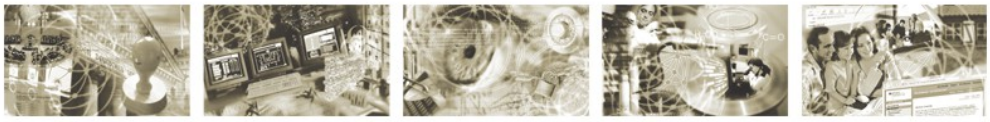
Bundesamt
für Sicherheit in der
Informationstechnik



Hinweise zur Bereitstellung der Referenzdokumente im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Version 2.1

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6222
E-Mail: gs-zert-pruef@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

Versionshistorie

Datum	Version	Verfasser	Bemerkungen
	0.99	BSI	Version zur Kommentierung durch die Auditoren
30.03.11	1.0	BSI	
11.10.17	2.0	BSI	Anpassung an die Methodik gemäß dem IT-Grundschutz-Kompendium
24.04.19	2.1	BSI	Ergänzung „Liste der Dienstleister“, Sprachliche Verfeinerung zu A.6 Realisierungsplan

1 Einleitung

Für einer Auditierung nach ISO 27001 auf der Basis von IT-Grundschutz sind durch den Antragsteller eine Vielzahl von Dokumente für Prüfzwecke bereitzustellen. Diese sind in elektronischer Form dem Auditor zu übergeben. Die Dokumente sind - entsprechend der tabellarischen Aufstellung im Anhang dieses Dokuments - in einer Verzeichnisstruktur abzulegen. Der Antragsteller ergänzt die fehlenden Angaben in der vorgenannten Tabelle und leitet sie an den Auditor weiter. Die Tabelle ist im Rahmen von Überwachungsaudits oder einer Re-Zertifizierung durch den Antragsteller fortzuschreiben.

Die grundsätzliche Vorgehensweise ist im BSI-Standard 200-2 beschrieben.

2 Referenzdokumente

Die folgenden Referenzdokumente bilden die Grundlage für die Auditierung und sind dem Auditor und der Zertifizierungsstelle vom Antragsteller als Arbeitsgrundlage zur Verfügung zu stellen:

- Richtlinien für Informationssicherheit (A.0)
- Strukturanalyse (A.1)
- Schutzbedarfsfeststellung (A.2)
- Modellierung des Informationsverbunds (A.3)
- Ergebnis des IT-Grundschutz-Checks (A.4)
- Risikoanalyse (A.5)
- Realisierungsplan (A.6)

Der Auditor wird darüber hinaus während des Vor-Ort-Audits weitere Dokumente und Aufzeichnungen einsehen.

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

Soweit der Antragsteller und der Auditor der Ansicht sind, dass Maßnahmen zur Gewährleistung der Vertraulichkeit bei der Übergabe der Dokumentation erforderlich sind, sollten geeignete Schritte ergriffen werden. Der Auditor ist durch vertragliche Vereinbarungen mit dem BSI verpflichtet, im Rahmen des Audits gewonnenen Informationen streng vertraulich zu behandeln sowie Beschäftigten und Dritten Informationen nur zu geben, soweit ihre Kenntnis unbedingt notwendig und mit den vertraglichen Vereinbarungen mit dem BSI und der auditierten Organisation vereinbar ist.

Neben den Referenzdokumenten ist die Übersicht “Liste der Referenzdokumente“ einzureichen, vgl. Kapitel 3. In dieser Liste der Referenzdokumente müssen ferner relevante Änderungen (bei Überwachungsaudits und Re-Zertifizierungsverfahren) verzeichnet sein.

2.1 A.0 Richtlinien für Informationssicherheit

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

- Sicherheitsleitlinie
- Richtlinie zur Risikoanalyse

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

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

2.2 A.1 Strukturanalyse

In diesem Dokument wird der zu untersuchende Informationsverbund dargestellt. Nähere Informationen zur Strukturanalyse finden sich im BSI-Standard 200-2. Im Einzelnen müssen folgende Informationen vorliegen:

- Definition des Untersuchungsgegenstands

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

- Integration des Untersuchungsgegenstands in das Gesamtunternehmen

  In einem kurzen Firmen-/Behördenprofil müssen u.a. die wesentlichen Tätigkeitsfelder der Institution und die Größe des Informationsverbunds deutlich werden. Die Bedeutung des Untersuchungsgegenstands für die Institution als Ganzes ist darzustellen.

- Bereinigter Netzplan

- Der bereinigte Netzplan stellt die Komponenten im Informationsverbund und deren Vernetzung dar. Dabei sind gleichartige Komponenten zu Gruppen zusammengefasst.

- Liste der Geschäftsprozesse

- Die für den Informationsverbund relevanten Geschäftsprozesse sind darzustellen.

- Liste der IT-Anwendungen

- Ausgehend von den identifizierten Geschäftsprozessen sind die damit zusammenhängenden Anwendungen aufzuführen.

- Liste der IT-Systeme

- In dieser Liste sind alle im Informationsverbund vorhandenen IT-Systeme (Server, Clients, TK-Anlagen, aktive Netzkomponenten, industrielle Steuerungssysteme (ICS), Internet of Things (IoT)-Geräte, etc.) aufgeführt.

- Liste der Räume, Gebäude und Standorte

- In dieser Liste sind alle Räume, Gebäude und Standorte im Informationsverbund aufgeführt.

- Liste der Kommunikationsverbindungen
- In dieser Liste sind einerseits alle im Informationsverbund vorhandenen und andererseits alle über die Grenzen des Informationsverbunds gehenden Kommunikationsverbindungen angegeben.
- Liste der Dienstleister
- In dieser Liste sind alle externen Dienstleister erfasst, die Einfluss auf den Informationsverbund nehmen können.

2.3 A.2 Schutzbedarfsfeststellung

Dieses Dokument beschreibt die Ergebnisse der Schutzbedarfsfeststellung, wie sie im BSI-Standard 200-2 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 Schadensszenarien (Verstoß gegen Gesetze/Vorschriften/Verträge, Beeinträchtigung des informationellen Selbstbestimmungsrechts, Beeinträchtigung der persönlichen Unversehrtheit, Beeinträchtigung der Aufgabenerfüllung, negative Innen- oder Außenwirkung sowie finanzielle Auswirkungen) in Bezug auf die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

- Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen

  Originär wird der Schutzbedarf der Geschäftsprozesse und Anwendungen ermittelt. Darauf aufbauend wird daraus der Schutzbedarf der einzelnen IT-Systeme, Räume, Gebäude und Standorte sowie Kommunikationsverbindungen abgeleitet.

- Schutzbedarfsfeststellung für IT-Systeme

  Der Schutzbedarf eines IT-Systems (inkl. ICS und IoT-Geräte) leitet sich aus dem Schutzbedarf der Geschäftsprozesse und Anwendungen ab, die auf dem IT-System ablaufen oder deren Daten das IT-System transportiert oder verarbeitet. Für jedes in der Liste der IT-Systeme aufgeführte IT-System ist der Schutzbedarf in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit zu dokumentieren und zu begründen.

- Schutzbedarfsfeststellung für Räume, Gebäude und Standorte

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

- Schutzbedarfsfeststellung für Kommunikationsverbindungen

Der Schutzbedarf der Kommunikationsverbindungen ist zu dokumentieren.

2.4 A.3 Modellierung des Informationsverbunds

Die Modellierung des Informationsverbundes legt fest, welche Bausteine der IT-Grundschutz-Vorgehensweise auf welche Zielobjekte im betrachteten Informationsverbund angewandt werden, vgl. BSI-Standard 200-2. Diese Zuordnung erfolgt individuell für den betrachteten Informationsverbund in Form einer Tabelle. Es ist möglich, Zielobjekte sinnvoll zu gruppieren. Im Einzelnen müssen folgende Informationen enthalten sein:

- Auflistung aller Bausteine im Informationsverbund
- Auflistung aller Bausteine bei den externen Dienstleistern

Mit den Bausteinen der Modellierung wird der konkrete Sicherheitsmaßstab für die Institution definiert, da in den Bausteinen des IT-Grundschutz-Kompendiums die Anforderungen enthalten sind.

2.5 A.4 Ergebnis des IT-Grundschutz-Checks

Ausgehend von den Baustein-Zielobjekte-Zuordnungen, die in der Modellierung identifiziert wurden, wird im IT-Grundschutz-Check geprüft, inwiefern jede einzelne Anforderung umgesetzt wird. Dabei ist ein Verweis auf weiterführende Dokumente zulässig. Ferner ist es möglich, die Umsetzung einer Anforderung als “entbehrlich“ zu setzen.

Damit ist für jede Anforderung aus jedem Baustein und bezogen auf jedes Zielobjekt insbesondere darzulegen:

- Umsetzungsstatus: “entbehrlich“, “ja“, “nein“, “teilweise“
- Umsetzung: Beschreibung der aktuellen Umsetzung
- Bemerkungen/Begründungen

Weitere Erläuterungen zum IT-Grundschutz-Check finden sich im BSI-Standard 200-2. Wichtig ist, den aktuellen Umsetzungsstand konkret zu beschreiben, da im IT-Grundschutz-Kompendiums lediglich Anforderungen formuliert werden.

Selbstverständlich ist es zulässig, Zielobjekte sinnvoll zu gruppieren.

2.6 A.5 Risikoanalyse

Die Risikoanalyse ist entsprechend der selbst definierten Richtlinie zur Risikoanalyse durchzuführen und zu dokumentieren. Modelle zur Durchführung von Risikoanalysen sind beispielsweise im BSI-Standard 200-3 “Risikoanalyse auf der Basis von IT-Grundschutz“ sowie in ISO/IEC 27005 enthalten.

2.7 A.6 Realisierungsplan

Die vollständige Erfüllung der im IT-Grundschutz geforderten Standard-Anforderungen und gegebenenfalls die Anforderungen für den erhöhten Schutzbedarf ist ein hoher Anspruch an jede Institution. In der Praxis lassen sich nicht alle Anforderungen erfüllen, sei es, dass Umstände vorliegen, die eine Erfüllung nicht sinnvoll erscheinen lassen (Neubeschaffung von Informationstechnik, Umzugspläne oder Ähnliches) oder dass eine Anforderung aus organisatorischen oder technischen Rahmenbedingungen nicht möglich ist, vgl. dazu Ausführungen in den BSI-Standards 200-2 und 200-3.

Bestehende Defizite bei der Umsetzung von Sicherheitsmaßnahmen, die aus den Sicherheitsanforderungen resultieren und die damit verbundenen Risiken müssen in Form eines Managementberichtes dokumentiert werden, einschließlich einer Umsetzungsplanung für die weitere Behandlung der bestehenden Risiken. Der Risikobehandlungs-bzw. Realisierungsplan sollte eine Beschreibung der geplanten Ressourcen und zeitliche Vorgaben enthalten. Er wird durch Unterschrift der Institutionsleitung genehmigt.

Basis-Anforderungen sind uneingeschränkte Anforderungen, die umgesetzt sein müssen und für die keine Risikoübernahme möglich ist. Entsprechend können Basis-Anforderungen nicht im A.6 Dokument erscheinen.Liste der Referenzdokumente

Doku.	*Kurzbezeichnung*	*Dateiname /Verweis*	*Version, Datum, Seitenzahl*	*Relevante Änderungen*
A.0	**Richtlinien für Informationssicherheit**			
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 Informationsverbunds			
A.1.2	Bereinigter Netzplan			
A.1.3	Liste der Geschäftsprozesse			
A.1.4	Liste der Anwendungen			

Doku.	*Kurzbezeichnung*	*Dateiname /Verweis*	*Version, Datum, Seitenzahl*	*Relevante Änderungen*
A.1.5	Liste der IT-Systeme			
A.1.6	Liste der Räume, Gebäude und Standorte			
A.1.7	Liste der Kommunikationsverbindungen			
A.1.8	Liste der Dienstleister			
A.2	**Schutzbedarfsfeststellung**			
A.2.1	Definition der Schutzbedarfskategorien			
A.2.2	Schutzbedarf der Geschäftsprozesse			
A.2.3	Schutzbedarf der Anwendungen			
A.2.4	Schutzbedarf der IT-Systeme			
A.2.5	Schutzbedarf der Räume, Gebäude und Standorte			
A.2.6	Schutzbedarf der Kommunikationsverbindungen			
A.3	**Modellierung des Informationsverbundes**			
A.3.1	Auflistung aller Bausteine im Informationsverbund			
A.3.2	Auflistung aller Bausteine bei den externen Dienstleistern			
A.4	**Ergebnis des IT-Grundschutz-Checks**			
A.5	**Risikoanalyse**			
A.6	**Realisierungsplan (Risikobehandlungsplan)**			