Bundesamt
für Sicherheit in der
Informationstechnik

Informationssicherheitsrevision

Ein Leitfaden für die IS-Revision auf Basis von IT-Grundschutz

Version 3.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: isrevision@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Versionshistorie

Stand	Version	Änderungen
September 2008	1.0	
März 2010	2.0	Ergänzung IS-Kurzrevision, Anpassung des Verfahrens IS-Querschnittsrevision
März 2018	3.0	Anpassung an den neuen IT-Grundschutz, Anpassung an UP-Bund 2017

1.2 Zielsetzung

Viele Geschäftsprozesse werden elektronisch unterstützt und große Mengen von Informationen sind digital gespeichert, werden digital verarbeitet und in IT-Netzen übermittelt. Damit sind Wirtschaft, Verwaltung und auch Bürgerinnen und Bürger von einem einwandfreien Funktionieren der eingesetzten Informationstechnik abhängig. Deshalb ist Informationssicherheit heute ein Muss für Jeden. Für Unternehmen und Behörden bedeutet dies u. a., ein angemessenes Informationssicherheitsmanagement zu etablieren, um so den steigenden Bedrohungen für die Verfügbarkeit, die Vertraulichkeit und die Integrität von Informationen, Geschäftsprozessen, Anwendungen und Systemen entgegenzuwirken. Informationssicherheitsrevision (IS-Revision) ist ein Bestandteil eines jeden erfolgreichen Informationssicherheitsmanagements. Nur durch die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheitsprozesses können Aussagen über deren wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution.

Die Hauptaufgabe der IS-Revision ist es, das Management, das IS-Management-Team und insbesondere den Informationssicherheitsbeauftragten (ISB) bei der Umsetzung und Optimierung der Informationssicherheit zu unterstützen und zu begleiten. Die Prüfungstätigkeit zielt darauf ab, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und der Sicherheitsprozesse zu optimieren. Dies sichert die Handlungsfähigkeit, das Ansehen und die Vermögenswerte (Assets) der Institution. Das Ergebnis einer IS-Revision, der IS-Revisionsbericht, zeigt der Institution in kompakter Form den Sicherheitsstatus und ggf. den Handlungsbedarf aufgrund bestehender Sicherheitsmängel auf und dient als Hilfsmittel für den weiteren Optimierungsprozess des Informationssicherheitsmanagementsystems (ISMS). Der IS-Revisionsbericht ist eine Informationsquelle für das Management und Arbeitsmittel für alle Sicherheitsverantwortlichen.

1.3 Adressatenkreis

Dieses Dokument richtet sich an alle Verantwortlichen, die IS-Revisionen auf Basis von IT-Grundschutz veranlassen oder durchführen möchten. Dies können z. B. Revisoren, ISO 27001-Auditoren, die Leitung der Institution, Informationssicherheitsbeauftragte oder sonstige Verantwortliche für die Informationssicherheit sein. Primärer Adressatenkreis sind die Funktionsträger in den Bundesbehörden, die zu regelmäßigen

IS-Revisionen verpflichtet sind sowie IS-Revisoren, die entsprechende Revisionen durchführen.

Informationssicherheitsbeauftragten und sonstigen Verantwortlichen für die IT-Sicherheit soll dieser Leitfaden insbesondere dazu dienen, sich einen Überblick über das Thema „IS-Revision“ zu verschaffen, die zu prüfenden Sicherheitsaspekte zu betrachten und sich mit dem Ablauf einer IS-Revision vertraut zu machen.

Den IS-Revisoren gibt der Leitfaden konkrete Vorgaben für die Durchführung einer IS-Revision. Diese sind insbesondere in Kapitel 4 „Durchführung einer IS-Revision“ zu finden.

1.4 Anwendungsweise

Der vorliegende „Leitfaden für die Informationssicherheitsrevision auf Basis von IT-Grundschutz“ ist ein Baustein bei der Umsetzung der „Cyber-Sicherheitsstrategie für Deutschland 2016“[BMI1] und des „Umsetzungsplan Bund 2017, Leitlinie für Informationssicherheit in der Bundesverwaltung (UP Bund 2017)“ [BMI2]. Er bildet die Grundlage für die Durchführung von IS-Revisionen in Bundesbehörden. Das Ziel des UP Bund ist es, mittel- und langfristig Informationssicherheit auf hohem Niveau in der gesamten Bundesverwaltung zu etablieren, um auch zukünftig eine zuverlässige und funktionsfähige Informationsinfrastruktur für die Bundesverwaltung zu gewährleisten. Der UP Bund wie auch die Cyber-Sicherheitsstrategie wurden unter der Federführung des Bundesministeriums des Innern (BMI) erarbeitet und gelten für alle Bundesressorts und deren Geschäftsbereiche.

Ziel dieses Dokumentes ist es, die Stellung der IS-Revision innerhalb des Sicherheitsprozesses darzustellen und die damit verbundenen Aufgaben detailliert zu erläutern. Der Leitfaden zeigt auf der einen Seite auf, wie eine Institution die IS-Revision im Haus etablieren kann und welche Aktivitäten für die Institution, wie z. B. Berichtsauswertung oder Planung und Koordinierung von IS-Revisionen, damit verbunden sind. Auf der anderen Seite wird den IS-Revisoren ein praxisnaher Handlungsleitfaden zur Verfügung gestellt, der konkrete Vorgaben und Hinweise für die Durchführung einer IS-Revision und die Berichtserstellung enthält. Zusätzlich ist er als Grundlage für Ausschreibungen von IS-Revisionen anzuwenden. Durch die Vereinheitlichung der Vorgehensweise bei einer IS-Revision soll eine gleichbleibend hohe Qualität der Revisionen gewährleistet werden. Darüber hinaus ist mit Einführung dieses Verfahrens die Möglichkeit gegeben, den Status der Informationssicherheit innerhalb der geprüften Institutionen festzustellen und die Entwicklung langfristig nachzuvollziehen.

In Kapitel 2.1 wird nach einem allgemeinen Überblick über das Verfahren der IS-Revision der Zusammenhang zwischen dem Informationssicherheitsprozess und der IS-Revision erläutert. Außerdem werden unterschiedliche Arten von IS-Revisionen vorgestellt und allgemeine Revisionsprinzipien beschrieben. Kapitel 3 erläutert die Elemente der IS-Revision. Hierzu gehören organisatorische Hinweise für die Institution, die Darstellung der einzelnen Phasen einer IS-Revision, die Beschreibung der Aufgaben, die durch die Einführung von regelmäßigen IS-Revisionen entstehen und Hinweise zur Weiterverarbeitung der Revisionsergebnisse. Die Durchführung einer IS-Revision, welche sowohl durch internes Personal als auch durch beauftragte IT-Sicherheitsdienstleister erfolgen kann, sowie die Anforderungen an das Berichtswesen werden in Kapitel 4 beschrieben. Kapitel 5 schließt mit Hinweisen zu verfügbaren Hilfsmitteln.

1.5 Das Verhältnis der IS-Revision zur IT-Revision

Zum Thema Revision und speziell IT-Revision stehen zahlreiche Veröffentlichungen von Standards und Leitfäden sowie allgemeine Literatur zur Verfügung, wie beispielsweise des Instituts der Wirtschaftsprüfer (IDW), des Instituts für Interne Revision (IIR), der Information Systems Audit and Control Association (ISACA) oder internationalen Organisationen wie dem International Auditing and Assurance Standards Board (IAASB) oder dem Institute of Internal Auditors (IIA). Diese Werke berücksichtigen IT als wichtigen Bestandteil von Unternehmen und deren Sicherheit in den Vorgaben zu Prüfungen.

Zentraler Gegenstand einer IT-Revision war in der Vergangenheit primär die Prüfung der IT-gestützten Buchführungssysteme. Diese Sichtweise wird heutzutage nicht mehr vertreten, da erkannt wurde, dass heutige Systeme stark vernetzt sind und viele Abhängigkeiten zwischen Systemen und Geschäftsprozessen

existieren. Daher wird inzwischen bei einer IT-Revision, genauso wie bei der IS-Revision, die gesamte IT-Infrastruktur einer Institution betrachtet.

Bei der IT-Revision stehen die drei Prüfkriterien Wirtschaftlichkeit (IT-Prozess, IT-Organisation, Sicherheitsmaßnahmen), Sicherheit und Ordnungsmäßigkeit (Einhaltung von Rechnungslegungsgrundsätzen wie Vollständigkeit, Richtigkeit, Zeitgerechtigkeit, Nachvollziehbarkeit, Ordnung) gleichwertig nebeneinander. Die Gewichtung dieser drei Ziele bestimmt individuell die Institution bzw. der Revisor und ist abhängig von der Unternehmens- bzw. Behördenstrategie sowie dem konkreten Prüfauftrag.

Die IS-Revision hingegen als "neue" Disziplin der Revision, legt den Schwerpunkt auf die ganzheitliche Prüfung der Informationssicherheit. Das bedeutet, dass hier vom Aufbau einer Informationssicherheitsorganisation über Personalaspekte bis zur Konfiguration von Systemen alle Ebenen geprüft werden. Die Prüfungskriterien Wirtschaftlichkeit und Ordnungsmäßigkeit werden nachrangig betrachtet. Die Sicherheit (einschließlich die Angemessenheit der Sicherheitsmaßnahmen) ist somit das wesentliche Prüfkriterium der IS-Revision.

Haben Institutionen bereits eine IT-Revision im Hause etabliert, kann aufgrund der vielen Gemeinsamkeiten die IS-Revision unter Beachtung der Anforderungen dieses Leitfadens zusammen mit der IT-Revision durchgeführt werden.

Auf das Zusammenspiel von IS-Revision und Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz wird in Kapitel 2.2 eingegangen.

1.6 Verwendete Begriffe

Die folgenden Begrifflichkeiten werden in diesem Dokument verwendet:

Die **Revision** im Allgemeinen hat die Aufgabe, Geschäftsvorgänge und die dafür verwendeten Hilfsmittel nachträglich auf Richtigkeit, Sicherheit, Ordnungs-, Gesetz- und Zweckmäßigkeit zu überprüfen.

Die **IS-Revision** legt im Vergleich zur allgemeinen Revision den Fokus auf die Informationssicherheit der Institution. Das Ziel einer IS-Revision ist es, das aktuelle Sicherheitsniveau innerhalb der Institution durch eine unabhängige Instanz festzustellen und Hinweise zu bestehenden Sicherheitslücken und -mängeln zu geben. Die IS-Revision ist ein Spezialfall der (allgemeinen) Revision. Ergebnis ist ein IS-Revisionsbericht mit Empfehlungen zur Verbesserung der Informationssicherheit.

Der Begriff **Audit** wird in diesem Dokument für das Verfahren zur Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz verwendet.

Bei der IS-Revision wird der **risikoorientierte Ansatz** der Revision übernommen (siehe [IDW]). Dies bedeutet, dass die einem höheren Risiko unterliegenden Bereiche intensiver und häufiger geprüft werden, als die weniger risikobehafteten. Auf dieser Grundlage wird die Prüfstrategie entwickelt und hieraus der IS-Prüfplan abgeleitet.

Der **IS-Prüfplan** beschreibt den gesamten Ablauf der Prüfung, von der ersten Auswahl der Baustein-Zielobjekte, bis zur Dokumentation der Vor-Ort-Prüfung. Um Verwechselungen mit Prüfplänen in anderen Bereichen zu vermeiden, wird der Prüfplan im Zusammenhang mit IS-Revisionen in diesem Dokument immer als IS-Prüfplan bezeichnet.

Der Begriff **Anforderungen** in diesem Dokument bezeichnet die Anforderungen aus dem IT-Grundschutz-Kompendium sowie die ergänzenden Sicherheitsmaßnahmen, die aufgrund einer Risikoanalyse und aufgrund von Vorschriften umzusetzen sind.

Der Begriff **Baustein-Zielobjekt** bezeichnet ein konkretes Prüfobjekt oder eine nach BSI-Standard 200-2 Kapitel 8.1.1 zusammengefasste Gruppe von Prüfobjekten, auf welche ein bestimmter Baustein angewendet wird (z. B. Baustein SYS.2.2.3 „Clients unter Windows 10" wird auf eine Gruppe von 80 Windows 10 Clients in der Personalverwaltung angewendet.).

Kritische Geschäftsprozesse sind Fachaufgaben, die eine hohe Bedeutung für die Wertschöpfung der Institution haben. Die Klassifizierung in unkritische, wenig kritische, kritische und hoch kritische Geschäftsprozesse erfolgt analog bekannter Schadensszenarien aus der Schutzbedarfsfeststellung (siehe [BSI2]). Alle Geschäftsprozesse, die als kritisch oder hoch kritisch einzustufen sind, werden in einer Liste der kritischen Geschäftsprozesse erfasst (Näheres siehe BSI Standard 100-4 Notfallmanagement [BSI3]).

Prüfthemen sind im Rahmen der Revisionspraxis gesammelte, besonders prüfungsrelevante Aspekte und Fragestellungen der Informationssicherheit. Hierzu gehören Themen des Sicherheitsmanagements genauso wie technische Aspekte.

In diesem Dokument wird der Begriff „**Institution**“ benutzt. Institution wird als Oberbegriff für Behörden, Unternehmen und sonstige öffentliche oder private Organisationen verwendet.

Alle Personalbegriffe in diesem Dokument beziehen sich in gleicher Weise auf Frauen und Männer. Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

1.7 Literaturverzeichnis

[BMI1] Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, November 2016, http://www.bmi.bund.de/cybersicherheitsstrategie/

[BMI2] Bundesministerium des Innern, Umsetzungsplan Bund 2017, Leitlinie für Informationssicherheit in der Bundesverwaltung, Juli 2017, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/2017/up-bund-2017.html

[BMI3] Bundesministerium des Innern, Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen, April 2010, http://www.verwaltungsvorschriften-im-internet.de

[BMWI] Bundesministerium für Wirtschaft und Technologie, Handbuch für den Geheimschutz in der Wirtschaft, August 2017, http://www.bmwi.de

[BSI] Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheitsmanagement und IT-Grundschutz – BSI Standards, 2018, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[BSI1] Bundesamt für Sicherheit in der Informationstechnik, Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 200-1, Version 1.0, Oktober 2017, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[BSI2] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Vorgehensweise, BSI-Standard 200-2, Version 1.0, Oktober 2017, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html

[BSI3] Bundesamt für Sicherheit in der Informationstechnik, Notfallmanagement, BSI-Standard 100-4, Version 1.0, 2008, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html

[BSI4] Bundesamt für Sicherheit in der Informationstechnik, Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html

[GSK] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, BSI, jährlich neu, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

[IDW] Institut der deutschen Wirtschaftsprüfer, IDW PS 261 „Feststellung und Beurteilung von Fehlerrisiken und Reaktionen des Abschlussprüfers auf die beurteilten Fehlerrisiken“, September 2006, http://www.idw.de

[SÜG] Sicherheitsüberprüfungsgesetz (SÜG), Februar 2008, http://www.gesetze-im-internet.de

[ZERT] Bundesamt für Sicherheit in der Informationstechnik, Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Auditierungsschema, Version 1.0, März 2011, https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Managementsystemzertifizierung_node.html

2 Einführung in die IS-Revision

2.1 Überblick über die IS-Revision

In den Bundesbehörden wird mit den Festlegungen des UP Bund 2017 als Informationssicherheitsleitlinie des Bundes die Anwendung des modernisierten IT-Grundschutzes und die darin beschriebene Standard-Absicherung als Mindestanforderung zum Schutz der in der Bundesverwaltung verarbeiteten Informationen festgelegt. Neben der Erstellung und Umsetzung eines Sicherheitskonzepts werden auch die Vorgaben aus den BSI-Standards 200-1 [BSI1] und 200-2 [BSI2] sowie Erfolgskontrollen im Rahmen von IS-Revisionen gefordert, die der Aufrechterhaltung der Informationssicherheit und deren kontinuierlicher Verbesserung dienen sollen. Die Verantwortung für die IS-Revision als integralem Bestandteil des Informationssicherheitsmanagements ebenso wie für die Initiierung und Steuerung des Informationssicherheitsprozesses liegt bei der Leitung der Institution.

Der nachfolgende Überblick zeigt wesentliche Kriterienwerke und Standards für die IS-Revision.

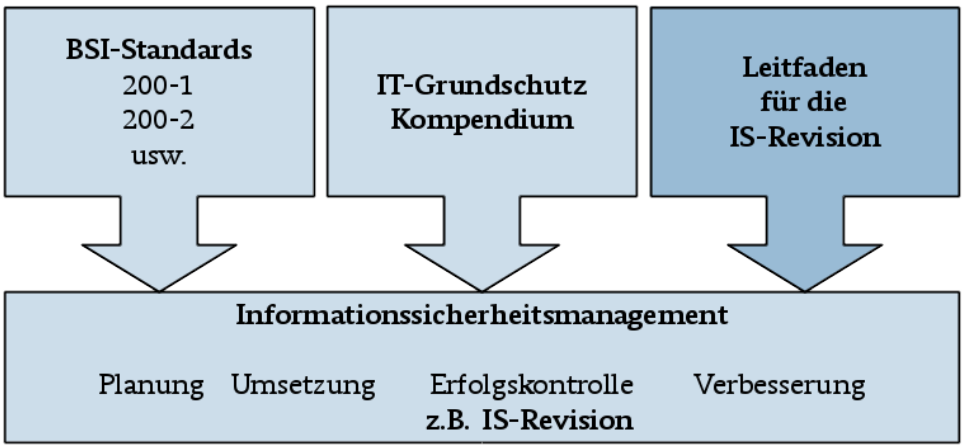

Abbildung 1: Kriterienwerke und Standards für die IS-Revision

Die IS-Revision prüft die Effektivität der Sicherheitsorganisation sowie die Angemessenheit und Umsetzung des Sicherheitskonzeptes der Institution. Dabei wird die Sicherheitsstrategie und die Umsetzung technischer, organisatorischer und personeller Anforderungen betrachtet (siehe [BMI2]).

Gemäß UP Bund sind Bundesbehörden im Rahmen der Evaluierung der Informationssicherheit verpflichtet, in angemessenen Abständen eine IS-Revision durchzuführen. Diese beinhaltet immer eine Gesamtbetrachtung der Institution unter Berücksichtigung aller Schichten aus dem IT-Grundschutz. Grundlage jeder IS-Revision sind die vorhandenen Dokumente zur Informationssicherheit (z. B. Leitlinie zur Informationssicherheit, Netzplan, IT-Grundschutz-Check).

Eine IS-Revision kann durch Angehörige der eigenen Institution (interne Revision) oder durch Dritte (externe Revision) durchgeführt werden. Wesentlich ist, dass die Prüfer, die eine IS-Revision durchführen, nicht unmittelbar bei der Konzeption, Entwicklung und Umsetzung der Maßnahmen zum untersuchten Objekt beteiligt waren.

Ergebnis der IS-Revision ist der IS-Revisionsbericht mit Aussagen zum Status der Informationssicherheit sowie ggf. Empfehlungen zu erforderlichen Verbesserungen oder Anpassungen von IT-Sicherheitsmaßnahmen, -strukturen und -prozessen. Hierdurch unterstützt die IS-Revision die Leitung der Institution bei der Wahrnehmung der Gesamtverantwortung und auch das Sicherheitsmanagement, das mit dem IS-Revisionsbericht ein zusätzliches Mittel erhält, um notwendigen Handlungsbedarf aufzuzeigen.

2.2 Integration in den ISMS-Prozess

Die Praxis zeigt, dass eine umfassende, unternehmens- bzw. behördenweite Informationssicherheit, die auf dauerhafte Erfüllung der Anforderungen und nachhaltige Begrenzung der Risiken ausgerichtet ist, nur durch ein Informationssicherheitsmanagement erreicht werden kann. Der BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS)“ (siehe [BSI1]) beschreibt den Informationssicherheitsprozess. Innerhalb des ISMS ist die IS-Revision Teil des Informationssicherheitsprozesses und fügt sich in die „Check“-Phase nach dem PDCA-Modell von Deming ein.

Der Informationssicherheitsprozess wird von der Leitungsebene initiiert und beginnt mit der „Plan“-Phase. In dieser Phase wird die Sicherheitsorganisation aufgebaut.

In der anschließenden „Do“-Phase werden das Sicherheitskonzept erstellt und die erforderlichen Maßnahmen umgesetzt.

Die folgende „Check“-Phase dient der Überprüfung der IT-Sicherheitsstrategie, der IT-Sicherheitsorganisation, des Sicherheitskonzepts und der Umsetzung der IT-Grundschutz-Anforderungen. Grundlage für die Erfolgskontrollen in der „Check“-Phase ist immer das Sicherheitskonzept. Eine mögliche Methode der Erfolgskontrolle ist die IS-Revision.

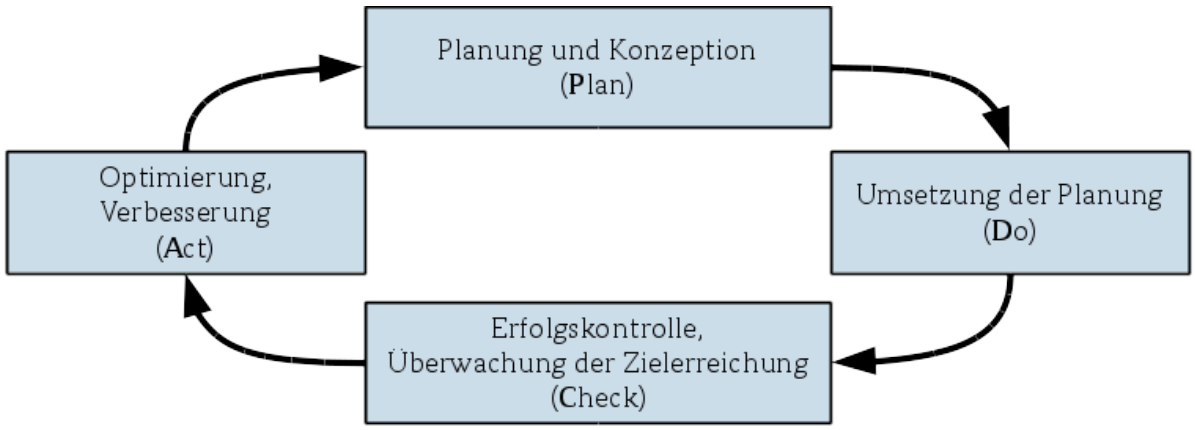

Abbildung 2: PDCA-Modell nach Deming

Das Ergebnis der „Check“-Phase, z. B. der IS-Revisionsbericht, wird gemäß dem Informationssicherheitsprozess in der darauf folgenden „Act“-Phase ausgewertet und weiterverarbeitet. Das bedeutet, dass die Geschäftsprozesse optimiert und Sicherheitslücken bei der Umsetzung der IT-Grundschutz-Anforderungen geschlossen werden.

Falls sich durch die Ergebnisse der „Check“-Phase grundlegende oder umfangreiche Veränderungen ergeben, so beginnt der Informationssicherheitsprozess vorzeitig wieder mit der „Plan“-Phase (siehe [BSI1]).

Der Kreislauf der IT-Grundschutz Vorgehensweise mit den prozessbeeinflussenden Ein- und Ausgabedokumenten wird im folgenden Diagramm dargestellt.

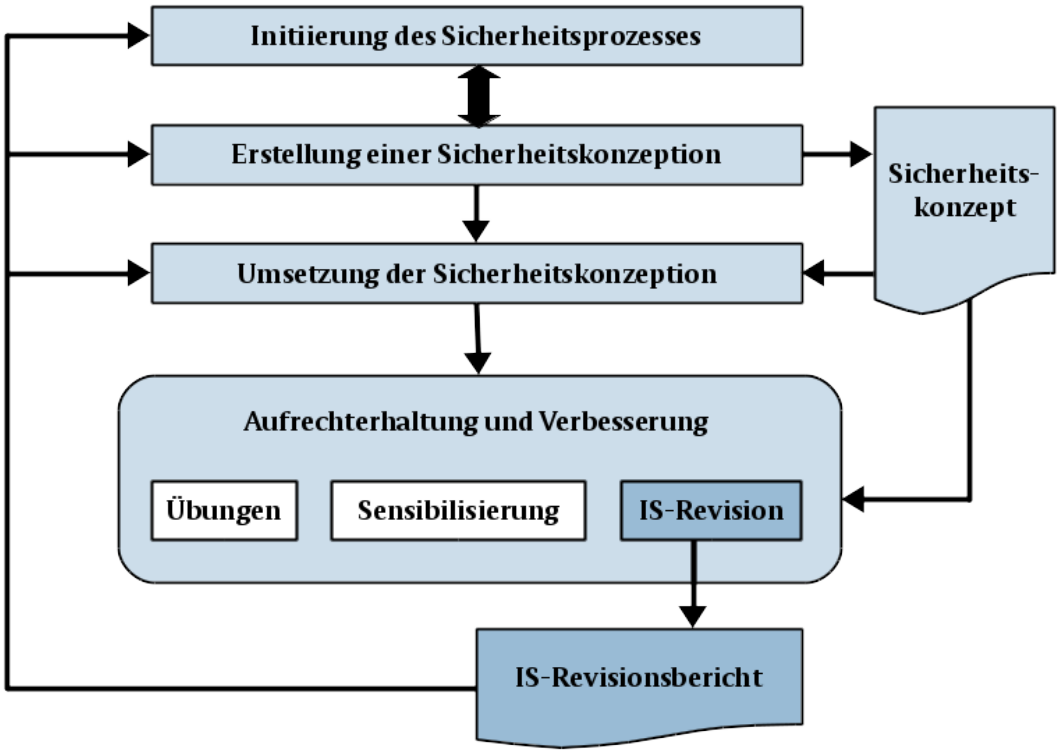

Abbildung 3: Einbettung der IS-Revision in das ISMS

Die IS-Revision und die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (siehe [ZERT]) ergänzen sich. IS-Revisionen können den Weg zur Zertifizierung begleiten und im Gegensatz zur Zertifizierung bereits am Anfang 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 nach Möglichkeit zusammen durchgeführt werden. Erkenntnisse aus Überwachungsaudits oder dem Zertifizierungsverfahren können für die IS-Revision genutzt werden.

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

2.3 Unterschiedliche Arten einer IS-Revision

Es existieren unterschiedliche Ausprägungen der IS-Revision, wobei in diesem Dokument zwischen IS-Kurzrevision, IS-Querschnittsrevision, und IS-Partialrevision unterschieden wird.

2.3.1 IS-Kurzrevision – das Einstiegsverfahren

Die IS-Kurzrevision verschafft dem IS-Management mit wenig Aufwand 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 problembehaftet

erwiesen haben (z. B. Sicherheitsorganisation, Umgang mit mobilen Datenträgern). Die IS-Kurzrevision betrachtet dabei die gesamte Institution. Um ein strukturiertes Verfahren mit gleichbleibend hoher Qualität zu gewährleisten, sind die zu verwendenden Prüfthemen in einer Liste zusammengefasst (https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISRevision/isrevision_node.html unter Hilfsmittel – Prüfthemen IS-Kurzrevision).

Die Durchführung einer IS-Kurzrevision kann bereits am Anfang des Sicherheitsprozesses angestoßen werden. Es bestehen keine Voraussetzungen für die geprüfte Institution hinsichtlich Dokumentation und Umsetzungsstatus der Anforderungen. Die IS-Kurzrevision dient zudem der Überprüfung, ob die wesentlichen Voraussetzungen für eine IS-Querschnittsrevision gegeben sind. Häufig ist in einer Institution nicht gewährleistet, dass eine konsistente Strukturanalyse und Modellierung einschließlich Schutzbedarfsfeststellung vorliegen. Daher sollte vor der ersten IS-Querschnittsrevision grundsätzlich eine IS-Kurzrevision durchgeführt werden.

Die IS-Kurzrevision ist die IS-Revisionsart zum Einstieg in das regelmäßige Revisionsverfahren und ein erster Schritt zur Erreichung der Anforderungen des UP Bund.

Anwendungsszenarien einer IS-Kurzrevision sind zum Beispiel:

- Die Leitung der Institution, die Innenrevision oder ein Dritter möchte einen ersten Überblick über den bestehenden Informationssicherheitsstatus erhalten.
- Ein Mitarbeiter übernimmt die Aufgabe des „Informationssicherheitsbeauftragten“ und möchte sich einen Überblick über das neue Aufgabengebiet und anstehende Arbeiten verschaffen.
- Die Institution möchte sich vor Beauftragung einer IS-Querschnittsrevision einen Überblick über den IT-Sicherheitsstatus verschaffen.

2.3.2 IS-Querschnittsrevision – das IS-Revisionsverfahren als Vorbereitung auf ein Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz

Ist der Sicherheitsprozess weiter fortgeschritten und ein Großteil der IT-Grundschutz-Anforderungen erfüllt, kann eine IS-Querschnittsrevision durchgeführt werden. Eine IS-Querschnittsrevision hat einen ganzheitlichem Ansatz und ein breites Prüfspektrum. Bei einer IS-Querschnittsrevision werden alle Schichten des IT-Grundschutzes anhand von Stichproben geprüft.

Prüfgegenstand bei der IS-Querschnittsrevision ist immer die gesamte Institution. Sie hat das Ziel, einen umfassenden Eindruck von dem Informationssicherheitsstatus der Institution zu geben.

2.3.3 IS-Partialrevision – die IS-Revision für Spezialfälle

Eine IS-Partialrevision beschränkt sich auf einen speziellen Ausschnitt der Institution und wird bei Bedarf z. B. durch das IS-Management-Team angestoßen. Die Prüftiefe ist wesentlich größer als bei der IS-Querschnittsrevision.

Die IS-Partialrevision ist eine anlassbezogene IS-Revision, die z. B. nach größeren Umstrukturierungen, Sicherheitsvorfällen oder bei Einführung neuer Geschäftsprozesse bzw. neuer Technologien durchgeführt wird. Sie ist prädestiniert für die IS-Revision von kritischen Geschäftsprozessen. Da sich eine IS-Partialrevision auf bestimmte Geschäftsprozesse oder IT-Verfahren beschränkt, werden auch nur die damit verbundenen Systeme und die hierfür anzuwendenden Bausteine des IT-Grundschutzes betrachtet. Dadurch kann die Prüftiefe deutlich erhöht werden. Abhängig vom definierten Prüfumfang kann bei einer IS-Partialrevision eine stichprobenbasierte Prüfung oder eine vollständige Prüfung aller zutreffenden Anforderungen des IT-Grundschutz sinnvoll sein. Darüber hinaus gelten die gleichen Regelungen und Abläufe wie bei der IS-Querschnittsrevision.

2.4 Grundsätze der IS-Revision

Das IS-Revisionsteam ist unabhängig und objektiv. Es unterstützt die Institution bei der Erreichung ihrer Ziele, indem das Team mit einem systematischen und zielgerichteten Ansatz die Effektivität des Sicherheitsprozesses bewertet und diesen zu verbessern hilft.

Grundvoraussetzung für jede Revision, somit auch für die IS-Revision, ist ein uneingeschränktes Informations- und Einsichtnahmerecht. Dies bedeutet, dass dem IS-Revisionsteam keine Informationen vorenthalten werden dürfen. Dies beinhaltet auch die Einsichtnahme in sensible oder amtlich geheimgehaltene Informationen, die das Informationssicherheitsmanagement und den IT-Betrieb betreffen, sofern das IS-Revisionsteam einen entsprechenden Bedarf glaubhaft machen kann. Das IS-Revisionsteam muss im letzten Fall entsprechend der „Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen“ (VSA – siehe [BMI3]) bzw. dem Handbuch für den Geheimschutz in der Wirtschaft (siehe [BMWI]) sicherheitsüberprüft und ermächtigt sein, wobei die Stufe der Sicherheitsüberprüfung vom Vertraulichkeitsgrad der betreffenden Informationen abhängig ist.

Das Referenzwerk für IS-Revisionen ist das IT-Grundschutz Kompendium (siehe [GSK]) und die BSI-Standards (siehe [BSI]). Insoweit diese Werke zu den eingesetzten technischen Systemen keine Aussage treffen, sind die BSI Umsetzungshinweise zu den Anforderungen und andere einschlägige Vorschriften, Gesetze, Standards oder Vorgaben durch Hersteller zu verwenden. Die Nutzung dieser Regelwerke ist zu dokumentieren und zu begründen.

Jedes IS-Revisionsteam sollte zur Gewährleistung der Unabhängigkeit und Objektivität aus mindestens zwei IS-Revisoren bestehen („4-Augen-Prinzip“). Wesentliche Besprechungen für die IS-Revision, wie z. B. das Auftaktgespräch und das Abschlussgespräch sowie Interviews, sollten möglichst im Team durchgeführt werden. Diese Vorgehensweise dient der Objektivität, Sorgfalt und der Sachlichkeit. Alle Mitglieder des Teams sollten aus Gründen der Unabhängigkeit und Objektivität vorher nicht unmittelbar im geprüften Bereich beratend oder auch ausführend, z. B. bei der Erstellung von Konzepten oder Konfiguration von IT-Systemen, tätig gewesen sein.

Die IS-Revisoren benötigen sowohl breites als auch tiefes Wissen auf dem Gebiet der Informationssicherheit. Eine permanente Weiter- und Fortbildung der IS-Revisoren ist eine Grundvoraussetzung für ihre Arbeit. Sinnvoll ist der Nachweis der Qualifikation durch Zertifikate (z. B. Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz).

Grundsätzlich sollte bereits bei der Initiierung der IS-Revision beachtet werden, dass der laufende Betrieb in der Institution durch die IS-Revision nicht wesentlich gestört wird. IS-Revisoren greifen niemals selbst aktiv in Systeme ein und erteilen auch keine Handlungsanweisungen zu Änderungen am Revisionsgegenstand.

2.5 Berufsethik

Um Vertrauen in eine objektive Prüfung zu schaffen, ist die Einhaltung einer Berufsethik notwendig. Die Berufsethik muss sowohl durch die Einzelpersonen als auch durch die Unternehmen, die Dienstleistungen im Bereich IS-Revision erbringen, eingehalten werden. Sie umfasst folgende Prinzipien (siehe [ZERT]):

- **Rechtschaffenheit und Vertraulichkeit**

  Die Rechtschaffenheit begründet Vertrauen und schafft damit die Grundlage für die Zuverlässigkeit eines Urteils. Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Informationen zu finden sind, ist die Vertraulichkeit der während einer Revision erlangten Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der IS-Revision sicherzustellen. IS-Revisoren beachten den Wert und das Eigentum der erhaltenen Informationen und legen diese nicht ohne entsprechende Befugnis offen, es sei denn, es bestehen dazu rechtliche oder berufliche Verpflichtungen.

- **Fachkompetenz**

  IS-Revisoren übernehmen nur solche Aufgaben, für die sie das erforderliche Wissen, Können und die entsprechende Erfahrung haben und setzen diese bei der Durchführung ihrer Arbeit ein. Sie verbessern kontinuierlich ihre Fachkenntnisse sowie die Effektivität und Qualität ihrer Arbeit.

- **Objektivität und Sorgfalt**

  Ein IS-Revisor hat ein Höchstmaß an sachverständiger Objektivität und Sorgfalt beim Zusammenführen, Bewerten und Weitergeben von Informationen über geprüfte Aktivitäten oder Geschäftsprozesse zu zeigen. Die Beurteilung aller relevanten Umstände hat mit Ausgewogenheit zu erfolgen und darf nicht durch eigene Interessen oder durch Andere beeinflusst werden.

- **Sachliche Darstellung**

  Ein IS-Revisor hat die Pflicht, seinem Auftraggeber wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehören die objektive und nachvollziehbare Darstellung der Sachverhalte in den IS-Revisionsberichten, die konstruktive Bewertung der dargestellten Sachverhalte und die konkreten Empfehlungen zur Verbesserung der Maßnahmen und Prozesse.

- **Nachweise und Nachvollziehbarkeit**

  Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Schlussfolgerungen und Ergebnissen zu kommen, ist die eindeutige und folgerichtige Dokumentation der Sachverhalte. Hierzu gehört auch eine dokumentierte und nachvollziehbare Methodik (IS-Prüfplan, IS-Revisionsbericht), mit der das IS-Revisionsteam zu seinen Schlussfolgerungen kommt.

3 IS-Revision in der Institution

IS-Revisionen sollten regelmäßig durchgeführt werden, dies ist für Bundesbehörden gem. UP Bund 2017 verpflichtend. Dabei sollte ein Zeitraum von 3 Jahren zwischen den einzelnen IS-Revisionen nicht überschritten werden. Daher ist es zweckmäßig, diese in Form eines IS-Revisionsverfahrens in den Informationssicherheitsprozess der Institution zu integrieren. Notwendige organisatorische, personelle und finanzielle Rahmenbedingungen sind sicherzustellen, entsprechende Verantwortlichkeiten und Aufgaben zuzuweisen.

3.1 Grundlagen und Verantwortlichkeiten

Institutionen sollten ihr ISMS regelmäßig überprüfen. Dies geschieht u. a. durch die Etablierung eines IS-Revisionsverfahrens auf Grundlage der von der Institution verabschiedeten Leitlinie zur Informationssicherheit. Das „Lagebild“ über den Informationssicherheitsstatus der Institution kann z. B. durch regelmäßige IS-Revisionen festgestellt werden.

Die Leitungsebene einer Institution trägt immer die Gesamtverantwortung für die IS-Revision. Sie muss regelmäßig über Probleme, Ergebnisse und Aktivitäten der IS-Revision, aber auch über neue Entwicklungen, geänderte Rahmenbedingungen oder Verbesserungsmöglichkeiten informiert werden, um ihrer Steuerungsfunktion nachkommen zu können.

Zur Begleitung des Gesamtprozesses und bei der konkreten Durchführung von IS-Revisionen in der Institution ist ein Verantwortlicher für IS-Revisionen zu benennen (z. B. der Informationssicherheitsbeauftragte). Dieser sollte:

- über eine unabhängige Stellung in der Aufbauorganisation der Institution (Vermeidung von Interessenskonflikten),
- ein unmittelbares Vorspracherecht bei der Leitung der Institution sowie
- über ausreichende Kenntnisse der Informationssicherheit, insbesondere der Vorgehensweise nach IT-Grundschutz, verfügen.

Aufgabe des Verantwortlichen für IS-Revisionen in der Institution ist die Erstellung einer mehrjährigen Grobplanung für das IS-Revisionsvorhaben anhand des vorliegenden Leitfadens, die durch eine jährliche Detailplanung konkretisiert werden sollte. Darüber hinaus ist er zentraler Ansprechpartner des IS-Revisionsteams während der gesamten Dauer der IS-Revision und insbesondere verantwortlich für die Bereitstellung der Referenzdokumente (siehe Kapitel 4.2) sowie für die Koordinierung von Terminen und personellen/materiellen Ressourcen während der Vor-Ort-Prüfung.

Die Festlegungen bezüglich IS-Revisionsverfahren und Aufgabenzuweisungen sind in einem IS-Revisionshandbuch individuell zu dokumentieren. Dieses sollte folgende Aspekte enthalten:

- angestrebte strategische Ziele der IS-Revision,
- evtl. einzuhaltende gesetzliche Vorgaben und Verordnungen,
- Organisation der IS-Revision innerhalb der Institution,
- Ressourcen (zeitlich, finanziell, personell),
- innerbehördliche Rahmenbedingungen und
- Archivierung der Dokumentation.

Das IS-Revisionshandbuch ist die zentrale Arbeitgrundlage und Handlungsanweisung für die IS-Revision. Da es Rechte und Pflichten der an einer IS-Revision Beteiligten sowie das Informations- und Einsichtnahmerecht des IS-Revisionsteams regelt, sollte vor dessen Verabschiedung durch die Leitungsebene die Personalvertretung beteiligt werden.

Auf Basis des IS-Revisionshandbuchs werden die geplanten IS-Revisionen von einem internen oder externen IS-Revisionsteam (siehe Kapitel 3.3) durchgeführt und von dem Verantwortlichen für IS-Revisionen in der Institution begleitet. Die resultierenden IS-Revisionsberichte sind Grundlage für Folgeaktivitäten zur Aufrechterhaltung und Verbesserung der Informationssicherheit.

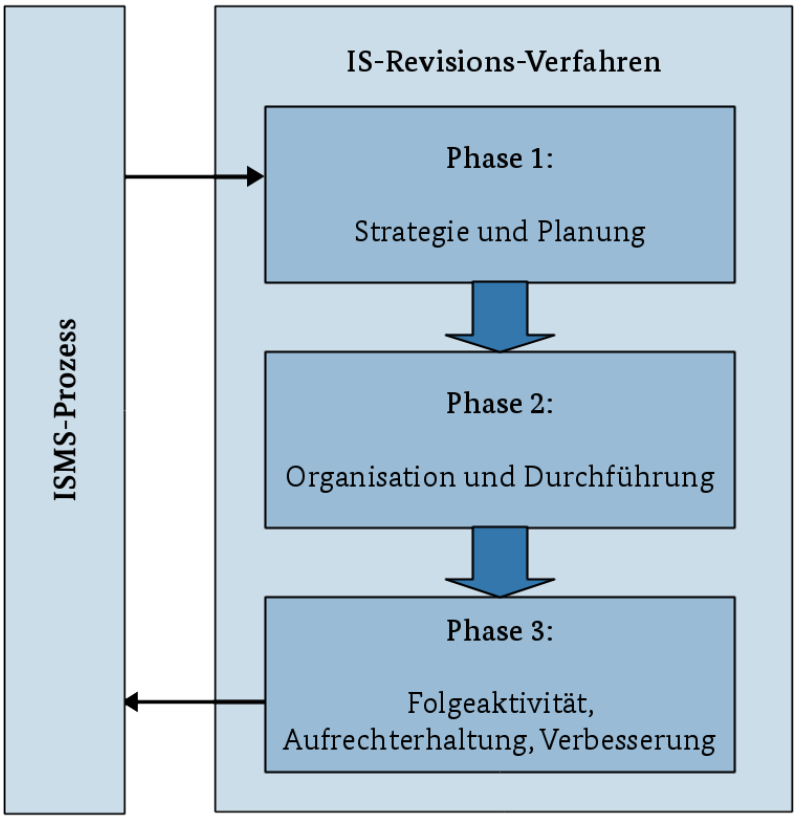

Abbildung 4: Phasen des IS-Revisionsverfahren aus Sicht der Institution

3.2 Planung von einzelnen IS-Revisionen

Grundlage für die Planung und Durchführung von IS-Revisionen ist das Verständnis der Geschäftsprozesse und Risiken der Institution. Die zu erstellende Grob- sowie die detaillierte Jahresplanung berücksichtigt den Schutzbedarf der Geschäftsprozesse der Institution sowie der eingesetzten IT. Für IS-Revisionen nach unvorhergesehenen Sicherheitsvorfällen sollten Reserven in der jährlichen Ressourcenplanung vorgesehen werden.

Grundsätzlich ist es auch möglich, eine IS-Revision nach Standorten zu teilen. Dabei ist sicherzustellen, dass die Anforderungen des UP Bund 2017 und dieses Leitfadens weiterhin erfüllt werden. Bei einer Teilung der IS-Revision in mehrere Aufträge sind die hieraus resultierenden IS-Revisionsberichte von einer unabhängigen Stelle zu einem Gesamtbericht zusammenzuführen.

Eine IS-Querschnittsrevision kann erst dann sinnvoll durchgeführt werden, wenn eine Strukturanalyse und Modellierung gemäß IT-Grundschutz (siehe [BSI2]) für die Institution vorliegt. Hierzu gehört, dass:

- die Geschäftsprozesse, Anwendungen und Informationen der Institution erfasst wurden,
- der Netzplan vorhanden ist,
- IT-Systeme und ähnliche Objekte (z. B. Router, Switch, Drucker, Fax) sowie
- die Räumlichkeiten erfasst wurden und
- die IT-Grundschutzbausteine diesen zugeordnet wurden.

Die Institution hat ebenso zu berücksichtigen, dass für eine IS-Querschnittsrevision eine konsistente Modellierung vorliegen muss. Strukturanalyse und Modellierung sind Basisaufgaben des Sicherheitsmanagements und gehören zum Sicherheitskonzept, welches gemäß UP Bund von Bundesbehörden zwingend zu erstellen und konsequent umzusetzen ist.

Der durch eine IS-Revision verursachte interne Aufwand bei Nutzung eines externen Sicherheitsdienstleisters beschränkt sich i.d.R. auf die Zusammenstellung der vorhandenen Dokumente, die Organisation und Koordinierung der IS-Revision, Interviewzeiten der Ansprechpartner und die Auswertung des IS-Revisionsberichts.

IS-Revisionszyklen

- Gemäß UP Bund 2017 sind Bundesbehörden verpflichtet, in regelmäßigen Abständen IS-Revisionen durchzuführen.
- Zwischen den einzelnen IS-Revisionen sollte ein Zeitraum von 3 Jahren nicht überschritten werden.
- Vor der erstmaligen Durchführung einer IS-Querschnittsrevision sollte eine IS-Kurzrevision erfolgen, um zu überprüfen, ob die wesentlichen Voraussetzungen für eine IS-Querschnittsrevision vorliegen.
- Zusätzlich sind IS-Partialrevisionen für kritische Geschäftsprozesse einzuplanen. Kritische Geschäftsprozesse, insbesondere solche, die Hochverfügbarkeit nach dem BSI-Kompendium „Hochverfügbarkeit“ erfordern, sollten in der jeweiligen Kritikalität angemessenen Zeitabständen einer IS-Partialrevision unterzogen werden.
- Weitere IS-Partialrevisionen können z. B. als vertiefende Prüfung, nach Sicherheitsvorfällen, nach Einführung neuer Verfahren oder nach Umstrukturierungen durchgeführt werden.

Begleitung einer IS-Revision

Der Verantwortliche für IS-Revisionen ist auch Kontaktperson und Ansprechpartner während der Durchführung einer IS-Revision. Er unterstützt das IS-Revisionsteam bei organisatorischen und fachlichen Fragen (z. B. bei der Organisation von Besprechungen, bei der Zusammenstellung von Dokumenten und bei der Betreuung der Vor-Ort-Prüfung).

Im nachfolgenden Ablaufdiagramm sind die organisatorischen Aufgaben des Verantwortlichen für IS-Revisionen in der Institution zusammengestellt.

Abbildung 5: Durchführung der IS-Revision aus Sicht der Institution

3.3 IS-Revisionsteam

Zur konkreten Durchführung einer IS-Revision ist ein geeignetes IS-Revisionsteam zusammenzustellen. Die Mitglieder dieses IS-Revisionsteams sollten sowohl über entsprechende fachliche als auch persönliche Qualifikationen verfügen. Aspekte, die bei der Auswahl eines IS-Revisionsteams beachtet werden sollten, sind in Kapitel 2.4 und 2.5 dargestellt. Für die Zusammenstellung eines IS-Revisionsteams in der Institution bestehen unterschiedliche Möglichkeiten:

Internes IS-Revisionteam:

Je nach Ausrichtung und Größe der Institution kann es sinnvoll sein, ein eigenes IS-Revisionteam aufzubauen, d. h. innerhalb der Institution eine Personengruppe mit der Durchführung von IS-Revisionen zu beauftragen. Dies hat den Vorteil, dass Wissen über Organisationsstrukturen und Verfahrensabläufe vorhanden ist. Allerdings verfügen viele Institutionen nicht über das erforderliche Know-how und/oder die notwendigen personellen Ressourcen, um eine effektive und unabhängige Durchführung der IS-Revision zu gewährleisten. Falls das IS-Revisionsteam aus eigenen Mitarbeitern besteht, ist es empfehlenswert, diese organisatorisch als Stabsfunktion einzubinden. Ein direktes Vorspracherecht bei der Leitung sowie die fachliche Unabhängigkeit müssen gewährleistet sein (siehe Kapitel 2.4).

Kooperationen von IS-Revisionsteams:

Da nicht alle Institutionen die Bildung eines vollständigen, internen IS-Revisionsteams leisten können, kann eine Zusammenarbeit mit anderen Institutionen sinnvoll sein. Eine denkbare Lösung zur Abdeckung aller benötigten Themenbereiche können Kooperationsabkommen mit anderen Institutionen sein, um IS-Revisoren auszutauschen.

Ressort-IS-Revisionsteam:

Eine weitere Alternative für die Bundesverwaltung kann die Einrichtung von IS-Revisionsteams bzw. Kompetenzzentren innerhalb eines Ressorts sein. Die IS-Revisionsteams könnten zentral, auf Ebene der obersten Bundesbehörden eingerichtet werden. Die Behörden haben so die Möglichkeit, auf kompetente IS-Revisionsteams mit ressortspezifischen Kenntnissen zurückzugreifen. Eine Auskunft, ob in bestimmten Ressorts bereits IS-Revisionsteams existieren, kann der jeweilige Ressort-IT-Sicherheitsbeauftragte geben.

BSI-IS-Revisionsteam:

Von Bundesbehörden kann die entsprechende, grundsätzlich kostenfreie Dienstleistung des BSI in Anspruch genommen werden. Bei Ressourcenengpässen haben Sicherheitsbehörden Vorrang. Nähere Informationen zur Dienstleistung IS-Revision des BSI finden Sie auf unseren Webseiten (www.bsi.bund.de). Zur Terminkoordination und für Fragen steht das BSI unter sicherheitsberatung@bsi.bund.de zur Verfügung.

Die Antragstellung zur Durchführung einer IS-Revision erfolgt durch die Leitung der Institution (Antragsformular unter
https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISRevision/isrevision_node.html - Menüpunkt "Hilfsmittel").

Externer Dienstleister „IS-Revision“:

Auch externe Dienstleister bieten IS-Revisionen an. Bundesbehörden sollten auf vom BSI zertifizierte IT-Sicherheitsdienstleister zurückgreifen. Das entsprechende Zertifizierungsverfahren für Unternehmen sowie die Zusatzschulung zum IS-Revisor für Auditoren wird vom BSI in regelmäßigen Abständen angeboten.

Das BSI veröffentlicht eine Liste aller beim BSI zertifizierten IT-Sicherheitsdienstleister. In einem Zertifizierungsverfahren haben diese Dienstleister ihre Vertrauenswürdigkeit und Fachkompetenz gegenüber dem BSI nachgewiesen.

https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/IS_REV_PEN/IS_REV_Dienstleister/IS_REV_Dienstleister_node.html

3.4 Ausschreibungsverfahren

Falls sich die zu prüfende Institution für einen externen Dienstleister entschieden hat, sollten insbesondere Bundesbehörden bei der Ausschreibung neben den üblichen Vergabevorschriften zusätzlich folgende Aspekte in der Ausschreibung berücksichtigen:

- Die IS-Revision erfolgt auf Basis des aktuellen „Leitfadens für IS-Revisionen auf der Basis von IT-Grundschutz“.
- Die Art der Revision, IS-Kurzrevision, IS-Querschnittsrevision oder IS-Partialrevision, ist zu benennen. Bei der IS-Partialrevision ist zusätzlich der Prüfgegenstand genau einzugrenzen (z. B. Verfahren, Systeme, Netze, Außenstellen, Informationsverbund).
- Der Zeitrahmen, innerhalb dessen die IS-Revision stattfinden soll, ist zu definieren.
- Ggf. sind Abbruchkriterien zu definieren (z. B. wenn die Voraussetzungen für eine IS-Querschnittsrevision fehlen, siehe auch Kapitel 4.2.2).
- Bundesbehörden sollten auf vom BSI zertifizierte IT-Sicherheitsdienstleister zurückgreifen.

Der Prüfgegenstand sollte detailliert beschrieben werden. Hierzu gehören:

- die Beschreibung der Institution allgemein (Lage, Anzahl der Außenstellen, Anzahl der Mitarbeiter, Aufgaben / Ziele der Institution),
- die Nennung der wesentlichen Aufgaben und Prozesse der Institution / des zu prüfenden Bereichs / des zu prüfenden Informationsverbundes,
- ggf. die Aufzählung der Standorte der zu prüfenden Institution,
- die Beschreibung der eingesetzten IT-Systeme, -Anwendungen und -Verfahren,
- die Art der Vernetzung im zu prüfenden Bereich,
- die Anzahl der Kritischen Geschäftsprozesse und
- die Nennung von ausgelagerten Geschäftsprozessen und IT-Systemen (Outsourcing), die mit zum Prüfungsgegenstand gehören.

Von dem Dienstleister bzw. dem IS-Revisionsteam sollten folgende Anforderungen erfüllt werden (siehe hierzu auch Kapitel 2.4 und 2.5):

- breite IT-Sicherheitskenntnisse,
- tiefe Kenntnisse des IT-Grundschutzes,
- Erfahrungen bei Informationssicherheitsrevisionen sowie
- spezifische Fachkenntnisse in dem Prüfungsbereich.

Da bereits im Ausschreibungsverfahren für eine IS-Revision ggf. sensible Daten der Institution bekannt werden, ist je nach Tätigkeitsumfeld der Institution eine beschränkte Ausschreibung bzw. ein Teilnahmewettbewerb durchzuführen, um die Vertraulichkeit der Informationen zu gewährleisten.

Je nach Schutzbedarf der Informationen müssen Dienstleister und IS-Revisoren ihre Vertrauenswürdigkeit gemäß dem „Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes“ (SÜG – siehe [SÜG]) nachweisen können. Die Ermächtigung zur Einsichtnahme in Verschlusssachen ist bei Bedarf durch die Vorlage einer gültigen Konferenzbescheinigung zu belegen.

Vertraglich ist zusätzlich festzulegen, welche erhobenen Daten vom Auftragnehmer nach der IS-Revision zu vernichten, zu verwahren oder zu übergeben sind. Es sollte eine Geheimhaltungsvereinbarung (Non-Disclosure-Agreement) zwischen der Institution und dem Auftragnehmer abgeschlossen werden.

Die vorgesehene IS-Revisionsdauer wird bereits vorab von der Institution in der Ausschreibung festgelegt.

Aufwand für eine IS-Kurzrevision

Bei der IS-Kurzrevision ist von geringen zeitlichen Aufwänden auszugehen. In der Praxis zeigte sich, dass eine Institution grundsätzlich innerhalb von 6 bis 8 Personentagen (bezogen auf ein Revisionsteam von 2 Personen) überprüft werden kann. Diese Zeitangabe beinhaltet bereits die Aufwände für die Dokumentenprüfung, Vor-Ort-Prüfung, Reisezeiten und Berichterstellung. Bei Institutionen mit mehreren Standorten ist mit zusätzlichem Aufwand zu rechnen.

Aufwand für eine IS-Querschnittsrevision

Die Dauer einer IS-Querschnittsrevision ist sowohl von der Größe als auch der Komplexität der Institution abhängig. Die Größe der Institution wird durch die Anzahl der Mitarbeiter und Standorte bestimmt, wobei beide Aspekte auch für sich allein betrachtet zu einem höheren Prüfaufwand führen können. Der Faktor

Komplexität wird in die drei Stufen „normal“, „hoch“ und „sehr hoch“ eingeteilt. Eine Zuordnung der Institution zu einer Komplexitätsstufe kann nur individuell z. B. anhand der folgenden Kriterien ermittelt werden:

- Wie ist die Systemlandschaft (Anzahl der Systeme und Heterogenität der eingesetzten Systeme)?
- Wie viele Netzübergänge gibt es?
- Welche und wie viele IT-Anwendungen werden in der Institution eingesetzt? Werden damit kritische Geschäftsprozesse unterstützt?
- Werden übergeordnete Verfahren eingesetzt, die Einfluss auf Bereiche außerhalb der Institution haben?
- Wie hoch ist der Schutzbedarf für Infrastruktur, Systeme und IT-Anwendungen?
- Handelt es sich um eine Institution, die in sicherheitskritischen Bereichen (z. B. Sicherheitsbehörden) tätig ist?

Zur Abschätzung des Gesamtaufwands für eine IS-Querschnittsrevision nach UP Bund (siehe Kapitel 4 „Durchführung einer IS-Revision“) können folgende, auf Erfahrungswerten beruhende Richtwerte für Personalressourcen des IS-Revisionsteams als Orientierung dienen:

	Größe der Institution: Klein bis 100 Mitarbeiter	**Größe der Institution: Mittel bis 500 Mitarbeiter**	**Größe der Institution: Groß über 500 Mitarbeiter**
Komplexität „normal“	30 Personentage	50 Personentage	60 Personentage
Komplexität „hoch“	50 Personentage	65 Personentage	80 Personentage
Komplexität „Sehr hoch“	60 Personentage	80 Personentage	100 Personentage

Tabelle 1: Richtwerte für den Personalaufwand bei einer IS-Querschnittsrevision

Hier handelt es sich um eine grobe Abschätzung auf Grundlage der bisherigen Revisionstätigkeiten des BSI und anderer Behörden. Sie kann nicht auf die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz übertragen werden.

Bei der Festlegung der Dauer einer IS-Querschnittsrevision sind keine Verzögerungen z. B. durch Wartezeiten auf Dokumente oder terminliche Verzögerungen berücksichtigt. Die Zeiten sind nur grobe Richtwerte, die an die tatsächlichen Gegebenheiten der Institution anzupassen sind. Es wird davon ausgegangen, dass die IS-Revision von einem versierten IS-Revisionsteam durchgeführt wird.

Aufwand für eine IS-Partialrevision

Die Aufwand einer IS-Partialrevision hängt stark von der Komplexität des zu prüfenden Ausschnitts der Institution, den Prüfmethoden und der vorgesehenen Prüftiefe ab. Richtwerte können daher nicht vorgegeben werden.

3.5 Nachbereitung einer IS-Revision

Die Ergebnisse der IS-Revision werden der Leitung der Institution, dem Verantwortlichen für IS-Revisionen sowie dem Informationssicherheitsbeauftragten berichtet (siehe Kapitel 4.1.1) und fließen in den ISMS-Prozess ein. Hierzu sollte ein klar definiertes Verfahren existieren, das in einer Richtlinie zur Überprüfung und Verbesserung des Sicherheitsprozesses niedergelegt ist (siehe [BSI2]). Aus der Auswertung des IS-Revisionsberichts ergeben sich Anforderungen zur Mängelbeseitigung und Qualitätsverbesserung. Der Informationssicherheitsbeauftragte leitet daraus die entsprechenden Folgeaktivitäten ab. Dazu gehört auch, die Sicherheitsdokumente, wie z. B. Sicherheitsrichtlinien und IT-Grundschutzcheck, zu aktualisieren. Im Einzelfall können ergänzende IS-Partialrevisionen erforderlich sein. Die Grob- und Detailplanung der IS-Revision ist anzupassen.

Die durchgeführten IS-Revisionen, deren Ergebnisse sowie eine Zusammenfassung der Aktivitäten zur Mängelbeseitigung und Qualitätsverbesserung sind in den regelmäßigen Berichten des Informationssicherheitsbeauftragten an die Leitungsebene aufzunehmen.

4 Durchführung einer IS-Revision

Die folgenden Abschnitte erläutern die Aufgaben des IS-Revisionsteams bei der Durchführung einer IS-Revision von der Initiierung bis zum Abschluss des Projektes. Die für die Institution anfallenden Arbeiten sind im Kapitel 3 näher beschrieben.

4.1 Allgemeines zur Durchführung von IS-Revisionen

Mit den nachfolgend dargestellten Prüfverfahren soll eine einheitlich hohe Qualität von IS-Revisionen erzielt und die Vergleichbarkeit der Revisionsergebnisse gewährleistet werden. In allen Schritten ist das Revisionsvorgehen vom IS-Revisionsteam nachvollziehbar und ordnungsgemäß zu dokumentieren.

Der IS-Revisionsbericht, als Zusammenfassung aller Sicherheitsmängel, ist mindestens als „VS – Nur für den Dienstgebrauch“ einzustufen. Die individuelle Einstufung ist ggf. mit der Amtsleitung der zu prüfenden Institution, den betroffenen Fachreferaten und ggf. in Kooperation mit dem Geheimschutzbeauftragten festzulegen.

Das IS-Revisionsverfahren wird mit der Auftragserteilung durch die Leitung der zu prüfenden Institution initiiert.

4.1.1 Vorgehensweise IS-Revision

Schritt 1

Zu Beginn des Verfahrens werden in einem Auftaktgespräch wesentliche Rahmenbedingungen der IS-Revision zwischen Institution und IS-Revisionsteam abgestimmt und erforderliche Dokumente angefordert.

Schritt 2

Auf Grundlage der dann vorliegenden Dokumente verschafft sich das IS-Revisionsteam einen Überblick über die zu prüfende Institution und erstellt den IS-Prüfplan.

Schritt 3

Anhand des IS-Prüfplans werden die vorliegenden Dokumente einer inhaltlichen Prüfung unterzogen. Gegebenenfalls werden weitere Dokumente nachgefordert.

Auf Basis der Dokumentenprüfung und des dabei fortgeschriebenen IS-Prüfplans wird die Vor-Ort-Prüfung gemeinsam mit dem Ansprechpartner der Institution zeitlich und organisatorisch koordiniert.

Schritt 4

Die Vor-Ort-Prüfung beginnt mit einem Eröffnungsgespräch mit den Hauptbeteiligten. Dann folgen Interviews und Inaugenscheinnahmen sowie eine vorläufige Auswertung. Beendet wird die Vor-Ort-Prüfung mit einem Abschlussgespräch.

Schritt 5

Die Informationen, die während der Vor-Ort-Prüfung erhoben wurden, werden vom IS-Revisionsteam weiter konsolidiert und ausgewertet.

Schritt 6

Die Ergebnisse der IS-Revision werden am Ende der Prüfung in einem IS-Revisionsbericht zusammengefasst. Dieser wird der geprüften Institution bekannt gegeben. Bei Bedarf erläutert das IS-Revisionsteam der Leitungsebene im Rahmen einer Abschlusspräsentation die IS-Revisionsergebnisse.

Die Vorgehensweise ist im folgenden Diagramm abgebildet:

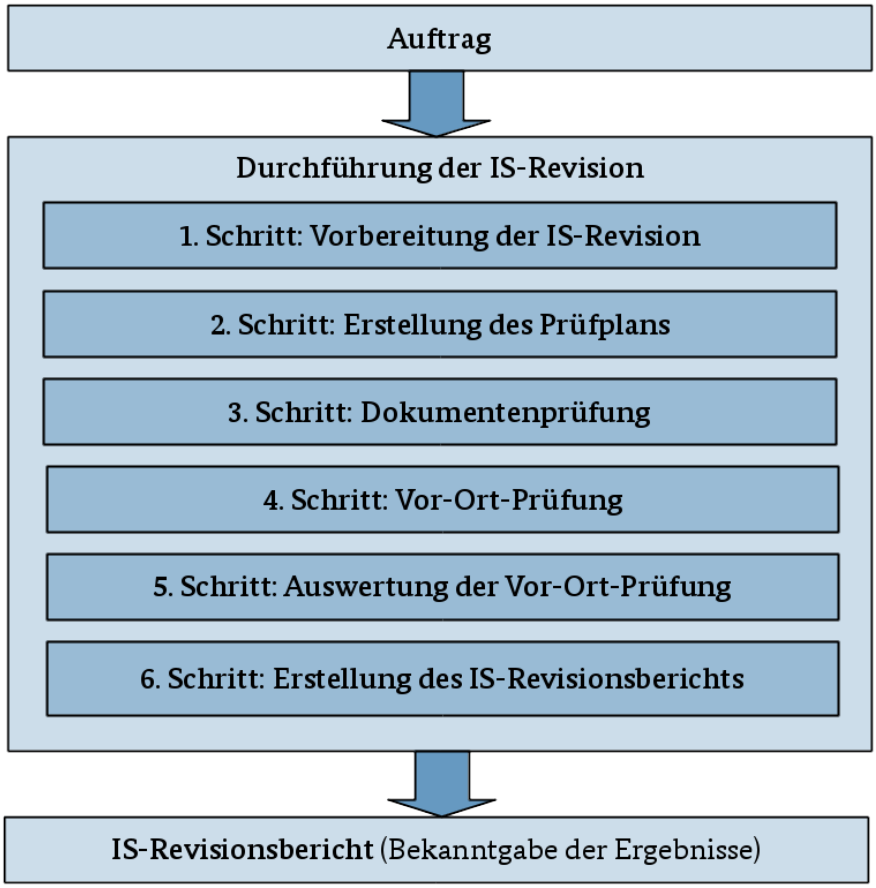

Abbildung 6: Schritte bei der Durchführung einer IS-Revision

4.1.2 Prüfmethoden

Unter „Prüfmethoden“ werden alle für die Ermittlung eines Sachverhaltes verwendeten Methoden verstanden. Während einer IS-Revision können folgende unterschiedliche Prüfmethoden genutzt werden:

- 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. Logfiles, Auswertung von Datenbanken etc.) und
- schriftliche Befragung (z. B. Fragebogen).

Welche Prüfmethoden angewendet werden, hängt vom konkreten Fall ab und ist durch das IS-Revisionsteam festzulegen. Das IS-Revisionsteam hat zu beachten, dass bei allen Prüfungen der Grundsatz der Verhältnismäßigkeit eingehalten wird.

Stellt das IS-Revisionsteam bei der Prüfung einer ausgewählten Stichprobe Abweichungen zum dokumentierten Status fest, erweitert es bedarfsorientiert die Stichprobe zur Sachverhaltsklärung. Es schließt die Prüfung erst ab, sobald der Sachverhalt ausreichend geklärt ist. Für die Sachverhaltsermittlung können mehrere Prüfmethoden kombiniert zur Anwendung kommen.

Die konkrete Durchführung einer IS-Revision wird im folgenden Kapitel zunächst anhand der umfassendsten Revisionsart, der IS-Querschnittsrevision beschrieben. Für die IS-Partialrevision (Kapitel 4.3) und IS-Kurzrevision (Kapitel 4.4) werden dann die Abweichungen hiervon dargestellt.

4.2 Die IS-Querschnittsrevision

Wesentliche Voraussetzung für die Durchführung einer IS-Querschnittsrevision ist, dass der Informationssicherheitsprozess etabliert ist und dass mindestens die folgenden Dokumentationen in der Institution vorliegen:

- eine Strukturanalyse gemäß BSI-Standard 200-2 (siehe [BSI2] Kapitel 8.1),
- ein vollständiger und aktueller Netzplan,
- die Modellierung (siehe [BSI2] Kapitel 8.3) und
- die Schutzbedarfsfeststellung (siehe [BSI2] Kapitel 8.2).

Falls das IS-Revisionsteam bei der Dokumentenanforderung oder den nachfolgenden Schritten feststellt, dass wesentliche Voraussetzungen für eine IS-Querschnittsrevision fehlen, ist die IS-Revision abzubrechen.

4.2.1 Bewertungsschema

Die festgestellten Sachverhalte zu jeder geprüften Maßnahme sind im IS-Prüfplan (siehe Kapitel 5 „Hilfsmittel“) aufzunehmen und hinsichtlich des Umsetzungsstatus zu bewerten.

Die Bewertung im ersten Schritt erfolgt angelehnt an den IT-Grundschutz-Check nach einem einheitlichen Bewertungsschema (siehe [GSK]):

- Anforderung erfüllt,
  „Zu der Anforderung wurden geeignete Maßnahmen vollständig, wirksam und angemessen umgesetzt“,
- Anforderung teilweise erfüllt,
  „Einige Maßnahmen zur Erfüllung der Anforderung wurden umgesetzt, andere noch nicht oder nur teilweise.“,
- Anforderung nicht erfüllt,
  „Geeignete Maßnahmen zur Erfüllung der Anforderung wurden größtenteils noch nicht umgesetzt“,
- Anforderung entbehrlich,
  „Die Erfüllung der Anforderung ist in der vorgeschlagenen Art nicht notwendig, weil die Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden) oder durch Alternativmaßnahmen behandelt wird)“.

Sind Anforderungen nicht oder nur teilweise erfüllt, so hat das IS-Revisionsteam spätestens bei der IS-Revisionsberichtserstellung zu beurteilen, ob dadurch ein Sicherheitsmangel oder ein schwerwiegender Sicherheitsmangel für die Institution vorliegt.

Folgende Kriterien sind für die Bewertung im zweiten Schritt zu beachten:

- kein Sicherheitsmangel
  Es liegt kein Sicherheitsmangel vor, wenn geeignete Maßnahmen zur Erfüllung der Anforderung vollständig, wirksam und angemessen umgesetzt wurden. Es gibt keine ergänzenden Hinweise.
- Sicherheitsempfehlung
  Eine Sicherheitempfehlung kann vorliegen, wenn einige der Maßnahmen zur Erfüllung der Anforderung umgesetzt sind, andere noch nicht oder nur teilweise. Auch eine vollständig erfüllte Anforderung kann mit einer Sicherheitsempfehlung versehen werden.
  Durch die Umsetzung der im Sachverhalt beschriebenen Maßnahmenempfehlungen kann die Sicherheit erhöht werden. Sicherheitsempfehlungen können Verbesserungsvorschläge für die Umsetzung von Maßnahmen sein, ergänzende Maßnahmen, die sich in der Praxis bewährt haben, oder Kommentare hinsichtlich der Angemessenheit von Maßnahmen.
  Eine teilweise oder nicht erfüllte Anforderung darf nur dann als Sicherheitsempfehlung eingestuft werden, wenn das IS-Revisionsteam davon ausgehen kann, dass mittelfristig nicht mit einer Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit der Daten zu rechnen ist.
- Sicherheitsmangel
  Bei einem „Sicherheitsmangel" liegt eine Sicherheitslücke vor, die mittelfristig behoben werden muss. Die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen kann beeinträchtigt werden. Hierunter fällt zum Beispiel auch eine unzureichende oder fehlende Dokumentation, die in einer Anforderung gefordert wird.
- Schwerwiegender Sicherheitsmangel
  Ein „schwerwiegender Sicherheitsmangel" ist eine Sicherheitslücke, die unverzüglich geschlossen werden muss, da die Vertraulichkeit, die Integrität oder die Verfügbarkeit der Informationen stark gefährdet ist und erheblicher Schaden zu erwarten ist.

Sicherheitsmängel und -empfehlungen sind bei den betroffenen Anforderungen im IS-Revisionsbericht zu dokumentieren. Wird ein Sicherheitsmangel als schwerwiegend bewertet, so ist dies im IS-Revisionsbericht nachvollziehbar zu begründen.

Bewertung – Umsetzungsstatus (Schritt 1)	**Bewertung – Sicherheitsmangel (Schritt 2)**
Anforderung nicht erfüllt	Sicherheitsmangel oder schwerwiegender Sicherheitsmangel
Anforderung teilweise erfüllt	Sicherheitsmangel oder schwerwiegender Sicherheitsmangel
Anforderung erfüllt	Kein Sicherheitsmangel oder Sicherheitsempfehlung
Anforderung entbehrlich	Kein Sicherheitsmangel oder Sicherheitsempfehlung

Tabelle 2: Bewertung nach Umsetzungsstatus und Sicherheitsmangel

Mit dem zweigliedrigen Bewertungsschema (Umsetzungsstatus und Sicherheitsmangel) erhält das IS-Revisionsteam ein Instrument, das die schnelle und differenzierte Visualisierung des aktuellen Informationssicherheitsstatus der Institution ermöglicht. Die Institution kann mittels der Anzahl der Anforderungen deren Erfüllung bemängelt wurden, sortiert nach Schicht und Schweregrad des Sicherheitsmangels, den Sicherheitsstatus in der jeweiligen IT-Grundschutzschicht erkennen. Daraus ist zu folgern, in welchen Bereichen verstärkte Aktivitäten hinsichtlich Informationssicherheit erfolgen müssen. Weiterhin kann über mehrere Jahre die Entwicklung des Status der Informationssicherheit in der Institution nachverfolgt werden.

4.2.2 Vorbereitung der IS-Revision (Schritt 1)

Bei der Initiierung einer IS-Revision (z. B. durch den Informationssicherheitsbeauftragten oder den Verantwortlichen für IS-Revisionen) ist die Leitung der zu prüfenden Institution zu beteiligen. In diesem Stadium wird der Prüfgegenstand festgelegt, der Auftrag vergeben und das beauftragte IS-Revisionsteam mit den notwendigen Befugnissen (z. B. Einsichtnahmerechte) ausgestattet.

Die Leitung der Institution sollte den Betriebs- bzw. Personalrat über die geplante IS-Revision informieren.

Das IS-Revisionsteam führt mit den Ansprechpartnern der zu prüfenden Institution ein Auftaktgespräch. In diesem Gespräch wird das IS-Revisionsverfahren erläutert und dargestellt, welche Aufgaben auf die zu prüfende Institution während der IS-Revision zukommen. Der Verantwortliche in der Institution hingegen sollte den IS-Revisoren die Aufgabenschwerpunkte der Institution erläutern und einen kurzen Überblick über die eingesetzte IT geben. Erste Rahmenbedingungen der Vor-Ort-Prüfung sind abzustimmen (wann, an welchem Standort, organisatorische Fragen etc.).

Die folgenden Referenzdokumente müssen von der geprüften Institution dem IS-Revisionsteam zur Verfügung gestellt werden und bilden die Grundlage für die IS-Revision:

Organisatorische Dokumente

- Organigramm,
- IT-Rahmenkonzept und
- Geschäftsverteilungsplan.

Fachbezogene Dokumente

- Sicherheitskonzept
  Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess und sollte mindestens die Strukturanalyse, den Netzplan, die Schutzbedarfsfeststellung, die Modellierung nach IT-Grundschutz, den IT-Grundschutz-Check und die Risikoanalyse enthalten. Ebenso sind die Entscheidungen zur Behandlung von Risiken und die Realisierungspläne der sich daraus ergebenden, ergänzenden Maßnahmen beizufügen (siehe [BSI2]).
- Export der Informationssicherheitsmanagement-Datenbank, falls vorhanden.
- Leitlinie zur Informationssicherheit
  Die Leitungsebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Organisation und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Informationssicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zu Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.
- Liste der kritischen Geschäftsprozesse
  Es ist eine Liste mit den kritischen Geschäftsprozessen vorzulegen. Die Liste der kritischen Geschäftsprozesse ist insbesondere wichtig für die Auswahl der Zielobjekte und die weitere Ausarbeitung des IS-Prüfplans unter Berücksichtigung des risikoorientierten Ansatzes.
- die IS-Revisionsberichte der vorherigen sechs Jahre (soweit vorhanden).

Unabhängig von den aufgezählten Dokumenten kann das IS-Revisionsteam bei Bedarf weitere Dokumente in Papier oder elektronischer Form anfordern.

4.2.3 Erstellung des IS-Prüfplans und Dokumentensichtung (Schritt 2)

Alle Referenzdokumente werden auf Aktualität und Vollständigkeit geprüft.

Bei der Beurteilung der Aktualität der Dokumente ist zu beachten, dass einige Dokumente allgemeiner formuliert sind als andere, so dass Änderungen in den Dokumenten unterschiedlich häufig vorgenommen werden müssen. Die Institution muss alle Dokumente jedoch regelmäßig bewerten, ob sie noch den aktuellen Gegebenheiten entsprechen. Das IS-Revisionsteam überprüft diese Vorgehensweise anhand der Sichtung von Dokumenten und gegebenenfalls durch Abgleich bei der Vor-Ort-Prüfung.

Hinsichtlich der Vollständigkeit ist inhaltlich zu prüfen, ob alle wesentlichen Aspekte erfasst wurden bzw. ob geeignete Rollen zugewiesen wurden. Die vorgelegten Dokumente müssen für das IS-Revisionsteam nachvollziehbar sein. Insbesondere Entscheidungen sollten nachvollziehbar begründet werden.

Mit der Dokumentensichtung verschafft sich das IS-Revisionsteam einen Überblick über die wesentlichen Aufgaben, die Organisation und den IT-Einsatz in der zu prüfenden Institution. Auf dieser Grundlage beginnt das IS-Revisionsteam mit der Erstellung des IS-Prüfplans. Dieser ist das wesentliche Arbeitsmittel für die gesamte Prüfung, in dem alle Prüfungshandlungen während der IS-Revision dokumentiert werden.

Grundlage zur Erstellung des IS-Prüfplans ist die IT-Grundschutz-Modellierung sowie die Schutzbedarfsfeststellung (siehe [BSI2] und [BSI4]). Diese sollten mit dem Sicherheitskonzept und dem Export der Informationssicherheitsmanagement-Datenbank vorliegen. Aus der Grundschutz-Modellierung ergibt sich eine Zuordnung von Grundschutzbausteinen (inkl. benutzerdefinierten Bausteinen) zu bestimmten Zielobjekten, im Folgenden „Baustein-Zielobjekt“ genannt (siehe Kapitel 1.6).

Bei einer IS-Querschnittsrevision ist eine stichprobenbasierte Prüfung durchzuführen. Hierbei wird eine Auswahl von Baustein-Zielobjekten und daraus wiederum eine begrenzte Anzahl von Anforderungen betrachtet.

Aus jeder Schicht sind mindestens 30% der modellierten Baustein-Zielobjekte auszuwählen. Der Baustein ISMS.1 – Sicherheitsmanagement ist dabei verpflichtend auszuwählen und mit allen seinen Anforderungen vollständig zu prüfen.

Bei der Auswahl ist zu beachten, dass eine Gruppe gleichartiger Zielobjekte als ein Baustein-Zielobjekt in die Auswahlmenge eingeht. Sollte der IS-Revisor im Rahmen der Vor-Ort-Prüfung feststellen, dass ausgewählte Baustein-Zielobjekte gleichartig konfiguriert und administriert werden, kann die Anzahl der Stichproben verringert werden. Diese Verfahrensweise ist im IS-Prüfplan nachvollziehbar zu begründen.

Die Auswahl der zu prüfenden Baustein-Zielobjekte erfolgt nach dem risikoorientierten Prüfansatz. Um eine risikoorientierte Baustein-Zielobjekt-Auswahl zu erhalten, sind insbesondere die folgenden Fragestellungen hilfreich:

- Was sind die wesentlichen oder kritischen Geschäftsprozesse der Organisation? Welche Verfahren unterstützen diese Geschäftsprozesse? Welche Baustein-Zielobjekte betreffen diese Verfahren?
- Welche Baustein-Zielobjekte sind erfahrungsgemäß besonders fehleranfällig?
- Welche Baustein-Zielobjekte haben einen hohen oder sehr hohen Schutzbedarf laut Schutzbedarfsfeststellung im Sicherheitskonzept?
- Wurde das Zielobjekt / Dokument noch nie oder schon lange nicht mehr von der IS-Revision betrachtet?
- Wurden große Änderungen in der IT-Landschaft der Institution (z. B. neue IT-Systeme, veränderte oder neue Verfahren, andere Betriebssysteme) seit der letzten IS-Revision vorgenommen? Waren davon wichtige Geschäftsprozesse betroffen? Welche Baustein-Zielobjekte sind von der Veränderung betroffen?

Die Auswahl der Baustein-Zielobjekte sollte bei Folgerevisionen variieren, um langfristig eine möglichst gute Prüfabdeckung des gesamten Informationsverbundes zu gewährleisten.

In einem weiteren Reduktionsschritt werden pro Baustein-Zielobjekt mindestens 30 % der Anforderungen zur Prüfung ausgewählt. Prüfungsrelevant sind nur die Anforderungen der Basis- und Standard-Absicherung sowie zusätzlich die ergänzenden Maßnahmen, welche sich aus der Behandlung von Risiken aus der Risikoanalyse ergeben.

Die Auswahl der Anforderungen sollte wie die Baustein-Zielobjekt-Auswahl nach dem risikoorientierten Prüfansatz erfolgen.

Unabhängig von der vorherigen Baustein-Zielobjekt-Auswahl sind zusätzlich möglichst alle Anforderungen zu prüfen, die in der vorhergehenden IS-Revision bemängelt wurden. Es sind mindestens alle Anforderungen mit schwerwiegenden Sicherheitsmängeln zu berücksichtigen.

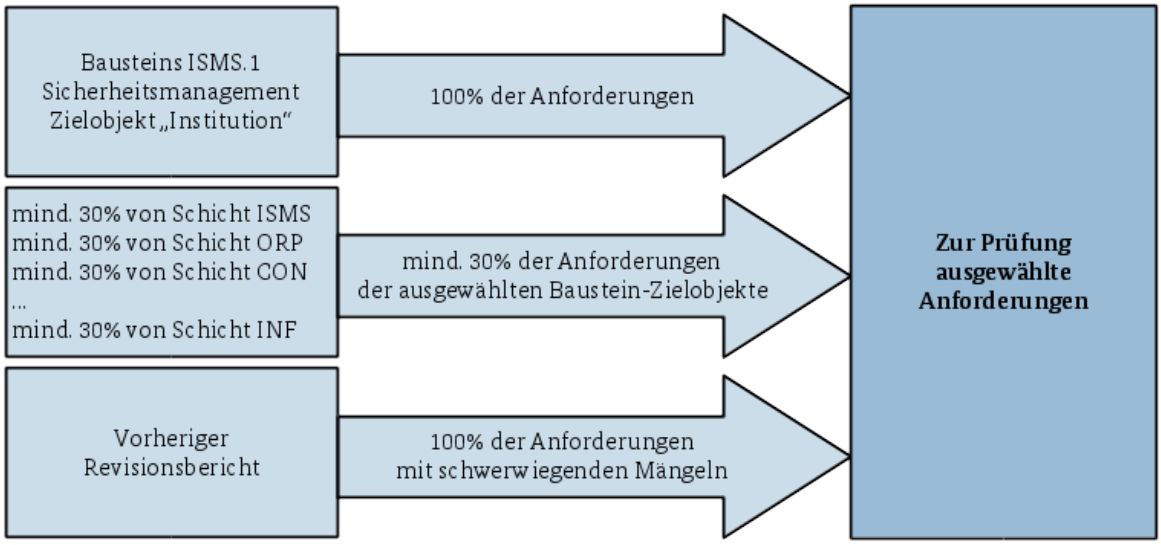

Abbildung 7: Auswahl der Stichprobe bei einer IS-Querschnittsrevision

Auch bereits zertifizierte oder auditierte Informationsverbünde der Institution sind im Rahmen der IS-Revision zu prüfen, sie stehen jedoch aufgrund des risikoorientierten Prüfansatzes (siehe [IDW]) und der dort bereits getätigten Audits nicht im Fokus einer IS-Revision. Ergebnisse von Audits können bei der IS-Revision berücksichtigt werden, wenn die Vorgaben dieses Leitfadens bei den Audits beachtet wurden und die Daten innerhalb des aktuellen IS-Revisionszyklus (maximal 3 Jahre) erhoben worden sind.

4.2.4 Dokumentenprüfung und Fortschreibung des IS-Prüfplans (Schritt 3)

Die Dokumentenprüfung erfolgt auf Basis der im IS-Prüfplan festgelegten Anforderungen. Bei der Dokumentenprüfung steht die inhaltliche Vollständigkeit der Dokumente und die Nachvollziehbarkeit im Fokus. Soweit möglich, ist auch die Angemessenheit der zu prüfenden Maßnahmen zur Erfüllung der Anforderung zu betrachten.

Hinsichtlich der Vollständigkeit ist zu prüfen, ob alle wesentlichen Aspekte wie z. B. Systeme, Netze, IT-Anwendungen und Räume erfasst sowie die beschriebenen Rollen zugewiesen wurden.

Die Angemessenheit beinhaltet die Beurteilung der personellen, organisatorischen und technischen Maßnahmen im Hinblick auf deren Wirksamkeit. Um die Angemessenheit einer Maßnahme zu bewerten, sind nach Möglichkeit folgende Fragen (siehe [BSI2] - Kapitel 8.4) zu beantworten:

- Welche Gefährdungen sollen durch die Realisierung der Maßnahme verringert werden?
- Welches Restrisiko verbleibt bei der Institution? Ist dieses Restrisiko lt. Aktenlage für die Organisation tragbar?
- Ist die Maßnahme geeignet um die Anforderung zu erfüllen und in der Praxis umsetzbar?
- Ist die Maßnahme zur Erfüllung der Anforderung anwendbar, leicht verständlich und wenig fehleranfällig?

Die vorgelegten Dokumente müssen für das IS-Revisionsteam nachvollziehbar sein. Entscheidungen der Institution sollten in der zu prüfenden Dokumentation begründet sein.

Ein geringer Anteil der zu prüfenden Anforderungen kann bereits in der Dokumentenprüfung abschließend bewertet werden. Die verbleibenden Anforderungen sind bei der Vor-Ort-Prüfung weiter zu untersuchen. Ergänzt wird der IS-Prüfplan um Anforderungen, die sich aus Auffälligkeiten bei der Dokumentenprüfung ergeben.

Zu jeder Anforderung im IS-Prüfplan werden die wesentlichen zu klärenden Fragen unter Angabe der angedachten Prüfmethode (siehe Kapitel 4.1.2) und des Interviewpartners der Institution (soweit aus Dokumentenlage ableitbar) für die Vor-Ort-Prüfung zusammengestellt.

Anschließend sind diese Fragen zu konsolidieren. Das bedeutet, dass Fragen zu den Anforderungen möglichst sortiert nach Interviewpartner und zu prüfendem System zusammengefasst und redundante Fragen gestrichen werden. Dies erleichtert den Ablauf der IS-Revision, verbessert die Nachvollziehbarkeit der Ergebnisse und dient der Dokumentation der Prüfungshandlungen.

In Kooperation mit dem Ansprechpartner der zu prüfenden Institution erarbeitet das IS-Revisionsteam den Ablaufplan für die Vor-Ort-Prüfung (Termin für Eröffnungsgespräch, Interviews, Inaugenscheinnahme von Systemen und Abschlussgespräch) und nimmt diesen in den IS-Prüfplan auf. Der Ansprechpartner in der zu prüfenden Institution ist für die Koordinierung der Termine und Räumlichkeiten verantwortlich. Er hat insbesondere auch dafür zu sorgen, dass dem IS-Revisionsteam während der Vor-Ort-Prüfung ein eigener, abschließbarer Raum zur Verfügung steht.

Der IS-Prüfplan umfasst zu diesem Zeitpunkt:

- die Festlegung der zu prüfenden Baustein-Zielobjekte und der zu prüfenden Anforderungen,
- zusätzlich zu prüfende Anforderungen im Zusammenhang mit Auffälligkeiten bei der Dokumentenprüfung,
- die Wahl der Prüfmethoden für die jeweiligen Anforderungen,
- wenn möglich die Bestimmung der Interviewpartner einschließlich ihrer Rolle und
- die Festlegung des Terminplans.

4.2.5 Vor-Ort-Prüfung (Schritt 4)

Ziel der Vor-Ort-Prüfung ist es, die vorgelegten Dokumente, z. B. die Konzepte und Richtlinien, mit den Gegebenheiten vor Ort abzugleichen und zu prüfen, ob mit den gewählten Maßnahmen zur Erfüllung der Anforderungen die Informationssicherheit in angemessener und praxistauglicher Form gewährleistet wird.

Es wird nach dem ausgearbeiteten IS-Prüfplan vorgegangen. Dies bedeutet jedoch nicht, dass der IS-Revisor sich zwingend immer an den IS-Prüfplan halten muss. Es kann durchaus zielführend und sinnvoll sein, die Prüfung von Bereichen aus dem IS-Prüfplan abzubrechen. Dies ist insbesondere dann der Fall, wenn bereits bei den ersten Stichproben feststeht, dass die Anforderungen eines Zielobjekts nicht hinreichend umgesetzt wurden und sich weitergehende tiefergehende Prüfungen damit erübrigen. Umgekehrt kann es notwendig sein, Prüfungen zu erweitern, um die Feststellung von Sicherheitslücken oder -mängeln zu erhärten. Der IS-Prüfplan wird entsprechend fortgeschrieben. Die Entscheidung, die Prüfung zu Baustein-Zielobjekten bzw. Anforderungen zu erweitern oder abzubrechen, liegt im Ermessen des IS-Revisionsteams. Erweiterungen von Prüfungen beschränken sich dabei auf den vertraglich festgelegten Prüfgegenstand.

Eröffnungsgespräch

Zu Beginn der Vor-Ort-Prüfung führt das IS-Revisionsteam ein Eröffnungsgespräch mit der Leitung der zu prüfenden Institution, dem Verantwortlichen für IS-Revisionen, dem Leiter der IT und dem Informationssicherheitsbeauftragten. Weitere Personen, wie z. B. der Leiter der Personalabteilung, Administratoren und weitere Interviewpartner, können bei Bedarf teilnehmen. Neben dem grundsätzlichen Verfahren einer IS-Revision werden Prüfgegenstand und Prüfablauf erläutert. Es soll dargelegt und dokumentiert werden, welche Unterstützung von der geprüften Organisation für eine reibungslose Abwicklung der IS-Revision erwartet wird. Unterstützungsleistungen in diesem Sinne sind, dem Auskunfts- und / oder Vorlageverlangen nachzukommen und die notwendigen Kommunikationsmittel (z. B. Intranet, Telefon) für die Prüfungsdauer bereitzustellen. Genauso wichtig ist, dass die IS-Revisoren in der Organisation persönlich bekannt gemacht werden und sich mit den äußeren Rahmenbedingungen, wie beispielsweise den Dienstzeiten und Zutrittsregelungen, vertraut machen können.

Vorgehensweise bei der IS-Revision vor Ort

Der IS-Prüfplan dient dem IS-Revisionsteam als Hilfsmittel, um die Vor-Ort-Prüfung strukturiert und zügig durchzuführen und sollte zur Dokumentation der Prüfhandlungen genutzt werden.

Die Prüfungen werden zunächst mit den vorgesehenen Prüfmethoden, meistens dem Interview und der Inaugenscheinnahme, durchgeführt. Bei technischen Aspekten bedeutet dies eine Demonstration durch den zuständigen Administrator oder Vertreter. Das IS-Revisionsteam greift dabei nie selbst in das System ein. Bei komplexen Systemen und Verfahren oder einer hohen Datenmenge ist eine direkte Auswertung der Informationen vor Ort nicht immer möglich. In diesem Fall können weitere Informationen zur späteren Auswertung vom IS-Revisionsteam in elektronischer oder Papierform angefordert werden. Der IS-Prüfplan wird entsprechend fortgeschrieben.

Stellt das IS-Revisionsteam bei der Prüfung einer ausgewählten Stichprobe Abweichungen zum dokumentierten Status fest, erweitert es diese Stichprobe bedarfsorientiert. Das IS-Revisionsteam schließt die Stichprobe erst ab, wenn der Sachverhalt ausreichend geklärt ist (z. B. methodischer oder einmaliger Fehler).

Während der Vor-Ort-Prüfung sind sowohl die wesentlichen Sachverhalte als auch Angaben über Quellen, Auskunfts- und Vorlageersuchen sowie durchgeführte Besprechungen schriftlich festzuhalten. Eventuell können zu Dokumentationszwecken auch technische Hilfsmittel wie z. B. Fotos und Screenshots genutzt werden. Alle technischen Dokumentationsmittel sind vorab mit der Leitungsebene der Institution abzustimmen und dürfen nur mit Zustimmung der Beteiligten angewendet werden.

Abschlussgespräch

Nach Abschluss der Vor-Ort-Prüfung werden der bisherige Verlauf der Prüfung, exemplarisch einige der getroffenen Feststellungen ohne Bewertung und der weitere Verfahrensgang der geprüften Institution in einem zu protokollierenden Abschlussgespräch kurz dargestellt. An diesem Gespräch sollte der Informationssicherheitsbeauftragte, der Verantwortliche für IS-Revisionen sowie der Leiter der IT der geprüften Institution teilnehmen. Weitere Teilnehmer können bei Bedarf hinzugezogen werden.

4.2.6 Nachbereitung der Vor-Ort-Prüfung (Schritt 5)

Nach der Vor-Ort-Prüfung werden die erhobenen Informationen weiter konsolidiert und ausgewertet. Die Bewertung kann, soweit die erforderlichen speziellen Fachkenntnisse nicht im IS-Revisionsteam vorhanden sind, auch durch hinzugezogene Experten erfolgen. Insoweit Experten hinzugezogen werden, ist entweder das Einverständnis der geprüften Institution erforderlich oder die Informationen sind zu anonymisieren, so dass nicht auf die Institution oder Personen zurückgeschlossen werden kann. Die Bewertung der Informationen fließt in die Gesamtbeurteilung der geprüften Anforderung ein.

Nach der Auswertung der nachgeforderten Dokumentationen und der zusätzlichen Informationen werden die geprüften Anforderungen endgültig gewertet und in einem IS-Revisionsbericht zusammengefasst.

4.2.7 Erstellung des IS-Revisionsberichts (Schritt 6)

Der IS-Revisionsbericht einschließlich Referenzdokumenten ist der Leitung der geprüften Institution bzw. dem Auftraggeber, dem Verantwortlichen für IS-Revisionen und dem Informationssicherheitsbeauftragten schriftlich bekannt zu geben. Falls die Institution es wünscht, werden die IS-Revisionsergebnisse nach Bekanntgabe des IS-Revisionsberichts vom IS-Revisionsteam der Leitungsebene und den betroffenen Verantwortlichen im Rahmen einer Präsentation näher erläutert. Das Treffen sollte in engem zeitlichen Zusammenhang mit der Zustellung des IS-Revisionsberichts erfolgen.

Eine Entwurfsversion des IS-Revisionsberichts ohne Bewertungen sollte der geprüften Institution vorab übermittelt werden, um zu verifizieren, ob die durch das IS-Revisionsteam festgestellten Sachverhalte richtig aufgenommen wurden.

Die geprüfte Institution ist dafür verantwortlich, dass alle betroffenen Stellen in der Institution innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des IS-Revisionsberichts erhalten. Hier gilt die Regel: “Kenntnis nur soweit notwendig!“

Der IS-Revisionsbericht besteht mindestens aus einem Management-Summary, einer graphischen Auswertung des festgestellten Informationssicherheitsstatus und der ausführlichen Darstellung der Sachverhalte sowie deren Bewertung je geprüfter Anforderung.

Teil 0

In diesem Teil sind die organisatorischen Informationen, wie z. B. Revisionsgrundlagen, der zeitliche Verlauf der IS-Revision sowie eine kurze Beschreibung des Prüfauftrags enthalten.

Teil 1

Teil 1 ist das Management-Summary. Dieses sollte max. zwei Seiten umfassen und in knapper, verständlicher Form die wesentlichen Feststellungen und daraus hervorgehende Empfehlungen enthalten.

Teil 2

Neben dem Management-Summary ist eine graphische Darstellung der Revisionsergebnisse empfehlenswert. Hier sollten insbesondere Übersichten zu Umsetzungsstatus und Sicherheitsmängeln, bezogen auf die Schichten des IT-Grundschutzes, aufgenommen werden.

Teil 3

Dieser Teil des IS-Revisionsberichts beinhaltet die ausführliche Darstellung der geprüften Themenfelder, die Feststellungen mit den technischen Details sowie Empfehlungen. Es wird eine Sortierung nach geprüften Baustein-Zielobjekten und Anforderungen empfohlen. Erfasst werden lediglich die bemängelten Anforderungen bzw. Maßnahmen zur Umsetzung von Anforderungen mit Sicherheitsempfehlungen. Um die Bewertung der Sicherheitsmaßnahmen schnell zu erkennen, bietet sich innerhalb des Berichts eine farbliche Kennzeichnung wie folgt an:

Sicherheitsbewertung	Visualisierung im IS-Revisionsbericht
Schwerwiegender Sicherheitsmangel	Rot
Sicherheitsmangel	Gelb
Sicherheitsempfehlung	Grau

Tabelle 3: Visualisierung von Sicherheitsmängeln

Formale Aspekte zum IS-Revisionsbericht

Bei der Erstellung des IS-Revisionsberichts sind folgende formale Aspekte zu berücksichtigen. Die durchgeführten Einzelprüfungen, Ergebnisse und Bewertungen müssen reproduzierbar und nachvollziehbar dokumentiert werden.

- Das Inhaltsverzeichnis sollte sowohl den eigentlichen Bericht, als auch alle Anhänge (wie z. B. Screenshots, Logdateien) umfassen. Jeder Anhang muss identifizierbar sein, so dass die Vollständigkeit des IS-Revisionsberichts und der Anhänge überprüft werden kann.
- Alle genutzten Referenzdokumente sind aufzuführen.
- Aufzeichnungen, wie z. B. Gesprächsnotizen oder Auswertungen von Logdateien, auf die im Bericht verwiesen wird, müssen als Anhang beigefügt werden.
- Die Seitenkennzeichnung muss so gestaltet sein, dass jede Seite eindeutig identifiziert werden kann (z. B. mit Seitennummer sowie Versionsnummer, Bezeichnung und Datum des Berichts).
- Wenn zur Unterstützung der Prüfaktivitäten Software-Tools verwendet wurden, z. B. Analyse-Tools, müssen diese Tools mit Namen und Versionsnummer genannt werden. Sofern im Revisionsbericht auf in diesen Tools erfasste Informationen verwiesen wird, müssen entsprechende Reports (Ausdrucke) als zusätzliche Aufzeichnungen beigefügt werden.
- Verwendete Fachbegriffe oder Abkürzungen, die nicht allgemein gebräuchlich sind, müssen in einem Glossar bzw. Abkürzungsverzeichnis zusammengefasst werden.

Verwendung von IS-Revisionsberichten in Managementreports

Damit die Unternehmens- bzw. Behördenleitung die richtigen Entscheidungen bei der Steuerung und Lenkung des Informationssicherheitsprozesses treffen kann, benötigt sie einen Überblick über den Stand der Informationssicherheit. Hierzu gehören auch die vom IT-Sicherheitsbeauftragten aufbereiteten Ergebnisse der IS-Revisionen (siehe [BSI2]). Der Leitungsebene sollten in regelmäßigen Reporten:

- die wesentlichen Aussagen der IS-Revisionsberichte,
- der aus den IS-Revisionsberichten festgestellte Sicherheitsstatus bzw. die Entwicklung des Sicherheitsstatus und
- die notwendigen Folgeaktivitäten dargestellt werden.

4.2.8 Aufwand

Die Arbeitsaufwände für die einzelnen Schritte sollten sich an folgendem Zeitraster orientieren:

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 %

Tabelle 4: Relativer Zeitaufwand bei der Durchführung einer IS-Revision

4.3 Die IS-Partialrevision

Bei der IS-Partialrevision geht das IS-Revisionsteam wie bei der IS-Querschnittsrevision orientiert an den Anforderungen des IT-Grundschutzes vor. Da es sich hier aber um einen kleineren Informationsverbund handelt, ist eine deutlich umfangreichere bis vollständige Prüfung der Baustein-Zielobjekte und Anforderungen anzustreben. Der Aufbau der Prüfung sowie die Zeitanteile für die einzelnen Prüfschritte entsprechen denen der IS-Querschnittsrevision (siehe Tabelle 4: Relativer Zeitaufwand bei der Durchführung einer IS-Revision). Die Ausführungen in Kapitel 4.2 sind analog anzuwenden.

4.4 Die IS-Kurzrevision

Bei der IS-Kurzrevision geht das IS-Revisionsteam nicht orientiert an den Anforderungen des IT-Grundschutzes, sondern themenorientiert vor. Die Prüfthemen sind in einer Liste festgelegt. Diese ist im Internet auf den Webseiten des BSI als Hilfsmittel veröffentlicht

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISRevision/isrevision_node.html - Menüpunkt "Hilfsmittel").

Die IS-Kurzrevision ersetzt nicht eine IS-Querschnittsrevision, da sie aufgrund des beschränkten Aufwands nur auf spezielle Aspekte der Informationssicherheit eingehen kann.

Im Gegensatz zu der IS-Querschnittsrevison kann die IS-Kurzrevision bereits zu Beginn des Sicherheitsprozesses initiiert werden, da sie die Umsetzung der IT-Grundschutz-Vorgehensweise nicht voraussetzt. Eine Dokumentation, wie z. B. die Schutzbedarfsfeststellung oder Modellierung des Informationsverbunds gemäß IT-Grundschutz, ist für die IS-Kurzrevision nicht notwendig. Anhand ausgewählter Themen wird die Umsetzung von Sicherheitsmaßnahmen risikoorientiert überprüft.

4.4.1 Bewertungsschema

Sämtliche Prüfthemen werden unter Zuhilfenahme des IT-Grundschutz-Kompendiums und der BSI-Standards (siehe Kapitel 2.1) geprüft und bewertet. Sind Prüfthemen nicht grundschutzkonform umgesetzt und es liegen Sicherheitslücken vor, so werden diese als „Sicherheitsmangel“ oder „schwerwiegender Sicherheitsmangel“ eingestuft. Für diese Einstufung gelten die im Kapitel 4.2.1 genannten Kriterien. Eine Bewertung des Umsetzungsstatus zu einzelnen Maßnahmen zur Erfüllung von Anforderungen, wie in Kapitel 4.2.1 beschrieben, erfolgt nicht.

4.4.2 Vorgehensweise

Die grundsätzliche Vorgehensweise bei der IS-Kurzrevision ist angelehnt an das beschriebene Verfahren zur IS-Querschnittsrevision.

Die IS-Kurzrevision unterscheidet sich von der IS-Querschnittsrevision insbesondere durch die Vorgabe der Prüfthemen und die von der Baustein-Modellierung losgelösten Stichprobenauswahl.

Nachfolgend werden die Besonderheiten der IS-Kurzrevision bei den einzelnen Schritten erläutert:

Schritt 1:

Zur Durchführung einer IS-Kurzrevision bestehen keine Voraussetzungen. Es müssen keine Dokumente zum Sicherheitsprozess vorliegen. Daher kann die IS-Kurzrevision in jedem Umfeld und in jedem Stadium des Sicherheitsprozesses initiiert werden.

Schritt 2:

Der Prüfplan und die Prüftiefe stehen durch die vorgegebenen Prüfthemen und dem zeitlichen Umfang der Prüfung im Wesentlichen fest. In Absprache mit der Institution wird bereits im Vorfeld festgelegt, ob ein oder mehrere Standorte vor Ort geprüft werden müssen. Diese Entscheidung basiert auf allgemeinen Informationen zu der Institution, wie z. B. Außendarstellung der Institution (Webauftritt), Organigramm und Geschäftsverteilungsplan.

Schritt 3:

Die Dokumentenprüfung beinhaltet eine grobe Sichtung der zur Verfügung gestellten Dokumente. Hierbei werden (soweit vorliegend) insbesondere das IT-Rahmenkonzept, die Liste der kritischen Geschäftsprozesse, die IT-Sicherheitsleitlinie und das Sicherheitskonzept betrachtet. Das IS-Revisionsteam verschafft sich hiermit einen Überblick über die Aufgaben, Verfahren und die unterstützende IT-Landschaft der Institution. Auf Basis dieser gewonnenen Erkenntnisse werden die Stichproben und Schwerpunkte der IS-Kurzrevison nach dem risikoorientierten Prüfansatz bestimmt und in einem Ablaufplan für die Vor-Ort-Prüfung festgehalten. Dieser Ablaufplan enthält die Themen und die dafür erforderlichen Gesprächspartner. Der Plan wird an den Verantwortlichen für IS-Revision zur Koordinierung und Organisation der Vor-Ort-Prüfung übermittelt.

Schritt 4:

Die Vor-Ort-Prüfung beginnt immer mit einem kurzen Eröffnungsgespräch und endet mit einem Abschlussgespräch. Im Eröffnungsgespräch wird der Institution die Vorgehensweise und Zielrichtung der IS-Kurzrevision erläutert. Außerdem werden organisatorische Punkte geklärt, wie z. B. Zutrittskontrolle, Besprechungsraum für das IS-Revisionsteam, Änderungen zum Ablauf der Vor-Ort-Prüfung. Nachfolgend erfolgt die Vor-Ort-Prüfung. Bei der Vor-Ort-Prüfung werden Interviews geführt, die Liegenschaften begangen und Systeme in Augenschein genommen. Eine ausführliche Dokumentation der Vor-Ort-Prüfung, wie bei der IS-Querschnittsrevision gefordert, ist bei der IS-Kurzrevision nicht erforderlich. Grundsätzlich sollte das IS-Revisionsteam während der Vor-Ort-Prüfung vom Informationssicherheitsbeauftragten begleitet werden. Im Abschlussgespräch wird eine allgemeine Einschätzung zur Sicherheitsorganisation und den zugehörigen Prozessen gegeben. Weiterhin werden insbesondere Mängel dargelegt, die möglichst kurzfristig abgestellt werden sollten.

Schritt 5:

Die IS-Kurzrevision wird mit einem IS-Kurzrevisionsbericht abgeschlossen. Dieser sollte durchschnittlich 5 Seiten umfassen. Der Bericht gibt lediglich ein grobes Lagebild der IT-Sicherheit und zeigt schichtenorientiert, wo die größten Problemfelder hinsichtlich IT-Sicherheit liegen. Zusätzlich bekommt die Institution eine Rückmeldung, inwieweit die vorhandene Dokumentation (z. B. Sicherheitskonzept, Schutzbedarfsfest-

stellung) bereits den Anforderungen einer IS-Querschnittsrevision entspricht.

Abschließend wird im IS-Kurzrevisionsbericht ein Votum abgegeben, ob

- als nächste IS-Revision eine IS-Querschnittsrevision durchgeführt werden kann,
- dies nur nach bestimmten, konkret zu benennenden Nachbesserungen empfohlen wird oder
- nochmals eine IS-Kurzrevision erfolgen sollte.

Ausschlaggebend für das Votum ist die Einschätzung des IS-Revisionsteams, ob bereits die wesentlichen Voraussetzungen für eine IS-Querschnittsrevision vorliegen bzw. innerhalb von einem Jahr geschaffen werden können (siehe Kapitel 4.2). Bei vielen schwerwiegenden Sicherheitsmängeln im Bereich des Informationssicherheitsmanagements (siehe Baustein ISMS.1 Sicherheitsmanagement“) sollte eine weitere IS-Kurzrevision empfohlen werden.

Der Aufbau des IS-Revisionsberichts sieht wie folgt aus:

- Eckdaten zur IS-Kurzrevision,
- Managementübersicht zur Einschätzung der Sicherheitslage in der Institution,
- kurze Beschreibung der Sicherheitsmängel pro Prüfthemenfeld (der Prüfthemenliste),
- Votum für die nächste durchzuführende Revisionsart.

Spätestens drei Jahre nach Bekanntgabe des IS-Kurzrevisionsberichtes sollte eine weitere IS-Revision gemäß Votum durchgeführt werden.

4.4.3 Aufwand

Eine IS-Kurzrevision läuft in 5 Schritten ab und erzeugt den folgenden Aufwand:[1]

Phase	Tätigkeit	Zeitanteile
Schritt 1	Vorbereitung der IS-Revision	1 Tag
Schritt 2	Erstellung des Ablaufplans	
Schritt 3	Dokumentenprüfung	
Schritt 4	Vor-Ort-Prüfung	1 Tag – 2 Tage (je Standort)
Schritt 5	Nachbereitung der Vor-Ort-Prüfung, Erstellung des IS-Revisionsberichts	1 Tag

Tabelle 5: Zeitaufwand bei der Durchführung einer IS-Kurzrevision

Zusätzlich sind Reisezeiten zu berücksichtigen. Für ein IS-Revisionsteam sind demnach etwa 6 bis 8 Personentage je Prüfung durchschnittlich einzuplanen.

Der interne Aufwand der geprüften Institution zur Koordinierung einer IS-Kurzrevision beträgt ungefähr einem Arbeitstag (z. B. für Organisation, Termine, Referenzdokumente zusammenstellen).

1 Schritt 5 „Nachbereitung“ und Schritt 6 „Berichterstellung“ der IS-Querschnittsrevision wurden zu einem Schritt zusammengefasst, da im vorgesehenen Zeitfenster keine tiefer gehende technische Prüfung und damit verbundene Auswertung möglich ist.

4.5 Aufbewahrung und Archivierung von IS-Revisionsberichten

Der IS-Revisionsbericht und die diesem zugrunde liegenden Referenzdokumente müssen durch die geprüfte Institution mindestens für die Dauer von 10 Jahren ab Zustellung des Berichts revisionssicher aufbewahrt werden. Sie sind Grundlage für die Auswahl der zu prüfenden Baustein-Zielobjekte und Maßnahmen zur Erfüllung von Anforderungen bei künftigen Revisionen (u. a. zur langfristig vollständigen Prüfung der Institution, Nachverfolgung von Sicherheitsmängeln).

Anforderungen an die revisionssichere Archivierung finden sich im Grundschutzbaustein OPS.1.2.2 „Archivierung“ und im § 239 HGB:

- Ordnungsmäßigkeit,
- Vollständigkeit,
- Schutz vor Veränderung und Verfälschung,
- Sicherung vor Verlust,
- Nutzung nur durch Berechtigte,
- Einhaltung der Aufbewahrungsfristen,
- Dokumentation des Verfahrens,
- Prüfbarkeit sowie
- Nachvollziehbarkeit.

Mit der Zustellung des IS-Revisionsberichts endet die IS-Revision für das beauftragte IS-Revisionsteam.

5 Hilfsmittel

Als Unterstützung bei der Anwendung des Leitfadens IS-Revision hat das Bundesamt für Sicherheit in der Informationstechnik Hilfsmittel entwickelt, die regelmäßig fortgeschrieben werden. Hilfsmittel wie z. B. Mustervorlagen für das IS-Revisionshandbuch, den IS-Prüfplan oder den IS-Revisionsbericht werden in der jeweils aktuellen Version unter folgendem Link zum Download bereitgestellt:

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISRevision/isrevision_node.html – Menüpunkt „Hilfsmittel“