Bundesamt
für Sicherheit in der
Informationstechnik

Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern

VB-Stellen

Version 3.3Stand 06.02.2018

Änderungshistorie

Version	Datum	Name	Beschreibung
1.0	09.07.2009	Anerkennungsstelle S 25	Erstausgabe
2.0	06.08.2010	Anerkennungsstelle S 25	Neuausgabe
2.6	26.11.2013	Anerkennungsstelle S 25	Letzte Revision vor Neuausgabe
3.0	20.07.2015	QMB S	Neuausgabe nach Umgestaltung der Dokumentenstruktur
3.1	02.08.2016	QMB D	Revision: • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) • Ergänzung in Kapitel 2 „Anerkennungs- und Zertifizierungsprogramm für Stellen“ sowie • kleinere sprachliche Korrekturen.
3.1.1	20.12.2016	QMB D	Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm)
3.2	14.08.2017	QMB D	Revision: • im gesamten Dokument: Geltungsbereiche UP-Bund ersetzt durch IS-Revision und IS-Penetrationstest • im gesamten Dokument: Entfernung des nicht gültigen Geltungsbereichs eID-Integration • Kapitel 3.2.2: Präzisierung der Begutachtungsgrundlagen • Kapitel 3.2.2: Anpassung der Vorgaben zur Behebung von Abweichungen vor (Re)Anerkennung/(Re)Zertifizierung • Kapitel 5.3.1: Präzisierung Obliegenheiten der Prüfstelle bzgl. Termingestaltung • Kapitel 5.4.2: Präzisierung von Anforderungen an die Unterbeauftragung • kleinere sprachliche Korrekturen
3.3	06.02.2018	Anerkennungsstelle D25	Revision • Gesamtes Dokument: Anpassungen hinsichtlich der gültigen Fassung der DIN EN ISO/IEC 17025 • Kapitel 2.1: Klarstellung bzgl. des Auslaufens des

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Version	Datum	Name	Beschreibung
			Geltungsbereichs ITSEC • Kapitel 3.2.2 Anpassungen an neue Regelungen und Verfahren der Anerkennung, insbesondere Einstufung der Abweichungen in „kritisch“ und „nicht-kritisch“ • Kapitel 3.2.3 Präzisierung zum Ablauf der Anerknnungs- bzw. Zertifizierungsphase • kleinere sprachliche Korrekturen • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm)

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem BSI-Gesetz [BSIG] die Aufgabe, Zertifizierungen informationstechnischer Produkte oder Komponenten sowie informationstechnischer Systeme durchzuführen. Die Prüfungen für diese Zertifizierungen führen vom BSI anerkannte Prüfstellen oder zertifizierte Personen durch. Zudem kann das BSI IT-Sicherheitsdienstleister zertifizieren.

Um diese Aufgaben zu erfüllen, betreibt das BSI Zertifizierungs- und Anerkennungsprogramme, in denen jeweils die Regeln (Geltungsbereiche, bedarfsgerechte Prüfkriterien, Anforderungen und Nachweise), das Verfahren sowie das Management zur Durchführung der Zertifizierung bzw. Anerkennung festgelegt und beschrieben sind.

Eine Anerkennung als Prüfstelle oder Zertifizierung als IT-Sicherheitsdienstleister wird auf Antrag eines Antragstellers (Betreiber einer Stelle) durchgeführt. Grundvoraussetzung für eine Anerkennung als Prüfstelle oder Zertifizierung als IT-Sicherheitsdienstleister ist die Erfüllung der Anforderungen der DIN EN ISO/IEC 17025 [17025] in ihrer jeweils gültigen Fassung[1]sowie dieser Verfahrensbeschreibung mit den zugehörigen Anforderungsdokumenten.

Sowohl bei einer Anerkennung als Prüfstelle als auch bei einer Zertifizierung als IT-Sicherheitsdienstleister ist das zugrundeliegende fachliche Verfahren identisch. Daher wird im Folgenden der Begriff Verfahren einheitlich für beide genutzt. Prüfstellen und IT-Sicherheitsdienstleister werden in diesem Dokument kurz unter dem Begriff Stellen zusammengefasst.

1.1 Zielsetzung und Eingliederung der VB-Stellen

Einen Überblick über die Zertifizierungs- und Anerkennungsprogramme sowie der zugehörigen Dokumente gibt die folgende Abbildung. Diese Dokumente stellen Informationen zielgruppenorientiert zur Verfügung.

1 Aktuell sind dieses die DIN EN ISO/IEC 17025:2005 (bei bestehenden Prüfstellen und IT-Sicherheitsdienstleistern, sofern diese noch nicht umgestellt haben) sowie die im März erscheinende DIN EN ISO/IEC 17025:2018 (für neue Prüfstellen bzw. IT-Sicherheitsdienstleister).

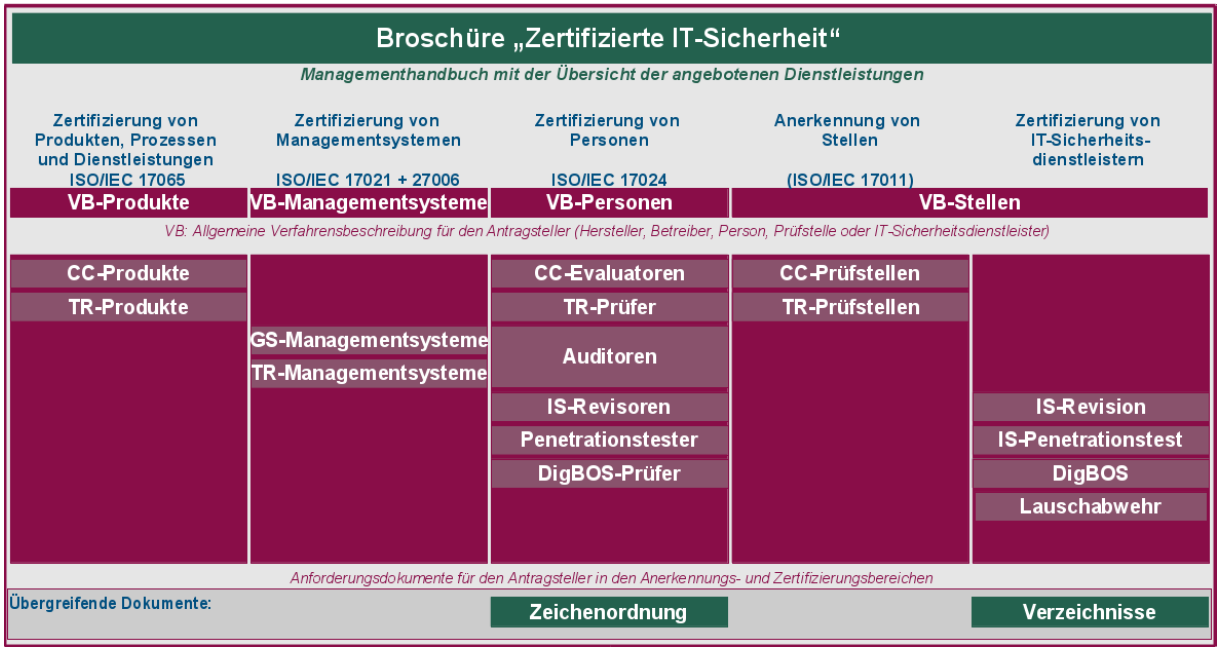

Abbildung 1: Zertifizierungs- und Anerkennungsprogramme (Dokumentenübersicht)

Die übergeordnete Broschüre „Zertifizierte IT-Sicherheit“ [Broschüre] richtet sich an Personen, die sich über den Auftrag des BSI im Bereich der Konformitätsbewertung im Allgemeinen informieren möchten.

In den jeweiligen „Verfahrensbeschreibungen“ (VB) des Zertifzierungs- und Anerkennungsprogramms werden der Nutzen für den Antragsteller, das Verfahren und die damit verbundenen Rechte und Pflichten sowie Obliegenheiten dargestellt. Sie sind Entscheidungshilfe, wenn die Absicht besteht, einen Antrag zu stellen und richten sich somit an:

- Hersteller, die ihre Produkte zertifizieren [VB-Produkte],
- Betreiber, die ihre Systeme zertifizieren [VB-Managementsysteme],
- Personen, die sich zertifizieren [VB-Personen],
- Prüfstellen, die sich anerkennen (vorliegende VB-Stellen) und
- IT-Sicherheitsdienstleister, die sich zertifizieren (vorliegende VB-Stellen)

lassen wollen.

Spezielle Anforderungen für den jeweiligen Geltungsbereich mit detaillierten Hinweisen zu Verfahrens-abläufen befinden sich in den jeweiligen „Anforderungsdokumenten“ und richten sich an den konkreten Antragsteller.

Die vorliegende VB-Stellen wird durch die Anforderungsdokumente:

- Anforderungen für Antragsteller zur Anerkennung als Prüfstelle im Bereich Common Criteria [CC-Prüfstellen],
- Anforderungen für Antragsteller zur Anerkennung als Prüfstelle im Bereich Technische Richtlinien [TR-Prüfstellen],
- Anforderungen für Antragsteller zur Zertifizierung als IT-Sicherheitsdienstleister im Bereich IS-Revision [IS-Revision],

- Anforderungen für Antragsteller zur Zertifizierung als IT-Sicherheitsdienstleister im Bereich IS-Penetrationstest [IS-Penetrationstest],
- Anforderungen für Antragsteller zur Zertifizierung als IT-Sicherheitsdienstleister im Bereich Digitalfunk BOS [DigBOS]
- und
- Anforderungen für Antragsteller zur Zertifizierung als IT-Sicherheitsdienstleister im Bereich Lauschabwehr [Lauschabwehr]

ergänzt.

Das Dokument „Verzeichnisse“ [Verzeichnisse] gibt einen Überblick über alle benötigten Hilfs- und Informationsquellen (Literaturverzeichnis) und enthält ein Stichwort- und Abkürzungsverzeichnis (Glossar).

Das Dokument „Zeichenordnung“ [Zeichenordnung] enthält alle Zeichen der Konformitätsbewertung mit den jeweiligen Rechten und Bedingungen.

1.2 Nutzen der Anerkennung bzw. Zertifizierung für den Antragsteller

1.2.1 Nutzen der Anerkennung als Prüfstelle

Zur Durchführung einer Produktzertifizierung benötigt ein Produkthersteller eine Prüfstelle, die die Evaluierung des zu zertifizierenden Produktes durchführt. Die Prüfstelle wird vom Produkthersteller ausgewählt und (in der Regel kostenpflichtig) beauftragt. Eine Prüfstelle kann grundsätzlich nur dann als sachverständige Stelle für die Produktzertifizierungsstellen des BSI Evaluierungen durchführen, wenn sie durch das BSI als sachverständige Stelle anerkannt wurde.

Anerkannte Prüfstellen haben die Möglichkeit, aktiv an der Stärkung der Sicherheit von nationalen und internationalen IT- Produkten mitzuwirken und sind berechtigt, Evaluierungen im Rahmen von Produktzertifizierungen des BSI durchzuführen.

Viele anerkannte Prüfstellen des BSI haben sich für bestimme Produktbereiche besonders qualifiziert und werden beispielsweise für Beratungstätigkeiten beauftragt.

1.2.2 Nutzen der Zertifizierung als IT-Sicherheitsdienstleister

Mit der Zertifizierung als IT-Sicherheitsdienstleister wird durch das BSI bestätigt, dass eine Organisation die beschriebenen Anforderungen erfüllt. Insbesondere im gesetzlich geregelten Bereich (Behördenbereich) wird bei bestimmten Tätigkeiten oder Ausschreibungen die Zertifizierung als IT-Sicherheitsdienstleister für einen besonderen Geltungsbereich vorausgesetzt. Die Zertifizierung als IT-Sicherheitsdienstleister stellt aber auch auf dem freien Markt eine Empfehlung dar, mit der sich der Dienstleister gegenüber möglichen Wettbewerbern Vorteile verschaffen kann.

2 Anerkennungs- und Zertifizierungsprogramm für Stellen

Die Anerkennungsstelle des BSI betreibt ein Anerkennungs- und Zertifizierungsprogramm, in dem die Regeln (Geltungsbereiche, bedarfsgerechte Prüfkriterien, Anforderungen und Nachweise), das Verfahren sowie das Management zur Durchführung der Anerkennung bzw. Zertifizierung festgelegt und beschrieben sind.

Im Folgenden sind alle Geltungsbereiche mit den zugehörigen Dokumenten aufgeführt.

2.1 Geltungsbereiche für die Anerkennung von Prüfstellen

Folgende Anerkennungen können beim BSI beantragt werden:

1. Anerkennung als Prüfstelle im Bereich Common Criteria (CC), präzisiert im Anforderungsdokument [CC-Prüfstellen].
2. Anerkennung als Prüfstelle im Bereich „Smartcards and Similar Devices", präzisiert im Anforderungsdokument [CC-Prüfstellen].
3. Anerkennung als Prüfstelle im Bereich „Hardware Devices with Security Boxes", präzisiert im Anforderungsdokument [CC-Prüfstellen].
4. Anerkennung als Prüfstelle im Bereich Information Technology Security Evaluation Criteria (ITSEC)[2], präzisiert im Anforderungsdokument [CC-Prüfstellen].
5. Anerkennung als Prüfstelle im Bereich Technischer Richtlinien (TR), präzisiert im Anforderungsdokument [TR-Prüfstellen].

Die Verfahrensbeschreibung für den jeweiligen Geltungsbereich besteht aus der vorliegenden VB-Stellen und den präzisierenden Anforderungsdokumenten [CC-Prüfstellen] bzw. [TR-Prüfstellen].

Die Anerkennung der Prüfstelle in einem bestimmten Geltungsbereich setzt zudem ein Verständnis der entsprechenden Produktzertifizierung und somit die Kenntnis des Dokuments „Verfahrensbeschreibung zur Zertifizierung von Produkten" [VB-Produkte] mit den entsprechenden Anforderungsdokumenten [CC-Produkte] und [TR-Produkte] voraus. In diesen Dokumenten ist der Ablauf der Produktzertifizierung beim BSI für den Produkthersteller im Ganzen dargestellt. Aus diesem Grund wird das Produktzertifizierungsverfahren im vorliegenden Dokument VB-Stellen nicht noch einmal beschrieben.

2.2 Geltungsbereiche für die Zertifizierung von IT-Sicherheitsdienstleistern

Folgende Zertifizierungen können beim BSI beantragt werden:

1. Zertifizierung als IT-Sicherheitsdienstleister im Bereich IS-Revision, präzisiert im Anforderungsdokument [IS-Revision].
2. Zertifizierung als IT-Sicherheitsdienstleister im Bereich IS-Penetrationstests, präzisiert im Anforderungsdokument [IS-Penetrationstest].
3. Zertifizierung als IT-Sicherheitsdienstleister im Bereich Digitalfunk BOS, präzisiert im Anforderungsdokument [DigBOS].

2 Hierbei handelt es sich um einen auslaufenden Geltungsbereich. Eine Erstanerkennung in diesem Bereich ist nicht mehr möglich. Eine Reanerkennung ist nur im Zusammenhang mit bestimmten Projekten möglich.

4. Zertifizierung als IT-Sicherheitsdienstleister im Bereich Lauschabwehr,
   präzisiert im Anforderungsdokument [Lauschabwehr].
   Dieses Dokument ist beim BSI nur auf Nachfrage erhältlich.

Die Verfahrensbeschreibung für den jeweiligen Geltungsbereich besteht aus der vorliegenden VB-Stellen und den präzisierenden Anforderungsdokumenten [IS-Revision], [IS-Penetrationstest], [DigBOS], oder [Lauschabwehr].

3 Verfahren zur Anerkennung bzw. Zertifizierung

Eine Anerkennung als Prüfstelle bzw. Zertifizierung als IT-Sicherheitsdienstleister erfolgt, wenn festgestellt wird, dass die jeweiligen Anforderungen erfüllt sind und dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

Für die Ausübung der Tätigkeiten im jeweiligen Geltungsbereich müssen i. d. R. mindestens zwei fachlich kompetente Mitarbeiter seitens des Antragstellers benannt werden. Details hierzu sind in den jeweiligen Anforderungsdokumenten festgelegt. Das zur Kompetenzfeststellung bzw. zur Zertifizierung dieser Personen notwendige Verfahren ist in der „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“ [VB-Personen] beschrieben.

3.1 Beteiligte Stellen im BSI

3.1.1 Anerkennung von Prüfstellen

3.1.1.1 Die Anerkennungsstelle im BSI

Die Aufgabe der Anerkennungsstelle ist es festzustellen, ob eine Prüfstelle die entsprechenden Anforderungen erfüllt.

3.1.1.2 Die Produktzertifizierungsstellen im BSI

Die Fachkompetenz der Prüfstellen wird im Rahmen der Fachbegutachtungen bewertet.

Überdies ist es Aufgabe der jeweiligen Produktzertifizierungsstelle, während der Gültigkeit einer Anerkennung die Gleichwertigkeit aller Evaluierungsergebnisse und den vollständigen und korrekten Ablauf aller Produktzertifizierungsverfahren sicherzustellen. Um dies zu erreichen, führen die Produktzertifizierungsstellen in jedem Verfahren eine Prüfbegleitung im Hinblick auf eine einheitliche Vorgehensweise und Methodik durch.

Zur Überprüfung der formalen und fachlichen Voraussetzungen tauschen die Anerkennungsstelle und die Produktzertifizierungsstelle des BSI untereinander Informationen aus.

Werden bei einer Produktprüfung Mängel bekannt, erfolgt eine Information der Anerkennungsstelle zur möglichen Einleitung eines Mahn- und Aussetzungsverfahrens.

3.1.2 Zertifizierung von IT-Sicherheitsdienstleistern

3.1.2.1 Die Anerkennungsstelle im BSI

Aufgabe der Anerkennungsstelle ist es festzustellen, ob ein IT-Sicherheitsdienstleister die entsprechenden Anforderungen erfüllt. Zur Bewertung der Fachkompetenz des IT-Sicherheitsdienstleisters können Fachexperten hinzugezogen werden.

3.2 Phasen zur Anerkennung bzw. Zertifizierung

Die Anerkennung einer Prüfstelle bzw. Zertifizierung eines IT-Sicherheitsdienstleisters erfolgt in drei Phasen.

3.2.1 Vorbereitungsphase

Vor einer Antragstellung ist ein Informationsgespräch mit dem BSI möglich. Dieses Informationsgespräch findet statt, um dem Antragsteller einen Einblick in das Verfahren zu geben, die angestrebten Anerkennungs- bzw. Geltungsbereiche abzustimmen sowie u. a. die Themen Unabhängigkeit bzw. Unparteilichkeit der Stelle und anfallende Kosten zu besprechen.

Der Antragssteller stellt einen formalen Antrag auf Anerkennung bzw. Zertifizierung einer oder mehrerer Geltungsbereiche bei der Anerkennungsstelle des BSI.

Eine Vorlage für den Antrag wird auf der Webseite des BSI zur Verfügung gestellt. Die gestellten Anträge werden in der Reihenfolge des Eingangsdatums beim BSI bearbeitet. Hiervon kann abgewichen werden, wenn das BSI wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung einer Anerkennung oder einer Zertifizierung ein öffentliches Interesse besteht.

Der Antragsteller muss folgende Unterlagen dem Antrag zusätzlich als Nachweise beifügen:

- Firmendarstellung bei Erstanerkennung bzw. Erstzertifizierung,
- einen aktuellen Auszug aus dem Handels-, Genossenschafts-, Vereins- bzw. Partnerschaftsregister (nicht älter als 6 Monate). Neben den Eigentums- sind auch die Beteiligungsverhältnisse offenzulegen,
- Eigenversicherung, dass das Unternehmen sich nicht in Insolvenz oder in Liquidation befindet, gegen das Unternehmen kein Insolvenzverfahren eingeleitet ist oder das Unternehmen sich nicht in einer entsprechenden Lage befindet oder eine solche Lage einzutreten droht,
- Benennung der Mitarbeiter der Stelle (i.d.R. mindestens zwei pro Geltungsbereich) mit für den Geltungsbereich relevanter Projekt- und Arbeitshistorie sowie Kompetenzprofilen.
- Systemdokumentation Qualitätsmanagement:
  - Dokumentation eines Qualitätsmanagementsystems nach DIN EN ISO/IEC 17025 [17025] bezogen auf den beantragten Geltungsbereich,
  - dokumentierte Verfahren.
- Aufzeichnungen:
  - Aufzeichnungen zum letzten internen Systemaudit nach DIN EN ISO/IEC 17025 [17025] (entfällt, falls die Ersteinführung des Qualitätsmanagementsystems weniger als sechs Monate vor der Systembegutachtung erfolgte),
  - Aufzeichnungen zur letzten Managementbewertung (entfällt, falls die Ersteinführung des Qualitätsmanagementsystems weniger als sechs Monate vor der Systembegutachtung erfolgte),
  - Aufzeichnungen zum Personal über Verantwortungen und Befugnisse.
- Stellungnahme:
  - Eine schriftliche Stellungnahme zu allen Einzelaspekten der DIN EN ISO/IEC 17025im elektronischen Dokument „Begutachtungskatalog“ mit den Informationen darüber, durch welche Maßnahmen der Antragsteller die Einzelaspekte der Norm erfüllt und an welchen Stellen in der QM-Dokumentation die Maßnahmen dokumentiert sind. Der Begutachtungskatalog wird vom BSI zur Verfügung gestellt und ist der Anerkennungsstelle zur weiteren Bearbeitung in elektronischer, editierbarer Form zu übersenden.

Eine Auflistung weiterer zur Vorbereitung notwendiger Dokumentation zum Informationssicherheits-management sowie der Nachweise für die jeweiligen Geltungsbereiche befinden sich in den entsprechenden Anforderungsdokumenten.

Auf Grundlage der eingereichten Dokumente erfolgt eine erste Antragsprüfung, um festzustellen, ob die eingereichten Nachweise ausreichend für die Durchführung der Begutachtung sind. In dieser Dokumentenprüfung erfolgt somit ein Abgleich mit den für den Geltungsbereich relevanten Anforderungen. Bei Nichtkonformitäten hat der Antragsteller Gelegenheit, diese auszuräumen.

Nach Antragsannahme vereinbart der zuständige Begutachter mit dem Antragsteller Termine für die Systembegutachtung[3] . Der Antragsteller kann Einwände gegen die Bestellung der Begutachter erheben.

Alle Beteiligten am Verfahren sind verpflichtet, Abweichungen von der vereinbarten Zeitplanung den anderen Beteiligten mitzuteilen und erneut abzustimmen.

Nach einer Antragsprüfung mit negativem Ergebnis wird der Antrag vom BSI abgelehnt.

Auf Wunsch des Antragstellers kann eine kostenpflichtige Vorabbegehung durch das BSI durchgeführt werden, um Mängel im System der Stelle aufzudecken.

3.2.2 Begutachtungsphase

In der Begutachtungsphase wird durch Begutachter des BSI eine Systembegutachtung durchgeführt, die sich aus folgenden Teilen zusammensetzt:

- Begutachtung des Qualitätsmanagementsystems gemäß DIN EN ISO/IEC 17025 [17025],
- Begutachtung des Informationssicherheitsmanagementsystems nach dem nicht öffentlichem Dokument „Anforderung an die Sicherheit von Stellen“ [AS-Stellen] und
- ggf. einer Fachbegutachtung je Geltungsbereich.

Die Systembegutachtung wird durchgeführt, um zu überprüfen, ob die getroffenen Maßnahmen zur Erfüllung der Anforderungen umgesetzt und wirksam sind. Hierbei werden stichprobenartig auch Projekte und weitere Tätigkeiten des Antragstellers mit Bezug zu den jeweiligen Geltungsbereichen herangezogen.

Eine Systembegutachtung bei einem Geltungsbereich beläuft sich auf zwei Arbeitstage. Für jeden weiteren Geltungsbereich kann grundsätzlich bis zu einem weiteren Arbeitstag angesetzt werden.

Im Rahmen der Systembegutachtung wird grundsätzlich auch das Informationssicherheits-managementsystem (ISMS) des Antragstellers begutachtet. In bestimmten Geltungsbereichen kann stattdessen eine IS-Kurzrevision stattfinden. Details hierzu finden sich in den jeweiligen Anforderungs-dokumenten.

Fachbegutachtungen werden zur Kompetenzfeststellung der Prüfstelle entsprechend den jeweiligen Anforderungsdokumenten durchgeführt und sind insbesondere dann gefordert, wenn im jeweiligen Geltungsbereich keine Personenzertifizierung vorgesehen ist. Die Anforderungen und der Ablauf der Fachbegutachtung für den jeweiligen Geltungsbereich sind in den entsprechenden Anforderungs-dokumenten [CC-Prüfstellen], [TR-Prüfstellen], [IS-Revision], [IS-Penetrationstest], [DigBOS] und [Lauschabwehr] beschrieben.

Nach der Erhebungvon Begutachtungsnachweisen mittels Interviews mit den Mitarbeitern, Einsichtnahme in Aufzeichnungen und Dokumente des Antragstellers sowie weiterer Maßnahmen (z. B. Einsichtnahme in technische Systeme) werden die Begutachtungsfeststellungen (Abweichungen und Verbesserungspotenzial) getroffen. Diese und das daraus resultierende Begutachtungsergebnis werden dem Antragsteller in einem Abschlussgespräch mitgeteilt.

Falls Abweichungen festgestellt werden, muss im Abschlussgespräch ein gemeinsames Verständnis darüber entwickelt werden. Die Abstimmung und Terminierung von Korrekturmaßnahmen erfolgt im Abschluss-gespräch oder ggf. nach durchgeführter Ursachenanalyse.

3 Bei Reanerkennungen/Rezertifizierungen wurden in der Regel bereits vorab Termine im Rahmen einer Jahresplanung der Begutachtungen zwischen BSI und Antragssteller vereinbart.

Es gibt zwei Arten von Abweichungen:

Kritische Abweichungen:

- Abweichung von einer festgelegten Anforderung, die ein falsches Ergebnis der Arbeiten der Stelle verursacht bzw. verursachen kann
- Abweichung, die die grundlegende Wirksamkeit des QM-Systems in Frage stellt
- Wiederholtes Auftreten einer nicht kritischen Abweichung zur gleichen Anforderung

Bei kritischen Abweichungen ist die Durchführung einer Ursachenanalyse sowie die Umsetzung von geeigneten und wirksamen Korrekturmaßnahmen die Voraussetzung für die Erteilung einer Anerkennung/Zertifizierung. Bei Vorliegen einer nicht behobenen kritischen Abweichung kann keine positive Empfehlung zur Anerkennung bzw. Zertifizierung ausgesprochen werden.

Nicht kritische Abweichung:

- Abweichung von einer festgelegten Anforderung
- Es ist keine unmittelbare Auswirkung auf das Ergebnis der Arbeiten der Stelle zu erwarten
- Die grundlegende Wirksamkeit des QM-Systems wird nicht in Frage gestellt

Für festgestellte nicht kritische Abweichungen muss eine Ursachenanalyse durchgeführt werden auf deren Basis geeignete und wirksame Korrekturmaßnahmen entwickelt werden.Zur Behebung von nicht kritischen Abweichungen wird dem Antragssteller in der Regel eine Frist von max. 3 Monaten gewährt. Das Vorliegen einer nicht kritischen Abweichung steht einer positiven Empfehlung zur Erteilung der Anerkennung bzw. Zertifizierung nicht im Wege.

Das Begutachtungsergebnis wird mit einer Begutachtungsempfehlung in einem Begutachtungsbericht zusammengefasst.

3.2.3 Anerkennungs- bzw. Zertifizierungsphase

Auf Grundlage des Begutachtungsberichts sowie ggf. dem Ergebnis aus den Fachbegutachtungen bzw. der IS-Kurzrevision entscheidet das BSI gemäß den Regelungen § 9 Abs. 6 [BSIG] über die Anerkennung einer Stelle bzw. die Zertifizierung eines IT-Sicherheitsdienstleisters.

Vor Erteilung einer Anerkennung bzw. Zertifizierung wird dem Antragsteller der Begutachtungsbericht sowie ein Anhörungsschreiben inklusive der getroffenen Nebenbestimmungen zugesandt. Der Antragsteller hat die Gelegenheit, sich zu dem Erlass des Bescheids und dessen Nebenbestimmungen im Rahmen einer Anhörung zu äußern. Er kann auf eine Äußerung verzichten, um die weitere Bearbeitung zu beschleunigen.

Bei positiver Anerkennungs- bzw. Zertifizierungsentscheidung erstellt die Anerkennungsstelle nach erfolgter Anhörung die Urkundeund den Anerkennungs- bzw. Zertifizierungsbescheid.

Die Anerkennung bzw. Zertifizierung kann Nebenbestimmungen (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“) enthalten und ist zu befristen. Die Geltungsdauer für den jeweiligen technischen Geltungsbereich wird im Zertifikat festgesetzt. Regelmäßig beträgt dieser Zeitraum drei Jahre.

Eine negative Anerkennungs- bzw. Zertifizierungsentscheidung erfolgt, wenn keine Fachkompetenz für die beantragten Geltungsbereiche oder kein wirksames Managementsystem bezüglich Qualität (QMS) oder Informationssicherheit (ISMS) nachgewiesen werden konnte oder das Bundesministerium des Innern festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen. In diesem Fall werden dem Antragsteller vor

Ablehnung des Antrags die Gründe der voraussichtlichen Ablehnung mitgeteilt. Er hat innerhalb einer Frist Gelegenheit zur Äußerung und zur Nachbesserung.

Innerhalb eines Monats nach Bekanntgabe des Bescheides kann beim BSI, Godesberger Allee 185-189, 53175 Bonn, schriftlich oder zur Niederschrift Widerspruch erhoben werden. Der Antragsteller kann auf den Widerspruch verzichten, um eine schnellere Veröffentlichung der Anerkennung bzw. Zertifizierung zu ermöglichen.

4 Aufrechterhaltung der Anerkennung bzw. Zertifizierung

Während der Laufzeit der Anerkennung bzw. Zertifizierung wird regelmäßig und anlassbezogen überprüft, ob die Voraussetzungen für die Zertifizierung bzw. Anerkennung weiterhin vorliegen. Dazu werden in regelmäßigen Zeitabständen (11 und 22 Monate nach der Anerkennung bzw. Zertifizierung) eintägige Begutachtungen zur Systemförderung (siehe Kapitel 4.2 „Begutachtungen zur Systemförderung“) durchgeführt. Zudem können entsprechend dem Geltungsbereich Fachbegutachtungen (siehe Kapitel 4.3 „Fachbegutachtungen“) vorgenommen werden. Falls notwendig, können anlassbezogene Begutachtungen gemäß Kapitel 4.4 durchgeführt werden.

Des weiteren muss die anerkannte bzw. zertifizierte Stelle im Bescheid enthaltene Nebenbestimmungen einhalten und ihre (Prüf-)Tätigkeiten gemäß Kapitel 4.1 „Durchführung der (Prüf-)Tätigkeiten im betreffenden Geltungsbereich“ durchführen.

Werden während der Laufzeit oder im Rahmen von Überprüfungen Mängel bekannt, kann ein Mahnverfahren gemäß Kapitel 5.6.1 „Mahn- und Aussetzungsverfahren“ eingeleitet werden.

Fünf Monate vor Ablauf der Anerkennung bzw. Zertifizierung muss der Antragsteller einen erneuten Antrag auf Anerkennung bzw. Zertifizierung stellen, damit gewährleistet wird, dass die Anerkennung bzw. Zertifizierung lückenlos aufrechterhalten werden kann.

4.1 Durchführung der (Prüf-)Tätigkeiten im betreffenden Geltungsbereich

Die Anforderungen an die Durchführung der (Prüf-)Tätigkeiten der Stellen im betreffenden Geltungsbereich sind in den entsprechenden Anforderungsdokumenten (jeweils in Kapitel 4.1) beschrieben.

4.2 Begutachtungen zur Systemförderung

Ziel der Begutachtung zur Systemförderung ist es zu überprüfen, ob die Anforderungen dauerhaft eingehalten werden. Es muss der Nachweis erbracht werden, dass das Managementsystem wirksam aufrechterhalten und weiterentwickelt wird. Zur Begutachtung der Stelle können Projekte und Arbeiten mit Bezug zu den jeweiligen Geltungsbereichen herangezogen werden.

Die Stelle kann Begutachtungsthemen für diese Begutachtung vorschlagen.

Die Ergebnisse werden analog zu Kapitel 3.2.2 „Begutachtungsphase“ in einem Abschlussgespräch mitgeteilt und in einem Begutachtungsbericht zusammengefasst.

Sollten in einer Begutachtung zur Systemförderung kritische Abweichungen festgestellt werden, so ist für diese eine Ursachenanalyse durchzuführen. Geeignete und wirksame Sofortmaßnahmen müssen innerhalb von 4 Wochen ergriffen und nachgewiesen werden. Kann die kritische Abweichung innerhalb dieser Frist nicht behoben werden, wird ein Aussetzungsverfahren nach Kapitel 5.6.1 für die betroffenen Geltungsbereiche eingeleitet. In besonders schwerwiegenden Fällen kann dieses auch sofort ohne Einhaltung einer Frist eingeleitet werden.

4.3 Fachbegutachtungen

Fachbegutachtungen werden zur Kompetenzfeststellung der Prüfstelle und der Personen durchgeführt und sind insbesondere dann erforderlich, wenn im jeweiligen Geltungsbereich keine Personenzertifizierung vorgesehen ist.

Die Anforderungen und der Ablauf der Fachbegutachtung für den jeweiligen Geltungsbereich sind in den entsprechenden Anforderungsdokumenten [CC-Prüfstellen], [TR-Prüfstellen], [IS Revision], [IS-Penetrationstest], [DigBOS] und [Lauschabwehr] beschrieben.

4.4 Anlassbezogene Begutachtungen

Anlassbezogene Begutachtungen können stattfinden, insbesondere wenn

1. sich in der Stelle Änderungen (z. B. örtliche Verlagerung der Stelle oder Änderung der Unternehmenszugehörigkeit) ergeben, die Auswirkungen auf die Erfüllung der DIN EN ISO/IEC 17025 haben;
2. begründete Zweifel an der Einhaltung der DIN EN ISO/IEC 17025 oder an der Kompetenz der Stelle besteht;
3. wiederholt gegen die Verfahrensbeschreibungen oder Anforderungsdokumente verstoßen wird;
4. Verfahrensänderungen seitens des BSI u. a. aufgrund von Vorschriften, internationalen Vereinbarungen oder eines Kriterienwechsels notwendig werden;
5. von dritter Stelle Informationen über Unregelmäßigkeiten an die Anerkennungsstelle des BSI herangetragen werden.

5 Rahmenbedingungen

5.1 Grundlage für die Anerkennung bzw. Zertifizierung

Das Verfahren wird nach der „Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik“ [BSI-ZertV], dieser Verfahrensbeschreibung mit den zugehörigen Anforderungsdokumenten sowie dem Verwaltungsverfahrensgesetz (VwVfG) durchgeführt.

5.2 Genereller Dokumentenaustausch mit der Anerkennungsstelle

Die elektronische Kommunikation mit dem BSI erfolgt grundsätzlich über das Postfach postfach-anerkennung@bsi.bund.de und mit Chiasmus verschlüsselt. Der entsprechende Schlüssel ist beim BSI erhältlich.

5.3 Rahmenbedingungen zum Verfahren

5.3.1 Obliegenheiten des Antragstellers

Dem Antragsteller obliegt es:

- die notwendigen Nachweise zur Ermittlung des Sachverhalts beizubringen.
  Bei fehlenden oder unzureichenden Nachweisen kann ein Verfahren durch die Anerkennungsstelle mit negativem Ergebnis beendet werden.
- im Rahmen seiner Mitwirkungsobliegenheiten die notwendige Mitwirkung etwaiger Dritter sicherzustellen.
- dem Begutachterteam des BSI oder den vom Bundesamt beauftragten Personen in erforderlichem Umfang kostenfrei Zugang zu den Standorten, zu den zur Prüfung vorgesehenen Systemen sowie zu den notwendigen, vom BSI festgelegten Nachweisen zu gewähren.
- das BSI oder die vom BSI beauftragten Personen kostenfrei durch fachkompetente Mitarbeiter der Stelle zu unterstützen.
- aktiv an der Termingestaltung mitzuwirken und die Einhaltung der vereinbarten Termine sicherzustellen. Bei sich abzeichnenden Veränderungen muss die Anerkennungsstelle umgehend informiert werden, um eine aktualisierte Verfahrensplanung abzustimmen.

5.3.2 Rücknahme eines Antrags

Zu jedem Zeitpunkt im Verfahren kann der Antragsteller den Antrag auf Anerkennung bzw. Zertifizierung zurückziehen. In diesem Fall wird das Verfahren beendet.

Seitens des BSI werden die angefallenen Kosten und Auslagen erhoben.

5.3.3 Ablehnung eines Antrags

Das BSI kann bei nicht Vorliegen der im BSIG § 9 genannten Voraussetzungen sowie, wenn ein unvollständig eingereichter Antrag zur Anerkennung bzw. Zertifizierung nicht innerhalb von 3 Monaten vervollständigt wird, einen Antrag ablehnen.

5.4 Rahmenbedingungen zur Aufrechterhaltung der Anerkennung bzw. Zertifizierung

5.4.1 Bestimmungen zur Aufrechterhaltung

Zur Aufrechterhaltung der Anerkennung bzw. Zertifizierung muss die Stelle die Festlegungen der [VB-Stellen] sowie im Bescheid enthaltene Nebenbestimmungen einhalten.

Im Rahmen der Festlegungen der [VB-Stellen] wird insbesondere bestimmt, dass:

- die Stelle bei der Nutzung der Anerkennung bzw. Zertifizierung, insbesondere bei der Verwendung zu Werbezwecken, Vorlage und Nachweisführung, auf den Anerkennungs- bzw. Zertifizierungsbescheid und die Anerkennungsurkunde bzw. das Zertifikat hinweisen und diese Dokumente zur Verfügung stellen muss.
- die Stelle regelmäßig oder anlassbezogen Überprüfungen zur Aufrechterhaltung der Anerkennung bzw. Zertifizierung (siehe Kapitel 4) zulassen muss. Die Kosten sind von der Stelle zu tragen.
- die Stelle dem BSI unverzüglich schriftlich mitteilen muss, wenn sich ihre Arbeitsweise in Bezug auf die Einhaltung der Anforderungen, ihre Unternehmensform, ihre Eigentums- und Beteiligungsverhältnisse oder ihr Unternehmenssitz ändert.
- die Stelle dem BSI unverzüglich schriftlich mitteilen muss, wenn Umzüge oder bauliche Änderungen an den Räumlichkeiten der Stelle geplant sind:
  Sobald eine anerkannte oder zertifizierte Stelle plant, in neue Räumlichkeiten umzuziehen, muss das BSI über diese Absicht informiert werden. Vor Umzug der Stelle muss eine Eignungsprüfung der neuen Räumlichkeiten durch das BSI erfolgen. Zur Eignungsprüfung muss dem BSI die aktualisierte Dokumentation des Informationssicherheitsmanagementsystems (inkl. Netztopologie) sowie die aktualisierte Dokumentation der materiellen Sicherheit (inkl. Lageplan der Räumlichkeiten) zur Verfügung gestellt werden. Falls notwendig wird eine anlassbezogene Begutachtung der neuen Räumlichkeiten durch das BSI durchgeführt. Erst nach Freigabe durch das BSI darf die Stelle ihre Prüftätigkeiten an einem neuen Standort fortsetzen.
  Zieht eine Stelle ohne Freigabe der neuen Räumlichkeiten um, besteht keine Anerkennung bzw. Zertifizierung der Stelle in den neuen Räumlichkeiten. Es dürfen dann keine Arbeiten im Rahmen der Anerkennung als Prüfstelle oder der Zertifizierung als IT-Sicherheitsdienstleister in den neuen Räumlichkeiten durchgeführt werden. Unterlagen, Datenträger sowie Prüfgegenstände, die im Zusammenhang mit der Arbeit als Stelle beim BSI stehen, dürfen vor Freigabe ebenfalls nicht in den neuen Räumlichkeiten aufbewahrt werden.
- die Stelle eine bestimmte Zahl von Personen für den jeweiligen Geltungsbereich beschäftigen muss.
  Neues Personal, das im Geltungsbereich der Anerkennung bzw. Zertifizierung eingesetzt werden soll, ist der Anerkennungsstelle vor der Aufnahme von Tätigkeiten im entsprechenden Geltungsbereich zu melden.
- die Stelle an vom BSI angebotenen Arbeitstreffen zum Geltungsbereich teilnehmen muss.
  Das BSI stellt durch diese Treffen und Workshops eine kontinuierliche Zusammenarbeit mit den Stellen und ggf. den Produktzertifizierungsstellen sicher.

5.4.2 Regelungen zur Unterbeauftragung

Grundsätzlich muss eine Tätigkeit im Geltungsbereich vollständig und ausschließlich durch die Stelle erfolgen. Eine Unterbeauftragung kann keine in der unterbeauftragenden Prüfstelle nicht vorhandenen Kompetenzbereiche ausgleichen.

Bei Prüfstellen ist in begründeten Ausnahmen und bei Vorliegen der folgenden Voraussetzungen eine Unterbeauftragung möglich:

1. Die Verantwortung für alle Prüfergebnisse verbleibt bei der unterbeauftragenden Stelle. Diese muss somit das Prüfkonzept sowie die Testspezifikationen erstellen und die Ergebnisse der Tests auswerten.
2. Dem BSI muss eine Beschreibung vorliegen, welche Teile einer Prüfung oder Evaluierung unterbeauftragt werden sollen. Die Fachkompetenz der beteiligten Evaluatoren zu diesen Teilen muss dem BSI gegenüber nachgewiesen und deren Namen müssen dem BSI benannt werden.
3. Die unterbeauftragte Stelle muss eine vom BSI anerkannte Prüfstelle sein oder dem Lizenzierungsprozess des jeweiligen Schemas unterliegen und in den betreffenden Bereichen ihre Fachkompetenz nachgewiesen haben. Zur Durchführung der Evaluierungen und Prüfungen sind nur die fest angestellten, benannten, zertifizierten bzw. nachgewiesen kompetenten Personen der unterbeauftragten Stelle einzusetzen.
4. Der Hersteller bzw. Antragsteller muss einer Unterbeauftragung zustimmen.
5. Die Zustimmung des BSI muss in jedem Einzelfall vorliegen.

Eine Vergabe von Unteraufträgen von IT-Sicherheitsdienstleistern ist nicht zulässig.

Des Weiteren gelten die speziellen Anforderungen des jeweiligen Geltungsbereichs.

5.4.3 Regelungen zur Vertraulichkeit

Der Antragsteller gewährleistet die streng vertrauliche Behandlung der Interna von Verfahren und Projekten in den Geltungsbereichen. Er wird Beschäftigten und Dritten Informationen nur geben, soweit ihre Kenntnis notwendig ist („Kenntnis-nur-wenn-nötig-Prinzip“).

Die Stelle wahrt Verschwiegenheit über Betriebsgeheimnisse Dritter sowie über alle Informationen, die ihr im Zusammenhang mit dem Anerkennungs- bzw. Zertifizierungsverfahren und im Rahmen einer späteren Tätigkeit als anerkannte bzw. zertifizierten Stelle bekannt werden (Informationen, Daten, Gesprächsinhalte und sonstige Sachverhalte, etc.) und der hieraus gewonnenen vertraulichen Erkenntnisse. Eine Weitergabe an Dritte, Aufzeichnung oder sonstige Verwendung darf nur zur Durchführung des Verfahrens im betreffenden Geltungsbereich oder mit Zustimmung des BSI erfolgen. Gesetzliche Verpflichtungen bleiben unberührt.

Die Bearbeitung, Kenntnisnahme und Aufbewahrung jeglicher Unterlagen zur Bearbeitung, Zertifizierung, Prüfung und Evaluierung in Telearbeit, Heimarbeit und ähnlichen Formen ist nicht gestattet. Sie ist ausschließlich in den anerkannten bzw. zertifizierten Stellen oder bei dem jeweiligen Hersteller, Antragsteller bzw. der jeweiligen Behörde gestattet. Ausnahmen bedürfen der ausdrücklichen Zustimmung des BSI.

Die Nutzung der im Zusammenhang mit der Anerkennung bzw. Zertifizierung erworbenen Informationen ist auf den mit der Anerkennung bzw. Zertifizierung verfolgten Zweck beschränkt.

5.4.4 Vorkehrungen zum Schutz von Verschlusssachen

Wenn einer Stelle im Rahmen der Tätigkeiten im Geltungsbereich Verschlusssachen (VS) des Geheimhaltungsgrades „VS-NUR FÜR DEN DIENSTGEBRAUCH“ (VS-NfD) zur Kenntnis gelangen sollen, verpflichtet sich die Stelle zuvor die Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen [VSA] bzw. das Geheimschutzhandbuch [GHB] (siehe dortige Anlage 3), in der jeweils aktuellen Fassung, insbesondere das Merkblatt für die Behandlung von Verschlusssachen des Geheimhaltungsgrades „VS-NUR FÜR DEN DIENSTGEBRAUCH“, einzuhalten.

Eine Verpflichtung der Personen, denen Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NfD gewährt werden muss, wird durch die zuständige Behörde bzw. auf deren Veranlassung vorgenommen.

Als zentraler Ansprechpartner und Verantwortlicher für Angelegenheiten des Geheimschutzes muss die Stelle eine für den Schutz von VS-NfD verantwortliche Person (bei geheimschutzbetreuten Unternehmen ist dies der Sicherheitsbevollmächtigte) benennen. Im Besonderen ist dieser für die Sicherstellung des Schutzes von Verschlusssachen und die Umsetzung und Einhaltung der in der VSA und im GHB enthaltenen Vorschriften verantwortlich.

Wenn Verschlusssachen mit dem Geheimhaltungsgrad „VS-VERTRAULICH“ (VS-V) und höher ausgetauscht werden sollen, sind die entsprechenden Regelungen des Sicherheitsüberpüfungsgesetzes (SÜG), der Verschlusssachenanweisung und des Geheimschutzhandbuches umzusetzen und einzuhalten.

Neben den organisatorischen und materiellen Schutzmaßnahmen werden ab dem Geheimhaltungsgrad VS-V und höher auch Maßnahmen des personellen Geheimschutzes erforderlich.

Ggf. stellt die zuständige Behörde beim Bundesministerium für Wirtschaft und Energie (BMWi) einen Antrag auf Aufnahme der Stelle in die Geheimschutzbetreuung.

Sofern die Stelle für die Bearbeitung von Verschlusssachen IT einsetzt, hat sie ebenfalls die Vorschriften der VSA bzw. des GHB zu beachten.

Dem BSI ist auf Verlangen darzulegen, wie die Schutzmaßnahmen umgesetzt wurden. Dem BSI oder dessen Bevollmächtigten ist eine Überprüfung zu ermöglichen.

5.4.5 Regelungen zur Archivierung von Dokumenten und Aufzeichnungen

Der Antragsteller stellt sicher, dass alle Dokumente und Aufzeichnungen zu den Tätigkeiten im jeweiligen Geltungsbereich der Anerkennung bzw. Zertifizierung 3 Jahre nach Ablauf der Anerkennung bzw. Zertifizierung für Rückfragen des BSI vorgehalten werden.

Nach Auslaufen eines Geltungsbereichs wird die weitere Archivierung dieser Dokumente und Aufzeichnungen mit dem BSI vereinbart.

5.5 Erweiterung der Anerkennung bzw. Zertifizierung

Zur Erweiterung des Geltungsbereichs bei einer bestehenden Anerkennung bzw. Zertifizierung wird ein Antrag über den zu erweiternden Geltungsbereich gestellt.

Es wird grundsätzlich eine entsprechende Fachbegutachtung durchgeführt, um alle erforderlichen Anforderungen für den beantragten Geltungsbereich entsprechend dem Anforderungsdokument zu überprüfen.

Endet die Fachbegutachtung erfolgreich und wird dieAnerkennung bzw. Zertifizierung für den neu beantragten Geltungsbereich ausgesprochen, so wird auch die gültige Urkunde durch eine um den neuen Geltungsbereich ergänzte Urkunde ersetzt.

Die Laufzeit der Anerkennung bzw. Zertifizierung bleibt unverändert.

5.6 Aufhebung einer Anerkennung bzw. Zertifizierung

Zur Aufhebung einer Anerkennung bzw. Zertifizierung werden die Regelungen des Verwaltungsverfahrensgesetzes berücksichtigt. Ein Mahn- und Aussetzungsverfahren ist im folgenden Kapitel 5.6.1 definiert.

Ist eine Anerkennung bzw. Zertifizierung für einen oder alle Geltungsbereiche unanfechtbar aufgehoben (d.h. widerrufen oder zurückgenommen) oder ist die Gültigkeit der Anerkennung bzw. Zertifizierung aus einem anderen Grund nicht oder nicht mehr gegeben, so kann das BSI die auf Grund der Anerkennung bzw. Zertifizierung erteilten Urkunden bzw. Zertifikate, die zum Nachweis der Anerkennung bzw. Zertifizierung

im betreffenden Geltungsbereich bestimmt sind, zurückfordern. Der Antragsteller ist zu ihrer Herausgabe verpflichtet. Er kann jedoch verlangen, dass ihm die Urkunden bzw. Zertifikate wieder ausgehändigt werden, nachdem sie durch das BSI als ungültig gekennzeichnet wurden.

Die Stelle wird nicht mehr auf der öffentlichen Liste der anerkannten bzw. zertifizierte Stellen für die entsprechenden Geltungsbereiche gelistet und die Kontaktdaten der Stelle werden entfernt.

5.6.1 Mahn- und Aussetzungsverfahren

Stellt das BSI einen Verstoß der Stelle gegen die BSI-Zertifizierungs- und Anerkennungsverordnung [BSIZertV], die jeweils gültigen Verfahrensbeschreibungen oder den Anforderungsdokumenten fest oder weist die Stelle Kompetenzmängel auf, kann das BSI die Aussetzung oder die Aufhebung der Anerkennung bzw. Zertifizierung aussprechen.

Das BSI spricht der Stelle gegenüber eine schriftliche Mahnung aus. In der Mahnung wird der Grund der Mahnung mitgeteilt und eine angemessene Frist zur Beseitigung beziehungsweise zur Stellungnahme gesetzt.

Die Stelle erhält somit Gelegenheit, sich zum Grund für die Mahnung zu äußern sowie diesen ggf. zu korrigieren und Maßnahmen zur zukünftigen Vermeidung zu ergreifen. Durchgeführte Maßnahmen sind dem BSI schriftlich mitzuteilen und nachzuweisen. Ggf. erfolgt eine anlassbezogene Begutachtung.

Das BSI kann bis zur Entkräftung beziehungsweise Beseitigung des Mahnungsgrundes eine Aussetzung der Anerkennung/Zertifizierung aussprechen, wenn dies wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint. In diesem Fall ist der Stelle eine Verwendung der Anerkennungsurkunde/des Zertifikats und Werbung mit der Anerkennungsurkunde/dem Zertifikat untersagt. Neue Projekte dürfen während der Frist zur Beseitigung beziehungsweise Stellungnahme nicht begonnen und laufende nur mit ausdrücklicher Zustimmung des BSI fortgeführt werden.

Die Stelle muss die an laufenden Projekten beteiligten Kunden schriftlich über die Aussetzung benachrichtigen. Kopien dieser Schreiben müssen dem BSI spätestens zehn Kalendertage nach der Aussetzung vorliegen.

Die Aussetzung wird aufgehoben, wenn der Mahnungsgrund, der zur Aussetzung geführt hat, beseitigt wurde.

Können die Gründe, die zur Mahnung bzw. Aussetzung geführt haben, nicht fristgerecht entkräftet oder beseitigt werden, wird die Aufhebung der Anerkennung/Zertifizierung für den jeweiligen Geltungsbereich ausgesprochen.

Die Stelle muss die an laufenden Projekten beteiligten Kunden schriftlich über die Aufhebung benachrichtigen. Kopien dieser Schreiben müssen dem BSI spätestens zehn Kalendertage nach der Aufhebung vorliegen.

Das BSI kann auch eine sofortige Aufhebung der Anerkennung bzw. Zertifizierung der Stelle aussprechen, soweit dies erforderlich ist.

In den Geltungsbereichen, in denen eine Stelle verpflichtet ist, insbesondere die Anforderungen der Anlage 7 der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen [VSA] sowie darüber hinaus insbesondere die Anlage 4 des Geheimschutzhandbuchs [GHB] (siehe dortige Anlage 3) einzuhalten, ist das BSI berechtigt, die Anerkennung bzw. Zertifizierung ohne Einhaltung einer Frist zu widerrufen, wenn die Stelle gegen die in den Kapiteln 5.4.3„Regelungen zur Vertraulichkeit“und 5.4.4 „Vorkehrungen zum Schutz von Verschlusssachen“ genannten Verpflichtungen oder anderen Vorschriften der VSA bzw. des GHB verstößt und den Verstoß trotz einer schriftlichen Mahnung (s.o.) nicht unverzüglich abstellt.

Einer Mahnung bedarf es jedoch nicht, wenn der Verstoß gegen die Anforderungen des Geheimschutzhandbuches oder der Verschlusssachenanweisung so gravierend ist, dass eine weitere Zusammenarbeit mit der Stelle nicht mehr vertretbar ist.

5.6.2 Widerruf einer rechtmäßigen Anerkennung bzw. Zertifizierung

Ein Widerruf einer rechtmäßigen Anerkennung bzw. Zertifizierung kann aufgrund nachträglich eingetretener Tatsachen bzgl. der zugrundeliegenden Sach- und Rechtslage erfolgen (siehe hierzu §§ 48 und 49 [VwVfG]).

Gründe, die zu einem Widerruf einer Anerkennung bzw. Zertifizierung führen können, sind beispielsweise, wenn der Antragsteller:

- im Bescheid enthaltene Nebenbestimmungen nicht beachtet (siehe Kapitel 5.4.1 „Bestimmungen zur Aufrechterhaltung“.
- Änderungen dieser Verfahrensbeschreibung oder den jeweils gültigen Anforderungen widerspricht.
- gegen Anforderungen aus den jeweils gültigen Verfahrensbeschreibungen oder Anforderungsdokumenten verstößt.
  Dies kann beispielsweise der Fall sein, wenn sowohl beim Verfahren zur Anerkennung von Prüfstellen oder bei der Zertifizierung als IT-Sicherheitsdienstleister als auch bei einem konkreten Produktzertifizierungsverfahren es in der Zusammenarbeit zwischen dem BSI und der Stelle aufgrund von Nichteinhaltung von Anforderungen, Vorgaben und Terminen bzw. von mangelhaften Prüftätigkeiten einer Stelle zu erheblichen Problemen kommt.
- Vertraulichkeits- oder Sicherheitsvorschriften verletzt (siehe Kapitel 5.4.3„Regelungen zur Vertraulichkeit“und 5.4.4 „Vorkehrungen zum Schutz von Verschlusssachen“).
- Anerkennungsurkunden bzw. Zertifikate oder Anerkennungs- und Zertifizierungszeichen missbräuchlich verwendet.

5.6.3 Rücknahme einer rechtswidrigen Anerkennung bzw. Zertifizierung

Eine rechtswidrige Anerkennung bzw. Zertifizierung kann ganz oder teilweise zurückgenommen werden, beispielsweise, wenn:

- bewusst falsche Angaben zu den Anerkennungs- bzw. Zertifizierungsvoraussetzungen gemacht wurden.
- für die Anerkennungs- bzw. Zertifizierungsentscheidung bewusst wesentliche Informationen verschwiegen wurden.

5.7 Beschwerde- und Verbesserungsmanagement

Die Anerkennungsstelle verfügt über ein Verfahren, um Beschwerden und Verbesserungsvorschläge entgegenzunehmen, zu evaluieren, sowie Entscheidungen über diese zu treffen. Das Verfahren ist auf der Webseite des BSI veröffentlicht. Der Erhalt der Beschwerde wird bestätigt. Der Beschwerdeführer wird, sofern möglich, über das Ergebnis und den Abschluss des Verfahrens informiert.

Es wird in der Konformitätsbewertung ein Beschwerde- und Verbesserungsmanagement gelebt. Dabei fließt jegliche Anregung ein.

Auslöser für den Verbesserungsprozess sind unter anderem:

- Beschwerden und fehlerhafte Arbeitsergebnisse sowie
- Verbesserungsvorschläge und festgestellte Abweichungen.

5.8 Haftung

Für die wirtschaftliche Verwertbarkeit der Anerkennung bzw. Zertifizierung als Stelle im Sinne dieser Verfahrensbeschreibung wird keine Gewähr übernommen.

Die Qualität der Prüfungen, Evaluierungen oder Dienstleistungen der anerkannten bzw. zertifizierten Stellen verantwortet die jeweilige Stelle gegenüber ihren Auftragnehmern. Das BSI haftet ausschließlich nach den gesetzlichen Vorschriften.

5.9 Kosten

Für alle Tätigkeiten des BSI im Rahmen der Anerkennung oder Zertifizierung werden Kosten und Auslagen nach entstandenem Aufwand erhoben.

Die Kosten sind auch bei negativem Ergebnis des Verfahrens zu zahlen.

Ein Informationsgespräch mit dem BSI vor Antragstellung ist kostenfrei.

Im Falle einer Aussetzung oder Aufhebung der Anerkennung/Zertifizierung sind auch die hierfür entstandenen Kosten zu erstatten.

6 Veröffentlichung der Anerkennung bzw. Zertifizierung

Grundsätzlich wird nach Erteilung der Anerkennung bzw. Zertifizierung der Name der Stelle mit einer Kontaktperson und Kontaktdaten (Telefon, E-Mail) sowie die Geltungsbereiche mit dem Gültigkeitszeitraum veröffentlicht. Bei zertifizierten IT-Sicherheitsdienstleistern im Geltungsbereich „IS-Revision und IS-Beratung“ werden zudem die Namen der zertifizierten Personen veröffentlicht.

Der Veröffentlichung kann widersprochen werden.

Das BSI sieht von einer Veröffentlichung ab, soweit durch die Veröffentlichung die öffentliche Sicherheit beeinträchtigt werden könnte. Zudem kann das BSI von der Veröffentlichung ganz oder teilweise absehen, wenn durch die Veröffentlichung öffentliche oder private Interessen beeinträchtigt würden. Dies geschieht z. B. während eines laufenden Mahn- und Aussetzungsverfahrens für den entsprechenden Zeitraum.

6.1 Anerkennungs- bzw. Zertifizierungsnummer

Alle vom BSI anerkannten bzw. zertifizierten Stellen erhalten eine Anerkennungs- bzw. Zertifizierungsnummer in der Form „BSI-APS 9XXX“ (BSI-Vorgangskennung-fortlaufende Vorgangsnummer).

Sie dient als Bezug für die BSI-internen Vorgänge, den Schriftwechsel und die Kennzeichnung von Dokumenten (im Rahmen des Verfahrens).

6.2 Anerkennungs- bzw. Zertifizierungszeichen

Der Antragsteller hat die Möglichkeit, bei positivem Abschluss des Verfahrens ein Anerkennungs- bzw. Zertifizierungszeichen (als elektronische Druckvorlage) zu erhalten, das z. B. im Rahmen des Marketings verwendet werden kann.

Die Zeichenordnung des BSI enthält die Nutzungsbedingungen der Anerkennungs- und Zertifizierungszeichen.

6.3 Urkunden- bzw. Zertifikatsübergabe und Presseerklärung

Veröffentlicht der Antragsteller nach Abschluss des Verfahrens eine Presseerklärung, so bittet das BSI den Wortlaut zuvor mit der Anerkennungsstelle des BSI abzustimmen.

Das BSI bietet die Möglichkeit, auf bestimmten öffentlichen Veranstaltungen wie z. B. Kongressen und Messen, auf denen das BSI vertreten ist, die Urkunde bzw. das Zertifikat an einen Vertreter des Unternehmens auszuhändigen.

Nach Absprache kann ebenso eine Übergabe an einen Vertreter des Unternehmens in den Räumen des BSI organisiert werden.

7 Referenzen und Glossar

Die Aufschlüsselung der referenzierten Dokumente und das Glossar befindet sich im Dokument „Verzeichnisse“ [Verzeichnisse].