



Bundesamt
für Sicherheit in der
Informationstechnik

Integration und IT-Revision von Netzübergängen

Teil II: Revisionshilfsmittel



Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

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

© Bundesamt für Sicherheit in der Informationstechnik 2006

Inhaltsverzeichnis

Integration und IT-Revision von Netzübergängen

Teil II: Revisionshilfsmittel

1 Revisionshilfsmittel

Checklisten für den Ablauf einer Revision

Dokumentvorlage für eine Checkliste

Formblätter

Dokumentationsvorlage für einen Revisionsbericht

1. Einleitung

Beteiligte Organisationseinheiten/Personen

2 Vorbereitung der IT-Revision

Prüfplan

3 Durchführung der IT-Revision

Dokumentation

Betriebsprozesse

Architektur

Komponenten

4 Ergebnisse der IT-Revision

Dokumentation

Betriebsprozesse

Architektur

Komponenten

5 Zusammenfassung und Management-Report

6 Handlungsempfehlung

1 Revisionshilfsmittel

Die hier vorgestellten Hilfsmittel unterstützen den Revisor bei der Planung, Durchführung und Dokumentation einer Revision. Dabei werden in diesem Dokument folgende Hilfsmittel angeboten:

- **Checklisten** (s. Kap. 1.1) zur technischen Durchführung der Revision
Die technische Durchführung einer Revision wird durch eine Zusammenstellung einzelner Checklisten unterstützt. Diese sind gemäß der im Leitfaden, Abschnitt 3.1 beschriebenen Kernmodule strukturiert.
Die hier angebotenen Checklisten können als Basis für eigene, weiterverfeinerte Checklisten verwendet werden. Als Grundlage für eigene Ergänzungen können z. B. weiterführende Handbücher (wie [BSI-SICH-GW]) herangezogen werden. Eine leere Dokumentenvorlage für die Checklisten ist daher ebenfalls beigelegt.
- **Formblätter** (s. Kap. 1.2) als organisatorischer Rahmen einer Revision
Während die Checklisten eine technische Orientierung oder auch einen roten Faden für die Revision auf technischer Ebene darstellen, ermöglichen die Formblätter, den organisatorischen Rahmen einer Revision zu strukturieren. Dieser Rahmen umfasst Aspekte wie die Identifizierung des Revisionsobjektes im Detail, die Benennung eines Revisors, die Festlegung eines zeitlichen Rahmens, die Dokumentation der wesentlichen Resultate und Folgerungen sowie ggf. die zeitliche Verfolgung der vorgeschlagenen oder beschlossenen Maßnahmen.
- **Dokumentationsvorlage** (s. Kap. 1.3) als Grundlage für den Revisionsbericht
Ergänzend zu den Hilfsmitteln für die technische Durchführung der Revision und dem organisatorischen Rahmen, die ebenfalls bereits die Dokumentation der Revision unterstützen, ist zusätzlich noch eine Dokumentationsvorlage für den Revisionsbericht beigelegt.

Checklisten für den Ablauf einer Revision

Wie bereits oben angedeutet, stellen die folgenden Checklisten eine Basis für eine IT-Revision von Netzübergängen und den betreffenden Systemen dar. Um die Einsatzmöglichkeiten nicht von vornherein einzuschränken und auch für zukünftige Entwicklungen offen zu halten, wurde ein modularer Ansatz gewählt. Der einzelne Revisor kann sich dadurch im Laufe der Zeit sein eigenes Revisionsinstrumentarium zusammenstellen.

Dabei wurde sowohl Wert auf einen strukturell vollständigen Ansatz gelegt als auch auf eine universell verwendbare Vorgehensweise. Beide Kriterien lassen sich optimal durch einen modularen Ansatz erfüllen, indem die einzelnen Aspekte einer Revision zu vier Kernaspekten gruppiert werden: Dokumentation, Betriebsprozesse, Szenarien und Komponenten.

Die hier dargestellten Checklisten erheben nicht den Anspruch auf Vollständigkeit hinsichtlich aller möglichen Einsatz- und Prüfscenarien: Es sind Situationen denkbar, in denen Szenarien (Architekturen), Betriebsprozesse oder Komponenten angetroffen werden, die derzeit nicht durch konkrete Checklisten beschrieben und abgedeckt werden. Gleichzeitig stellt eine Revision immer die Prüfung dar, inwieweit die Sicherheitsleitlinie einer Organisation implementiert und gelebt wird. Da es aber keine Sicherheitsleitlinie mit universellem Anspruch geben kann, fehlt ein allgemein gültiger Prüfmaßstab. Außerdem kann eine bestehende Maßgabe in einer Leitlinie in unterschiedlicher Weise implementiert werden.

Der modulare Aufbau und die Zusammenstellung der Checklisten eröffnet aber die Möglichkeit, dass vorhandene Checklisten ergänzt und neue erstellt werden. Auf diese Weise können neue Module entstehen und in die Gesamtstruktur integriert werden.

Die Checklisten folgen in ihrer Gliederung der im Teil 1 der Studie vorgeschlagenen Struktur. Die folgende Abbildung I zeigt nochmals die hier verwendete Gliederung.

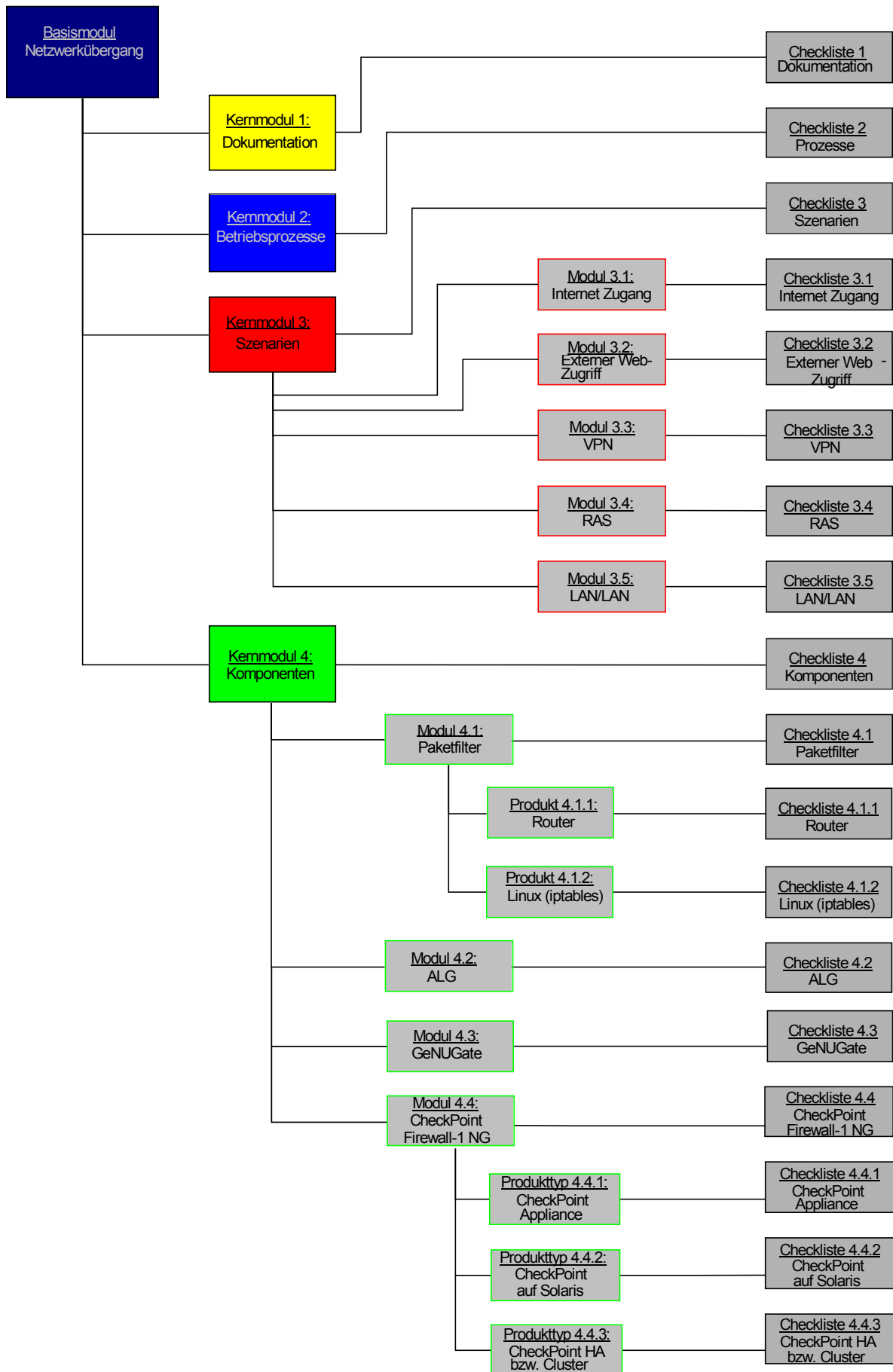


Abbildung 1: Übersicht über die Module und Checklisten.

Beachtet werden sollten dabei die folgenden Hinweise:

- Die Checklisten stellen eine Orientierung dar und bedürfen in der konkreten Prüfung ausnahmslos der Interpretation des fachkundigen Revisors. Insofern sind sie nicht dazu gedacht, technisch unkundigen Personen die Revision eines Netzübergangs zu ermöglichen.
- Die Checklisten beinhalten keine konkreten Systembefehle oder Anleitungen zur Überprüfung einzelner Sachverhalte. Denn je detaillierter eine derartige Anleitung ist, desto eingeschränkter ist ihr Einsatz, da sie für genau ein System mit einem Software-Stand gültig ist und für alle anderen lediglich eingeschränkt oder möglicherweise nicht anwendbar ist. Dies erfordert aber vom Revisor detaillierte Kenntnisse von den betrachteten Systemen und Strukturen. Er muss in der Lage sein, die Prüfkriterien zu verifizieren, um das Gesamtergebnis der Prüfung angemessen beurteilen zu können.
- Einzelne Prüfkriterien müssen individuell betrachtet und bewertet werden. Sie können notwendig oder auch ggf. nicht angemessen sein. Dies muss jeder Revisor individuell und für jede Situation neu entscheiden. In den Checklisten findet man deshalb ein Bemerkungsfeld, in dem die Begründungen für die jeweilige Entscheidung vermerkt werden können.

Weiterführende inhaltliche Hinweise insbesondere bei der Revision von Komponenten findet man in den Dokumentationen, die in der Referenzliste (Teil I, Anlage 4) aufgeführt sind.

Über die Dokumentationen der Referenzliste hinaus sind Vorschläge zu speziellen Maßnahmen bei der Revision von Komponenten der Herstellerdokumentation zu entnehmen. Vielfach finden sich Anregungen auch bei geeigneten Internet-Communities (spezielle Foren, Mailinglisten o. Ä.).

Struktur der Checklisten

Die nachfolgenden Checklisten sind wie folgt aufgebaut:

Checkliste #¹: <Name der Checkliste>

- **Übersichtsartige Beschreibung zum Prüfgegenstand:**
 - Prüfkriterien:
Sie geben einen Überblick über den Prüfzweck und fassen die später folgenden Prüfaspekte zusammen.
 - Vorgehensweise:
Die Vorgehensweise beschreibt die Methoden bei der Prüfung (z. B. Interview, Dokumentensichtung, Konfigurationsprüfung etc.)
 - Beschreibung:
Sie gibt einen zusammenfassenden Überblick über grundlegende Anforderungen in Bezug auf den Prüfgegenstand und beschreibt die spezifischen Ziele der Prüfung. Ferner kann dort beschrieben sein, unter welchen Umständen die Checkliste anzuwenden ist und welche Checklisten ggf. ebenfalls anzuwenden sind.
- Prüfaspekt <Name des Aspekts>:
Der Prüfaspekt beschreibt in Abhängigkeit vom jeweiligen Modul die zu prüfenden Kriterien im Einzelnen. Zu jedem Aspekt werden dazu verschiedene zu beantwortende Fragen gestellt.
- ## <Frage>:
Jede Frage ist innerhalb einer Checkliste eindeutig gekennzeichnet (Nummerierung aus Buchstaben und Zahlen).
- <Antwortfeld>:
Für die Dokumentation der Beantwortung der Fragen empfiehlt sich folgendes Schema:
n(nein) Prüfaspekt ist nicht erfüllt.
c² (compliant) für den Prüfaspekt wurde die Übereinstimmung mit den geltenden Richtlinien festgestellt; ein Nachweistest wurde nicht durchgeführt bzw. ist in dem Kontext nicht sinnvoll.
s² (substantive) für den Prüfaspekt wurde mittels Nachweistest die korrekte Funktion der vorgesehenen Maßnahmen festgestellt.
Für die Mehrzahl der Fragen ist „c“ typischerweise ausreichend. Es empfiehlt sich für Nachweistests entsprechend erweiterte Checklisten zu erstellen, die auf die konkrete Untersuchungsumgebung abgestimmt sind.

Für Erläuterungen und besondere Feststellungen ist zu jedem Prüfaspekt ein Feld „Bemerkungen“ vorgesehen.

¹ Nummerierung s. Abbildung 1

² s. hierzu auch Teil I, Abschnitt 3.1

Checkliste 1: Dokumentation	
Prüfkriterien	Vollständigkeit, Widerspruchsfreiheit und Aktualität der Dokumentation
Vorgehensweise	Interview geeigneter Personen sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die Dokumentation repräsentiert im weitesten Sinne einen festgeschriebenen Katalog konkreter (Sicherheits-)Anforderungen an das zugrunde liegende Objekt. Diese beziehen sich sowohl auf das Objekt selbst (Konfiguration, Architektur, Aufbau) als auch auf Anforderungen bezüglich konkreter Verhaltensweisen und Aktivitäten des Wartungspersonals [Prozeduren³, Anweisungen].</p> <p>Ausschließlich schriftlich dokumentierte Anforderungen können eine kontinuierliche und gleich bleibende Qualität der Umsetzung ermöglichen. Demgegenüber stehen mündliche Überlieferung oder Weitergabe bzw. die Abwesenheit jeder Art von Vorgaben und Anforderungen.</p> <p>Grundlegende Anforderungen sollten als Minimalsatz schriftlich fixiert sein. Dieser Minimalsatz kann – je nach Organisationsgröße – auf mehrere separate Dokumente verteilt oder aber auch in einem einzigen zusammengefasst sein.</p> <p>Grundlegende Anforderungen sind:</p> <ul style="list-style-type: none"> – systemunabhängige Basis-Sicherheitsanforderungen der Organisation (Sicherheitsleitlinie), – Risikoanalyse und resultierende Maßnahmen zur Sicherheit des Netzübergangs (Sicherheitskonzept), – Beschreibung grundlegender betrieblicher Abläufe zur Wartung des Netzübergangs (Betriebskonzept), – aktuelle Dokumentation des Aufbaus, der Konfiguration und des Software-Standes des Netzübergangs (Systemdokumentation), – beschriebene Maßnahmen bei einem Notfall (Notfallvorsorge-Konzept). <p>Die Dokumentation sollte grundsätzlich folgende Kernanforderungen erfüllen:</p> <ul style="list-style-type: none"> – Vollständigkeit: Die Dokumentation sollte als Minimalanforderung im Sinne der obigen Liste vollständig sein. Hierbei ist zu berücksichtigen, dass bestimmte Aspekte möglicherweise zusammengefasst sind oder aber auch auf mehrere Dokumente verteilt sein können. – Korrektheit: die dokumentierten Sachverhalte müssen konsistent und durch die Organisationsleitung abgenommen sein. – Aktualität: Die Dokumentation muss aktuell sein. Dies kann – je nach Dokument – unterschiedliche Bedeutung haben: eine Sicherheitsleitlinie muss den durch die Organisationsleitung verabschiedeten Stand aufweisen; die Systemdokumentation den aktuellen Konfigurationsstand wiedergeben. – Praktikabilität:

³ „Prozedur“ wird hier im Sinne von Ablaufbeschreibung oder Workflow verwendet.

Insbesondere die Wartungsprozeduren sollten, wie beschrieben, durchführbar sein.

– Verfügbarkeit:

Die Dokumentation muss jederzeit für berechtigte Personen verfügbar sein; für nicht berechtigte Personen ist der Zugriff wirkungsvoll auszuschließen.

– Bekanntheit:

Es ist sicherzustellen, dass jeder Person bekannt ist, welche Dokumente für die betreffende Person in welcher Version relevant sind und wo sie zu finden sind.

– Widerspruchsfreiheit:

Die vorhandene Dokumentation muss in ihrer Gesamtheit widerspruchsfrei sein, da sonst die korrekte Anwendung einzelner Dokumente nicht gegeben ist.

Darüber hinaus sollten die einzelnen Dokumente konkrete und typusspezifische Anforderungen erfüllen, die im Folgenden – neben den oben beschriebenen – dargestellt werden.

Prüfaspekt Grundlagen	
A1 Vollständigkeit der Dokumentation	
A1.1	Ist eine Sicherheitsleitlinie vorhanden?
A1.2	Ist ein Sicherheitskonzept für den Netzübergang vorhanden?
A1.3	Ist die Architektur dokumentiert?
A1.4	Ist ein Betriebshandbuch vorhanden?
A1.5	Sind alle relevanten Prozeduren dokumentiert?
A1.6	Sind Systemhandbücher vorhanden?
A1.7	Ist ein Notfallvorsorge-Konzept vorhanden?
Bemerkungen	
A2 Widerspruchsfreiheit	
A2.1	Sind alle dokumentierten Anforderungen und alle Prozeduren sowie andere Angaben widerspruchsfrei?
Bemerkungen	

Prüfaspekt Sicherheitsleitlinie	
B1 Vollständigkeit der Dokumentation	
B1.1	Ist die Sicherheitsleitlinie durch die Organisationsleitung abgenommen?
B1.2	Sind alle Angaben innerhalb der vorgelegten Sicherheitsleitlinie konsistent?
Bemerkungen	
B2 Aktualität	
B2.1	Ist die Sicherheitsleitlinie auf dem aktuellen Stand und gibt sie die aktuellen Organisationsziele wieder?
B2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität der Sicherheitsleitlinie regelmäßig überprüft wird?
Bemerkungen	
B3 Praktikabilität	
B3.1	Sind die dokumentierten Anforderungen praktikabel und realistisch? (Führen sie zum gewünschten Ergebnis?)
B3.2	Sind die dokumentierten Anforderungen zielführend?
Bemerkungen	

Prüfaspekt Sicherheitsleitlinie	
kungen	
B4 Verfügbarkeit	
B4.1	Ist die Sicherheitsleitlinie für die betreffenden Personen in der aktuellen Version verfügbar?
B4.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemer- kungen	
B5 Bekanntheit	
B5.1	Ist die Sicherheitsleitlinie allen relevanten Personen bekannt?
B5.2	Ist in der Sicherheitsleitlinie dokumentiert, welchen Personen diese bekannt sein muss?
Bemer- kungen	
B6 Sicherheitsleitlinie spezifisch	
B6.1	Sind Anforderungen bezüglich Informationssicherheit im Hinblick auf Integrität, Vertraulichkeit und Verfügbarkeit festgelegt?
B6.2	Ist ein Raster definiert, mit dessen Hilfe der Schutzbedarf bestimmt werden kann?
Bemer- kungen	

Prüfaspekt Sicherheitskonzept	
C1 Vollständigkeit der Dokumentation	
C1.1	Ist das Sicherheitskonzept durch die Organisationsleitung abgenommen?
C1.2	Sind alle Angaben innerhalb des vorgelegten Sicherheitskonzepts konsistent?
Bemerkungen	
C2 Aktualität	
C2.1	Ist das Sicherheitskonzept aktuell?
C2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität des Sicherheitskonzepts überprüft wird?
C2.3	Wird nach jeder Änderung der Soft- und Hardware das Sicherheitskonzept aktualisiert?
Bemerkungen	
C3 Praktikabilität	
C3.1	Sind die dokumentierten Sicherheitsmaßnahmen praktikabel und realistisch?
C3.2	Sind die dokumentierten Maßnahmen zielführend?
Bemerkungen	
C4 Verfügbarkeit	
C4.1	Ist das Sicherheitskonzept für die betreffenden Personen in der aktuellen Version verfügbar?
C4.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemerkungen	
C5 Bekanntheit	
C5.1	Ist das Sicherheitskonzept allen relevanten Personen bekannt?
C5.2	Ist im Sicherheitskonzept dokumentiert, welchen Personen dieses bekannt sein muss?
Bemerkungen	
C6 Sicherheitskonzept spezifisch	
C6.1	Sind die Risiken identifiziert und analysiert worden?
C6.2	Sind die Maßnahmen zur Risikominderung beschrieben?
C6.3	Sind die Restrisiken abgeschätzt worden?

Prüfaspekt Sicherheitskonzept	
C6.4 Sind die zugelassenen Dienste dokumentiert?	
C6.5 Sind die Verfahren beschrieben, wie die Dienste abzusichern sind?	
C6.6 Sind die Minimalanforderungen an die Stärke der Authentisierungsverfahren zur Administration der Systeme beschrieben?	
Bemerkungen	

Prüfaspekt Betriebshandbuch	
D1 Korrektheit	
D1.1	Ist das Betriebshandbuch durch die Organisationsleitung abgenommen?
D1.2	Sind alle Angaben innerhalb des vorgelegten Betriebshandbuches konsistent?
D1.3	Ist das Betriebshandbuch vollständig?
Bemerkungen	
D2 Aktualität	
D2.1	Ist das Betriebshandbuch aktuell?
D2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität des Betriebshandbuchs regelmäßig überprüft wird?
Bemerkungen	
D3 Praktikabilität	
D3.1	Sind die beschriebenen Vorgänge und Regelungen praktikabel und realistisch?
D3.2	Sind die dokumentierten Anforderungen zielführend?
Bemerkungen	
D4 Verfügbarkeit	
D4.1	Ist das Betriebshandbuch für die betreffenden Personen in der aktuellen Version verfügbar?
D4.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemerkungen	
D5 Bekanntheit	
D5.1	Ist das Betriebshandbuch allen relevanten Personen bekannt?
D5.2	Ist im Betriebshandbuch dokumentiert, welchen Personen dies bekannt sein muss?
Bemerkungen	
D6 Betriebshandbuch spezifisch	
D6.1	Sind Zuständigkeiten konkreten Rollen/Personen zugewiesen?

Prüfaspekt Prozeduren⁴	
E1 Korrektheit	
E1.1	Sind alle Prozeduren durch die Organisationsleitung abgenommen?
E1.2	Sind alle Angaben innerhalb der vorgelegten Prozeduren konsistent?
Bemerkungen	
E2 Aktualität	
E2.1	Sind alle relevanten Prozeduren auf dem aktuellen Stand?
E2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität der dokumentierten Prozeduren regelmäßig überprüft wird?
Bemerkungen	
E3 Praktikabilität	
E3.1	Sind die dokumentierten Prozeduren praktikabel und realistisch?
E3.2	Sind die dokumentierten Prozeduren zielführend?
E3.3	Sind die dokumentierten Prozeduren sicher durchführbar?
Bemerkungen	
E4 Verfügbarkeit	
E4.1	Sind alle relevanten Prozeduren für die betreffenden Personen in der aktuellen Version jederzeit verfügbar?
E4.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemerkungen	
E5 Bekanntheit	
E5.1	Sind die dokumentierten Prozeduren allen relevanten Personen bekannt?
E5.2	Ist im Betriebskonzept beschrieben, welchen Personen diese Prozeduren bekannt sein müssen?
Bemerkungen	

⁴ „Prozedur“ wird hier im Sinne von Ablaufbeschreibung oder Workflow verwendet.

Prüfaspekt Architekturdokumentation	
F1 Korrektheit	
F1.1	Ist die Architekturdokumentation durch die Organisationsleitung abgenommen?
F1.2	Sind alle Angaben innerhalb der vorgelegten Dokumentation konsistent?
Bemerkungen	
F2 Aktualität	
F2.1	Ist die Architekturdokumentation aktuell?
F2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität der Architekturdokumentation regelmäßig überprüft wird?
Bemerkungen	
F3 Verfügbarkeit	
F3.1	Ist die Architekturdokumentation für die betreffenden Personen in der aktuellen Version jederzeit verfügbar?
F3.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemerkungen	
F4 Bekanntheit	
F4.1	Ist die Architekturdokumentation allen relevanten Personen bekannt?
F4.2	Ist in der Architekturdokumentation beschrieben, welchen Personen diese bekannt sein muss?
Bemerkungen	
F5 Architekturdokumentation spezifisch	
F5.1	Ist ein Netzplan enthalten, der alle Systeme sowie alle Verbindungen zwischen diesen Systemen darstellt?
Bemerkungen	

Prüfaspekt Systemdokumentation	
G1 Korrektheit	
G1.1	Ist die Systemdokumentation durch den Systemverantwortlichen abgenommen?
G1.2	Sind alle Angaben innerhalb der vorgelegten Systemdokumentation konsistent?
Bemerkungen	
G2 Aktualität	
G2.1	Gibt die Systemdokumentation die aktuellen Softwarestände wieder?
G2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität der Systemdokumentation regelmäßig überprüft wird?
Bemerkungen	
G3 Verfügbarkeit	
G3.1	Ist die Systemdokumentation für die betreffenden Personen in der aktuellen Version jederzeit verfügbar?
G3.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemerkungen	
G4 Bekanntheit	
G4.1	Ist die Systemdokumentation allen relevanten Personen bekannt?
G4.2	Ist in der Systemdokumentation beschrieben, welchen Personen diese bekannt sein muss?
Bemerkungen	
G5 Systemdokumentation spezifisch	
G5.1	Sind die aktuellen Konfigurationsparameter vollständig und für jedes System dokumentiert?
G5.2	Ist die zeitliche Entwicklung der Konfiguration aus der Dokumentation ersichtlich, sodass jede Konfiguration zu einem späteren Zeitpunkt rekonstruiert werden kann?
G5.3	Ist dokumentiert, welche Person/Funktion welche Modifikationen am System vorgenommen hat?
G5.4	Ist der Systemaufbau vollständig dokumentiert – mit Hardware-Anordnung, Verkabelung, Einzelsystemaufbau?
Bemerkungen	

Prüfaspekt Systemhandbücher	
H1 Aktualität	
H1.1	Sind die vorhandenen Systemhandbücher aktuell?
H1.2	Wird mit neuen Systemen oder neuer Software automatisch auch die dazugehörige Systemdokumentation angeschafft?
Bemerkungen	
H2 Verfügbarkeit	
H2.1	Sind alle relevanten Systemhandbücher für die betreffenden Personen in der aktuellen Version jederzeit verfügbar?
H2.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
Bemerkungen	
H3 Bekanntheit	
H3.1	Sind die Systemhandbücher allen relevanten Personen bekannt?
H3.2	Ist im Betriebskonzept beschrieben, welchen Personen diese Handbücher bekannt sein müssen?
Bemerkungen	

Prüfaspekt Notfallvorsorge-Konzept	
I1 Korrektheit	
I1.1	Ist das Notfallvorsorge-Konzept durch die Organisationsleitung abgenommen?
I1.2	Sind alle Angaben innerhalb des vorgelegten Notfallvorsorge-Konzepts konsistent?
Bemerkungen	
I2 Aktualität	
I2.1	Ist das Notfallvorsorge-Konzept aktuell?
I2.2	Sind feste Intervalle vorgesehen, nach deren Ablauf die Aktualität des Notfallvorsorge-Konzeptes regelmäßig überprüft wird?
Bemerkungen	
I3 Praktikabilität	
I3.1	Sind die dokumentierten Anforderungen praktikabel und realistisch?
I3.2	Sind die dokumentierten Anforderungen zielführend?
Bemerkungen	
I4 Verfügbarkeit	
I4.1	Ist das Notfallvorsorge-Konzept für die betreffenden Personen in der aktuellen Version verfügbar?
I4.2	Wird der Zugriff für nicht berechtigte Personen wirkungsvoll unterbunden?
I4.3	Ist sichergestellt, dass das Konzept sowie die erforderlichen Notfallprozeduren auch in Notfällen verfügbar und zugreifbar sind?
Bemerkungen	
I5 Bekanntheit	
I5.1	Ist das Notfallvorsorge-Konzept allen relevanten Personen bekannt?
I5.2	Ist im Notfallvorsorge-Konzept dokumentiert, welchen Personen dieses bekannt sein muss?
Bemerkungen	
I6 Notfallvorsorge-Konzept spezifisch	
I6.1	Sind Notfallklassen oder -fälle definiert?
I6.2	Sind konkrete Handlungsanweisungen für die einzelnen Klassen beschrieben?

Prüfaspekt Notfallvorsorge-Konzept		
I6.3	Sind Eskalationsprozeduren beschrieben?	
I6.4	Sind alle relevanten Kontaktdaten dokumentiert und aktuell?	
I6.5	Ist ein Alarmierungsplan beschrieben?	
I6.6	Sind die Verantwortlichkeiten in einem Notfall festgelegt?	
I6.7	Sind Handlungs- und Kommunikationsalternativen vorgesehen und beschrieben?	
I6.8	Sind (regelmäßige) Tests oder Notfallübungen vorgesehen?	
I6.9	Fließen die Resultate der Tests und Übungen als Verbesserung in das Notfallvorsorge-Konzept ein?	
Bemerkungen		

Checkliste 2: Betriebsprozesse	
Prüfkriterien	Vollständigkeit, Korrektheit und Praktikabilität der Betriebsprozesse
Vorgehensweise	Interview geeigneter Personen sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Jedes Computersystem braucht für seine korrekte und beabsichtigte Funktion eine Reihe von regelmäßig bzw. unregelmäßig wiederkehrenden oder auch einmaligen, spontanen Tätigkeiten oder Arbeiten.</p> <p>Wesentliche, betriebliche Prozesse eines Netzübergangs sind:</p> <ul style="list-style-type: none">- Beschaffung neuer Hardware oder Software,- Integration weiterer Netzübergänge,- Regelmäßige und spontane Wartungsprozesse,- Änderung der Konfiguration,- Softwarepflege,- Fehlerbeseitigung,- Hardwareaustausch,- Backup,- Notfallbearbeitung,- Außerbetriebnahme von Systemen oder Komponenten,- Reporting,- Monitoring. <p>Als Minimalforderung sollten diese Betriebsprozesse mindestens vorhanden sein. Idealerweise sind sie dokumentiert und werden auch regelmäßig aktualisiert und an veränderte Situationen und Systeme angepasst.</p>

Prüfaspekt Grundlagen	
A1 Existenz zentraler Betriebsprozesse	
A1.1	Existiert ein Beschaffungsprozess für Hard- und Software?
A1.2	Existiert ein Integrationsprozess?
A1.3	Existieren zentrale Wartungsprozesse?
A1.4	Existiert ein Änderungsprozess?
A1.5	Existiert ein Prozess zur Softwarepflege?
A1.6	Existiert ein Prozess zur Fehlerbeseitigung?
A1.7	Existiert ein Prozess zum Hardwareaustausch?
A1.8	Existiert ein Datensicherungsprozess?
A1.9	Existiert ein Notfallprozess?
A1.10	Existiert ein Prozess zur Außerbetriebnahme von Systemen?
A1.11	Existiert ein Reporting-Prozess?
A1.12	Existiert ein Monitoring-Prozess?
Bemerkungen	
A2 Vollständigkeit	
A2.1	Wird der vollständige Lebenszyklus durch Betriebsprozesse lückenlos abgebildet?
A2.2	Gibt es Überlappungen bei unterschiedlichen Betriebsprozessen?
Bemerkungen	
A3 Bekanntheit	
A3.1	Sind allen relevanten Personen/Rollen die für sie notwendigen Betriebsprozesse bekannt?
Bemerkungen	

Prüfaspekt Einkauf (Beschaffung) von Hard- und Software	
B1 Verantwortung für den Beschaffungsprozess und Dokumentation	
B1.1	Ist ein Verantwortlicher für den Beschaffungsprozess benannt?
B1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
B1.3	Ist der Beschaffungsprozess, so wie er ausgeführt wird, dokumentiert?
B1.4	Wird der vorab dokumentierte Beschaffungsprozess regelmäßig mit dem tatsächlich ausgeführten Beschaffungsprozess abgeglichen?
Bemerkungen	
B2 Aktualität	
B2.1	Ist der Beschaffungsprozess an der aktuell vorhandenen Soft- und Hardware ausgerichtet?
B2.2	Ist sichergestellt, dass bei der Beschaffung aktuelle Entwicklungen berücksichtigt werden?
Bemerkungen	
B3 Beschaffungsprozess spezifisch	
B3.1	Wird eine Bedarfsanalyse vor einer Beschaffung durchgeführt?
B3.2	Werden die betroffenen Nutzer ggf. nach deren Anforderungen befragt?
B3.3	Werden Vergleichsangebote eingeholt und ausgewertet?
B3.4	Werden ggf. andere Organisationen, die Vergleichssysteme und Installationen betreiben, konsultiert und befragt?
B3.5	Werden ausgewählte Systeme in Testumgebungen geprüft?
B3.6	Wird eine Abnahmeprüfung durchgeführt?
Bemerkungen	

Prüfaspekt Integration eines Netzübergangs	
C1 Verantwortung für den Integrationsprozess und Dokumentation	
C1.1	Ist ein Verantwortlicher für den Integrationsprozess benannt?
C1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
C1.3	Ist der Integrationsprozess, so wie er ausgeführt wird, dokumentiert?
C1.4	Wird der vorab dokumentierte Integrationsprozess regelmäßig mit dem tatsächlich ausgeführten Prozess abgeglichen?
Bemerkungen	
C2 Aktualität	
C2.1	Ist der Integrationsprozess an den vorhandenen Systemen orientiert?
Bemerkungen	
C3 Integration spezifisch	
C3.1	Wird bei der Planung zur Integration eine Anforderungsanalyse sowie eine Schutzbedarfsanalyse durchgeführt?
C3.2	Wird parallel dazu der Ist-Stand des Netzübergangs analysiert und aufgenommen?
C3.3	Werden Testszenarien gemäß den gestellten Anforderungen bereitgestellt?
C3.4	Werden Auswahlssysteme gegeneinander getestet und bewertet?
C3.5	Werden neue Systeme vor dem Produktiveinsatz vollständig getestet?
C3.6	Erfolgt eine formale Produktabnahme vor dem Produktiveinsatz?
Bemerkungen	

Prüfaspekt Wartung	
D1 Verantwortung für den Wartungsprozess und Dokumentation	
D1.1	Ist ein Verantwortlicher für den Wartungsprozess benannt?
D1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
D1.3	Sind die Wartungsprozesse, so wie sie ausgeführt werden, dokumentiert?
D1.4	Werden die vorab dokumentierten Wartungsprozesse regelmäßig mit den tatsächlich ausgeführten Prozessen abgeglichen?
Bemerkungen	
D2 Aktualität	
D2.1	Ist der Wartungsprozess an den aktuellen Systemen ausgerichtet?
D2.2	Wird der Wartungsprozess regelmäßig auf konsistente und effiziente Funktionsweise überprüft?
Bemerkungen	
D3 Wartung spezifisch	
D3.1	Sind regelmäßige Intervalle festgelegt, in denen definierte Systeme auf konsistente Funktion bzw. Fehlfunktionen geprüft werden?
D3.2	Gibt es einen Wartungsplan, welche Systeme durch wen (intern, extern) gewartet werden?
D3.3	Sind für alle Systeme, die extern gewartet werden, gültige Verträge abgeschlossen?
D3.4	Sind alle Lizenzen durch Wartungsverträge abgesichert?
D3.5	Sind Ereignisse definiert, bei deren Auftreten eine Wartung durchzuführen ist?
D3.6	Ist mit dem Abschluss der Wartung ein Report verbunden?
Bemerkungen	

Prüfaspekt Änderungen	
E1 Verantwortung für den Änderungsprozess und Dokumentation	
E1.1	Ist ein Verantwortlicher für den Änderungsprozess benannt?
E1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
E1.3	Sind die Änderungsprozesse, so wie sie ausgeführt werden, dokumentiert?
E1.4	Werden die vorab dokumentierten Änderungsprozesse regelmäßig mit den tatsächlich ausgeführten Prozessen abgeglichen?
Bemerkungen	
E2 Aktualität	
E2.1	Ist der Änderungsprozess an den aktuellen Systemen ausgerichtet?
E2.2	Wird der Änderungsprozess regelmäßig auf konsistente und effiziente Funktionsweise überprüft?
Bemerkungen	
E3 Änderung spezifisch	
E3.1	Sind regelmäßige Intervalle festgelegt, in denen die Systeme auf durchgeführte Änderungen geprüft werden?
E3.2	Gibt es einen Änderungsplan, an welchen Systemen durch wen (intern, extern) Änderungen durchgeführt werden?
E3.3	Sind für alle Systeme, an denen von extern Änderungen durchgeführt werden, gültige Verträge abgeschlossen?
E3.4	Sind Ereignisse definiert, bei deren Auftreten definierte Änderungen durchgeführt werden?
E3.5	Ist mit dem Abschluss der Änderungsmaßnahmen ein Report verbunden?
Bemerkungen	
Prüfaspekt Softwarepflege	
F1 Verantwortung für den Softwarepflegeprozess und Dokumentation	
F1.1	Ist ein Verantwortlicher für die Softwarepflege benannt?
F1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
F1.3	Sind die Prozesse zur Softwarepflege, so wie sie ausgeführt werden, dokumentiert?
F1.4	Werden die vorab dokumentierten Softwarepflegeprozesse regelmäßig mit den tatsächlich ausgeführten Prozessen abgeglichen?
Bemerkungen	

F2 Aktualität	
F2.1	Sind die momentan gültigen Softwarepflegeprozesse aktuell?
F2.2	Wird der Softwarepflegeprozess regelmäßig auf konsistente und effiziente Funktionsweise überprüft?
Bemerkungen	
F3 Softwarepflege spezifisch	
F3.1	Sind regelmäßige Intervalle festgelegt, in denen die Softwarestände der Systeme überprüft werden?
F3.2	Werden vor dem Austausch von Software Tests durchgeführt?
F3.3	Gibt es einen Softwarepflegeplan, an welchen Systemen durch wen (intern, extern) Softwarepflege durchgeführt wird?
F3.4	Sind für alle Systeme, an denen von extern Softwarepflege durchgeführt wird, gültige Verträge abgeschlossen?
F3.5	Sind Ereignisse definiert, bei deren Auftreten Softwarepflege durchgeführt wird?
F3.6	Ist mit dem Abschluss der Softwarepflegemaßnahmen ein Report verbunden?
Bemerkungen	
Prüfaspekt Fehlerbeseitigung	
G1 Verantwortung für den Fehlerbeseitigungsprozess und Dokumentation	
G1.1	Ist ein Verantwortlicher für die Fehlerbeseitigungen benannt?
G1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
G1.3	Sind die Prozesse zur Fehlerbeseitigung, so wie sie ausgeführt werden, dokumentiert?
G1.4	Werden die vorab dokumentierten Fehlerbeseitigungen regelmäßig mit den tatsächlich ausgeführten Prozessen abgeglichen?
Bemerkungen	
G2 Aktualität	
G2.1	Sind die momentan gültigen Fehlerbeseitigungsprozesse aktuell?
G2.2	Wird der Fehlerbeseitigungsprozess regelmäßig auf konsistente und effiziente Funktionsweise überprüft?
Bemerkungen	
G3 Fehlerbeseitigung spezifisch	

G3.1	Sind regelmäßige Intervalle festgelegt, in denen die Systeme auf Fehler überprüft werden?	
G3.2	Gibt es einen Fehlerbeseitigungsplan, an welchen Systemen durch wen (intern, extern) Fehlerbeseitigung durchgeführt wird?	
G3.3	Sind für alle Systeme, an denen von extern Fehlerbeseitigung durchgeführt wird, gültige Verträge abgeschlossen?	
G3.4	Sind Fehler mit unterschiedlichen Reaktionszeiten definiert?	
G3.5	Ist mit dem Abschluss der Fehlerbeseitigungsmaßnahmen ein Report verbunden?	
Bemerkungen		
Prüfaspekt Hardware-Austausch		
H1 Verantwortung für den Hardware-Austauschprozess und Dokumentation		
H1.1	Ist ein Verantwortlicher für den Hardware-Austausch benannt?	
H1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?	
H1.3	Sind die Prozesse zum Hardware-Austausch, so wie sie ausgeführt werden, dokumentiert?	
H1.4	Werden die vorab dokumentierten Hardware-Austauschprozesse regelmäßig mit den tatsächlich ausgeführten Prozessen abgeglichen?	
Bemerkungen		
H2 Aktualität		
H2.1	Sind die momentan gültigen Hardware-Austauschprozesse aktuell?	
H2.2	Wird der Hardware-Austauschprozess regelmäßig auf konsistente und effiziente Funktionsweise überprüft?	
Bemerkungen		
H3 Hardwareaustausch spezifisch		
H3.1	Sind regelmäßige Intervalle festgelegt, in denen die Systeme auf fehlerhafte Hardware überprüft werden?	
H3.2	Wird Austauschhardware zentral gelagert bzw. sind die Lagerorte dokumentiert und bekannt?	
H3.3	Gibt es einen Hardware-Austauschplan, an welchen Systemen durch wen (intern, extern) Hardware-Austausch durchgeführt wird?	
H3.4	Werden vor dem Austausch Tests durchgeführt?	
H3.5	Sind für alle Systeme, an denen von extern Hardware-Austausch durchgeführt wird, gültige Verträge abgeschlossen?	
H3.6	Ist mit dem Abschluss der Hardware-Austauschmaßnahmen ein Report verbunden?	

Bemerkungen	
Prüfaspekt Datensicherung	
I1 Verantwortung für den Backup-Prozess und Dokumentation	
I1.1 Ist ein Verantwortlicher für den Backup-Prozess benannt?	
I1.2 Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?	
I1.3 Ist der Backup-Prozess, so wie er ausgeführt wird, dokumentiert?	
I1.4 Wird der vorab dokumentierte Backup-Prozess regelmäßig mit dem tatsächlich ausgeführten Prozess abgeglichen?	
Bemerkungen	
E2 Aktualität	
I2.1 Orientiert sich der Backup-Prozess an den aktuellen Gegebenheiten und Anforderungen?	
I2.2 Wird die Funktionalität und Effizienz des Backup-Prozesses regelmäßig überprüft?	
Bemerkungen	
E3 Backup spezifisch	
I3.1 Werden Backup-Systeme bei entsprechender System-Verfügbarkeitsanforderung vorgehalten?	
I3.2 Sind ggf. Verträge mit System-Lieferanten abgeschlossen?	
I3.3 Sind alle aktuellen System-Konfigurationen gesichert?	
I3.4 Liegen für alle Systeme aktuelle Backups (Images) vor?	
I3.5 Sind ggf. Backup-Daten und gesicherte Konfigurationsdaten geografisch getrennt gelagert?	
I3.6 Werden Backup- und Konfigurationsdaten regelmäßig auf Einspielbarkeit geprüft?	
Bemerkungen	

Prüfaspekt Bearbeitung des Notfallvorsorge-Konzepts	
J1 Verantwortung für den Notfallprozess und Dokumentation	
J1.1	Ist ein Verantwortlicher für den Notfallprozess benannt?
J1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
J1.3	Sind die Notfallprozesse, so wie sie ausgeführt werden, dokumentiert?
J1.4	Werden die vorab dokumentierten Notfallprozesse regelmäßig mit den tatsächlich ausgeführten Prozessen abgeglichen?
Bemerkungen	
J2 Aktualität	
J2.1	Sind die momentan gültigen Notfallprozesse aktuell?
J2.2	Werden die Notfallprozesse regelmäßig auf Aktualität überprüft?
Bemerkungen	
J3 Notfallprozess spezifisch	
J3.1	Sind Notfallprozesse für alle wichtigen Systeme beschrieben?
J3.2	Werden diese Notfallprozesse regelmäßig auf Durchführbarkeit und Praktikabilität getestet?
J3.3	Fließen die Erkenntnisse der Testauswertung in die Notfallprozesse ein?
Bemerkungen	

Prüfaspekt Außerbetriebnahme von Systemen oder Komponenten	
K1 Verantwortung für die Außerbetriebnahme von Systemen oder Komponenten und Dokumentation	
K1.1	Ist ein Verantwortlicher für den Prozess zur Außerbetriebnahme benannt?
K1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
K1.3	Ist der Prozess der Außerbetriebnahme, so wie er ausgeführt wird, dokumentiert?
K1.4	Wird der vorab dokumentierte Prozess zur Außerbetriebnahme regelmäßig mit dem tatsächlich ausgeführten Prozess abgeglichen?
Bemerkungen	
K2 Aktualität	
K2.1	Sind die Prozesse zur Außerbetriebnahme aktuell?
K2.2	Werden neueste Erkenntnisse bezüglich Datenwiederherstellungsmöglichkeiten auf Relevanz untersucht?
Bemerkungen	
K3 Außerbetriebnahme spezifisch	
K3.1	Sind alle Systeme klassifiziert, wie sie zu entsorgen sind?
K3.2	Ist sichergestellt, dass Datenträger mit sensiblen Informationen zuverlässig gelöscht/zerstört werden vor der Entsorgung?
K3.3	Ist ein Prozess zur zentralen Sammlung sensibler Datenträger eingerichtet?
K3.4	Sind Sammelstellen eingerichtet?
Bemerkungen	

Prüfaspekt Reporting (Berichtswesen)	
L1 Verantwortung für den Reporting-Prozess und Dokumentation	
L1.1	Ist ein Verantwortlicher für den Reporting-Prozess benannt?
L1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
L1.3	Ist der Reporting-Prozess, so wie er ausgeführt wird, dokumentiert?
L1.4	Wird der vorab dokumentierte Reporting-Prozess regelmäßig mit dem tatsächlich ausgeführten Prozess abgeglichen?
Bemerkungen	
L2 Aktualität	
L2.1	Sind die Reporting-Prozesse aktuell?
L2.2	Wird die aktuelle Organisationsstruktur berücksichtigt?
L2.3	Wird die Aktualität regelmäßig überprüft?
Bemerkungen	
L3 Reporting spezifisch	
L3.1	Sind Eskalationsprozeduren allen relevanten Personen bekannt?
L3.2	Sind die relevanten Ansprechpartner allen anderen bekannt?
L3.3	Gibt es Übersichten, welcher Ansprechpartner für welches Gebiet zuständig ist?
L3.4	Gibt es Übersichten, welche Ereignisse oder Sachverhalte dem Reporting unterliegen?
Bemerkungen	

Prüfaspekt Monitoring	
M1 Verantwortung für den Monitoring-Prozess und Dokumentation	
M1.1	Ist ein Verantwortlicher für den Monitoring-Prozess benannt?
M1.2	Sind die Aufgaben und Pflichten beschrieben und werden diese wahrgenommen?
M1.3	Ist der Monitoring-Prozess, so wie er ausgeführt wird, dokumentiert?
M1.4	Wird der vorab dokumentierte Monitoring-Prozess regelmäßig mit dem tatsächlich ausgeführten Prozess abgeglichen?
Bemerkungen	
M2 Aktualität	
M2.1	Ist der Monitoring-Prozess aktuell?
M2.2	Werden alle derzeit betriebenen Systeme berücksichtigt?
M2.3	Wird die Aktualität regelmäßig überprüft?
Bemerkungen	
M3 Monitoring-Prozess spezifisch	
M3.1	Sind die Systeme festgelegt, die einem Monitoring unterliegen?
M3.2	Sind die verantwortlichen Rollen/Personen durch einen Plan festgelegt?
M3.3	Ist festgelegt, was zu überwachen ist?
M3.4	Ist ein Pfad zum Reporting beschrieben?
M3.5	Sind Eskalationsprozesse beschrieben?
Bemerkungen	

Checkliste 3: Szenarien	
Prüfkriterien	Allgemeine Anforderungen an eine Netzkopplung Anforderungen an die Architektur Umsetzungsgrad der erforderlichen Sicherheitsgrundfunktionen
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Netzübergänge haben in der Regel – und im Verständnis dieser Checkliste – Funktionalitäten zu erfüllen, die über die reine Verbindung unterschiedlicher Netztechniken, wie Protokolle oder Transportmedien, weit hinausgehen. Typische Netzkopplungsszenaren sind:</p> <ul style="list-style-type: none">– Internet-Zugang,– Externer Web-Zugriff,– VPN,– RAS,– LAN/LAN. <p>Neben den individuellen Anforderungen an unterschiedliche Netzkopplungsszenarien bestehen darüber hinaus eine Reihe von grundsätzlichen Anforderungen (Sicherheitsgrundfunktionen), die je nach Ausprägung und Art der Nutzung des Netzübergangs stärker oder schwächer ausgeprägt sein können.</p> <p>In der vorliegenden Checkliste werden, unabhängig von der individuellen Realisierung, allgemeine Anforderungen an eine Netzkopplung als Fragestellung für eine IT-Revision formuliert.</p>

Prüfaspekt Architektur	
A1 Konzeption	
A1.1	Existieren Sicherheitsvorgaben ⁵ für die Architektur?
A1.2	Sind in der Architektur Bereiche mit unterschiedlichen Sicherheitsstufen (Sicherheitszonen ⁶) identifiziert worden?
A1.3	Ist das Sicherheitsgefälle an den Übergängen zwischen den identifizierten Sicherheitszonen klassifiziert worden und sind daraus Sicherheitsanforderungen ⁷ an die Architektur abgeleitet worden?
A1.4	Sind alle Komponenten und Strukturen des Netzübergangs anhand einer einheitlichen Namenskonvention bezeichnet?
Bemerkungen	
A2 Implementierung	
A2.1	Sind die Sicherheitsvorgaben in der Architektur implementiert worden?
A2.2	Sind die identifizierten Sicherheitszonen in der Architektur konsequent umgesetzt worden? Ist der Netzübergang – gemessen am Schutzbedarf der verbundenen Netze – entsprechend mehrstufig ausgelegt?
A2.3	Gibt es dem Schutzbedarf und dem Sicherheitsgefälle angemessene Sicherheitsgateways (einstufig oder mehrstufig, Paketfilter und/oder Application Level Gateways) zwischen den Zonen?
A2.4	Kann ein Umgehen der implementierten Sicherheitsstruktur ausgeschlossen werden?
A2.5	Wird der Nutzdatenverkehr systematisch von anderem Datenverkehr ⁸ getrennt durch ein separates Netz geführt?
A2.6	Sind die Verfügbarkeitsanforderungen ⁹ in der Architektur angemessen berücksichtigt worden?
A2.7	Erfolgt die Protokollierung/Beweissicherung getrennt von den Nutzsyste-men auf separaten Systemen?
A2.8	Sind etwaige in der Architektur vorgesehenen Überwachungselemente (z. B. IDS - Intrusion Detection System und weitere Früherkennungssysteme) implementiert worden?
Bemerkungen	

⁵ Verfügbarkeit, Integrität, Vertraulichkeit

⁶ Beispiele: Internet, Extranet, Management-LAN, Business DMZ

⁷ Identifikation und Authentisierung, Datenflusskontrolle, Beweissicherung, Verschlüsselungsfunktionen

⁸ Hierzu sind zu zählen z. B.: Management der Komponenten, Betriebsüberwachung, Kommunikation von Einzelkomponenten untereinander (z. B. heartbeat bei HA-Komponenten), Datensicherung, Protokollierung und Beweissicherung

⁹ Ausfallsicherheit durch Redundanz, hot stand by, cold stand by, Übernahme von Sessions bei Ausfall einer Komponente, Vermeidung von single point of failures

Prüfaspekt Sicherheitsgrundfunktionen	
B1 Identifikation und Authentisierung	
B1.1	Können die Nutzer des Netzübergangs den Anforderungen entsprechend in hinreichender Stärke identifiziert und authentisiert werden?
Bemerkungen	
B2 Datenflusskontrolle	
B2.1	Besteht jederzeit die erforderliche Kontrolle über die Daten, die über den Netzübergang transferiert werden?
Bemerkungen	
B3 Beweissicherung	
B3.1	Werden – entsprechend den Sicherheitsanforderungen – Verbindungsinformationen (Adresse, Zeit, Nutzer, Datenklassifizierung) sowie ggf. Zusatzinformationen bei kritischen Ereignissen aufgezeichnet und aufbewahrt?
B3.2	Werden die Protokollierungsdaten der unterschiedlichen Komponenten mit zeitsynchronen Marken generiert?
B3.3	Findet eine zentrale Auswertung der Protokolle statt?
Bemerkungen	
B4 Übertragungssicherung und Schlüsselmanagement	
B4.1	Ist die Übertragung der Daten und Informationen entsprechend ihrem Schutzbedarf abgesichert?
B4.1	Bestehen zuverlässige Verfahren zur Schlüsselerzeugung, -verteilung, -speicherung sowie zum Zurückziehen einzelner Schlüssel?
Bemerkungen	

Checkliste 3.1: Szenario Internet-Zugang	
Prüfkriterien	Struktur und Auslegung eines Internet-Zuganges Funktionale Aspekte Verbindungskontrolle
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Im Szenario „Internet-Zugang“ geht es darum, ein internes, vertrauenswürdigenes Netz an das Internet anzubinden. Im Wesentlichen werden dabei Internet-Dienste für Systeme im internen Netz zugänglich gemacht, typischerweise browsen, Mail abholen und versenden oder Dateien transferieren.</p> <p>Charakteristisch für dieses Szenario ist die grundsätzliche Eigenschaft, dass Datenverbindungen immer von eigenen Systemen in das Internet initiiert werden. Jeder aktive Verbindungsaufbau von Internet-Systemen zu eigenen Systemen ist somit nicht zulässig und wird unterbunden.</p> <p>Als Variante dieses Grundszenarios „Internet-Zugang“ können zwei Erweiterungen gelten:</p> <ul style="list-style-type: none"> – Eingehende Mail wird nicht von internen Systemen abgeholt, sondern von externen Systemen einem internen System in das vertrauenswürdige Netz zugestellt: In diesem Fall müssen spezielle Datenverbindungen (Mail-Transfer, SMTP-Protokoll) eingeschränkt vom Internet aus in das vertrauenswürdige Netz möglich sein. – Es werden Informationen auf öffentlich zugänglichen Servern innerhalb des vertrauenswürdigen Netzes bereitgestellt. In diesem Fall müssen spezielle Datenverbindungen (HTTP-Protokoll sowie ggf. File-Transfer, FTP-Protokoll) eingeschränkt vom Internet aus in das vertrauenswürdige Netz möglich sein. <p>Im Unterschied zum Szenario „Externer Web-Zugriff“ beschränkt sich die Bereitstellung von Informationen auf öffentlich zugänglichen Systemen auf statische Dokumente, so dass die eigenen öffentlich zugänglichen Systeme keine aktiven Verbindungen zu weiteren Systemen in das interne Netz aufbauen müssen.</p> <p>Ist dies nicht der Fall, ist zusätzlich das Szenario „Externer Web-Zugriff“ (s. Checkliste 3.2) heranzuziehen.</p> <p>Neben der vorliegenden Checkliste für das Szenario „Internet-Zugang“ ist die Checkliste 3 für das Modul „Szenarien“ heranzuziehen. In der Checkliste 3 werden eine Reihe von grundsätzlichen Fragen insbesondere hinsichtlich der Sicherheitsgrundfunktionen an Netzübergänge gestellt.</p>

Prüfaspekt Dimensionierung	
A1 Skalierbarkeit und Auslastung	
A1.1 Decken die vorhandenen Lizenzen der eingesetzten Komponenten die zu erwartende Nutzauslastung ¹⁰ ab?	

	A1.2 Besteht die Möglichkeit der Lizenzerweiterung bei höherer Auslastung?	
	A1.3 Kann der Zugang den angeforderten Netzverkehr bewältigen?	
	A1.4 Wird die Systemauslastung kontinuierlich überwacht?	
Bemerkungen		
A2 Verfügbarkeit		
	A2.1 Erfüllt der Internet-Zugang die Verfügbarkeitsanforderungen der Nutzer?	
	A2.2 Sind Single Points of Failure vorhanden?	
	A2.3 Sind alternative Anbindungen vorhanden und aktiv?	
Bemerkungen		

¹⁰ Je nach Lizenzmodell abhängig von Durchsatz, Anzahl der Schnittstellen, Anzahl Nutzer (Gesamtzahl oder Anzahl gleichzeitig aktiver Nutzer), Anzahl Systeme (Gesamtzahl oder Anzahl gleichzeitig aktiver Systeme)

Prüfaspekt Schutz des vertrauenswürdigen Netzes	
B1 Struktur	
B1.1	Weist der Internet-Zugang eine angemessene Sicherheitsstruktur auf? Ist der Zugang abgesichert durch eine kaskadierte Kette von Paketfilter – Application-Level-Gateway – Paketfilter?
B1.2	Ist jedes Teilnetz (internes Netz, ggf. DMZ) angemessen abgesichert und geschützt?
B1.3	Sind sensible Systeme isoliert abgesichert (z. B. Web-, Mail- oder DNS-Server)?
B1.4	Ist eine sichere und vertrauenswürdige Administration gegeben?
Bemerkungen	
B2 Kontrolle der Verbindungen	
B2.1	Ist die Kommunikation vom vertrauenswürdigen Netz in das Internet auf zugelassene Dienste eingeschränkt?
B2.2	Wird die Kommunikation vom Internet in das vertrauenswürdige Netz unterbunden? Sind Zugriffe aus dem Internet in das vertrauenswürdige Netz ausschließlich in eine Sicherheitszone (DMZ) erlaubt?
B2.3	Werden die zugelassenen Dienste auf Applikationsebene kontrolliert (Proxy)?
B2.4	Erfolgt an der Schnittstelle zum Internet eine wirksame Kontrolle auf unerwünschte Inhalte (Viren, aktive Inhalte)?
B2.5	Gibt es eine default-deny-policy (grundsätzliches Kommunikationsverbot mit definierten Ausnahmen)?
Bemerkungen	

Checkliste 3.2: Szenario Externer Web-Zugriff	
Prüfkriterien	Struktur und Auslegung eines externen Web-Zugriffs Funktionale Aspekte Verbindungskontrolle
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Das Szenario „Externer Web-Zugriff“ stellt eine Erweiterung des Internet-Zugangs dar, bei dem mehr oder weniger umfangreiche eigene Dienste für externe Verbindungsanfragen angeboten werden. Dabei werden je nach Bedarf mehrere Teilnetze mit gestaffelten Vertrauensstufen gebildet und jeweils durch ein Sicherheitsgateway gegeneinander abgesichert.</p> <p>Die vorliegende Checkliste ist dabei so zu interpretieren, dass hiermit nur das öffentlich zugängliche Angebot des externen Web-Zugriffs abgedeckt wird. Sämtliche Fragestellungen und Prüfungen beziehen sich ausschließlich auf die Bereitstellung eigener Dienste für die Öffentlichkeit.</p> <p>Wenn der für den externen Web-Zugriff genutzte Internet-Zugang gleichzeitig für die Bereitstellung von Internet-Diensten für interne Systeme dient, und beide Nutzungsarten einer Revision zu unterziehen sind, ist dafür zusätzlich die Checkliste 3.1 für das Szenario „Internet-Zugang“ heranzuziehen.</p> <p>Neben der vorliegenden Checkliste für das Szenario „Externer Web-Zugriff“ ist die Checkliste 3 für das Modul „Szenarien“ heranzuziehen. In der Checkliste 3 werden eine Reihe von grundsätzlichen Anforderungen insbesondere hinsichtlich der Sicherheitsgrundfunktionen an Netzübergänge gestellt.</p>

Prüfaspekt Dimensionierung	
A1 Skalierbarkeit und Auslastung	
A1.1	Decken die vorhandenen Lizenzen der eingesetzten Komponenten die zu erwartende Nutzerauslastung ¹¹ ab?
A1.2	Besteht die Möglichkeit der Lizenzerweiterung bei höherer Auslastung?
A1.3	Kann der Zugang den angeforderten Netzverkehr bewältigen?
A1.4	Wird die Systemauslastung kontinuierlich überwacht?
Bemerkungen	
A2 Verfügbarkeit	
A2.1	Erfüllt der externe Web-Zugang die Verfügbarkeitsanforderungen der Nutzer?
A2.2	Sind Single Points of Failure vorhanden?
A2.3	Gehen bei einem Ausfall einzelner Komponenten einzelne Verbindungssessions verloren oder werden sie aufrechterhalten?
A2.4	Sind alternative Anbindungen vorhanden und aktiv?
Bemerkungen	

¹¹ Je nach Lizenzmodell abhängig von Durchsatz, Anzahl der Schnittstellen, Anzahl Nutzer (Gesamtzahl oder Anzahl gleichzeitig aktiver Nutzer), Anzahl Systeme (Gesamtzahl oder Anzahl gleichzeitig aktiver Systeme)

Prüfaspekt Schutz des vertrauenswürdigen Netzes	
B1 Struktur	
B1.1	Weist der externe Web-Zugang eine angemessene Sicherheitsstruktur auf?
B1.2	Ist der externe Web-Zugang in mehrere separate Sicherheitszonen unterteilt, wobei jede Zone durch Sicherheitskomponenten voneinander separiert wird? Ist jedes Teilnetz (internes Netz, DMZ) angemessen abgesichert und geschützt?
B1.3	Sind sensible Systeme isoliert abgesichert (z. B. Web-, Mail-, Applikations- oder Datenbankserver)?
B1.4	Ist eine sichere und vertrauenswürdige Administration gegeben?
Bemerkungen	
B2 Kontrolle der Verbindungen	
B2.1	Ist die Kommunikation vom vertrauenswürdigen Netz in das Internet auf zugelassene Dienste eingeschränkt?
B2.2	Wird die Kommunikation vom Internet in das vertrauenswürdige Netz unterbunden?
B2.3	Ist die Kommunikation vom Internet in die zulässigen Sicherheitszonen, auf die dort betriebenen Systeme und auf die notwendigen Dienste beschränkt?
B2.4	Wird die Kommunikation zwischen den Sicherheitszonen untereinander oder zwischen den Sicherheitszonen und dem internen Netz auf die dort betriebenen Systeme und auf die notwendigen Dienste beschränkt?
B2.5	Werden die zugelassenen Dienste auf Applikationsebene kontrolliert (Proxy)?
B2.6	Erfolgt an der Schnittstelle zum Internet eine wirksame Kontrolle auf unerwünschte Inhalte (Viren, aktive Inhalte)?
B2.7	Gibt es eine default-deny-policy (grundsätzliches Kommunikationsverbot mit definierten Ausnahmen)?
Bemerkungen	

Checkliste 3.3: Szenario VPN-Zugang	
Prüfkriterien	Struktur und Auslegung eines VPN-Zuganges Funktionale Aspekte Verbindungskontrolle
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Das Szenario „VPN-Zugang“ stellt eine Erweiterung des Internet-Zugangs dar. Die VPN-Technologie erlaubt, die Verbindung zweier vertrauenswürdiger Netzwerke über ein drittes nicht vertrauenswürdiges Netzwerk (hier: Internet) zu realisieren.</p> <p>Als besondere Variante besteht die Möglichkeit, einzelne mobile Systeme (wie Telearbeitsplätze, Laptop des Außendienstes etc.) durch ein VPN über ein nicht vertrauenswürdiges Netzwerk (hier: Internet) temporär oder permanent an ein vertrauenswürdiges Netzwerk zu binden.</p> <p>Die vorliegende Checkliste ist dabei so zu interpretieren, dass hiermit nur die VPN-Nutzung abgedeckt wird. Sämtliche Fragestellungen und Prüfungen beziehen sich ausschließlich auf diese Nutzungsart.</p> <p>Wenn der für VPN genutzte Internet-Zugang gleichzeitig für die Bereitstellung von Internet-Diensten für interne Systeme dient und beide Nutzungsarten einer Revision zu unterziehen sind, ist dafür zusätzlich die Checkliste für das Szenario „Internet-Zugang“ heranzuziehen.</p> <p>Neben der vorliegenden Checkliste für das Szenario „VPN-Zugang“ ist die Checkliste 3 für das Modul „Szenarien“ heranzuziehen. In der Checkliste 3 werden eine Reihe von grundsätzlichen Anforderungen insbesondere hinsichtlich der Sicherheitsgrundfunktionen an Netzübergänge gestellt.</p>

Prüfaspekt Dimensionierung	
A1 Skalierbarkeit und Auslastung	
A1.1	Decken die vorhandenen Lizenzen der eingesetzten Komponenten die zu erwartende Nutzauslastung ¹² ab?
A1.2	Besteht die Möglichkeit der Lizenzerweiterung bei höherer Auslastung?
A1.3	Kann der Zugang den angeforderten Netzverkehr im Schnitt bewältigen?
A1.4	Wird die Systemauslastung kontinuierlich überwacht?
Bemerkungen	
A2 Verfügbarkeit	
A2.1	Erfüllt der VPN-Zugang im Schnitt die Verfügbarkeitsanforderungen der Nutzer?
A2.2	Sind Single Points of Failure vorhanden?
A2.3	Gehen bei einem Ausfall einzelner Komponenten einzelne Verbindungssessions verloren oder werden sie aufrechterhalten?
A2.4	Sind alternative Anbindungen vorhanden und aktiv?
Bemerkungen	

¹² Je nach Lizenzmodell abhängig von Durchsatz, Anzahl der Schnittstellen, Anzahl Nutzer (Gesamtzahl oder Anzahl gleichzeitig aktiver Nutzer), Anzahl Systeme (Gesamtzahl oder Anzahl gleichzeitig aktiver Systeme)

Prüfaspekt Schutz der vertrauenswürdigen Teilnetze	
B1 Struktur	
B1.1	Weist der VPN-Zugang eine angemessene Sicherheitsstruktur auf?
B1.2	Wird eine starke Verschlüsselung eingesetzt? (Bei VS-Netzen: eine durch das BSI zugelassene, der Einstufung entsprechende Verschlüsselung)
B1.3	Ist jedes Teilnetz (internes Netz, DMZ) angemessen abgesichert und geschützt?
B1.4	Ist der VPN-Zugang hinreichend gegenüber dem Internet abgesichert?
B1.5	Ist eine sichere und vertrauenswürdige Administration gegeben?
Bemerkungen	
B2 Kontrolle der Verbindungen	
B2.1	Ist die Kommunikation vom Internet in die zulässigen Sicherheitszonen, auf die dort betriebenen Systeme und auf die notwendigen Dienste beschränkt?
B2.2	Werden die aus dem VPN in das interne Netz zugelassenen Dienste auf Applikationsebene kontrolliert (Proxy)?
B2.3	Erfolgt an der Schnittstelle zum VPN eine wirksame Kontrolle auf unerwünschte Inhalte (Viren, aktive Inhalte)?
B2.4	Wird der VPN-Zugang Dritter zum internen Netz (z. B. für Fernwartungszwecke) angemessen kontrolliert und kanalisiert? ¹³
Bemerkungen	

¹³ Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

Checkliste 3.4: Szenario RAS-Zugang	
Prüfkriterien	Struktur und Auslegung eines RAS-Zuganges Funktionale Aspekte Verbindungskontrolle
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die RAS-Technologie erlaubt, die Verbindung zweier vertrauenswürdiger Netzwerke über ein drittes nicht vertrauenswürdiges Netzwerk (Internet, Telefonienetzwerk) zu realisieren, z. B. zwecks Fernwartung oder Telearbeit.</p> <p>Als besondere Variante besteht die Möglichkeit, einzelne mobile Systeme durch RAS über ein nicht vertrauenswürdiges Netzwerk (Telefonienetzwerk) temporär oder permanent an ein vertrauenswürdiges Netzwerk zu binden.</p> <p>Im Unterschied zur VPN-Technologie gibt es bei RAS jedoch keine durchgängige Netzwerktechnologie. Im Gegensatz zum VPN-Zugang erfolgt hierbei i. d. R. die Verbindung über Modem, ISDN oder X.25-Verbindungen.</p> <p>Neben der vorliegenden Checkliste für das Szenario „RAS-Zugang“ ist die Checkliste 3 für das Modul „Szenarien“ heranzuziehen. In der Checkliste 3 werden eine Reihe von grundsätzlichen Anforderungen insbesondere hinsichtlich der Sicherheitsgrundfunktionen an Netzübergänge gestellt.</p>

Prüfaspekt Dimensionierung	
A1 Skalierbarkeit und Auslastung	
A1.1	Kann der RAS-Zugang den angeforderten Netzverkehr im Schnitt bewältigen?
A1.2	Besteht die Möglichkeit der Erweiterung des RAS-Zugangs im Falle einer höheren Auslastung?
A1.3	Wird die Systemauslastung kontinuierlich überwacht?
Bemerkungen	
A2 Verfügbarkeit	
A2.1	Erfüllt der RAS-Zugang im Schnitt die Verfügbarkeitsanforderungen der Nutzer?
A2.2	Sind Single Points of Failure vorhanden?
A2.3	Sind alternative Anbindungen vorhanden und aktiv?
Bemerkungen	

Prüfaspekt Schutz des vertrauenswürdigen Netzes	
B1 Struktur	
B1.1	Weist der RAS-Zugang eine angemessene Sicherheitsstruktur auf? Ist der RAS-Zugang in einem isolierten Netzabschnitt lokalisiert?
B1.2	Wird eine starke Verschlüsselung eingesetzt? (Bei VS-Netzen wird dringend eine durch das BSI zugelassene, der Einstufung entsprechende Verschlüsselung empfohlen.) ¹⁴
B1.3	Ist jedes Teilnetz (internes Netz, RAS-Zugangnetz) angemessen abgesichert bzw. geschützt?
B1.4	Sind sensible Systeme isoliert abgesichert (z. B. Authentisierungsserver)?
B1.5	Ist eine sichere und vertrauenswürdige Administration gegeben?
Bemerkungen	
B2 Kontrolle der Verbindungen	
B2.1	Wird eine dem Schutzbedarf des internen Netzes angemessene Authentisierung verwendet? Wird, wo es möglich ist, ein Call-back-Verfahren eingesetzt?
B2.2	Wird die Kommunikation zwischen der RAS-Sicherheitszone und dem internen Netz auf die dort betriebenen Systeme und auf die notwendigen Dienste beschränkt?
B2.3	Werden die zugelassenen Dienste auf Applikationsebene kontrolliert (Proxy)?
B2.4	Erfolgt an der Schnittstelle zum RAS eine wirksame Kontrolle auf unerwünschte Inhalte (Viren, aktive Inhalte)?
B2.5	Gibt es eine default-deny-policy (grundsätzliches Kommunikationsverbot mit definierten Ausnahmen)?
B2.6	Besteht ein sicheres Verfahren zur Zulassung bzw. Einrichtung neuer RAS-Zugänge?
B2.7	Sind ausreichende Sicherheitsmaßnahmen bei dem externen Partner umgesetzt?
Bemerkungen	

¹⁴ Bei VS-Netzen wird Fernwartung nicht empfohlen.

Checkliste 3.5: Szenario LAN/LAN-Kopplung	
Prüfkriterien	Struktur und Auslegung einer LAN/LAN-Kopplung Funktionale Aspekte Verbindungskontrolle
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Unter einer LAN/LAN-Kopplung versteht man eine direkte Kopplung zweier Netzwerke gleicher Technologie. Alle beteiligten Netzwerke sind vertrauenswürdig, aber ein Teilnetz mit höheren Schutzanforderungen (z. B. Entwicklungsabteilung, Buchhaltung oder Geschäftsführung) soll gegen ein anderes Teilnetz mit geringeren Schutzanforderungen abgesichert werden. Auch bei gleichem Schutzbedarf ist die Einrichtung eines kontrollierten Netzübergangs erforderlich, falls die Verbreitung von sicherheitsrelevanten Informationen auf das jeweilige Teilnetz beschränkt bleiben soll.</p> <p>Die vorliegende Checkliste ist dabei so zu interpretieren, dass hiermit nur die LAN/LAN-Kopplung abgedeckt wird. Sämtliche Fragestellungen und Prüfungen beziehen sich ausschließlich auf diese Nutzungsart.</p> <p>Wenn die LAN/LAN-Kopplung beispielsweise mit Hilfe der VPN-Technologie aufgebaut wird, ist dafür zusätzlich die Checkliste für das Szenario „VPN-Zugang“ heranzuziehen. Ggf. sind weitere Checklisten (Internet-Zugang, externer Web-Zugriff) im Falle eines multifunktionalen Internet-Zuganges zusätzlich heranzuziehen.</p> <p>Neben der vorliegenden Checkliste für das Szenario „LAN/LAN-Kopplung“ ist die Checkliste 3 für das Modul „Szenarien“ heranzuziehen. In der Checkliste 3 werden eine Reihe von grundsätzlichen Anforderungen insbesondere hinsichtlich der Sicherheitsgrundfunktionen an Netzübergänge gestellt.</p>

Prüfaspekt Dimensionierung	
A1 Skalierbarkeit und Auslastung	
A1.1	Kann die LAN/LAN-Kopplung den angeforderten Netzverkehr im Schnitt bewältigen?
A1.2	Besteht die Möglichkeit der Erweiterung bei höherer Auslastung?
A1.3	Wird die Systemauslastung kontinuierlich überwacht?
Bemerkungen	
A2 Verfügbarkeit	
A2.1	Erfüllt die LAN/LAN-Kopplung im Schnitt die Verfügbarkeitsanforderungen der Nutzer?
A2.2	Sind Single Points of Failure vorhanden?
Bemerkungen	

Prüfaspekt Schutz des vertrauenswürdigen Netzes	
B1 Struktur	
B1.1	Weist die LAN/LAN-Kopplung eine angemessene Sicherheitsstruktur auf? Bestehen Möglichkeiten, die Absicherung der LAN/LAN-Kopplung zu umgehen?
B1.2	Ist eine sichere und vertrauenswürdige Administration gegeben?
Bemerkungen	
B2 Kontrolle der Verbindungen	
B2.1	Ist die Kommunikation vom vertrauenswürdigeren Netz in das weniger vertrauenswürdige Netz auf zugelassene Dienste eingeschränkt?
B2.2	Wird die Kommunikation vom weniger vertrauenswürdigen Netz in das vertrauenswürdige Netz unterbunden?
B2.3	Wird eine dem Schutzbedarf angemessene Authentisierung eingesetzt?
B2.4	Gibt es eine default-deny-policy (grundsätzliches Kommunikationsverbot mit definierten Ausnahmen)?
Bemerkungen	

Checkliste 4: Komponenten	
Prüfkriterien	Sichere Grundkonfiguration einer Komponente Härtung gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang Realisierung eines Basisschutzes auf Netzwerk- und Anwendungsebene
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die Checkliste „Komponenten“ beschreibt Prüfkriterien auf einem sehr abstrakten Level, die von allen Komponenten eines Netzübergangs, unabhängig von ihrer konkreten Funktion, erfüllt werden sollten.</p> <p>Dazu gehören im Einzelnen:</p> <ul style="list-style-type: none"> – Absicherung der Systeme gegen unautorisierten Zugriff und Modifikation: Eine zuverlässige und sichere Administration aller Systeme muss gegeben sein. – Umsetzung und Realisierung der Empfehlungen und Vorgaben des Herstellers: Die Vorgaben des Herstellers bezüglich Software-Version, Patch-Level oder temporärer Workarounds zur Absicherung der Systeme müssen eingehalten werden. – Konfiguration gemäß aktueller Vorgaben: Alle organisationsinternen Vorgaben (highlevel und systemspezifisch) sind umzusetzen. – Härtung des Systems: Überflüssige Dienste und Anwendungen auf einzelnen Systemen, die für die eigentliche Aufgabe nicht benötigt werden, sind zu deaktivieren bzw. zu deinstallieren, damit potenzielle Angriffspunkte minimiert werden. – Protokollierung: Jedes System sollte Verbindungsdaten aufzeichnen und an einen zentralen Log-Server weiterleiten. <p>Weiterführende Hinweise zu diesen Punkten findet man beispielsweise in [BSI-SICH-GW].</p>

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf das System	
A1.1	Sind alle notwendigen Dienste auf den Systemen in Betrieb und abgesichert?
A1.2	Sind alle nicht benötigten Dienste auf den Systemen mindestens deaktiviert bzw. deren Programmcode bzw. deren Programmbibliotheken sogar deinstalliert?
A1.3	Werden die Versionsnummern der eingesetzten Dienste verschleiert?
A1.4	Wird das Betriebssystem bei Verbindungsdialogen verschleiert?
A1.5	Sind nicht benötigte bzw. potenziell gefährdete Programme (Pakete) von den Systemen entfernt worden?
A1.6	Ist die laut Herstellerempfehlung neueste Software installiert und in Betrieb? ¹⁵
A1.7	Sind alle aktuellen Patches / fehlerbereinigte Binaries installiert? ¹⁵
A1.8	Sind ggf. empfohlene Workarounds realisiert?
Bemerkungen	
A2 Sichere Administration	
A2.1	Kann ausschließlich von berechtigten Systemen administrativ auf die Komponenten zugegriffen werden?
A2.2	Sind alle Zugriffsmöglichkeiten durch eine Passwortabfrage gesichert?
A2.3	Ist bei einer Fernwartung der Zugang entsprechend abgesichert? ¹⁶
A2.4	Sind die Zugriffe auf administrative Konsolen abgesichert?
A2.5	Ist die Kommunikation bei administrativen Vorgängen über nicht vertrauenswürdige Netze verschlüsselt?
Bemerkungen	

¹⁵ Hinweis: Patches und Updates werden vielfach nur dann vom Hersteller zur Verfügung gestellt, wenn ein Wartungsvertrag abgeschlossen wurde.

¹⁶ Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	
B1.1	Wird IP Source-Routing ¹⁷ am System gesperrt?
B1.2	Ist das System geschützt gegen Routing-Manipulationen durch icmp-redirect Attacken?
B1.3	Werden sichere Routing-Verfahren (statische Routen) eingesetzt?
Bemerkungen	
B2 Konfiguration gemäß der Vorgaben	
B2.1	Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?
B2.2	Sind Ausnahmen davon separat zugelassen und abgenommen?
Bemerkungen	

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden die wichtigsten Verbindungsdaten aufgezeichnet? Werden sicherheitsrelevante Ereignisse (z. B. Verstoß gegen die Zugriffskontrollregeln) durch die Komponente protokolliert? Werden kritische Ereignisse aufgezeichnet?
C1.2	Ist eine Default-Deny-Regel implementiert, die alle nicht erlaubten Verbindungen protokolliert?
C1.3	Ist sichergestellt, dass die Protokollierung sicherheitsrelevanter Ereignisse mit Zeitmarken erfolgt, die mit allen Protokollereignissen anderer Systeme synchron sind?
C1.4	Werden die Daten manipulationssicher gespeichert? Werden die Protokolle (z. B. per SYSLOG) auf einem dedizierten System abgelegt?
Bemerkungen	
C2 Auswertung / Alarmierung	
C2.1	Wird eine Alarmierung ausgelöst bei definierten Ereignissen?
C2.2	Werden die Protokolldaten überwacht?
Bemerkungen	
Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	

¹⁷ IP Source-Routing: Der Absender der IP-Datagramme legt den Weg der Datenpakete zum Ziel vollständig (strict) oder teilweise (loose) fest. Siehe auch RFC 791

D1.1	Sind Backup-Prozeduren für das System etabliert, die einen schnellen Wiederanlauf des Systems nach einem Ausfall gewährleisten?	
D1.2	Sind Eskalationsprozeduren etabliert, die eine zügige Problembehebung beim Ausfall eines Systems gewährleisten?	
D1.3	Sind die Verantwortlichkeiten und Vertretungsregelungen für die Systeme klar formuliert?	
D1.4	Sind Wartungs- und Supportverträge mit dem Hersteller der Systeme vorhanden?	
Bemerkungen		

Checkliste 4.1: Paketfilter	
Prüfkriterien	Sichere Grundkonfiguration eines Paketfilters Härtung des Paketfilters gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die ein Paketfilter im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Die Anforderungen sind generisch und im Kontext zu anderen Komponenten zu werten. Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p> <p>Dies betrifft insbesondere die folgenden Prüfaspekte:</p> <ul style="list-style-type: none"> - A2 (Sichere Administration) Im Sicherheitskonzept muss festgelegt werden, ob überhaupt Fernwartungszugänge (nicht bei VS-Netzen) über ein Netz zum Paketfilter erlaubt sind oder ob das Paketfilter-Management durch ein getrenntes Management-LAN und ausschließlichem Zugang über Konsole via Terminal-Server angemessener ist. Auch muss festgeschrieben sein, ob der Einsatz eines externen Authentisierungsservice (RADIUS, TACACS) angemessen ist. - B1.3 (Routing-Verfahren), B3 (Filterung) Welche Access-Listen und Routing-Protokolle sicherheitstechnisch angemessen sind, kann ebenfalls nur im Sicherheitskonzept festgelegt werden und ist nicht generisch konkreter formulierbar. Insbesondere ist die Wirksamkeit von Filterfunktionen durch Access-Listen nur im Kontext mit anderen Maßnahmen (z. B. Sicherheitsgateway-Regeln und architektonische Maßnahmen) zu werten.

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf den Paketfilter	
A1.1	Sind alle nicht benötigten Dienste auf dem Paketfilter deaktiviert?
A1.2	Sind unsichere Systemzugänge (RSH, RLOGIN, RCP) gesperrt?
A1.3	Existiert ein Maßnahmenkatalog (Systemhersteller oder eigener Katalog), um das eingesetzte System zu härten, und wurden diese Maßnahmen vollständig umgesetzt?
A1.4	Sind alle vom Hersteller veröffentlichten Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (fehlerkorrigierte Binaries und/oder Workarounds) umgesetzt? ¹⁸
A1.5	Werden die eingestellten Passwörter sicher abgespeichert (shadow-Passwortdatei), so dass ein Ausspähen der Passwörter verhindert wird?
Bemerkungen	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zum Paketfilter über das Netz auf berechnete Systeme und Teilnetze eingeschränkt?
A2.2	Werden alle Zugänge zum Paketfilter über das Netz durch Kennwörter geschützt? Werden – wenn möglich - nur kryptografisch sichere Zugänge genutzt?
A2.3	Werden ggf. vorhandene anonyme Zugänge zum Paketfilter über das Netz durch Kennwörter geschützt oder sind sie deaktiviert bzw. gesperrt?
A2.4	Wird der direkte Zugang zum Paketfilter (Konsole) durch ein Kennwort geschützt?
A2.5	Wird der Zugang zum Betriebssystem des Paketfilters durch Authentisierung (Benutzername und Kennwort) geschützt?
A2.6	Sind die Passwörter für den privilegierten Zugang zum Paketfilter (Administration) unterschiedlich zu dem des unprivilegierten Zugangs gewählt?
A2.7	Falls vorhanden: Ist der Fernwartungszugang für den root-Account deaktiviert?
A2.8	Werden die eingestellten Passwörter verschlüsselt abgespeichert und dargestellt, so dass ein Ausspähen der Passwörter verhindert wird?
A2.9	Falls es Fernwartungszugänge durch Dritte gibt: Werden diese Zugänge überwacht? ¹⁹
Bemerkungen	
Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	

¹⁸ Hinweis: Der Zugang zu Patches und Updates ist in der Regel mit Kosten verbunden (z. B. mit Abschluss eines Wartungsvertrages).

¹⁹ Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

B1.1	Ist IP Source-Routing ²⁰ am Paketfilter deaktiviert?	
B1.2	Ist der Paketfilter gegen Routing-Manipulationen durch icmp-redirect Attacken geschützt?	
B1.3	Werden sichere Routing-Verfahren (ausschließlich statische Routen) eingesetzt?	
B1.4	Ist Forwarding deaktiviert?	
Bemerkungen		
B2 Konfiguration gemäß der Vorgaben		
B2.1	Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?	
B2.2	Sind Ausnahmen davon separat zugelassen und abgenommen?	
Bemerkungen		
B3 Filterung des Netzwerkverkehrs		
B3.1	Sind Filter (Access-Listen) am Paketfilter gesetzt, die die Kommunikation zwischen den angeschlossenen Teilnetzen wirkungsvoll und gemäß den Sicherheitsvorgaben kanalisieren?	
B3.2	Sind Filter am Paketfilter gesetzt, die ein Umgehen der Zugriffskontrolle durch Fälschen von Netzwerkadressen (IP-Spoofing) soweit wie möglich verhindern?	
B3.3	Ist das System so konfiguriert, dass fragmentierte Pakete reassembliert werden?	
Bemerkungen		

²⁰ IP Source-Routing: Der Absender der IP-Datagramme legt den Weg der Datenpakete zum Ziel vollständig (strict) oder teilweise (loose) fest. Siehe auch RFC 791

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden sicherheitsrelevante Ereignisse (z. B. Verstoß gegen die Zugriffskontrollregeln) durch den Paketfilter protokolliert?
C1.2	Ist eine Default-Deny-Regel implementiert, die alle nicht erlaubten Verbindungen protokolliert?
C1.3	Erfolgt die Protokollierung sicherheitsrelevanter Ereignisse mit zeitsynchronen Zeitmarken?
C1.4	Werden die Protokolle (z. B. per SYSLOG) auf einem dedizierten System abgelegt?
Bemerkungen	
C2 Auswertung/Alarmierung	
C2.1	Erfolgt eine (automatische) Alarmierung bei besonders auffälligen Ereignissen (z. B. Adress- und Portscans)?
C2.2	Werden die Sicherheitsprotokolle des Paketfilters ausgewertet?
Bemerkungen	

Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	
D1.1	Sind Backup-Prozeduren für die Systemkonfiguration etabliert, die einen schnellen Wiederanlauf des Systems nach einem Ausfall gewährleisten?
D1.2	Sind Eskalationsprozeduren etabliert, die eine zügige Problembeseitigung beim Ausfall eines Systems gewährleisten?
D1.3	Sind die Verantwortlichkeiten und Vertretungsregelungen für die Systeme klar formuliert?
D1.4	Sind Wartungs- und Supportverträge mit dem Hersteller der Systeme vorhanden?
Bemerkungen	

Checkliste 4.1.1: Router	
Prüfkriterien	Sichere Grundkonfiguration eines Cisco-Routers Härtung des Routers gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die ein Cisco Router im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Die Anforderungen sind generischer Natur und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten. Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p> <p>Dies betrifft insbesondere die folgenden Prüfaspekte:</p> <ul style="list-style-type: none"> - A2 (Sichere Administration) Im Sicherheitskonzept muss festgelegt werden, ob überhaupt Fernwartungszugänge über ein Netz (SSH, HTTP, SNMP) zum Cisco-Router erlaubt sind oder ob das Router-Management durch ein getrenntes Management-LAN und ausschließlichem Zugang über Konsole via Terminal-Server angemessener ist. Auch muss festgeschrieben sein, ob der Einsatz eines externen Authentisierungsservice (RADIUS, TACACS) angemessen ist. - B1.3 (Routing-Verfahren), B3 (Filterung) Welche Access-Listen und Routing-Protokolle sicherheitstechnisch angemessen sind, kann ebenfalls nur im Sicherheitskonzept festgelegt werden und ist nicht generisch konkreter formulierbar. Insbesondere ist die Wirksamkeit von Filterfunktionen durch Access-Listen nur im Kontext mit anderen Maßnahmen (z. B. Sicherheitsgateway-Regeln und architektonische Maßnahmen) zu werten.

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf den Router	
A1.1	Sind alle nicht benötigten Dienste auf dem Router deaktiviert?
A1.2	Ist die Zahl der tty-Lines auf das unbedingt notwendige Maß eingeschränkt?
A1.3	Sind alle vom Hersteller veröffentlichten Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (fehlerkorrigierte Binaries und/oder Workarounds) umgesetzt? ²¹
Bemerkungen	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zum Router über das Netz (TELNET, SSH, HTTP(S), SNMP) auf berechnigte Systeme und Teilnetze eingeschränkt?
A2.2	Werden alle Zugänge zum Router über das Netz (TELNET, SSH, HTTP(S), SNMP) durch Kennworte geschützt? Werden nur kryptografisch sichere Zugänge (SSH, HTTPS) genutzt?
A2.3	Wird der direkte Zugang zum Router (Konsole) durch ein Kennwort geschützt?
A2.4	Gibt es einen privilegierten Modus (enable) des Routers und wird der Zugang dazu durch ein Kennwort geschützt?
A2.5	Sind die Passworte für den Zugang zum Router und für den privilegierten Modus unterschiedlich gewählt?
A2.6	Werden die eingestellten Passwörter verschlüsselt abgespeichert und dargestellt, so dass ein Ausspähen der Passwörter verhindert wird?
A2.7	Falls es Fernwartungszugänge durch Dritte gibt: Werden diese Zugänge überwacht?
Bemerkungen	

²¹ Hinweis: Der Zugang zu Patches und Updates ist mit Kosten verbunden (z. B. mit Abschluss eines Wartungsvertrages).

Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	
B1.1	Ist IP Source-Routing ²² am Router deaktiviert?
B1.2	Ist der Router gegen Routing-Manipulationen durch icmp-redirect Attacken geschützt?
B1.3	Werden sichere Routing-Verfahren (ausschließlich statische Routen) eingesetzt?
B1.4	Ist Forwarding deaktiviert?
Bemerkungen	
B2 Konfiguration gemäß der Vorgaben	
B2.1	Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?
B2.2	Sind Ausnahmen davon separat zugelassen und abgenommen?
Bemerkungen	
B3 Filterung des Netzwerkverkehrs	
B3.1	Sind Filter (Access-Listen) am Router gesetzt, die die Kommunikation zwischen den angeschlossenen Teilnetzen wirkungsvoll und gemäß den Sicherheitsvorgaben kanalisieren?
B3.2	Sind Filter am Router gesetzt, die ein Umgehen der Zugriffskontrolle durch Fälschen von Netzwerkadressen (IP-Spoofing) soweit als möglich verhindern?
Bemerkungen	

²² IP Source-Routing: Der Absender der IP-Datagramme legt den Weg der Datenpakete zum Ziel vollständig (strict) oder teilweise (loose) fest. Siehe auch RFC 791

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden sicherheitsrelevante Ereignisse (z. B. Verstoß gegen die Zugriffskontrollregeln) durch den Router protokolliert?
C1.2	Ist eine Default-Deny-Regel implementiert, die alle nicht erlaubten Verbindungen protokolliert?
C1.3	Ist sichergestellt, dass die Protokollierung sicherheitsrelevanter Ereignisse mit Zeitmarken erfolgt, die mit allen Protokollereignissen anderer Systeme synchron sind?
C1.4	Werden die Protokolle (z. B. per SYSLOG) auf einem dedizierten System abgelegt?
Bemerkungen	
C2 Auswertung/Alarmierung	
C2.1	Erfolgt eine (automatische) Alarmierung bei besonders auffälligen Ereignissen (z. B. Adress- und Portscans)?
C2.2	Werden die Sicherheitsprotokolle des Routers überwacht?
Bemerkungen	

Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	
D1.1	Sind Backup-Prozeduren für die Systemkonfiguration etabliert, die einen schnellen Wiederanlauf des Systems nach einem Ausfall gewährleisten?
D1.2	Sind Eskalationsprozeduren etabliert, die eine zügige Problembeseitigung beim Ausfall eines Systems gewährleisten?
D1.3	Sind die Verantwortlichkeiten und Vertretungsregelungen für die Systeme klar formuliert?
D1.4	Sind Wartungs- und Supportverträge mit dem Hersteller der Systeme vorhanden?
Bemerkungen	

Checkliste 4.1.2: Linux Paketfilter (iptables)	
Prüfkriterien	Sichere Grundkonfiguration eines Linux Paketfilters Härtung des Systems gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die ein Linux Paketfilter im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Die Anforderungen sind generischer Natur und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten. Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p> <p>Dies betrifft insbesondere die folgenden Prüfaspekte:</p> <ul style="list-style-type: none"> - A1 (Sichere Administration) Im Sicherheitskonzept muss festgelegt werden, ob überhaupt Fernwartungszugänge über ein Netz (SSH, HTTPS) zum System erlaubt sind oder ob das Paketfilter-Management durch ein getrenntes Management-LAN und ausschließlichem Zugang über Konsole via Terminal-Server angemessener ist. Auch muss festgeschrieben sein, ob der Einsatz eines externen Authentisierungsservice (RADIUS, TACACS) angemessen ist. - B1.3 (Routing-Verfahren), B3 (Filterung) Welche Access-Listen und Routing-Protokolle sicherheitstechnisch angemessen sind, kann ebenfalls nur vom Sicherheitskonzept festgelegt werden und ist nicht generisch konkreter formulierbar. Insbesondere ist die Wirksamkeit von Filterfunktionen durch Access-Listen nur im Kontext mit anderen Maßnahmen (z. B. Sicherheitsgateway-Regeln und architektonische Maßnahmen) zu werten.

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf das System	
A1.1	Sind alle nicht benötigten Dienste auf dem System deaktiviert?
A1.2	Sind alle unsicheren Systemzugänge (RSH, RLOGIN, RCP etc.) gesperrt?
A1.3	Existiert ein Maßnahmenkatalog (Systemhersteller/Linux-Distribution oder eigener Katalog), um das eingesetzte System zu härten, und wurden diese Maßnahmen vollständig umgesetzt?
A1.4	Sind alle vom Hersteller der verwendeten Linux-Distribution oder von Dritten veröffentlichten Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (Patches und/oder Workarounds) umgesetzt? ²³
A1.5	Werden die eingestellten Passwörter sicher abgespeichert (shadow-Passwortdatei), so dass ein Ausspähen der Passwörter verhindert wird?
Bemerkungen	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zum System über das Netz (TELNET/SSH, HTTP(S), SNMP) auf berechnete Systeme und Teilnetze eingeschränkt?
A2.2	Sind die Zugänge zum System über das Netz auf kryptographisch sichere Dienste (SSH, HTTPS) beschränkt?
A2.3	Werden alle anonymen Zugänge zum System über das Netz (SNMP) durch Kennwörter geschützt, oder sind sie deaktiviert bzw. gesperrt?
A2.4	Werden alle Benutzer-Accounts durch Kennwörter geschützt?
A2.5	Sind die Passwörter für nichtprivilegierte Accounts und für den root-Account unterschiedlich gewählt?
A2.6	Ist der Fernwartungszugang für den root-Account deaktiviert?
A2.7	Falls es Fernwartungszugänge durch Dritte gibt: Werden diese Zugänge angemessen kontrolliert? ²⁴
Bemerkungen	

²³ Hinweis: Der Zugang zu Patches und Updates ist u. U. nur mit Abschluss eines Wartungsvertrages möglich.

²⁴ Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	
B1.1	Wird IP Source-Routing ²⁵ am System gesperrt?
B1.2	Ist das System gegen Routing-Manipulationen durch icmp-redirect Attacken geschützt?
B1.3	Werden sichere Routing-Verfahren (statische Routen) eingesetzt?
B1.4	Ist Forwarding deaktiviert?
Bemerkungen	
B2 Konfiguration gemäß der Vorgaben	
B2.1	Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?
B2.2	Sind Ausnahmen davon separat zugelassen und abgenommen?
Bemerkungen	
B3 Filterung des Netzwerkverkehrs	
B3.1	Sind Filter (Access-Listen) am System gesetzt, die die Kommunikation zwischen den angeschlossenen Teilnetzen wirkungsvoll und gemäß den Sicherheitsvorgaben kanalisieren?
B3.2	Sind Filter am System gesetzt, die ein Umgehen der Zugriffskontrolle durch Fälschen von Netzwerkadressen (IP-Spoofing) soweit als möglich verhindern?
B3.3	Ist das System so konfiguriert, dass der Status von Verbindungen ausgewertet wird (stateful packet filter/connection tracking)?
B3.4	Ist das System so konfiguriert, dass fragmentierte Pakete reassembliert werden?
Bemerkungen	

²⁵ IP Source-Routing: Der Absender der IP-Datagramme legt den Weg der Datenpakete zum Ziel vollständig (strict) oder teilweise (loose) fest. Siehe auch RFC 791

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden sicherheitsrelevante Ereignisse (z. B. Verstoß gegen die Zugriffskontrollregeln) durch das System protokolliert? Werden kritische Ereignisse aufgezeichnet?
C1.2	Ist eine Default-Deny-Regel implementiert, die alle nicht erlaubten Verbindungen protokolliert?
C1.3	Ist sichergestellt, dass die Protokollierung sicherheitsrelevanter Ereignisse mit Zeitmarken erfolgt, die mit allen Protokollereignissen anderer Systeme synchron sind?
C1.4	Werden die Protokolle (z. B. per SYSLOG) auf einem dedizierten System abgelegt?
Bemerkungen	
C2 Auswertung/Alarmierung	
C2.1	Erfolgt eine (automatische) Alarmierung bei besonders auffälligen Ereignissen (z. B. Adress- und Portscans)?
C2.2	Werden die Sicherheitsprotokolle des Systems überwacht?
C2.3	Wird die Konfiguration des Systems regelmäßig automatisch gegen Manipulationen überprüft (z. B. mit tripwire)?
Bemerkungen	

Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	
D1.1	Sind Backup-Prozeduren für das System etabliert, die einen schnellen Wiederanlauf des Systems nach einem Ausfall gewährleisten?
D1.2	Sind Eskalationsprozeduren etabliert, die eine zügige Problembeseitigung beim Ausfall eines Systems gewährleisten?
D1.3	Sind die Verantwortlichkeiten und Vertretungsregelungen für die Systeme klar formuliert?
D1.4	Sind Wartungs- und Supportverträge mit dem Hersteller der Systeme vorhanden?
Bemerkungen	

Checkliste 4.2: ALG	
Prüfkriterien	<p>Sichere Grundkonfiguration eines ALG (Application Layer Gateway)</p> <p>Härtung des ALG gegen Umgehung von Schutzfunktionen</p> <p>Herstellung eines Basisschutzes am Netzübergang</p> <p>Realisierung eines Basisschutzes auf Anwendungsebene</p>
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die ein ALG im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Die Anforderungen sind generischer Natur und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten. Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p> <p>Dies betrifft insbesondere die folgenden Prüfaspekte:</p> <ul style="list-style-type: none"> - A2 (Sichere Administration) Im Sicherheitskonzept muss festgelegt werden, ob überhaupt Fernwartungszugänge über produktive Netze zum ALG erlaubt sind oder ob das ALG-Management durch ein getrenntes Management-LAN angemessener ist. - B1 (Routing-Verfahren), B3 (Filterung) Welche Regeln und Routing-Protokolle sicherheitstechnisch angemessen sind, kann ebenfalls nur vom Sicherheitskonzept festgelegt werden und ist nicht generisch konkreter formulierbar. Insbesondere ist die Wirksamkeit von Filterfunktionen durch Regeln nur im Kontext mit anderen Maßnahmen (z. B. globale Firewall-Einstellungen und architektonische Maßnahmen) zu werten.

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf das ALG	
A1.1	Sind alle nicht benötigten Dienste des Betriebssystems deaktiviert?
A1.2	Wurde das Betriebssystem gehärtet?
A1.3	Wurden die neuesten Sicherheits-Patches installiert?
A1.4	Ist die neueste Version der ALG-Software installiert? ²⁶
A1.5	Sind alle vom Hersteller veröffentlichten Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (Patches und/oder Workarounds) umgesetzt? ²¹
Bemerkungen	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zum ALG über das Netz im Regelwerk auf berechtigte Systeme eingeschränkt?
A2.2	Werden alle Zugänge zum ALG über das Netz durch Kennworte geschützt?
A2.3	Sind die Administratorrechte entsprechend den Tätigkeiten der Administratoren gewählt?
A2.4	Falls es Fernwartungszugänge durch Dritte gibt: Werden diese Zugänge überwacht? ²⁷
A2.5	Werden die Tätigkeiten der Administratoren im Audit-Log regelmäßig überwacht?
A2.6	Sind die Regeln übersichtlich gegliedert und eindeutig kommentiert?
Bemerkungen	

²⁶ Hinweis: Der Zugang zu Patches und Updates ist in der Regel nur mit Abschluss eines Wartungsvertrages möglich.

²⁷ Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	
B1.1	Werden sichere Routing-Verfahren (statische Routen) eingesetzt?
B1.2	Ist Forwarding deaktiviert?
Bemer- kungen	
B2 Konfiguration gemäß der Vorgaben	
B2.1	Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?
B2.2	Sind Ausnahmen davon separat zugelassen und abgenommen?
Bemer- kungen	
B3 Filterung des Netzwerkverkehrs	
B3.1	Ist der Schutz vor IP-Spoofing konfiguriert (Definition der erlaubten Netze an die jeweiligen Schnittstellen der Firewall), der ein Umgehen der Zugriffskontrolle durch Fälschen von Netzwerkadressen soweit als möglich verhindert?
B3.2	Sind Regeln installiert, die die Kommunikation zwischen den angeschlossenen Teilnetzen wirkungsvoll und gemäß den Sicherheitsvorgaben kontrollieren?
B3.3	Werden – soweit vorhanden – Kontrollfunktionen des ALG auf Anwendungsebene genutzt? Sind die erlaubten Protokolle so konfiguriert, dass nicht nur der Port, sondern auch der Protokoll-Typ (FTP, HTTP, SMTP) verifiziert wird?
B3.4	Erfolgt eine Verifizierung der Empfänger-Domänen mit Hilfe einer SMTP-Resource, wenn Mail aus dem Internet empfangen wird (nur relevant, wenn Mail aus dem Internet über das zu untersuchende System empfangen wird)?
Bemer- kungen	

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden sicherheitsrelevante Ereignisse (z. B. Verstoß gegen die Zugriffskontrollregeln) durch das ALG protokolliert? Werden kritische Ereignisse aufgezeichnet?
C1.2	Ist eine Default-Deny-Regel implementiert, die alle nicht erlaubten Verbindungen protokolliert?
C1.3	Ist sichergestellt, dass die Protokollierung sicherheitsrelevanter Ereignisse mit Zeitmarken erfolgt, die mit allen Protokollereignissen anderer Systeme synchron sind?
Bemerkungen	
C2 Auswertung / Alarmierung	
C2.1	Erfolgt eine (automatische) Alarmierung bei besonders auffälligen Ereignissen (z. B. Adress- und Portscans)?
C2.2	Werden die Sicherheitsprotokolle des ALG überwacht?
Bemerkungen	

Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	
D1.1	Sind Backup-Prozeduren für das ALG etabliert, die einen schnellen Wiederanlauf des Systems nach einem Ausfall gewährleisten?
D1.2	Sind Eskalationsprozeduren etabliert, die eine zügige Problembeseitigung beim Ausfall eines Systems gewährleisten?
D1.3	Sind die Verantwortlichkeiten und Vertretungsregelungen für das ALG klar formuliert?
D1.4	Sind Wartungs- und Supportverträge mit dem Hersteller des ALG vorhanden?
Bemerkungen	

Checkliste 4.3: GeNUGate	
Prüfkriterien	Sichere Grundkonfiguration einer GeNUGate Firewall Härtung der Firewall gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang Realisierung eines Basisschutzes auf Anwendungsebene
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>In dieser Checkliste werden neben der ALG-Funktion der GeNUGate auch Aspekte des zugehörigen Paketfilters betrachtet. Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die eine GeNUGate Firewall im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Die Anforderungen sind generischer Natur, basieren auf keiner speziellen Firewall-Version und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten. Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p>

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf die Firewall	
A1.1	Ist die neueste Version der Firewall-Software installiert? ²⁸
A1.2	Wurden die neuesten Sicherheits-Patches installiert? ²¹
A1.3	Wird eine zertifizierte Version eingesetzt?
A1.4	Sind alle vom Hersteller veröffentlichten zusätzliche Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (Workarounds) umgesetzt?
A1.5	Sind alle notwendigen Dienste auf den Systemen in Betrieb und abgesichert?
A1.6	Sind alle nicht benötigten Dienste auf den Systemen mindestens deaktiviert und wenn möglich deinstalliert? Im Installations- und Konfigurationshandbuch (Kap.4.4.2 Standard-Konfiguration) werden die standardmäßig laufenden Prozesse angegeben. Laufen zusätzliche Prozesse?
A1.7	Sind nicht zertifizierte GeNUGate Pakete installiert (z. B. util, Virens Scanner, VPN, HA Modul)?
A1.8	Wurden zusätzliche Filterregeln für den Paketfilter angelegt?
A1.9	Ist SNMP aktiv?
A1.10	Wird NTP benutzt?
A1.11	Ist ein zusätzlicher externer Paketfilter vorhanden?
Bemerkungen	
A2 Sichere Administration	
A2.1	Kann ausschließlich von berechtigten Systemen administrativ auf die Komponenten zugegriffen werden?
A2.2	Sind alle Zugriffsmöglichkeiten durch eine Passwortabfrage gesichert?
A2.3	Sind die Passwörter gesichert auf den Systemen abgelegt?
A2.4	Ist bei einer Fernwartung der Zugang entsprechend abgesichert? ²⁹
A2.5	Sind die Zugriffe auf administrative Konsolen abgesichert? Insbesondere sollte ein Konsolenzugang zum GeNUGate-Paketfilter nicht über das ALG erfolgen, sondern über einen separaten Terminalserver abgesichert werden.
A2.6	Ist die Kommunikation bei administrativen Vorgängen über nicht vertrauenswürdige Netze verschlüsselt?
A2.7	Kann das System remote rebootet werden?
A2.8	Werden andere (nicht lokale) Authentifikationsverfahren unterstützt?

²⁸ Hinweis: Der Zugang zu Patches und Updates ist nur mit Abschluss eines Wartungsvertrages möglich.

²⁹ Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

Prüfaspekt Selbstschutz	
A2.9	Findet bei Inaktivität ein Autologoff statt?
A2.10	Können Administrationsvorgänge nachvollziehbar verschiedenen Administratoren zugeordnet werden?
A2.11	Wird nur über das Administrationsinterface konfiguriert?
A2.12	Ist die Administration auf bestimmte Zugriffsarten beschränkt (Konsole, SSH, WWW...)? Ist der Zugriff per Telnet deaktiviert?
A2.13	Ist das Patch-Management remote möglich?
A2.14	Werden die Passwörter regelmäßig geändert?
A2.15	Ist ein zusätzlicher externer Paketfilter vorhanden?
Bemerkungen	
A3 Einhaltung der Herstellerempfehlungen	
A3.1	Sind laut Hersteller bedenkliche Authentifikationsverfahren im Einsatz (Sidechannel-Authentisierung)?
A3.2	Ist /AUTOBOOT deaktiviert?
A3.3	Ist die Bootdiskette des Paketfilters schreibgeschützt?
A3.4	Ist das BIOS des Paketfilters auf Nur-Lesezugriff bei Disketten konfiguriert?
A3.5	Ist das GeNUGate CA Passwort an einem sicheren Ort hinterlegt?
A3.6	Wird der Standard Kernel ohne IP Forwarding benutzt?
A3.7	Wird auf dem HTTP und SMTP Relay Weeding nach „script, applet, object, embed“ betrieben?
A3.8	Wird auf den POP- und NNTP-Relays Weeding betrieben?
A3.9	Ist die Konfiguration auf externen Medien (Floppy; Tape) gesichert?
A3.10	Gibt es mehrere Paketfilter-Disketten als Reserve?
Bemerkungen	
Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	
B1.1	Werden sichere Routing-Verfahren (statische Routen) eingesetzt?
B1.2	Ist OSPF aktiv?
Bemerkungen	
B2 Konfiguration gemäß der Vorgaben	
B2.1	Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?

Prüfaspekt Selbstschutz	
B2.2	Sind Ausnahmen davon separat erlaubt und abgenommen?
Bemerkungen	
B3 Filterung des Netzwerkverkehrs	
B3.1	Ist der Schutz vor IP-Spoofing konfiguriert (Definition der erlaubten Netze an die jeweiligen Schnittstellen der Firewall), der ein Umgehen der Zugriffskontrolle durch Fälschen von Netzwerkadressen soweit als möglich verhindert?
B3.2	Sind Relays, die einen Datenaustausch zwischen angeschlossenen Teilnetzen zulassen, entsprechend den Sicherheitsvorgaben konfiguriert?
Bemerkungen	

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden die wichtigsten Verbindungsdaten aufgezeichnet?
C1.2	Werden die Daten sicher gespeichert? Gibt es ein Sicherheitskonzept?
C1.3	Wo werden die gesicherten Daten gespeichert, physikalischer Zugriff, Brandschutz, Was geschieht mit alten Datenträgern?
C1.4	Werden kritische Ereignisse aufgezeichnet?
C1.5	Sind benutzerdefinierte Ereignisse konfiguriert?
C1.6	Werden auf dem GeNUGate von externen Geräten Meldungen gesichert (z.B. per SYSLOG)?
C1.7	Werden im Konfigurationslog nicht geplante Ereignisse angezeigt (z.B. Reboot, Ausführung von Bootinstallscripten)?
C1.8	Sind für den Logwatch-Prozess gemäß den Sicherheitsrichtlinien entsprechende Aktionen definiert?
Bemerkungen	
C2 Auswertung/Alarmierung	
C2.1	Wird eine Alarmierung ausgelöst bei definierten Ereignissen?
C2.2	Können die Protokolle vom Revisor zur weiteren Analyse kopiert werden (z.B. SCP)?
C2.3	Wurden Programme verändert (mögliche Alarmmeldungen des filecop-Prozesses)?
C2.4	Entspricht die Konfiguration des Prozessmasters den Sicherheitsvorgaben?
Bemerkungen	

Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	
D1.1	Wird ein RAID benutzt? Sind Ersatzfestplatten/Streamer vorhanden?
D1.2	Wurde getestet, ob das Wiedereinspielen der Daten(Konfiguration/Logging) funktioniert?
D1.3	Werden alle relevanten Dateien gesichert (/usr/local/sbin/save_fwcfg)?
Bemerkungen	
D2 Hochverfügbarkeit	
D2.1	Gibt es ein Stand-By-Reservesystem (Cold Stand-By)?
D2.2	Wird ein Cluster eingesetzt?
D2.3	Sind alle Cluster-Knoten auf demselben Stand (Patches/Konfiguration)?
D2.4	Funktioniert die automatische Übernahme bei Ausfall eines Cluster-Knotens?
D2.5	Bei einer Cluster-Konfiguration ist ein interner mit OSPF betriebener Router erforderlich. Ist dieser Router in die Revision eingezogen worden?
Bemerkungen	

Checkliste 4.4: Check Point Firewall-1 NG	
Prüfkriterien	Sichere Grundkonfiguration einer Check Point Firewall Härtung der Firewall gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang Realisierung eines Basisschutzes auf Anwendungsebene
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>In dieser Checkliste werden nur die von der Check Point bereitgestellten Proxies betrachtet. Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die eine Check Point Firewall im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Die Anforderungen sind generischer Natur, basieren auf keinen speziellen Firewall-Versionen und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten. Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p> <p>Dies betrifft insbesondere die folgenden Prüfaspekte:</p> <ul style="list-style-type: none"> - A2 (Sichere Administration) Im Sicherheitskonzept muss festgelegt werden, ob überhaupt Fernwartungszugänge über produktive Netze (Check Point Managementverbindungen, SSH) zur Firewall erlaubt sind oder ob das Firewall-Management durch ein getrenntes Management-LAN angemessener ist. - B1 (Routing-Verfahren), B3 (Filterung) Welche Regeln und Routing-Protokolle sicherheitstechnisch angemessen sind, kann ebenfalls nur vom Sicherheitskonzept festgelegt werden und ist nicht generisch konkreter formulierbar. Insbesondere ist die Wirksamkeit von Filterfunktionen durch Regeln nur im Kontext mit anderen Maßnahmen (z. B. globale Einstellungen der Firewall und architektonische Maßnahmen) zu werten.

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf die Firewall	
A1.1	Sind alle nicht benötigten Dienste des Betriebssystems deaktiviert?
A1.2	Wurde das Betriebssystem gehärtet?
A1.3	Wurden die neuesten Sicherheits-Patches installiert? ³⁰
A1.4	Ist die neueste Version der Firewall-Software installiert?
A1.5	Sind alle vom Hersteller veröffentlichten Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (Patches und/oder Workarounds) umgesetzt?
A1.6	Wurde der SYNDefender zum Schutz gegen SYN-Attacken aktiviert?
A1.7	Wurden weitere Schutzmechanismen (TCP Sequence Verifier, Kontrolle dynamischer Portverbindungen) konfiguriert?
Bemerkungen	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zur Firewall über das Netz (z. B. SSH) im Regelwerk auf berechnete Systeme eingeschränkt?
A2.2	Werden alle Zugänge zur Firewall über das Netz (z. B. SSH) durch Kennworte geschützt?
A2.3	Werden alle Zugänge zum Firewall-Managementsystem über das Netz (FireWall-1 GUI) auf berechnete Systeme eingeschränkt?
A2.4	Werden alle Zugänge zum Firewall-Managementsystem über das Netz (FireWall-1 GUI) durch eindeutige Administratorkennungen und Kennworte geschützt?
A2.5	Sind die Administratorrechte entsprechend den Tätigkeiten der Administratoren gewählt?
A2.6	Falls es Fernwartungszugänge durch Dritte gibt: Werden diese Zugänge überwacht?
A2.7	Werden die Tätigkeiten der Administratoren im Audit-Log regelmäßig kontrolliert?
A2.8	Sind die Regeln übersichtlich gegliedert?
A2.9	Sind die Regeln eindeutig kommentiert?
A2.10	Ist gewährleistet, dass Sicherheitslücken der Firewall-Software rechtzeitig bekannt und behoben werden?
Bemerkungen	
Prüfaspekt Schutz des Netzüberganges	
B1 Härtung gegen Angriffe auf Routing-Funktionen	
B1.1	Werden sichere Routing-Verfahren (statische Routen) eingesetzt?

³⁰ Hinweis: Der Zugang zu Patches und Updates ist nur mit Abschluss eines Wartungsvertrages möglich.

B1.2 Ist Forwarding deaktiviert?		
Bemerkungen		
B2 Konfiguration gemäß der Vorgaben		
B2.1 Sind interne Vorgaben für die Systeme vollständig umgesetzt worden?		
B2.2 Sind Ausnahmen davon separat zugelassen und abgenommen?		
Bemerkungen		
B3 Filterung des Netzwerkverkehrs		
B3.1 Ist der Schutz vor IP-Spoofing konfiguriert (Definition der erlaubten Netze an die jeweiligen Schnittstellen der Firewall), der ein Umgehen der Zugriffskontrolle durch Fälschen von Netzwerkadressen soweit als möglich verhindert?		
B3.2 Sind Regeln installiert, die die Kommunikation zwischen den angeschlossenen Teilnetzen wirkungsvoll und gemäß den Sicherheitsvorgaben kontrollieren?		
B3.3 Sind die erlaubten Protokolle so konfiguriert, dass nicht nur der Port, sondern auch der Protokoll-Typ (FTP, HTTP) verifiziert wird?		
B3.4 Erfolgt eine Verifizierung der Empfänger-Domänen mit Hilfe einer SMTP-Resource, wenn Mail aus dem Internet empfangen wird (nur relevant, wenn Mail aus dem Internet über das zu untersuchende System empfangen wird)?		
B3.5 Werden HTTP-Zugriffe aus dem Internet auf Server in der DMZ mit Hilfe einer URI-Resource kontrolliert?		
B3.6 Werden FTP-Zugriffe aus dem Internet auf Server in der DMZ mit Hilfe einer FTP-Resource kontrolliert?		
B3.7 Werden automatische Rückverbindungen (z. B. FTP-Data) auf bekannte Ports (<1024) abgewiesen?		
B3.8 Wird die Nutzung von „any“ in den Feldern „Source“ und „Destination“ der accept-Regeln vermieden?		
B3.9 Wird die Nutzung von „any“ im „Services“-Feld der accept-Regeln vermieden?		
Bemerkungen		

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden sicherheitsrelevante Ereignisse (z. B. Verstoß gegen die Zugriffskontrollregeln) durch die Firewall protokolliert? Werden kritische Ereignisse aufgezeichnet?
C1.2	Ist eine Default-Deny-Regel implementiert, die alle nicht erlaubten Verbindungen protokolliert?
C1.3	Ist sichergestellt, dass die Protokollierung sicherheitsrelevanter Ereignisse mit Zeitmarken erfolgt, die mit allen Protokollereignissen anderer Systeme synchron sind?
Bemerkungen	
C2 Auswertung/Alarmierung	
C2.1	Erfolgt eine (automatische) Alarmierung bei besonders kritischen Ereignissen?
C2.2	Werden die Sicherheitsprotokolle der Firewall überwacht?
Bemerkungen	

Prüfaspekt Verfügbarkeit	
D1 Ausfallvorsorge und Wiederanlauf	
D1.1	Sind Backup-Prozeduren für das Firewall- und das Managementsystem etabliert, die einen schnellen Wiederanlauf des Systems nach einem Ausfall gewährleisten?
D1.2	Sind Eskalationsprozeduren etabliert, die eine zügige Problembeseitigung beim Ausfall eines Systems gewährleisten?
D1.3	Sind die Verantwortlichkeiten und Vertretungsregelungen für die Firewall-Systeme klar formuliert?
D1.4	Sind Wartungs- und Supportverträge mit dem Hersteller der Firewall-Software vorhanden?
Bemerkungen	

Checkliste 4.4.1: Check Point Firewall Appliance	
Prüfkriterien	Sichere Grundkonfiguration einer Check Point Firewall Appliance Härtung der Firewall gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang Realisierung eines Basisschutzes auf Anwendungsebene
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die eine Check Point Firewall im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Diese Checkliste ist zusätzlich zur Checkliste des IT-Revisionsobjekts „Check Point Firewall-1 NG“ zu verwenden, wenn die Firewall-Software auf einer Appliance eingesetzt wird.</p> <p>Die Anforderungen sind generischer Natur, basieren auf keiner speziellen Firewall-Version und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten.</p> <p>Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p>

Prüfaspekt Selbstschutz	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zur Appliance über das Netz (HTTPS, SSH) auf berechnigte Systeme und Teilnetze eingeschränkt?
A2.2	Werden alle Zugänge zur Appliance über das Netz (HTTPS, SSH) durch Kennworte geschützt?
A2.3	Wird beim Zugang zur Appliance aus externen Netzen mindestens ein Browser-Zertifikat am Client verwendet?
A2.4	Werden alle Zugänge zur Appliance über das Netz ausreichend verschlüsselt?
A2.5	Ist die Schnittstelle zum Download von Betriebssystem- und Software-Images über das Netz (FTP, TFTP) auf berechnigte Systeme eingeschränkt?
A2.6	Ist gewährleistet, dass Sicherheitslücken des Betriebssystems der Firewallkomponente (Appliance) rechtzeitig bekannt und behoben werden?
Bemerkungen	

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1	Werden die erzeugten Protokolle (z. B. per SYSLOG) auf einem dedizierten System abgelegt?
Bemerkungen	

Checkliste 4.4.2: Check Point Firewall-1/Solaris	
Prüfkriterien	Sichere Grundkonfiguration einer Check Point Firewall auf Solaris Härtung der Firewall gegen Umgehung von Schutzfunktionen Herstellung eines Basisschutzes am Netzübergang Realisierung eines Basisschutzes auf Anwendungsebene
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die eine Check Point Firewall im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Diese Checkliste ist zusätzlich zur Checkliste des IT-Revisionsobjekts „Check Point FireWall-1 NG“ zu verwenden, wenn die Firewall-Software auf dem Betriebssystem Solaris eingesetzt wird.</p> <p>Die Anforderungen sind generischer Natur, basieren auf keiner speziellen Firewall-Version und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten.</p> <p>Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p>

Prüfaspekt Selbstschutz	
A1 Härtung gegen Angriffe auf das System	
A1.1	Sind alle nicht benötigten Dienste auf dem System deaktiviert?
A1.2	Sind alle unsicheren Systemzugänge (RSH, RLOGIN, RCP) gesperrt?
A1.3	Existiert ein Maßnahmenkatalog (Systemhersteller/Solaris-Distribution oder eigener Katalog), um das eingesetzte System zu härten, und wurden diese Maßnahmen vollständig umgesetzt?
A1.4	Sind alle vom Hersteller der verwendeten Solaris-Distribution oder von Dritten veröffentlichten Maßnahmen gegen bekannte Schwachstellen und Fehlfunktionen (Patches und/oder Workarounds) umgesetzt? ³¹
A1.5	Werden die eingestellten Passwörter sicher abgespeichert (shadow-Passwortdatei), so dass ein Ausspähen der Passwörter verhindert wird?
Bemerkungen	
A2 Sichere Administration	
A2.1	Werden alle Zugänge zum System über das Netz (z. B. SSH) auf berechnigte Systeme und Teilnetze eingeschränkt?
A2.2	Sind die Zugänge zum System über das Netz auf kryptographisch sichere Dienste (SSH) beschränkt?
A2.3	Werden alle Benutzer-Accounts durch Kennworte geschützt?
A2.4	Sind die Passwörter für nichtprivilegierte Accounts und für den root-Account unterschiedlich gewählt?
A2.5	Ist der Fernwartungszugang für den root-Account deaktiviert?
A2.6	Falls es Fernwartungszugänge durch Dritte gibt: Werden diese Zugänge überwacht? ³²
Bemerkungen	

³¹ Hinweis: Der Zugang zu Patches und Updates ist u. U. nur mit Abschluss eines Wartungsvertrages möglich.

³² Bei VS-Netzen und Netzen mit hohem oder sehr hohem Schutzbedarf sowie bei Netzen mit datenschutzrelevanten Daten wird Fernwartung durch Dritte nicht empfohlen.

Prüfaspekt Beweissicherung	
C1 Protokollierung	
C1.1 Werden die vom Betriebssystem Solaris erzeugten Protokolle (z. B. per SYSLOG) auf einem dedizierten System abgelegt?	
Bemerkungen	

Checkliste 4.4.3: Check Point Firewall-1 HA	
Prüfkriterien	<p>Sichere Grundkonfiguration einer redundanten Check Point Firewall</p> <p>Prüfung der Hochverfügbarkeitsanforderungen</p> <p>Härtung der Firewall gegen Umgehung von Schutzfunktionen</p> <p>Herstellung eines Basisschutzes am Netzübergang</p> <p>Realisierung eines Basisschutzes auf Anwendungsebene</p>
Vorgehensweise	Interview geeigneter Personen, Sichtung der Konfiguration sowie Vorlage und Analyse der betreffenden Dokumente
Beschreibung	<p>Die in dieser Checkliste beschriebenen Prüfaspekte beziehen sich auf diejenigen Anforderungen, die eine Check Point Firewall im Einsatzumfeld einer Netzkopplung erfüllen sollte.</p> <p>Diese Checkliste ist zusätzlich zur Checkliste des IT-Revisionsobjekts „Check Point FireWall-1 NG“ zu verwenden, wenn die HA (High Availability)-Funktion eingesetzt wird.</p> <p>Die Anforderungen sind generischer Natur, basieren auf keiner speziellen Firewall-Version und erheben weder den Anspruch auf Allgemeingültigkeit noch können sie alle denkbaren Konstellationen abdecken. Vielmehr sind sie im Kontext zu anderen Komponenten zu werten.</p> <p>Generell muss das Anforderungsprofil an die jeweilige Einsatzumgebung angepasst werden.</p>

Prüfaspekt Verfügbarkeit	
D2 Hochverfügbarkeit	
D2.1	Wurde die Hochverfügbarkeit des Systems so konfiguriert, wie es nach den Vorgaben im Sicherheitskonzept gefordert wurde?
D2.2	Ist die Synchronisierung der Statustabellen korrekt konfiguriert?
D2.3	Sind mehrere Schnittstellen für die Synchronisierung der Status-Informationen und die Prüfung der Cluster-Systeme (Heartbeat) vorhanden?
D2.4	Sind Mechanismen zur Selbstüberprüfung der Firewall-Systeme (Speicherplatz, Prozessorlast, Stati der Netzwerkschnittstellen usw.) implementiert?
D2.5	Ist gewährleistet, dass die Kommunikationsbeziehungen bei einem Ausfall einer Firewall-Komponente nicht unterbrochen werden?
Bemerkungen	

Dokumentvorlage für eine Checkliste

Die folgende Checkliste kann als Basis für eigene, weiter verfeinerte Checklisten verwendet werden.

Checkliste # <Name der Checkliste>	
Prüfkriterien	
Vorgehensweise	
Beschreibung	

Prüfaspekt <A>	
A1 <Prüfthema A1>	
A1.1 <Fragestellung>	
A1.2 <Fragestellung>	
A1.3 <Fragestellung>	
Bemerkungen	
A2 <Prüfthema A2>	
A2.1 <Fragestellung>	
A2.2 <Fragestellung>	
A2.3 <Fragestellung>	
Bemerkungen	

Prüfaspekt 	
B1 <Prüfthema B1>	
B1.1 <Fragestellung>	
B1.2 <Fragestellung>	
B1.3 <Fragestellung>	
Bemerkungen	

Formblätter

Während die Checklisten eine technische Orientierung oder auch einen roten Faden für die Revision auf technischer Ebene darstellen, sollen die Formblätter helfen, den organisatorischen Rahmen einer Revision zu strukturieren und auch rudimentär zu dokumentieren. Sie sind kein Ersatz für die vollständige und umfassende Dokumentation einer Revision, ermöglichen aber einen zusammenfassenden Überblick des Ablaufs und der wesentlichen Resultate.

Zu diesem Zweck stehen insgesamt – in Anlehnung an die Kernmodule – vier Formblätter plus ein Übersichtsformblatt für die gesamte Revision zur Verfügung:

- Deckblatt Revision,
- Formblatt Dokumentation,
- Formblatt Szenarien,
- Formblatt Betriebsprozesse und
- Formblatt Komponenten.

Falls in Revisionen mehrere Dokumente, Betriebsprozesse oder Komponenten relevant sind, kann je Objekt ein Formblatt verwendet und auf diese Weise eine vollständige Dokumentation ermöglicht werden.

Allgemeine Revisionsinformationen

IT-Revisionsobjekt	
Revisionsplan ID	
Ziel der Revision	
Beauftragter Revisor	
Verantwortlicher für das Revisionsobjekt	

Teilkomponenten	Architektur		Objektverantwortlicher	
	Plan ID		Ziel	
	Komponenten		Objektverantwortlicher	
	Plan ID		Ziel	
	Betriebsprozesse		Objektverantwortlicher	
	Plan ID		Ziel	
	Dokumente		Objektverantwortlicher	
	Plan ID		Ziel	

Zeitplan der Revision	Initiierung	
	Ausführung	
	Präsentation Report draft	
	Kommentierung erhalten	
	Revisionsreport Finalversion	
	Abschluss der Maßnahmen	

Betriebsprozessrevision

Plan:				
Anmerkungen:				
Beschreibung der Ist-Situation:				
Handlungsbedarf:	Ja		Nein	

Plan erfüllt	
Plan teilweise erfüllt	
Plan nicht erfüllt	

Beschreibung des Handlungsbedarfes

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Stellungnahme des Verantwortlichen für das Revisionsobjekt

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Liste der Maßnahmen (durch den Verantwortlichen für das Revisionsobjekt)

<Handlungsbedarf 1>		<Termin>	<Prio>	<Verantwortlich>
<Handlungsbedarf 2>				
<Handlungsbedarf 3>				

Dokumentenrevision

Plan:				
Anmerkungen:				
Beschreibung der Ist-Situation:				
Handlungsbedarf:	Ja		Nein	

Plan erfüllt	
Plan teilweise erfüllt	
Plan nicht erfüllt	

Beschreibung des Handlungsbedarfes

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Stellungnahme des Verantwortlichen für das Revisionsobjekt

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Liste der Maßnahmen (durch den Verantwortlichen für das Revisionsobjekt)

<Handlungsbedarf 1>		<Termin>	<Prio>	<Verantwortlich>
<Handlungsbedarf 2>				
<Handlungsbedarf 3>				

Komponentenrevision

Plan:				
Anmerkungen:				
Beschreibung der Ist-Situation:				
Handlungsbedarf:	Ja		Nein	

Plan erfüllt	
Plan teilweise erfüllt	
Plan nicht erfüllt	

Beschreibung des Handlungsbedarfes

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Stellungnahme des Verantwortlichen für das Revisionsobjekt

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Liste der Maßnahmen (durch den Verantwortlichen für das Revisionsobjekt)

<Handlungsbedarf 1>		<Termin>	<Prio>	<Verantwortlich>
<Handlungsbedarf 2>				
<Handlungsbedarf 3>				

Szenarienrevision

Plan:				
Anmerkungen:				
Beschreibung der Ist-Situation:				
Handlungsbedarf:	Ja		Nein	

Plan erfüllt	
Plan teilweise erfüllt	
Plan nicht erfüllt	

Beschreibung des Handlungsbedarfes

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Stellungnahme des Verantwortlichen für das Revisionsobjekt

<Handlungsbedarf 1>		<Einstufung>
<Handlungsbedarf 2>		
<Handlungsbedarf 3>		

Liste der Maßnahmen (durch den Verantwortlichen für das Revisionsobjekt)

<Handlungsbedarf 1>		<Termin>	<Prio>	<Verantwortlich>
<Handlungsbedarf 2>				
<Handlungsbedarf 3>				

Dokumentationsvorlage für einen Revisionsbericht

Die Dokumentationsvorlage dient dazu, eine Vorlage für einen schriftlichen Bericht der durchgeführten Revision zu liefern.

Im Einzelfall ist zu entscheiden, welchen Umfang die Dokumentation der Revision bekommen soll. Die Checklisten ermöglichen den einfachsten Fall der Aufzeichnung. Unter Zuhilfenahme der Formblätter kann eine Revision eine vollständigere Dokumentation, auch im Hinblick auf die Durchführung, den zeitlichen Ablauf sowie den beteiligten Personen vorweisen.

Vollständig abgeschlossen ist eine Revision aber erst inklusive eines umfassenden, schriftlichen Berichts, der ebenfalls die Resultate der Prüfungen in Form der Checklisten, Formblätter und anderer protokollierter Informationen (Konfigurationsfiles, Screenshots etc.) enthält.

Darüber hinaus ermöglicht ein schriftlicher Bericht aber auch, Resultate zu beurteilen und zu gewichten sowie insbesondere eine zusammenfassende Beurteilung zu erstellen.

Ergebnisbericht zur IT-Revision

Revisionsobjekt <Netzübergang>

<Organisation X>

<Einstufung>

Datum:

Version:

Dokumentinformation

Projekt:

Dok_ID:

Version:

Stand:

Status:

Autor(en):

Verteiler

Name	Organisation	Abteilung	Kontakt

Historie

Version	Stand	Autor	Änderung

Inhaltsverzeichnis

Integration und IT-Revision von Netzübergängen.....	1
Teil II: Revisionshilfsmittel.....	1
1 Revisionshilfsmittel.....	4
Checklisten für den Ablauf einer Revision.....	5
Formblätter.....	1
Dokumentationsvorlage für einen Revisionsbericht.....	1
1. Einleitung.....	5
Beteiligte Organisationseinheiten/Personen.....	5
2 Vorbereitung der IT-Revision.....	6
Prüfplan.....	6
3 Durchführung der IT-Revision.....	7
Dokumentation.....	7
Betriebsprozesse.....	7
Architektur.....	7
Komponenten.....	7
4 Ergebnisse der IT-Revision.....	8
Dokumentation.....	8
Betriebsprozesse.....	8
Architektur.....	8
Komponenten.....	8
5 Zusammenfassung und Management-Report.....	9
6 Handlungsempfehlung.....	10

Anlagen

1. Einleitung

[Beschreibung der gestellten Aufgabe, des zu untersuchenden Gegenstandes sowie die erwarteten Ziele.]

Beteiligte Organisationseinheiten/Personen

[Auflistung der beteiligten Organisationseinheiten und Personen sowohl auf Seiten des Auftraggebers als auch auf Seiten des Auftragnehmers.]

2 Vorbereitung der IT-Revision

[*Vorgehensweise und Ergebnisse der Vorbereitungsphase.*]

Prüfplan

3 Durchführung der IT-Revision

[*Vorgehensweise und Inhalte der Prüfung.*]

Dokumentation

Betriebsprozesse

Architektur

Komponenten

4 Ergebnisse der IT-Revision

[*Gefundene Soll-Abweichungen und Maßnahmen.*]

Dokumentation

Betriebsprozesse

Architektur

Komponenten

5 Zusammenfassung und Management-Report

[*Knappe Zusammenfassung der erzielten Resultate.*]

6 Handlungsempfehlung

Anlage A: Ergänzende Verzeichnisse

Anlage A.1: Abkürzungsverzeichnis

[*Auflistung der verwendeten Abkürzungen im Dokument.*]

Anlage A.2: Definitionen

[*Auflistung der verwendeten Definitionen im Dokument.*]

Anlage B: Rahmendokumentation zur IT-Revision

Anlage B.1: Formblätter

Folgende Formblätter wurden bei der IT-Revision verwendet:

[*Auflistung der Formblätter und Anfügen der Papierdokumente.*]

Anlage B.2: Checklisten

Folgende Checklisten wurden bei der IT-Revision verwendet:

[*Auflistung der Checklisten und Anfügen der Papierdokumente.*]

Anlage C: Protokollierte Daten der Konfigurationen

[*Anfügen der Protokolldaten aus der Konfiguration der Systeme.*]