A12 Erstellung eines Prüfplans (S) [IS-Revisionsteam]**

Vor einer IS-Revision SOLLTE das IS-Revisionsteam einen Prüfplan erstellen. Ist es während der IS-Revision notwendig, die geplanten Abläufe zu erweitern oder anderweitig anzupassen, SOLLTE der Prüfplan entsprechend angepasst werden. Der Prüfplan SOLLTE zudem in den abschließenden IS-Revisionsbericht aufgenommen werden.

Bei der IS-Kurzrevision SOLLTE die verbindlich festgelegte Prüfthemenliste des BSI an die Stelle des Prüfplans treten.

### **DER.3.2.A13 Sichtung und Prüfung der Dokumente (S) [IS-Revisionsteam]**

Bei der Dokumentenprüfung SOLLTE das IS-Revisionsteam die im Prüfplan festgelegten Anforderungen prüfen. Das IS-Revisionsteam SOLLTE überprüfen, ob alle relevanten Dokumente aktuell und vollständig sind. Bei der Prüfung auf Aktualität SOLLTE die Granularität der Dokumente berücksichtigt werden. Es SOLLTE darauf geachtet werden, dass alle wesentlichen Aspekte erfasst und geeignete Rollen zugewiesen wurden.

Weiter SOLLTE geprüft werden, ob die vorliegenden Dokumente und die darin getroffenen Entscheidungen nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung SOLLTEN dokumentiert werden und, soweit sinnvoll, in die Vor-Ort-Prüfung einfließen.

### **DER.3.2.A14 Auswahl der Zielobjekte und der zu prüfenden Anforderungen (S) [IS-Revisionsteam]**

In einer IS-Querschnittsrevision oder IS-Partialrevision SOLLTE das IS-Revisionsteam anhand der Ergebnisse der Dokumentenprüfung die Baustein-Zielobjekte für die Vor-Ort-Prüfung auswählen. Der Baustein zum Informationssicherheitsmanagement (siehe ISMS.1 *Sicherheitsmanagement*) des IT-Grundschutz-Kompodiums einschließlich aller zugehörigen Anforderungen SOLLTE jedoch immer vollständig geprüft werden. Weitere dreißig Prozent der modellierten Baustein-Zielobjekte SOLLTEN risikoorientiert zur Prüfung ausgewählt werden. Die Auswahl SOLLTE nachvollziehbar dokumentiert werden. Von den so ausgewählten Baustein-Zielobjekten SOLLTEN dreißig Prozent der jeweiligen Anforderungen bei der IS-Revision geprüft werden.

Darüber hinaus SOLLTEN bei der Auswahl der zu prüfenden Baustein-Zielobjekte die bemängelten Anforderungen aus vorhergehenden IS-Revisionen berücksichtigt werden. Alle Anforderungen mit schwerwiegenden Sicherheitsmängeln aus vorhergehenden IS-Revisionen SOLLTEN mit geprüft werden.

### **DER.3.2.A15 Auswahl von geeigneten Prüfmethode(n) (S) [IS-Revisionsteam]**

Das IS-Revisionsteam SOLLTE sicherstellen, dass geeignete Prüfmethode(n) eingesetzt werden, um die zu prüfenden Sachverhalte zu ermitteln. Alle Prüfungen SOLLTEN verhältnismäßig sein.

### **DER.3.2.A16 Erstellung eines Ablaufplans für die Vor-Ort-Prüfung (S) [IS-Revisionsteam]**

Gemeinsam mit der zu prüfenden Institution SOLLTE das IS-Revisionsteam einen Ablaufplan für die Vor-Ort-Prüfung erarbeiten. Die Ergebnisse SOLLTEN zusammen mit dem IS-Prüfplan dokumentiert werden.

### **DER.3.2.A17 Durchführung der Vor-Ort-Prüfung (S) [IS-Revisionsteam]**

Bei der Vor-Ort-Prüfung SOLLTE das IS-Revisionsteam untersuchen und feststellen, ob die ausgewählten Maßnahmen die Anforderungen des IT-Grundschutzes angemessen und praxistauglich erfüllen.

Die Prüfung SOLLTE mit einem Eröffnungsgespräch beginnen. Danach SOLLTEN alle für die Prüfung ausgewählten Anforderungen des Prüfplans bzw. alle Themenfelder der Prüftemenliste überprüft werden. Dafür SOLLTEN die vorgesehenen Prüfmethode(n) angewandt werden. Werden bei einer ausgewählten Stichprobe Abweichungen zum dokumentierten Status festgestellt, SOLLTE die Stichprobe bedarfsorientiert erweitert werden, bis der Sachverhalt geklärt ist.

Während der Vor-Ort-Prüfung SOLLTEN das IS-Revisionsteam niemals aktiv in IT-Systeme eingreifen und auch keine Handlungsanweisungen zu Änderungen am Revisionsgegenstand erteilen.

Alle wesentlichen Sachverhalte und Angaben zu Quellen-, Auskunft- und Vorlage-Ersuchen sowie durchgeführten Besprechungen SOLLTEN schriftlich festgehalten werden.

In einem Abschlussgespräch SOLLTE das IS-Revisionsteam der geprüften Institution wesentliche Feststellungen kurz darstellen. Dabei SOLLTE das IS-Revisionsteam die Feststellungen nicht konkret bewerten, sondern Hinweise auf etwaige Mängel und die weitere Verfahrensweise geben. Auch dieses Abschlussgespräch SOLLTE protokolliert werden.

### **DER.3.2.A18 Durchführung von Interviews (S) [IS-Revisionsteam]**

Interviews durch das IS-Revisionsteam SOLLTEN strukturiert erfolgen. Fragen SOLLTEN knapp, präzise und leicht verständlich formuliert werden. Zudem SOLLTEN geeignete Fragetechniken eingesetzt werden.

### **DER.3.2.A19 Überprüfung der gewählten Risikobehandlungsoptionen (S) [IS-Revisionsteam]**

Das IS-Revisionsteam SOLLTE prüfen, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind und ob sie verbindlich durch die Institutionsleitung getragen werden. Das IS-Revisionsteam SOLLTE stichprobenartig verifizieren, ob bzw. inwieweit die gewählten Risikobehandlungsoptionen umgesetzt sind.

### **DER.3.2.A20 Nachbereitung der Vor-Ort-Prüfung (S) [IS-Revisionsteam]**

Nach der Vor-Ort-Prüfung SOLLTEN die erhobenen Informationen weiter durch das IS-Revisionsteam konsolidiert und ausgewertet werden. Nachdem die eventuell nachgeforderten Dokumente, Dokumentationen und zusätzlichen Informationen ausgewertet wurden, SOLLTEN die geprüften Anforderungen endgültig bewertet werden.

### **DER.3.2.A21 Erstellung eines IS-Revisionsberichts (S) [IS-Revisionsteam]**

Das IS-Revisionsteam SOLLTE die gewonnenen Ergebnisse in einen IS-Revisionsbericht überführen und dort nachvollziehbar dokumentieren. Eine Entwurfsversion des Berichts SOLLTE der geprüften Institution vorab übermittelt werden. Es SOLLTE verifiziert werden, ob die durch das IS-Revisionsteam festgestellten Sachverhalte richtig aufgenommen wurden.

Die geprüfte Institution SOLLTE sicherstellen, dass alle betroffenen Stellen in der Institution innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des IS-Revisionsberichts erhalten. Insbesondere SOLLTEN die Inhalte an die Institutionsleitung, an die Verantwortlichen für die IS-Revision sowie den oder die ISB kommuniziert werden.

IS-Revisionsberichte SOLLTEN aufgrund der enthaltenen schützenswerten Informationen mit einer geeigneten Vertraulichkeitseinstufung versehen werden.

Es SOLLTE überlegt werden, die Ergebnisse der IS-Revision der Institutionsleitung vom IS-Revisionsteam in Form einer Präsentation vorzustellen.

### **DER.3.2.A22 Nachbereitung einer IS-Revision (S)**

Die im IS-Revisionsbericht festgestellten Abweichungen SOLLTEN in einer angemessenen Zeit durch die Institution korrigiert werden. Die durchzuführenden Korrekturmaßnahmen SOLLTEN mit Zuständigkeiten, Umsetzungstermin und dem jeweiligen Status dokumentiert sein. Die Umsetzung SOLLTE kontinuierlich nachverfolgt und der Umsetzungsstatus fortgeschrieben werden.

Grundsätzlich SOLLTE geprüft werden, ob ergänzende IS-Revisionen notwendig sind. Die Institution SOLLTE die Grob- und Detailplanung zur IS-Revision anpassen.

## **3.3. Anforderungen bei erhöhtem Schutzbedarf**

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

### **DER.3.2.A23 ENTFALLEN (H)**

Diese Anforderung ist entfallen.



## 4. Weiterführende Informationen

### 4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinem Leitfaden „Informationssicherheitsrevision: Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz“, wie eine IS-Revision durchgeführt werden muss.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinem Dokument „Verbindliche Prüfthemen für die IS-Kurzrevision“, welche Themen bei einer IS-Kurzrevision geprüft werden sollen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt mit einem „Revisionshandbuch zur Informationssicherheit nach UP Bund“ ein Musterhandbuch für die IS-Revision bereit.

Das Bundesministerium des Inneren (BMI) beschreibt in der Verschlusssachenanweisung (VSA), welche Vorgaben beim Umgang mit Verschlusssachen zu beachten sind.