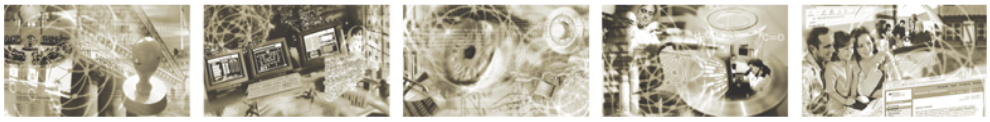
Bundesamt
für Sicherheit in der
Informationstechnik



Muster mit Beispiel

Verifikation des Basis-Sicherheitschecks im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Antragsteller:

Zertifizierungskennung: BSI-XXX-XXXX

Der Inhalt dieses Dokumentes ist „Firmenvertraulich“.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-111
E-Mail: gszertifizierung@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

Versionshistorie

Datum	Version	Verfasser	Bemerkungen
26.10.10	0.99	BSI	Version zur Kommentierung durch Auditoren
30.03.11	1.0	BSI	

1 Verifikation des Basis-Sicherheitschecks

Bei der Vor-Ort-Prüfung wird für jede ausgewählte Bausteinzuordnung durch Inspektion des jeweiligen Zielobjekts überprüft, ob der im Basis-Sicherheitscheck festgestellte Umsetzungsstatus der in diesen Bausteinen enthaltenen Maßnahmen den tatsächlichen Gegebenheiten entspricht.

Die einzelnen Prüfungen sollen direkt am Zielobjekt vor Ort erfolgen, nicht nur anhand der Papierlage. Bei technischen Aspekten bedeutet dies eine Demonstration durch den jeweils zuständigen Administrator oder dessen Vertreter. Zusätzlich wird die Umsetzung der ausgewählten Maßnahmen aus der Ergänzenden Risikoanalyse überprüft.

Zudem muss sichergestellt sein, dass die in der Strukturanalyse (A.1) aufgeführten Eigenschaften der IT-Systeme mit den tatsächlichen Gegebenheiten, wie beispielsweise dem jeweils verwendeten Betriebssystem und dem Aufstellungsort, übereinstimmen.

Die Überprüfung des **Umsetzungsstatus** vorgegeben durch den Antragsteller im Basis-Sicherheitscheck, ist durch den Auditor ist zu überprüfen. Dabei kann das unten angegebene Muster dienen. Alternativ kann der Auditor auch individuelle Prüfprotokolle verwenden, diese müssen aber alle wesentlichen Informationen in geeigneterer 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 **Festfelllungen** 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 Abeichungen (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.

Ergeben sich im Zertifizierungsaudit Abweichungen bzw. Empfehlungen, so sind diese wie folgt zu dokumentieren und abschließend in einer „Liste der Abweichungen und Empfehlungen“ zusammenzufassen. Diese Liste ist dann in den folgenden Überwachungsaudits festzuschreiben.

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.

1.1 Sicherheitsmanagement

Baustein: B.1.0 Sicherheitsmanagement bezogen auf Zielobjekt: gesamter Informationsverbund			
Auditiert am: Auditor(en): Befragt wurde:			
Nr. / Stufe	Maßnahme	Umsetzungs-status	Feststellung
M 2.192 (A)	Erstellung einer Leitlinie zur Informationssicherheit	Ja/Nein/ Teilweise Entbehrlich	teilweise AG_1
Prüfmethode: (I),(S),(A),... Auditfeststellung im Detail mit Nachweisen... ….			
Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist): Es besteht folgender Aktualisierungsbedarf ....AG-1 Behebungsfrist: 1 Überwachungsaudit			
M 2.... (A)	Maßnahmentitel		
Prüfmethode: (I),(S),(A),... Auditfeststellung im Detail mit Nachweisen....			
Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist):			

1.2 Risiko orientierte Auswahl von Bausteinen

1.2.1 Schicht 1

Baustein: B.x ... bezogen auf Zielobjekt: Datensicherungskonzept
Auditiert am: Auditor(en):

Baustein: B.x ...
bezogen auf Zielobjekt: Datensicherungskonzept

Befragt wurde:

Nr.	Maßnahme	Umsetzungs-status	Feststellung
M ... (...)	...		

Prüfmethode: (I),(S),(A),...
Auditfeststellung im Detail mit Nachweisen....
….

M ..... (A)	Maßnahmentitel		

Prüfmethode: (I),(S),(A),...
Auditfeststellung im Detail mit Nachweisen....

Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist):

1.2.2 Schicht 2

Baustein: B.x ...
bezogen auf Zielobjekt: SR OG1 R1.05

Auditiert am:
Auditor(en):
Befragt wurde:

Nr.	Maßnahme	Umsetzungs-status	Feststellung
M ... (...)	Maßnahmentitel		

Prüfmethode: (I),(S),(A),...
Auditfeststellung im Detail mit Nachweisen....
….

Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist):

….

1.3 Im Losverfahren ausgewählte Bausteine

Baustein: B.x ...

bezogen auf Zielobjekt:

Auditiert am:

Auditor(en):

Befragt wurde:

Nr.	Maßnahme	Umsetzungs-status	Feststellung
M ... (...)	...		

Prüfmethode: (I),(S),(A),...

Auditfeststellung im Detail mit Nachweisen....

….

Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist):

M ..... (A)	...		

Prüfmethode: (I),(S),(A),...

Auditfeststellung im Detail mit Nachweisen....

Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist):

1.4 Sicherheitsmaßnahmen aus der Risikoanalyse

Als Ergebnis der Risikoanalyse sind für Komponenten mit hohem oder sehr hohem Schutzbedarf zusätzliche höherwertige Maßnahmen herangezogen worden. Der Umsetzungsstatus der jeweiligen Zielobjekte wurde über alle zusätzlichen Maßnahmen hinweg mit „ja“ angegeben. Der Auditor stellte sicher, dass die hier dokumentierten Ergebnisse mit dem tatsächlich vorhandenen Sicherheitszustand des jeweiligen Zielobjekts übereinstimmen.

Für jede ausgewählte zusätzliche Maßnahme überprüft der Auditor durch Inspektion des jeweiligen Zielobjekts, ob der festgestellte Umsetzungsstatus der Maßnahmen den tatsächlichen Gegebenheiten entspricht, d. h., ob die Maßnahme so wie sie festgelegt wurde, sinnvoll umgesetzt ist, so dass sie den identifizierten Gefährdungen entgegenwirken kann.

Die ausgewählten zusätzlichen Maßnahmen und das Ergebnis der einzelnen Überprüfungen sind im Folgenden dokumentiert.

Maßnahme: bM x.x Maßnahmenname bezogen auf Zielobjekt(e): S-12 Server 1, S-12.... Betroffene Gefährdungen: (b)G 4.12 …..		
Auditiert am: Auditor(en): Befragt wurde:		
Beschreibung der Maßnahme	Umsetzungs-status	Feststellung
Kurzbeschreibung der Maßnahme ...	Ja/Nein/ teilweise	Mangelhaft
Prüfmethode: (I), (S), (A), ... Auditfeststellung im Detail mit Nachweisen		
Feststellung von Abweichungen (Grad der Abweichung; Behebungsfrist):		

…