

Bundesamt für Sicherheit in der Informationstechnik



Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Prüfschema für ISO 27001-Audits

Stand: 1. Februar 2006

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik

Redaktion: <mailto:zertifizierung@bsi.bund.de>

Inhaltsverzeichnis

Vorwort	4
1 Einleitung	5
1.1 Versionshistorie	5
1.2 Zielsetzung	5
1.3 Adressatenkreis	5
1.4 Anwendungsweise	5
1.5 Literaturverzeichnis	6
2 Audit-Prinzipien	7
3 Ablauf des Audit-Prozesses	8
3.1 Überblick über den Audit-Prozess	8
3.2 Zielsetzung und Umfang des Audits	8
3.3 Rollen und Zuständigkeiten im Audit-Prozess	8
3.4 Geforderte Referenzdokumente	9
3.5 Zertifizierungsantrag beim BSI	11
3.6 Durchführung des Audits	12
3.7 Erstellung des Audit-Reports	12
3.8 Zertifizierungsprozess	12
3.9 Re-Zertifizierung	13
4 Sichtung der Referenzdokumente	14
4.1 Überblick über die Audit-Aktivitäten	14
4.2 IT-Strukturanalyse	14
4.3 Schutzbedarfsfeststellung	15
4.4 Modellierung des IT-Verbunds	17
4.5 Ergebnis des Basis-Sicherheitschecks	18
4.6 Ergänzende Sicherheitsanalyse und Ergänzende Risikoanalyse	19
5 Vorbereitung der Audit-Tätigkeit vor Ort	22
5.1 Erstellung eines Prüfplans	22
5.2 Vorbereitung der Arbeitsdokumente	22
5.3 Auswahl der Prüfbausteine	22
6 Inspektion vor Ort	24
6.1 Überblick über die Audit-Aktivitäten vor Ort	24
6.2 Verifikation des Netzplans	24
6.3 Verifikation der Liste der IT-Systeme	24
6.4 Verifikation des Basis-Sicherheitschecks	25

6.5	Verifikation der Umsetzung der Zusätzlichen Maßnahmen aus der Ergänzenden Risikoanalyse	26
7	Nachbesserungen und Nachforderungen	27
7.1	Nachbesserungen	27
7.2	Nachforderungen	27
7.3	Schiedsstelle des BSI	27
8	Gesamtvotum	28
9	Auditierung im Rahmen einer Re-Zertifizierung	29
10	Praktische Hilfen	30
10.1	Audit-Report	30
10.2	Formale Aspekte des Audit-Reports	30
11	Auditor-Testat	32
11.1	Abgabe des Auditor-Testats	32
11.2	Verlängerung eines Auditor-Testats	32
12	Anhang	33
12.1	Anträge	33
12.2	Formular für die Unabhängigkeitserklärung des Auditors	33
12.3	Gliederung des Audit-Reports	33

Vorwort

ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz geben Behörden und Unternehmen die Möglichkeit, ihre Bemühungen um IT-Sicherheit 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 ein entsprechender Erlass des Bundesministeriums des Innern vom 06. Februar 2001. Grundlage dieses Dokumentes ist die Norm EN ISO 19011:2002 "Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen". Diese internationale Norm gibt eine Anleitung für den Ablauf und die Durchführung von Audits. 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
01.01.2006	1.0	BSI
01.02.2006	1.1	BSI

1.2 Zielsetzung

Das vorliegende Prüfschema für Auditoren beschreibt die verbindliche Vorgehensweise, wie Auditoren die für die Erlangung eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz oder eines Auditor-Testats (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/schema.htm> veröffentlicht sind. In ergänzenden Verfahrensanweisungen werden unter Anderem Grundsatzentscheidungen des BSI veröffentlicht.

1.3 Adressatenkreis

Dieses Dokument richtet sich vor allem an lizenzierte Auditoren, die ein unabhängiges Audit durchführen, um die Umsetzung eines IT-Sicherheitskonzeptes 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 folgendem Dokument werden die Voraussetzungen und die Vorgehensweise für eine ISO 27001-Zertifizierung beschrieben. Nach allgemeinen Anforderungen an ein Audit in Kapitel 2 gibt Kapitel 3 einen Überblick über den Audit-Prozess. Danach wird in drei Phasen die Durchführung des Audits beschrieben.

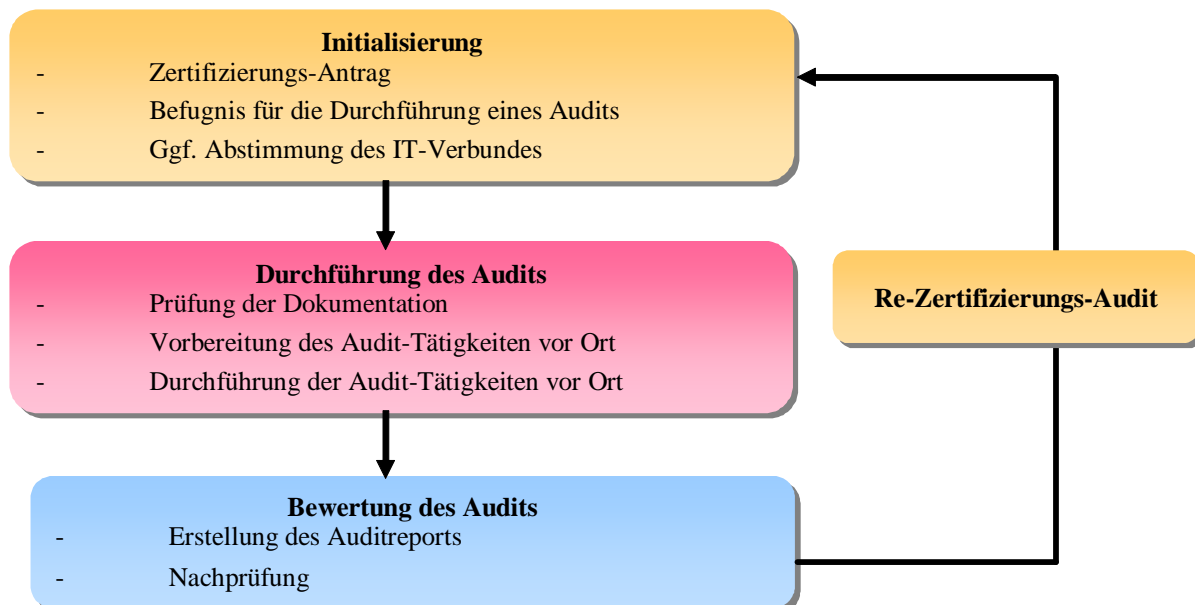


Abbildung: Phasen des Audit-Prozesses

Auf der Grundlage einer Dokumenten-Prüfung (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 2 Jahre gültig, nach denen die Institution eine Re-Zertifizierung (Kapitel 9) veranlassen muss, um die kontinuierliche Umsetzung der Anforderungen weiterhin nachweisen zu können.

Um dem Auditor zusätzliche Hilfsmittel bei der Anwendung des Prüfschemas zu geben und somit die Gleichwertigkeit des Verfahrens besser zu gewährleisten, werden in Kapitel 10 praktische Hilfen gegeben.

Für die Durchführung eines Auditor-Testates (Einstiegstufe bzw. Aufbaustufe) muss das Prüfschema ebenfalls angewendet werden. In Kapitel 11 wird explizit auf dieses Verfahren eingegangen. Um das Dokument übersichtlicher zu gestalten, wird an allen Stellen nur der Begriff Zertifikat verwendet, auch wenn sich das Verfahren auf beide Vorgehensweisen bezieht.

1.5 Literaturverzeichnis

- [GSV] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, <http://www.bsi.bund.de>
- [GSHB] IT-Grundschutzhandbuch - 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
- [OECD-02] Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, <http://www.oecd.org/sti/security-privacy>
- [ZERT] Allgemeine Informationen zum IT-Grundschutz-Zertifikat, zum Lizenzierungsschema für Auditoren und zum Zertifizierungsschema für IT-Grundschutz unter <http://www.bsi.bund.de/gshb/zert>
- [13335] ISO 13335 "Management of information and communications technology security"
- [17799] ISO/IEC 17799:2005 "Information technology - Security techniques - Code of practice for information security management"
- [27001] ISO/IEC 27001 "Information technology - Security techniques - Information security management systems requirements specification"

2 Audit-Prinzipien

Die Audit-Prinzipien fassen die grundlegenden Punkte des Audit-Prozesses 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 Audit-Prinzipien sind eine Voraussetzung für nachvollziehbare und wiederholbare Audit-Ergebnisse, die gleichartig und aussagekräftig sind, um eine nachfolgende Zertifizierung zu ermöglichen.

Die folgenden Prinzipien müssen erfüllt werden:

Ethisches Verhalten:

Die Grundlage des Berufsbildes eines Auditors ist die Vertrautheit mit der Informationssicherheitstechnik.

Da im Umfeld IT-Sicherheit oft sensible Geschäftsprozesse und Daten zu finden sind, sind die Vertraulichkeit der Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der Audit-Prüfung eine wichtige Arbeitsgrundlage.

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 Audit-Feststellungen, Audit-Schlussfolgerungen und dem Audit-Bericht. Die Prüfungsergebnisse des Audits müssen wiederholbar sein (bei unverändertem Sachstand).

Angemessene Sorgfalt:

Ein Auditor muss beim Auditieren mit Sorgfalt vorgehen. Sein Urteilsvermögen ist unerlässliche Voraussetzung für sachgerechte und fundierte Audits.

Unabhängigkeit und Objektivität:

Die Grundlage für die Unparteilichkeit des Audits weist der Auditor in Form einer Unabhängigkeitserklärung nach. Dabei ist zu bestätigen, dass die Ergebnisse des Audit-Reportes auf eigenen Prüfungen beruhen, weisungsfrei und unabhängig durchgeführt wurden. Dabei darf der Auditor in den letzten zwei Jahren nicht im Umfeld des Untersuchungsgegenstandes beratend tätig gewesen sein.

Alle Audit-Schlussfolgerungen müssen objektiv nachvollzogen werden können.

Nachweise:

Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Audit-Schlussfolgerungen in einem systematischen Audit-Prozess zu kommen, ist die eindeutige und folgerichtige Dokumentation der Ergebnisse. Die Audit-Nachweise 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 relevant und in einem sinnvollen Umfang vorgenommen werden.

3 Ablauf des Audit-Prozesses

3.1 Überblick über den Audit-Prozess

Nachdem eine Institution die IT-Grundschutz-Methodik umgesetzt hat und alle relevanten Dokumente vorliegen, kann sie einen lizenzierten Auditor beauftragen, anhand des Prüfschemas in einer unabhängigen Prüfung die Umsetzung der Anforderungen eines ISO 27001-Zertifizierungsverfahrens auf der Basis von IT-Grundschutz zu überprüfen. Der Auditor dokumentiert seine Prüfergebnisse in einem Audit-Report, der zusammen mit dem Zertifizierungsantrag der Zertifizierungsstelle als Grundlage für ein ISO 27001-Zertifikat dient.

3.2 Zielsetzung und Umfang des Audits

Ziel des Audits ist die unabhängige Überprüfung der Einhaltung sowohl von ISO 27001 als auch von IT-Grundschutz durch einen vom BSI lizenzierten Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz. Die Überprüfung umfasst sowohl eine Dokumentenprüfung als auch eine Umsetzungsprüfung der erforderlichen IT-Sicherheitsmaßnahmen vor Ort.

3.3 Rollen und Zuständigkeiten im Audit-Prozess

Im Audit-Prozess gibt es drei unterschiedliche Rollen:

- den Antragsteller,
- den Auditor bzw. das Audit-Team sowie eventuell Erfüllungsgehilfen und
- die Zertifizierungsstelle.

Der **Antragsteller** stellt die erforderlichen Dokumente zur Verfügung und unterstützt den Auditor bei der Vor-Ort-Prüfung des IT-Verbundes. Er ist Initiator des Audit-Prozesses. Er beauftragt einen Auditor und stellt den Zertifizierungsantrag beim BSI.

Die Auditierung muss durch einen beim BSI hierfür lizenzierten **Auditor** erfolgen. Ein Auditor sollte nur Themengebiete prüfen, wenn er das notwendige Fachwissen und ausreichend Erfahrung mitbringt. Falls der Auditor nicht über das nötige Spezialwissen verfügt, sollte er zur Unterstützung der Prüftätigkeiten und zur Absicherung der Prüfaussagen einen oder mehrere Experten als **Erfüllungsgehilfen** hinzuziehen.

Zwei oder mehr Auditoren (Fachexperten) können sich zu einem ein **Audit-Team** zusammenschließen, um ein gemeinsames Audit durchzuführen. In einem solchen Fall sollte ein Audit-Verantwortlicher bestimmt werden. Die Rollen und Zuständigkeiten der Teammitglieder sind zu Beginn des Audit-Prozesses festzulegen. Auch ein Audit-Team kann noch Erfüllungsgehilfen zur Unterstützung dazuziehen. Mitglieder des Audit-Teams (Auditor, Erfüllungsgehilfen, Experten) dürfen in den letzten 2 Jahren nicht im Umfeld des zu zertifizierenden IT-Verbunds (z. B. Fachabteilung) beratend tätig gewesen sein. Eine **Unabhängigkeitserklärung** aller Teammitglieder muss vor Beginn des Verfahrens, d. h. vor dem Audit, bei der Zertifizierungsstelle eingereicht werden. Das BSI muss dem Einsatz des Auditors bzw. des Audit-Teams zustimmen. Alle Mitglieder des Audit-Teams müssen im Audit-Report aufgeführt sein

Hilfskräfte für reine Verwaltungstätigkeiten, beispielsweise Schreibkräfte, können eingesetzt werden, wenn diese vom Auditor entsprechend überwacht und kontrolliert werden. Für Hilfskräfte gelten keine einschränkenden Bedingungen, sie müssen auch nicht im Audit-Report genannt werden. Die Verantwortung für den Audit-Prozess verbleibt in jedem Fall beim lizenzierten Auditor.

Die **Zertifizierungsstelle** des BSI ist eine unabhängige dritte Instanz, die die Gleichwertigkeit der Prüfungen und der Audit-Reporte gewährleistet. Sie veröffentlicht die Kriterien, Schemata und Interpretationen und agiert als Schiedsstelle zwischen Auditor und Antragsteller.

3.4 Geforderte Referenzdokumente

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

- IT-Strukturanalyse (A.1)
- Schutzbedarfsfeststellung (A.2)
- Modellierung des IT-Verbunds (A.3)
- Ergebnis des Basis-Sicherheitschecks (A.4) (optional)
- 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.

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

Die Referenzdokumente sind Bestandteil des Audit-Reports. 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 Audit-Reports 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.

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. Die Gesamtheit der informationstechnischen Komponenten, die den Untersuchungsgegenstand unterstützen, heißt IT-Verbund. Der IT-Verbund 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.

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. finanzieller Schaden oder Verstoß 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

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. 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.

- Schutzbedarf der Kommunikationsverbindungen

Im Gegensatz zu IT-Anwendungen und IT-Systemen wird bei den Kommunikationsverbindungen lediglich zwischen kritischen und nicht-kritischen 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 Verbindung graphisch hervorgehoben sind.

- Schutzbedarf der IT-Räume

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

A.3 Modellierung des IT-Verbunds

Die Modellierung des IT-Verbunds 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-Kataloge 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-Sicherheitscheck 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 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,

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 einer Managementbewertung 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.

Eine Vorgehensweise zur Durchführung einer Ergänzenden Risikoanalyse ist im BSI-Standard 100-3 "Risikoanalyse auf der Basis von IT-Grundschutz" beschrieben.

3.5 Zertifizierungsantrag beim BSI

Vor Beginn des Audits beim Antragsteller müssen folgende Voraussetzungen erfüllt sein:

- Dem BSI muss der vollständige Zertifizierungsantrag 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**, d. h. ein kurzes Behörden- bzw. Firmenprofil, ist vorzulegen. Dabei müssen die wesentlichen Tätigkeitsfelder der Institution sowie die Größe und Bedeutung des IT-Verbunds für die Institution deutlich werden.

Der zu zertifizierende **IT-Verbund** ist zu beschreiben sowie ein **bereinigter Netzplan** vorzulegen. Der Antrag ist erst vollständig, wenn die prinzipielle Zertifizierbarkeit, also die sinnvolle Abgrenzung des IT-Verbunds, vom BSI bestätigt ist. Dies kann durch telefonischen Kontakt oder, falls notwendig, durch eine Besprechung geschehen.

Um zu vermeiden, dass ein Antrag gestellt wird, dessen IT-Verbund nicht zertifizierbar ist, besteht die Möglichkeit, die Dokumente schon vor dem eigentlichen Antrag beim BSI zur Abstimmung einzureichen.
 - 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 erweiterter 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 sowie zur Abgabe des Audit-Reports beim BSI zu machen. Terminänderungen, die sich nach Beantragung der Zertifizierung ergeben, sind dem BSI mitzuteilen.
- Jeder Auditor des Audit-Teams muss dem BSI gegenüber eine Unabhängigkeitserklärung abgeben. Diese besagt, dass der Auditor / die Auditoren sowie ggf. beteiligte Erfüllungsgehilfen in den letzten zwei Jahren nicht im Bereich des Untersuchungsgegenstandes beratend tätig gewesen sind. Diese Unabhängigkeitserklärung muss dem BSI mindestens zwei Wochen vor Beginn der

Auditierungstätigkeit vorliegen. Die Unabhängigkeitserklärung kann vom Antragsteller mit dem Zertifizierungsantrag eingereicht werden.

Das BSI behält sich vor, zusätzliche Informationen zum Beschäftigungsverhältnis zwischen Auditor und Antragsteller anzufordern. Besteht der Verdacht, dass die Unabhängigkeit des Auditors nicht gewährleistet ist, hat das BSI das Recht, der Durchführung des Audits durch diesen Auditor zu widersprechen.

3.6 Durchführung des Audits

Das Audit wird von einem Auditor durchgeführt, der vom BSI für die Durchführung von "ISO 27001-Audits auf der Basis von IT-Grundschutz" lizenziert ist. Kontaktadressen der zugelassenen Auditoren finden sich im Internet unter <http://www.bsi.bund.de/gshb/zert/lizenzauditoren.htm>.

Nach der Umsetzung der IT-Grundschutz-Anforderungen beauftragt die Institution einen lizenzierten Auditor damit, in einer unabhängigen Prüfung den Status der IT-Sicherheit in der Institution zu verifizieren. Dabei wird eine Prüfung in zwei Teilschritten durchgeführt. Als erstes werden die vom Antragsteller vorgelegten Referenzdokumente gesichtet und anhand der Prüfkriterien (siehe Kapitel 4) verifiziert. Die Ergebnisse werden im Audit-Report dokumentiert. Im zweiten Teilschritt bereitet der Auditor eine "vor Ort-Prüfung" bei dem Antragsteller (siehe Kapitel 5) vor und begutachtet stichprobenartig die Umsetzung der dokumentierten Sachverhalte (siehe Kapitel 6). Mängel werden im Audit-Report festgehalten. Der Antragsteller hat die Möglichkeit, diese Mängel in einer vom Auditor festgelegten Frist zu beheben. Kommt der Auditor zu einem positiven Prüfergebnis, sendet der Antragsteller den Audit-Report zum BSI. Bei einem negativen Ergebnis muss das BSI ebenfalls hierüber informiert werden. Die neutrale Zertifizierungsstelle des BSI überprüft den Audit-Report auf Vollständigkeit, Nachvollziehbarkeit und Reproduzierbarkeit der Prüfergebnisse. Nachforderungen oder Nachfragen werden an den Auditor gestellt, der die ggf. bestehenden Unklarheiten beseitigt. Nach positivem Abschluss des Prüfprozesses erteilt das BSI auf der Grundlage des Audit-Reports ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz.

3.7 Erstellung des Audit-Reports

Der Audit-Report enthält alle Prüfergebnisse des Auditors.

Das Format eines Audit-Reports ist von der Zertifizierungsstelle vorgegeben und ist im Anhang dieses Dokumentes beschrieben. Die Referenzdokumente des Antragstellers sind als Anlagen dem Audit-Report beizufügen.

Der Audit-Report richtet sich ausschließlich an den Antragsteller und die Zertifizierungsstelle. Die Ergebnisse des Audit-Reports werden vom Auditor und dem BSI vertraulich behandelt und nicht an Dritte weiter gegeben.

Anhand des Audit-Reports kann der Antragsteller Mängel oder Verbesserungsmöglichkeiten in seinem IT-Sicherheitsprozess erkennen. Der Zertifizierungsstelle dient der Audit-Report als Grundlage für die Erteilung des Zertifikats.

3.8 Zertifizierungsprozess

Wenn der Audit-Report bei der Zertifizierungsstelle vorliegt und die Rechnung vom Antragsteller beglichen wurde, prüft die Zertifizierungsstelle den Audit-Report. Dadurch wird ein einheitliches Niveau aller Zertifizierungen gewährleistet.

Der Audit-Report darf sich nur auf Prüfungen des Auditors (Dokumentenprüfungen und Audit) stützen, die zum Zeitpunkt der Übergabe des Audit-Reports 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 weitere Nachforderungen an den Audit-Report durch das BSI möglich. Wenn drei Monate nach Abgabe des ersten Audit-Reports das Verfahren noch nicht abgeschlossen ist, muss geprüft werden, ob auf der Basis des vorliegenden Reports noch ein Zertifikat erteilt werden kann.

Ein Zertifikat wird nur erteilt, wenn der Audit-Report durch die Zertifizierungsstelle akzeptiert wurde sowie ein positives Prüfungsergebnis vorliegt. Die Zertifizierungsstelle erteilt das Zertifikat und fertigt einen Anhang mit zusätzlichen Informationen an. Sofern der Antragsteller einer Veröffentlichung des Zertifikates zugestimmt hat, werden Zertifizierungsurkunde und Anhang auf den Internetseiten des BSI veröffentlicht.

Die zertifizierte Institution darf die Urkunde sowie ein vom BSI zur Verfügung gestelltes Logo unter der Bedingung verwenden, dass der Zertifizierungsanhang jederzeit zur Verfügung gestellt wird.

3.9 Re-Zertifizierung

Ein Zertifikat ist 2 Jahre gültig und kann dann durch eine erneute Antragstellung und Erstellung eines aktuellen Audit-Reports durch einen lizenzierten Auditor vom Antragsteller beim BSI beantragt werden. Nähere Informationen zur Durchführung einer Re-Zertifizierung finden sich in Kapitel 9.

Eine Verlängerung von Auditor-Testaten ist nicht möglich. Um die Qualifizierung nach der zweijährigen Gültigkeitsdauer fortzusetzen, muss stattdessen eine höhere Stufe im Qualifizierungsschema erreicht werden. Weitere Informationen zu der Verlängerung von Auditor-Testaten sind im Kapitel 11.2 zu finden.

4 Sichtung der Referenzdokumente

4.1 Überblick über die Audit-Aktivitäten

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

4.2 IT-Strukturanalyse

4.2.1 Nachvollziehbarkeit der Abgrenzung des IT-Verbunds

Ziel: Ein IT-Verbund ist sinnvoll abgegrenzt, wenn er alle IT-Komponenten umfasst, die zur Unterstützung einer oder mehrerer Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen.

Der IT-Verbund muss außerdem eine sinnvolle Mindestgröße im Gesamtkontext des Unternehmens haben, d. h. er muss substantiell zum Funktionieren der Institution oder eines Teils der Institution beitragen.

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

Votum: Ist der IT-Verbund sinnvoll abgegrenzt?

Hinweis: 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 Untersuchungsgegenstands zu initiieren.

4.2.2 Aktualität der Version der Prüfgrundlagen

Ziel: Es muss festgelegt werden, welche Version der IT-Grundschutz-Methodik und der IT-Grundschutz-Kataloge als Grundlage für die Auditierung verwendet werden soll. Zulässig ist die Verwendung der jeweils aktuellen und der unmittelbar vorhergehenden Version. Es wird jedoch dringend empfohlen, die jeweils aktuelle Version der Methodik/Kataloge zu verwenden, da zum Zeitpunkt der Zertifikatsvergabe geprüft wird, ob eine zulässige Version verwendet wurde. Für Auditierungen auf der Grundlage älterer Versionen der Methodik/Kataloge kann kein Zertifikat vergeben werden.

Aktion: Der Auditor dokumentiert die Versionen (Monat, Jahr) der BSI-Dokumente, auf deren Grundlage die Auditierung des Untersuchungsgegenstands erfolgen soll.

Votum: Werden zulässige Versionen angewendet?

4.2.3 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?

4.2.4 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. Mängel.

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

4.2.5 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?

4.2.6 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 Mängel.

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

4.3 Schutzbedarfsfeststellung

4.3.1 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.

Votum: Ist die Definition der Schutzbedarfskategorien plausibel?

4.3.2 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 Mängel werden im Audit-Report vermerkt.

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

4.3.3 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 Mängel werden im Audit-Report vermerkt.

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

4.3.4 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 Maximum-Prinzip, 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?

4.3.5 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 oder Mängel werden im Audit-Report dokumentiert.

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

4.3.6 Plausibilität der Schutzbedarfsfeststellung der IT-Räume

Ziel: Der Schutzbedarf der IT-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 und der Kumulationseffekt 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. Widersprüchlichkeiten.

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

4.4 Modellierung des IT-Verbunds

4.4.1 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.

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. Falls sich Abweichungen ergeben, muss dokumentiert werden, welche Zielobjekte in der Modellierung fehlen bzw. auf welche Zielobjekte ein bestimmter Baustein nicht anwendbar ist.

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

4.4.2 Anwendbarkeit der IT-Grundschutz-Methodik

Ziel: 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. Dabei müssen alle drei folgenden Anforderungen erfüllt sein:

1. Der überwiegende Teil des IT-Verbunds muss direkt durch entsprechende Bausteine der IT-Grundschutz-Kataloge modelliert sein.
2. Der Schutzbedarf derjenigen Komponenten, die nicht direkt durch entsprechende Bausteine modelliert werden können, muss "normal" oder "hoch" (nicht "sehr hoch") sein.
3. Ähnliche oder generische Bausteine, die für solche Komponenten ersatzweise herangezogen wurden, müssen korrekt angewandt sein.

Aktion: 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 Audit-Report 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.

Votum: Ist der überwiegende Teil des IT-Verbunds direkt durch entsprechende Bausteine der IT-Grundschutz-Kataloge modelliert?

Ist der Schutzbedarf derjenigen Komponenten, die nicht direkt durch entsprechende Bausteine modelliert werden können, "normal" oder "hoch" (nicht "sehr hoch")?

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

Der Auditor begründet sein Votum.

4.4.3 Korrektheit der Gruppenbildung

Ziel: Komponenten dürfen zu einer Gruppe zusammengefasst werden, wenn 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 nachvollziehbar 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?

4.5 Ergebnis des Basis-Sicherheitschecks

4.5.1 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?

4.5.2 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 dies anhand des vorgelegten Basis-Sicherheitschecks und dokumentiert etwaige Mängel.

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

4.5.3 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, wenn 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 Auditor-Testat Einstiegsstufe sind die mit A gekennzeichneten Maßnahmen und für ein Auditor-Testat Aufbaustufe sind die mit A und B gekennzeichneten Maßnahmen umzusetzen.
- Mit "Z" gekennzeichnete Maßnahmen müssen für keine der drei Ausprägungen zwingend umgesetzt 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 Audit-Report dokumentiert.

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

4.6 Ergänzende Sicherheitsanalyse und Ergänzende Risikoanalyse

Für Auditor-Testate ist die Prüfung der Ergänzenden Sicherheitsanalyse bzw. Ergänzenden Risikoanalyse nicht erforderlich, da für Auditor-Testate weniger IT-Grundschutz-Maßnahmen umgesetzt werden müssen als für ISO 27001-Zertifikate. Dadurch würden bei der Durchführung von einer Ergänzenden Risikoanalyse die fehlenden IT-Grundschutz-Maßnahmen erneut erkannt, so dass das Verfahren ineffektiv wird. Eine Ergänzende Risikoanalyse ist nach dem vorgegebenen Prüfschema erst dann durchzuführen, wenn alle relevanten IT-Grundschutz-Maßnahmen identifiziert wurden.

4.6.1 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 sind und ob 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?

4.6.2 Vollständigkeit und Plausibilität der Ergänzenden Risikoanalyse

Ziel: Für alle Komponenten, für die ein zusätzlicher Sicherheitsbedarf identifiziert wurde (siehe Abschnitt 4.6.1), muss eine Ergänzende Risikoanalyse durchgeführt worden sein. 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?

4.6.3 Umsetzungsgrad aller Maßnahmen

Ziel: Der Umsetzungsstatus der konsolidierten Maßnahmen ist zu dokumentieren. Für jede zusätzliche Maßnahme muss der Umsetzungsstatus ("entbehrlich", "ja", "teilweise", "nein") vermerkt sein. Dabei ist der Umsetzungsstatus der zusätzlichen Maßnahmen festzustellen und ggf. der Umsetzungsstatus der IT-Grundschutz-Maßnahmen zu aktualisieren. Die Ergebnisse sind als „Ergänzung des Basis-Sicherheitschecks“ 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 Audit-Report dokumentiert.

Votum: Ist der Ergänzende Basis-Sicherheitscheck vollständig? Ist der Umsetzungsgrad der zusätzlichen Maßnahmen ausreichen?

5 Vorbereitung der Audit-Tätigkeit vor Ort

5.1 Erstellung eines Prüfplans

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

5.2 Vorbereitung der Arbeitsdokumente

Natürgemäß sind die in den IT-Grundschatz-Katalogen enthaltenen Maßnahmentexte in Bezug auf die Formulierung der Anforderungen nicht vollständig homogen. Um möglichst eine 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 IT-Sicherheit zusätzlich erhöhen.
- Wenn im Maßnahmentext auf andere Maßnahmen der IT-Grundschatz-Bausteine verwiesen wird, so führt dies nicht automatisch dazu, dass auch diese Maßnahmen umgesetzt werden müssen. Im Rahmen der IT-Grundschatz-Zertifizierung sind lediglich die Maßnahmen relevant, die im jeweiligen Baustein genannt sind.
- Falls in ergänzenden Kontrollfragen IT-Sicherheitsaspekte 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-Grundschatz-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-Grundschatz-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.

5.3 Auswahl der Prüfbausteine

Bei der Vor-Ort-Prüfung muss sich der Auditor 10 Bausteinzuordnungen und 5 zusätzliche Maßnahmen auswählen. Diese Stichproben sind folgendermaßen zu bestimmen:

5.3.1 IT-Sicherheitsmanagement

Ziel: Da von der Wirksamkeit des IT-Sicherheitsmanagements die Qualität des gesamten IT-Sicherheitsprozesses abhängt, ist die Prüfung des Bausteins B 1.0 IT-Sicherheitsmanagement vorrangig und zwingend erforderlich. Der Auditor überprüft vor Ort die Umsetzung aller Maßnahmen des Bausteins B 1.0 "IT-Sicherheitsmanagement" für den IT-Verbund.

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

5.3.2 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-Bausteines 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.

5.3.3 Gezielte 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.

5.3.4 Stichproben aus der Ergänzenden Risikoanalyse

Ziel: Aus der Menge der zusätzlichen Sicherheitsmaßnahmen, die im Rahmen der Ergänzenden Risikoanalyse festgelegt wurden, wählt der Auditor nach eigenem Ermessen 5 Maßnahmen für verschiedene Komponenten aus.

Wurden im Rahmen der Ergänzenden Risikoanalyse weniger als 5 zusätzliche IT-Sicherheitsmaßnahmen festgelegt, so werden alle Maßnahmen überprüft.

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

6 Inspektion vor Ort

6.1 Überblick über die Audit-Aktivitäten vor Ort

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

Die einzelnen Prüfungen sollten direkt am Zielobjekt erfolgen, nicht nur anhand der Papierlage. Bei technischen Aspekten bedeutet dies eine Demonstration durch den jeweils zuständigen Administrator oder Vertreter. **Der Auditor sollte nicht selbst in das System eingreifen.**

6.2 Verifikation des Netzplans

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 Komponenten und Kommunikationsverbindungen aus dem bereinigten Netzplan als Stichproben aus und überprüft, ob sie sich in der gleichen Struktur im real existierenden Netz wiederfinden.

Umgekehrt wählt der Auditor 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.

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 zu werten:

- Komponenten oder Kommunikationsverbindungen, die im bereinigten Netzplan aufgeführt sind, sich aber nicht im realen Netz wiederfinden, sowie
- Komponenten oder Kommunikationsverbindungen, die im realen Netz vorhanden sind, dem betrachteten IT-Verbund zuzurechnen sind, sich aber nicht im bereinigten Netzplan wiederfinden.

Votum: Entsprechen die im bereinigtem Netzplan dargestellten Komponenten und deren Kommunikationsverbindungen der tatsächlichen Netzstruktur und ist der bereinigte Netzplan auf dem aktuellen Stand?

6.3 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 das jeweils verwendete Betriebssystem und der 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 Audit-Report festgehalten.

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

6.4 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 IT-Sicherheitszustand 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 5.3) 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.
- 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 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". Entscheidend ist, dass eine Maßnahme ihrem Sinn und Zweck nach umgesetzt wird. 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 Audit-Report kurz erläutert werden, was genau geprüft wurde, wer jeweils wofür befragt wurde und welche Ergebnisse zu vermerken sind (Begründung).

Votum: Stimmt der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der Maßnahmen mit dem tatsächlich vorhandenen IT-Sicherheitszustand des jeweiligen Zielobjekts überein? Ist die Begründung der „entbehrlichen“ Maßnahmen zulässig und nachvollziehbar? Sind alle ergänzenden Sicherheitsmaßnahmen aus der Risikoanalyse umgesetzt?

6.5 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 IT-Sicherheitszustand des jeweiligen Zielobjekts übereinstimmen

Aktion: Für die jede ausgewählte zusätzlichen Maßnahmen (vergleiche Kapitel 5.3) 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 IT-Sicherheitszustand des jeweiligen Zielobjekts überein?

7 Nachbesserungen und Nachforderungen

7.1 Nachbesserungen

Ziel: Sowohl bei der ersten Sichtung der Referenzdokumente als auch bei der ersten Inspektion vor Ort werden sich in manchen Fällen Mängel ergeben. Diese Mängel müssen sachgerecht behoben werden.

Aktion: Der Auditor informiert die Institution möglichst frühzeitig schriftlich über festgestellte Mängel, damit diese zeitnah behoben werden können. Er muss der Institution hierzu eine angemessene Frist einräumen. Die Mängelliste und die Nachbesserungsfrist für die Korrekturmaßnahmen werden im Audit-Report dokumentiert.

Je nach Art der festgestellten Mängel 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 Mängel behoben wurden, und dokumentiert die Prüfungsergebnisse im Audit-Report.

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

Hinweis: Falls sich auch nach der Nachbesserung noch größere Defizite ergeben, ist keine weitere Nachbesserung durch den Antragsteller mehr möglich.

7.2 Nachforderungen

Ziel: Die Zertifizierungsstelle wird den Auditor kurzfristig über einen Termin für die Bearbeitung des Auditreports informieren. Inhaltliche, formale oder sonstige Nachforderungen zu dem Auditreport werden dem Auditor 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, z. B. wenn die Stichprobenauswahl der zu überprüfenden Bausteine nicht nachvollziehbar war.

Aktion: Der Auditor konkretisiert den Audit-Report und sendet diesen an die Institution und die Zertifizierungsstelle zur erneuten Prüfung.

Hinweis: Falls sich nach der ersten Nachforderung noch Defizite ergeben, sind weitere Nachforderungen des BSI an den Audit-Report 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**.

7.3 Schiedsstelle des BSI

Hat die Institution bezüglich festgestellter Mängel eine andere Auffassung als der Auditor, kann sie sich schriftlich zu dem vom Auditor dokumentierten Mangel äußern. Der Kommentar wird in die Mängelliste und den Audit-Report übernommen. Der Zertifizierungsstelle obliegt dann die Entscheidung, ob der Mangel behoben werden muss und innerhalb welcher Frist dies zu geschehen hat.

8 Gesamtvotum

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

Aktion: Der Auditor 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 Form umfassen:

"Aufgrund der durchgeführten Einzelprüfungen im Rahmen des IT-Grundschutz-Audits wird festgestellt, dass der Untersuchungsgegenstand die Anforderungen des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz (nicht) erfüllt." [*Nicht Zutreffendes bitte streichen.*]

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 Auditor-Testats?

Hinweis: Das Gesamtvotum ist vom Auditor mit Datum zu **unterschreiben**.

9 Auditierung im Rahmen einer Re-Zertifizierung

Ziel: Die Gültigkeit von ISO 27001-Zertifikaten ist auf 2 Jahre begrenzt. Sind in dieser Zeit wesentliche Änderungen (z. B. größere Umstrukturierungen, Fusion, Outsourcing, Wechsel des Outsourcing-Dienstleisters) am zertifizierten IT-Verbund aufgetreten, müssen der IT-Sicherheitsbeauftragte des Antragstellers diese dem 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 noch erfüllt sind.

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 erfüllen,
- dass durch den Wegfall von Komponenten, beispielsweise Paketfiltern, seit der vorhergehenden Zertifizierung die IT-Sicherheit des IT-Verbunds nicht beeinträchtigt wird,
- dass alle seit der vorhergehenden Zertifizierung neu hinzugekommenen Komponenten im IT-Verbund die Anforderungen des ISO 27001-Zertifikats erfüllen und
- dass die IT-Sicherheit 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. Der Auditor greift jedoch soweit wie möglich auf die Ergebnisse der vorhergehenden Auditierung zurück und konzentriert die Prüfungen auf die Veränderungen innerhalb des IT-Verbundes seit der letzten Auditierung. Die Institution sollte diese Veränderungen in den Referenzdokumenten, die dem Auditor zur Verfügung gestellt werden, hervorheben.

Votum: siehe Kapitel 4 bis 8.

10 Praktische Hilfen

10.1 Audit-Report

Der Audit-Report dokumentiert die Grundlagen, die Durchführung und die Ergebnisse der Auditierung. Der Audit-Report ist vom Auditor und vom Antragsteller zu unterzeichnen.

Auf der Grundlage des Audit-Reports wird über die Vergabe eines ISO 27001-Zertifikats entschieden.

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

10.2 Formale Aspekte des Audit-Reports

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 Audit-Report reproduzierbar und nachvollziehbar dokumentiert werden.

10.2.1 Allgemeines

- Das Inhaltsverzeichnis sollte sowohl den eigentlichen Report, als auch alle Anhänge umfassen. Jeder einzelne Abschnitt eines Anhangs muss identifizierbar sein, so dass die Vollständigkeit des Audit-Reportes und der Anhänge überprüft werden kann.
- Alle vom Auditor angeforderten Dokumente, insbesondere die Referenzdokumente A.1 bis A.3 sowie A.5 und A.6 sind Bestandteil des Audit-Reports 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, wenn im Audit-Report darauf verwiesen wird. Ausnahmen hiervon sind mit der Zertifizierungsstelle abzustimmen.
- Die Seitennummerierung muss so gestaltet werden, dass jede Seite eindeutig identifiziert werden kann.
- Wenn zur Unterstützung der Prüfaktivitäten Software-Tools verwendet werden, z. B. das GSTOOL oder Analyse-Tools, müssen diese Tools identifizierbar mit Namen und Versionsnummer genannt werden. Sofern im Audit-Report auf in diesen Tools erfasste Informationen verwiesen wird, müssen entsprechende Reports (Ausdrucke) als zusätzliche Aufzeichnungen beigelegt werden.
- Verwendete Fachbegriffe oder Abkürzungen, die nicht allgemein gebräuchlich sind, müssen in einem Glossar bzw. Abkürzungsverzeichnis zusammengefasst werden.

10.2.2 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 - z. B. A.1 - zu verweisen, es sind die konkreten Textpassagen anzugeben.

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 dargestellt werden.

c) Votum des Auditors

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

11 Auditor-Testat

11.1 Abgabe des Auditor-Testats

Wenn der IT-Grundschatz-Auditor im Audit-Report festgestellt hat, dass der betrachtete Untersuchungsgegenstand den Anforderungen eines Auditor-Testats (Einstiegsstufe oder Aufbaustufe) genügt, kann die Institution ein entsprechendes Auditor-Testat erhalten.

Das Auditor-Testat muss mindestens folgende Informationen umfassen:

- Name und Adresse der Institution,
- Name und Adresse des Auditors,
- ggf. Name und Adresse des Unternehmens, für das der Auditor tätig ist,
- Beschreibung des Untersuchungsgegenstands,
- Stufe des Auditor-Testats (Einstiegsstufe oder Aufbaustufe),
- Version der IT-Grundschatz-Methodik und der IT-Grundschatz-Kataloge (Monat, Jahr), auf deren Grundlage der Basis-Sicherheitscheck durchgeführt wurde,
- Beginn der Gültigkeit des Auditor-Testats (Ausstellungsdatum des Audit-Reports) und
- Ende der Gültigkeit des Auditor-Testats (nach 2 Jahre).

Die unabhängige Prüfung der Umsetzung der IT-Grundschatz-Methodik wird beim Auditor-Testat durch einen IT-Grundschatz-Auditor durchgeführt, der im Antrag 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 IT-Grundschatz-Audit durchgeführt. Ich bestätige, dass der Untersuchungsgegenstand die vom BSI festgelegten Anforderungen für das Auditor-Testat <Einstiegsstufe oder Aufbaustufe> der IT-Grundschatz-Qualifizierung erfüllt. <Datum>, <Unterschrift des Auditors>".

Der Audit-Report ist **nicht** beim BSI zur Prüfung einzureichen. Dem BSI ist auf Verlangen Einsicht in den Audit-Report zu gewähren.

11.2 Verlängerung eines Auditor-Testats

Auditor-Testate können nach Ablauf der maximal zweijährigen Gültigkeitsdauer nicht verlängert werden. Um die Qualifizierung fortzusetzen, muss stattdessen eine höhere Stufe im Qualifizierungsschema erreicht werden. Beim Auditor-Testat "Einstiegsstufe" bedeutet dies, dass nach Ablauf der Gültigkeit ein Auditor-Testat "Aufbaustufe" oder das ISO 27001-Zertifikat erreicht werden muss. Nach Ablauf der Gültigkeit des Auditor-Testats "Aufbaustufe" muss das ISO 27001-Zertifikat erreicht werden. Anderenfalls endet die Qualifizierung nach IT-Grundschatz.

12 Anhang

12.1 Anträge

Der Zertifizierungsantrag für die ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz ist unter <http://www.bsi.bund.de/gshb/zert/antraege.htm> veröffentlicht.

Ein Liste aller Auditoren, die Audits für die ISO 27001-Zertifizierung durchführen dürfen, ist unter <http://www.bsi.bund.de/gshb/zert/auditor.htm> veröffentlicht.

Für die Veröffentlichung der Auditor-Testat Einstigstufe bzw. Aufbaustufe ist der Antrag unter <http://www.bsi.bund.de/gshb/zert/antraege.htm> zu finden. Alle IT-Grundschutz-Auditoren und alle Auditoren für ISO 27001 sind berechtigt, diese Audits durchzuführen

12.2 Formular für die Unabhängigkeitserklärung des Auditors

Zu Beginn eines ISO 27001-Verfahrens ist, wie in Kapitel 3 beschrieben, eine Unabhängigkeitserklärung des Auditores bei der Zertifizierungsstelle einzureichen. Diese ist unter <http://www.bsi.bund.de/gshb/zert/antraege.htm> veröffentlicht.

12.3 Gliederung des Audit-Reports

1 Allgemeines

1.1 Qualifizierung/Zertifizierung nach IT-Grundschutz

An dieser Stelle soll die Zielsetzung, der Verfahrensablauf und die Funktion des Audit-Reports kurzer Form darstellt werden.

1.2 Auditerte Institution

An dieser Stelle werden die vollständigen Kontaktinformationen der auditerten Institution, einschließlich vollständiger Adresse und Benennung eines Ansprechpartners bzw. des Projektleiters, aufgeführt.

1.3 Auditor

An dieser Stelle werden die vollständigen Kontaktinformationen des Auditors, des Audit-Teams und ggf. der Erfüllungsgehilfen aufgeführt, d. h. vollständiger Name, postalische Erreichbarkeit am Arbeitsplatz, ggf. E-Mail-Adresse. 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 Auditors:

"Ich bin für die Durchführung von IT-Grundschutz-Audits beim BSI lizenziert. In den zurückliegenden zwei Jahren war ich und ggf. beteiligte Erfüllungsgehilfen im Umfeld des Untersuchungsgegenstands nicht beratend tätig. Die Ergebnisse des Audit-Reportes beruhen auf meinen eigenen Prüfungen, die ich weisungsfrei und unabhängig durchgeführt habe.

<Datum>, <Unterschrift des Auditors>"

Hat das Unternehmen, in dessen Auftrag der Auditor tätig ist, im Umfeld des Untersuchungsgegenstands Beratungsdienstleistungen erbracht, so sind diese an dieser Stelle zu vermerken. Die Dienstleistungen sind stichpunktartig aufzuführen.

1.4 Vertragsgrundlage

Grundlagen der Auditierung sind

- eine Vertragsvereinbarung des Antragstellers mit dem Auditor,
- ein gültiger Lizenzierungsvertrag des Auditors 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 IT-Verbundes in Bezug auf das Gesamtunternehmen muss dargestellt werden. Es kann die Darstellung des Untersuchungsgegenstands aus Anhang A.1 wiedergegeben werden.

1.6 Projektierung

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

- Beginn der Auditierung,
- Anzahl der Audit-Tage,
- Abgabe der Referenzdokumente,
- Sichtung der Referenzdokumente,
- Inspektion vor Ort,
- Prüfung der Nachbesserungen,
- Erstellung des Audit-Reports und
- Abschluss der Auditierung

enthalten sein.

1.7 Verteiler

An dieser Stelle wird aufgeführt, wem der Audit-Report vorgelegt wird. Dies umfasst in der Regel mindestens den Auditor, die auditierte Institution und die Zertifizierungsstelle (falls ein ISO 27001-Zertifikat angestrebt wird). Da der Audit-Report in den meisten Fällen vertrauliche Informationen enthält, wird dieses Kapitel mit folgendem Hinweis abgeschlossen:

"Der Inhalt dieses Audit-Reports 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 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 IT-Strukturanalyse

2.1.1 Nachvollziehbarkeit der Abgrenzung des IT-Verbunds

- 2.1.2 Aktualität der Version der Prüfgrundlagen
- 2.1.3 Identifizierbarkeit der Komponenten im bereinigten Netzplan
- 2.1.4 Umfang der Liste der IT-Systeme
- 2.1.5 Konformität der Liste der IT-Systeme mit dem Netzplan
- 2.1.6 Umfang der Liste der IT-Anwendungen
- 2.2 Schutzbedarfsfeststellung
 - 2.2.1 Plausibilität der Definition der Schutzbedarfskategorien
 - 2.2.2 Vollständigkeit der Schutzbedarfsfeststellung der IT-Anwendungen
 - 2.2.3 Vollständigkeit der Schutzbedarfsfeststellung der IT-Systeme
 - 2.2.4 Plausibilität der Schutzbedarfsfeststellung der IT-Systeme
 - 2.2.5 Kritikalität der Kommunikationsverbindungen
 - 2.2.6 Plausibilität der Schutzbedarfsfeststellung der IT-Räume
- 2.3 Modellierung des IT-Verbunds
 - 2.3.1 Nachvollziehbarkeit der Modellierung
 - 2.3.2 Anwendbarkeit der IT-Grundschutz-Methodik
 - 2.3.3 Korrektheit der Gruppenbildung
- 2.4 Ergebnis des Basis-Sicherheitschecks
 - 2.4.1 Konformität zur Modellierung
 - 2.4.2 Transparenz der Interviewpartner
 - 2.4.3 Umsetzungsgrad der IT-Grundschutz-Maßnahmen
- 2.5 Ergänzende Sicherheitsanalyse und Ergänzende Risikoanalyse
 - 2.5.1 Vollständigkeit und Plausibilität der Ergänzenden Sicherheitsanalyse
 - 2.5.2 Vollständigkeit und Plausibilität der Ergänzenden Risikoanalyse
 - 2.5.3 Umsetzungsgrad aller Maßnahmen

3 Vorbereitung der Auditoren-Tätigkeit

Hier wird insbesondere die Auswahl der Stichproben des Basis-Sicherheitschecks dokumentiert.

4 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 Verifikation des Netzplans
- 4.2 Verifikation der Liste der IT-Systeme
- 4.3 Verifikation des Basis-Sicherheitschecks
- 4.4 Verifikation der Umsetzung der zusätzlichen Maßnahmen

5 Nachbesserungen

In diesem Kapitel wird die Durchführung, Überprüfung und die Ergebnisse von Nachbesserungen in Bezug auf zuvor festgestellte Mängel oder Inkonsistenzen dargestellt. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 7 dieses Prüfplans aufgeführt.

6 Gesamtvotum

Dieses Kapitel enthält das Gesamtvotum des Auditors, ob der betrachtete Untersuchungsgegenstand die Anforderungen der ISO 27001-Zertifizierung bzw. die angestrebte Stufe der IT-Grundschutz-Qualifizierung erfüllt. Die Aktionen des Auditors und die zu dokumentierenden Informationen sind in Kapitel 8 dieses Prüfplans 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. Aus Gründen der Vertraulichkeit ist es dem Antragsteller freigestellt, ob er das Dokument A.4 *Ergebnis des Basis-Sicherheitschecks* der Zertifizierungsstelle zur Verfügung stellt. Mängel oder Inkonsistenzen, die der Auditor im Zusammenhang mit A.4 festgestellt hat, sind jedoch im Audit-Report dokumentiert.

- 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