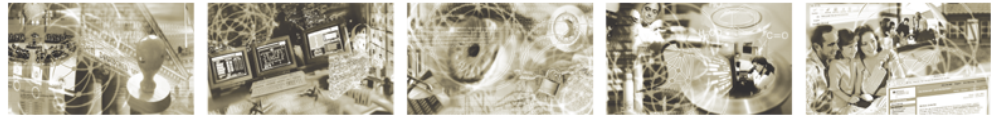




Bundesamt
für Sicherheit in der
Informationstechnik



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

Version 1.0

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

Tel.: +49 228 99 9582-111

E-Mail: gszertifizierung@bsi.bund.de

Internet: <http://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2011

Inhaltsverzeichnis

1	Einleitung.....	5
2	Referenzdokumente.....	5
2.1	A.0 IT-Sicherheitsrichtlinien Richtlinien für Informationssicherheit.....	6
2.2	A.1 Strukturanalyse.....	6
2.3	A.2 Schutzbedarfsfeststellung.....	7
2.4	A.3 Modellierung des Informationsverbunds.....	8
2.5	A.4 Ergebnis des Basis-Sicherheitschecks.....	8
2.6	A.5 Ergänzende Sicherheitsanalyse	8
2.7	A.6 Risikoanalyse.....	9
2.8	A.7 Managementbewertung über bestehende RisikenRisikobehandlungsplan.....	9
3	Liste der Referenzdokumente.....	10

Versionshistorie

Datum	Version	Verfasser	Bemerkungen
	0.99	BSI	Version zur Kommentierung durch die Auditoren
30.03.11	1.0	BSI	

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.

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 Basis-Sicherheitschecks (A.4)
- Ergänzende Sicherheitsanalyse (A.5)
- Risikoanalyse (A.6)
- Risikobehandlungsplan (A.7)

Die Vorlage der Ergebnisse des Basis-Sicherheitschecks (A.4) bei der Zertifizierungsstelle ist optional. Dem Auditor muss das Referenzdokument A.4 jedoch auf jeden Fall als Arbeitsgrundlage zur Verfügung gestellt werden. Der Auditor 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.

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 der Schicht 1 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 in Kapitel 4.2 der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2). Im Einzelnen müssen folgende Informationen vorliegen:

1. Definition des Untersuchungsgegenstands

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

2. 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.

3. Bereinigter Netzplan

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

4. Liste der IT-Systeme

In dieser Liste sind alle im Informationsverbund vorhandenen IT-Systeme (Server, Clients, TK-Anlagen, aktive Netzkomponenten, etc.) aufgeführt.

5. Liste der IT-Anwendungen

In dieser Liste sind die wichtigsten im Informationsverbund 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.

6. Liste der Kommunikationsverbindungen

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

7. Liste der Räume

In dieser Liste sind alle Räume im Informationsverbund mit Funktion aufgeführt. Es kann sinnvoll sein, hier einen Raumplan ergänzend beizufügen.

2.3 A.2 Schutzbedarfsfeststellung

Dieses Dokument beschreibt die Ergebnisse der Schutzbedarfsfeststellung, wie sie in Kapitel 4.3 der IT-Grundschutz-Vorgehensweise beschrieben ist. Im Einzelnen müssen folgende Informationen enthalten sein:

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

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. Diese Zuordnung erfolgt individuell für den betrachteten Informationsverbund in Form einer Tabelle. Als Richtlinie hierzu findet sich in den IT-Grundschutz-Katalogen ein Modellierungshinweis. In diesem wird für jeden Baustein beschrieben, auf welche Arten er auf verschiedenen Zielobjekten anzuwenden ist.

2.5 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 4.5 der IT-Grundschutz-Vorgehensweise zur Verfügung.

2.6 A.5 Ergänzende Sicherheitsanalyse

Für alle Zielobjekte des Informationsverbundes, die

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

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

2.7 A.6 Risikoanalyse

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.

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

2.8 A.7 Risikobehandlungsplan

Eine vollständige Umsetzung der in den IT-Grundschutz-Katalogen geforderten Maßnahmen ist ein hoher Anspruch. In der Praxis lässt sich diese Forderung nicht immer umsetzen, sei es, dass dies an fehlenden Ressourcen scheitert oder Umstände vorliegen, die eine Umsetzung nicht sinnvoll erscheinen lassen (Neubeschaffung von Informationstechnik, Umzugspläne, u. Ä.)

In Form eines Managementberichtes sind die bestehenden Umsetzungsdefizite und die damit verbundenen Risiken zu dokumentieren, einschließlich einer Umsetzungsplanung für eine weitere Reduktion der bestehenden Restrisiken. Der Risikobehandlungsplan muss Ressourcen und zeitliche Vorgaben enthalten und von der obersten Leitung durch Unterschrift genehmigt sein.

Es sind auch solche Maßnahmen zu dokumentieren, auf deren Umsetzung gänzlich verzichtet wird (im Sinne von Kap 5.3 von BSI 100-2), die Risikobehandlung muss regelmäßig überdacht und überarbeitet werden.

Die oberste Leitung muss die damit verbundenen Risiken kennen und durch Unterschrift die Risikoübernahme akzeptieren.

3 Liste der Referenzdokumente

<i>Doku.</i>	<i>Kurzbezeichnung</i>	<i>Dateiname/V erweis</i>	<i>Version, Datum, Seitenzahl</i>	<i>Relevante Änderungen</i>
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	IT-Strukturanalyse			
A.1.1	Abgrenzung des Informationsverbunds			
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 Gebäude und Räume			
A.2	Schutzbedarfsfeststellung			
A.2.1	Definition der Schutzbedarfskategorien			
A.2.2	Schutzbedarf der IT-Anwendungen			
A.2.3	Schutzbedarf der IT-Systeme			
A.2.4	Schutzbedarf der Kommunikationsverbindungen			
A.2.5	Schutzbedarf der Gebäude und Räume			

<i>Doku.</i>	<i>Kurzbezeichnung</i>	<i>Dateiname/Verweis</i>	<i>Version, Datum, Seitenzahl</i>	<i>Relevante Änderungen</i>
A.3	Modellierung des Informationsverbundes			
A.4	Ergebnis des Basis-Sicherheitschecks			
A.5	Ergänzende Sicherheitsanalyse			
A.6	Risikoanalyse			
A.7	Risikobehandlungsplan			