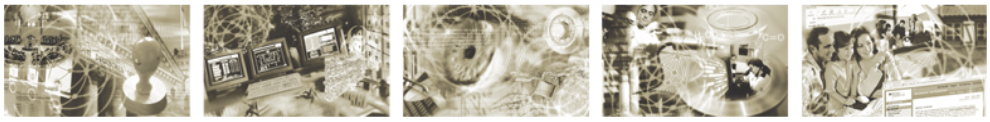
Bundesamt
für Sicherheit in der
Informationstechnik



Muster mit Beispiel

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

Auditierte Institution:

Zertifizierungskennung: BSI-XXX-XXXX

Der Inhalt dieses Auditreports ist „Firmenvertraulich“ und richtet sich ausschließlich an die in Kapitel 1.7 genannten Empfänger.

Bundesamt für Sicherheit in der Informationstechnik
Referat 114
Postfach 20 03 63
53133 Bonn

Tel.: +49 22899 9582- 5369
E-Mail: gszertifizierung@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

Versionshistorie des Musters

Datum	Version	Verfasser	Bemerkungen
17.03.11	1.0	BSI	

1 Allgemeines

Ziel dieser Zertifizierung ist es, die Erreichung der Sicherheitsziele der Organisation und die Korrektheit und Vollständigkeit der Umsetzung der Sicherheitsmaßnahmen zu prüfen, zu bewerten und zu dokumentieren.

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

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.

Im vorliegenden Auditbericht sind die Ergebnisse der Prüfungen dokumentiert. Darüber hinaus wird durch die Auditoren ein Votum abgegeben, ob die Organisation bzw. deren ISMS generell geeignet ist, durch die Zertifizierungsstelle des BSI ein Zertifikat nach ISO 27001 auf Basis von IT-Grundschutz erteilt zu bekommen.

ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz geben Behörden und Unternehmen die Möglichkeit, ihre Bemühungen um Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen zu dokumentieren.

Rechtliche Grundlagen des Verfahrens sind das Errichtungsgesetz des Bundesamts für Sicherheit in der Informationstechnik sowie entsprechende Erlasse des Bundesministeriums des Innern vom 06. Februar 2001 und vom 22. Dezember 2005 zum Zertifizierungsschema im Bereich IT-Grundschutz. Grundlage dieses Dokumentes sind die Normen DIN EN ISO 19011 "Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen", ISO/IEC 27006:2007 „Information technology – Security techniques - Requirements for bodies providing audit and certification of information security management systems“ sowie DIN EN ISO/IEC 17021:2006 "Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren", welche Anleitungen und Anforderungen für den Ablauf und die Durchführung von Audits enthalten.

Kriterienwerke des Verfahrens sind ISO/IEC 27001:2005 "Information technology – Security techniques - Information security management systems – Requirements", der BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“, BSI-Standard 100-3 „Ergänzende Risikoanalyse auf Basis von IT-Grundschutz“ sowie die IT-Grundschutz-Kataloge des BSI.

Hinweise:

- 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. Ergeben sich aus der Feststellung des Auditors Abweichungen zu den Prüfgrundlagen, sind diese im Feld „Votum“ zu dokumentieren. Anmerkungen des Auditors können in diesem Feld mit erfasst werden.

1.1 Versionshistorie

Datum	Version	Verfasser	Bemerkungen
15.03.11	1.0	Auditor	

1.2 Auditierte Institution

Kontaktinformationen des Antragstellers (auditierte Institution):

Institution:	
Straße:	
PLZ:	Ort:
E-Mail:	

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. Lizenzierungsnummer:	
Straße:	
PLZ:	Ort:
E-Mail:	

Folgende Auditoren / Erfüllungsgehilfen haben an der Auditierung mitgewirkt:

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

☐ Für jedes Mitglied des Auditteams liegt der Zertifizierungsstelle eine Unabhängigkeitserklärung vor.

1.4 Untersuchungsgegenstand

Die nachfolgenden Daten sind dem Zertifizierungsantrag zu entnehmen. Die Langbeschreibung prüft der Auditor inhaltlich und stimmt diese – sofern erforderlich – mit dem Antragsteller ab. Beide Angaben werden für den Zertifizierungsreport benötigt.

Kurzbezeichnung:	
Langbeschreibung:	

1.5 Audittyp

Es handelt sich bei dem durchgeführten Audit um ein:

- ❑ ▪ Zertifizierungsaudit
- ❑ Re-Zertifizierungsaudit

1.6 Auditprojektierung

In diesem Kapitel wird der zeitliche Ablauf der Auditierung in tabellarischer Form aufgeführt. Der Plan enthält die Anzahl der benötigten Audittage (gegliedert in Tage zur Dokumentenprüfung, Tage für die Durchführung eines Voraudits, Tage für die Vor-Ort-Prüfung und Tage zur Erstellung des Auditberichts; ohne Reisezeiten).

Audit-Phasen	*Zeitraum (Datum)/ Aufwand (Anzahl PT)*
Voraudit (nur bei Erst-Zertifizierung)	Datum: TT.MM.JJJJ – 01.02.2xxx
	PT: X Tage
Sichtung der Referenzdokumente	Datum: TT.MM.JJJJ – 01.02.2xxx
	PT: X Tage

Audit-Phasen		*Zeitraum (Datum)/ Aufwand (Anzahl PT)*
	Inspektion vor Ort	Datum: TT.MM.JJJJ – 01.02.2xxx
		PT: X Tage
	Prüfung der Nachbesserungen	Datum: TT.MM.JJJJ – 01.02.2xxx
		PT: X Tage
	Erstellung des Auditberichts	Datum: TT.MM.JJJJ – 01.02.2xxx
		PT: X Tage
	Nachforderungen der Zertifizierungsstelle	Datum: TT.MM.JJJJ – 01.02.2xxx
	Bearbeitung der Nachforderungen und ggf. Nachbesserungen durch den Antragsteller	Datum: TT.MM.JJJJ – 01.02.2xxx
	Abschluss der Auditierung	Datum: TT.MM.JJJJ

1.7 Verteiler

Der Audit-Teamleiter 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			
S...				

Der Inhalt dieses Auditreports ist vertraulich und richtet sich nur an oben genannte Empfänger.

1.8 Formale Grundlagen der Auditierung

Die nachfolgende Liste enthält die formalen Grundlagen für die Prüfungshandlungen und die Erstellung des Auditberichtes durch den Audit-Teamleiter.

Dokument	*Bezeichnung*	*Version, Datum*
F.1	ISO 27001-Grundschutz-Zertifizierungsschema (PDF)	V.2.1 , 03/08

Dokument	*Bezeichnung*	*Version, Datum*
F.2	ISO 27001-Grundschutz-Auditierungsschema (PDF)	
F.3	DIN EN ISO 19011 "Leitfaden für Audits von Qualitätsmanagement- und/oder Umweltmanagementsystemen"	
F.4	ISO/IEC 27006:2007 „Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems“	
F.5	DIN EN ISO/IEC 17021:2006 "Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren"	
F.6	ISO/IEC 27001:2005 "Information technology - Security techniques - Information security managementsystems – Requirements"	
F.7	BSI-Standard 100-1 „Managementsysteme für Informationssicherheit (ISMS)“	Version 1.5, (05/08)
F.8	BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“	Version 2.0, (05/08)
F.9	BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“	Version 2.5, (05/08)
F.10	IT-Grundschutz-Kataloge des BSI	(Version/) Nummer. Ergänzungslieferung

1.9 Vertragsgrundlagen

Dokument	*Bezeichnung*	*Datum*
V.1	Vertragsvereinbarung (Beauftragung) des Antragstellers (als zu auditierende Institution) mit dem Auftragnehmer (als Arbeitgeber des Auditleiters)	TT.MM.JJJJ
V.2	Zertifizierungsantrag des Antragstellers, abgenommen vom BSI am ...	TT.MM.JJJJ
V.x	...	

1.10 Inhaltliche Grundlagen

Die nachfolgende Tabelle ist vom Antragsteller zusammen mit den Referenzdokumente an den Audit-Teamleiter zu übergeben. Die darin genannten Referenzdokumente müssen von dem

Antragsteller dem Audit-Team als Arbeitsgrundlage zur Verfügung gestellt werden und bilden die Grundlage für die Auditierung. Sollte ein vorheriges Audit stattgefunden haben, muss für jedes Referenzdokument herausgestellt werden, welche Veränderungen sich gegenüber der vorhergehenden Version ergeben haben.

Dokument	*Kurzbezeichnung*	*Dateiname/Verweis*	*Version, Datum, Seitenzahl*	*Relevante Änderungen*
A.0	Sicherheitsleitlinien			
A.0.1	Leitlinie zur Informationssicherheit			
A.0.2	Richtlinie zur Risikoanalyse			
A.0.3	Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen			
A.0.4	Richtlinie zur internen ISMS-Auditierung			
A.0.5	Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen			
A.1	Strukturanalyse			
A.1.1	Abgrenzung des IT-Verbunds			
A.1.2	Bereinigter Netzplan			
A.1.3	Liste der IT-Systeme			
A.1.4	Liste der IT-Anwendungen und Geschäftsprozesse			
A.1.5	Liste der Kommunikationsverbindungen			
A.1.6	Liste der Räume			
A.2	Schutzbedarfsfeststellung			
A.2.1	Definition der Schutzbedarfskategorien			
A.2.2	Schutzbedarf der Anwendungen			
A.2.3	Schutzbedarf der IT-			

Dokument	*Kurzbezeichnung*	*Dateiname/Verweis*	*Version, Datum, Seitenzahl*	*Relevante Änderungen*
	Systeme			
A.2.4	Schutzbedarf der Kommunikationsverbindungen			
A.2.5	Schutzbedarf der Räume			
A.3	Modellierung des Informationsverbund			
A.4	Ergebnis des Basis-Sicherheitschecks			
A.5	Ergänzende Sicherheitsanalyse			
A.5.1	Managementreport			
A.6	Risikoanalyse			
A.7	Managementbericht über bestehende Risiken			

Weiterhin wurden folgende Dateien zur Verfügung gestellt (ggf. Anlage Dateiliste):

Dokument	*Kurzbezeichnung*	*Dateiname/Verweis*	*Version, Datum*	*Relevante Änderungen*
E.1	Outsourcing-Vertrag mit XY			
E.2	SLA			
...				

1.11 Toolbasierte Audit-Unterstützung

Folgende Tools würden zur Unterstützung der Auditaktivitäten verwendet:

Tool: GSTool

Versionsnummer: 4.7

Stand der Grundschutzkataloge: 2009100011 (11. EL)

2 Voraudit

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

Wenn der Auditor ein Voraudit durchführt, ist es sinnvoll, unter anderem die Aktualität von Dokumenten, die Sicherheitsrichtlinien, die Nachvollziehbarkeit der Abgrenzung des Verbunds und die Wirksamkeit des Managementsystems für Informationssicherheit zu prüfen oder anzureißen.

Ziel des Voraudits ist die Einschätzung durch den Audit-Teamleiter, ob sich der Informationsverbund mit einem positiven Votum zertifizieren lässt. Sollten an einem positiven Abschluss Zweifel bestehen, so sind die Möglichkeiten des Abbruchs der Auditierung, der Aussetzung des Verfahrens und der Verschiebung des Verfahrens in Erwägung zu ziehen.

Fragestellung:	*Feststellung:*
Wurde ein Voraudit durchgeführt?	❑ Ja Die Prüfungshandlungen werden im Votum dokumentiert
	❑ Nein
(Votum zum Voraudit einschließlich Prüfungshandlungen):	-

3 Dokumentenprüfung

Die nachfolgenden Prüfpunkte werden mit einem Votum zu den Einzelprüfungen geschlossen. Das Votum bezieht sich auf den Stand **nach** einer möglichen Nachbesserung durch den Antragsteller.

Die Historie über die festgestellten Abweichungen und Empfehlungen befinden sich im Kapitel 3.11, diese Liste ist im Folgenden für die Vor-Ort-Prüfung unter 5.6 und bei den Überwachungsaudits fortzuführen.

3.1 Aktualität der Version der Prüfgrundlagen

Die Aktualität der verwendeten Standards bei dem Antragsteller ist Voraussetzung für die Zertifizierung. Insbesondere die eingesetzte Version des BSI-Standards 100-2 und damit der Version des Standards ISO/IEC 27001 sowie die Version der IT-Grundschutz-Kataloge muss dokumentiert sein. Hierzu sind auch die aktuellen Vorgaben der Zertifizierungsstelle unter https://www.bsi.bund.de/grundschutz/zert/ISO27001/Schema/zertifizierungsschema.html zu berücksichtigen.

Fragestellung:	*Feststellung:*
Werden zulässige Versionen der Prüfungs-grundlagen (Kapitel 1.8) angewendet?	❑ Ja
	❑ Nein
(Votum):	-

3.2 Aktualität der Referenzdokumente

Die Aktualität der verwendeten Referenzdokumente muss festgestellt werden.

Fragestellung:	*Feststellung:*
Sind die Referenzdokumente A.0, A.1, A.2, A.3, A.5, A.6 und A.7 aktuell?	❑ Ja
	❑ Nein
Ist der Basis-Sicherheitsscheck (A.4) aktuell?	❑ Ja, A.4 ist nicht älter als 1 Jahr
	❑ Nein
Datum der letzten inhaltlichen Änderungen im Referenzdokument A.4	TT.MM.JJJJ
(Votum):	Alle Referenzdokumente sind aktuell und vollständig.

3.3 Sicherheitsrichtlinien A.0

Die oberste Managementebene ist verantwortlich für das zielgerichtete und ordnungsgemäße Funktionieren einer Organisation und damit auch für die Gewährleistung der Informationssicherheit nach innen und außen. Daher muss diese den Informationssicherheitsprozess initiieren, steuern und kontrollieren. Dazu gehören strategische Leitaussagen zur Informationssicherheit, konzeptionellen Vorgaben und auch organisatorische Rahmenbedingungen, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können. Konzeptionelle Vorgaben und auch organisatorische Rahmenbedingungen werden benötigt, um Informationssicherheit innerhalb aller Geschäftsprozesse erreichen zu können.

Die Richtlinien müssen für die Situation der Institution geeignet und angemessen sein. In der Maßnahme „M 2.192 Erstellung einer Leitlinie zur Informationssicherheit“ des Bausteins “B 1.0 Sicherheitsmanagement” ist aufgezeigt, welche Punkte bei der Erstellung einer IT-Sicherheitsleitlinie beachtet werden müssen. Diese Punkte können entsprechend auch auf die Konzeption anderer Richtlinien übertragen werden.

Fragestellung:	*Feststellung:*	
Erfüllen die Sicherheitsrichtlinien (A.0) nachvollziehbar alle Aspekte der Grundschutz-Maßnahme M 2.192?	❑	Ja
	❑	Nein
Werden die Sicherheitsrichtlinien (A.0) durch das Management getragen und wurden sie veröffentlicht?	❑	Ja
	❑	Nein
Ist die Leitlinie zur Informationssicherheit (A.0.1) sinnvoll und angemessen für den Antragsteller, sowie konsistent zu den anderen Richtlinien in A.0?	❑	Ja
	❑	Nein
Ist die Richtlinie zur Risikoanalyse (A.0.2) sinnvoll und angemessen für den Antragsteller, sowie konsistent zu den anderen Richtlinien in A.0?	❑	Ja
	❑	Nein
Ist die Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen (A.0.3) sinnvoll und angemessen für den Antragsteller, sowie konsistent zu den anderen Richtlinien in A.0?	❑	Ja
	❑	Nein
Ist die Richtlinie zur internen ISMS-Auditierung (A.0.4) sinnvoll und angemessen für den Antragsteller, sowie konsistent zu den anderen Richtlinien in A.0?	❑	Ja
	❑	Nein

Fragestellung:		*Feststellung:*
	Ist die Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen (A.0.5) sinnvoll und angemessen für den Antragsteller, sowie konsistent zu den anderen Richtlinien in A.0?	❑ Ja
		❑ Nein
	Sind die oben genannten Referenzdokumente für den Informationsverbund nachvollziehbar und vollständig?	❑ Ja
		❑ Nein
(Votum):		-

3.4 Strukturanalyse A.1

In diesem Dokument wird der zu untersuchende Informationsverbund dargestellt. Nähere Informationen zur Strukturanalyse finden sich in Kapitel 4.2 der IT-Grundschutz-Methodik.

3.4.1 Definition des Untersuchungsgegenstands

Die Nachvollziehbarkeit der Abgrenzung des Informationsverbundes wird durch den Audit-Teamleiter geprüft.

Ein Informationsverbund ist sinnvoll abgegrenzt, wenn er alle IT-Komponenten umfasst, die zur Unterstützung einer oder mehrerer Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten dienen. Schnittstellen zu externen Partner müssen aufgezeigt und sinnvoll abgegrenzt werden.

Der Informationsverbund 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.

Fragestellung:	*Feststellung:*
Trägt der Informationsverbund substantiell zum Funktionieren der Institution oder eines Teils der Institution bei?	❑ Ja
	❑ Nein
Hat der Informationsverbund eine sinnvolle Abgrenzung?	❑ Ja, unter Votum dokumentieren
	❑ Nein
Hat der Informationsverbund eine geeignete Mindestgröße?	❑ Ja, unter Votum dokumentieren
	❑ Nein
(Votum):	-

3.4.2 Bereinigter Netzplan

Fragestellung:	*Feststellung:*
Liegt ein aktueller und vollständiger bereinigter Netzplan vor?	❑ Ja
	❑ Nein
Sind alle Komponenten im Netzplan mit eindeutigen Bezeichnern versehen?	❑ Ja
	❑ Nein
(Votum):	

3.4.3 Liste der IT-Systeme

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.

Fragestellung:	*Feststellung:*
Enthält die Liste der IT-Systeme alle benötigten Informationen?	❑ Ja
	❑ Nein
Besteht eine Übereinstimmung zwischen der Liste der IT-Systemen und dem Netzplan? (Stichprobe, mindestens 10).	❑ Ja, siehe Stichprobendokumentation
	❑ Nein
(Votum):	-

Stichprobendokumentation zu der Liste der IT-Systeme:

Bezeichnung	*Beschreibung*	*Anzahl*	*Enthält alle Informationen*	*Enthalten im Netzplan*
S-331	Server 1	2	Ja/Nein	Ja/Nein
...				

3.4.4 Liste der Anwendungen und Geschäftsprozesse

In der Liste der Anwendungen bzw. Geschäftsprozesse muss für jede Anwendung eine eindeutige Bezeichnung vergeben sein. Neben einer Klassifizierung der verarbeiteten Daten sind die Verantwortlichen und die Benutzer zu erfassen. Weiterhin muss ersichtlich sein, welche wesentlichen Geschäftsprozesse von der Ausführung der einzelnen Anwendungen abhängen und welche IT-Systeme für die Ausführung der jeweiligen Anwendung benötigt werden.

Fragestellung:	*Feststellung:*
Enthält die Liste der Anwendungen alle benötigten Informationen?	❑ Ja
	❑ Nein
Ist eine Zuordnung der Anwendungen zu den IT-Systemen vorhanden?	❑ Ja
	❑ Nein

Fragestellung:	*Feststellung:*
Ist eine Zuordnung der Anwendungen zu den Geschäftsprozessen vorhanden?	❑ Ja
	❑ Nein
Liegt eine Tabelle mit Abhängigkeiten der Anwendungen untereinander vor? (optional)	❑ Ja
	❑ Nein
(Votum):	-

3.4.5 Liste der Kommunikationsverbindungen

In dieser Liste sind einerseits alle im Informationsverbund vorhandenen und andererseits alle über die Grenzen des Informationsverbundes gehenden Kommunikationsverbindungen aufzuführen.

Fragestellung:	*Feststellung:*
Liegt eine aktuelle und vollständige Liste aller Kommunikationsverbindungen vor?	❑ Ja
	❑ Nein
(Votum):	-

3.4.6 Liste der Räume

Fragestellung:	*Feststellung:*
Liegt eine aktuelle und vollständige Liste aller Räume, Gebäude und Standorten vor?	❑ Ja
	❑ Nein
(Votum):	-

3.4.7 Ergebnis der Teilprüfung „Strukturanalyse“

Ein kurzes Votum des Auditors zur Strukturanalyse wird gegeben.

3.5 Schutzbedarfsfeststellung A.2

Dieses Dokument beschreibt die Ergebnisse der Schutzbedarfsfeststellung, wie sie in Kapitel 4.3 der IT-Grundschutz-Methodik beschrieben ist.

3.5.1 Definition der Schutzbedarfskategorien

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.

Fragestellung:	*Feststellung:*
Ist die Definition der Schutzbedarfskategorien plausibel und für den Informationsverbund angemessen?	❑ Ja
	❑ Nein
(Votum):	-

Wenn mehr als drei Schutzbedarfskategorien definiert wurden, ist vom Auditor zu dokumentieren, welche dieser Schutzbedarfskategorien „hoch“ bzw. „sehr hoch“ entsprechen. Diese Information wird zur Überprüfung der Entscheidung benötigt, welche Objekte in die ergänzende Sicherheitsanalyse aufgenommen werden.

Fragestellung:	*Feststellung:*
Wurden mehr als drei Schutzbedarfskategorien definiert?	❑ Ja, Erläuterungen unter Votum
	❑ Nein
(Votum):	-

3.5.2 Schutzbedarf der Anwendungen

Für jede in der Liste der 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.

Fragestellung:	*Feststellung:*
Ist der Schutzbedarf der Anwendungen bzgl. Vertraulichkeit, Integrität und Verfügbarkeit vollständig dokumentiert?	❑ Ja
	❑ Nein

Fragestellung:	*Feststellung:*
Ist der Schutzbedarf der Anwendungen nachvollziehbar begründet?	❑ Ja
	❑ Nein
(Votum):	-

3.5.3 Schutzbedarf der IT-Systeme

Für jedes in der Liste der IT-Systeme aufgeführte System muss der Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert und begründet sein. Der Auditor nimmt bei der nachfolgenden Prüfung insbesondere die Systeme in Augenschein, auf denen Anwendungen mit erhöhtem Schutzbedarf zum Einsatz kommen.

Fragestellung:	*Feststellung:*
Ist der Schutzbedarf der IT-Systeme nachvollziehbar begründet?	❑ Ja
	❑ Nein
Ist die Ableitung des Schutzbedarfs von Anwendungen auf die IT-Systeme plausibel dokumentiert und begründet ? (Stichprobe über mindestens fünf IT-Systeme)	❑ Ja, siehe Stichprobendokumentation
	❑ Nein
(Votum):	-

Stichprobendokumentation zum Schutzbedarf der IT-Systeme:

Bezeichnung	*Beschreibung*	*Verknüpfung zu folgenden Anwendungen*	*Ableitung des Schutzbedarfs nachvollziehbar*
S-331	Server 1	Anwendung 1 Anwendung 2	Ja/Nein
...			

3.5.4 Schutzbedarf der Kommunikationsverbindungen

Eine Verbindung kann kritisch sein, weil sie eine Außenverbindung darstellt (K1), weil sie hochvertrauliche (K2), hoch integere (K3) oder hoch verfügbare (K4) Daten transportiert, oder weil über sie bestimmte hochschutzbedürftige Daten nicht transportiert werden dürfen (K5). Für jede Kommunikationsverbindung muss vermerkt sein, ob ein oder mehrere der vorgenannten Gründe (K1-K5) zutreffend sind.

Fragestellung:	*Feststellung:*
Liegt eine Liste, aller kritischen Verbindungen liegt vor? *oder* Werden alle kritischen Verbindungen im Netzplan grafisch hervorgehoben?	❑ Ja ❑ Nein
(Votum):	-

3.5.5 Schutzbedarf der Räume

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

Fragestellung:	*Feststellung:*
Ist der Schutzbedarf der Räume nachvollziehbar begründet?	❑ Ja ❑ Nein
Ist der Schutzbedarf der Räume korrekt aus dem Schutzbedarf der IT-Anwendungen und IT-Systeme abgeleitet? (mindestens drei Stichproben)	❑ Ja, siehe Stichprobendokumentation ❑ Nein
(Votum):	-

Stichprobendokumentation zum Schutzbedarf der Räume:

Bezeichnung	*Beschreibung*	*Verknüpfung zu folgenden Anwendungen*	*Verknüpfung zu folgenden IT-Systemen*	*Ableitung des Schutzbedarfs nachvollziehbar*
R-01	Rechenzentrum	A-01 Anwendung 1 A-02 Anwendung 2	S-331 Server1 C-1 Client1	Ja/Nein
...				

3.5.6 Schutzbedarf der Gebäude

Der Schutzbedarf der Gebäude leitet sich aus dem Schutzbedarf der darin befindlichen Räumen ab. Dabei sind das Maximum-Prinzip und der Kumulationseffekt zu berücksichtigen. Vor dem Hintergrund einer Risiko orientierten Standortbetrachtung ist der Schutzbedarf sämtlicher Gebäude / Standorte zu prüfen (vgl. Kap. 4.6 Begutachtung der Standorte des Informationsverbundes).

Fragestellung:	*Feststellung:*
Ist der Schutzbedarf der Gebäude nachvollziehbar begründet?	❑ Ja
	❑ Nein
Ist der Schutzbedarf der Gebäude korrekt aus dem Schutzbedarf der Räume abgeleitet?	❑ Ja
	❑ Nein
(Votum):	-

Vollständige Schutzbedarfsbetrachtung der Gebäude / Liegenschaften:

Bezeichnung	*Beschreibung*	*Verknüpfung zu folgenden (gruppierten) Räumen*	*Ableitung des Schutzbedarfs nachvollziehbar*
G-01	Standort 1	R-01 Rechenzentrum 1 R-02 Büroraum 2	Ja/Nein
...			

3.5.7 Korrektheit der Gruppenbildung

Komponenten dürfen zu einer Gruppe zusammengefasst werden, falls sie vom gleichen Typ, gleich oder nahezu gleich konfiguriert bzw. gleich oder nahezu gleich in das Netz eingebunden sind, den gleichen administrativen, infrastrukturellen Rahmenbedingungen unterliegen, die gleichen Anwendungen bedienen und den gleichen Schutzbedarf aufweisen (vergleiche BSI-Standard 100-2).

Fragestellung:	*Feststellung:*
Wurde die Gruppenbildung korrekt durchgeführt (Stichprobe, mindestens drei der gruppierten Objekte)?	❑ Ja, siehe Stichprobendokumentation
	❑ Nein
(Votum):	-

Stichprobendokumentation zur Gruppenbildung:

Bezeichnung	*Beschreibung*	*Anzahl*	*Gruppenbildung bei der Modellierung korrekt*
C-01	Client1	10000	Ja/Nein
A-12	Webauftritte	15	Ja/Nein

3.5.8 Ergebnis der Teilprüfung „Schutzbedarfsfeststellung“

Ein kurzes Votum des Auditors zur Schutzbedarfsfeststellung wird gegeben.

3.6 Modellierung des Informationsverbunds A.3

Die Modellierung des Informationsverbundes legt fest, welche Bausteine der IT-Grundschutz-Kataloge auf welche Zielobjekte im betrachteten Informationsverbund angewandt werden. Diese Zuordnung erfolgt individuell für den betrachteten Informationsverbund in Form einer Tabelle. Als Richtlinie hierzu findet sich in den IT-Grundschutz-Katalogen ein Modellierungshinweis (https://www.bsi.bund.de/cln_136/ContentBSI/grundschutz/kataloge/allgemein/modellierung/02001.html). In diesem wird für jeden Baustein beschrieben, auf welche Arten er auf verschiedenen Zielobjekten anzuwenden ist. Für Outsourcing sind die Hinweise des Dokuments IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten ausschlaggebend.

Fragestellung:	*Feststellung:*
Wurden die Modellierungsvorschriften korrekt angewandt?	❑ Ja
	❑ Nein
(Votum):	-

3.6.1 Modellierungsdetails

Fragestellung:	*Feststellung:*
Ist jeder Baustein der IT-Grundschutzkataloge auf alle relevanten Zielobjekte angewandt?	❑ Ja
	❑ Nein, unter Votum dokumentieren
Ist für jeden Baustein der IT-Grundschutzkataloge, der nicht angewandt wurde, eine plausible Begründung vorhanden?	❑ Ja
	❑ Nein
(Votum):	-

Fragestellung:	*Feststellung:*
Wie wurden auch Objekte verfahren, für die keine Bausteine in den Grundschutz-Katalogen vorhanden sind?	...
(Votum):	-

3.6.2 Ergebnis der Teilprüfung

Ein kurzes Votum des Auditors zur Modellierung wird gegeben.

3.7 Ergebnis des Basis-Sicherheitschecks A.4

Der Auditor prüft den Basis-Sicherheitsscheck anhand der Vorgaben des BSI-Standards 100-2 Kapitel 4.4 und 4.5 . Hierbei steht nicht die Detailprüfung jeder einzelnen Maßnahme im Vordergrund, sondern die korrekte Vorgehensweise. Der Auditor legt bei seinen Prüfungen jedoch ein besonders Augenmerk darauf, ob die für das ISO 27001-Zertifikat auf der Basis von IT-Grundschutz relevanten Maßnahmen (in den Bausteinen mit „A“, „B“ und „C“ gekennzeichnet) umgesetzt wurden.

3.7.1 Anpassungen von Maßnahmen aus den Grundschutzkatalogen

Der BSI Standard 100-2 sieht vor, dass eine Anpassung von Maßnahmen aus den Grundschutzkatalogen an die Rahmenbedingungen der Institution sinnvoll sein kein (vgl. Kapitel 4.4.3). In solchen Fällen muss sich der Auditor davon überzeugen, dass die vorgenommen Anpassungen dem Schutzbedarf der Institution entsprechen. Hierzu wählt der Auditor eine Stichprobe von mindestens fünf Maßnahmen.

Fragestellung:	*Feststellung:*
Wurden Anpassungen der Maßnahme der Grundschutzkataloge vorgenommen? (Stichprobe, mindestens fünf)?	❑ Ja, Stichprobendokumentation
	❑ Nein

Stichprobendokumentation zur Anpassung von Maßnahmen:

M. Nr.	*Beschreibung*	*Beschreibung der Anpassungen*	*Prüfung der Angemessenheit*
M 1.27	Lokale unterbrechungsfreie Stromversorgung	....	Ja/Nein
(Votum):	-		

3.7.2 Details Basis-Sicherheitscheck

Fragestellung:		*Feststellung:*
	Wurden für die Zielobjekte die richtigen Bausteine zugrunde gelegt?	❑ Ja
		❑ Nein
	Wurden die in den Bausteinen aufgeführten Maßnahmen vollständig am Zielobjekt geprüft?	❑ Ja
		❑ Nein
	Wurde zu jeder Maßnahme der Umsetzungsstatus erhoben?	❑ Ja
		❑ Nein
	Wurden alle Maßnahmen mit Umsetzungsstatus 'entbehrlich' plausibel begründet?	❑ Ja
		❑ Nein
	Wurden die nicht oder nur teilweise umgesetzten Maßnahmen im Referenzdokument A.7 dokumentiert?	❑ Ja
		❑ Nein
	Wurden die aus der Risikoanalyse resultierenden ergänzenden Maßnahmen den Zielobjekten zugeordnet und deren Umsetzung im Basis-Sicherheitscheck dokumentiert?	❑ Ja
		❑ Nein
	Ist der Umsetzungsgrad der Maßnahmen ausreichend für die Zertifikatserteilung?	❑ Ja
		❑ Nein
(Votum):		-

3.7.3 Ergebnis der Teilprüfung „Basis-Sicherheitsscheck“

Ein kurzes Votum des Auditors zum Basis-Sicherheitsscheck wird gegeben.

3.8 Ergänzende Sicherheitsanalyse A.5

Für alle Zielobjekte des Informationsverbundes (Räume, IT-Anwendungen, IT-Systeme, Kommunikationsverbindungen), die

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

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

Fragestellung:	*Feststellung:*
Ist der Management-Report (A.5) aussagekräftig und nachvollziehbar?	❑ Ja
	❑ Nein
Wurde der Management-Report zur Sicherheitsanalyse von der obersten Leitung verabschiedet und unterscheiben?	❑ Ja
	❑ Nein
(Votum):	-

3.8.1 Details zur ergänzenden Sicherheitsanalyse

Fragestellung:	*Feststellung:*
Wurden alle Zielobjekte betrachtet, deren Schutzbedarf über „normal“ liegt?	❑ Ja
	❑ Nein
Wurden alle Zielobjekte betrachtet, die mit den verfügbaren Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können?	❑ Ja
	❑ Nein
Wurden alle Zielobjekte betrachtet, die in Einsatzszenarien (Umgebung, Anwendung)	❑ Ja
	❑ Nein

Fragestellung:	*Feststellung:*
betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind?	
Liegt für jedes Zielobjekt eine nachvollziehbar Begründung vor?	❑ Ja
	❑ Nein
(Votum):	-

3.8.2 Ergebnis der Teilprüfung „Ergänzende Sicherheitsanalyse“

Ein kurzes Votum des Auditors zur Ergänzenden Sicherheitsanalyse wird gegeben.

3.9 Risikoanalyse A.6

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

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

Fragestellung:	*Feststellung:*
Wurde für alle in A.5 identifizierten Zielobjekte mit Risikoanalyse-Bedarf eine Risikoanalyse durchgeführt und dokumentiert?	❑ Ja ❑ Nein
(Votum):	-

3.9.1 Details zur Risikoanalyse

Fragestellung:	*Feststellung:*
Ist die Risikoanalysen nachvollziehbar und plausibel begründet?	❑ Ja ❑ Nein
Sind die zusätzlichen Sicherheitsmaßnahmen ausreichend bzw. angemessen für die identifizierten Gefährdungen?	❑ Ja ❑ Nein
Sind die zusätzlichen Sicherheitsmaßnahmen mit den Maßnahmen aus A.4 konsolidiert?	❑ Ja ❑ Nein
Sind die zusätzlichen Sicherheitsmaßnahmen als Ergänzung zu A.4 dokumentiert?	❑ Ja ❑ Nein
Wurde der Management-Report zur Risikoanalyse von der obersten Leitung verabschiedet und unterscheiben?	❑ Ja ❑ Nein
(Votum):	-

3.9.2 Ergebnis der Teilprüfung „Risikoanalyse“

Ein kurzes Votum des Auditors zur Risikoanalyse des Antragstellers wird gegeben.

3.10 Risikobehandlungsplan A.7

Sind zum Zeitpunkt der Auditierung GS-Maßnahmen des Umsetzungsplans noch nicht oder nur teilweise umgesetzt, entscheidet der Auditor, ob eine Zertifizierung zu diesem Zeitpunkt möglich ist. Der Auditor muss Risiko orientiert den Gesamtkontext des Informationsverbundes und der kritischen Geschäftsprozesse betrachten. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten Institution beitragen, dürfen nicht in eine Risikoübernahmen einfließen.

Fragestellung:	*Feststellung:*
Liegt ein Risikobehandlungsplan vor (A.7) und werden die bestehenden Risiken nachvollziehbar dokumentiert?	❑ Ja
	❑ Nein
Ist das vom Management getragene Restrisiko für den Informationsverbund angemessen?	❑ Ja
	❑ Nein
Besteht ein Umsetzungsplan für die Reduzierung des Restrisikos?	❑ Ja
	❑ Nein
(Votum):	-

3.10.1 Ergebnis der Teilprüfung „Managementbewertung über bestehende Risiken“

Ein kurzes Votum des Auditors zur „Managementbewertung über bestehende Risiken“ wird gegeben.

3.11 Abweichungen und Empfehlungen aus der Dokumentenprüfung

Während der Phase 1 des Audits wurden bei der ersten Sichtung der Referenzdokumente vom ***Datum*** folgende Abweichungen sowie Empfehlungen festgestellt. Der Auditteamleiter beschreibt die Abweichung bzw. Empfehlung **kurz** und referenziert auf diese an den entsprechenden Stellen im Votum. Dem Antragsteller wird die Liste der Abweichungen und Empfehlungen zur Nachbesserung umgehend mitgeteilt.

Die Liste der Abweichungen und Empfehlungen wird im gesamten Auditprozess und auch bei den Überwachungsaudits weiter gepflegt.

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.

Für jede Abweichung wird eine Nachbesserungsfrist festgelegt, in der sie beseitigt werden sollte.

Liste der Abweichungen und Empfehlungen:

Lauf. Nr.	*Abweichung*	*Abweichungstyp (E/AG/AS)*	*Behebungs-frist/ Nachweis*	*Status der Behebung*
1	AS-1 Verweis Auditfeststellung Verweis Referenzdokument kurze Beschreibung	AG-1.: eine geringfügige Abweichung	01/ Protokoll	

Bei der Prüfung der Nachbesserungen 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.
- **Offen:** die Umsetzung der Abweichungen oder Empfehlungen erfolgt erst im nächsten Überwachungsaudit.

4 Erstellung eines Prüfplans

4.1 Weiterführung des Audits

An dieser Stelle wird die Entscheidung zur Weiterführung des Audits mit Phase 2 dokumentiert.

Während der Phase 1 des Audits wurden bei der ersten Sichtung der Referenzdokumente vom *Datum* einige, wenige Inkonsistenzen mit unterschiedlicher Relevanz festgestellt. Diese gliedern sich in schwerwiegende und geringfügige Abweichungen sowie Empfehlungen und sind im Abschnitt 3.11 dokumentiert.

Fragestellung:	*Feststellung:*
Ist eine Fortführung des Audits mit der Vor-Ort-Prüfung möglich?	❑ Ja
	❑ Nein
(Votum):	-

4.2 Audit-Team

Im Anschluss an Phase 1 wurden vom Audit-Teamleiter die Fachkenntnisse des Audit-Teams überprüft. Dabei wurde sowohl die Branche, in der der Antragsteller arbeitet, als auch technische und organisatorische Aspekte im Geltungsbereich berücksichtigt.

Übersicht des Audit-Teams:

Nr	*Funktion*	*Name,*	*Expertise*	*Kontaktdaten*
F.0	Audit-Teamleiterin	Frau Dr. Müller...	Lead-Auditor, Infrastruktur, SAP	Hofgarten 122, 01000 Berlin Telefon: 030932836 E-Mail: auditor@muellerdrfr.fr
F.1	Auditor	….		
F.2	Auditor	….		
F...	Fachexperte...			

Damit liegen ausreichende Fachkenntnisse im Audit-Team vor.

4.3 Auswahl der Auditbausteine

Der Baustein Sicherheitsmanagement ist immer zu überprüfen. Des weiteren sind minimal fünf IT-Grundschutz-Bausteinzuordnungen risikoorientiert über alle Schichten und ein Baustein zufällig auszuwählen. Zusätzliche sind fünf Maßnahmen aus der Risikoanalyse zu prüfen.

Von der Auswahl ausgeschlossen sind die Bausteine Datenschutz und benutzerdefinierte Bausteine.

4.3.1 Sicherheitsmanagement

Die Prüfung dieses Bausteins ist obligatorisch. Da von der Wirksamkeit des Sicherheitsmanagements die Qualität des gesamten Informationssicherheitsprozesses abhängt, ist die Prüfung des Bausteins B 1.0 Sicherheitsmanagement (mit der Überprüfung des Sicherheitskonzeptes des Informationsverbundes nach dem BSI-Standard 100-2 in der Maßnahme M 2.195 Erstellung eines Sicherheitskonzepts) vorrangig und zwingend erforderlich.

4.3.2 Gezielt ausgewählte Bausteine

Der Audit-Teamleiter wählt **Risiko orientiert** aus jeder Schicht ein Baustein-Zielobjekte aus.

Schicht:	*Bausteinname / Zielobjekt:*
Übergeordnete Aspekte	Nummer Bausteinname: Zielobjekt: Begründung:
Infrastruktur	Nummer Bausteinname: Zielobjekt: Begründung:
IT-Systeme	Nummer Bausteinname: Zielobjekt: Begründung:
Netze	Nummer Bausteinname: Zielobjekt: Begründung:
Anwendungen	Nummer Bausteinname: Zielobjekt: Begründung:
Anmerkungen zur Auswahl:	-

4.3.3 Baustein im Losverfahren

Aus allen Baustein-Zielobjekte wird ein Baustein ausgewählt.

Schicht	*Bausteinname / Zielobjekt*
z.B. IT-Systeme	Nummer Bausteinname: Zielobjekt:
Anmerkungen zur Auswahl:	-

4.4 Erweiterung der Stichprobe

Über die im Auditierungsschema geforderten Stichproben hinaus, kann der Auditor im eigenen Ermessen die Strichproben erweitern.

Schicht	*Bausteinname / Zielobjekt*
IT-Systeme	Nummer Bausteinname: Zielobjekt:
Anmerkungen zur Auswahl:	-

4.5 Sicherheitsmaßnahmen aus der Risikoanalyse

Aus der Menge der zusätzlichen Sicherheitsmaßnahmen, die im Rahmen der Risikoanalyse festgelegt wurden, wählt der Audit-Teamleiter mindestens **fünf Stichproben** aus.

Schicht:	*Maßnahme/Zielobjekt:*
Anwendungen	**bB 1.2 Risikoreduktion bei Tests/A-02** bM 1.293 Tests in sicheren Umgebungen /S-04
….	
Anmerkungen zur Auswahl:	-

4.6 Begutachtung der Standorte des Informationsverbundes

Im Rahmen der Auditierung ist eine Begutachtung der Standorte des Informationsverbunds erforderlich. Der Auditor dokumentiert die Standorte und begründet seine Auswahl.

Auswahl von Standorten

Bezeichnung der Standorte	*Hinweise zur Gruppenbildung/*	*Begründung für die Risiko orientierte Auswahl*
Standort 1		
….		
Anmerkungen zur Auswahl:	-	

5 Vor-Ort-Audit

Die nachfolgenden Prüfpunkte werden mit einem Votum zu den Einzelprüfungen geschlossen. Das Votum bezieht sich auf den Stand **nach** einer möglichen Nachbesserung durch den Antragsteller.

Der Auditteamleiter beschreibt die Abweichung bzw. Empfehlung **kurz** und referenziert für die näheren Details auf die Umsetzungsprüfung.

Die Historie über die erfolgten Abweichungen aus Kapitel 3.11 wird in Kapitel 5.6 fortgeschrieben und im Überwachungsaudit fortzuführen.

5.1 Auditmethoden

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
- (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

Das Audit erfolgte auf der Grundlage systemorientierter Prüfungshandlungen. Im Rahmen der Funktionsprüfung wurden Stichproben unter Zugrundelegung der formalen Grundlagen geprüft.

Branche, Größe, Komplexität, Anforderungen, Risiken und Unternehmensziele beeinflussen die Ausgestaltung eines ISMS konkret und müssen daher auch bei der Bewertung der Angemessenheit eines ISMS und seiner Maßnahmen besondere Berücksichtigung finden.

5.2 Wirksamkeit des Sicherheitsmanagementsystems

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

Fragestellung:	*Feststellung:*
Ist das ISMS effektiv und effizient im Einsatz? (Interview, Gesamteindruck)	❑ Ja

Fragestellung:	*Feststellung:*
	❑ Nein
Werden die in den Sicherheitsleitlinien vorgegebenen Ziele erreicht?	❑ Ja
	❑ Nein
Werden alle wichtigen Prozesse des Informationsverbundes dokumentiert?	❑ Ja
	❑ Nein
Wird der PDCA-Zyklus gelebt und das ISMS kontinuierlich verbessert?	❑ Ja
	❑ Nein
(Votum):	-

5.3 Verifikation des Informationsverbunds

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.

Fragestellung:	*Feststellung:*
Entsprechen die dokumentierten IT-Systeme und deren Eigenschaften bzw. Kommunikationsverbindungen der tatsächlichen Netzstruktur? (mindestens fünf Stichprobe)	❑ Ja, Stichprobendokumentation
	❑ Nein
Ist der bereinigte Netzplan auf dem aktuellen Stand?	❑ Ja
	❑ Nein
(Votum):	-

Stichprobendokumentation zur Überprüfung der tatsächlichen Netzstruktur:

Bezeichnung	*Beschreibung*	*Anzahl*	*Entsprechung bestätigt*
C-01	Client1	10000	Ja/Nein
K-01	Internetverbindung	15	Ja/Nein
...			

5.4 Verifikation des Basis-Sicherheitschecks

Beim Basis-Sicherheitscheck wird jeder Maßnahme, die in den für die Modellierung herangezogenen Bausteinen enthalten ist, für das jeweilige Zielobjekt der Umsetzungsstatus ("entbehrlich", "ja", "teilweise" oder "nein") zugeordnet. Die Ergebnisse liegen als Basis-Sicherheitscheck (A.4) vor. Es muss sichergestellt sein, dass die hier dokumentierten Ergebnisse mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts übereinstimmen.

Für die Einzelprüfungen der gewählten Bausteine; zu jedem ausgewählten Baustein wird auf der Maßnahmenebene in der Anlage kurz erläutert, was genau geprüft wurde, wer jeweils wofür befragt wurde und welche Ergebnisse zu vermerken sind (Begründung). Für die Dokumentation der Einzelprüfungen stellt das BSI das Dokument Anlage 1 „Umsetzungsprüfung Basis-Sicherheitsscheck" zur Verfügung. Alternativ kann der Auditor auch individuelle Prüfprotokolle verwenden, diese müssen aber alle wesentlichen Informationen der Anlage 1 Basis-Sicherheitscheck in geeigneterer Form enthalten.

Fragestellung:	*Feststellung:*
Stimmt der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der Maßnahmen mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts überein? (Alle Maßnahmen)	❑ Ja ❑ Nein
Ist die Begründung der „entbehrlichen" Maßnahmen zulässig und nachvollziehbar?	❑ Ja ❑ Nein
Sind alle Maßnahmen mit dem Umsetzungsstatus „teilweise" oder „nein" im Referenzdokument A.7 enthalten?	❑ Ja ❑ Nein

5.5 Verifikation der Umsetzung der ergänzenden Maßnahmen aus der Risikoanalyse

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

Für die durchgeführte **Stichprobenuntersuchung** sind die nachfolgenden Fragestellungen zu beantworten.

Fragestellung:	*Feststellung:*
Stimmt der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der ergänzten Sicherheitsmaßnahmen mit dem tatsächlich vorhandenen Informationssicherheitszustand des jeweiligen Zielobjekts überein?	❑ Ja ❑ Nein
Sind alle ergänzenden Sicherheitsmaßnahmen aus der Risikoanalyse als umgesetzt gekennzeichnet?	❑ Ja ❑ Nein
Werden nicht umgesetzte Maßnahmen der ergänzenden Risikoanalyse im Referenzdokument A.7 aufgeführt?	❑ Ja ❑ Nein
(Votum):	-

5.6 Abweichungen und Empfehlungen aus der Vor-Ort-Prüfung

Während der Vor-Ort-Prüfung des Audits vom Datum wurden vor Ort bei dem Antragsteller, im Rahmen der Verifikation des Basis-Sicherheitschecks folgende Abweichungen und Empfehlungen festgestellt. Der Auditteamleiter beschreibt die Abweichung bzw. Empfehlung **kurz** und referenziert auf die ausführliche Fehlerbeschreibung im Dokument „Umsetzungsprüfung_Basissicherheitsscheck_Muster.odt“ oder entsprechenden Prüfprotokollen. Dem Antragsteller wird die Liste der Abweichungen und Empfehlungen zur Nachbesserung umgehend mitgeteilt. Für jede Abweichung wird eine Nachbesserungsfrist festgelegt, in der sie beseitigt werden sollte.

Die Liste der Abweichungen und Empfehlungen wird im gesamten Auditprozess und auch bei den Überwachungsaudits weiter gepflegt.

Liste der Abweichungen und Empfehlungen:

Lauf. Nr.	*Abweichung*	*Abweichungstyp (E/AG/AS)*	*Behebungs-frist/ Nachweis*	*Status der Behebung*
1	AS-1 Verweis Auditfeststellung Verweis Referenzdokument kurze Beschreibung	AG-1.: eine geringfügige Abweichung	01/ Protokoll	

6 Gesamtvotum

6.1 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 Audit-Teamleiters, ob der betrachtete Untersuchungsgegenstand die jeweiligen Anforderungen erfüllt.

Der Audit-Teamleiter stellt in kurzer Form seine Gesamteinschätzung dar, die auf den Ergebnissen der für das Zertifizierungsaudit beschriebenen Prüfschritten beruht. Umstände oder Auditierungsergebnisse, die die Erteilung 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 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 IT-Grundschutz-Audits wird festgestellt, dass der Untersuchungsgegenstand die Anforderungen eines der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz erfüllt / nicht erfüllt. _____ _____ Datum Unterschrift des Auditteamleiters