



Muster mit Beispiel

Auditbericht des **Überwachungsaudits** im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT- Grundschutz

Auditierte Institution:

Zertifizierungskennung: BSI-000000000

Eine Anpassung der Deckblätter, Logo, Schrifttypen etc. kann durch den Auditor vorgenommen werden. Auch die Seite mit der Versionshistorie des Musters (Seite 5) kann im Auditbericht entfallen.

Der Inhalt dieses Überwachungsauditreportes ist „Firmenvertraulich“ und richtet sich ausschließlich an die in Kapitel 1.8 genannten Empfänger.

Bundesamt für Sicherheit in
der Informationstechnik

Referat B 21

Postfach 20 03 63

53133 Bonn

Tel.: +49 22899 9582- 6222

E-Mail: gszertifizierung@bsi.bund.de, Internet: <http://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2011

Inhaltsverzeichnis

1	Allgemeines.....	7
1.1	Versionshistorie.....	7
1.2	Auditierte Institution.....	7
1.3	Auditteam.....	8
1.4	Untersuchungsgegenstand.....	9
1.5	Audittyp.....	9
1.6	Prüfgrundlage des Auditberichts.....	9
1.7	Projektierung.....	9
1.8	Verteiler.....	10
1.9	Inhaltliche Grundlagen, Auskünfte und Nachweise.....	10
1.10	Toolbasierte Auditunterstützung.....	10
2	Erstellung eines Prüfplans.....	12
2.1	Sichtung der Referenzdokumente.....	12
2.2	Auswahl von Standorten.....	12
2.3	Prüfaspekte zur Wirksamkeit des ISMS.....	13
2.4	Prüfaspekte zu Änderungen am Informationsverbund.....	13
2.5	Prüfaspekte zu Abweichungen und Empfehlungen.....	14
2.6	Prüfaspekte zu Auflagen aus dem Zertifikat.....	15
2.7	Risiko orientierte Auswahl eines Baustein-Zielobjektes.....	15
2.8	Prüfaspekte zum Risikobehandlungsplan (A.7).....	15
3	Prüfergebnisse des Überwachungsaudit.....	17
3.1	Wirksamkeit des ISMS.....	17
3.2	Änderungen am Informationsverbund.....	18
3.3	Behebung der Abweichungen und Empfehlungen.....	18
3.4	Umsetzung/Einhaltung der Auflagen aus dem Zertifikat.....	19
3.5	Umsetzung der IT-Grundschutz-Bausteine.....	19
3.6	Umsetzung von Maßnahmen aus dem Risikobehandlungsplan (A.7).....	20
3.7	Nachbesserungen zur Vor-Ort-Prüfung des Überwachungsaudits.....	21
4	Umsetzungsprüfung im Überwachungsaudit.....	23
4.1	Überprüfung der Wirksamkeit des ISMS.....	23
4.2	Überprüfung der Änderungen am Informationsverbund.....	24
4.3	Umsetzungsprüfung der Abweichungen und Empfehlungen.....	25
4.4	Prüfung der Einhaltung von Auflagen.....	25
4.5	Umsetzung des ausgewählten IT-Grundschutzbausteins.....	25
4.6	Umsetzung von Maßnahmen aus dem Risikobehandlungsplan A.7.....	26
5	Gesamtvotum.....	27
5.1	Empfehlung an die Zertifizierungsstelle.....	27

Versionshistorie des Musters:

Datum	Version	Verfasser	Bemerkungen
22.02.11	1.0	BSI	
30.03.11	1.1	BSI	Anpassungen nach Kommentierung durch die Auditoren
20.06.11	1.2	BSI	Fehlerkorrektur und Überarbeitung

1 Allgemeines

Ziel des jährlichen Überwachungsaudits ist es, während der dreijährigen Zertifikatsdauer, die Aufrechterhaltung und Verbesserung des zertifizierten Informationsverbundes nachzuweisen.

Das angewandte Prüfverfahren richtet sich dabei nach den Vorgaben des BSI, die im Zertifizierungsschema für ISO 27001-Audits festgelegt sind.

Im vorliegenden Auditbericht sind die Ergebnisse der Prüfungen dokumentiert. Der Auditbericht endet mit einem Votum, ob die Organisation bzw. deren ISMS weiterhin geeignet ist, das Zertifikat nach ISO 27001 auf Basis von IT-Grundschutz aufrecht zu erhalten.

Hinweis: Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit. Die hinterlegten Textteile sind Beispiele für das Ausfüllen des Musterberichtes.

Die Formulierungen bzw. Fragen im Musterauditreport dürfen vom Auditor nicht abgeändert werden, damit die Vergleichbarkeit der Ergebnisse gewährleistet bleibt.

Im Feld „Votum“ erfasst der Auditor eine zusammenfassenden Erläuterung seiner Prüfungsergebnisse. Ist ein Prüfschritt nicht erforderlich, z. B. weil ein entsprechendes Referenzdokument nicht vorliegt - vgl. Kapitel 2.8 Prüfaspekte zum Risikobehandlungsplan (A.7) - vermerkt der Auditor dies im Feld „Votum“

1.1 Versionshistorie

Datum	Version	Verfasser	Bemerkungen
15.03.11	1.0	Auditor	1. Version des Überwachungsauditreportes

1.2 Audierte Institution

Kontaktinformationen des Antragstellers (audierte Institution):

Institution:	
Straße:	

PLZ, Ort:	
-----------	--

Ansprechpartner für die Zertifizierung beim Antragsteller:

Name:	
Funktion:	
Telefon:	
E-Mail:	
abweichende Anschrift:	

1.3 Auditteam

Die Auditteamleitung erfolgte durch folgenden vom BSI zertifizierten Auditor:

Name:	
Institution:	
Zertifizierungs- bzw. Lizenzierungs- nummer:	
Straße:	
PLZ, Ort:	
E-Mail:	

Folgende Auditoren / Erfüllungsgehilfen haben an der Auditierung mitgewirkt:

Funktion	Name, Institution, Zertifizierungsnummer, Anschrift, E-Mail

- Für jedes Auditteammitglied liegt der Zertifizierungsstelle eine Unabhängigkeitserklärung vor.

1.4 Untersuchungsgegenstand

Kurzbezeichnung:

Kurzbeschreibung des Informationsverbundes¹:

1.5 Audittyp

Es handelt sich bei dem durchgeführten Audit um das:

- 1. Überwachungsaudit
- 2. Überwachungsaudit

1.6 Prüfgrundlage des Auditberichts

Das vorliegende Audit wurde auf Basis des folgenden Schemas durchgeführt:

- Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits (Version 2.1)
- Zertifizierungsschema (Version 1.0)

Als Vorlage für diesen Auditbericht diente das Muster für Überwachungsaudits, Version 1.2.

1.7 Projektierung

In diesem Kapitel wird der zeitliche Ablauf des Überwachungsaudits in tabellarischer Form aufgeführt.

Audit-Phasen	Zeitraum (Datum) / Aufwand (Anzahl PT)
Beginn der Auditierung Dokumentenprüfung und Erstellung des Prüfplans	Datum:
	PT:
Inspektion vor Ort	Datum:
	PT:

¹ Die Beschreibung des Untersuchungsgegenstands ist dem Zertifikat zu entnehmen. Sollten Änderungen erforderlich sein, ist dies zu begründen.

Audit-Phasen	Zeitraum (Datum) / Aufwand (Anzahl PT)
Erstellung des Auditberichts	Datum:
	PT:
Abschluss der Auditierung	Datum:

1.8 Verteiler

Der Inhalt dieses Auditreports ist vertraulich und richtet sich nur an die genannten Empfänger.

Der Auditteamleiter versendet den Auditreport an folgende Stellen:

Stelle	Kurzbezeichnung	Anschrift, Ort	Datum	Bemerkungen
S.1	BSI	Godesberger Allee 185-189, 53175 Bonn		
S.2	Antragsteller			
S.3	Ggf. Auditor x			

1.9 Inhaltliche Grundlagen, Auskünfte und Nachweise

Eine Liste der Referenzdokumente wurde vom Antragsteller erstellt. Für jedes Referenzdokument ist vom Antragsteller zusammenfassend herauszustellen, welche wesentlichen Veränderungen sich gegenüber der vorhergehenden Version ergeben haben. Die geänderten Referenzdokumente müssen dem Auditteam als Arbeitsgrundlage zur Verfügung gestellt werden. Darüber hinausgehende wesentliche Änderungen am Informationsverbund (z. B. Änderungen der Geschäftsprozesse, Wechsel des Dienstleisters usw.) sind zusätzlich in die Liste mit aufzunehmen.

Die Liste der Referenzdokument mit allen wesentlichen Änderungen liegt diesem Überwachungsauditreport als Anlage bei.

- Liste der Referenzdokumente als Anlage

1.10 Toolbasierte Auditunterstützung

Folgende Tools wurden zur Unterstützung der Auditaktivitäten verwendet:

Tool: GSTOOL

Versionsnummer: 4.7

Stand der Grundschatzkataloge: 2009100011 (11. EL)

2 Erstellung eines Prüfplans

Für ein Überwachungsaudit muss der Auditor im Vorfeld seiner Vor-Ort-Prüfung einen Prüfplan erstellen. Der Umfang des Vor-Ort-Audits sollte angemessen sein und **mindestens 2-3 Personentage** umfassen, um einen Status über den ISMS-Prozessen zu erhalten. Die Dokumentation der Ergebnisse dieser Prüfungen erfolgt im Kapitel 4 dieses Dokuments. Der gesamte Prüfprozess des Überwachungsaudits soll insgesamt ca. ein Drittel des Erstzertifizierungsaudits umfassen.

2.1 Sichtung der Referenzdokumente

Auf der Grundlage der Liste der Referenzdokumente des Antragstellers, welche Veränderungen sich gegenüber der vorhergehenden Version ergeben haben, wird überprüft, ob die geänderten Referenzdokumente vollständigen als Arbeitsgrundlage zur Verfügung gestellt wurden und ob diese aktuell sind. Insbesondere ist die Anwendung der gültigen Version der Grundschutz-Kataloge nachzuvollziehen

(<https://www.bsi.bund.de/grundschutz/zert/ISO27001/Schema/zertifizierungsschema.html>).

<i>Fragestellung:</i>	<i>Feststellung:</i>
Liegt eine vollständige Liste der Referenzdokumente für die Vorbereitung und Planung des Überwachungsaudits vor?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Sind Veränderungen des letzten Jahres in die Dokumentation eingeflossen?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Wurden die aktuellen Prüfgrundlagen verwendet? Sind Änderungen der Grundschutzkataloge bzw. der IT-Grundschutz-Methodik in die Dokumentation eingeflossen?	<input type="checkbox"/> Ja, Version siehe Votum
	<input type="checkbox"/> Nein
<i>Votum:</i>	

2.2 Auswahl von Standorten

Im Rahmen der Auditierung ist eine Begutachtung der Standorte des Informationsverbunds erforderlich. Der Auditor dokumentiert die Standorte und begründet seine Auswahl unter Berücksichtigung der im Audit bzw. im 1. Überwachungsaudit getroffenen Auswahl der Standorte.

Nachfolgende Tabelle aus dem letzten Audit ist fortzuschreiben.

Auswahl von Standorten

<i>Bezeichnung der Standorte</i>	<i>Hinweise zur Gruppenbildung/</i>	<i>Begründung für die Risiko orientierte Auswahl</i>
Standort 1		
....		
<i>Anmerkungen zur Auswahl:</i>	-	

- Alternativ ist die Liste der Standorte als Anlage <Nummer> beigefügt.

2.3 Prüfaspekte zur Wirksamkeit des ISMS

Ziel des Überwachungsaudits ist es, die Wirksamkeit des ISMS für den Informationsverbund zu überprüfen. Hierbei ist zu hinterfragen, ob durch einen Verbesserungsprozess (KVP) die Informationssicherheit aufrechterhalten bzw. verbessert werden konnte.

Durch Stichproben über alle Schichten des IT-Grundschutzes ist zu prüfen, ob die Einhaltung der technischen Sicherheitsmaßnahmen (z. B. hinsichtlich der Konfiguration) und die der organisatorischen Regelungen (z. B. Prozesse, Verfahren und Abläufe) funktionieren. Relevante Prüfaspekte können hierzu den Hilfsmitteln (H100_Anlage_Prüfthemen) entnommen werden.

Der Prüfumfang umfasst Prüfaspekte **aller** Prüfthemen, die für den Informationsverbund relevant sind, des Dokumentes H100_Anlage_Prüfthemen. Die Prüftiefe liegt dabei auf der Ebene der Prüfaspekte, die Themen sind **nicht** auf Bausteine bzw. Maßnahmen herunterzubrechen.

2.4 Prüfaspekte zu Änderungen am Informationsverbund

Auf der Basis der Änderungszusammenstellung des Antragstellers legt der Auditor spezielle Prüfaspekte fest. Dabei sollte ein ganzheitlicher und Risiko orientierter Ansatz gewählt werden, um die Umsetzung und Auswirkungen der **wesentlichen** Änderungen im Informationsverbund nachzuvollziehen zu können. Falls erforderlich, sind auch Änderungen der Dokumentation Vor-Ort zu sichten.

Auswahl spezielle Prüfaspekte zu den Änderungen:

<i>Schicht:</i>	<i>Prüfaspekt:</i>	<i>Änderung:</i>
Übergeordnete	Sicherheitsorganisation	Neuer IT-SiBe ernannt

<i>Schicht:</i>	<i>Prüfaspekt:</i>	<i>Änderung:</i>
<i>Aspekte</i>	<ul style="list-style-type: none"> • Qualifizierung IT-SiBe ... 	
Infrastruktur	Referenzdokumente prüfen einschließlich Begehung	zusätzlicher Serverraum (S 38)
IT-Systeme		
Netze		
Anwendungen		
<i>Anmerkungen zur Auswahl:</i>	-	

2.5 Prüfaspekte zu Abweichungen und Empfehlungen

Der Auditor überführt die im letzten Audit festgestellten offenen Punkte (Abweichungen bzw. Empfehlungen) in dieses Dokument. Diese Liste wird im Rahmen des Überwachungsaudits fortgeschrieben (siehe 3.3 Behebung der Abweichungen und Empfehlungen).

Liste der Abweichungen und Empfehlungen

<i>Lfd. Nr.</i>	<i>Offene Punkte</i>	<i>Abweichungstyp (E/AG/AS)</i>	<i>Behebung sfrist</i>	<i>Status der Behebung</i>
1	Verweis Auditfeststellung Verweis Referenzdokument Beschreibung	AG	01/ ...	Kommentar ...

Alternativ ist die Liste der Abweichungen und Empfehlungen als Anlage <Nummer> beigefügt.

2.6 Prüfaspekte zu Auflagen aus dem Zertifikat

Wurde das Zertifikat mit Auflagen erteilt (vgl. Kap. 2.11 Zertifizierungsschema), legt der Auditor Prüfaspekte fest, um deren Einhaltung zu verifizieren.

2.7 Risiko orientierte Auswahl eines Baustein-Zielobjektes

Diese Prüfung **entfällt**, wenn bereits 10 Baustein-Zielobjekte im letzten Zertifizierungsaudit (Erst- bzw. Re-Zertifizierung) geprüft wurden.

Der Auditteamleiter wählt **Risiko orientiert** ein Baustein-Zielobjekte aus der aktuellen Modellierung A3 des Antragstellers aus.

Auswahl Baustein-Zielobjekt:

<i>Bausteinname:</i>	<i>Begründung der Auswahl:</i>
B 1.10 Outsourcing Zielobjekt: gesamte Institution	

2.8 Prüfaspekte zum Risikobehandlungsplan (A.7)

Für eine kontinuierliche Verbesserung des ISMS ist es erforderlich, die vom Management getragenen Restrisiken zu reduzieren. Im Überwachungsaudit ist der Fortschritt der Umsetzung der dokumentierten Maßnahmen zu verifizieren. Hierzu wählt der Auditor eine Stichprobe aus.

<i>Fragestellung:</i>	<i>Feststellung:</i>
Wurden Maßnahmen gemäß Umsetzungsplan für die Reduzierung des Informationssicherheitsrisikos umgesetzt?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
<i>Votum:</i>	

<i>Lfd. Nr.</i>	<i>Auswahl der zu prüfenden Maßnahmen</i>
1	
2	
3	

3 Prüfergebnisse des Überwachungsaudit

Die Ergebnisse der Umsetzungsprüfung des Überwachungsaudits werden vom Auditor zusammengefasst und anhand der folgenden Fragestellungen bewertet und mit einem Votum zu den Einzelprüfungen geschlossen. Das Votum bezieht sich auf den Stand einer möglichen Nachbesserung durch den Antragsteller.

Die Historie über die festgestellten Abweichungen aus dem vorherigen Audit bzw. Überwachungsaudit ist im Kapitel 3.7 fortzuführen.

Die detaillierten Prüfergebnisse sind im Kapitel 4 oder einem separaten Prüfprotokoll zu erfassen. Die geforderten Begründungen fasst der Auditor im Votum zusammen, dabei kann er auf die detaillierten Prüfergebnisse referenzieren.

3.1 Wirksamkeit des ISMS

Das Sicherheitsmanagementsystem des Informationsverbunds muss effektiv und effizient sein. Es muss stetig weiterentwickelt werden und von allen beteiligten Personen aktiv gelebt werden. Dazu gehört auch, dass alle wichtigen Prozesse des Informationsverbundes dokumentiert sind, umgesetzt werden und das System kontinuierlich weiter verbessert wird.

<i>Fragestellung:</i>	<i>Feststellung:</i>
Ist das ISMS effektiv und effizient im Einsatz (Interview, Gesamteindruck)?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Wird der PDCA-Zyklus gelebt und wird das ISMS kontinuierlich verbessert?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Ist das Beschwerdemanagement im ISMS aktiv?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Liegen Managementbewertungen vor ?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Wird die Verantwortung für das ISMS vom Management getragen?	<input type="checkbox"/> Ja,
	<input type="checkbox"/> Nein
Wurden interne Audits durchgeführt?	<input type="checkbox"/> Ja

<i>Fragestellung:</i>	<i>Feststellung:</i>
	<input type="checkbox"/> Nein
<i>Votum:</i>	

3.2 Änderungen am Informationsverbund

Es muss sichergestellt sein, dass Änderungen am zertifizierten Informationsverbund keine Auswirkungen auf die Aufrechterhaltung des Zertifikats haben.

<i>Fragestellung:</i>	<i>Feststellung:</i>
Erfordern Änderungen am Informationsverbund eine Re-Zertifizierung?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Sind die Änderungen in der Dokumentation des Sicherheitskonzeptes kontinuierlich eingeflossen?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Sind die dokumentierten Änderungen gemäß IT-Grundschutz-Vorgehensweise (BSI 100-2) und IT-Grundschutz-Katalogen umgesetzt?	<input type="checkbox"/> Ja,
	<input type="checkbox"/> Nein
Wird durch den Wegfall von Komponenten aus dem Informationsverbund die Sicherheit beeinträchtigt?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Wird die Sicherheit durch geänderte oder hinzugefügte Komponenten beeinträchtigt?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
<i>Votum:</i>	

3.3 Behebung der Abweichungen und Empfehlungen

Im Überwachungsaudit muss überprüft werden, ob die im Audit bzw. im 1. Überwachungsaudit festgestellten Abweichungen und Empfehlungen (siehe Liste der Abweichungen und Empfehlungen) umgesetzt wurden. Dabei müssen nicht alle Empfehlungen aus dem Audit umgesetzt sein, es ist aber aufzuzeigen, dass das Verbesserungspotenzial durch die Empfehlungen berücksichtigt wurde. Eine Empfehlung, der nicht in adäquater Form nachgegangen wurde, sollte zu einer geringfügigen Abweichung führen.

<i>Fragestellung:</i>	<i>Feststellung:</i>
Gab es im vorhergehenden Auditbericht Abweichungen bzw. Empfehlungen?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Sind alle Abweichungen fristgerecht behoben worden?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Wurden alle Empfehlungen angemessen berücksichtigt?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
<i>Votum:</i>	

3.4 Einhaltung der Auflagen aus dem Zertifikat

<i>Fragestellung:</i>	<i>Feststellung:</i>
Gibt es Auflagen an den Antragsteller aus dem Zertifizierungsreport?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein, weiter
Wurden die Auflagen eingehalten?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
<i>Votum:</i>	

3.5 Umsetzung der IT-Grundsicherheits-Bausteine

Für den risikoorientierten Baustein ist die Umsetzung aller geforderten IT-Grundsicherheitsmaßnahmen zu überprüfen.

<i>Fragestellung:</i>	<i>Feststellung:</i>
Stimmt der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der Maßnahmen mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts überein?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
	<input type="checkbox"/> Ja

<i>Fragestellung:</i>	<i>Feststellung:</i>
Ist die Begründung der „entbehrlichen“ Maßnahmen zulässig und nachvollziehbar?	<input type="checkbox"/> Nein
Sind alle Maßnahmen mit dem Umsetzungsstatus „teilweise“ oder „nein“ im Referenzdokument A.7 Risikobehandlungsplan?	<input type="checkbox"/> Ja,
	<input type="checkbox"/> Nein
<i>Votum:</i>	

3.6 Umsetzung von Maßnahmen aus dem Risikobehandlungsplan (A.7)

Es ist zu prüfen, ob die im Risikobehandlungsplan (A.7) aufgeführten Maßnahmen gemäß Umsetzungsplan bearbeitet wurden.

<i>Fragestellung:</i>	<i>Feststellung:</i>
Gibt es durch das Management getragene Restrisiken?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein, weiter
Wurden die getragenen Risiken seit der letzten Auditierung reduziert?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
Hat das Management den verbleibenden Restrisiken, durch Unterschrift, zugestimmt?	<input type="checkbox"/> Ja,
	<input type="checkbox"/> Nein
Sind die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar?	<input type="checkbox"/> Ja
	<input type="checkbox"/> Nein
<i>Votum:</i>	

3.7 Nachbesserungen zur Vor-Ort-Prüfung des Überwachungsaudits

Ergeben sich im Überwachungsaudit weitere Abweichungen bzw. Empfehlungen, so ist die Liste der Abweichungen und Empfehlungen aus dem letzten Audit bzw. 1. Überwachungsaudits fortzuschreiben und im nächsten Überwachungsaudit bzw. Re-Zertifizierungsaudit zu verwenden.

Zu jedem Prüfpunkt sind folgende Kritikpunkte zulässig:

- *Empfehlung (E)*,
- *geringfügige Abweichung (AG)*,
- *schwerwiegende Abweichung (AS)*.

Die Kritikpunkte werden durchnummeriert:

- E-lfdNr.
- AG-lfdNr.
- AS-lfdNr.

Der Auditteamleiter beschreibt die Abweichung bzw. Empfehlung **kurz** und referenziert für die näheren Details auf die Umsetzungsprüfung. Für jede Abweichung wird eine Frist festgelegt, in der sie beseitigt werden sollte, spätestens bis zum nächsten Audit. Zusätzlich ist festzulegen, in welcher Form die Institution den Nachweis gegenüber dem Auditorteamleiter zu erbringen hat. Hier kann der Auditteamleiter z. B. interne Protokolle, Beschaffungsbelege etc. anfordern. Die detaillierte Prüfung der Umsetzung erfolgt in jedem Fall im nächsten Audit. Solange bleibt der „Status der Behebung“ noch offen.

Liste der Abweichungen und Empfehlungen:

Lauf. Nr.	Abweichung	Abweichungstyp (E/AG/AS)	Behebungs- frist/ Nach- weis	Status der Behebung
1	AG-1 Verweis Auditfeststellung Verweis Referenzdokument kurze Beschreibung	AG-1.: eine geringfügige Abweichung	01/ Protokoll	Kommentar Protokoll wurde am 19.01.10 eingereicht Korrekt

Bei der Umsetzungsprüfung im nachfolgenden Audit dokumentiert der Auditor zu jeder Empfehlung und Abweichung den Status der Behebung. Dabei kann es zu folgenden Feststellungen kommen:

- **Korrekt:** alles ist vollständig und fristgerecht umgesetzt,
- **Teilweise:** es gibt einzelne Prüfpunkte, die nicht oder unzureichend umgesetzt sind oder betrachtet wurden. Die Abweichung bleibt bestehen oder eine Empfehlung führt zu einer geringfügigen Abweichung. Es wird eine neue lfdNr. vergeben und auf die alte Nummer referenziert.
- **Mangelhaft:** geringfügige Abweichungen sind nicht fristgerecht oder unzureichend behoben, es kommt zu schwerwiegenden Abweichungen. Der Auditor setzt eine angemessene Frist zur Behebung, wird der Mangel nicht fristgerecht behoben, wird das Zertifikat von der Zertifizierungsstelle ausgesetzt oder entzogen.

4 Umsetzungsprüfung im Überwachungsaudit

Die Überprüfung des Umsetzungsstatus durch den Auditor ist zu dokumentieren. Dabei kann das unten angegebene Muster dienen. Alternativ kann der Auditor auch individuelle Prüfprotokolle verwenden, diese müssen aber alle wesentlichen Informationen in geeigneter Form enthalten.

Folgende Prüfmethoden sind bei der Umsetzungsprüfung anzuwenden und zu dokumentieren:

- (D) Dokumentationsprüfung (der Dokumente des Sicherheitskonzeptes A0- A7)
- (I) Interviews und Befragungen
- (C) Inaugenscheinnahme z. B. Begehung, Einsicht in Konfigurationen usw.
- (S) Durchsicht von Unterlagen, z. B Richtlinien, Anweisungen usw.
- (A) Analyse und ggf. Verwertung von Unterlagen Dritter, z. B. Protokolle oder Verträge
- (B) Beobachtung von Aktivitäten und Arbeitsabläufen

Jeder Prüfaspekt ist insgesamt vom Auditteamleiter zu bewerten, dabei kann es zu einer der folgenden **Feststellungen** kommen:

- **Korrekt:** alles ist vollständig und fristgerecht umgesetzt,
- **Teilweise:** es gibt einzelne Prüfpunkte, die nicht oder unzureichend umgesetzt sind, hieraus folgt eine geringfügige Abweichung oder eine Empfehlung (Referenz auf die Liste der Abweichungen und Empfehlungen).
- **Mangelhaft:** es kommt zu schwerwiegenden Abweichungen (Referenz auf die Liste der Abweichungen und Empfehlungen). Der Auditor setzt eine angemessene Frist zur Behebung, wird der Mangel nicht fristgerecht behoben, wird das Zertifikat von der Zertifizierungsstelle ausgesetzt oder entzogen.

Werden im Auditierungsschema oder in diesem Dokument Forderungen hinsichtlich Anzahl oder Umfang von durchzuführenden Prüfungen vorgegeben, so sind dies Mindestanforderungen. Dem Auditor ist es freigestellt, den Umfang der Prüfungshandlungen zu erweitern.

4.1 Überprüfung der Wirksamkeit des ISMS

Es sollte geprüft werden, ob die Einhaltung der technischen Sicherheitsmaßnahmen (z. B. hinsichtlich der Konfiguration) und die der organisatorischen Regelungen (z. B. Prozesse, Verfahren und Abläufe) funktionieren. Die Prüfaspkte sollten daher Stichproben über alle Schichten des IT-Grundschatzes enthalten. Der Rahmen der Stichproben ist dabei durch die Prüfung aller Prüfthemen festgelegt.

Prüfthema: Schicht: Bezogen auf Zielobjekt/ ggf. Standort (bei unterschiedlichen Standorten):		
Auditiert am: Auditor(en):		
Nr.	Prüfaspekt	Feststellung
		Korrekt
Prüfmethode: (I), (S), (A), ... Auditfeststellung im Detail mit Nachweisen		

4.2 Überprüfung der Änderungen am Informationsverbund

Spezieller Prüfaspekt zu den Änderungen Bezogen auf Zielobjekt/ ggf. Standort:			
Interviewpartner:			
Nr.	Prüfaspekt	Änderung	Feststellung
			Teilweise Abweichung AG_X
Prüfmethode: (I), (S), (A), ... Auditfeststellung im Detail mit Nachweisen			

4.3 Umsetzungsprüfung der Abweichungen und Empfehlungen

Abweichung:			
Bezogen auf Zielobjekt/ ggf. Standort:			
Interviewpartner:			
Lauf. Nr.	Abweichung	Status der Behebung	Feststellung
Prüfmethode: (I), (S), (A), ...			
Auditfeststellung im Detail mit Nachweisen ...			

4.4 Prüfung der Einhaltung von Auflagen

Beschreibung der Auflage:
Interviewpartner:
Prüfmethode: (I), (S), (A), ...
Auditfeststellung im Detail mit Nachweisen ...

4.5 Umsetzung des ausgewählten IT-Grundschutzbausteins

Maßnahme			
Interviewpartner:			
Nr.	Maßnahme	Umsetzungs- status	Feststellung
Prüfmethode: (I), (S), (A), ...			
Auditfeststellung im Detail mit Nachweisen ...			

Maßnahme
.....

4.6 Umsetzung von Maßnahmen aus dem Risikobehandlungsplan A.7

Maßnahmen			
Bezogen auf Zielobjekt:			
Interviewpartner:			
Nr.	Maßnahme	Umsetzungs-zeitpunkt	Feststellung
Prüfmethode: (I), (S), (A), ...			
Auditfeststellung im Detail mit Nachweisen ...			
.....			

5 Gesamtvotum

5.1 Empfehlung an die Zertifizierungsstelle

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

Der Auditteamleiter 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. D. h. es gibt keine schwerwiegenden Abweichungen oder eine Häufung von geringfügigen Abweichungen (siehe Kapitel 3.7 Liste der Abweichungen und Empfehlungen). 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.

Gesamteinschätzung und Begründung:

Votum:

Aufgrund der durchgeführten Einzelprüfungen im Rahmen des Überwachungsaudits wird festgestellt, dass der Untersuchungsgegenstand die Anforderungen einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz weiterhin erfüllt / nicht erfüllt.

Datum

Unterschrift des Auditteamleiters