Bundesamt
für Sicherheit in der
Informationstechnik

Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Prüfschema für ISO 27001-Audits

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: http://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 Errichtungsgesetz des Bundesamts für Sicherheit in der Informationstechnik sowie entsprechende Erlasse des Bundesministeriums des Innern vom 06. Februar 2001 und vom 22. Dezember 2005 zum Zertifizierungsschema im Bereich IT-Grundschutz. Grundlage dieses Dokumentes sind die Normen DIN EN ISO 19011 "Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen", ISO/IEC 27006:2007 „Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems“ sowie DIN EN ISO/IEC 17021:2006 "Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren", welche Anleitungen und Anforderungen für den Ablauf und die Durchführung von Audits enthalten. Kriterienwerke des Verfahrens sind ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems – Requirements", der BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, BSI-Standard 100-3 „Ergänzende Risikoanalyse auf Basis von IT-Grundschutz“ sowie die IT-Grundschutz-Kataloge des BSI.

1. Einleitung

1.1 Versionshistorie

Datum	Version	Verfasser	Bemerkungen
01.01.2006	1.0	BSI	
01.02.2006	1.1	BSI	Änderungen in Kapitel 3.5
14.01.2008	2.0	BSI	Überarbeitung unter Berücksichtigung der ISO 27006, Version zur Kommentierung durch Auditoren
03.03.2008	2.1	BSI	Berücksichtigung der Kommentare der Auditoren

1.2 Zielsetzung

Das vorliegende Prüfschema für ISO 27001-Audits auf der Basis von IT-Grundschutz beschreibt die verbindliche Vorgehensweise, wie Auditoren die für die Erlangung eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz oder eines Auditortestates (Einstiegsstufe oder Aufbaustufe) erforderlichen Prüfungen durchführen müssen. Das Prüfschema dient gleichzeitig als Checkliste und Hilfsmittel für die Prüfung der IT-Grundschutz-Methodik. Zusätzlich zu den vorliegenden Vorgaben sind ergänzende Verfahrensanweisungen zu beachten und anzuwenden, die unter *http://www.bsi.bund.de/gshb/zert/ISO27001/schema.htm* veröffentlicht sind. In ergänzenden Verfahrensanweisungen werden unter anderem Grundsatzentscheidungen des BSI veröffentlicht.

1.3 Adressatenkreis

Dieses Dokument richtet sich vor allem an Auditteamleiter, die ein unabhängiges Audit durchführen, um die Konformität eines Managementsystems für Informationssicherheit gemäß ISO 27001 auf der Basis von IT-Grundschutz in einer Institution zu bestätigen. Auch IT-Sicherheitsverantwortliche können sich einen Überblick darüber verschaffen, welche Prüfanforderungen bei einem Audit gestellt werden und welche Referenzdokumente zur Verfügung gestellt werden müssen (siehe Kapitel 3.4 „Geforderte Referenzdokumente“).

1.4 Anwendungsweise

Im folgenden Dokument werden die Voraussetzungen und die Vorgehensweise für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz beschrieben. Nach allgemeinen Anforderungen an ein Audit in Kapitel 2 gibt Kapitel 3 einen Überblick über den Auditprozess. Anschließend werden die Phasen der Durchführung des Audits beschrieben.

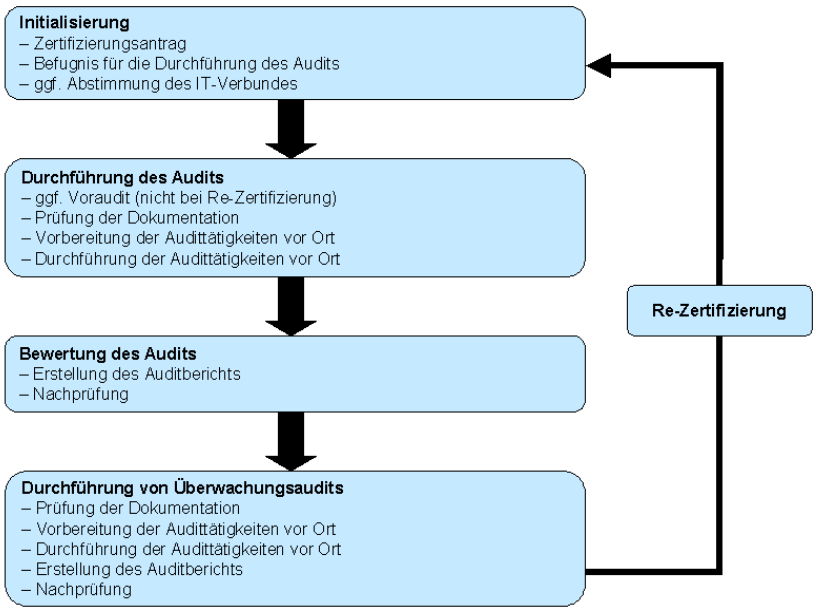

Abbildung 1: Auditprozess

Auf der Grundlage einer Dokumentenprüfung (Kapitel 4) bereitet sich der Auditor auf die Vor-Ort-Prüfung (Kapitel 5) vor, ehe er die konkrete Umsetzung der geforderten Anforderungen überprüft (Kapitel 6). Stellt der Auditor hier Defizite fest, muss die Institution Nachbesserungen durchführen (Kapitel 7). Es sind maximal 2 Nachbesserungen vorgesehen, bis der Auditor das Gesamtvotum (Kapitel 8) abgibt. Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz ist 3 Jahre gültig, nach denen die Institution eine Re-Zertifizierung (Kapitel 10) veranlassen muss, um die kontinuierliche Umsetzung der Anforderungen weiterhin nachweisen zu können. Während dieser 3 Jahre wird jährlich ein Überwachungsaudit (Kapitel 9) durchgeführt, das zeigen soll, dass das Informationssicherheits-managementsystem aktiv ist und weiterentwickelt wird.

Um dem Auditor zusätzliche Hilfsmittel bei der Anwendung des Prüfschemas zu geben und somit die Gleichwertigkeit des Verfahrens besser zu gewährleisten, werden in Kapitel 11 praktische Hilfen gegeben.

Für die Durchführung eines Auditortestates (Einstiegstufe bzw. Aufbaustufe) muss das Prüfschema ebenfalls angewendet werden. In Kapitel 12 wird explizit auf dieses Verfahren eingegangen. Um dieses Dokument übersichtlicher zu gestalten, wird an allen Stellen der Begriff Zertifikat verwendet, auch wenn sich das Verfahren auf beide Vorgehensweisen bezieht.

1.5 Begriffe und Definitionen

In diesem Dokument wird der Begriff IT-Verbund benutzt. Er stellt nicht nur den Verbund der betrachteten IT-Systeme dar, sondern umfasst auch das damit verbundene Informationssicherheits-Managementsystem. Der IT-Verbund ist der Geltungsbereich der Zertifizierung (Untersuchungsgegenstand).

Audits können von einem oder mehreren Auditoren durchgeführt werden, die vom Bundesamt für Sicherheit in der Informationstechnik lizenziert sind. Der für die Durchführung eines Audits verantwortliche Auditor wird in diesem Dokument Auditteamleiter genannt. Zu einem Auditteam können auch Fachexperten (Erfüllungsgehilfen) angehören, die entweder spezielle

Branchenkenntnisse oder solide Kenntnisse und Erfahrungen hinsichtlich der im IT-Verbund eingesetzten Informations- und Kommunikationstechnik besitzen.

1.6 Literaturverzeichnis

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

[GSHB] IT-Grundschutzkataloge - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[SHB] IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0 - März 1992, Bundesdruckerei

[ZERT] Informationen zum Zertifizierungsschema für ISO 27001 auf der Basis von IT-Grundschutz und zum Lizenzierungsschema für Auditoren für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz unter http://www.bsi.bund.de/gshb/zert

[17021] DIN EN ISO/IEC 17021:2006 "Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren"

[19011] DIN EN ISO 19011 „Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen“

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

[27002] ISO/IEC 27002:2005 "Information technology - Security techniques - Code of practice for information security management"

[27006] ISO/IEC 27006:2007 „Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems“

2. Auditprinzipien

Die Auditprinzipien fassen die grundlegenden Punkte des Auditprozesses zusammen. Ihre Einhaltung ist für den erfolgreichen Verlauf eines Zertifizierungsverfahrens erforderlich.

Die Auditierung stützt sich auf eine Reihe von Prinzipien. Diese machen das Audit zu einem wirksamen und zuverlässigen Werkzeug. Die Einhaltung der Auditprinzipien ist eine Voraussetzung für nachvollziehbare, wiederholbare und vergleichbare Auditergebnisse, um eine nachfolgende Zertifizierung zu ermöglichen.

Die folgenden Prinzipien müssen erfüllt werden:

- Ethisches Verhalten:
  Da im Umfeld Informationssicherheit oft sensible Geschäftsprozesse und Daten zu finden sind, sind die Vertraulichkeit der Informationen und der diskrete Umgang mit den Ergebnissen des Audits eine wichtige Arbeitsgrundlage. Sowohl das BSI als auch die auditierte Organisation müssen dem Auditor und seinem Vorgehen vertrauen können.
- Sachliche Darstellung:
  Ein Auditor hat die Pflicht, sowohl seinem Auftraggeber als auch der Zertifizierungsstelle wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehört die wahrheitsgemäße und nachvollziehbare Darstellung des Sachverhalts in den Auditfeststellungen, Auditschlussfolgerungen und dem Auditbericht. Die Prüfungsergebnisse des Audits müssen (bei unverändertem Sachstand) wiederholbar sein.
- Angemessene Sorgfalt:
  Ein Auditor muss bei der Durchführung des Audits mit Sorgfalt vorgehen. Sein Urteilsvermögen ist unerlässliche Voraussetzung für sachgerechte und fundierte Audits. Hierzu gehört auch der jeweils aktuelle Kenntnisstand der Informations- und IT-Sicherheit beim Auditor.
- Unabhängigkeit und Objektivität:
  Jeder Auditor des Auditteams muss dem BSI gegenüber eine Unabhängigkeitserklärung mit Begründung abgeben. Wenn der Auditor oder die Firma, für die er tätig ist, in einer Beziehung zu der zu auditierenden Institution oder Teilen davon stehen, die einen Interessenskonflikt hervorrufen, ist anzunehmen, dass diese Unabhängigkeit nicht gegeben ist.
- Nachvollziehbarkeit:
  Alle Auditschlussfolgerungen müssen objektiv nachvollzogen werden können. Hierzu gehört eine dokumentierte und nachvollziehbare Methodik, mit der der Auditor zu seinen Schlussfolgerungen kommt.
- Nachweise:
  Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Auditschlussfolgerungen in einem systematischen Auditprozess zu kommen, ist die eindeutige und folgerichtige Dokumentation der Ergebnisse. Die Auditnachweise müssen verifizierbar sein. Hierbei können die Ergebnisse auf Stichproben der verfügbaren Informationen beruhen, da ein Audit während eines begrenzten Zeitraumes und mit begrenzten Ressourcen vorgenommen wird. Die Auswahl der Stichproben muss für den IT-Verbund und seine Sicherheitsstruktur relevant und in einem sinnvollen Umfang vorgenommen werden.

3. Ablauf des Auditprozesses

3.1 Überblick über den Auditprozess

Nachdem eine Institution ein Informationssicherheits-Managementsystem nach ISO 27001 auf der Basis der IT-Grundschutz-Methodik umgesetzt hat und alle relevanten Dokumente vorliegen, kann sie einen Auditor beauftragen, auf Grundlage des vorliegenden Prüfschemas den IT-Verbund und seine Sicherheitsstruktur unabhängig zu überprüfen. Der Auditor 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.

3.2 Zielsetzung und Umfang des Audits

Ziel des Audits ist die unabhängige Überprüfung der Umsetzung der ISO 27001-Vorgaben mit Hilfe der IT-Grundschutz-Methodik in einem fest definierten IT-Verbund einer Organisation. Aus diesem Grund muss der Auditor sowohl auf die ISO 27001 als auch auf die BSI-Standards zu IT-Grundschutz und die IT-Grundschutz-Kataloge Zugriff haben. Die Prüfung wird durch einen oder mehrere Auditoren durchgeführt, die hierzu eine gültige BSI-Lizenz besitzen.

Jedes Audit im Sinne dieses Dokumentes umfasst zwei Phasen: Eine Dokumentenprüfung und eine Umsetzungsprüfung vor Ort. Die Ergebnisse des Audits werden von der Zertifizierungsstelle des BSI analysiert und bewertet. Bei im Rahmen eines geregelten Zertifizierungsaudits nachgewiesener Eignung der Organisation erteilt die Zertifizierungsstelle des BSI ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz, das grundsätzlich drei Jahre gültig ist, sich aber jährlich im Rahmen eines Überwachungsaudits bewähren muss. Nach drei Jahren kann das Zertifikat nach einem Re-Zertifizierungsaudit um weitere 3 Jahre verlängert werden.

3.3 Rollen und Zuständigkeiten im Auditprozess

Im Auditprozess gibt es drei unterschiedliche Rollen:

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

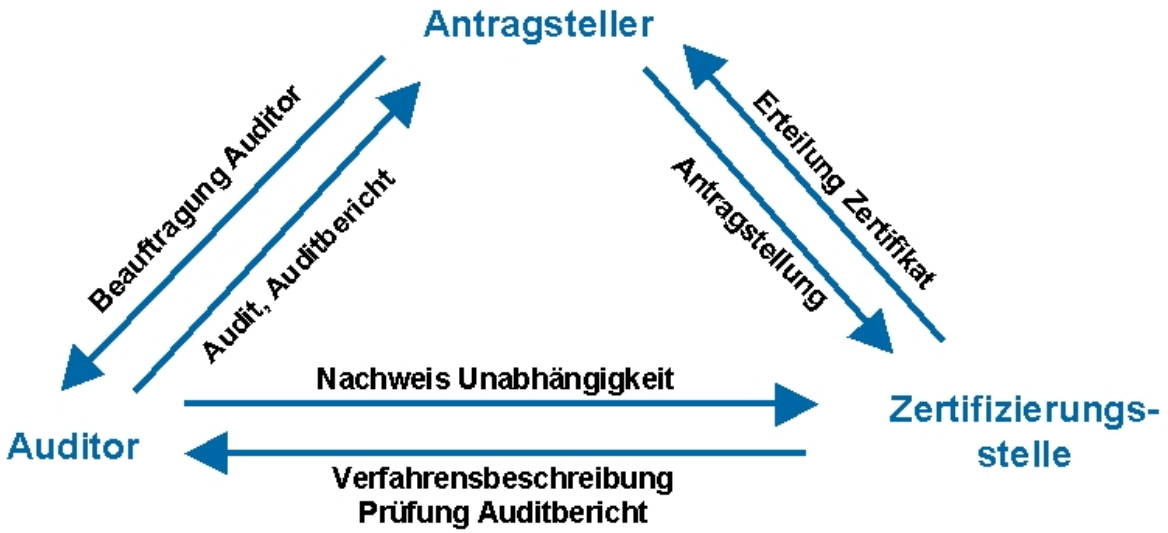

Abbildung 2: Rollen im Auditprozess

Der **Antragsteller** setzt die IT-Grundschutz-Methodik um und stellt die erforderlichen Dokumente und Nachweise der Umsetzung zur Verfügung und unterstützt die Auditoren bei der Vor-Ort-Prüfung des IT-Verbundes. Er ist Initiator des Auditprozesses. Er beauftragt einen Auditteamleiter und stellt den Zertifizierungsantrag beim BSI.

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 (Erfüllungsgehilfen) hinzuziehen.

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

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 den Auditprozess verbleibt in jedem Fall beim Auditteamleiter.

Die **Zertifizierungsstelle** des BSI ist eine unabhängige dritte Instanz, die die Gleichwertigkeit der Prüfungen und der Auditberichte gewährleistet. Sie veröffentlicht die Schemata und Interpretationen.

3.4 Geforderte Referenzdokumente

Die folgenden Referenzdokumente bilden die Grundlage für die Auditierung und müssen vom Antragsteller dem Auditor und der Zertifizierungsstelle als Arbeitsgrundlage zur Verfügung gestellt werden:

- IT-Sicherheitsrichtlinien (A.0)
- IT-Strukturanalyse (A.1)
- Schutzbedarfsfeststellung (A.2)

- Modellierung des IT-Verbunds (A.3)
- Ergebnis des Basis-Sicherheitschecks (A.4)
- Ergänzende Sicherheitsanalyse (A.5)
- Risikoanalyse (A.6)

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

Falls die Auditierung im Rahmen einer Re-Zertifizierung erfolgt, muss für jedes Referenzdokument kurz herausgestellt werden, welche Veränderungen sich gegenüber der vorhergehenden Zertifizierung ergeben haben.

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

Soweit der Antragsteller und der Auditor der Ansicht sind, dass Maßnahmen zur Gewährleistung der Vertraulichkeit bei der Übergabe der Dokumentation erforderlich sind, sollten geeignete Schritte ergriffen werden. Der Auditor ist durch vertragliche Vereinbarungen mit dem BSI verpflichtet, Details zum Audit- und Zertifizierungsverfahren, im Rahmen des Audits gewonnenen Informationen streng vertraulich zu behandeln sowie Beschäftigten 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.

A.0 IT-Sicherheitsrichtlinien

Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Organisation und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Informationssicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zu Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können. Aus diesem Grund müssen mindestens folgende Richtlinien dokumentiert sein:

- IT-Sicherheitsleitlinie
- Richtlinie zur Risikoanalyse
- Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
- Richtlinie zur internen ISMS-Auditierung (Auditierung des Managementsystems für Informationssicherheit)
- Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen

Der Auditor kann sonstige Richtlinien und Konzepte stichprobenartig prüfen. Dies können beispielsweise dokumentierte Verfahren der Schicht 1 sein, die die Organisation zur Sicherstellung der wirksamen Planung, Durchführung und Kontrolle ihrer Informationssicherheitsprozesse benötigt.

A.1 IT-Strukturanalyse

In diesem Dokument wird der zu untersuchende IT-Verbund dargestellt. Nähere Informationen zur IT-Strukturanalyse finden sich in Kapitel 4.1 der IT-Grundschutz-Methodik. Im Einzelnen müssen folgende Informationen vorliegen:

- Definition des Untersuchungsgegenstands
  Zertifizierbar sind eine oder mehrere Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten. Der Untersuchungsgegenstand muss eine geeignete Mindestgröße besitzen.

- Integration des Untersuchungsgegenstands in das Gesamtunternehmen
  In einem kurzen Firmen-/Behördenprofil (ca. 10 Zeilen) müssen u. a. die wesentlichen Tätigkeitsfelder der Institution und die Größe des IT-Verbunds deutlich werden. Die Bedeutung des Untersuchungsgegenstands für die Institution als Ganzes ist darzustellen.
- Bereinigter Netzplan
  Der bereinigte Netzplan stellt die Komponenten im IT-Verbund und deren Vernetzung dar. Dabei sind gleichartige Komponenten zu Gruppen zusammengefasst.
- Liste der IT-Systeme
  In dieser Liste sind alle im IT-Verbund vorhandenen IT-Systeme (Server, Clients, TK-Anlagen, aktive Netzkomponenten, etc.) aufgeführt.
- Liste der IT-Anwendungen
  In dieser Liste sind die wichtigsten im IT-Verbund eingesetzten Anwendungen aufgeführt. Eine IT-Anwendung kann dabei ein bestimmtes Software-Produkt (beispielsweise ein Programm zur Ressourcenplanung), eine sinnvoll abgegrenzte Einzelaufgabe (beispielsweise Bürokommunikation) oder ein Geschäftsprozess (z. B. Abrechnung von Reisekosten) sein. Eine Zuordnung der Anwendungen zu den IT-Systemen ist zu erstellen. Häufig ist es auch sinnvoll, die Abhängigkeiten der Anwendungen untereinander zu verdeutlichen, um den Schutzbedarf später besser festlegen zu können.
- Liste der Kommunikationsverbindungen
  In dieser Liste sind einerseits alle im IT-Verbund vorhandenen und andererseits alle über die Grenzen des IT-Verbunds gehenden Kommunikationsverbindungen aufgeführt.
- Liste der Räume
  In dieser Liste sind alle Räume im IT-Verbund mit Funktion aufgeführt. Es kann sinnvoll sein, hier einen Raumplan ergänzend beizufügen.

A.2 Schutzbedarfsfeststellung

Dieses Dokument beschreibt die Ergebnisse der Schutzbedarfsfeststellung, wie sie in Kapitel 4.2 der IT-Grundschutz-Methodik beschrieben ist. Im Einzelnen müssen folgende Informationen enthalten sein:

- Definition der Schutzbedarfskategorien
  Die Definition der drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ geschieht anhand von möglichen Schäden (z. B. finanzielle Schäden oder Verstöße gegen Gesetze), die bei Beeinträchtigung von IT-Anwendungen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit auftreten können.
- Schutzbedarf der IT-Anwendungen
  Ausgehend von den Geschäftsprozessen ist für jede in der Liste der IT-Anwendungen aufgeführte Anwendung der Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu dokumentieren und zu begründen.
- Schutzbedarf der IT-Systeme
  Der Schutzbedarf eines IT-Systems leitet sich aus dem Schutzbedarf der IT-Anwendungen ab, die auf dem IT-System ablaufen oder deren Daten das IT-System transportiert oder verarbeitet. Für jedes in der Liste der IT-Systeme aufgeführte IT-System ist der Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu dokumentieren und zu begründen.
- Schutzbedarf der Kommunikationsverbindungen
  Im Gegensatz zu IT-Anwendungen und IT-Systemen wird bei den Kommunikationsverbindungen lediglich zwischen kritischen und nichtkritischen Verbindungen unterschieden. Kritisch ist eine Verbindung, wenn sie eine Außenverbindung darstellt, wenn sie hochschutzbedürftige Daten transportiert oder wenn über diese Verbindung bestimmte hochschutzbedürftige Daten nicht transportiert werden dürfen. Vorzulegen ist entweder eine Liste der kritischen Verbindungen oder ein Netzplan, in dem die kritischen Verbindungen graphisch hervorgehoben sind.

- Schutzbedarf der Räume
  Der Schutzbedarf leitet sich von den dort betriebenen IT-Systemen, aufbewahrten Datenträgern und Dokumenten ab. Der Schutzbedarf der Räume, in denen IT-Systeme betrieben oder die anderweitig für den IT-Betrieb genutzt werden, ist zu dokumentieren.

A.3 Modellierung des IT-Verbunds

Die Modellierung des IT-Verbundes legt fest, welche Bausteine der IT-Grundschutz-Kataloge auf welche Zielobjekte im betrachteten IT-Verbund angewandt werden. Diese Zuordnung erfolgt individuell für den betrachteten IT-Verbund in Form einer Tabelle. Als Richtlinie hierzu findet sich in den IT-Grundschutz-Katalogen ein Modellierungshinweis. In diesem wird für jeden Baustein beschrieben, auf welche Arten er auf verschiedenen Zielobjekten anzuwenden ist.

A.4 Ergebnis des Basis-Sicherheitschecks

Für jede Maßnahme, die in den für die Modellierung herangezogenen Bausteinen enthalten ist, ist der Umsetzungsstatus („entbehrlich“, „ja“, „teilweise“ oder „nein“) vermerkt. Für jede Maßnahme mit Umsetzungsstatus „entbehrlich" muss außerdem eine Begründung aufgeführt sein. Erläuterungen zum Basis-Sicherheitsscheck stehen in Kapitel 4.4 der IT-Grundschutz-Methodik zur Verfügung.

A.5 Ergänzende Sicherheitsanalyse

Für alle Zielobjekte des IT-Verbundes, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen der IT-Grundschutz-Kataloge nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind,

ist zu entscheiden, ob weitere Risikobetrachtungen erforderlich sind. Dieser Entscheidungsprozess auf Managementebene wird als ergänzende Sicherheitsanalyse bezeichnet. Die Ergebnisse der ergänzenden Sicherheitsanalyse sind begründet und nachvollziehbar in Form eines Managementberichtes über die ergänzende Sicherheitsanalyse vorzulegen.

A.6 Ergänzende Risikoanalyse

Im Rahmen der ergänzenden Sicherheitsanalyse ist eine Entscheidung getroffen worden, für welche Zielobjekte eine ergänzende Risikoanalyse durchgeführt werden muss. Die Dokumentation einer Risikoanalyse und deren Ergebnisse sind als Referenzdokument A.6 vorzulegen.

Die ergänzende Risikoanalyse ist entsprechend der selbst definierten Richtlinie zur Risikoanalyse durchzuführen und zu dokumentieren. Modelle zur Durchführung von Risikoanalysen sind beispielsweise im BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“ sowie in der ISO/IEC 27005 enthalten

3.5 Zertifizierungsantrag beim BSI

Vor Beginn des Audits müssen folgende Voraussetzungen erfüllt sein:

- Dem BSI muss der vollständige Zertifizierungsantrag mindestens 2 Monate vor Beginn des Audits (Sichtung der Referenzdokumente) vorliegen. Der Zertifizierungsantrag enthält Angaben zum Antragsteller und verschiedene Daten zum Untersuchungsgegenstand sowie der Auditierungstätigkeit. Dabei müssen u.a. die untenstehenden Angaben vollständig sein:
  - Eine Beschreibung des Untersuchungsgegenstandes. Dazu ist ein kurzes Behörden- bzw. Firmenprofil vorzulegen, aus dem u.a. die wesentlichen Tätigkeitsfelder der Institution sowie

die Größe und Bedeutung des Untersuchungsgegenstandes für die Institution deutlich werden. Der zu zertifizierende Untersuchungsgegenstand ist zu beschreiben sowie ein bereinigter Netzplan vorzulegen. Die Zertifizierungskennung wird erst vergeben, wenn die prinzipielle Zertifizierbarkeit, also die sinnvolle Abgrenzung des IT-Verbunds, vom BSI geprüft wurde. Abstimmungen oder Rückfragen dazu können durch telefonischen Kontakt oder, falls notwendig, durch eine Besprechung geschehen.
Um zu vermeiden, dass ein Antrag für einen nicht sinnvoll abgegrenzten IT-Verbund gestellt wird, besteht die Möglichkeit, die Dokumente schon vor dem eigentlichen Antrag beim BSI zur Abstimmung einzureichen und die prinzipielle Zertifizierbarkeit des IT-Verbundes zu klären.

- Bei einer Re-Zertifizierung sind die Änderungen im IT-Verbund im Vergleich zum IT-Verbund der Erst-Zertifizierung anzugeben und kurz zu beschreiben.
  Bei der Verwendung überarbeiteter oder neuer Bausteine sind diese im Antrag mit anzugeben und zu beschreiben. Gegebenenfalls ist auch hier eine Absprache mit dem BSI notwendig.
- Im Zertifizierungsantrag sind Angaben zum Zeitplan des Audits (Erst- bzw. Re-Zertifizierungsaudit) sowie der Abgabe des Auditberichtes an das BSI zu machen. Terminänderungen sind dem BSI per E-Mail an zertifizierung@bsi.bund.de rechtzeitig mitzuteilen. Hinweis: Die Planung der Überwachungsaudits (Zeitplan, Auditteamleiter, usw.) ist Bestandteil des im Rahmen des Zertifizierungsverfahrens entstehenden Auditberichtes.

- Jeder Auditor des Auditteams muss dem BSI gegenüber die Unabhängigkeitserklärung mit Begründung abgeben. Wenn der Auditor oder die Firma, für die er tätig ist, in einer Beziehung zu der zu auditierenden Institution oder Teilen davon stehen, die einen Interessenskonflikt hervorrufen können, ist diese Unabhängigkeit in der Regel nicht mehr gegeben. Eine solche Gefährdung kann z.B. bei folgenden Konstellationen auftreten:
  - vorhergehende Beratung der Institution durch den Auditor selbst oder einen Kollegen / Vorgesetzten des Auditors
  - andere geschäftliche Verbindungen des Arbeitgebers des Auditors und der auditierten Institution
  - Verwandtschaftsverhältnis des Auditors mit Mitgliedern / verantwortlichen Personen der auditierten Institution oder eines Beraters

  Diese Unabhängigkeitserklärung muss dem BSI ebenfalls mindestens 2 Monate vor Beginn der Auditierungstätigkeit vorliegen. Die Unabhängigkeitserklärung sollte vom Antragsteller mit dem Zertifizierungsantrag eingereicht werden. Wenn der Nachweis nicht oder nicht rechtzeitig vorliegt oder ungenügend ist, kann das BSI den Auditor ablehnen.
- Das BSI behält sich vor, zusätzliche Informationen zum Beschäftigungsverhältnis zwischen Auditor und Antragsteller anzufordern. Sieht das BSI die Unabhängigkeit des Auditors nicht gewährleistet, widerspricht es der Durchführung des Audits durch diesen Auditor.

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

3.6 Durchführung von Audits

3.6.1 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:

- Erstzertifizierungsaudit: Im Rahmen eines Erstzertifizierungsaudits wird erstmalig der betreffende IT-Verbund der Institution unter ISO 27001- und IT-Grundschutz-Aspekten auditiert.

- Überwachungsaudit: In die dreijährige Laufzeit eines Zertifikates integriert sind jährliche Überwachungsaudits der zertifizierten Institution, die auf die Kontrolle der für das Zertifikat nachgewiesenen IT-Sicherheit im IT-Verbund zielen. Das Audit dient dem Nachweis, dass der zertifizierte IT-Verbund weiterhin den Sicherheitsansprüchen bzgl. ISO 27001 und IT-Grundschutz genügt.
- Re-Zertifizierungsaudit: Nach Ablauf der Zertifikatslaufzeit von drei Jahren wird eine Re-Zertifizierung des IT-Verbundes fällig. Diese umfasst insbesondere ein Re-Zertifizierungsaudit des IT-Verbundes, das zum großen Teil identisch zum Erstzertifizierungsaudit abläuft.

Erstzertifizierungsaudit, Überwachungsaudit und Re-Zertifizierungsaudit unterscheiden sich hinsichtlich ihrer Zielsetzung und ihres Umfangs voneinander. Bei jedem Audittyp findet eine Initialisierung (z.B. Antragstellung, Klärung von Zuständigkeiten und Befugnissen, Abstimmungen) und eine Bewertung (Schreiben des Auditberichts durch den Auditor, Sicherstellen der Vergleichbarkeit von Zertifizierungsverfahren durch die Zertifizierungsstelle) statt.

Führt der Auditor ein Audit zur Ausstellung eines Auditortestats durch, entspricht das Verfahren des Audits dem eines Erstzertifizierungsaudits bzw. eines Re-Zertifizierungsaudits.

Ein Voraudit ist im Rahmen der ersten in Anspruch genommenen Stufe des Auditortestats bzw. im Rahmen des Erstzertifizierungsaudits zulässig. Im Rahmen eines Re-Zertifizierungsaudits ist ein Voraudit nur bei einer wesentlicher Erweiterung/Veränderung des Geltungsbereichs zulässig.

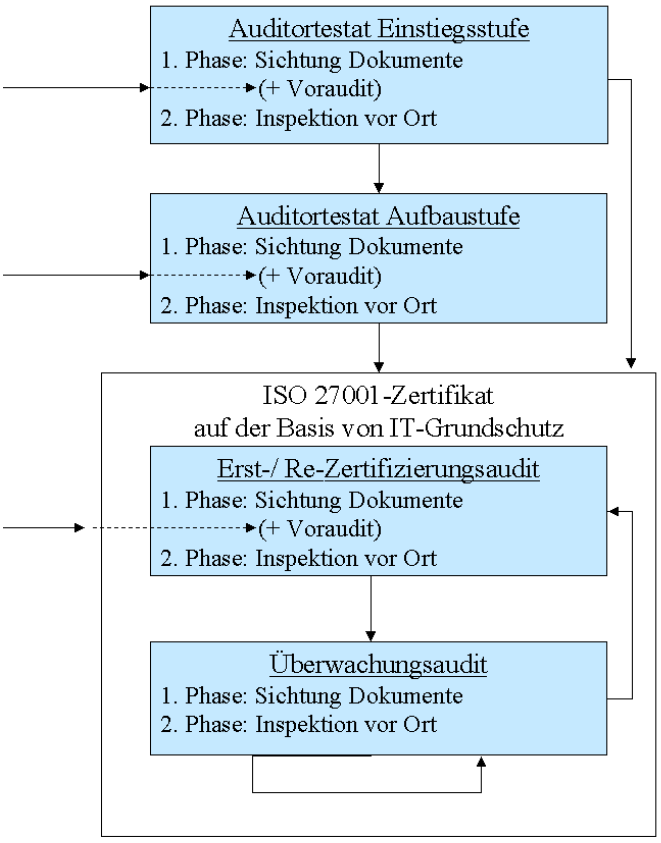

Abbildung 3: Audittypen

3.6.2 Auditphasen

Jedes Audit setzt sich grundsätzlich aus zwei getrennten, aufeinander aufbauenden Phasen zusammen. 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. In Phase 2 schließt sich eine Vor-Ort-Prüfung des IT-Verbundes durch den Auditor an, in der im realen IT-Verbund die praktische Umsetzung der in den Referenzdokumenten dokumentierten Sicherheitsmaßnahmen bzgl. ISO 27001 und IT-Grundschutz auf ihre Vollständigkeit, Korrektheit und Wirksamkeit hin überprüft wird (Umsetzungsprüfung).

3.6.2.1 Erstzertifizierungsaudit

Die erste Auditphase des Erstzertifizierungsaudits dient dazu, dass der Auditor ein ausreichendes Verständnis für den IT-Verbund erlangt und feststellt, ob die Konzeption der IT-Sicherheitsstruktur des IT-Verbundes bzgl. ISO 27001 und IT-Grundschutz schlüssig und sinnvoll und der Grad der Umsetzung der IT-Grundschutz-Anforderungen für eine Fortsetzung des Audits ausreichend ist.

Damit der Auditor ein ausreichendes Verständnis vom IT-Verbund gewinnen kann, ist es sinnvoll, einen Teil der Phase 1 bei der zu auditierenden Institution durchzuführen.

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

Das Voraudit darf nicht mehr als ein Drittel der für das nachfolgende konkrete Audit angesetzten Zeit in Anspruch nehmen. Kommt der Auditor nach dem Voraudit zu der Empfehlung, das Audit mindestens um eine von ihm festgesetzte Zeit aufzuschieben, so teilt er diese dem Antragsteller mit. Folgt ihm dieser in seiner Entscheidung, wird der Rest des Audits später an diesem Punkt weitergeführt. Ein erneutes Voraudit ist nicht möglich. Das BSI wird von dieser Entscheidung informiert. Ein Voraudit ist nur im Rahmen eines Zertifizierungsverfahrens möglich.

In Phase 1 des Audits werden die vom Antragsteller vorgelegten Referenzdokumente gesichtet und anhand der Prüfkriterien (siehe Kapitel 4) verifiziert. Die Prüfergebnisse werden im Auditbericht dokumentiert. Stellt der Auditor bei der Dokumentenprüfung Abweichungen (z.B. in der Dokumentation oder in der Sicherheitskonzeption des IT-Verbundes) fest, teilt er diese dem Antragsteller zusammen mit einer angemessenen Frist zur Behebung mit.

Nach Abschluss der Phase 1 des Audits entscheidet der Auditor auf Grundlage der Ergebnisse aus dieser Auditphase, ob eine Fortsetzung des Audits mit Phase 2 sinnvoll ist. Der Auditor prüft auch, ob im Auditteam die Fachkenntnisse und Kompetenzen vorhanden sind, um mit der 2. Phase des Audits fortzufahren und erweitert gegebenenfalls das Auditteam. Zusätzliche Auditoren und Erfüllungsgehilfen müssen der Zertifizierungsstelle des BSI gemeldet werden und ebenfalls eine Unabhängigkeitserklärung einreichen.

Bei Fortführung des Audits bereitet der Auditor auf Grundlage der Ergebnisse aus der Phase 1 des Audits die Vor-Ort-Prüfung in Phase 2 beim Antragsteller (siehe Kapitel 5) vor, indem er einen Auditplan erstellt und insbesondere die am realen IT-Verbund zu prüfenden Bausteinzuordnungen und Maßnahmen nach Vorgabe der Prüfkriterien auswählt und zusammenstellt. Der Auditplan wird in den Auditbericht mit aufgenommen und dient zugleich der zeitlichen Planung der Überwachungsaudits. Insbesondere bei einer Nicht-Fortführung des Audits muss der Auditteamleiter die Zertifizierungsstelle im BSI informieren.

Anschließend begutachtet der Auditor in Phase 2 des Audits auf Basis seines Auditplans stichprobenartig die Umsetzung der dokumentierten Sachverhalte (siehe Kapitel 6). Die Prüfergebnisse, insbesondere Abweichungen, werden im Auditbericht festgehalten. Der Antragsteller hat die Möglichkeit, diese Abweichungen in einer vom Auditor festgelegten Frist zu beheben.

Kommt der Auditor insgesamt über beide Auditphasen zu einem positiven Prüfergebnis, sendet der Antragsteller oder 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. Nach positiver Bewertung des Auditprozesses durch die Zertifizierungsstelle des BSI erteilt das BSI auf der Grundlage des Zertifizierungsantrages und des finalen Auditberichtes ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz.

3.6.2.2 Re-Zertifizierungsaudit

Ein Re-Zertifizierungsaudit ist zum großen Teil identisch mit einem Erstzertifizierungsaudit. Änderungen zur Erstzertifizierung müssen im Auditbericht dargestellt werden. Die Möglichkeit eines Voraudits besteht allerdings nicht mehr.

3.6.2.3 Überwachungsaudit

Ein Überwachungsaudit dient der Überwachung der für das Zertifikat nachgewiesenen Informationssicherheit im IT-Verbund im laufenden Betrieb des IT-Verbundes und hat einen geringeren Umfang als das Zertifizierungsaudit. Das Überwachungsaudit sowie der darauf basierende Auditbericht und dessen Prüfung bei der Zertifizierungsstelle des BSI müssen 1 Jahr bzw. 2 Jahre nach Ausstellung des Zertifikates abgeschlossen sein. Bei Auditortestaten werden keine Überwachungsaudits durchgeführt. Die Überwachungsaudits werden in dem beim vorhergehenden Zertifizierungsaudit geplanten Zeitrahmen (s. Kapitel 5.2) durchgeführt.

In der Phase 1 des Audits werden die aus der zugrundeliegenden Zertifizierung vorliegenden bzw. vom Antragsteller überarbeiteten Referenzdokumente gesichtet. Berücksichtigt werden darüber hinaus die Auditberichte aus dem laufenden Zertifikatszyklus, d.h. der Auditbericht aus dem zugrundeliegenden Zertifizierungsprozess selbst sowie ggf. der Auditbericht aus dem ersten Überwachungsaudit. Die Prüfergebnisse werden im Auditbericht dokumentiert. Stellt der Auditor bei der Dokumentenprüfung Abweichungen (z.B. in der Dokumentation oder in der Sicherheitskonzeption des IT-Verbundes) fest, teilt er diese dem Antragsteller mit einer angemessenen Frist zur Behebung mit und dokumentiert diese im Auditbericht.

Anschließend begutachtet der Auditor in der Phase 2 des Audits auf Basis des Auditplans stichprobenartig die Umsetzung der dokumentierten Sachverhalte. Die Prüfergebnisse, insbesondere Abweichungen, werden im Auditbericht festgehalten. Der Antragsteller hat die Möglichkeit, diese Abweichungen in einer vom Auditor festgelegten Frist zu beheben.

Kommt der Auditor insgesamt über beide Auditphasen zu einem positiven Prüfergebnis, sendet der Antragsteller den vom Auditteamleiter erstellten 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 Prüfprozesse bleibt das vom BSI erteilte ISO 27001-Zertifikat auf der Basis von IT-Grundschutz weiterhin gültig.

3.6.3 Auswahl der Auditoren

Für die Auditierung des IT-Verbundes der Institution beauftragt sie diese Auditoren mit gültiger BSI-Lizenz damit, in einer unabhängigen Prüfung den Status der Informationssicherheit im IT-Verbund zu prüfen und zu verifizieren. Kontaktadressen der zugelassenen Auditoren finden sich im Internet unter der Adresse *http://www.bsi.bund.de/gshb/zert/veroeffentl/auditor27001.htm*

Die Auditoren werden von der antragstellenden Institution ausgewählt und beauftragt und dem BSI im Zertifizierungsantrag bekanntgegeben. Bei der Auswahl der Auditoren müssen Besonderheiten im Aufbau, der Prozesse und Gegebenheiten der beauftragenden Institution berücksichtigt werden. Die Auditoren müssen die Fachkenntnisse besitzen, die sie zur Auditierung der Organisation benötigen.

Die Auditoren müssen dem BSI frühzeitig einen ausführlichen Nachweis vorlegen, dass ihre Unabhängigkeit in den geplanten Audits nicht gefährdet ist (s. auch Kapitel 3.5). Das 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 den Auditor aus dem Zertifizierungsaudit zu wählen. Wechselt der Auditor, ist von der antragstellenden Institution dafür Sorge zu sorgen, dass (mindestens) die Referenzdokomente der antragstellenden Institution sowie alle vorhergehenden Auditberichte aus der zugrundeliegenden Zertifizierung (Auditbericht aus dem Zertifizierungsprozess selbst sowie ggf. der Auditbericht aus dem ersten Überwachungsaudit, falls erfolgt) dem Auditor für das Überwachungsaudit zur Verfügung stehen. Außerdem ist damit zu rechnen, dass die Aufwände des Auditors deutlich höher sind, da dieser sich wegen des Wechsels neu einarbeiten muss.

3.6.4 Wahl von Stichproben für das Audit

Viele Prüfpunkte des vorliegenden Prüfschemas können nur stichprobenartig überprüft werden.

Für eine solche Stichproben-Prüfung wählt der Auditor aus der Gesamtmenge aller Komponenten, auf die sich der jeweilige Prüfpunkt bezieht, geeignete Kandidaten in ausreichender Anzahl für die Stichprobe aus.

Hinsichtlich der Größe der für einen Prüfpunkt ausgewählten Stichprobe gelten folgende Randbedingungen:

- Stehen im vorliegenden Prüfschema konkrete Werte für die Größe einer Stichprobe, sind diese nur als Anhaltspunkte gedacht, die aber nicht unterschritten werden dürfen.
- Bei einer großen Gesamtmenge von Komponenten, auf die sich der betreffende Prüfpunkt bezieht, wählt der Auditor einen sinnvollen Prozentsatz von Kandidaten aus der Gesamtmenge als Stichprobe aus. Bei einer kleinen Gesamtmenge prüft der Auditor eine gewisse feste Anzahl von Kandidaten aus der Gesamtmenge als Stichprobe. Unterschreitet die Gesamtmenge eine untere Grenze, entfällt die Auswahl einer Stichprobe und die Gesamtmenge wird komplett überprüft.
- Stellt der Auditor bei der Prüfung einer ausgewählten Stichprobe Diskrepanzen fest, erweitert er diese Stichprobe, indem er konkret prüft, ob es sich um methodische Fehler oder um Flüchtigkeitsfehler handelt. Er schließt die Stichprobe erst ab, sobald er davon überzeugt ist, um welche Art Fehler es sich handelt. Wenn ein methodischer Fehler Grund für die Diskrepanzen war, muss von Seiten der antragstellenden Institution der komplette geprüfte Bereich überarbeitet werden.

Die Auswahl der Stichproben sowie ihre Größe wird vom Auditteamleiter im Auditbericht dargestellt und begründet. Das BSI behält sich das Recht vor, Änderungen an der Auswahl der Stichproben zu verlangen.

Bei einer Re-Zertifizierung werden im Allgemeinen andere Stichproben gezogen als bei einer Erstzertifizierung. In manchen Fällen kann es aber sinnvoll sein, gezielt die gleichen Stichproben noch einmal zur Prüfung heranzuziehen. Dies wird im Auditbericht für die Re-Zertifizierung entsprechend dargestellt und begründet.

3.6.5 Prüfbegleitung und Auditbegleitung

Die Zertifizierungsstelle und die Lizenzierungsstelle des BSI haben ein Zertifizierungs- bzw. Lizenzierungsschema aufgebaut, das die Vergleichbarkeit von Zertifizierungsverfahren und die Kompetenz der Auditoren sicherstellt.

Die Prüfbegleitung der Zertifizierungsstelle erfolgt durch die intensive Prüfung des Auditberichtes. Dabei wird vor allem auf die Vergleichbarkeit zwischen unterschiedlichen Zertifizierungsverfahren geachtet. Antragsteller und Auditoren sollten bei der Planung von Zertifizierungsverfahren darauf achten, dass genügend Zeit und Ressourcen (Budget, Personal, ...) für Kommentierungszyklen und eventuelle Nachbesserungen eingeplant werden.

Die Zertifizierungsstelle kann in Absprache mit dem Antragsteller einen Teil des Audits begleiten. Diese Kosten werden dem Antragsteller gemäß Kostenverordnung §3 in Rechnung gestellt.

Wie im Lizenzierungsschema beschrieben, begleitet die Lizenzierungsstelle ein Audit des Auditors während der Vertragslaufzeit. Ferner kann sie bei Verdacht auf erhebliche Kompetenzmängel verlangen, den Auditor partiell bei seinen Auditaktivitäten zu begleiten und z.B. an der Prüfung vor Ort (Phase 2 des Audits) teilzunehmen, s. auch Lizenzierungsschema Kap. 2.9. Die Kosten hierfür werden dem Auditor gemäß Kostenverordnung §3 in Rechnung gestellt.

3.7 Erstellung des Auditberichtes

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

Das Format und die Inhalte eines Auditberichtes sind im Prüfschema vordefiniert und im Anhang dieses Dokumentes enthalten. Der auf Phase 1 des Audits bezogene Auditbericht umfasst aus der für einen Auditbericht vorgegebenen Gliederung die Kapitel 1, 2 und 5 sowie die Anlagen (s.u.). Für Phase 2 des Audits sind im Auditbericht die Kapitel 3 bis 6 und die Anlagen aus der vorgegebenen Gliederung zu ergänzen. Insbesondere wird in den Auditbericht eines Erst- bzw. Re-Zertifizierungsaudits auch der im Rahmen der Vorbereitung der Vor-Ort-Prüfung ausgearbeitete Auditplan eingefügt, da dieser die Planung der Überwachungsaudits beinhaltet. Die Referenzdokumente des Antragstellers sind als Anlagen dem Auditbericht beizufügen und gelten als Bestandteil des Auditberichtes.

An die Zertifizierungsstelle geht nur der finale Auditbericht, d.h. der Auditbericht, der komplett die Prüfergebnisse für Phase 1 *und* Phase 2 des Audits beinhaltet, weiter. Der Antragsteller kann sowohl den Auditbericht für Phase 1 wie auch für Phase 2 des Audits erhalten, so dass der Antragsteller auf im Auditbericht festgehaltene und aus den Prüfergebnissen resultierende Auflagen und Empfehlungen des Auditteamleiters rechtzeitig reagieren kann. Es besteht aber auch die Möglichkeit, dass der Auditteamleiter nach Phase 1 nur die festgestellten Abweichungen an den Antragsteller weitergibt.

Der Auditbericht richtet sich ausschließlich an den Antragsteller und die Zertifizierungsstelle. Die Ergebnisse des Auditberichts werden von Auditteam und BSI vertraulich behandelt und nicht an Dritte weitergegeben. Sofern ein anderer Auditor als der initial eingesetzte ein Überwachungsaudit durchführt, müssen vom Antragsteller die Auditdokumente, darunter auch der Auditbericht der Erstzertifizierung, an den neuen Auditteamleiter weitergegeben werden.

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

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

Der Auditbericht wird der Zertifizierungsstelle in Papierform mit den Unterschriften des Auditleiters sowie in elektronischer Form zur Verfügung gestellt. Sofern es sich bei der elektronischen Version um ein pdf-Dokument mit gültiger qualifizierter elektronischer Signatur des Auditteamleiters handelt,

kann auf die Papierform verzichtet werden. Die elektronische Übermittlung des Auditberichtes durch den Auditteamleiter muss verschlüsselt erfolgen.

3.8 Erstzertifizierung

Sobald der Auditbericht zu einem Erstzertifizierungsaudit 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 vorliegenden Prüfschemas. Die Prüfung gegen das Prüfschema erfolgt mit der Zielsetzung, ein einheitliches Niveau aller Zertifizierungen und die Vergleichbarkeit von Zertifizierungsaussagen zu gewährleisten.

Der Auditbericht darf sich nur auf Prüfungen des Auditors (Dokumentenprüfungen und Audit) 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 den Auditor erfüllt werden, diese dürfen maximal eine Nachbesserung durch den Antragsteller nach sich ziehen. Dagegen sind mehrere Nachforderungen an den Auditbericht durch das BSI möglich. Wenn drei Monate nach Abgabe des ersten Auditberichts das Verfahren noch nicht abgeschlossen ist, muss geprüft werden, ob auf der Basis des vorliegenden Berichts noch ein Zertifikat erteilt werden kann.

Ein Zertifikat wird nur erteilt, wenn der finale Auditbericht ein positives Gesamtvotum aufweist und durch die Zertifizierungsstelle akzeptiert wurde. Die Zertifizierungsstelle erteilt das Zertifikat und fertigt einen Anhang zur Urkunde mit zusätzlichen Informationen zum Zertifizierungsverfahren an sowie falls gewünscht einen Zertifikatsbutton zu Werbezwecken. Sofern der Antragsteller einer Veröffentlichung des Zertifikates zugestimmt hat, wird die Tatsache der Zertifizierung auf den Internetseiten des BSI veröffentlicht. Auf Nachfrage muss die Zertifizierungsstelle des BSI jedoch Informationen zu allen erteilten Zertifikaten mitteilen.

Ein erteiltes Zertifikat ist mit jährlichen Überwachungsaudits verbunden. Für nähere Informationen zur Durchführung eines Überwachungsaudits sei auf Kap. 9 verwiesen.

Ein Auditbericht zu einem Überwachungsaudit (in finaler Fassung) wird ebenfalls von der Zertifizierungsstelle gegen die Vorgaben des definierten Prüfschemas geprüft. Nur im Falle der Einhaltung aller Vorgaben bleibt das erteilte Zertifikat gültig. Es erfolgt keine Neuausstellung der Zertifikatsurkunde oder Ergänzung des zugehörigen Anhangs durch die Zertifizierungsstelle.

Die zertifizierte Institution darf die Urkunde sowie einen vom BSI zur Verfügung gestellten Zertifikatsbutton nur unter der Bedingung verwenden, dass die Zertifikatsurkunde und der zugehörige Anhang 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.

3.9 Re-Zertifizierung

Ein Zertifikat ist drei Jahre gültig. Vor Ablauf der Gültigkeit des Zertifikates kann ein Re-Zertifizierungsverfahren durchgeführt werden.

Das Re-Zertifizierungsverfahren, sein Ablauf und seine Rahmenbedingungen sind einer Erst-Zertifizierung vergleichbar und sind sinngemäß zu übertragen, wobei Änderungen zum vorhergehenden Audit deutlich gemacht werden müssen. Ein Voraudit darf bei einer Re-Zertifizierung nicht erfolgen.

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

Eine Verlängerung von Auditortestaten ist nicht möglich. Um die Qualifizierung nach der zweijährigen Gültigkeitsdauer der Auditortestate fortzusetzen, muss stattdessen eine höhere Stufe im

Qualifizierungsschema erreicht werden. Weitere Informationen zu der Verlängerung von Auditortestaten sind im Kapitel 11.2 zu finden.

3.10 Aussetzung und Zurückziehung von Zertifikaten

3.10.1 Aussetzung von Zertifikaten

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

- Das Überwachungsaudit wird nicht fristgerecht durchgeführt.
- Der Auditbericht zum Überwachungsaudit wird zu spät bei der Zertifizierungsstelle eingereicht.
- Im Überwachungsaudit werden Abweichungen im IT-Verbund bzgl. seiner Dokumentation und/oder Realisierung erkannt, die vom Antragsteller innerhalb der Frist noch nicht behoben sind.

Ferner kann auf Wunsch der zertifizierten Institution nach Rücksprache mit der Zertifizierungsstelle die Aussetzung eines Zertifikates erfolgen.

Ausgesetzte Zertifikate werden aus der Liste der ISO 27001-Zertifikate auf der Basis von IT-Grundschutz auf den Internetseiten des BSI entfernt. Die Zertifikatsurkunde inklusive Anhang wird vom Zertifikatsinhaber im Original zurückgefordert und ist an die Zertifizierungsstelle zurückzugeben. 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.

3.10.2 Zurückziehung von Zertifikaten

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

- Im Überwachungsaudit werden gravierende Abweichungen im IT-Verbund bzgl. seiner Dokumentation und / oder Realisierung erkannt, die vom Antragsteller nicht in einem angemessenen Zeitraum behoben werden können.
- Ein Überwachungsaudit ergibt, dass der IT-Verbund die Anforderungen an ein ISMS nicht mehr erfüllt bzw. den Anforderungen des IT-Grundschutzes nicht mehr gerecht wird.
- Der Verstoß gegen Auflagen aus der Zertifzierung wird bekannt (beispielsweise ein Verstoß gegen die Verwendungsbedingungen für das Zertifikat, die Nichteinhaltung von Auflagen, die sich aus dem Zertifizierungsprozess bzw. dem Zertifikats(anhang), Zertifizierungsbescheid oder Auditbericht ergeben, wie etwa wesentliche Veränderungen am zertifizierten IT-Verbund ohne Information an die Zertifizierungsstelle, Irreführungen und Täuschungen der Institution gegenüber dem Auditor bzw. dem BSI, begründete Beschwerden beim BSI über die Institution)

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 inklusive Anhang wird von der zertifizierten Institution im Original zurückgefordert und ist 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 IT-Verbund ist, falls vorgesehen, ein neues Zertifizierungsverfahren aufzusetzen.

Hält das BSI es z.B. nach Beschwerden über die Institution für erforderlich, kurzfristig ein Audit durchzuführen oder durch einen Auditor durchführen zu lassen, so läuft dies nach den Vorgaben dieses Dokumentes ab. Bei begründeten Beschwerden ist die Durchführung dieses Audits kostenpflichtig.

4. Phase 1 des Zertifizierungsaudits: Sichtung der Referenzdokumente

4.1 Überblick über die Auditaktivitäten

Die vom Antragsteller vorgelegten Referenzdokumente werden gesichtet und anhand der folgenden Kriterien bewertet. Alle Bewertungen der Referenzdokumente werden in den Auditbericht übernommen. Die durchgeführten Prüfungen müssen angemessen und reproduzierbar sein. Die Prüfergebnisse und Bewertungen müssen im Auditbericht verständlich und nachvollziehbar dokumentiert werden.

4.2 Voraudit

Beim Voraudit kann der Auditor gezielt einzelne Aspekte aus Phase 1 und 2 auswählen und stichprobenartig prüfen. Außer intensiven Gesprächen mit dem Antragsteller hat der Auditor die Möglichkeit, sich Dokumente, Prozeduren und Implementierungen anzusehen, um einen Eindruck davon zu bekommen, ob ein Zertifizierungsaudit prinzipiell zu einem positiven Ergebnis führen könnte. Falls der Auditor hierbei nicht zu einem positiven Votum kommt, ist es sinnvoll, das Audit abzubrechen und zu einem späteren Zeitpunkt fortzuführen.

Prüfungen, die dem Auditor nur dazu dienen, ein Verständnis des IT-Verbundes zu gewinnen, müssen nicht ausführlich dokumentiert werden. Das Voraudit darf nicht mehr als ein Drittel der für das nachfolgende konkrete Audit angesetzten Zeit in Anspruch nehmen. Das Voraudit darf nicht dem Zweck dienen, die Institution auf später geprüfte Aspekte vorzubereiten, indem identische Prüfungen wiederholt werden. Es können aber Prüfungen vorgezogen werden, d.h. Prüfungen aus dem vorliegenden Prüfschema werden bereits im Voraudit durchgeführt und im Auditbericht dokumentiert. Wird ein Voraudit durchgeführt, so muss im Auditbericht dessen Umfang und Dauer kurz dargestellt werden.

Wenn der Auditor ein Voraudit durchführt, ist es sinnvoll, unter anderem die Prüfpunkte zu „4.3 Aktualität der Dokumente“, „4.4 IT-Sicherheitsrichtlinien“, „4.5.1 Nachvollziehbarkeit der Abgrenzung des IT-Verbunds“ und „6.2 Wirksamkeit des Managementsystems für Informationssicherheit“ schon zu diesem Zeitpunkt durchzuführen oder anzureißen.

4.3 Aktualität der Dokumente

4.3.1 Aktualität der Version der Prüfgrundlagen

Ziel: Es muss festgelegt werden, welche Version des BSI-Standards 100-2 und damit der Version des Standards 27001 sowie welche Version der IT-Grundschutz-Kataloge als Grundlage für die Auditierung verwendet werden soll. Zulässig ist für den Standard 100-2 die Verwendung der aktuellen Version, für die IT-Grundschutz-Kataloge ist auch die Vorgängerversion zulässig. **Es wird jedoch dringend empfohlen, die jeweils aktuelle Version der IT-Grundschutz-Kataloge zu verwenden, da zum Zeitpunkt der Zertifikatsvergabe geprüft wird, ob eine zulässige Version verwendet wurde.** Nur für Auditierungen auf der Grundlage dieser Versionen kann ein Zertifikat vergeben werden.

Aktion: Der Auditor dokumentiert die Versionen (Monat, Jahr) der Dokumente, auf deren Grundlage die Auditierung des Untersuchungsgegenstands erfolgt ist.

Votum: Werden zulässige Versionen angewendet?

4.3.2 Aktualität der Referenzdokumente

Ziel: Der Auditor führt das Audit auf einem bestimmten Dokumentenstand durch, der zum Zeitpunkt der Abgabe der Referenzdokumente an den Auditor gültig ist. Der Auditor prüft, ob die ihm vorliegenden Dokumente von ausreichender Aktualität sind.

Aktion: Der Auditor bewertet die Aktualität der Referenzdokumente.

Hinweis: Da einige Dokumente (z.B. Richtlinien) allgemeiner formuliert sind als andere (z.B. der Basis-Sicherheitscheck), werden Änderungen in Dokumenten unterschiedlich häufig vorgenommen. Alle Dokumente müssen aber regelmäßig bewertet werden, ob sie noch den aktuellen Gegebenheiten entsprechen.

Votum: Sind die Referenzdokumente von ausreichender Aktualität?

4.3.3 Datum des Basis-Sicherheitschecks

Ziel: Das Audit ist durch das Datum des Basis-Sicherheitschecks gekennzeichnet. Da regelmäßig Neubewertungen des Sicherheitslage des IT-Verbundes erfolgen müssen, darf die letzte Aktualisierung des Basis-Sicherheitschecks zum Zeitpunkt der Abgabe des Auditberichtes an die Zertifizierungsstelle nicht älter als 1 Jahr sein.

Aktion: Der Auditor dokumentiert Datum und Version des Basis-Sicherheitschecks, der zur Prüfung herangezogen wurde.

4.4 IT-Sicherheitsrichtlinien

4.4.1 Vollständigkeit der IT-Sicherheitsrichtlinien

Ziel: Strategische Leitaussagen zu Informationssicherheit, konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen werden benötigt, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

Aktion: Der Auditor prüft die vorhandenen und als Referenzdokumente A.0 aufgelisteten Richtlinien auf Vollständigkeit. Insbesondere prüft der Auditor, ob sonstige Richtlinien und Konzepte in der Situation der Institution benötigt werden und fordert diese gegebenenfalls an.

Votum: Sind alle benötigten Richtlinien vorhanden?

4.4.2 Verantwortung des Managements

Ziel: Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Organisation und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Informationssicherheitsprozess initiieren, steuern und kontrollieren.

Aktion: Der Auditor prüft, ob alle vorhandenen Richtlinien vom Management getragen und durch das Management veröffentlicht werden. Dies kann beispielsweise durch die Unterschrift des Managements unter den Richtlinien sichtbar sein.

Votum: Werden die vorhandenen Richtlinien durch das Management verantwortet?

4.4.3 Nachvollziehbarkeit der Informationssicherheitsrichtlinien

Ziel: Die Richtlinien müssen für die Situation der Institution geeignet und angemessen sein. In der Maßnahme „M 2.192 Erstellung einer IT-Sicherheitsleitlinie“ des Bausteins „B 1.0 IT-

Sicherheitsmanagement“ ist aufgezeigt, welche Punkte bei der Erstellung einer IT-Sicherheitsleitlinie beachtet werden müssen. Diese Punkte können entsprechend auch auf die Konzeption anderer Richtlinien übertragen werden.

Aktion: Der Auditor bewertet die Sinnhaftigkeit der einzelnen Richtlinien und listet jeweils auf, inwiefern die Richtlinie plausibel und für die Institution geeignet ist.

Votum: Sind die vorhandenen Richtlinien sinnvoll und für die Institution angemessen? Sind sie konsistent zueinander und zu anderen vorhandenen Dokumenten?

4.5 IT-Strukturanalyse

4.5.1 Nachvollziehbarkeit der Abgrenzung des Untersuchungsgegenstandes

Ziel: Ein Untersuchungsgegenstand ist sinnvoll abgegrenzt, wenn er alle organisatorischen Maßnahmen, personellen Ressourcen sowie technischen und infrastrukturellen Komponenten umfasst, die zur Unterstützung einer oder mehrerer Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen.

Der Untersuchungsgegenstand muss außerdem eine sinnvolle Mindestgröße im Gesamtkontext des Unternehmens bzw. der Behörde haben, d. h. er muss substantiell zum Funktionieren der Institution oder eines wesentlichen Teils der Institution beitragen.

Aktion: Der Auditor begründet in kurzen Worten, warum der Untersuchungsgegenstand sinnvoll abgegrenzt ist. Anhaltspunkte, die gegen eine sinnvolle Abgrenzung des Untersuchungsgegenstands sprechen, werden dokumentiert.

Votum: Ist der Untersuchungsgegenstand sinnvoll abgegrenzt?

Hinweis: Dieser Prüfpunkt ist nicht mit der Abstimmung des IT-Verbundes durch die Zertifizierungsstelle gleichzusetzen. Der Auditor muss die Prüfung anhand der ihm vorliegenden Informationen selbst durchführen, da diese Informationen wesentlich umfangreicher sind als die der Zertifizierungsstelle zur Abstimmung eines IT-Verbunds vorliegenden.
Falls die Abgrenzung des IT-Verbunds für eine Zertifizierung grundsätzlich ungeeignet ist, wird die Auditierung abgebrochen, ohne dass der Institution die Möglichkeit einer Nachbesserung eingeräumt wird. Falls weiterhin ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz angestrebt wird, ist eine neue Auditierung eines geeignet definierten IT-Verbundes zu initiieren.

4.5.2 Identifizierbarkeit der Komponenten im bereinigten Netzplan

Ziel: Alle im bereinigten Netzplan dargestellten Komponenten müssen eindeutig identifiziert werden können, also mit einer eindeutigen Bezeichnung versehen sein.

Aktion: Der Auditor prüft, ob alle dargestellten Komponenten mit einer Bezeichnung gekennzeichnet sind, und dokumentiert dies.

Votum: Sind alle Komponenten im bereinigten Netzplan sinnvoll mit einer Bezeichnung gekennzeichnet?

4.5.3 Umfang der Liste der IT-Systeme

Ziel: In der Liste der IT-Systeme muss jeweils eine eindeutige Bezeichnung des IT-Systems, eine Beschreibung (Typ und Funktion), die Plattform (z. B. Hardware-Architektur/Betriebssystem), Anzahl der zusammengefassten IT-Systeme (bei Gruppen),

Aufstellungsort, Status des IT-Systems (in Betrieb, im Test, in Planung) und die Anwender/Administratoren des IT-Systems aufgeführt sein.

Aktion: Der Auditor prüft, ob in der Liste der IT-Systeme alle benötigten Informationen aufgeführt sind und dokumentiert ggf. Abweichungen.

Votum: Enthält die Liste der IT-Systeme alle benötigten Informationen?

4.5.4 Konformität der Liste der IT-Systeme mit dem Netzplan

Ziel: Die in der Liste der IT-Systeme aufgeführten Systeme müssen mit denen im bereinigten Netzplan übereinstimmen.

Aktion: Der Auditor vergleicht stichprobenartig die in der Liste der IT-Systeme aufgeführten Systeme mit denen im Netzplan und dokumentiert eventuelle Abweichungen.

Votum: Stimmt die Liste der IT-Systeme mit denen im bereinigten Netzplan überein?

4.5.5 Umfang der Liste der IT-Anwendungen

Ziel: In der Liste der IT-Anwendungen muss für jede Anwendung eine eindeutige Bezeichnung vergeben sein. Weiterhin muss ersichtlich sein, welche wesentlichen Geschäftsprozesse von der Ausführung der einzelnen IT-Anwendungen abhängen und welche IT-Systeme für die Ausführung der jeweiligen Anwendung benötigt werden.

Aktion: Der Auditor prüft, ob in der Liste der IT-Anwendungen alle benötigten Informationen aufgeführt sind, und dokumentiert ggf. vorhandene Abweichungen.

Votum: Enthält die Liste der IT-Anwendungen alle benötigten Informationen?

4.6 Schutzbedarfsfeststellung

4.6.1 Plausibilität der Definition der Schutzbedarfskategorien

Ziel: Die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ werden anhand von möglichen Schäden definiert. Insbesondere sollte die Höhe der genannten Schäden in der Reihenfolge „normal“, „hoch“, „sehr hoch“ ansteigen.

Aktion: Der Auditor prüft, ob die Definition der Schutzbedarfskategorien plausibel ist, und dokumentiert ggf. Inkonsistenzen.

Hinweis: Wenn mehr als drei Schutzbedarfskategorien definiert wurden, stellt der Auditor hier Überlegungen an, welche neu definierten Kategorien „hoch“ bzw. „sehr hoch“ entsprechen. Diese Information wird zur Überprüfung der Entscheidung benötigt, welche Objekte in die ergänzende Sicherheitsanalyse aufgenommen werden. Eine Definition von nur einer oder zwei Schutzbedarfskategorien ist nicht sinnvoll.

Votum: Ist die Definition der Schutzbedarfskategorien plausibel?

4.6.2 Vollständigkeit der Schutzbedarfsfeststellung der IT-Anwendungen

Ziel: Für jede in der Liste der IT-Anwendungen aufgeführte Anwendung muss der Schutzbedarf bzgl. Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert und begründet sein. Dabei ist der Schutzbedarf der Informationen und Daten der Geschäftsprozesse, die die Anwendung unterstützen, mit einzubeziehen.

Aktion: Der Auditor prüft, ob der Schutzbedarf der in der Liste der IT-Anwendungen aufgeführten Anwendungen vollständig dokumentiert und begründet ist. Eventuell vorhandene Abweichungen werden im Auditbericht vermerkt.

Votum: Ist der Schutzbedarf der IT-Anwendungen vollständig dokumentiert und begründet?

4.6.3 Vollständigkeit der Schutzbedarfsfeststellung der IT-Systeme

Ziel: Für jedes in der Liste der IT-Systeme aufgeführte System muss der Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert und begründet sein.

Aktion: Der Auditor prüft, ob für jedes in der Liste der IT-Systeme aufgeführte System der Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert und begründet ist. Eventuell vorhandene Abweichungen werden im Auditbericht vermerkt.

Votum: Ist der Schutzbedarf der IT-Systeme vollständig dokumentiert und begründet?

4.6.4 Plausibilität der Schutzbedarfsfeststellung der IT- Systeme

Ziel: Der Schutzbedarf für die IT-Systeme leitet sich aus dem Schutzbedarf der IT-Anwendungen ab (in der Liste der IT-Anwendungen ist vermerkt, von welchen IT-Systemen die Ausführung einer bestimmten IT-Anwendung abhängt). Dabei sind das Maximumprinzip, der Kumulationseffekt und der Verteilungseffekt zu berücksichtigen. Die Begründungen für den Schutzbedarf der einzelnen IT-Systeme müssen nachvollziehbar sein.

Aktion: Der Auditor führt hierzu anhand der Liste der IT-Systeme, der Liste der IT-Anwendungen und dem Schutzbedarf dieser Komponenten eine Stichprobenprüfung durch. Der Auditor dokumentiert, welche IT-Anwendungen und IT-Systeme als Stichproben ausgewählt wurden. Für jede Stichprobe dokumentiert der Auditor, ob der Schutzbedarf korrekt abgeleitet wurde und ob die Begründung nachvollziehbar ist.

Votum: Wurde der Schutzbedarf der IT-Systeme korrekt aus dem Schutzbedarf der IT-Anwendungen abgeleitet und sind die Begründungen nachvollziehbar?

4.6.5 Kritikalität der Kommunikationsverbindungen

Ziel: Eine Verbindung kann kritisch sein, weil sie eine Außenverbindung darstellt (K1), weil sie hochvertrauliche (K2), hochintegere (K3) oder hochverfügbare (K4) Daten transportiert, oder weil über sie bestimmte hochschutzbedürftige Daten nicht transportiert werden dürfen (K5). Für jede kritische Kommunikationsverbindung muss vermerkt sein, aus welchem oder welchen dieser Gründe sie kritisch ist (K1-K5). Weiterhin muss sichergestellt sein, dass alle Verbindungen, die in oder über unkontrollierte Bereiche führen (z. B. ins Internet, über Funknetze oder über nicht behörden- oder firmeneigenes Gelände), als Außenverbindungen gekennzeichnet sind (K1) und somit kritisch sind.

Aktion: Der Auditor prüft, ob für jede kritische Verbindung vermerkt ist, aus welchen Gründen (K1-K5) sie kritisch ist. Weiterhin prüft er anhand des bereinigten Netzplans, ob alle dort eingezeichneten Außenverbindungen als solche gekennzeichnet sind (K1). Evtl. vorhandene Abweichungen werden im Auditbericht dokumentiert.

Votum: Ist für jede kritische Kommunikationsverbindung vermerkt, aus welchen Gründen (K1-K5) sie kritisch ist, und sind alle Außenverbindungen als kritisch gekennzeichnet (K1)?

4.6.6 Plausibilität der Schutzbedarfsfeststellung der Räume

Ziel: Der Schutzbedarf der Räume leitet sich aus dem Schutzbedarf der darin betriebenen IT-Systeme bzw. der IT-Anwendungen ab, für die diese Räume genutzt werden. Dabei sind das Maximum-Prinzip, der Kumulationseffekt und der Verteilungseffekt zu berücksichtigen.

Aktion: Der Auditor führt hierzu anhand des Schutzbedarfs der IT-Systeme eine Stichprobenprüfung durch. Für jede Stichprobe ist zu überprüfen, ob der Schutzbedarf des Raums korrekt aus dem Schutzbedarf der IT-Anwendungen und IT-Systeme abgeleitet wurde. Dokumentiert werden die ausgewählten Stichproben, die Ergebnisse der Einzelprüfungen und ggf. Abweichungen bzw. Widersprüche.

Votum: Ist der Schutzbedarf der Räume korrekt aus dem Schutzbedarf der IT-Anwendungen und IT-Systeme abgeleitet?

4.7 Modellierung des IT-Verbunds

4.7.1 Nachvollziehbarkeit der Modellierung

Ziel: Es muss sichergestellt sein, dass jeder Baustein der IT-Grundschutz-Kataloge auf alle Zielobjekte im IT-Verbund angewandt wird, für die er relevant ist. Insbesondere müssen durch die Modellierung daher alle IT-Systeme (siehe Liste der IT-Systeme) und alle Räume, in denen diese IT-Systeme betrieben werden, abgedeckt sein. In den IT-Grundschutz-Katalogen ist für jeden Baustein beschrieben, auf welche Zielobjekte er anzuwenden ist.

Für einige Typen von IT-Systemen sind in den IT-Grundschutz-Katalogen derzeit keine eigenständigen Bausteine vorhanden, beispielsweise für Computer mit dem Betriebssystem OS/2. Falls der IT-Verbund solche IT-Systeme umfasst, sollten für die Modellierung ähnliche oder generische Bausteine herangezogen werden

Aktion: Der Auditor prüft für jeden in den IT-Grundschutz-Katalogen enthaltenen Baustein, ob er in der vorliegenden Modellierung auf alle relevanten Zielobjekte im betrachteten IT-Verbund angewandt wurde. Maßgeblich hierfür sind die Vorgaben zur Modellierung in den IT-Grundschutz-Katalogen. Zielobjekte können dabei übergeordnete Aspekte, Gruppen und Einzelkomponenten sein. Insbesondere ist zu prüfen, ob

- alle übergeordneten Aspekte (z. B. Personal) korrekt modelliert sind,
- alle beteiligten Gebäude, Räume, Schutzschränke und die Verkabelung im Hinblick auf bautechnische Sicherheit berücksichtigt sind,
- alle in der Liste der IT-Systeme enthaltenen IT-Systeme abgedeckt sind,
- die netztechnischen Sicherheitsaspekte durch die entsprechenden Bausteine korrekt modelliert sind und
- diejenigen IT-Anwendungen, für die eigenständige Bausteine existieren (z. B. Datenbanken), behandelt wurden.

Dokumentiert wird für jeden Baustein, ob er auf alle relevanten Zielobjekte angewandt wurde und auf welche Zielobjekte er angewandt wurde. Wenn ein Baustein nicht (oder auf ein Objekt nicht) angewandt wurde, muss dafür eine nachvollziehbare Begründung im Auditbericht angegeben und vom Auditor auf Plausibilität geprüft werden (Beispiel: der Baustein B 2.10 Mobiler Arbeitsplatz wird nicht angewandt, obwohl sich Notebooks im IT-Verbund befinden).

Der Auditor ermittelt anhand der Liste der IT-Systeme und der Modellierung, welche Komponenten nicht direkt durch Bausteine der IT-Grundschutz-Kataloge abgebildet werden können. Diese Komponenten (bzw. Gruppen) sowie deren Schutzbedarf werden im Auditbericht dokumentiert. Für jede dieser Komponenten prüft der Auditor, ob geeignete

generische oder ähnliche Bausteine der IT-Grundschutz-Kataloge zur Modellierung herangezogen und ob diese sinnvoll und korrekt eingesetzt wurden.

Hinweis: Der Baustein B 1.5 Datenschutz ist nicht zertifizierungsrelevant.

Votum: Wurde in der vorliegenden Modellierung jeder Baustein der IT-Grundschutz-Kataloge auf alle Zielobjekte angewandt, für die er relevant ist?

Sind ähnliche oder generische Bausteine, die für Komponenten ersatzweise herangezogen wurden, korrekt angewandt?

4.7.2 Korrektheit der Gruppenbildung

Ziel: Komponenten dürfen zu einer Gruppe zusammengefasst werden, falls sie vom gleichen Typ, gleich oder nahezu gleich konfiguriert bzw. gleich oder nahezu gleich in das Netz eingebunden sind, den gleichen administrativen, infrastrukturellen Rahmenbedingungen unterliegen und die gleichen Anwendungen bedienen. Soweit dies noch nicht vorher erfolgt ist (beispielsweise in der Liste der IT-Systeme), können im Rahmen der Modellierung weitere Komponenten zu Gruppen zusammengefasst werden.

Aktion: Der Auditor wählt aus der Modellierung einige Gruppen als Stichproben aus und prüft jeweils, ob die Gruppenbildung zulässig ist. Dokumentiert werden die ausgewählten Stichproben, die Ergebnisse der Einzelprüfungen und ggf. Abweichungen oder Widersprüche.

Votum: Sind die in der Modellierung verwendeten Gruppen korrekt gebildet?

4.8 Ergebnis des Basis-Sicherheitschecks

4.8.1 Konformität zur Modellierung

Ziel: Die beim Basis-Sicherheitscheck verwendeten Bausteine der IT-Grundschutz-Kataloge müssen mit denen in der Modellierung übereinstimmen.

Aktion: Der Auditor führt anhand der Modellierung eine vollständige Überprüfung durch. Etwaige Abweichungen werden dokumentiert.

Votum: Stimmen die im Basis-Sicherheitscheck verwendeten Bausteine der IT-Grundschutz-Kataloge mit denen in der Modellierung des IT-Verbunds überein?

4.8.2 Transparenz der Interviewpartner

Ziel: Für jeden Baustein im Basis-Sicherheitscheck muss erkennbar sein, welche Personen zur Ermittlung des Umsetzungsstatus befragt worden sind und wer die Befragung durchgeführt hat.
Die befragten Personen sollten mit Name und Funktion gekennzeichnet sein. Hierzu kann die Funktionsbezeichnung in der Institution verwendet werden, wenn diese klar und nachvollziehbar ist. Eine Abbildung auf die in der IT-Grundschutz-Vorgehensweise definierten Rollen ist nicht zwingend erforderlich, kann jedoch hilfreich sein.

Aktion: Der Auditor überprüft die Angaben zu den Interviewpartnern anhand des vorgelegten Basis-Sicherheitschecks und dokumentiert etwaige Abweichungen.

Votum: Ist für jeden Baustein im Basis-Sicherheitscheck erkennbar, welche Personen zur Ermittlung des Umsetzungsstatus befragt worden sind und wer die Befragung durchgeführt hat?

4.8.3 Umsetzungsgrad der IT-Grundschutz-Maßnahmen

Ziel: Alle im Basis-Sicherheitscheck bearbeiteten Maßnahmen müssen folgende Kriterien erfüllen:

- Die im Basis-Sicherheitscheck bearbeiteten Maßnahmen müssen alle Maßnahmen umfassen, die die IT-Grundschutz-Kataloge für den jeweiligen Baustein vorsehen. Es dürfen also keine Maßnahmen aus den Bausteinen gestrichen oder geändert werden. Die Prüfung muss anhand der Original-Maßnahmen aus den IT-Grundschutz-Katalogen erfolgen.
- Für jede Maßnahme muss in der Erhebung der Umsetzungsstatus („entbehrlich“, „ja“, „teilweise“, „nein“) vermerkt sein.
- Für jede Maßnahme mit Umsetzungsstatus „entbehrlich“ ist eine plausible Begründung erforderlich. Eine Maßnahme ist entbehrlich, falls eine mindestens gleichwertige Ersatzmaßnahme realisiert ist oder wenn die Funktionalität, deren Risiken durch die IT-Grundschutzmaßnahme minimiert werden sollen, nicht eingesetzt wird.
- Je nach angestrebter Ausprägung der Qualifizierung muss sichergestellt sein, dass der Umsetzungsstatus der erforderlichen Maßnahmen ausreichend ist. Eine Maßnahme gilt dabei als umgesetzt, wenn sie entweder den Status „ja“ oder den Status „entbehrlich“ hat.

Hinweis: Die Maßnahmen der IT-Grundschutz-Kataloge sind getrennt für jeden Baustein mit den Buchstaben „A“, „B“, „C“ und „Z“ gekennzeichnet.

- Für das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz sind alle relevanten Maßnahmen, die mit „A“, „B“ und „C“ gekennzeichnet sind, umzusetzen.
- Für ein Auditortestat Einstiegsstufe sind die mit „A“ gekennzeichneten Maßnahmen und für ein Auditortestat Aufbaustufe sind die mit „A“ und „B“ gekennzeichneten Maßnahmen umzusetzen.
- Mit „Z“ gekennzeichnete Maßnahmen müssen für keine der drei Ausprägungen zwingend umsetzt sein. Sie sind optional anzuwenden und meist für einen höheren Schutzbedarf gedacht.

Aktion: Der Auditor überprüft den Basis-Sicherheitscheck vollständig darauf, ob für alle enthaltenen IT-Grundschutz-Maßnahmen die oben genannten Kriterien erfüllt sind. Alle Defizite werden im Auditbericht dokumentiert.

Votum: Ist der Basis-Sicherheitscheck vollständig und ist der Umsetzungsgrad der IT-Grundschutz-Maßnahmen für die angestrebte Ausprägung der IT-Grundschutz-Qualifizierung ausreichend?

4.9 Ergänzende Sicherheitsanalyse und ergänzende Risikoanalyse

Für Auditortestate ist die Prüfung der ergänzenden Sicherheitsanalyse und der ergänzenden Risikoanalyse nicht erforderlich, da für Auditortestate weniger IT-Grundschutz-Maßnahmen umgesetzt werden müssen als für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz. Dadurch würden bei der Durchführung von einer ergänzenden Risikoanalyse die fehlenden IT-Grundschutz-Maßnahmen erneut erkannt, so dass das Verfahren ineffektiv würde.

4.9.1 Vollständigkeit und Plausibilität der ergänzenden Sicherheitsanalyse

Ziel: Für alle Zielobjekte des IT-Verbundes, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind,

muss entschieden worden sein, ob weitere Risikobetrachtungen erforderlich sind. Dieser Entscheidungsprozess auf Managementebene wird als ergänzende Sicherheitsanalyse bezeichnet. Die Ergebnisse der ergänzenden Sicherheitsanalyse müssen begründet und nachvollziehbar in Form eines Managementberichtes dokumentiert sein.

Aktion: Zunächst führt der Auditor eine vollständige Prüfung durch, ob für alle Zielobjekte, die eine oder mehrere der oben genannten Bedingungen erfüllen, eine ergänzende Sicherheitsanalyse durchgeführt wurde. Anschließend prüft der Auditor anhand von Stichproben aus allen o.g. Anwendungsfällen, ob die Ergebnisse begründet und die Begründungen plausibel sind. Der Auditor begründet die gewählten Stichproben und dokumentiert die Ergebnisse der Einzelprüfungen.

Votum: Ist die ergänzende Sicherheitsanalyse vollständig durchgeführt und sind die Begründungen nachvollziehbar?

4.9.2 Vollständigkeit und Plausibilität der ergänzenden Risikoanalyse

Ziel: In der ergänzenden Sicherheitsanalyse wurden die Komponenten identifiziert, für die eine ergänzende Risikoanalyse durchgeführt werden muss. Dabei sind neben den Gefährdungen der IT-Grundschutz-Kataloge zusätzliche Gefährdungen und Sicherheitslücken zu identifizieren und durch das Management zu bewerten. Die Entscheidung, ob ein Risiko getragen wird, ob der IT-Verbund so umgestaltet wird, dass die Gefährdung nicht mehr relevant ist, oder ob zusätzliche Sicherheitsmaßnahmen zu ergreifen sind, ist zu dokumentieren.

Aktion: Zunächst führt der Auditor eine vollständige Prüfung durch, ob für alle (laut ergänzender Sicherheitsanalyse) sicherheitskritischen Zielobjekte eine ergänzende Risikoanalyse durchgeführt wurde. Anschließend prüft der Auditor anhand von Stichproben aus allen o.g. Anwendungsfällen, ob die ergänzenden Risikoanalysen nachvollziehbar dokumentiert wurden und ob die jeweiligen Begründungen plausibel sind. Der Auditor begründet die gewählten Stichproben und dokumentiert die Ergebnisse der Einzelprüfungen.

Votum: Ist für alle sicherheitskritischen Komponenten eine ergänzende Risikoanalyse durchgeführt worden? Sind die Begründungen nachvollziehbar? Sind die zusätzlichen Sicherheitsmaßnahmen ausreichend, d. h. wirken sie angemessen gegen die identifizierten Gefährdungen? Wurden die Sicherheitsmaßnahmen konsolidiert?

4.9.3 Umsetzungsgrad aller Maßnahmen

Ziel: Der Umsetzungsstatus der konsolidierten Maßnahmen ist zu dokumentieren. Für jede zusätzliche in der ergänzenden Sicherheits- oder Risikoanalyse identifizierte Maßnahme muss der Umsetzungsstatus („entbehrlich“, „ja“, „teilweise“, „nein“) vermerkt sein. Ggf. ist der Umsetzungsstatus der früher geprüften IT-Grundschutz-Maßnahmen zu aktualisieren. Die Ergebnisse sind als Ergänzung des Basis-Sicherheitsschecks zu dokumentieren. Es muss sichergestellt sein, dass der Umsetzungsstatus der Maßnahmen ausreichend ist. Eine Maßnahme gilt dabei als umgesetzt, wenn sie entweder den Status „ja“ oder den Status „entbehrlich“ hat.

Aktion: Der Auditor überprüft den Umsetzungsstatus aller konsolidierten Maßnahmen und ermittelt, ob der Umsetzungsstatus der Maßnahmen ausreichend ist. Alle Defizite werden im Auditbericht dokumentiert.

Votum: Ist die Ergänzung des Basis-Sicherheitsschecks vollständig? Ist der Umsetzungsgrad der in der ergänzenden Sicherheits- oder Risikoanalyse zusätzlich identifizierten Maßnahmen ausreichend?

5. Zertifizierungsaudit: Vorbereitung der Audittätigkeit vor Ort

5.1 Entscheidung zur Weiterführung des Audits mit Phase 2

Während der Phase 1 des Audits dokumentiert der Auditteamleiter seine Prüfungen im ersten Teil des Auditberichtes. Sind dabei Abweichungen aufgetreten, teilt der Auditteamleiter der auditierten Institution diese mit und gibt ihr damit die Möglichkeit, sie schon vor Durchführung der Phase 2 des Audits zu beheben.

Hat der Auditor den Eindruck, eine Fortführung des Audits mit Phase 2 sei auch nach der Behebung der Abweichungen nicht möglich, besteht die Möglichkeit des Abbruchs. Dies ist beispielsweise der Fall, wenn bei der Institution nicht die Bereitschaft erkennbar ist, beim Zertifizierungsaudit aktiv mitzuwirken.

Nach der Dokumentation der Auditergebnisse von Phase 1 überprüft der Auditteamleiter, ob im Auditteam die Fachkenntnisse vorliegen, um das Audit mit der Phase 2 weiterzuführen. Dabei müssen sowohl sektorspezifische (d.h. die Institution arbeitet in einem Bereich, für das zum Verständnis der Prozesse spezielle Kenntnisse benötigt werden) als auch bausteinspezifische (d.h. der Auditor besitzt für für den IT-Verbund wichtige Bausteine nicht die tiefgreifenden Fachkenntnisse, z.B. für SAP) Fachkenntnisse in Betracht gezogen werden. Liegen die erforderlichen Fachkenntnisse auf einem oder mehreren Gebieten nicht vor, so erweitert der Auditteamleiter das Auditteam um einen Experten oder weitere Auditoren in diesem Gebiet. Für diese zusätzlichen Experten und Auditoren gelten entsprechende Anforderungen an ihre Unabhängigkeit im Verfahren wie für den Auditteamleiter selbst. Eine Unabhängigkeitserklärung für diese Auditoren oder Experten wird nachgereicht, sobald feststeht, dass sie ins Auditteam aufgenommen werden.

Die Entscheidungen werden im Auditbericht dokumentiert und insbesondere bei negativer Entscheidung an die Zertifizierungsstelle kommuniziert.

5.2 Erstellung eines Prüfplans

Zur Vorbereitung der Vor-Ort-Prüfung muss der Auditteamleiter einen Prüfplan erstellen, d.h. er muss sich aus den Ergebnissen der Dokumentenprüfung die erforderlichen Interviewpartner (Kapitel 4.5.2) heraussuchen, die Stichproben für die Umsetzungsüberprüfung des Basis-Sicherheitschecks (Kapitel 5.3) bestimmen und sich ggf. Fragen bezüglich der einzelnen Maßnahmen zusammenstellen.

Bei der Erstellung der Prüfplanes muss der Auditteamleiter auch die Planung der Überwachungsaudits mit einbeziehen. Diese werden in den Prüfplan mit aufgenommen und enthalten das Datum der Überwachungsaudits (Kalenderwoche, Monat) sowie die Standorte, die jeweils auditiert werden. Während der dreijährigen Zertifikatsdauer müssen alle Standorte auditiert werden. Spätere Änderungen des Prüfplans müssen der Zertifizierungsstelle mitgeteilt werden.

5.3 Vorbereitung der Arbeitsdokumente

Naturgemäß sind die in den IT-Grundschutz-Katalogen enthaltenen Maßnahmentexte in Bezug auf die Formulierung der Anforderungen nicht vollständig homogen. Um möglichst weitgehende Vergleichbarkeit und Reproduzierbarkeit zu erreichen, sollten bei der Interpretation der Texte folgende Hinweise berücksichtigt werden:

- Formulierungen der Art „Es muss getan werden.“, „Es sollte getan werden.“ oder „Es ist zu tun.“ sind als verbindliche Anforderungen zu verstehen, wenn sie durch den Text nicht explizit eingeschränkt werden.

- Formulierungen der Art „Es kann getan werden." oder „Es sollte überlegt werden, etwas zu tun." sind als optionale Aktionen zu verstehen, die die Informationssicherheit zusätzlich erhöhen.
- Wenn im Maßnahmentext auf andere Maßnahmen der IT-Grundschutz-Bausteine verwiesen wird, so führt dies nicht automatisch dazu, dass auch diese Maßnahmen umgesetzt werden müssen. Im Rahmen der IT-Grundschutz-Zertifizierung sind lediglich die Maßnahmen relevant, die im jeweiligen Baustein genannt sind.
- Falls in ergänzenden Kontrollfragen Informationssicherheitsaspekte angesprochen werden, die im vorhergehenden Maßnahmentext nicht behandelt sind, so ist durch den Auditor zu prüfen, ob diese Sicherheitsaspekte für das betrachtete Zielobjekt angemessen berücksichtigt worden sind.
- Bestimmte Maßnahmen der IT-Grundschutz-Bausteine dienen lediglich dazu, Grundlagenwissen über eine bestimmte Technologie oder ein Produkt zu vermitteln. Diese Maßnahmen enthalten wenige oder gar keine Handlungsanweisungen. Demzufolge entfällt bei diesen Maßnahmen auch weitgehend die Prüfung durch den Auditor.
- Bestimmte Maßnahmen der IT-Grundschutz-Bausteine betreffen hauptsächlich die Planungsphase eines Projekts oder die Auswahl eines bestimmten Produkts. Eine solche Maßnahme lässt sich in der Regel nur eingeschränkt auf ein Zielobjekt anwenden, das sich bereits in der Produktions- bzw. Betriebsphase befindet. Die Überprüfung durch den Auditor beschränkt sich hier auf die Aspekte, die offensichtliche und unmittelbare Konsequenzen für den laufenden Betrieb haben.

5.4 Auswahl der Prüfbausteine

Bei der Vor-Ort-Prüfung muss sich der Auditor 10 Bausteinzuordnungen und Maßnahmen aus der ergänzenden Sicherheits- bzw. Risikoanalyse auswählen. Diese Stichproben sind folgendermaßen zu bestimmen:

5.4.1 Informationssicherheitsmanagement

Ziel: Da von der Wirksamkeit des Informationssicherheitsmanagements die Qualität des gesamten Sicherheitsprozesses abhängt, ist die Prüfung des Bausteins B 1.0 IT-Sicherheitsmanagement (mit der Überprüfung des IT-Sicherheitskonzeptes des IT-Verbundes nach dem BSI-Standard 100-2 in der Maßnahme M 2.195 Erstellung eines IT-Sicherheitskonzepts) vorrangig und zwingend erforderlich. Der Auditor überprüft vor Ort die Umsetzung aller Maßnahmen des Bausteins B 1.0 IT-Sicherheitsmanagement für den IT-Verbund.

Hinweis: Die Überprüfung der Wirksamkeit des Informationssicherheitsmanagements und die Vorgehensweise nach Standard 100-2 ist nicht auf die Überprüfung dieses Bausteins beschränkt, sondern wird während des gesamten Audits und in jeder Maßnahme geprüft.

Aktion: Der Auditor legt die Überprüfung des Bausteins B 1.0 IT-Sicherheitsmanagement bei jedem Audit fest.

5.4.2 Zufällig ausgewählte Bausteine

Ziel: Um für die Auswahl der Baustein-Stichproben möglichst effektive Vorgaben zu treffen, ist eine zufällige Gleichverteilung über alle Schichten vorgesehen.
Zusätzlich zur Überprüfung des Management-Bausteins sind zufällige Stichproben aus den fünf Schichten

- Übergeordnete Aspekte,
- Infrastruktur,
- IT-Systeme,
- Netze und

- Anwendungen

zu wählen.

Dabei ist pro Schicht jeweils eine Bausteinzuordnung zufällig zu wählen. (Die erste Ziffer der Nummer eines Bausteins gibt die Schicht an, zu der jeweilige Baustein gehört. Baustein B 3.104 gehört beispielsweise zur Schicht 3 „IT-Systeme“.)

Je nach IT-Verbund kann es vorkommen, dass einzelne Schichten in der Modellierung keine Bausteinzuordnungen enthalten, insbesondere die Schichten „Netze“ und „Anwendungen“. In diesem Fall wählt der Auditor weitere Bausteinzuordnungen nach eigenem Ermessen (siehe 5.3.3) aus, bis insgesamt zehn Bausteinzuordnungen vorliegen.

Aktion: Der Auditor dokumentiert die Stichprobenauswahl und beschreibt, welche Methode er für die zufällige Auswahl der Stichprobe angewendet hat. Beispiele hierfür sind Zufallszahlen-Programm, Losung der Elemente einer Gruppe usw.

5.4.3 Gezielt ausgewählte Bausteine

Ziel: Damit der Auditor die Möglichkeit hat, Schwerpunkte bei der Auditierung der einzelnen Komponenten des IT-Verbundes festzulegen, bestimmt der Auditor weitere vier sicherheitsrelevante Bausteinzuordnungen nach eigenem Ermessen. Enthält die Modellierung des betrachteten IT-Verbunds weniger als zehn Bausteinzuordnungen, so werden alle Bausteinzuordnungen überprüft.

Aktion: Der Auditor dokumentiert die Stichproben-Auswahl und begründet sie nachvollziehbar. Bei einem Re-Zertifizierungsaudit werden normalerweise nicht die gleichen Bausteine ausgewählt wie im Erstzertifizierungsaudit; es kann aber auch Gründe geben, den gleichen Baustein oder sogar die gleiche Bausteinzuordnung noch einmal zu prüfen. Im Auditbericht wird bei einer Re-Zertifizierung dargelegt, inwiefern die gleichen Bausteine/Bausteinzuordnungen geprüft / nicht geprüft wurden sowie die Gründe hierfür.

5.4.4 Stichproben aus der ergänzenden Sicherheits- bzw. Risikoanalyse

Ziel: Aus der Menge der zusätzlichen Sicherheitsmaßnahmen, die im Rahmen der ergänzenden Sicherheits- bzw. Risikoanalyse festgelegt wurden, wählt der Auditor nach eigenem Ermessen eine Stichprobe für verschiedene Komponenten aus. Er begründet die Wahl dieser Stichprobe im Auditbericht.

Aktion: Der Auditor dokumentiert die Stichproben-Auswahl und begründet sie nachvollziehbar.

6. Phase 2 des Zertifizierungsaudits: Inspektion vor Ort

6.1 Überblick über die Auditaktivitäten vor Ort

Bei der Vor-Ort-Inspektion überprüft der Auditor, ob der dokumentierte Umsetzungsstatus mit der Realität übereinstimmt. Um den Aufwand angemessen zu halten, werden zufällige Stichproben genommen.

Die einzelnen Prüfungen sollen direkt am Zielobjekt erfolgen, nicht nur anhand der Papierlage. Bei technischen Aspekten bedeutet dies eine Demonstration durch den jeweils zuständigen Administrator oder dessen Vertreter.

6.2 Wirksamkeit des Managementsystems für Informationssicherheit

Ziel: Es ist wichtig, dass das Managementsystem für Informationssicherheit des IT-Verbundes wirksam und effektiv ist, gelebt und weiterentwickelt wird. Dazu gehört auch, dass alle wichtigen Prozesse des IT-Verbundes dokumentiert sind und nach den Prozessen verfahren wird. Existieren festgeschriebene Leitlinien, allen voran die Sicherheitsleitlinie, und werden sie gelebt? Werden die Ziele der Leitlinien erreicht? Wird im IT-Verbund nach den Standards ISO 27001 und 100-2 vorgegangen, wird insbesondere der PDCA-Zyklus gelebt und das System kontinuierlich weiterverbessert?

Aktion: Der Auditor prüft die Sicherheitsleitlinie und andere Dokumente und führt intensive Gespräche mit dem Antragsteller, um sich von Effektivität und Effizienz des Managementsystems zu überzeugen.

Hinweis: Dieser Prüfpunkt kann nicht innerhalb eines kurzen Gespräches abgehandelt werden, sondern wird während des ganzen Audits immer wieder überprüft.

Votum: Hat der Auditor den Eindruck gewonnen, dass das Informationssicherheits-Managementsystem des IT-Verbundes wirksam und effizient ist und die Ziele der Leitlinien erreicht werden?

6.3 Verifikation des Netzplans

6.3.1 Übereinstimmung des Netzplans mit der Realität

Ziel: Es muss sichergestellt sein, dass die im bereinigten Netzplan dargestellten Komponenten und deren Kommunikationsverbindungen der tatsächlichen Netzstruktur entsprechen und dass der bereinigte Netzplan auf dem aktuellen Stand ist.

Aktion: Der Auditor wählt hierzu verschiedene Komponenten und Kommunikationsverbindungen aus dem bereinigten Netzplan als Stichproben aus und überprüft, ob sie sich in der gleichen Struktur im real existierenden Netz wiederfinden. Es müssen mindestens 5 Stichproben geprüft werden, und die Auswahl der Art der Stichproben (z.B. Server, Clients, sonstige IT-Geräte, Kommunikationsverbindungen) soll dem IT-Verbund entsprechen.

Besonderes Augenmerk ist auf die Dokumentation der existierenden Außenverbindungen im bereinigten Netzplan zu legen. Stimmt die Institution dem zu, kann der Auditor auch auf geeignete Hilfsprogramme zurückgreifen, beispielsweise um sich die Netztopologie anzeigen zu lassen.

Der Auditor dokumentiert die ausgewählten Stichproben, die Ergebnisse der Einzelprüfungen und ggf. Diskrepanzen. Als Diskrepanzen in diesem Zusammenhang sind

Komponenten oder Kommunikationsverbindungen zu werten, die im bereinigten Netzplan aufgeführt sind, sich aber nicht im realen Netz wiederfinden.

Votum: Entsprechen die im bereinigtem Netzplan dargestellten Komponenten und deren Kommunikationsverbindungen der tatsächlichen Netzstruktur?

6.3.2 Übereinstimmung der Realität mit dem Netzplan

Ziel: Es muss sichergestellt sein, dass die im bereinigten Netzplan dargestellten Komponenten und deren Kommunikationsverbindungen der tatsächlichen Netzstruktur entsprechen und dass der bereinigte Netzplan auf dem aktuellen Stand ist.

Aktion: Der Auditor wählt stichprobenartig reale Komponenten und Kommunikationsverbindungen aus den beteiligten Teilnetzen aus und prüft, ob sie dem betrachteten IT-Verbund zuzurechnen sind und ob sie sich im bereinigten Netzplan wiederfinden. Es müssen mindestens 5 Stichproben geprüft werden, und die Auswahl der Art der Stichproben (z.B. Server, Clients, sonstige IT-Geräte, Kommunikationsverbindungen) soll dem IT-Verbund entsprechen.

Besonderes Augenmerk ist auf die Dokumentation der existierenden Außenverbindungen im bereinigten Netzplan zu legen. Stimmt die Institution dem zu, kann der Auditor auch auf geeignete Hilfsprogramme zurückgreifen, beispielsweise um sich die Netztopologie anzeigen zu lassen.
Der Auditor dokumentiert die ausgewählten Stichproben, die Ergebnisse der Einzelprüfungen und ggf. Diskrepanzen. Als Diskrepanzen in diesem Zusammenhang sind Komponenten oder Kommunikationsverbindungen zu werten, die im realen Netz vorhanden sowie dem betrachteten IT-Verbund zuzurechnen sind, sich aber nicht im bereinigten Netzplan wiederfinden.

Votum: Entsprechen die in der Realität vorhandenen Komponenten und deren Kommunikationsverbindungen der Darstellung im bereinigtem Netzplan und ist der bereinigte Netzplan auf dem aktuellen Stand?

6.4 Verifikation der Liste der IT-Systeme

Ziel: Es muss sichergestellt sein, dass die in der Strukturanalyse (A.1) aufgeführten Eigenschaften der IT-Systeme mit den tatsächlichen Gegebenheiten, wie beispielsweise dem jeweils verwendeten Betriebssystem und dem Aufstellungsort, übereinstimmen.

Aktion: Der Auditor wählt hierzu aus der Liste der IT-Systeme zehn Stichproben aus und überzeugt sich jeweils am Gerät davon, dass die in der Liste der IT-Systeme aufgeführten Eigenschaften mit den tatsächlichen Eigenschaften übereinstimmen. (Enthält der IT-Verbund weniger als zehn IT-Systeme, werden die Eigenschaften aller IT-Systeme geprüft.) Die ausgewählten Stichproben, die Ergebnisse der Einzelprüfungen und etwaige Diskrepanzen werden im Auditbericht festgehalten.

Votum: Entsprechen die in der Liste der IT-Systeme aufgeführten Eigenschaften den tatsächlichen Eigenschaften der realen IT-Systeme?

6.5 Verifikation des Basis-Sicherheitschecks

Ziel: Beim Basis-Sicherheitscheck wird jeder Maßnahme, die in den für die Modellierung herangezogenen Bausteinen enthalten ist, für das jeweilige Zielobjekt der Umsetzungsstatus („entbehrlich“, „ja“, „teilweise“ oder „nein“) zugeordnet. Die Ergebnisse liegen als Basis-Sicherheitscheck (A.4) vor. Es muss sichergestellt sein, dass die hier dokumentierten

Ergebnisse mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts übereinstimmen.

Aktion: Bei der Modellierung werden die Bausteine der IT-Grundschutz-Kataloge den entsprechenden Zielobjekten innerhalb des betrachteten IT-Verbunds zugeordnet. (Ein Beispiel für eine Bausteinzuordnung ist die Anwendung des Bausteins B 3.101 auf den Server S5.)

Für jede ausgewählte Bausteinzuordnung (vergleiche Kapitel 5.4) überprüft der Auditor durch Inspektion des jeweiligen Zielobjekts, ob der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der in diesen Bausteinen enthaltenen Maßnahmen den tatsächlichen Gegebenheiten entspricht.

- Ist für eine Maßnahme der Umsetzungsstatus „entbehrlich“ aufgeführt, so überprüft der Auditor, ob die jeweils genannte Begründung zutreffend ist, d. h. ob die entsprechende Funktionalität tatsächlich nicht genutzt wird bzw. ob die genannte Ersatzmaßnahme tatsächlich in Kraft ist.
- Ist für eine Maßnahme der Umsetzungsstatus „ja“ aufgeführt, so überprüft der Auditor anhand des jeweiligen Zielobjekts, ob alle im Maßnahmentext genannten Forderungen sinngemäß erfüllt sind. Hinweis: es genügt *nicht*, nur die Kontrollfragen abzuprüfen.
- Ist für eine umzusetzende Maßnahme (dies sind z.B. für ein Zertfizierungsaudit Maßnahmen der Stufe A, B oder C) der Umsetzungsstatus „teilweise“ oder „nein“ aufgeführt, so wird keine Überprüfung durchgeführt und es wird eine Nachbesserung (Kapitel 7) angestoßen.

Die ausgewählten Bausteinzuordnungen und das Ergebnis der einzelnen Überprüfungen sind zu dokumentieren, insbesondere etwaige Abweichungen von dem im Basis-Sicherheitscheck aufgeführten Umsetzungsstatus und Diskrepanzen beim Umsetzungsstatus „entbehrlich“. Die Überprüfung der Maßnahmen umfasst nicht nur die Kontrollfragen, sondern die Umsetzung der Maßnahme ihrem Sinn und Zweck nach. Aufgrund der Vielfalt der unterschiedlichen Einsatzszenarien und Realisierungsmöglichkeiten ist es nicht immer sinnvoll, die Maßnahmen der IT-Grundschutz-Kataloge wörtlich und ohne Anpassung an das Einsatzumfeld umzusetzen. In diesen Fällen hat der Auditor zu prüfen und zu dokumentieren, ob die Umsetzung sinngemäß erfolgt ist. Die Vorgehensweise muss nachvollziehbar dokumentiert werden.

Hinweis: Zu jedem ausgewählten Baustein sollte auf der Maßnahmenebene im Auditbericht kurz erläutert werden, was genau geprüft wurde, wer jeweils wofür befragt wurde und welche Ergebnisse zu vermerken sind (Begründung).
Für die Maßnahme „M 2.192 Erstellung einer IT-Sicherheitsleitlinie“ des Bausteins „B 1.0 IT-Sicherheitsmanagement“ kann auf Prüfpunkt 4.4.3 Nachvollziehbarkeit der IT-Sicherheitsrichtlinien verwiesen werden.

Votum: Stimmt der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der Maßnahmen mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts überein? Ist die Begründung der „entbehrlichen“ Maßnahmen zulässig und nachvollziehbar?

6.6 Verifikation der Umsetzung der zusätzlichen Maßnahmen aus der ergänzenden Risikoanalyse

Ziel: Als Ergebnis der ergänzenden Risikoanalyse (A.6) sind für Komponenten mit hohem oder sehr hohem Schutzbedarf zusätzliche höherwertige Maßnahmen herangezogen worden. Der Umsetzungsstatus der jeweiligen Zielobjekte ist mit („entbehrlich“, „ja“, „teilweise“ oder „nein“) angegeben. Es muss sichergestellt sein, dass die hier dokumentierten Ergebnisse mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts übereinstimmen

Aktion: Für jede der ausgewählten zusätzlichen Maßnahmen (vergleiche Kapitel 5.4) überprüft der Auditor durch Inspektion des jeweiligen Zielobjekts, ob der festgestellte Umsetzungsstatus der Maßnahmen den tatsächlichen Gegebenheiten entspricht.

- Ist für eine Maßnahme der Umsetzungsstatus „entbehrlich“ aufgeführt, so überprüft der Auditor, ob die jeweils genannte Begründung zutreffend ist, d. h. ob die entsprechende Funktionalität tatsächlich nicht genutzt wird bzw. ob die genannte Ersatzmaßnahme tatsächlich in Kraft ist.
- Ist für eine Maßnahme der Umsetzungsstatus „ja“ aufgeführt, so überprüft der Auditor anhand des jeweiligen Zielobjekts, ob die Maßnahme so wie sie festgelegt wurde, sinnvoll umgesetzt ist, so dass sie den identifizierten Gefährdungen entgegen wirken kann.
- Ist für eine Maßnahme der Umsetzungsstatus „teilweise“ oder „nein“ aufgeführt, so wird keine Überprüfung durchgeführt und es wird eine Nachbesserung (Kapitel 7) angestoßen.

Die ausgewählten zusätzlichen Maßnahmen und das Ergebnis der einzelnen Überprüfungen sind zu dokumentieren. In diesen Fällen hat der Auditor zu prüfen und zu dokumentieren, ob die Umsetzung wirksam ist .d.h. den zusätzlich identifizierten Gefährdungen tatsächlich ausreichend entgegen wirkt. Die Vorgehensweise muss nachvollziehbar dokumentiert werden.

Votum: Sind alle ergänzenden Sicherheitsmaßnahmen aus der Risikoanalyse umgesetzt? Stimmt der festgestellte Umsetzungsstatus der zusätzlichen Maßnahmen mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts überein?

7. Nachbesserungen und Nachforderungen

7.1 Nachbesserungen

Ziel: Sowohl bei der ersten Sichtung der Referenzdokumente als auch bei der Inspektion vor Ort werden sich in manchen Fällen Abweichungen ergeben. Diese müssen sachgerecht behoben werden.
Dabei gibt es verschiedene Stufen der Behandlung von Abweichungen:
1. Schwerwiegende Abweichungen sind Mängel, ohne deren Behebung nicht sichergestellt werden kann, dass das Informationssicherheits-Managementsystem effektiv und effizient funktioniert. Daher müssen diese Abweichungen vor Ausstellung des Zertifikates behoben werden.
2. Geringfügige Abweichungen sind zu kennzeichnen und mit einer Frist zur Behebung zu versehen. Eine Ausstellung des Zertifikates kann unter Umständen trotzdem erfolgen. Mehrere geringfügige Abweichungen können zusammen eine schwerwiegende Abweichung darstellen.
3. Der Auditor hat die Möglichkeit, Empfehlungen an die Institution auszusprechen. Diese sind nicht bindend, erhöhen aber die Effektivität und Effizienz des Informationssicherheits-Managementsystems.

Aktion: Der Auditor entscheidet bei Abweichungen, ob es sich um schwerwiegende oder geringe Abweichungen handelt. Dazu kann er sich im Zweifelsfall mit der Zertifizierungsstelle absprechen.
Er informiert die Institution möglichst frühzeitig schriftlich über festgestellte Abweichungen, damit diese zeitnah behoben werden können. Er muss der Institution hierzu eine angemessene Frist einräumen. Die Abweichungsliste und die Nachbesserungsfrist für die Korrekturmaßnahmen sowie die Empfehlungen werden im Auditbericht dokumentiert.

Je nach Art der festgestellten Abweichungen werden die nachgebesserten Dokumente fristgerecht dem Auditor zur Verfügung gestellt bzw. rechtzeitig mit dem Auditor ein Termin zur Begutachtung der Korrekturmaßnahmen vereinbart. Der Auditor prüft anhand der Dokumente oder vor Ort, ob alle festgestellten schwerwiegenden Abweichungen behoben wurden, und dokumentiert die Prüfungsergebnisse im Auditbericht. Dabei werden in Kapitel 5 des Auditberichts die inzwischen behobenen Abweichungen aufgeführt; in den Kapiteln 2 bis 4 dagegen wird die Situation nach Behebung der Abweichungen dargestellt.
Geringfügige Abweichungen werden ebenfalls mit einer Nachbesserungsfrist versehen, deren Behebung kann auch erst beim nächsten Überwachungs- oder Re-Zertifizierungsaudit begutachtet werden.

Votum: Wurden bei der Nachbesserung alle festgestellten schwerwiegenden Abweichungen behoben und haben sich keine neuen Abweichungen ergeben?

Hinweis: Falls sich auch nach der Nachbesserung noch größere Abweichungen ergeben, ist keine weitere Nachbesserung durch den Antragsteller mehr möglich. Dies gilt unabhängig sowohl für den Teil des Auditberichts zu Phase 1 als auch für den Teil des Auditberichts zu Phase 2. Treten also bei Dokumentenprüfungen größere Abweichungen auf und werden nach Mitteilung an die auditierte Institution behoben, so dürfen während des Vor-Ort-Audits trotzdem größere Abweichungen auftreten. Diese dürfen sich dann allerdings nicht mehr auf die Dokumentenprüfung beziehen.

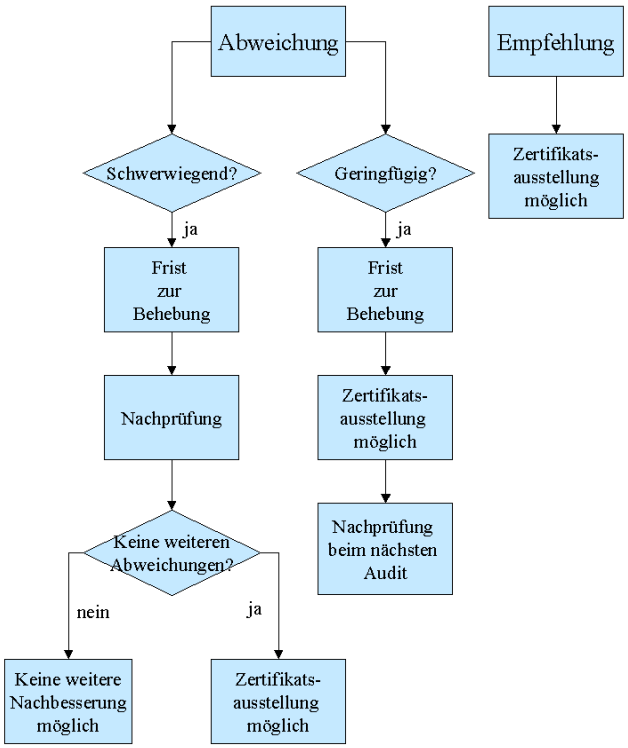

Abbildung 4: Abweichungen und Empfehlungen

7.2 Nachforderungen

Ziel: Die Zertifizierungsstelle wird den Auditteamleiter kurzfristig über einen Termin für die Bearbeitung des Auditberichts informieren. Inhaltliche, formale oder sonstige Nachforderungen zum Auditbericht werden dem Auditteamleiter bis zu diesem Termin mitgeteilt. Der Auditor muss innerhalb eines Monats diese Nachforderungen beheben. Hier kann es in Einzelfällen auch dazu kommen, dass der Auditor eine Nachbesserung gegenüber dem Antragsteller fordert, zum Beispiel falls die Stichprobenauswahl der zu überprüfenden Bausteine nicht nachvollziehbar war.

Aktion: Der Auditteamleiter konkretisiert den Auditbericht und sendet diesen an die Institution und die Zertifizierungsstelle zur erneuten Prüfung.

Hinweis: Falls sich nach der ersten Nachforderung der Zertifizierungsstelle an den Auditteamleiter noch weitere Defizite ergeben, sind zusätzliche Nachforderungen der Zertifizierungsstelle des BSI an den Auditbericht möglich. Dies darf nicht zu weiteren Nachbesserungen des Antragstellers führen.

Kommt es aufgrund der Nachforderungen der Zertifizierungsstelle zu Nachforderungen gegenüber dem Antragsteller, ist diese als zusätzliche Nachbesserung zu dokumentieren. Falls auch nach der zweiten Nachbesserung noch Defizite bestehen, muss die Auditierung vollständig wiederholt werden. Eine dritte Nachbesserung ist somit ausgeschlossen.
Hat die Institution bezüglich festgestellter Abweichungen eine andere Auffassung als der Auditor, kann sie sich schriftlich zu der vom Auditor dokumentierten Abweichungen äußern. Der Kommentar wird in die Liste der Abweichungen im Auditbericht übernommen. Der Zertifizierungsstelle obliegt dann die Entscheidung, ob die Abweichung behoben werden muss und innerhalb welcher Frist dies zu geschehen hat.

8. Gesamtvotum für die Erteilung eines Zertifikats

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

Aktion: Der Auditteamleiter stellt in kurzer Form seine Gesamteinschätzung dar, die auf den Ergebnissen der in den Kapiteln 4 bis 7 dieses Dokuments beschriebenen Prüfschritten beruht. Umstände oder Auditierungsergebnisse, die die Zertifikatsvergabe besonders positiv oder negativ beeinflussen, können an dieser Stelle noch einmal herausgestellt werden. Das nachfolgende Gesamtvotum kann in der Regel nur dann positiv ausfallen, wenn die Ergebnisse aller oben beschriebenen Prüfschritte positiv sind. Der Text des Gesamtvotums muss eine eindeutige Aussage der folgenden Art umfassen:

„Aufgrund der durchgeführten Einzelprüfungen im Rahmen des ISO 27001-Audits auf der Basis von IT-Grundschutz wird festgestellt, dass der Untersuchungsgegenstand die Anforderungen an ein ISO 27001-Zertifikats auf der Basis von IT-Grundschutz erfüllt / nicht erfüllt."

Falls die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz befürwortet wird, obwohl das Votum für einzelne Prüfschritte negativ ausfällt, ist dies ausführlich zu begründen.

Votum: Erfüllt der betrachtete Untersuchungsgegenstand die Anforderungen des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz bzw. des angestrebten Auditortestats?

Hinweis: Das Gesamtvotum ist vom Auditteamleiter mit Datum zu unterschreiben.

9. Überwachungsaudit

Während der dreijährigen Gültigkeit eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz werden von einem Auditor jährliche Überwachungsaudits des zertifizierten Untersuchungsgegenstandes durchgeführt.

9.1 Planung der Überwachungsaudits

Die organisatorische Planung der jährlichen Überwachungsaudits, die für die Überwachung eines für einen IT-Verbund erteilten Zertifikats durchzuführen sind, ist Gegenstand der zeitlichen Auditplanung, die im Rahmen des Erst- bzw. Re-Zertifizierungsverfahrens ausgearbeitet wurde. Der Auditplan ist Bestandteil des Auditberichtes des Zertifizierungsverfahrens.

Abweichungen vom bzw. Änderungen bzgl. der Planung der Überwachungsaudits sind der Zertifizierungsstelle rechtzeitig anzuzeigen. Insbesondere betrifft dies den Wechsel des Auditors sowie Verschiebungen von Ortsterminen und Fertigstellungs- und Lieferterminen von Auditdokumenten.

Der Auditbericht zum Überwachungsaudit muss der Zertifizierungsstelle mehr als ein Jahr bzw. zwei Jahre vor Ablauf des Zertifikats vorliegen. Die Planung der Überwachungsaudits durch den Auditteamleiter in Zusammenarbeit mit der antragstellenden Institution muss so erfolgen, dass die Durchführung der Überwachungsaudits sowie die fristgerechte Übergabe der Auditberichte möglich ist. Insbesondere ist genügend Raum für die Beseitigung von im Überwachungsaudit festgestellten Abweichungen sowie für die Erstellung der Auditberichte einzuplanen. Liegt der Auditbericht eines Überwachungsaudits der Zertifizierungsstelle nicht rechtzeitig vor, hat diese die Möglichkeit, das erteilte Zertifikat auszusetzen oder gar zurückzuziehen (siehe Kap. 3.10).

Während der Gültigkeit des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz sind alle Standorte im Anwendungsbereich des Managementsystems für Informationssicherheit des zertifizierten Untersuchungsgegenstandes zu auditieren.

9.2 Phase 1 des Überwachungsaudits: Sichtung der Referenzdokumente

Die für die Zertifizierung des IT-Verbundes von der Institution vorgelegten und vom Auditor geprüften Referenzdokumente werden von der Institution, falls erforderlich, aktualisiert und den Änderungen am IT-Verbund entsprechend angepasst. Sämtliche wichtigen Änderungen, Ergänzungen und Streichungen in den Referenzdokumenten müssen für den Auditor erkennbar sein.

Die aktualisierten Referenzdokumente werden dem Auditor von der zertifizierten Institution für das Überwachungsaudit zur Verfügung gestellt und vom Auditor gesichtet und bewertet. Der Auditor verschafft sich einen Überblick über die Änderungen im Untersuchungsgegenstand im Vergleich zum vorher geprüften Dokumentenstand.

Der Auditor prüft auf Basis der eingereichten Referenzdokumente, ob zwischenzeitlich durch den Antragsteller Änderungen am zertifizierten IT-Verbund vorgenommen wurden und in welchem Umfang sich diese Änderungen bewegen. Für gravierende Änderungen am IT-Verbund (wie z.B. größere Änderungen im Managementsystem, Änderungen in der Organisation, Änderungen im Outsourcing, Standortwechsel, Änderungen von Tätigkeitsfeldern) besteht generell für den Antragsteller eine Anzeigepflicht gegenüber der Zertifizierungsstelle. Stellt der Auditor bei seiner Prüfung gravierende Änderungen am IT-Verbund fest und ist der Antragsteller seiner Anzeigepflicht nicht nachgekommen, informiert der Auditteamleiter die Zertifizierungsstelle hierüber; die Zertifizierungsstelle entscheidet über das weitere Vorgehen und behält sich in diesem Falle vor, das Zertifikat zurückzuziehen. Sind gravierende Änderungen festzustellen, die gegenüber der Zertifizierungsstelle vom Antragsteller angezeigt wurden, entscheidet die Zertifizierungsstelle darüber,

ob eine Fortführung des Zertifikates prinzipiell möglich ist oder aber eine Re-Zertifizierung des IT-Verbundes erforderlich wird.

Falls das Delta im IT-Verbund überschaubar ist und keine Re-Zertifizierung erfordert oder aber bei gravierenden Änderungen im IT-Verbund die Zertifizierungsstelle die Gültigkeit des Zertifikates nicht aufhebt, fährt der Auditor mit dem Überwachungsaudit fort.

Die Referenzdokumente werden vom Auditor auch daraufhin geprüft, ob aus dem vorhergehenden Audit resultierende offene Punkte bzgl. der Dokumentation bei der Aktualisierung der Referenzdokumente eingearbeitet worden sind. Dies betrifft beispielsweise geringfügige Abweichungen, deren Frist zur Behebung seit dem letzten Audit abgelaufen ist.

Alle aus dem Dokumentenreview resultierenden Bewertungen der Referenzdokumente werden in den Auditbericht für das Überwachungsaudit aufgenommen. Hierbei stützt sich der Auditbericht für das Überwachungsaudit auf den Auditbericht der vorhergehenden Auditierung und weist Änderungen, Ergänzungen und Streichungen explizit aus.

9.3 Vorbereitung der Auditaktivität vor Ort

Die inhaltliche Planung eines Überwachungsaudits umfasst die Erstellung eines Prüfplans durch den Auditteamleiter auf Grundlage der Dokumentenpüfung in Phase 1 des Überwachungsaudits und auf Basis des groben Prüfplans aus dem Erstzertifizierungsaudit. Hierzu gehören insbesondere folgende Aktivitäten des Auditors:

- auf Basis des in Phase 1 des Überwachungsaudits identifizierten Deltas im IT-Verbund: Festlegung der im Überwachungsaudit zu prüfenden Teilaspekte
- Zusammenstellung der Liste der Abweichungen aus der vorhergehenden Auditierung, die im letzten Auditbericht dokumentiert ist (falls vorhanden)
- Zusammenstellung der Auflagenliste aus der Zertifizierung bzw. der vorhergehenden Auditierung, die sich im Zertifikat, im Anhang zum Zertifikat oder im letzten Auditbericht finden (falls vorhanden)
- Zusammenstellung der für das Überwachungsaudit erforderlichen Interviewpartner

9.4 Phase 2 des Überwachungsaudits: Inspektion vor Ort

Bei der Vor-Ort-Inspektion im Rahmen eines Überwachungsaudits konzentriert der Auditor seine Auditaktivitäten auf eine Kontrolle, ob im zertifizierten IT-Verbund die nachgewiesene Sicherheitsfunktionalität aktiv und wirksam gelebt wird. Zum einen wird das ISMS der zertifizierten Institution begutachtet, zum anderen wird das Delta im IT-Verbund seit der vorhergehenden Auditierung genauer betrachtet.

Das Überwachungsaudit dient *nicht* einer Wiederholung des Audits aus dem Zertifizierungsverfahren. Insbesondere wird daher nicht ein kompletter Check des realen IT-Verbundes unter dem Aspekt des IT-Grundschutzes wie im Audit des Zertifizierungsverfahrens durchgeführt.

Die einzelnen Prüfungen erfolgen direkt am Zielobjekt, nicht nur anhand der Papierlage. Bei technischen Aspekten bedeutet dies eine Demonstration durch den jeweils zuständigen Administrator oder dessen Vertreter.

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

- Prüfung, ob das Sicherheitsmanagement aktiv und wirksam gelebt wird
- Prüfung der Änderungen am zertifizierten IT-Verbund
- Prüfung der Behebung von Abweichungen, die im vorhergehenden Audit erkannt wurden
- Prüfung der Einhaltung von an das bestehende Zertifikat gekoppelten Auflagen (insbesondere bzgl. von Änderungen am zertifizierten IT-Verbund und bzgl. der Verwendung von

Zertifizierungsbuttons und/oder anderen Verweisen auf die Zertifizierung nach den Vorgaben der Zertifizierungsstelle)

- Prüfung des Beschwerdemanagements

9.4.1 Prüfung des Managementsystems für Informationssicherheit

Ziel: Da von der Wirksamkeit des Managementsystems für Informationssicherheit die Qualität des gesamten IT-Sicherheitsprozesses abhängt, werden bei einem Überwachungsaudit verschiedene Aussagen geprüft:

- Die von der zertifizierten Institution definierte Sicherheitsleitlinie wird aktiv gelebt und im zertifizierten IT-Verbund gemäß der abgeleiteten Sicherheitsstrategie umgesetzt.
- Die von der zertifizierten Institution definierten Managementprozesse sind wirksam und erreichen die für den IT-Verbund gesteckten Ziele.
- Die zertifizierte Institution strebt danach, das für die Institution aufgesetzte ISMS aktiv zu leben und ständig zu verbessern.
- Durch die zertifizierte Institution werden im laufenden Betrieb interne Audits und Managementbewertungen durchgeführt, und dies erfolgt auf angemessene und effektive Art und Weise.
- Beschwerden an die Institution, die im Zusammenhang mit dem Informationssicherheitsmanagement stehen, müssen angemessen behandelt werden.

Aktion: Der Auditor setzt die Schwerpunkte der Überprüfung auf die oben genannten Prüfaspekte.

Votum: Wird das Informationssicherheitsmanagements aktiv gelebt und verbessert und erfüllt es die für den IT-Verbund gesteckten Ziele?

9.4.2 Prüfung von Änderungen am IT-Verbund

Ziel: Der zertifizierte IT-Verbund wird überprüft, um sicherzustellen,

- dass die seit der Zertifizierung unveränderten Komponenten des IT-Verbunds weiterhin die Anforderungen an ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz erfüllen,
- dass durch den Wegfall von Komponenten seit der Zertifizierung die Informationssicherheit des IT-Verbunds nicht beeinträchtigt wird,
- dass alle seit der Zertifizierung neu hinzugekommenen Komponenten im IT-Verbund die Anforderungen an ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz prinzipiell erfüllen und
- dass die Informationssicherheit des IT-Verbunds durch Veränderungen in übergeordneten Aspekten, beispielsweise Änderungen der Organisationsstruktur und insbesondere des ISMS, seit der vorhergehenden Zertifizierung nicht beeinträchtigt wird.

Aktion: Der Auditor beschränkt sich im Überwachungsaudit auf die Überprüfung der Änderungen im IT-Verbund seit dem vorhergehenden Audit. Besonderes Augenmerk wird dabei darauf gelegt, Seiteneffekte durch Änderungen im IT-Verbund zu erkennen und zu begutachten. Sich durch die Änderungen am IT-Verbund ergebende Abweichungen und / oder Auflagen sind im Auditbericht festzuhalten.

Votum: Wird trotz Änderungen im IT-Verbund die Informationssicherheit weiter gewährleistet?

Hinweis: Das Überwachungsaudit dient *nicht* einer Wiederholung des Audits aus dem Zertifizierungsverfahren. Insbesondere wird daher nicht ein kompletter Check des realen IT-Verbundes unter dem Aspekt des IT-Grundschutzes wie im Audit des Zertifizierungsverfahrens durchgeführt. Auch müssen neu hinzugekommene Komponenten / Bausteine bzw. Änderungen am IT-Verbund nicht komplett geprüft werden. Der Auditor

muss aber überprüfen, ob insbesondere neuartige Komponenten oder Schlüsselkomponenten die Sicherheit des geprüften IT-Verbundes nicht gefährden.
Gravierende Änderungen am zertifizierten IT-Verbund (z.B. Umstrukturierungen oder Wechsel von Dienstleistern) können zu einer Re-Zertifizierung führen.

9.4.3 Prüfung der zwischenzeitlichen Behebung von Abweichungen

Ziel: Im Rahmen des vorhergehenden Audits erkannte und im zugehörigen Auditbericht vermerkte Abweichungen im realen IT-Verbund sind von der zertifizierten Institution zu beheben.

Aktion: Der Auditor überprüft, ob sämtliche im vorhergehenden Audit erkannten und im zugehörigen Auditbericht vermerkten Abweichungen in der gesetzten Frist angemessen und wirksam behoben wurden und die zugehörige Dokumentation sofern erforderlich entsprechend aktualisiert wurde. Die Überprüfung beinhaltet insbesondere die Begutachtung, ob die Behebung der Abweichungen in einer Art und Weise durchgeführt wurde, dass der gesamte IT-Verbund und seine Sicherheitsstruktur konsistent bleibt, und inwieweit die Beseitigung von Abweichungen zu neuen Abweichungen geführt hat. Aus der Behebung alter Abweichungen resultierende neue Abweichungen oder neue Auflagen sind im Auditbericht zu dokumentieren.

Votum: Sind sämtliche im vorhergehenden Audit erkannten und im zugehörigen Auditbericht vermerkten Abweichungen im realen IT-Verbund angemessen und wirksam behoben? Wurde, falls erforderlich, eine entsprechende Überarbeitung der Referenzdokumente durchgeführt?

Hinweis: Bei Nichtbehebung dokumentierter Abweichungen oder Schaffung neuer gravierender Abweichungen im Rahmen der Beseitigung alter Abweichungen behält sich die Zertifizierungsstelle das Recht vor, das bestehende Zertifikat auszusetzen oder ggf. zu entziehen (siehe Kap. 3.10).

9.4.4 Prüfung der Einhaltung von Auflagen

Ziel: Die im Rahmen der Zertifizierung sowie der vorhergehenden Audits an den zertifizierten IT-Verbund gestellten Auflagen sind einzuhalten, um den Anforderungen an ein gültiges Zertifikat gerecht zu werden.

Aktion: Der Auditor überprüft, ob die im Rahmen der Zertifizierung sowie der vorhergehenden Audits an den zertifizierten IT-Verbund gestellten Auflagen von der zertifizierten Institution angemessen und wirksam eingehalten wurden bzw. werden. Diese Auflagen können z.B. im Zertifizierungsreport spezifiziert worden sein, im Zertifizierungsbescheid dem Antragsteller mitgeteilt worden sein oder in Formularen (z.B. Verwendungsbedingungen des Zertifizierungsbuttons) vom Antragsteller unterzeichnet worden.
Die Überprüfung betrifft insbesondere die folgenden Punkte:

- Der Auditor überprüft, ob zwischenzeitlich gravierende Änderungen am zertifizierten IT-Verbund (wie z.B. größere Änderungen im Managementsystem, Änderungen in der Organisation, Änderungen im Outsourcing, Standortwechsel, Änderungen von Tätigkeitsfeldern) ohne Information an die Zertifizierungsstelle vorgenommen wurden. Bei gravierenden Änderungen am zertifizierten IT-Verbund besteht für den Antragsteller die Auflage, diesbzgl. Rücksprache mit der Zertifizierungsstelle zu nehmen. Stellt der Auditor bei seiner Prüfung vor Ort gravierende Änderungen am IT-Verbund fest, die im Rahmen der Dokumentenprüfung noch nicht aufgefallen sind, und ist der Antragsteller seiner Anzeigepflicht nicht nachgekommen, informiert der Auditteamleiter die Zertifizierungsstelle hierüber; die Zertifizierungsstelle entscheidet über das weitere Vorgehen und behält sich in diesem Falle vor, das Zertifikat zurückzuziehen. Sind gravierende Änderungen festzustellen, die gegenüber der Zertifizierungsstelle vom

Antragsteller angezeigt wurden, entscheidet die Zertifizierungsstelle darüber, ob eine Fortführung des Zertifikates prinzipiell möglich ist oder aber eine Re-Zertifizierung des IT-Verbundes erforderlich wird. Falls das Delta im IT-Verbund überschaubar ist und keine Re-Zertifizierung erfordert oder aber bei gravierenden Änderungen im IT-Verbund die Zertifizierungsstelle einen Fortbestand des Zertifikates erlaubt, fährt der Auditor mit dem Überwachungsaudit fort.

- Der Auditor überprüft, ob Zertifizierungsbuttons und/oder andere Verweise auf die Zertifizierung nach den Vorgaben der Zertifizierungsstelle genutzt wurden bzw. werden.

Votum: Wurden bzw. werden sämtliche im Rahmen der Zertifizierung sowie des vorhergehenden Audits an den zertifizierten IT-Verbund gestellten Auflagen von der zertifizierten Institution angemessen und wirksam eingehalten?

Hinweis: Bei Nichteinhaltung von Auflagen aus der Zertifizierung des IT-Verbundes behält sich die Zertifizierungsstelle das Recht vor, das bestehende Zertifikat auszusetzen oder ggf. zu entziehen (siehe Kap. 3.10).

9.5 Gesamtvotum für die Aufrechterhaltung des Zertifikats

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

Aktion: Der Auditteamleiter stellt in kurzer Form seine Gesamteinschätzung dar, die auf den Ergebnissen der für die Überwachungsaudits beschriebenen Prüfschritten beruht. Umstände oder Auditierungsergebnisse, die die Aufrechterhaltung des Zertifikats besonders positiv oder negativ beeinflussen, können an dieser Stelle noch einmal herausgestellt werden. Das nachfolgende Gesamtvotum kann in der Regel nur dann positiv ausfallen, wenn die Ergebnisse aller erforderlichen Prüfschritte positiv sind. Der Text des Gesamtvotums muss eine eindeutige Aussage der folgenden Form umfassen:

„Aufgrund der durchgeführten Prüfungen im Rahmen des Überwachungsaudits wird festgestellt, dass der Untersuchungsgegenstand die Anforderungen an ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz weiterhin erfüllt / nicht erfüllt."

Falls die Erhaltung des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz befürwortet wird, obwohl das Votum für einzelne Prüfschritte negativ ausfällt, ist dies ausführlich zu begründen.

Votum: Erfüllt der betrachtete Untersuchungsgegenstand weiterhin die Anforderungen des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz?

Hinweis: Das Gesamtvotum ist vom Auditteamleiter mit Datum zu unterschreiben.
Sollte der Aufwand eines Überwachungsaudits der zertifizierten Institution nicht angemessen erscheinen, so kann diese um Prüfung des Sachverhalts beim BSI bitten.

10. Auditierung im Rahmen einer Re-Zertifizierung

Ziel: 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 IT-Verbund aufgetreten, muss der IT-Sicherheitsbeauftragte des Antragstellers diese der Zertifizierungsstelle im BSI schriftlich mitteilen. Das BSI entscheidet dann, ob eine vorzeitige Re-Zertifizierung erforderlich ist.

Nach Ablauf des Gültigkeitszeitraums ist immer eine Re-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. Diese Re-Zertifizierung sollte vor Ablauf des Gültigkeitszeitraums erfolgt sein, so dass der Untersuchungsgegenstand durchgehend ein gültiges Zertifikat besitzt.

Bestandteil der Re-Zertifizierung ist eine erneute Auditierung, um sicherzustellen,

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

Aktion: Formal unterscheidet sich eine Auditierung im Rahmen einer Re-Zertifizierung nicht von einer erstmaligen Auditierung. Ein erneutes Voraudit ist allerdings nicht möglich. Der Auditor greift jedoch für das Re-Zertifizierungsaudit soweit wie möglich auf die Ergebnisse der Auditierungen der vorhergehenden Zertifizierung (Audit für das Zertifizierungsverfahren sowie Überwachungsaudits) zurück und konzentriert die Prüfungen auf die Veränderungen innerhalb des IT-Verbundes seit der letzten Zertifizierung und den zugehörigen Auditierungen. Die Institution hebt diese Veränderungen in den Referenzdokumenten, die dem Auditor zur Verfügung gestellt werden, hervor.

Hinsichtlich der Wahl von Stichproben, die bei einzelnen Prüfaspekten des Prüfschemas für ein Re-Zertifizierungsaudit erforderlich sind, sei auf Kap. 3.6 verwiesen.

Votum: Siehe Kapitel 4 bis 8.

11. Praktische Hilfen

11.1 Auditbericht

Der Auditbericht dokumentiert die Grundlagen, die Durchführung und die Ergebnisse der Auditierung. Der Auditbericht ist vom Auditteamleiter zu unterzeichnen.

Auf der Grundlage des Auditberichts wird über die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz entschieden.

Der Auditbericht und die übrigen Auditunterlagen müssen zumindest für die Gültigkeit des Zertifikats aufbewahrt werden. Verantwortlich für die Aufbewahrung ist der Auditteamleiter. Es kann jedoch vereinbart werden, dass die Unterlagen stattdessen bei der auditierten Institution oder beim Arbeitgeber des Auditteamleiters verwahrt werden. Die Auditunterlagen müssen nicht zwingend in Papierform aufbewahrt werden.

11.2 Formale Aspekte des Auditberichts

Prüfgrundlage für den Auditor ist das vorliegende Dokument „Prüfschema für ISO 27001-Audits“ und ergänzende BSI-Interpretationen, die vom BSI auf der Homepage unter http://www.bsi.bund.de/gshb/zert veröffentlicht sind.

Die durchgeführten Prüfungen, Prüfergebnisse und Bewertungen des Auditors müssen im Auditbericht reproduzierbar und nachvollziehbar dokumentiert werden.

11.2.1 Allgemeines

- Das Inhaltsverzeichnis umfasst sowohl den eigentlichen Bericht als auch alle Anhänge. Jeder einzelne Abschnitt eines Anhangs muss identifizierbar sein, so dass die Vollständigkeit des Auditberichtes und der Anhänge überprüft werden kann.
- Alle vom Auditor angeforderten Dokumente, insbesondere die Referenzdokumente A.0 bis A.3 sowie A.5 und A.6 sind Bestandteil des Auditberichts und müssen im Anhang aufgeführt werden. Es ist dem Antragsteller freigestellt, ob er der Zertifizierungsstelle auch das Referenzdokument A.4 zur Verfügung stellt.
- Eventuell vorhandene zusätzliche Aufzeichnungen des Auditors sind der Zertifizierungsstelle zur Verfügung zu stellen, falls im Auditbericht darauf verwiesen wird. Ausnahmen hiervon sind mit der Zertifizierungsstelle abzustimmen.
- Die Seitennummerierung muss so gestaltet werden, das jede Seite eindeutig identifiziert werden kann.
- Falls zur Unterstützung der Prüfaktivitäten Softwarewerkzeuge verwendet werden, z.B. das GSTOOL oder Analyse-Tools, müssen diese Tools identifizierbar mit Namen und Versionsnummer genannt werden. Sofern im Auditbericht auf in diesen Tools erfasste Informationen verwiesen wird, müssen entsprechende Reports (Ausdrucke) als zusätzliche Aufzeichnungen beigefügt werden.
- Verwendete Fachbegriffe oder Abkürzungen, die nicht allgemein gebräuchlich sind, müssen in einem Glossar bzw. Abkürzungsverzeichnis zusammengefasst werden.

11.2.2 Vorgehensweise

Für die Dokumentation der Prüfung und Bewertung sind für alle Einzelanforderungen folgende Teilschritte notwendig:

a) Kurzbeschreibung
Der Aufbau und der Inhalt der Referenzdokumente sind kurz darzulegen. Die Referenzen und Verweise müssen eindeutig sein. Es reicht nicht aus, auf das globale Dokument - zum Beispiel. A.1 - zu verweisen, es sind die konkreten Textpassagen anzugeben bzw. zu referenzieren.

b) Erläuterung der Prüfung/Aktion mit Begründung
Die einzelnen Aktionen des Auditors müssen nachvollziehbar und wiederholbar dokumentiert werden. Der Auditor muss die Vorgehensweise seiner Prüfung erläutern, so dass die Prüfergebnisse reproduzierbar sind. Die Darlegungen müssen verständlich und übersichtlich dargestellt werden.

Beispiele:

- Bei der Durchführung von Stichproben sind Auswahl und Umfang nachvollziehbar und begründet zu erläutern.
- Bei der Auditierung von Maßnahmen, die als „entbehrlich“ gekennzeichnet sind, muss die Plausibilität der Aussage des Antragstellers dargelegt werden.

c) Votum des Auditors
Nach Abarbeitung der Einzelanforderungen muss ein Urteil des Auditors erfolgen. Das Votum muss anhand der Prüfergebnisse nachvollzogen werden können.

12. Auditortestat

12.1 Abgabe des Auditortestats

Wenn der Auditteamleiter im Auditbericht festgestellt hat, dass der betrachtete Untersuchungsgegenstand den Anforderungen eines Auditortestats (Einstiegsstufe oder Aufbaustufe) genügt, kann er der Institution ein entsprechendes Auditortestat ausstellen.

Das Auditortestat muss mindestens folgende Informationen umfassen:

- Name und Adresse der Institution,
- Name und Adresse des Auditors,
- Name und Adresse des Unternehmens, für das der Auditor tätig ist (falls zutreffend),
- Beschreibung des Untersuchungsgegenstands,
- Stufe des Auditortestats (Einstiegsstufe oder Aufbaustufe),
- Version der IT-Grundschutz-Methodik und der IT-Grundschutz-Kataloge (Monat, Jahr), auf deren Grundlage der Basis-Sicherheitscheck durchgeführt wurde,
- Beginn der Gültigkeit des Auditortestats (Ausstellungsdatum des Auditberichts) und
- Ende der Gültigkeit des Auditortestats (nach 2 Jahren).

Die unabhängige Prüfung der Umsetzung der IT-Grundschutz-Methodik wird beim Auditortestat durch einen Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz oder einen IT-Grundschutz-Auditor durchgeführt, der die Umsetzung mit folgendem Text bestätigt:

„Gemäß den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) habe ich für den oben genannten Untersuchungsgegenstand ein Audit durchgeführt. Ich bestätige, dass der Untersuchungsgegenstand die vom BSI festgelegten Anforderungen für das Auditortestat <Einstiegsstufe oder Aufbaustufe> der IT-Grundschutz-Qualifizierung erfüllt. <Datum>, <Unterschrift des Auditors>“. Ein Antragsformular zur Veröffentlichung des Auditortestats auf den Webseiten des BSI findet sich unter http://www.bsi.bund.de/gshb/zert/veroeffentl/antraege.htm. Der Auditbericht ist nicht beim BSI zur Prüfung einzureichen. Dem BSI ist auf Verlangen Einsicht in den Auditbericht zu gewähren.

Sofern mit der Erlangung eines Auditortestats geworben wird, hat die Institution dafür Sorge zu tragen, dass nicht der Eindruck erweckt wird, es handle sich um ein Zertifikat.

12.2 Verlängerung eines Auditortestats

Im Gegensatz zu Zertifikaten gelten Auditortestate nur maximal zwei Jahre und es sind keine Überwachungsaudits erforderlich. Auditortestate können nach Ablauf der Gültigkeitsdauer nicht verlängert werden. Um die Qualifizierung fortzusetzen, muss stattdessen eine höhere Stufe im Qualifizierungsschema erreicht werden. Beim Auditortestat „Einstiegsstufe“ bedeutet dies, dass nach Ablauf der Gültigkeit ein Auditortestat „Aufbaustufe“ oder das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz erreicht werden muss. Nach Ablauf der Gültigkeit des Auditortestats „Aufbaustufe“ muss das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz erreicht werden. Anderenfalls endet die Qualifizierung nach IT-Grundschutz.

13. Anhang

13.1 Anträge

Alle Anträge und Formulare zur ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz sind auf den Webseiten des BSI unter http://www.bsi.bund.de/gshb/zert/index.htm veröffentlicht. Dort finden Sie den Lizenzierungsantrag für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz und eine Liste aller Auditoren, die Audits für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz durchführen dürfen.

Für die Veröffentlichung der Auditortestate Einstiegstufe bzw. Aufbaustufe ist der Antrag ebenfalls unter dieser Adresse zu finden. Alle IT-Grundschutz-Auditoren und alle Auditoren für ISO 27001 auf der Basis von IT-Grundschutz sind berechtigt, Audits für Auditortestate durchzuführen.

13.2 Unabhängigkeitserklärung der Auditoren

Zu Beginn eines ISO 27001-Zertifizierungsverfahrens auf der Basis von IT-Grundschutz ist, wie in Kapitel 3 beschrieben, eine Unabhängigkeitserklärung der Auditoren bei der Zertifizierungsstelle einzureichen. Ein Formular dafür ist ebenfalls auf der Webseite des BSI veröffentlicht.

13.3 Gliederung des Auditberichts eines Zertifizierungsaudits

1. Allgemeines

1.1 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz
An dieser Stelle soll die Zielsetzung, der Verfahrensablauf, die auditierten Bereiche und Standorte und die Funktion des Auditberichts in kurzer Form darstellt werden.

1.2 Auditierte Institution
An dieser Stelle werden die vollständigen Kontaktinformationen der auditierten Institution, einschließlich vollständiger Adresse und Benennung eines Ansprechpartners bzw. des Projektleiters (mit E-Mail-Adresse und Telefonnummer) aufgeführt. Falls auf dem Zertifikat eine andere Adresse angegeben werden soll als der Ansprechpartner besitzt, muss diese hier ebenfalls aufgeführt werden.

1.3 Auditteam
An dieser Stelle werden die vollständigen Kontaktinformationen aller Mitglieder des Auditteams, d. h. vollständiger Name, postalische Erreichbarkeit am Arbeitsplatz, E-Mail-Adresse, Telefonnummer. Ist der Auditor im Auftrag eines Unternehmens tätig, so ist auch dieses Unternehmen unter Angabe der vollständigen Kontaktinformationen anzugeben. Die Angaben des Auditteamleiters (Name und Adresse) werden so gelistet, wie sie im Anhang zum Zertifikat aufgeführt werden sollen.
Dieser Abschnitt enthält außerdem folgende Erklärung des Auditteamleiters sowie anderer beteiligter Auditoren oder Erfüllungsgehilfen:
„Ich bin für die Durchführung von ISO 27001-Audits auf der Basis von IT-Grundschutz beim BSI lizenziert.“ <Hier fügt das Mitglied des Auditteams die Unabhängigkeitserklärung mit Begründung ein.> „Die Ergebnisse des Auditberichtes beruhen auf meinen eigenen Prüfungen, die ich weisungsfrei und unabhängig durchgeführt habe.
<Datum>, <Unterschrift des Auditteammitglieds>“

1.4 Vertragsgrundlage
Grundlagen der Auditierung sind

- eine Vertragsvereinbarung des Antragstellers mit dem Auditteamleiter,

- ein gültiger Lizenzierungsvertrag des Auditteamleiters mit dem BSI,
- Abnahme der Unabhängigkeitserklärungen und des IT-Verbundes von der Zertifizierungsstelle sowie
- ein Zertifizierungsantrag der Institution beim BSI.

Auf diese Dokumente wird unter Angabe der jeweils beteiligten Parteien und des Datums verwiesen.

1.5 Untersuchungsgegenstand
In diesem Kapitel wird in kurzer Form der auditierte Untersuchungsgegenstand definiert. Die Integration des Untersuchungsgegenstandes in Bezug auf das Gesamtunternehmen muss dargestellt werden. Es kann die Darstellung des Untersuchungsgegenstands aus Anhang A.1 wiedergegeben werden. Falls der Wortlaut des Untersuchungsgegenstandes nicht in das Zertifikat übernommen werden kann, wird dies hier vermerkt.

1.6 Projektierung
In diesem Kapitel wird der zeitliche Ablauf der Auditierung in tabellarischer Form aufgeführt. Es sollten mindestens die Projektschritte

- Beginn der Auditierung,
- Erhalt der Referenzdokumente,
- Beginn der Sichtung der Referenzdokumente,
- Inspektion vor Ort,
- Prüfung der Nachbesserungen,
- Erstellung des Auditberichts und
- Abschluss der Auditierung

sowie die Anzahl der benötigten Audittage (gegliedert in Tage zur Dokumentenprüfung, Tage für die Durchführung eines Voraudits, Tage für die Vor-Ort-Prüfung und Tage zur Erstellung des Auditberichts; ohne Reisezeiten) enthalten sein.

1.7 Verteiler
An dieser Stelle werden Adressaten und Verfasser des Auditberichtes aufgeführt. Dies umfasst in der Regel mindestens den Auditteamleiter, die auditierte Institution und die Zertifizierungsstelle (falls ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz angestrebt wird). Da der Auditbericht in den meisten Fällen vertrauliche Informationen enthält, wird dieses Kapitel mit folgendem Hinweis abgeschlossen: „Der Inhalt dieses Auditberichts ist vertraulich und richtet sich nur an oben genannte Empfänger.“ Das Schriftstück sollte entsprechend gekennzeichnet werden. Hinweise zur Vertraulichkeit sollten auf dem Deckblatt und in der Kopfzeile der Seiten zu finden sein.

2 Phase 1 des Erst-/ Re-Zertifizierungsaudits: Sichtung der Referenzdokumente
In den nachfolgenden Unterkapiteln werden die Durchführung und die Ergebnisse der Sichtung der Referenzdokumente dargestellt. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 4 dieses Prüfplans aufgeführt.

2.1 Voraudit
In diesem Kapitel wird aufgeführt, ob ein Voraudit durchgeführt wurde, welche Aspekte dort geprüft wurden, welche Zeit die Prüfung in Anspruch genommen hat

2.2 Aktualität der Dokumente

2.2.1 Aktualität der Version der Prüfgrundlagen

2.2.2 Aktualität der Referenzdokumente

2.2.3 Datum des Basis-Sicherheitschecks

2.3 IT-Sicherheitsrichtlinien

2.3.1 Vollständigkeit der IT-Sicherheitsrichtlinien

2.3.2 Verantwortung des Managements

2.3.3 Nachvollziehbarkeit der IT-Sicherheitsrichtlinien
2.4 IT-Strukturanalyse
2.4.1 Nachvollziehbarkeit der Abgrenzung des IT-Verbunds
2.4.2 Aktualität der Version der Prüfgrundlagen und Datum des Basis-Sicherheitschecks
2.4.3 Identifizierbarkeit der Komponenten im bereinigten Netzplan
2.4.4 Umfang der Liste der IT-Systeme
2.4.5 Konformität der Liste der IT-Systeme mit dem Netzplan
2.4.6 Umfang der Liste der IT-Anwendungen
2.5 Schutzbedarfsfeststellung
2.5.1 Plausibilität der Definition der Schutzbedarfskategorien
2.5.2 Vollständigkeit der Schutzbedarfsfeststellung der IT-Anwendungen
2.5.3 Vollständigkeit der Schutzbedarfsfeststellung der IT-Systeme
2.5.4 Plausibilität der Schutzbedarfsfeststellung der IT-Systeme
2.5.5 Kritikalität der Kommunikationsverbindungen
2.5.6 Plausibilität der Schutzbedarfsfeststellung der Räume
2.6 Modellierung des IT-Verbunds
2.6.1 Nachvollziehbarkeit der Modellierung
2.6.2 Korrektheit der Gruppenbildung
2.7 Ergebnis des Basis-Sicherheitschecks
2.7.1 Konformität zur Modellierung
2.7.2 Transparenz der Interviewpartner
2.7.3 Umsetzungsgrad der IT-Grundschutz-Maßnahmen
2.8 Ergänzende Sicherheitsanalyse und ergänzende Risikoanalyse
2.8.1 Vollständigkeit und Plausibilität der ergänzenden Sicherheitsanalyse
2.8.2 Vollständigkeit und Plausibilität der ergänzenden Risikoanalyse
2.8.3 Umsetzungsgrad aller Maßnahmen
3 Vorbereitung der Audittätigkeit vor Ort
3.1 Entscheidung zur Weiterführung des Audits mit Phase 2
3.2 Erstellung eines Prüfplans
3.3 Auswahl der Prüfbausteine

Hier wird insbesondere die Auswahl der Stichproben des Basis-Sicherheitschecks wie in Kapitel 5 beschrieben dokumentiert.

4 Phase 2 des Erst-/Re-Zertifizierungsaudits: Inspektion vor Ort

In den nachfolgenden Unterkapiteln werden die Durchführung und die Ergebnisse der Inspektion vor Ort dargestellt. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 6 dieses Prüfplans aufgeführt.

4.1 Wirksamkeit des Managementsystems für Informationssicherheit
4.2 Verifikation des Netzplans
4.3 Verifikation der Liste der IT-Systeme
4.4 Verifikation des Basis-Sicherheitschecks
4.5 Verifikation der Umsetzung der zusätzlichen Maßnahmen aus der ergänzenden Risikoanalyse
5 Nachbesserungen und Empfehlungen

In diesem Kapitel werden Abweichungen dargestellt und mit einer Frist zur Behebung versehen. Nach der Überprüfung der Nachbesserungen werden hier die inzwischen behobenen Abweichungen aufgeführt; in den Kapiteln 2 bis 4 dagegen wird die Situation nach Behebung

der Abweichungen dargestellt. Empfehlungen können hier ausgesprochen werden. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 7 dieses Prüfschemas aufgeführt.

6 Gesamtvotum

Dieses Kapitel enthält das Gesamtvotum des Auditors, ob der betrachtete Untersuchungsgegenstand die Anforderungen der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz bzw. die angestrebte Stufe der IT-Grundschutz-Qualifizierung erfüllt. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 8 dieses Prüfschemas aufgeführt.

Anhang

A Referenzdokumente

Anhang A enthält die Referenzdokumente, die die Grundlage für die Auditierung bilden. Der genaue Inhalt dieser Dokumente ist in Kapitel 3.4 dieses Prüfplans bzw. in der IT-Grundschutz-Methodik beschrieben. Es ist dem Antragsteller freigestellt, ob er das Dokument A.4 Ergebnis des Basis-Sicherheitschecks der Zertifizierungsstelle zur Verfügung stellt. Abweichungen, die der Auditor im Zusammenhang mit A.4 festgestellt hat, sind jedoch im Auditbericht dokumentiert.

A.0 IT-Sicherheitsrichtlinien

A.1 IT-Strukturanalyse

A.2 Schutzbedarfsfeststellung

A.3 Modellierung des IT-Verbunds

A.4 Ergebnis des Basis-Sicherheitschecks (optional)

A.5 Ergänzende Sicherheitsanalyse

A.6 Ergänzende Risikoanalyse

13.4 Gliederung des Auditberichts eines Überwachungsaudits

1. Allgemeines

1.1 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz
An dieser Stelle soll die Zielsetzung, der Verfahrensablauf, die auditierten Bereiche und Standorte und die Funktion des Auditberichts in kurzer Form darstellt werden.

1.2 Auditierte Institution
An dieser Stelle werden die vollständigen Kontaktinformationen der auditierten Institution, einschließlich vollständiger Adresse und Benennung eines Ansprechpartners bzw. des Projektleiters (mit E-Mail-Adresse und Telefonnummer) aufgeführt.

1.3 Auditteam
An dieser Stelle werden die vollständigen Kontaktinformationen aller Mitglieder des Auditteams, d. h. vollständiger Name, postalische Erreichbarkeit am Arbeitsplatz, E-Mail-Adresse, Telefonnummer. Ist der Auditor im Auftrag eines Unternehmens tätig, so ist auch dieses Unternehmen unter Angabe der vollständigen Kontaktinformationen anzugeben.
Dieser Abschnitt enthält außerdem folgende Erklärung des Auditteamleiters sowie anderer beteiligter Auditoren oder Erfüllungsgehilfen:
„Ich bin für die Durchführung von ISO 27001-Audits auf der Basis von IT-Grundschutz beim BSI lizenziert.“ <Hier fügt das Mitglied des Auditteams die Unabhängigkeitserklärung mit Begründung ein.> „Die Ergebnisse des Auditberichtes beruhen auf meinen eigenen Prüfungen, die ich weisungsfrei und unabhängig durchgeführt habe.
<Datum>, <Unterschrift des Auditteammitglieds>“

1.4 Vertragsgrundlage
Grundlagen der Auditierung sind

- eine Vertragsvereinbarung des Antragstellers mit dem Auditteamleiter,
- ein gültiger Lizenzierungsvertrag des Auditteamleiters mit dem BSI sowie
- ein gültiges ISO 27001-Zertifikat auf der Basis von IT-Grundschutz.

Auf diese Dokumente wird unter Angabe der jeweils beteiligten Parteien und des Datums verwiesen.

1.5 Untersuchungsgegenstand
In diesem Kapitel wird in kurzer Form der auditierte Untersuchungsgegenstand definiert. Die Integration des Untersuchungsgegenstandes in Bezug auf das Gesamtunternehmen muss dargestellt werden. Insbesondere Änderungen zum letzten Audit werden dargestellt.

1.6 Projektierung
In diesem Kapitel wird der zeitliche Ablauf der Auditierung in tabellarischer Form aufgeführt. Es sollten mindestens die Projektschritte

- Beginn der Auditierung,
- Erhalt der Referenzdokumente,
- Beginn der Sichtung der Referenzdokumente,
- Inspektion vor Ort,
- Prüfung der Nachbesserungen,
- Erstellung des Auditberichts und
- Abschluss der Auditierung

sowie die Anzahl der benötigten Audittage (gegliedert in Tage zur Dokumentenprüfung, Tage für die Vor-Ort-Prüfung und Tage zur Erstellung des Auditberichts; ohne Reisezeiten) enthalten sein.

1.7 Verteiler
An dieser Stelle werden Adressaten und Verfasser des Auditberichtes aufgeführt. Dies umfasst in der Regel mindestens den Auditteamleiter, die auditierte Institution und die Zertifizierungsstelle (falls ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz angestrebt wird). Da der Auditbericht in den meisten Fällen vertrauliche Informationen enthält, wird dieses Kapitel mit folgendem Hinweis abgeschlossen:
„Der Inhalt dieses Auditberichts ist vertraulich und richtet sich nur an oben genannte Empfänger."
Das Schriftstück sollte entsprechend gekennzeichnet werden. Hinweise zur Vertraulichkeit sollten auf dem Deckblatt und in der Kopfzeile der Seiten zu finden sein.

2 Phase 1 des Überwachungsaudits: Sichtung der Referenzdokumente
In den nachfolgenden Unterkapiteln werden die Durchführung und die Ergebnisse der Sichtung der Referenzdokumente dargestellt.

3 Vorbereitung der Audittätigkeit vor Ort

4 Phase 2 des Überwachungsaudits: Inspektion vor Ort

In den nachfolgenden Unterkapiteln werden die Durchführung und die Ergebnisse der Inspektion vor Ort dargestellt.

4.1 Prüfung des Managementsystems für Informationssicherheit

4.2 Prüfung von Änderungen am IT-Verbund

4.3 Prüfung der zwischenzeitlichen Behebung von Abweichungen

4.4 Prüfung der Einhaltung von Auflagen

5 Nachbesserungen und Empfehlungen

In diesem Kapitel werden Abweichungen dargestellt und mit einer Frist zur Behebung versehen. Nach der Überprüfung der Nachbesserungen werden hier die inzwischen behobenen Abweichungen aufgeführt; in den Kapiteln 2 bis 4 dagegen wird die Situation nach Behebung der Abweichungen dargestellt. Optional dazu ist es auch möglich, bei den einzelnen Prüfungen

den Zustand vor und nach Nachbesserungen zu schildern und in diesem Kapitel einen genauen Verweis darauf zu geben, in welchen Kapiteln Nachbesserungen notwendig sind bzw. waren und ob sie inzwischen durchgeführt wurden.

Empfehlungen können hier ausgesprochen werden. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 7 dieses Prüfschemas aufgeführt.

6 Gesamtvotum für die Aufrechterhaltung des Zertifikats

Dieses Kapitel enthält das Gesamtvotum des Auditors, ob der betrachtete Untersuchungsgegenstand die Anforderungen der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz bzw. die angestrebte Stufe der IT-Grundschutz-Qualifizierung erfüllt. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 8 dieses Prüfschemas aufgeführt.

Anhang

A Referenzdokumente

Anhang A enthält die Referenzdokumente, die die Grundlage für die Auditierung bilden. Der genaue Inhalt dieser Dokumente ist in Kapitel 3.4 dieses Prüfplans bzw. in der IT-Grundschutz-Methodik beschrieben. Es ist dem Antragsteller freigestellt, ob er das Dokument A.4 Ergebnis des Basis-Sicherheitschecks der Zertifizierungsstelle zur Verfügung stellt. Abweichungen, die der Auditor im Zusammenhang mit A.4 festgestellt hat, sind jedoch im Auditbericht dokumentiert.

A.0 IT-Sicherheitsrichtlinien

A.1 IT-Strukturanalyse

A.2 Schutzbedarfsfeststellung

A.3 Modellierung des IT-Verbunds

A.4 Ergebnis des Basis-Sicherheitschecks (optional)

A.5 Ergänzende Sicherheitsanalyse

A.6 Ergänzende Risikoanalyse