Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Zertifizierungsschema

Version 2.1

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

E-Mail: gs-zert@bsi.bund.de oder De-Mail: gs-zert@bsi-bund.de-mail.de
Internet: https://www.bsi.bund.de/

Inhaltsverzeichnis

Vorwort

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.

Rechtliche Grundlagen des Verfahrens sind das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG, [BSIG]) und die Zertifizierungsverordnung zum BSI-Gesetz [ZVO].

Die für ISO 27001-Zertifizierungsverfahren auf der Basis von IT-Grundschutz relevanten Kriterienwerke sind ISO/IEC 27001 "Information technology - Security techniques - Information security management systems – Requirements", die BSI-Standards 200-2 „IT-Grundschutz-Methodik“ [2002] und BSI-Standard 200-3 „Risikoanalyse auf Basis von IT-Grundschutz“ [2003] sowie das IT-Grundschutz-Kompendium des BSI. Für weitere Informationen sei auf Kap. 1.6 verwiesen.

Grundlage dieses Dokumentes bilden ferner die Normen ISO/IEC 27006 „Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems“ sowie DIN EN ISO/IEC 17021 "Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren", welche Anleitungen und Anforderungen für den Ablauf und die Durchführung von Audits und Zertifizierungsverfahren enthalten.

1. Einleitung

1.1 Versionshistorie

Datum	Version	Verfasser	Bemerkungen
29.03.2011	1.0	BSI	1. veröffentlichte Version
12.03.2013	1.1	BSI	**Überarbeitung Kapitel 2.6** Vertraulichkeit von Informationen: Ergänzung der Verschlüsselungsprogramme GnuPG, Pretty Good Privacy (PGP) und TrueCrypt
18.06.2013	1.11	BSI	**Editorelle Änderungen** (Referatsbezeichnungen)
13.03.2014	1.12	BSI	**Editorelle Änderungen** (E-Mail-Adresse, Referatsbezeichnung)
22.05.2014	1.2	BSI	**Editorelle Änderungen** (Kontaktadressen, Mailpostfächer, Ersetzung Erfüllungsgehilfe durch Fachexperte) Ergänzung Kapitel 2.4, Unabhängigkeitserklärung **Kapitel 2.8.3**: Konkretisierung der Meldung ggü. BSI bei wesentlichen Änderungen des Informationsverbundes **Kapitel 2.6:** Streichung Verschlüsselungsprogramm TrueCrypt
08.09.2016	1.21	BSI	**Editorelle Änderungen** (Kontaktadressen)
29.09.2017	2.0	BSI	Anpassung an GS-Kompendium
23.07.2019	2.1	BSI	**Editorelle Änderungen** (Referatsbezeichnungen, Kontaktadressen) **Kapitel 1.7:** Redaktionelle Änderung **Kapitel 2.4:** Konkretisierung zu Unabhängigkeitserklärungen **Kapitel 2.8.3:** Abstimmung Bausteinauswahl bei Re-Zertifizierung **Kapitel 2.10:** Änderung Unterschriften Auditbericht

1.2 Zielsetzung

Das vorliegende Zertifizierungsschema beschreibt die grundsätzliche Vorgehensweise und die Voraussetzungen für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz. Das Dokument gibt insbesondere Informationen zu den am Zertifizierungsverfahren beteiligten Parteien und deren Verantwortlichkeiten, Aufgaben, Aktivitäten und Zusammenwirken.

1.3 Adressatenkreis

Dieses Dokument richtet sich an Institutionen, die eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz anstreben, sowie an ISO 27001-Auditoren auf der Basis von IT-Grundschutz, die ein unabhängiges Audit durchführen, um die Konformität eines Managementsystems für Informationssicherheit gemäß ISO 27001 auf der Basis von IT-Grundschutz in einer Einrichtung oder Institution zu bestätigen. Insbesondere können sich Einrichtungen und Institutionen und deren IT-Sicherheitsverantwortliche sowie Auditoren einen Überblick über die grundsätzlichen Anforderungen an eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz verschaffen und über die Vorgehensweise einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz informieren.

1.4 Anwendungshinweise

Im folgenden Dokument werden die grundsätzliche Vorgehensweise und die Voraussetzungen für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz beschrieben.

Detaillierte Informationen zur Zielsetzung und Durchführung von ISO 27001-Audits auf der Basis von IT-Grundschutz und insbesondere eine detaillierte Beschreibung des Auditprozesses und seiner Phasen, der Auditprinzipien, der Verantwortlichkeiten der Mitglieder des Auditteams und der im einzelnen vom Auditteam durchzuführenden Prüfaufgaben und -aktivitäten sowie der Mitwirkung des Antragstellers werden im Rahmen eines eigenen Schemadokuments zum Auditierungsschema für ISO 27001-Audits auf der Basis von IT-Grundschutz gegeben (siehe [AUD]).

1.5 Begriffe und Definitionen

Ein Informationsverbund stellt nicht nur den Verbund der betrachteten IT-Systeme dar, sondern umfasst auch das damit verbundene Informationssicherheits-Managementsystem (ab hier ISMS abgekürzt). Der Informationsverbund ist der Geltungsbereich der Zertifizierung (sog. Untersuchungsgegenstand).

Audits können von einem oder mehreren Auditoren durchgeführt werden, die vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert[1] sind. Der für die Durchführung eines Audits verantwortliche Auditor wird in diesem Dokument Auditteamleiter genannt. Einem Auditteam können auch Fachexperten angehören, die spezielle Branchenkenntnisse oder solide Kenntnisse und Erfahrungen hinsichtlich der im Informationsverbund eingesetzten Informations- und Kommunikationstechnik besitzen. Die Rollen der beteiligten Parteien im Zertifizierungsaudit sind in Kap. 2.2 näher ausgeführt.

1.6 Literaturverzeichnis

[AUD]	Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Auditierungsschema mit Anlagen, Version 2.2
[PRÜFGR]	Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz in der jeweils veröffentlichten Version
[REFDOK]	Hinweise zur Bereitstellung der Referenzdokumente im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Version 2.0
[ZERTAUD]	Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen
[17021]	DIN EN ISO/IEC 17021-1:2011 "Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren"
[19011]	DIN EN ISO 19011:2011 „Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen“
[27001]	DIN EN ISO/IEC 27001:2017 „Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen "
[27002]	DIN EN ISO/IEC 27002:2005 "Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management"
[27006]	ISO/IEC 27006:2011 „Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems“
[2002]	BSI-Standard 2002 „IT-Grundschutz-Methodik“
[2003]	BSI-Standard 2003 „Risikoanalyse auf Basis von IT-Grundschutz“
[GSK]	IT-Grundschutz-Kompendium, BSI
[BSIG]	BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist

[1] In diesem Dokument wird nicht unterschieden zwischen zertifizierten und den nach dem früheren Lizenzierungsschema lizenzierten Auditoren, beide werden hier als zertifizierte Auditoren bezeichnet.

[ZVO] BSI-Zertifizierungs- und -Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231), die durch Artikel 40 des Gesetzes vom 29. März 2017 (BGBl. I S. 626) geändert worden ist"

1.7 Kontakt, Fragen und Anregungen

Bei Fragen zum Zertifizierungsprozess, Anregungen zur Verbesserung und Weiterentwicklung des Zertifizierungsschemas, und für die Zusendung von Zertifizierungsunterlagen (z. B. Zertifizierungsantrag, Unabhängigkeitserklärung, abgenommener Auditbericht in Schriftform) verwenden Sie bitte die nachfolgenden Kontaktdaten:

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 25
Postfach 20 03 63
53133 Bonn
Telefon: 0228 99 9582-6660
E-Mail: gs-zert@bsi.bund.de
De-Mail: gs-zert@bsi-bund.de-mail.de

Wenn Sie Fragen oder Anregungen zur Durchführung von Audits, zum Auditierungsschema und der Prüfbegleitung haben, wenden Sie sich bitte an:

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 13
Postfach 20 03 63
53133 Bonn
Telefon: 0228 99 9582-6222
E-Mail: gs-zert-pruef@bsi.bund.de
De-Mail: gs-zert-pruef@bsi-bund.de-mail.de

Fragen und Anregungen rund um IT-Grundschutz können Sie richten an:

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 13
Postfach 20 03 63
53133 Bonn
Telefon: 0228 99 9582-5369
E-Mail: grundschutz@bsi.bund.de

Auditberichte zur Abnahme durch BSI schicken Sie bitte verschlüsselt (siehe Kapitel 2.6) an:
E-Mail: gs-zert-pruef@bsi.bund.de

2. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

2.1 Überblick über den Zertifizierungsprozess

Die IT-Grundschutz-Vorgehensweisen Standard- und Kern-Absicherung stellen zusammen mit dem IT-Grundschutz-Kompendium und dessen Empfehlungen von Standard-Sicherheitsmaßnahmen inzwischen einen De-Facto-Standard für Informationssicherheit dar.

Voraussetzung für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist eine Überprüfung des Untersuchungsgegenstandes durch einen vom BSI zertifizierten Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz. Im Rahmen des Audits werden von der Institution erstellte Referenzdokumente gesichtet, eine Vor-Ort-Prüfung durchgeführt und ein Auditbericht erstellt. Für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz wird dieser Auditbericht von der Zertifizierungsstelle im BSI geprüft. Während der Gültigkeit des daraufhin ausgestellten Zertifikats werden jährlich Überwachungsaudits durchgeführt.

In den folgenden Kapiteln wird der Zertifizierungsprozess detaillierter betrachtet.

2.2 Rollen und Zuständigkeiten im Zertifizierungsverfahren

In das Zertifizierungsverfahren für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sind die folgenden drei Rollen involviert:

- Antragsteller,
- Auditor bzw. Auditteamleiter als befugter Vertreter des Auditteams
- Zertifizierungsstelle

Folgende Abbildung zeigt schematisch die den Rollen zugeordneten Aufgaben und das Zusammenwirken der Rollen im Zertifizierungsverfahren:

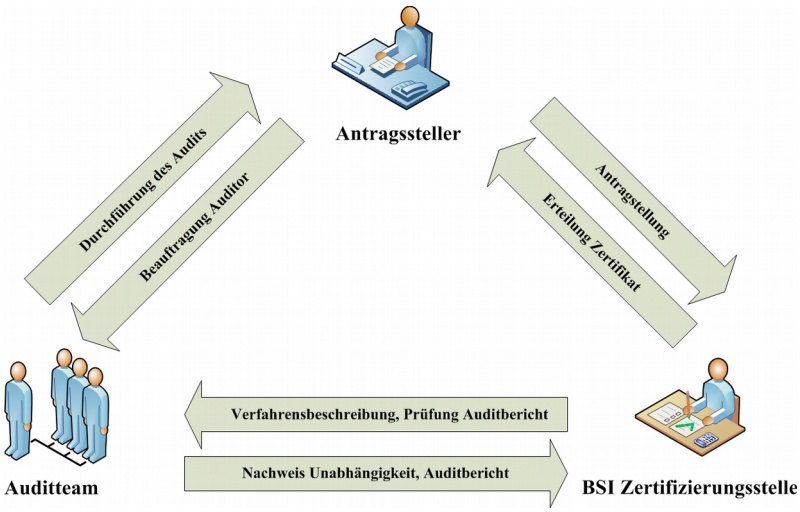

Abbildung 1: Rollen im Zertifizierungsverfahren

Hat eine Institution ein ISMS nach ISO 27001 auf Basis der IT-Grundschutz-Methodik umgesetzt und liegen alle erforderlichen Nachweise der Umsetzung (sog. Referenzdokumente [REFDOK]) vor, kann

die Institution ein Zertifizierungsverfahren für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz bei der Zertifizierungsstelle initiieren und einen Zertifizierungsantrag stellen. Die Institution beauftragt ein Auditteam, auf Grundlage des vorliegenden Zertifizierungsschemas und des zugehörigen Auditierungsschemas für ISO 27001-Audits auf der Basis von IT-Grundschutz den Informationsverbund, sein ISMS und seine Sicherheitsstruktur zu überprüfen.

Der **Antragsteller** ist Initiator des Zertifizierungsverfahrens und unterstützt das Auditteam bei der Sichtung der Referenzdokumente und der Vor-Ort-Prüfung des Informationsverbundes. Das Auditteam dokumentiert seine Prüfergebnisse in einem Auditbericht, der zusammen mit dem Zertifizierungsantrag der Zertifizierungsstelle als Grundlage für ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz dient.

Auditoren dürfen nur Themengebiete prüfen, für die sie das notwendige Fachwissen und ausreichend Erfahrung mitbringen. Falls weder der Auditteamleiter noch die anderen Auditoren des Teams über das nötige Spezialwissen verfügen, muss der Auditteamleiter zur Unterstützung der Prüftätigkeiten und zur Absicherung der Prüfaussagen einen oder mehrere Fachexperten hinzuziehen.

Zwei oder mehr Auditoren können sich zu einem Auditteam zusammenschließen, um ein gemeinsames Audit durchzuführen. In einem solchen Fall wird ein Auditteamleiter (Auditverantwortlicher) bestimmt. Die Rollen und Zuständigkeiten der Teammitglieder sind zu Beginn des Zertifizierungsverfahrens festzulegen. Ein Auditteam kann darüber hinaus noch Fachexperten zur Unterstützung hinzuziehen. Fachexperten müssen ebenso wie die Auditoren Fachwissen sowie Erfahrung im Bereich Informationssicherheit besitzen und sind Teil des Auditteams. Jedes Mitglied des Auditteams muss vor Beginn des Verfahrens, d. h. mit dem Zertifizierungsantrag, sowie vor einem Überwachungsaudit eine Unabhängigkeitserklärung bei der Zertifizierungsstelle einreichen. Die Zertifizierungsstelle des BSI muss dem Einsatz des Auditors bzw. des Auditteams zustimmen. Alle Mitglieder des Auditteams müssen im Auditbericht aufgeführt sein.

Der Ansprechpartner der Zertifizierungsstelle ist der Auditteamleiter. Dieser sendet den Auditbericht verschlüsselt an die Zertifizierungsstelle des BSI und ergänzt Nachforderungen. Je nach Vertragsinhalt kann der Auditor dem Antragsteller den Auditbericht jederzeit zur Verfügung stellen.

Hilfskräfte für reine Verwaltungstätigkeiten, beispielsweise Schreibkräfte, können eingesetzt werden, wenn diese vom Auditteamleiter entsprechend überwacht und kontrolliert werden. Für Hilfskräfte gelten keine einschränkenden Bedingungen; sie müssen auch nicht im Auditbericht genannt werden. Die Verantwortung für die Prüftätigkeiten verbleibt in jedem Fall beim Auditteamleiter.

Die **Zertifizierungsstelle** des BSI übernimmt die Rolle einer unabhängigen dritten Instanz, die die Gleichwertigkeit der Prüfungen und der Auditberichte gewährleistet. Sie veröffentlicht die Schemata und Interpretationen zum Zertifizierungsverfahren. Die Zertifizierungsstelle prüft den Zertifizierungsantrag des Antragstellers und den eingereichten Auditbericht des Auditteams auf Grundlage des vorliegenden Zertifizierungsschemas und des zugehörigen Auditierungsschemas für ISO 27001-Audits auf der Basis von IT-Grundschutz. Bei positivem Prüfergebnis erteilt die Zertifizierungsstelle für den Informationsverbund des Antragstellers ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz.

Antragsteller und Auditteamleiter sollten bei der Planung von Zertifizierungsverfahren darauf achten, dass genügend Zeit und Ressourcen (Budget, Personal, ...) für Kommentierungszyklen von Auditberichten und eventuelle Nachbesserungen bzw. Nachforderungen eingeplant werden.

2.3 Zertifizierungsantrag

Zur Initiierung des Zertifizierungsverfahrens ist vom Antragsteller ein Antrag auf eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz bei der Zertifizierungsstelle des BSI zu stellen. Hierbei sind folgende Anforderungen zu erfüllen:

- Der Zertifizierungsstelle des BSI muss der vollständige Zertifizierungsantrag mindestens 1 Monat vor Beginn des Audits (d. h. vor Beginn der Sichtung der Referenzdokumente) vorliegen. In Einzelfällen kann die Prüfung länger dauern, sodass evtl. Audittermine angepasst werden müssen.
- Der Zertifizierungsantrag enthält Angaben zum Antragsteller und verschiedene weitere Informationen zum Untersuchungsgegenstand (d. h. zum zu zertifizierenden Informationsverbund) sowie zur Auditierungstätigkeit. Insbesondere müssen die im Folgenden genannten Angaben vollständig sein:
  - Der zu zertifizierende Untersuchungsgegenstand ist zu beschreiben. Ferner ist ein kurzes Behörden- bzw. Firmenprofil zu geben, aus dem u. a. die wesentlichen Tätigkeitsfelder der Institution sowie die Größe und Bedeutung des Untersuchungsgegenstandes für die Institution deutlich werden.
  - Bei einer Re-Zertifizierung sind die Änderungen im Informationsverbund im Vergleich zum Informationsverbund der Erst-Zertifizierung anzugeben und kurz zu beschreiben. Bei der Verwendung überarbeiteter oder neuer Bausteine sind diese im Antrag mit anzugeben und zu beschreiben. Dabei werden nur große / gravierende Änderungen aufgeführt.
  - Im Zertifizierungsantrag sind Angaben zur Abgabe des Auditberichts an die Zertifizierungsstelle des BSI zu machen. Der Zeitplan ist mit der Zertifizierungsstelle des BSI abzustimmen. Terminänderungen sind dem BSI rechtzeitig schriftlich mitzuteilen.
  - Teil des Zertifizierungsantrags ist die Unabhängigkeitserklärung der Auditteammitglieder (s. nächstes Kapitel).

Formulare zur Antragstellung sowie für die Unabhängigkeitserklärung sind auf den Webseiten des BSI zu finden. Als Prüfungsgrundlage für Auditierungen im Rahmen der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz müssen die in „Prüfgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz“ [PRÜFGR] aufgeführten Dokumente in der dort genannten Version verwendet werden.

Der Zertifizierungsantrag muss im Original in Papierform oder als absenderbestätigte De-Mail dem BSI zugestellt werden.

Die Zertifizierungsstelle prüft den eingereichten Zertifizierungsantrag auf Vollständigkeit, Konsistenz und Erfüllung der o. g. Anforderungen. Ferner wird im Rahmen der Antragsprüfung die prinzipielle Zertifizierbarkeit des Untersuchungsgegenstandes, also die sinnvolle Abgrenzung des Informationsverbunds geprüft und wenn nötig abgestimmt. Bei positiver Prüfung des Zertifizierungsantrags wird das Zertifizierungsverfahren in Reihenfolge der vollständig eingegangenen Anträge offiziell eröffnet und eine Zertifizierungskennung vergeben. Die Verfahrenseröffnung und die Zertifizierungskennung werden dem Antragsteller schriftlich und dem Auditteamleiter per E-Mail bzw. telefonisch mitgeteilt und wenn gewünscht auf der BSI-Webseite veröffentlicht. Mit der Sichtung der Referenzdokumente darf nicht vor Verfahrenseröffnung begonnen werden, d.h. das Audit darf erst nach Mitteilung der Zertifizierungskennung beginnen.

2.4 Unabhängigkeitserklärung

Jedes Mitglied des Auditteams (Auditteamleiter, Auditoren, Fachexperten) muss der Zertifizierungsstelle des BSI gegenüber eine Unabhängigkeitserklärung mit Begründung abgeben. Wenn ein Mitglied des Auditteams (Auditteamleiter, Auditor, Fachexperten) oder die Firma, für die der Betreffende tätig ist, in Beziehung zu der zu auditierenden Institution oder Teilen davon bzw. zu beratenden Institutionen oder Personen steht, die einen Interessenskonflikt hervorrufen kann, ist diese Unabhängigkeit in der Regel nicht mehr gegeben. Eine solche Gefährdung kann z. B. bei folgenden Konstellationen auftreten, wobei ein Zeitraum von drei Jahren betrachtet wird:

- Beratung der Institution durch den Auditor selbst oder einen Kollegen / Vorgesetzten / Mitarbeiter des Auditors
- andere geschäftliche Verbindungen des Auditors oder des Arbeitgebers des Auditors und der auditierten Institution
- Verwandtschaftsverhältnis des Auditors mit Mitgliedern / verantwortlichen Personen der auditierten Institution oder eines Beraters
- Geschäftsanbahnung (z.B. nicht erfolgreiche Bewerbung um eine Beratung)

Rein auditierende Tätigkeiten sind hiervon explizit ausgenommen.

Diese Unabhängigkeitserklärung muss der Zertifizierungsstelle des BSI bei einer Erst- oder Re-Zertifizierung mindestens 1 Monat vor Beginn der Auditierungstätigkeit vorliegen. Die Unabhängigkeitserklärung muss im Original in Papierform vom Antragsteller mit dem Zertifizierungsantrag eingereicht werden. Alternativ kann die Unabhängkeitserklärung auch direkt vom Auditor im Original in Papierform oder per absenderbestätigter De-Mail eingereicht werden.Solange der Nachweis nicht vorliegt oder ungenügend ist, kann dieses Mitglied des Auditteams für das beantragte Verfahren nicht eingesetzt werden. Nachmeldungen von Auditteammitgliedern müssen der Zertifizierungsstelle formlos, gerne per E-Mail, mitgeteilt werden.

Die Zertifizierungsstelle des BSI behält sich vor, zusätzliche Informationen zum Verhältnis zwischen Auditor und Antragsteller bzw. beratender Institution einzufordern. Sieht sie die Unabhängigkeit von Mitgliedern des Auditteams nicht gewährleistet, widerspricht sie der Teilnahme dieser Auditteammitglieder am Audit. Mit Vergabe der Zertifizierungskennung wird das im Antrag aufgeführte Auditteam akzeptiert.

Stellt das Auditteam z.B. bei der Vorbereitung auf die Phase 2 des Audits (Vor-Ort-Prüfung) fest, dass weitere Auditteammitglieder benötigt werden, so müssen diese Unabhängigkeitserklärungen nachreichen[2]. Das neue Auditteammitglied darf erst eingesetzt werden, nachdem dessen Unabhängigkeit durch das BSI bestätigt wurde. Dies geschieht in der Regel durch eine E-Mail vom BSI an den Auditteamleiter mit Kopie an Antragsteller und das neue Auditteammitglied.

Für Überwachungsaudits ist ebenfalls eine (erneute) Unabhängigkeitserklärung für jedes Mitglied des Auditteams einzureichen. Diese Unabhängigkeitserklärung muss der Zertifizierungsstelle mindestens 1 Monat vor Beginn der Auditierungstätigkeit vorliegen. Die Bestätigung der Unabhängigkeit erfolgt in der Regel durch E-Mail vom BSI an den Auditteamleiter mit Kopie an den Antragsteller und alle anderen Auditteammitglieder.

Formulare zur Antragstellung sowie für die Unabhängigkeitserklärung sind auf den Webseiten des BSI zu finden.

2.5 Auswahl des Auditteams

Für die Auditierung des Informationsverbundes der Institution beauftragt diese ein Auditteam damit, in einer unabhängigen Prüfung den Status der Informationssicherheit im Informationsverbund zu prüfen und zu verifizieren. Mindestens der Auditteamleiter und die Auditoren müssen eine gültige BSI-

[2] Die Unabhängigkeitserklärung ist unverzüglich der Zertifizierungsstelle des BSI einzureichen. Eine Frist von 1 Monat vor Auditweiterführung ist nicht einzuhalten.

Zertifizierung (s. [ZERTAUD]) besitzen. Kontaktadressen der zertifizierten Auditoren finden sich im Internet auf den Webseiten des BSI.

Das Auditteam wird von der antragstellenden Institution beauftragt und der Zertifizierungsstelle des BSI im Zertifizierungsantrag bekannt gegeben. Bei der Auswahl des Auditteams müssen Besonderheiten im Aufbau und in den Prozessen und Gegebenheiten der beauftragenden Institution berücksichtigt werden. Die Mitglieder des Auditteams müssen die Fachkenntnisse besitzen, die sie zur Auditierung der Institution benötigen. Da der Auditteamleiter durch sein positives oder negatives Votum für das Ergebnis des Zertifizierungsaudits verantwortlich ist, muss er die Auditteammitglieder nach Qualifikation und Erfahrung auswählen und einsetzen.

Die Mitglieder des Auditteams müssen der Zertifizierungsstelle des BSI frühzeitig einen ausführlichen Nachweis vorlegen, dass ihre Unabhängigkeit in den geplanten Audits nicht gefährdet ist. Die Zertifizierungsstelle des BSI behält sich das Recht vor, von der antragstellenden Institution gewählte Auditoren abzulehnen.

Für eine optimale Prozessgestaltung empfiehlt es sich, für die beiden während der Zertifikatslaufzeit erforderlichen Überwachungsaudits das Auditteam aus dem Zertifizierungsaudit zu wählen. Wechselt das Auditteam, ist von der antragstellenden Institution dafür Sorge zu sorgen, dass (mindestens) die Referenzdokumente sowie alle vorhergehenden Auditberichte aus der zugrunde liegenden Zertifizierung (Auditbericht aus dem Zertifizierungsprozess selbst sowie ggf. der Auditbericht aus dem ersten Überwachungsaudit, falls bereits erfolgt) dem Auditteam für das Überwachungsaudit zur Verfügung stehen. Außerdem ist damit zu rechnen, dass die Aufwände des Auditteams wegen der erneuten Einarbeitung deutlich höher sein können.

2.6 Vertraulichkeit von Informationen

Zur Gewährleistung der Vertraulichkeit zum Beispiel bei der Übergabe der Referenzdokumente müssen geeignete Maßnahmen ergriffen werden. Zertifizierte Auditoren sind durch vertragliche Vereinbarungen mit dem BSI verpflichtet, Details zum Auditierungs- und Zertifizierungsverfahren und zu im Rahmen des Audits gewonnenen Informationen streng vertraulich zu behandeln sowie Kollegen und Dritten Informationen nur zu geben, soweit ihre Kenntnis unbedingt notwendig und mit den vertraglichen Vereinbarungen mit dem BSI und der auditierten Organisation vereinbar ist.

Die elektronische Übermittlung des Auditberichts durch den Auditteamleiter an das BSI muss aus Gründen der Vertraulichkeit unbedingt verschlüsselt erfolgen. Der Auditbericht wird unter Verweis auf die entsprechende Zertifizierungskennnummer (BSI-IGZ-0xxx) an das Postfach gs-zert-pruef@bsi.bund.de geschickt, optional kann er auch in Kopie an den zuständigen Zertifizierer gesandt werden.

Zur Verschlüsselung können nachfolgende Programme eingesetzt werden:

- Chiasmus
- GnuPG
- Pretty Good Privacy (PGP)

Eine kostenlose Version von Chiasmus wird dem Auditteam auf Anfrage zur Verfügung gestellt, eine Nutzung der o.g. Verschlüsselungsprogramme im GS-Tool ist nicht möglich.

2.7 Ziel eines Audits und Auditphasen

Ziel des Audits ist die unabhängige Überprüfung des ISMS nach ISO 27001 auf der Basis von IT-Grundschutz in einem fest definierten Geltungsbereich einer Organisation.

Jedes Audit setzt sich grundsätzlich aus zwei getrennten, aufeinander aufbauenden Phasen zusammen:

- Phase 1: Dokumentenprüfung
  Phase 1 umfasst zunächst die Dokumentenprüfung, d. h. die Prüfung der

Referenzdokumente, die von der zu auditierenden Institution erstellt und für die Zertifizierung eingereicht werden.

- Phase 2: Umsetzungsprüfung vor Ort
  Auf der Grundlage der Dokumentenprüfung bereitet sich das Auditteam auf die Vor-Ort-Prüfung vor. In Phase 2 schließt sich eine Vor-Ort-Prüfung des Informationsverbundes durch das Auditteam an, in der im realen Informationsverbund die praktische Umsetzung der in den Referenzdokumenten dokumentierten Sicherheitsmaßnahmen bzgl. ISO 27001 und IT-Grundschutz auf ihre Angemessenheit, Korrektheit und die Wirksamkeit des ISMS hin überprüft wird (Umsetzungsprüfung).

Details zur Planung und Durchführung von Audits sowie der Anfertigung von Auditberichten sind in den Dokumenten [AUD] nachzulesen.

2.8 Audittypen

Für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sind – bezogen auf die dreijährige Laufzeit eines Zertifikates – verschiedene Typen von Audits zu unterscheiden:

- Erst-Zertifizierungsaudit: Im Rahmen eines Erst-Zertifizierungsaudits wird erstmalig der betreffende Informationsverbund der Institution unter ISO 27001- und IT-Grundschutz-Aspekten auditiert. Im Rahmen des Erst-Zertifizierungsaudits kann ein sogenanntes Voraudit (s. Kap. 2.8.1) durchgeführt werden.
- Überwachungsaudit: In die dreijährige Laufzeit eines Zertifikates integriert sind jährliche Überwachungsaudits des zertifizierten Informationsverbundes, die auf die Kontrolle der für das Zertifikat nachgewiesenen Informationssicherheit im Informationsverbund zielen. Das Audit dient dem Nachweis, dass der zertifizierte Informationsverbund weiterhin den Anforderungen bzgl. ISO 27001 und IT-Grundschutz genügt.
- Re-Zertifizierungsaudit: Nach Ablauf der Zertifikatslaufzeit von drei Jahren wird eine Re-Zertifizierung des Informationsverbundes erforderlich, sofern weiter eine Zertifizierung des Informationsverbundes angestrebt ist. Diese umfasst insbesondere ein Re-Zertifizierungsaudit des Informationsverbundes, das zum großen Teil identisch zum Erst-Zertifizierungsaudit abläuft.

Erst-Zertifizierungsaudit, Überwachungsaudit und Re-Zertifizierungsaudit unterscheiden sich hinsichtlich ihrer Zielsetzung und ihres Umfangs voneinander. Bei jedem Typ von Audit findet aber eine Initialisierung (wie z. B. Antragstellung, Klärung von Zuständigkeiten und Befugnissen, Abstimmungen) und eine Bewertung (Schreiben des Auditberichts durch das Auditteam, Sicherstellen der Vergleichbarkeit von Zertifizierungsverfahren durch die Zertifizierungsstelle) statt.

Ein Voraudit ist im Rahmen des Erst-Zertifizierungsaudits zulässig. Im Rahmen eines Re-Zertifizierungsaudits ist ein Voraudit nur bei einer wesentlichen Erweiterung oder Veränderung des Geltungsbereichs der Zertifizierung, also des Informationsverbundes, zulässig.

2.8.1 Erst-Zertifizierung

Ein Erst-Zertifizierungsverfahren wird mit der Annahme des Zertifizierungsantrags durch die Zertifizierungsstelle des BSI eröffnet. Erst nach Beginn des Zertifizierungsverfahrens und Vergabe der Zertifizierungskennung kann mit der Prüfung begonnen werden.

Im Rahmen eines Erst-Zertifizierungsverfahrens kann ein sogenannten Voraudit durchgeführt werden. Dabei kann das Auditteam gezielt einzelne Aspekte aus Phase 1 und 2 auswählen und stichprobenartig prüfen. Außer intensiven Gesprächen mit dem Antragsteller hat das Auditteam die Möglichkeit, sich Dokumente, Prozeduren und Implementierungen anzusehen, um einen Eindruck davon zu bekommen, ob ein Zertifizierungsaudit prinzipiell zu einem positiven Ergebnis führen könnte.

In der Dokumentenprüfung werden die vom Antragsteller vorgelegten Referenzdokumente durch das Auditteam geprüft. Nach Abschluss der Dokumentenprüfung entscheidet das Auditteam auf Grundlage

der Ergebnisse aus dieser Auditphase, ob eine Fortsetzung des Audits mit der Umsetzungsprüfung vor Ort sinnvoll ist und erweitert ggf. das Auditteam. Anschließend begutachtet das Auditteam in der Umsetzungsprüfung vor Ort auf Basis seines Auditplans stichprobenartig die Umsetzung der dokumentierten Sachverhalte. Die Prüfergebnisse werden im Auditbericht festgehalten. Teil des Auditberichts ist der Auditplan, welcher eine erste, grobe Planung der Überwachungsaudits enthält.

Sobald der Auditbericht zu einem Erst-Zertifizierungsaudit in vollständiger Fassung bei der Zertifizierungsstelle vorliegt und die Rechnung für die Zertifizierung vom Antragsteller beglichen wurde, prüft die Zertifizierungsstelle diesen Auditbericht auf Einhaltung aller Vorgaben des Auditierungsschemas für ISO 27001-Audits auf der Basis von IT-Grundschutz. Die Prüfung gegen das Auditierungsschema erfolgt mit der Zielsetzung, ein einheitliches Niveau aller ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz und die Vergleichbarkeit von Zertifizierungsaussagen zu gewährleisten.

Der Auditbericht darf sich nur auf Prüfungen des Auditteams (Dokumentenprüfungen und Umsetzungsprüfung) stützen, die zum Zeitpunkt der Übergabe des Auditberichts an die Zertifizierungsstelle nicht älter als drei Monate sind. Nachforderungen der Zertifizierungsstelle müssen innerhalb von einem Monat durch das Auditteam erfüllt werden, diese dürfen maximal eine Nachbesserung durch den Antragsteller nach sich ziehen. Dagegen sind mehrere Nachforderungen an den Auditbericht durch die Zertifizierungsstelle des BSI möglich. Wenn drei Monate nach Abgabe des ersten Auditberichts das Verfahren noch nicht abgeschlossen ist, prüft die Zertifizierungsstelle des BSI, ob auf der Basis des vorliegenden Berichts noch ein Zertifikat erteilt werden kann.

Ist im Rahmen der Zertifizierung vom Antragsteller eine Pressemitteilung geplant, so sollte diese mit dem BSI abgestimmt und rechtzeitig vor Veröffentlichung der Zertifizierungsstelle des BSI zur Kommentierung zur Verfügung gestellt werden.

Ein im Rahmen einer Erst-Zertifizierung erteiltes Zertifikat ist drei Jahre gültig und mit jährlichen Überwachungsaudits verbunden. Treten während der Zertifikatslaufdauer wesentliche Änderungen am zertifizierten Informationsverbund auf (wie z.B. größere Änderungen im Managementsystem, Änderungen in der Organisation, Änderungen im Outsourcing, Standortwechsel, Änderungen von Tätigkeitsfeldern), muss der Antragsteller diese der Zertifizierungsstelle des BSI schriftlich mitteilen, s. Kapitel 2.8.3.

2.8.2 Überwachungsaudits

Die Überwachungsaudits sind Teil des Erst- bzw. Re-Zertifizierungsverfahrens. Aus diesem Grund ist kein erneuter Antrag notwendig. Eine erneute Unabhängigkeitserklärung aller Auditteammitglieder muss der Zertifizierungsstelle des BSI 1 Monat vor Beginn des Audits vorliegen.

Das Überwachungsaudit sowie der zugehörige Auditbericht und dessen Prüfung durch die Zertifizierungsstelle des BSI müssen 1 Jahr bzw. 2 Jahre nach Ausstellung des Zertifikates abgeschlossen sein. Dabei ist vom Auditteamleiter darauf zu achten, dass genügend Raum für die Beseitigung von im Überwachungsaudit festgestellten Abweichungen sowie für die Erstellung des Auditberichts eingeplant wird.

Die Prüfungen des Überwachungsaudits dürfen nicht früher als 3 Monate vor Ablauf des 1. bzw. 2. Jahres nach Zertifikatserteilung beginnen und der Auditbericht darf nicht später als 2 Monate vor diesem Zeitpunkt bei der Zertifizierungsstelle eingetroffen sein (Vergleich zusammenfassende Darstellung in Kap. 3.3). Ausnahmen sind rechtzeitig mit dem zuständigen Zertifizierer abzustimmen. Andere Rahmenbedingungen wie z. B. ein Wechsel des Auditteams im Vergleich zum Erst-Audit oder zum 1. Überwachungsaudit müssen frühzeitig (mind. 1 Monat vorher) der Zertifizierungsstelle angezeigt werden. Nachforderungen der Zertifizierungsstelle müssen innerhalb von einem Monat durch das Auditteam erfüllt werden, diese dürfen maximal eine Nachbesserung durch den Antragsteller nach sich ziehen.

Kommt das Auditteam insgesamt über beide Auditphasen zu einem positiven Prüfergebnis, sendet der Auditteamleiter den finalen Auditbericht an die Zertifizierungsstelle des BSI. Bei einem negativen Ergebnis muss das BSI ebenfalls hierüber informiert werden. Die Zertifizierungsstelle des BSI

überprüft den finalen Auditbericht auf Vollständigkeit, Nachvollziehbarkeit und Reproduzierbarkeit der Prüfergebnisse. Nachforderungen oder Nachfragen werden an den Auditteamleiter gestellt, der die ggf. bestehenden Unklarheiten beseitigt. Nur bei positivem Abschluss des Prüfprozesses bleibt das vom BSI erteilte ISO 27001-Zertifikat auf der Basis von IT-Grundschutz weiterhin gültig.

Nach einem Überwachungsaudit erfolgt keine Neuausstellung der Zertifikatsurkunde oder Ergänzung des zugehörigen Anhangs durch die Zertifizierungsstelle. Der Antragsteller erhält nach positiver Prüfung durch Auditteam und Zertifizierungsstelle ein Schreiben über diese Tatsache, welches die Zertifikatsurkunde ergänzt.

Bei nicht fristgerechter Einreichung des Auditberichts oder negativem Abschluss des Überwachungsaudits behält sich die Zertifizierungsstelle das Recht vor, das bestehende Zertifikat auszusetzen oder ggf. zu entziehen, s. Kap. 2.12.

Außer den planmäßigen Überwachungsaudits, welche zweimal im Zertifizierungsverfahren durchgeführt werden, können außerplanmäßige Überwachungsaudits notwendig werden. Ein außerplanmäßiges Überwachungsaudit kann beispielsweise zur Überprüfung der Behebung schwerwiegender Abweichungen oder durch die Änderung des Untersuchungsgegenstandes notwendig werden. Die Kosten, die in der Zertifizierungsstelle durch außerplanmäßige Überwachungsaudits entstehen, sind nicht in die Pauschale für die Zertifizierung eingerechnet und werden zusätzlich nach Kostenverordnung abgerechnet.

2.8.3 Re-Zertifizierung

Die Gültigkeit von ISO 27001-Zertifikaten auf der Basis von IT-Grundschutz ist auf drei Jahre begrenzt. Sind in dieser Zeit wesentliche Änderungen (wie z. B. größere Änderungen im Managementsystem, Änderungen in der Organisation, Änderungen im Outsourcing, Standortwechsel, Änderungen von Tätigkeitsfeldern) am zertifizierten Informationsverbund geplant, muss der Antragsteller diese der Zertifizierungsstelle des BSI unverzüglich schriftlich mitteilen. Das BSI entscheidet dann, ob eine vorzeitige Re-Zertifizierung erforderlich ist. Im Falle einer Re-Zertifizierung ist immer ein Zertifizierungsantrag zu stellen.

Vor Ablauf des Gültigkeitszeitraums eines Zertifikats ist im Falle, dass der Antragsteller weiterhin ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz für seinen Informationsverbund wünscht, stets eine erneute Zertifizierung des Untersuchungsgegenstands erforderlich, um zu dokumentieren, dass die Voraussetzungen für die Erfüllung der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz noch erfüllt sind. Dieses Zertifizierungsverfahren läuft als Re-Zertifizierungsverfahren, sofern sich der ursprüngliche Untersuchungsgegenstand nicht grundlegend geändert hat und die Re-Zertifizierung sich nahtlos an die Zertifizierung anschließt oder innerhalb angemessener Zeit nach Ablauf der Gültigkeit gestartet wird (ca. ein halbes Jahr). Um eine lückenlose Zertifizierung eines Untersuchungsgegenstands zu erreichen, muss die Re-Zertifizierung vor Ablauf des Gültigkeitszeitraums des Erstzertifikats abgeschlossen sein. Ein Antrag auf Re-Zertifizierung oder ein laufendes Re-Zertifizierungsverfahren verlängert die Gültigkeit des Erstzertifikats nicht.

Das Re-Zertifizierungsverfahren, sein Ablauf und seine Rahmenbedingungen sind einer Erst-Zertifizierung vergleichbar und sind sinngemäß zu übertragen, wobei der Bezug zum ablaufenden Zertifikat deutlich gemacht werden muss (z. B. Erläuterung Bausteinauswahl, Darstellung Änderungen). Ein Voraudit darf bei einer Re-Zertifizierung nur bei einer wesentlichen Erweiterung oder Veränderung des Geltungsbereichs der Zertifizierung, also des Informationsverbundes, erfolgen. Ein Re-Zertifizierungsaudit darf frühestens vier Monate vor Ablauf des Zertifikates beginnen, der Auditbericht muss der Zertifizierungsstelle des BSI spätestens zwei Monate vor Ablauf des Zertifikates vorliegen (Vergleich zusammenfassende Darstellung in Kap. 3.3). Nachforderungen der Zertifizierungsstelle müssen innerhalb von einem Monat durch das Auditteam erfüllt werden, diese dürfen maximal eine Nachbesserung durch den Antragsteller nach sich ziehen.

Ab der ersten Re-Zertifizierung eines nach Kompendium (re-)zertifizierten Untersuchungsgegenstands müssen die zu prüfenden Bausteine vor Beginn der Auditierung mit dem BSI formlos per E-Mail abgestimmt werden. Das BSI behält sich hierbei eine Änderung der Auswahl grundsätzlich vor.

Ein im Rahmen einer Re-Zertifizierung erteiltes Zertifikat ist wie ein Erst-Zertifikat für drei Jahre gültig und ebenfalls mit jährlichen Überwachungsaudits verknüpft.

2.9 Prüf- und Auditbegleitung der Zertifizierungsstelle des BSI

Das BSI hat ein Zertifizierungs- bzw. Anerkennungsschema [ZERTAUD] aufgebaut, das die Vergleichbarkeit von Zertifizierungsverfahren und die Kompetenz der zertifizierten Auditoren sicherstellt.

Die Prüfbegleitung durch die Zertifizierungsstelle erfolgt durch die intensive Prüfung des Auditberichts. Dabei wird vor allem auf die Vergleichbarkeit zwischen den Zertifizierungsverfahren geachtet.

Die Zertifizierungsstelle kann in Absprache mit dem Antragsteller einen Teil des Audits begleiten. Die Reisekosten werden dem Antragsteller in diesem Fall gemäß Kostenverordnung in Rechnung gestellt.

Ergänzender Hinweis: Nicht Thema dieses Dokuments ist die Begleitung eines Mitgliedes des Auditteams durch die Personenzertifizierungsstelle des BSI im Rahmen seines Vertrages mit dem BSI. Diese ist in der Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern und dem Programm zur Kompetenzfeststellung von Zertifizierung von Personen im Detail geregelt [ZERTAUD].

2.10 Auditbericht

Für jedes Audit ist zur Dokumentation aller Prüfaktivitäten und -ergebnisse vom Auditteamleiter ein Auditbericht zu erstellen. Das Format und die Inhalte eines Auditberichts sind im Detail im Auditierungsschema für ISO 27001-Audits auf der Basis von IT-Grundschutz [AUD] definiert. Die Referenzdokumente des Antragstellers sind als Anlagen dem Auditbericht beizufügen und gelten als Bestandteil des Auditberichts. Vorversionen des Auditberichts, welchen z.B. nur die Prüfergebnisse für Phase 1 enthalten, sind in der Regel nicht an die Zertifizierungsstelle zu übersenden.

Der Auditbericht richtet sich ausschließlich an den Antragsteller und die Zertifizierungsstelle des BSI. Die Ergebnisse des Auditberichts werden vom Auditteam und von der Zertifizierungsstelle des BSI vertraulich behandelt und nicht an Dritte weitergegeben. Sofern ein anderes Auditteam als das im Zertifizierungsaudit eingesetzte ein Überwachungsaudit durchführt, müssen vom Antragsteller die Auditdokumente, darunter auch der Auditbericht des Zertifizierungsaudits und im Falle des zweiten Überwachungsaudits auch der Auditbericht des ersten Überwachungsaudits an den neuen Auditteamleiter weitergegeben werden.

Im Falle eines Erst- oder Re-Zertifizierungsaudits dient der zugehörige Auditbericht der Zertifizierungsstelle als Grundlage für die Erteilung eines Zertifikats. Ein Auditbericht im Rahmen eines Überwachungsaudits bildet für die Zertifizierungsstelle die Grundlage für die Aufrechterhaltung eines bereits erteilten Zertifikates.

Alle an die Zertifizierungsstelle des BSI gesandten Versionen des Auditberichts werden zur einfacheren Bearbeitung in elektronischer Form zur Verfügung gestellt. Dabei müssen mindestens das Drucken und das Entnehmen von Inhalt zulässig sein. Bei Aktualisierungen des Auditberichts müssen Änderungen zur Vorversion kenntlich gemacht sein. Die abgenommene Version des Auditberichts wird der Zertifizierungsstelle zusätzlich im Original in Papierform mit der Unterschrift des Auditteamleiters oder als absenderbestätigte De-Mail zugesandt (s. Kap. 1.7). Der Auditbericht muss der Zertifizierungsstelle verschlüsselt zugesandt werden (s. Kap. 2.6).

2.11 Zertifikatserteilung

Nach positiver Bewertung des Auditprozesses durch die Zertifizierungsstelle des BSI erteilt das BSI auf der Grundlage des Zertifizierungsantrags und des abgenommenen Auditberichts für den

vorliegenden Informationsverbund ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz. Sie fertigt ein Zertifikat und einen Zertifizierungsreport mit zusätzlichen Informationen zum Zertifizierungsverfahren (z.B. Auflagen) sowie einen Zertifikatsbutton für Werbezwecke an. Diese Dokumente werden mit dem Zertifizierungsbescheid, dem Widerspruchsverzicht und ggf. den Verwendungsbedingungen für den Zertifikatsbutton an den Antragsteller gesandt.

Sofern der Antragsteller einer Veröffentlichung des Zertifikates nicht explizit widersprochen hat, wird die Tatsache der Zertifizierung einen Monat nach Zustellung des Zertifikats oder nach Rücksendung des Widerspruchsverzichts auf den Internetseiten des BSI veröffentlicht. Auf Nachfrage muss die Zertifizierungsstelle des BSI jedoch Auskünfte zu allen erteilten Zertifikaten geben.

Die zertifizierte Institution darf das Zertifikat sowie einen vom BSI zur Verfügung gestellten Zertifikatsbutton nur unter der Bedingung verwenden, dass das Zertifikat und der zugehörige Zertifizierungsreport jederzeit auf Nachfrage zur Verfügung gestellt werden sowie die mit dem Zertifikatsbutton verbundenen und der zertifizierten Institution mitgeteilten Verwendungsbedingungen für den Button beachtet werden. Ist das Zertifikat nicht mehr gültig oder ist das Zertifikat ausgesetzt, darf weder mit dem Zertifikatsbutton noch mit dem Zertifikat (weiter) geworben werden.

2.12 Aussetzung und Zurückziehung von Zertifikaten

2.12.1 Aussetzung von Zertifikaten

Die Zertifizierungsstelle des BSI behält sich vor, erteilte Zertifikate auszusetzen. Mögliche Gründe hierfür können sein:

- Das Überwachungsaudit wird nicht fristgerecht durchgeführt, die Zertifizierungsstelle des BSI ist über die Planung informiert.
- Der Auditbericht zum Überwachungsaudit wird zu spät bei der Zertifizierungsstelle eingereicht, die Zertifizierungsstelle des BSI ist über die Planung informiert.
- Im Überwachungsaudit werden schwerwiegende Abweichungen im Informationsverbund bzgl. seiner Dokumentation und/oder Realisierung erkannt, die vom Antragsteller innerhalb der vom Auditteam gesetzten Frist noch nicht behoben sind, sich aber in Umsetzung befinden.

Ausgesetzte Zertifikate werden aus der Liste der ISO 27001-Zertifikate auf der Basis von IT-Grundschutz auf den Internetseiten des BSI entfernt. Mit ausgesetzten Zertifikaten und dem zugehörigen Zertifikatsbutton darf keine Werbung mehr betrieben werden.

Die Zertifizierungsstelle macht Vorgaben bezüglich des Umgangs mit den für die Aussetzung eines Zertifikates festgestellten Gründen und bestimmt das weitere Vorgehen. Sind die Ursachen, die zur Aussetzung eines Zertifikates geführt haben, den Vorgaben der Zertifizierungsstelle entsprechend beseitigt, erhält das betreffende Zertifikat seine Gültigkeit zurück und wird unverändert wieder in die Liste der ISO 27001-Zertifikate auf der Basis von IT-Grundschutz auf den Internetseiten des BSI aufgenommen.

2.12.2 Zurückziehung von Zertifikaten

Die Zertifizierungsstelle des BSI hat die Möglichkeit, Zertifikate zurückzuziehen. Mögliche Gründe hierfür können sein:

- Das Überwachungsaudit wird nicht durchgeführt.
- Im Überwachungsaudit werden gravierende Abweichungen im Informationsverbund bzgl. seiner Dokumentation und / oder Realisierung erkannt, die vom Antragsteller nicht in einem angemessenen Zeitraum behoben werden können.
- Ein Überwachungsaudit ergibt, dass der Informationsverbund die Anforderungen an ein ISMS nicht mehr erfüllt bzw. den Anforderungen des IT-Grundschutzes nicht mehr gerecht wird.

- Der Verstoß gegen Auflagen aus der Zertifizierung wird bekannt (beispielsweise ein Verstoß gegen die Verwendungsbedingungen für das Zertifikat, die Nichteinhaltung von Auflagen, die sich aus dem Zertifizierungsreport oder Zertifizierungsbescheid ergeben, wie etwa wesentliche Veränderungen am zertifizierten Informationsverbund ohne Information an die Zertifizierungsstelle, Irreführungen und Täuschungen der Institution gegenüber dem Auditteam bzw. dem BSI, begründete Beschwerden beim BSI über die Institution).
- Abweichungen und Empfehlungen aus dem Auditbericht werden ohne ausreichende Begründung nicht behoben bzw. beachtet.

Zurückgezogene Zertifikate werden aus der Liste der ISO 27001-Zertifikate auf der Basis von IT-Grundschutz (auch auf den Internetseiten des BSI) entfernt. Die Zertifikatsurkunde und der Zertifizierungsreport werden vom Zertifikatsinhaber im Original zurückgefordert und sind an die Zertifizierungsstelle zurückzugeben. Mit zurückgezogenen Zertifikaten und dem zugehörigen Zertifikatsbutton darf keine Werbung mehr betrieben werden.

Ein zurückgezogenes Zertifikat kann nicht wieder aktiviert und in einen gültigen Zustand versetzt werden. Für den betreffenden Informationsverbund ist, falls vorgesehen, ein neues Zertifizierungsverfahren aufzusetzen.

Hält das BSI es z. B. nach Beschwerden über die Institution für erforderlich, kurzfristig ein außerplanmäßiges Audit durchzuführen oder durch ein Auditteam durchführen zu lassen, so läuft dies nach den Vorgaben dieses Dokumentes und dem Auditierungsschema für ISO 27001-Audits auf der Basis von IT-Grundschutz ab. Bei begründeten Beschwerden ist die Durchführung dieses Audits kostenpflichtig.

2.13 Beschwerdeverfahren

Beschwerden zum Zertifizierungsverfahren ISO 27001 auf der Basis von IT-Grundschutz können formlos per Post oder elektronisch an das

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 25
Postfach 200363
53133 Bonn
gs-zert@bsi.bund.de oder gs-zert@bsi-bund.de-mail.de

adressiert eingehen.

Eingang und Termin der Bearbeitung werden dem Beschwerdeführer daraufhin kurzfristig mitgeteilt. Die Beschwerde wird registriert und anschließend geprüft. Sofern die Beschwerde nach Prüfung berechtigt ist, werden entsprechende Korrektur- und Vorbeugungsmaßnahmen ergriffen, über die der Beschwerdeführer benachrichtigt wird.

Sollte die Prüfung zum Ergebnis haben, dass die Beschwerde ungerechtfertigt ist, so wird der Beschwerdeführer auch hierüber unterrichtet.

Gegen Bescheide der Zertifizierungsstelle ist das Rechtsmittel des Widerspruchs gegeben, der schriftlich oder zur Niederschrift an das Bundesamt für Sicherheit in der Informationstechnik zu richten ist.

3. Formulare und Übersichten

3.1 Anträge

Alle Anträge und Formulare zur ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sind auf den Webseiten des BSI veröffentlicht. Dort findet sich insbesondere der Zertifizierungsantrag für ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz und eine Auflistung, welche Dokumente zum jeweiligen Zeitpunkt Grundlage der Zertifizierung sind. Alle Auditoren, die ISO 27001-Audits auf der Basis von IT-Grundschutz durchführen dürfen, sind auf der BSI-Webseite gelistet.

3.2 Unabhängigkeitserklärung der Mitglieder des Auditteams

Zu Beginn eines ISO 27001-Zertifizierungsverfahrens auf der Basis von IT-Grundschutz und vor jedem Überwachungsaudit ist eine Unabhängigkeitserklärung aller am Verfahren beteiligten Auditteammitglieder bei der Zertifizierungsstelle einzureichen. Ein Formular dafür ist auf den Webseiten des BSI veröffentlicht.

3.3 Übersicht über den Zeitverlauf der Zertifizierung

Diese Zusammenfassung des Zeitverlaufs der Zertifizierung mit einzuhaltenden Fristen soll Antragsteller und Auditteam einen Überblick geben über die in der Zertifizierung einzuhaltenden Zeiten. In diesem Kapitel sind keine neuen Informationen enthalten, sondern nur in diesem Dokument bereits aufgeführte Fristen noch einmal zusammengestellt.

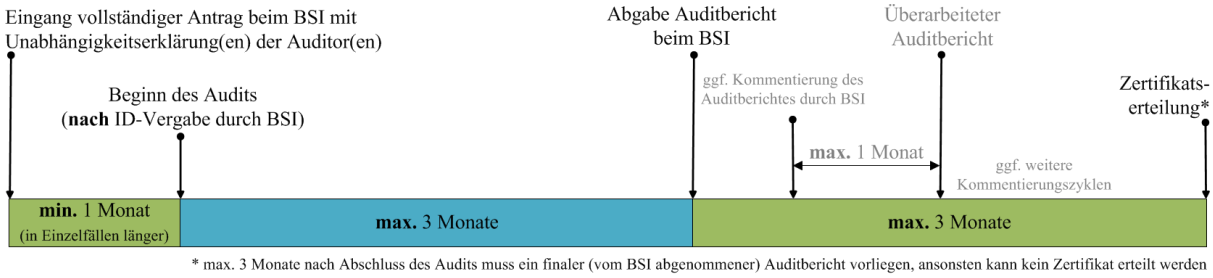

Abbildung 2: Antrags- und Auditierungsphase

Der vollständige Antrag inklusive der Unabhängigkeitserklärung der Auditteammitglieder muss der Zertifizierungsstelle des BSI mindestens 1 Monat vor Beginn des Audits, d. h. vor Beginn der Sichtung der Referenzdokumente, vorliegen. In Einzelfällen kann die Prüfung länger dauern, sodass evtl. Audittermine angepasst werden müssen.

Spätestens 3 Monate nach dem Beginn der Sichtung der Referenzdokumente muss der Auditbericht der Zertifizierungsstelle vorliegen. Nachforderungen der Zertifizierungsstelle müssen jeweils nach spätestens 1 Monat erfüllt sein. Wenn drei Monate nach Abgabe des ersten Auditberichts das Verfahren noch nicht abgeschlossen ist, prüft die Zertifizierungsstelle des BSI, ob auf der Basis des vorliegenden Berichts noch ein Zertifikat erteilt werden kann.

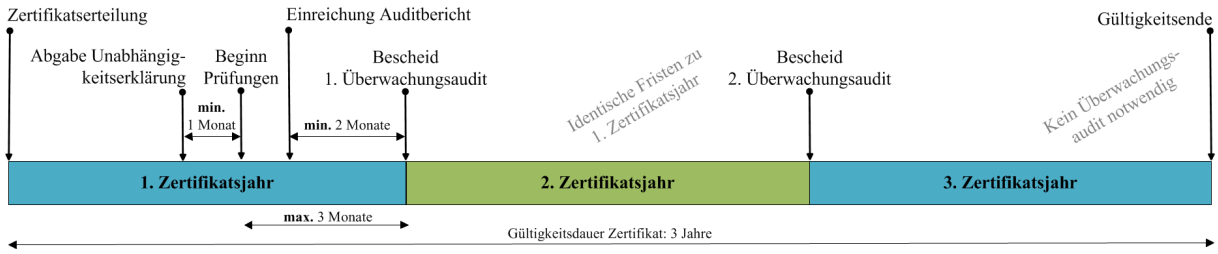

Abbildung 3: Fristen Überwachungsaudit

Das Überwachungsaudit sowie der zugehörige Auditbericht und dessen Prüfung durch die Zertifizierungsstelle des BSI müssen 1 Jahr bzw. 2 Jahre nach Ausstellung des Zertifikates abgeschlossen sein. Dabei sollten die Prüfungen nicht früher als 3 Monate vor Ablauf des 1. bzw. 2. Jahres nach Zertifikatserteilung beginnen und der Auditbericht sollte nicht später als 2 Monate vor diesem Zeitpunkt bei der Zertifizierungsstelle eingetroffen sein.

Die Unabhängigkeitserklärungen für das Überwachungsaudit müssen der Zertifizierungsstelle mindestens 1 Monat vor Beginn der Auditierungstätigkeit vorliegen.

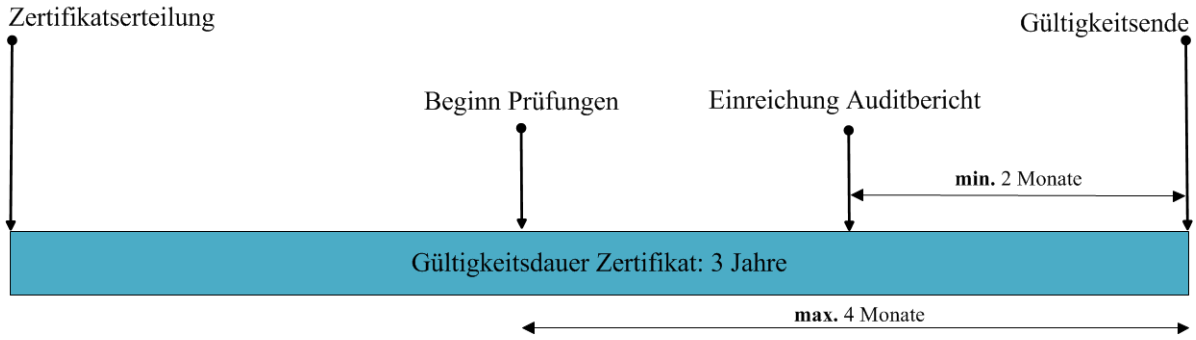

Abbildung 4: Fristen Re-Zertifizierung

Bei einer Re-Zertifizierung darf mit der Sichtung der Referenzdokumente frühestens 4 Monate vor Auslaufen des Zertifikates begonnen werden. Der Auditbericht muss der Zertifizierungsstelle des BSI mindestens 2 Monate vor dem Gültigkeitsende des Zertifikates vorliegen. Darüber hinaus gelten die gleichen Fristen wie für ein Erst-Zertifizierungsaudit (s. Abbildung 2: Antrags- und Auditierungsphase)