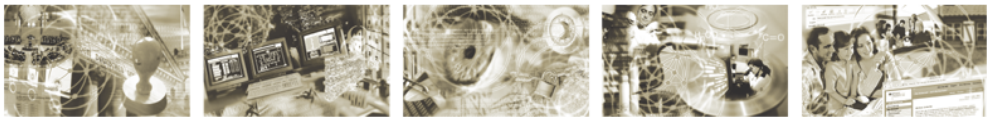
Bundesamt
für Sicherheit in der
Informationstechnik



Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Auditierungsschema

Version 1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-111
E-Mail: gszertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Versionshistorie

Datum	Version	Verfasser	Bemerkungen
26.10.10	0.99	BSI	Version zur Kommentierung durch Auditoren
16.03.11	1.0	BSI	

1.2 Vorwort

Für die Bestätigung der Konformität eines Managementsystems für Informationssicherheit (ISMS) gemäß ISO 27001 auf der Basis von IT-Grundschutz werden in diesem Dokument (Auditierungsschema) die Anforderungen an die Prüfungshandlungen der Mitglieder des Auditteams beschrieben.

Die grundsätzliche Vorgehensweise und die Voraussetzungen für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz werden im Zertifizierungsschema [ZERTAUD] beschrieben. ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz geben Behörden und Unternehmen die Möglichkeit, ihre Bemühungen um Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen zu dokumentieren.

Mit der Vergabe eines Zertifikats wird der Institution bescheinigt, dass

- Informationssicherheit ein anerkannter Wert ist,
- ein funktionierendes IS-Management vorhanden ist und außerdem,
- zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau erreicht wurde.

Prüfgrundlagen des Verfahrens sind ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems – Requirements" [27001], die BSI-Standards BSI-Standard 100-1 [1001] „Managementsystem für Informationssicherheit ISMS“, BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ [1002], BSI-Standard 100-3 „Ergänzende Risikoanalyse auf Basis von IT-Grundschutz“ [1003] sowie die IT-Grundschutz-Kataloge [GSK] des BSI.

1.3 Adressatenkreis

Dieses Dokument richtet sich vor allem an Auditteamleiter, die ein unabhängiges Audit durchführen, um die Konformität eines Managementsystems für Informationssicherheit (ISMS) gemäß ISO 27001 auf der Basis von IT-Grundschutz in einer Institution zu bestätigen. Verantwortlich für die Informationssicherheit können sich einen Überblick darüber verschaffen, welche Prüfanforderungen bei einem Audit gestellt werden und welche Referenzdokumente zur Verfügung gestellt werden müssen.

1.4 Anwendungshinweise

Zusätzlich zu den vorliegenden Vorgaben sind ergänzende Verfahrensanweisungen zu beachten und anzuwenden, die unter *http://www.bsi.bund.de/gshb/zert* veröffentlicht sind. In ergänzenden Verfahrensanweisungen werden unter anderem Grundsatzentscheidungen des BSI veröffentlicht und Hilfsmittel zur Umsetzung des Auditierungsschemas gegeben.

Darüber hinaus haben die Mitglieder des Auditteams die ergänzenden Hinweise zu den Prüfungshandlungen in den Vorlagen zu den Auditberichten (siehe Kapitel 8 Anlagen zum Auditierungsschema) zu beachten.

1.5 Literaturverzeichnis

[1001] Managementsystem für Informationssicherheit ISMS, BSI-Standard 100-1, http://www.bsi.bund.de/gshb

[1002] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, http://www.bsi.bund.de/gshb

[1003] Ergänzende Risikoanalyse, BSI-Standard 100-3, http://www.bsi.bund.de/gshb

[GSK] IT-Grundschutz-Kataloge - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[ZERTAUD] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz „Zertifzierungsschema“, http://www.bsi.bund.de/iso27001-zertifikate

[27001] DIN EN ISO/IEC 27001:2005 „Information technology - Security techniques - Information security management systems - Requirements"

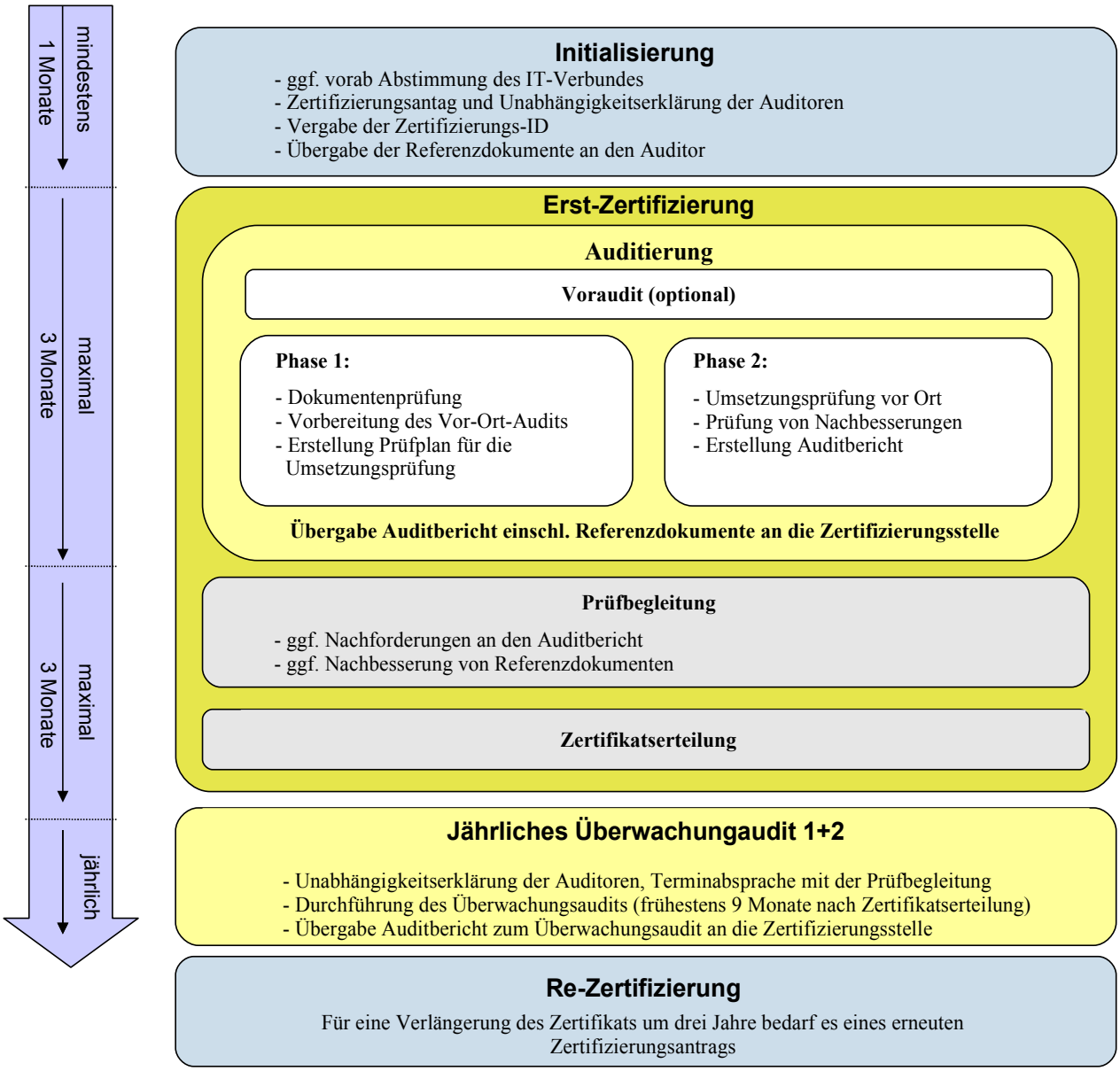
[IAF MD 1:2007] IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling. http://www.iaf.nu/

2 Überblick über das Zertifizierungsverfahren

2.1 Der Ablauf des Prozesses

Erst nach erfolgreicher Initialisierung des Zertifizierungsprozesses [ZERT] durch die Stellung eines Zertifizierungsantrags und Prüfung der Unabhängigkeitserklärungen aller Mitglieder des Auditteams, kann ein Audit durchgeführt werden.

Abbildung 1: Zertifizierungsprozess



Auf der Grundlage einer Dokumentenprüfung (s. Kapitel 4.1) bereiten sich die Mitglieder des Auditteams auf die Vor-Ort-Prüfung (s. Kapitel 4.2) vor, bevor das Auditteam die konkrete Umsetzung der Anforderungen Vor-Ort überprüft (s. Kapitel 4.4). Werden Defizite festgestellt, muss die Institution Nachbesserungen durchführen (s. Kapitel 4.6) damit der Auditteamleiter ein positives Gesamtvotum (s. Kapitel 4.8) abgeben kann. Nach Abgabe des Auditberichts an die Zertifizierungsstelle kann diese noch Nachforderungen (s. Kapitel 4.9) an den Auditbericht gegenüber dem Auditor oder dem Antragsteller haben. Nach positiver Abnahme des Auditberichtes wird ein Zertifikat erteilt.

2.2 Unterschiedliche Arten einer Auditierung

Ein **Erst-Zertifizierungsaudit** betrachtet den gesamten Sicherheitsprozess eines Informationsverbundes sowie die umzusetzenden Maßnahmen im Rahmen einer Stichprobenprüfung auf der Basis von Bausteinen aus den Grundschutzkatalogen. Hierbei kann sich der Auditor im Rahmen eines **Voraudits** einen Überblick über den Informationsverbund verschaffen.

Die Aufrechterhaltung der Sicherheit wird mit einem jährlich durchzuführenden **Überwachungsaudit** geprüft. Ein Überwachungsaudit betrachtet nur stichprobenartig den Sicherheitsprozess, um die Aufrechterhaltung der Sicherheit zu bestätigen.

Ein Zertifikat kann durch eine Re-Zertifizierung um drei Jahre verlängert werden. Der Auditor greift für das Re-Zertifizierungsaudit auf die Ergebnisse der Auditierungen der vorhergehenden Zertifizierung (Audit für das Zertifizierungsverfahren sowie Überwachungsaudits) zurück und konzentriert die Prüfungen auf die Veränderungen, die sich innerhalb des Informationsverbundes seit der letzten Zertifizierung und den zugehörigen Überwachungsaudits ergeben haben.

Jedes Audit umfasst zwei Phasen: eine Dokumentenprüfung und eine Vor-Ort-Prüfung. Die Ergebnisse werden immer in einem Auditbericht zusammengefasst.

2.3 Voraussetzungen auf Seiten des Antragstellers

Für jedes Audit stellt der Antragsteller die erforderlichen Referenzdokumente bereit. Zusätzlich sind in einer zusammenfassenden Übersicht der Stand der jeweiligen Referenzdokumente sowie wesentliche Veränderungen gegenüber dem letzten Audit aufzuzeigen (s. Kap. 8 Anlagen zum Auditierungsschema„Überblick über die Referenzdokumente“).

Voraussetzung für die Zertifizierung und Auditierung ist die Umsetzung der Grundschutz-Methodik und die Umsetzung der Grundschutz-Maßnahmen. Grundlage dafür ist die aktuelle Version des BSI-Standard 100-1, BSI-Standard 100-2 und gegebenenfalls der BSI-Standards 100-3, sowie die Verwendung der aktuellen oder Vorgängerversion der IT-Grundschutz-Kataloge. Es wird jedoch dringend empfohlen, die jeweils aktuelle Version der IT-Grundschutz-Kataloge zu verwenden, da zum Auditbeginn durch den Auditor geprüft wird, ob eine zulässige Version verwendet wurde (vgl. Kap. 8 Anlagen zum Auditierungsschema, “Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz“).

Folgende Referenzdokumente bilden die Grundlage für die Zertifizierung und müssen vom Antragsteller dem Auditor und der Zertifizierungsstelle zur Verfügung gestellt werden:

- Richtlinien für Informationssicherheit (A.0)
- Strukturanalyse (A.1)

- Schutzbedarfsfeststellung (A.2)
- Modellierung des Informationsverbundes (A.3)
- Ergebnis des Basis-Sicherheitschecks (A.4)
- Ergänzende Sicherheitsanalyse (A.5)
- Risikoanalyse (A.6)
- Risikobehandlungsplan (A.7)

Die Vorlage der Ergebnisse des Basis-Sicherheitschecks (A.4) bei der Zertifizierungsstelle ist optional. Dem Auditor muss das Referenzdokument A.4 jedoch auf jeden Fall als Arbeitsgrundlage zur Verfügung gestellt werden. Der Auditor kann darüber hinaus während des Vor-Ort-Audits weitere Dokumente und Aufzeichnungen einsehen.

Die Referenzdokumente sind Bestandteil des Auditberichtes. Sollten zusätzliche Dokumente erstellt worden sein, die zur Prüfung relevant sind, sind diese ebenfalls in der aktuellen Fassung dem Auditor vorzulegen und können ggf. Gegenstand des Auditberichtes werden.

3 Berufsethik

Die Auditierung stützt sich auf eine Reihe von Prinzipien. Diese machen das Audit zu einem wirksamen und zuverlässigen Werkzeug. Um Vertrauen in eine objektive Prüfung zu schaffen, ist die Einhaltung einer Berufsethik notwendig. Dies ist eine Voraussetzung für nachvollziehbare, wiederholbare und vergleichbare Auditergebnisse, um eine nachfolgende Zertifizierung zu ermöglichen.

Die Berufsethik umfasst folgende Prinzipien:

- Ethisches Verhalten
  Da im Umfeld Informationssicherheit oft sensible Geschäftsprozesse und Daten zu finden sind, sind die Vertraulichkeit der Informationen und der diskrete Umgang mit den Ergebnissen des Audits eine wichtige Arbeitsgrundlage. Sowohl die Zertifizierungsstelle als auch die auditierte Organisation müssen dem Auditor und seinem Vorgehen vertrauen können.
- Fachkompetenz
  Die Mitglieder des Auditteams übernehmen nur solche Aufgaben, für die sie das erforderliche Wissen, Können und die entsprechende Erfahrung haben, und setzen diese/s bei der Durchführung ihrer Arbeit ein. Sie verbessern kontinuierlich ihre Fachkenntnisse sowie die Effektivität und Qualität ihrer Arbeit.
- Vertrauenswürdigkeit
  Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Informationen zu finden sind, ist die Vertraulichkeit der während eines Audits erlangten Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der Prüfung eine wichtige Arbeitsgrundlage. Informationen sind nicht ohne entsprechende Befugnis offen zu legen, es sei denn, es bestehen dazu rechtliche oder berufliche Verpflichtungen.
- Sachliche Darstellung
  Ein Auditor hat die Pflicht, sowohl seinem Auftraggeber als auch der Zertifizierungsstelle wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehört die wahrheitsgemäße und nachvollziehbare Darstellung des Sachverhalts in den Auditfeststellungen, Auditschlussfolgerungen und dem Auditbericht. Die Prüfungsergebnisse des Audits müssen (bei unverändertem Sachstand) wiederholbar sein.
- 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, mit der der Auditor zu seinen Schlussfolgerungen kommt.
- Objektivität und Sorgfalt
  Ein Auditor 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 Dritte beeinflusst werden.

4 Der Auditprozess

Jedes Audit setzt sich grundsätzlich aus zwei getrennten, aufeinander aufbauenden Phasen zusammen. Phase 1 umfasst zunächst die Prüfung der vom Antragsteller eingereichten Referenzdokumente. In Phase 2 schließt sich eine Vor-Ort-Prüfung des Informationsverbundes durch das Auditteam an. Hierbei wird im realen Informationsverbund die praktische Umsetzung der in den Referenzdokumenten dokumentierten Sicherheitsmaßnahmen bzgl. ISO 27001 und IT-Grundschutz auf ihre Vollständigkeit, Korrektheit und Wirksamkeit hin überprüft (Vor-Ort-Prüfung).

Für jedes Audit ist vom Auditteamleiter ein Auditbericht zu erstellen, der alle Prüfergebnisse enthält. In Anlehnung an die Aufteilung eines Audits in zwei Phasen ist der Auditbericht ebenfalls in zwei Schritten zu erstellen: Im ersten Schritt dokumentiert der Auditbericht die Auditergebnisse für Phase 1 des Auditprozesses (Dokumentenprüfung), im zweiten Schritt sind die Auditergebnisse aus der Phase 2 des Auditprozesses (Vor-Ort-Prüfung) zu ergänzen. Der auf Phase 1 des Audits bezogene Auditbericht ist vor der Vorbereitung und Durchführung der Vor-Ort-Prüfung in Phase 2 des Audits abzuschließen.

Hinweis:

Die Erläuterungen zum Auditprozess gelten sowohl für das Erst- als auch für das Re-Zertifizierungsaudit. Abweichend hiervon gestalten sich das Voraudit (s. Kapitel 5) und das Überwachungsaudit (s. Kapitel 6).

Der Auditbericht ist auf der Basis des Musters für Auditberichte zu erstellen (siehe Hilfsmittel: http://www.bsi.bund.de/gshb/zert).

4.1 Phase 1 des Audits: Dokumentenprüfungen

Die erste Auditphase dient dazu, dass der Auditor ein ausreichendes Verständnis für den Informationsverbund erlangt und feststellt, ob die Konzeption der IT-Sicherheitsstruktur des Informationsverbundes bzgl. ISO 27001 und IT-Grundschutz schlüssig und sinnvoll ist. Der Auditor prüft insbesondere, ob die Zertifizierungsfähigkeit des Informationsverbunds grundsätzlich gegeben ist.

Damit der Auditor ein ausreichendes Verständnis vom Informationsverbund gewinnen kann, kann es sinnvoll sein, einen Teil der Dokumentenprüfung bei der zu auditierenden Institution durchzuführen. In einigen Fällen ist die Einsichtnahme von Dokumenten auch aus Vertraulichkeitsgründen nur vor Ort möglich.

In Phase 1 des Audits sichtet das Auditteam die Referenzdokumente des Antragstellers und bewertet diese auf der Basis der Vorgaben des Auditierungsschemas. Der Auditteamleiter dokumentiert die Ergebnisse in den vorliegenden Vorlagen für die Auditberichte. Die Grundlage der Bewertung der Referenzdokumente bilden die Vorgaben aus den BSI-Standards (100-2 und ggf. 100-3) und den IT-Grundschutz-Katalogen.

Festgestellte Abweichungen in den Referenzdokumenten teilt der Auditteamleiter dem Antragsteller zusammen mit einer angemessenen Frist zur Behebung mit. Der Antragsteller bekommt somit Gelegenheit, festgestellte Abweichungen bereits vor der Phase 2 des Audits zu beheben.

Der Prüfumfang und die Prüftiefe der Dokumentenprüfung werden in dem Muster für Auditberichte beschrieben.

4.2 Vorbereitung des Vor-Ort-Audits

Für den Auditteamleiter besteht die Möglichkeit eines Abbruchs der Auditierung nach der Dokumentenprüfung, wenn ein Abschluss der Auditierung mit einem positiven Votum ausgeschlossen erscheint. Dies ist beispielsweise dann der Fall, wenn die Dokumentation zum ISMS gravierende Defizite aufweist oder bei der Institution nicht die Bereitschaft erkennbar ist, beim Zertifizierungsaudit aktiv mitzuwirken. Das BSI wird hiervon unterrichtet.

Nach der Dokumentation der Auditergebnisse von Phase 1 überprüft der Auditteamleiter, ob im Auditteam die Fachkenntnisse vorliegen, um das Audit mit der Phase 2 weiterzuführen. Einerseits können Sektor spezifische Fachkenntnisse erforderlich sein, die zum Verständnis der Prozesse der Institution erforderlich sind. Andererseits müssen auch Baustein spezifische Fachkenntnisse (z. B. für SAP) vorhanden sein, die im Rahmen der Maßnahmenprüfung zwingend erforderlich sind. Liegen die erforderlichen Fachkenntnisse auf einem oder mehreren Gebieten nicht vor, so erweitert der Auditteamleiter das Auditteam um einen oder mehrere Auditoren bzw. Erfüllungsgehilfen. Für jedes einzelne Mitglied des Auditteams muss dem BSI eine Unabhängigkeitserklärung vorliegen.

4.3 Erstellung eines Prüfplans für die Vor-Ort-Prüfung

Zur Vorbereitung der Vor-Ort-Prüfung muss der Auditteamleiter einen Prüfplan erstellen, d. h. er muss sich aus den Ergebnissen der Dokumentenprüfung die erforderlichen Interviewpartner heraussuchen und die Stichproben für die Umsetzungsprüfung des Basis-Sicherheitschecks bestimmen.

4.3.1 Verifikation des Basis-Sicherheitschecks

Bei der Vor-Ort-Prüfung muss sich der Auditor sieben Bausteinzuordnungen und Maßnahmen aus der ergänzenden Sicherheits- bzw. Risikoanalyse auswählen. Der Auditteamleiter kann die Stichprobe in begründeten Fällen ausweiten.

Dabei werden folgende Rahmenbedingungen festgelegt:

- Der Auditor muss bei jedem Audit eine Überprüfung des Bausteins B 1.0 Sicherheitsmanagement vornehmen. Dabei ist zu beachten, dass die Überprüfung der Wirksamkeit des Informationssicherheitsmanagements und die Vorgehensweise nach Standard 100-2 nicht auf die Überprüfung dieses Bausteins beschränkt ist, sondern während des gesamten Audits und in jeder Maßnahme geprüft wird.
- Der Auditteamleiter wählt **Risiko orientiert** aus jeder Schicht ein Baustein-Zielobjekt aus.
- Zusätzlich wird ein weiteres Baustein-Zielobjekt im **Losverfahren** ermittelt.
- Aus der Menge der **zusätzlichen Sicherheitsmaßnahmen**, die im Rahmen der ergänzenden Risikoanalyse festgelegt wurden, wählt der Auditor mindestens fünf Stichproben nach eigenem Ermessen für verschiedene Komponenten aus.

Hinweis:

Der Baustein Datenschutz ist nicht zertifizierungsrelevant. Bei der oben beschriebenen Auswahl der sieben Bausteine ist der Baustein Datenschutz nicht zu berücksichtigen.

4.3.2 Begutachtung der Standorte des Informationsverbundes

Standorte können im Rahmen einer Gruppenbildung zusammengefasst werden. Maßgeblich hierfür ist, dass die Standorte von einem gemeinsamen ISMS betrieben werden und die dort ausgeführten Prozesse gleichartig sind und mit ähnlichen Methoden und Verfahren betrieben werden, Organisationsstrukturen, personelle und infrastrukturelle Rahmenbedingungen sowie die technischen Gegebenheiten (wie IT-Systeme und Netze) gleichartig sind. Sind diese Voraussetzungen erfüllt, genügt eine Stichprobe über die gruppierten Standorte. Die Größe der Stichprobe bemisst sich nach den Vorgaben des „ IAF Mandatory Document for the Certification of Multiple Sites Based on Sampling Issue 1, Version 2 (IAF MD 1:2007)“ [IAF MD 1:2007]

Abweichungen von der beschriebenen Vorgehensweise bei der Auswahl von Standorten sind zulässig, bedürfen jedoch der vorherigen Abstimmung mit der Zertifizierungsstelle.

4.3.3 Outsourcing

Sind Teile des Informationsverbundes ausgelagert (Outsourcing), ist die Auditierung auf der Basis der ergänzenden Bestimmungen zum Auditierungsschema (siehe *http://www.bsi.bund.de/gshb/zert*) vorzunehmen.

4.4 Phase 2: Umsetzungsprüfung vor Ort

Es ist wichtig, dass das Managementsystem für Informationssicherheit des Informationsverbundes wirksam und effektiv ist, gelebt und weiterentwickelt wird. Dazu gehört auch, dass alle wichtigen Prozesse des Informationsverbundes dokumentiert sind, und nach den Prozessen verfahren wird. Der Auditor prüft die Sicherheitsleitlinie und andere Dokumente und führt intensive Gespräche mit dem Antragsteller, um sich von Effektivität und Effizienz des ISMS zu überzeugen.

Bei der Vor-Ort-Prüfung wird für jede ausgewählte Bausteinzuordnung durch Inspektion des jeweiligen Zielobjekts überprüft, ob der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der in diesen Bausteinen enthaltenen Maßnahmen den tatsächlichen Gegebenheiten entspricht.

Die einzelnen Prüfungen sollen direkt am Zielobjekt vor Ort erfolgen, nicht nur anhand der Papierlage. Bei technischen Aspekten bedeutet dies eine Demonstration durch den jeweils zuständigen Administrator oder dessen Vertreter. Zusätzlich wird die Umsetzung der zusätzlichen Maßnahmen aus der Ergänzenden Risikoanalyse überprüft.

Zudem muss sichergestellt sein, dass die in der Strukturanalyse (A.1) aufgeführten Eigenschaften der IT-Systeme mit den tatsächlichen Gegebenheiten, wie beispielsweise dem jeweils verwendeten Betriebssystem und dem Aufstellungsort, übereinstimmen. Bei der Prüfung der Bausteine der Schicht 3 überprüft der Auditor stichprobenartig, ob die aufgeführten Eigenschaften der IT-Systeme mit den tatsächlichen Eigenschaften übereinstimmen.

Hinweis:

Aufgrund der Vielfalt der unterschiedlichen Einsatzszenarien und Realisierungsmöglichkeiten ist es nicht immer sinnvoll, die Maßnahmen der IT-Grundschutz-Kataloge wörtlich und ohne Anpassung an das Einsatzumfeld umzusetzen. Der Auditor berücksichtigt, ob die Maßnahmen ihrem Sinn und Zweck nach realisiert sind. Unter Berücksichtigung eines Risiko orientierten Ansatzes kann dies beispielsweise auch bedeuten, dass durch gezielte Erhöhung der Wirksamkeit einer Maßnahme eine

andere Maßnahme in ihrer Ausgestaltung von den Forderungen der IT-Grundschutz-Kataloge abweichen kann.

4.5 Übernahme von Risiken durch das Management

Im Rahmen eines Managementreports sind die bestehenden Risiken zu behandeln. Für Maßnahmen, die nicht oder noch nicht vollständig umgesetzt wurden, bedarf es eines Risikobehandlungsplans (vergleiche BSI-Standard 100-2, Kapitel 5.4). Die bestehenden Risiken bis zur vollständigen Umsetzung der noch offenen Maßnahmen sind für das Management transparent darzustellen. Darüber hinaus werden in diesem Dokument auch solche Risiken dokumentiert, für die das Management eine Risiko-Übernahme oder ein Risiko-Transfer (vergl. BSI Standard 100-3) befürwortet.

Die Risikoübernahme muss vom Management durch Unterschrift bestätigt werden (siehe Referenzdokument A.7 Risikobehandlungsplan).

Sind zum Zeitpunkt der Auditierung GS-Maßnahmen des Umsetzungsplans noch nicht oder nur teilweise umgesetzt, entscheidet der Auditor, ob eine Zertifizierung zu diesem Zeitpunkt möglich ist. Der Auditor muss Risiko orientiert den Gesamtkontext des Informationsverbundes und der kritischen Geschäftsprozesse betrachten. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten Institution beitragen, dürfen nicht in diese Risikoübernahmen einfließen.

4.6 Nachbesserungen

Sowohl bei der ersten Sichtung der Referenzdokumente als auch bei der Inspektion vor Ort werden sich in manchen Fällen Abweichungen ergeben. Diese müssen sachgerecht behoben werden. Dabei gibt es verschiedene Stufen der Behandlung von Abweichungen:

1. **Schwerwiegende Abweichungen** sind Mängel, ohne deren Behebung nicht sichergestellt werden kann, dass das Informationssicherheitsmanagementsystem effektiv und effizient funktioniert oder die Sicherheit des Informationsverbundes erheblich gefährdet ist. Ein solcher Mangel kann vorliegen, wenn Grundschutz-Maßnahmen nicht oder in wesentlichen Teilen nicht umgesetzt sind. Bei Vorliegen schwerwiegender Abweichungen ist die Ausstellung eines Zertifikats nicht möglich.
2. **Geringfügige Abweichungen** sind zu kennzeichnen und mit einer Frist zur Behebung zu versehen. D. h., wenn einzelne Aspekte einer Maßnahme nicht umgesetzt wurden, aber das wesentliche Ziel der Maßnahme realisiert ist. Dies ist z. B. dann der Fall, wenn einzelne Teile eines Konzeptes konkretisiert oder aktualisiert werden müssen. Eine Ausstellung des Zertifikats kann unter Umständen trotzdem erfolgen. Mehrere geringfügige Abweichungen können allerdings zusammen eine schwerwiegende Abweichung darstellen.
3. Der Auditor hat die Möglichkeit, **Empfehlungen** an die Institution auszusprechen. Diese sind zwar nicht bindend, erhöhen aber die Effektivität und Effizienz des ISMS. Empfehlungen sind z. B. Verbesserungsvorschläge, die im Rahmen der kontinuierlichen Verbesserung des Prozesses umgesetzt werden sollten, zumindest jedoch zu prüfen sind. Daher führt eine Nichtbeachtung zu einer geringfügigen Abweichung.

Der Auditor entscheidet bei Abweichungen, ob es sich um schwerwiegende oder geringe Abweichungen handelt. Er informiert die Institution möglichst frühzeitig schriftlich über festgestellte Abweichungen, damit diese zeitnah behoben werden können. Er muss der Institution hierzu eine

angemessene Frist einräumen. Die Liste mit den Abweichungen und die Frist zur Nachbesserung für die Korrekturmaßnahmen sowie die Empfehlungen werden im Auditbericht dokumentiert.

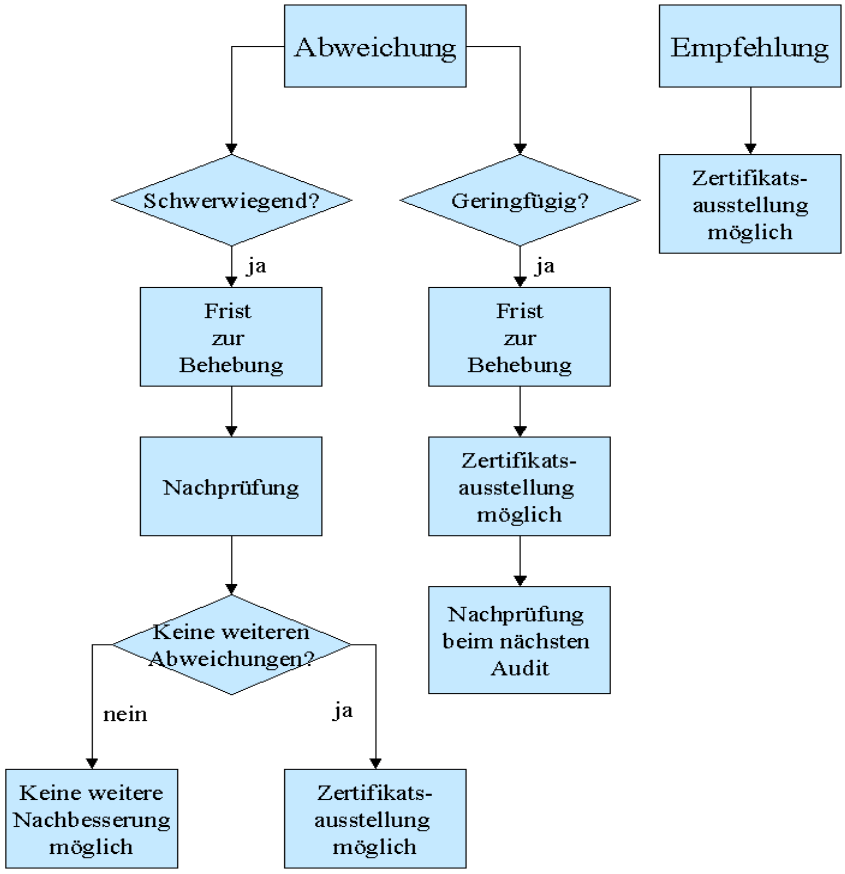


Abbildung 2: Nachbesserungen

Der Auditor prüft anhand der Dokumente und/oder vor Ort, ob alle festgestellten schwerwiegenden Abweichungen behoben wurden und dokumentiert die Prüfungsergebnisse im Auditbericht. Geringfügige Abweichungen werden ebenfalls mit einer Nachbesserungsfrist versehen, deren Behebung kann auch erst beim nächsten Überwachungsaudit begutachtet werden.

Abbildung 3: Abweichungen und Empfehlungen

4.7 Erstellung des Auditberichtes

Für jedes Audit ist vom Auditteamleiter ein Auditbericht zu erstellen, der alle Prüfergebnisse enthält. In Anlehnung an die Aufteilung eines Audits in zwei Phasen ist der Auditbericht in zwei Schritten zu erstellen: Im ersten Schritt dokumentiert der Auditbericht die Auditergebnisse für Phase 1 des Auditprozesses (Dokumentenprüfung), im zweiten Schritt sind die Auditergebnisse aus der Phase 2 des Auditprozesses (Vor-Ort-Prüfung) zu ergänzen. Der auf Phase 1 des Audits bezogene Auditbericht ist vor der Vorbereitung und Durchführung der Vor-Ort-Prüfung in Phase 2 des Audits abzuschließen.

Anhand des Auditberichtes kann der Antragsteller Abweichungen oder Verbesserungsmöglichkeiten in seinem Sicherheitsprozess erkennen.

Im Falle eines Erst- oder Re-Zertifizierungsaudits dient der zugehörige Auditbericht der Zertifizierungsstelle als Grundlage für die Erteilung des Zertifikats. Ein Auditbericht im Rahmen eines Überwachungsaudits bildet für die Zertifizierungsstelle die Grundlage für die Aufrechterhaltung eines erteilten Zertifikats. Der Auditbericht wird der Zertifizierungsstelle unterschrieben in Papierform sowie in elektronischer Form zur Verfügung gestellt.

4.8 Gesamtvotum für die Erteilung eines Zertifikats

Grundlage für die Entscheidung über die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Einschätzung des Auditteamleiters, ob der betrachtete Untersuchungsgegenstand die jeweiligen Anforderungen erfüllt.

Bei dem Gesamtvotum legt der Auditor dar, in welchen Bereichen es noch nicht umgesetzte GS-Maßnahmen gibt. Er bestätigt, dass die Übernahme des Restrisikos durch das Management erfolgt ist und dies auch nach seinen Kenntnissen akzeptabel ist.

Das Gesamtvotum ist vom Auditteamleiter und dem Auditteam mit Datum zu unterschreiben. Die Unterschriften der Mitglieder des Auditteams können dem Auditbericht auch als Anlage hinzugefügt werden.

4.9 Nachforderungen

Die Zertifizierungsstelle informiert den Auditteamleiter über den voraussichtlichen Bearbeitungstermin des eingereichten Auditberichts. Kommt es zu Nachforderungen der Zertifizierungsstelle, sind diese vom Auditteamleiter innerhalb eines Monats zu beheben.

Die Nachforderungen der Zertifizierungsstelle können zu einer Nachbesserung gegenüber dem Antragsteller führen. Der Auditor informiert den Antragsteller entsprechend. Für die Nachbesserung wird dem Antragsteller nur **einmalig** Gelegenheit zur Beseitigung der Defizite gegeben. Der Auditteamleiter dokumentiert die Nachbesserungen im Auditbericht und bewertet diese entsprechend Kapitel 4.6. Nachforderungen der Zertifizierungsstelle gegenüber dem Auditor können mehrmals gestellt werden.

Hat der Antragsteller bezüglich festgestellter Abweichungen eine andere Auffassung als der Auditor, kann er sich schriftlich zu den von dem Auditor dokumentierten Abweichungen äußern. Der Kommentar wird in die Liste der Abweichungen im Auditbericht übernommen. Der Zertifizierungsstelle obliegt dann die Entscheidung, ob die Abweichung behoben werden muss und innerhalb welcher Frist dies zu geschehen hat.

4.10 Zertifikatserteilung

Sobald der Auditbericht zu einem Erst-Zertifizierungsaudit, Überwachungsaudit bzw. Re-Zertifizierungsaudit in vollständiger Fassung bei der Zertifizierungsstelle vorliegt, prüft die Zertifizierungsstelle diesen Auditbericht auf Einhaltung aller Vorgaben des vorliegenden Auditierungsschemas. Die Prüfung gegen das Auditierungsschema erfolgt mit der Zielsetzung, ein einheitliches

Niveau aller Zertifizierungen und die Vergleichbarkeit von einzelnen Zertifizierungsaussagen zu gewährleisten.

5 Voraudit

Beim sogenannten Voraudit kann der Auditor gezielt einzelne Aspekte aus Phase 1 und 2 auswählen und stichprobenartig vor Ort prüfen. Außer intensiven Gesprächen mit dem Antragsteller hat der Auditor die Möglichkeit, sich Dokumente, Prozeduren und Implementierungen anzusehen, um einen Eindruck davon zu bekommen, ob ein Zertifizierungsaudit prinzipiell zu einem positiven Ergebnis führen könnte.

5.1 Umfang des Voraudits

Das Voraudit darf in Summe nicht mehr als ein Drittel der Gesamtzeit für das Zertifizierungsaudit in Anspruch nehmen. Das Voraudit darf nicht dem Zweck dienen, die Institution auf später geprüfte Aspekte vorzubereiten, indem identische Prüfungen wiederholt werden.

5.2 Dokumentation des Voraudits

Prüfungen, die dem Auditor nur dazu dienen, ein Verständnis des Informationsverbundes zu gewinnen, müssen nicht dokumentiert werden. Es können aber Prüfungen vorgezogen werden, d. h. Prüfungen aus dem vorliegenden Auditierungsschema werden bereits im Voraudit durchgeführt. In diesem Fall sind im Auditbericht neben dem Umfang des Voraudits zusätzlich die geprüften Aspekte mit anzuführen.

Hinweis:

Wenn der Auditor ein Voraudit durchführt, ist es sinnvoll, unter anderem die Prüfpunkte zu:

- Aktualität der Dokumente
- IT-Sicherheitsrichtlinien
- Nachvollziehbarkeit der Abgrenzung des Informationsverbunds und
- Wirksamkeit des ISMS

schon zu diesem Zeitpunkt durchzuführen oder anzureißen.

5.3 Verschiebung des Audits

Kommt der Auditor nach dem Voraudit zu der Empfehlung, das Audit mindestens um eine von ihm festgesetzte Zeit aufzuschieben, so teilt er diese dem Antragsteller schriftlich mit. Folgt ihm dieser in seiner Entscheidung, wird der Rest des Audits später an diesem Punkt weitergeführt. Ein erneutes Voraudit ist nicht möglich. Das BSI wird über die Verschiebung des Audits schriftlich informiert.

6 Überwachungsaudit

Ein erteiltes Zertifikat ist mit jährlichen Überwachungsaudits verbunden, das von einem beim BSI lizenzierten ISO 27001 Auditor auf der Basis von IT-Grundschutz durchgeführt werden muss.

Ein Überwachungsaudit dient der Überwachung der für das Zertifikat nachgewiesenen Informationssicherheit im laufenden Betrieb des Informationsverbundes und hat einen deutlich geringeren Umfang als das Erst-Zertifizierungsaudit. Das Überwachungsaudit soll nachweisen, dass das Informationssicherheitsmanagementsystem aktiv ist und weiterentwickelt wird. Zusätzlich erfolgt eine detaillierte Prüfung auf der Basis eines Bausteins aus den Grundschutzkatalogen.

Ein Auditbericht zu einem Überwachungsaudit wird von der Zertifizierungsstelle gegen die Vorgaben dieses Auditierungsschemas geprüft. Nur im Falle der Einhaltung aller Vorgaben bleibt das erteilte Zertifikat gültig. Es erfolgt keine Neuausstellung der Zertifikatsurkunde oder des Zertifizierungsreports.

6.1 Grundlagen des Überwachungsaudits

Für das Überwachungsaudit ist von der zertifizierten Institution eine Zusammenstellung der wesentlichen Änderungen seit letztem Audit bereitzustellen. Zusätzlich erfolgt eine Fortschreibung der vom Antragsteller zu erstellenden Liste der Referenzdokumente (s. Kap. 8 Anlagen zum Auditierungsschema, “Überblick über die Referenzdokumente“).

Aufgrund dieser Zusammenstellung verschafft sich der Auditor einen Überblick über die Änderungen im Untersuchungsgegenstand im Vergleich zum vorhergehenden Audit.

Stellt der Auditor bei seiner Prüfung gravierende Änderungen am Informationsverbund fest und ist der Antragsteller seiner Anzeigepflicht nicht nachgekommen (vergleiche Kapitel 2.8.3 Zertifizierungsschema), informiert der Auditteamleiter die Zertifizierungsstelle hierüber. Die Zertifizierungsstelle entscheidet über das weitere Vorgehen und behält sich in diesem Falle vor, das Zertifikat zurückzuziehen.

Durch die erneute Auditierung soll sichergestellt werden,

- dass die seit der vorhergehenden Zertifizierung unveränderten Komponenten des Informationsverbundes weiterhin die Anforderungen des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz erfüllen,
- dass neue Bausteine, die im Rahmen der regelmäßigen Aktualisierung der IT-Grundschutz-Kataloge hinzugekommen sind, in der Modellierung des Informationsverbundes korrekt berücksichtigt sind,
- dass neue oder aktualisierte Maßnahmen der IT-Grundschutz-Bausteine im vorliegenden Informationsverbund korrekt umgesetzt sind,
- dass durch den Wegfall von Komponenten seit der vorhergehenden Zertifizierung die Informationssicherheit des Informationsverbundes nicht beeinträchtigt wird,
- dass die Informationssicherheit des Informationsverbundes durch Veränderungen in übergeordneten Aspekten, beispielsweise Änderungen der Organisationsstruktur, beeinträchtigt wird.

6.2 Vorbereitung der Auditaktivitäten vor Ort

Die inhaltliche Planung eines Überwachungsaudits umfasst die Erstellung eines Prüfplans durch den Auditteamleiter.

Hierzu gehören insbesondere folgende Aktivitäten des Auditors:

- Ermittlung des Deltas im Informationsverbund
- Festlegung der im Überwachungsaudit zu prüfenden Teilaspekte
- Risiko orientierte Auswahl eines Baustein-Zielobjektes
- Zusammenstellung der Liste der Abweichungen aus der vorhergehenden Auditierung, die im letzten Auditbericht dokumentiert ist (falls vorhanden)
- Zusammenstellung der für das Überwachungsaudit erforderlichen Interviewpartner
- Festlegung der zu auditierenden Standorte

6.3 Überblick über die Auditaktivitäten

Bei der Vor-Ort-Inspektion im Rahmen eines Überwachungsaudits konzentriert der Auditor seine Auditaktivitäten dahingehend, die Wirksamkeit des ISMS zu überprüfen. Zum einen wird das ISMS der zertifizierten Institution stichprobenartig begutachtet, zum anderen wird das Delta im Informationsverbund seit der vorhergehenden Auditierung genauer betrachtet. Der Auditor hat durch die Risiko orientierte Auswahl eines Baustein-Zielobjektes zusätzlich die Möglichkeit, eine detaillierte Prüfung auf Maßnahmenebene vorzunehmen.

Die Auditaktivitäten im Rahmen der Vor-Ort-Inspektion umfassen folgende Punkte:

- Prüfung der Wirksamkeit des ISMS
- Prüfung der Verbesserung und Aufrechterhaltung der Informationssicherheit
- Prüfung der Änderungen am zertifizierten Informationsverbund
- Prüfung der Behebung von Abweichungen, die im vorhergehenden Audit erkannt wurden
- Prüfung eines Baustein-Zielobjektes
- Prüfung der Restrisiken gemäß Referenzdokument A.7
- Prüfung der Einhaltung mit dem Zertifikat verbundener Auflagen

Eine erneute Vor-Ort-Prüfung von Nachbesserung des Antragstellers während des Überwachungsaudits ist nicht vorgesehen.

6.4 Gesamtvotum für die Aufrechterhaltung des Zertifikats

Grundlage für die Entscheidung über die Aufrechterhaltung eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Einschätzung des Auditteamleiters, ob der betrachtete Untersuchungsgegenstand die jeweiligen Anforderungen erfüllt. Der Auditteamleiter dokumentiert die Ergebnisse des Überwachungsaudits in einem Auditbericht. Der Auditbericht ist auf der Basis des Musters für Überwachungsaudits zu erstellen (siehe Hilfsmittel: http://www.bsi.bund.de/gshb/zert).

7 Re-Zertifizierungsaudit

Eine Re-Zertifizierung setzt einen erneuten Antrag voraus (vergleiche Kapitel 2.8.3 Zertifizierungsschema).

Mit einer Re-Zertifizierung wird der auditierten Institution bescheinigt, dass die Voraussetzungen für die Erfüllung einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz weiterhin vorliegen.

Die Auditaktivitäten unterscheiden sich grundsätzlich nicht von denen eines Erst-Zertifizierungsaudits. Bei der Auswahl von Stichproben sind redundante Prüfungen zu den vorhergehenden Audits nur in begründeten Ausnahmefällen zulässig. Ein erneutes Voraudit ist nicht zulässig.

8 Anlagen zum Auditierungsschema

Nachfolgend aufgeführte Dokumente sind verbindlich anzuwenden. Die Dokumente stehen auf der BSI-Web-Seite
https://www.bsi.bund.de/grundschutz/zert/ISO27001/Schema/zertifizierungsschema.html
zur Verfügung.

Thema	Inhalt
Vorlage Auditbericht	Verbindliche Vorlage eines Auditberichts im Rahmen einer Erst-Zertifizierung oder für eine Re-Zertifizierung
Anlage Umsetzungsprüfung Basissicherheitsscheck	Beispiel zur Dokumentation der Umsetzungsprüfung eines Basissicherheitscheck, die als Anlage zum Auditbericht mit zu erfassen ist
Vorlage Auditbericht für ein Überwachungsaudit	Verbindliche Vorlage eines Auditberichts im Rahmen eines Überwachungsaudits
Überblick über die Referenzdokumente	Fortzuschreibendes Dokument, das vom Antragsteller zu liefernden ist und die wesentlichen Änderungen der Referenzdokumente beschreibt
Regelungen zum Outsourcing: „IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten“	Enthält Prüfungshinweise für den Auditor, wenn Teile des Informationsverbunds im Rahmen eines Outsourcing ausgelagert sind
Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz ()	Enthält die vom Auditteam zu beachtenden Prüfgrundlagen, insbesondere die gültigen Versionsstände der Grundschutzkataloge für die Auditierung