Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Auditierungsschema

Für ISO 27001 Zertifizierungen auf der Basis von IT-Grundschutz

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	16.03.2011	BSI	Initiale Erstellung für die IT-Grundschutz-Kataloge
2.0	11.10.2017	BSI	Grundlegende Überarbeitung zur Anpassung an die Methodik gemäß dem IT-Grundschutz-Kompendium
2.1	25.05.2018	BSI	Anpassung der Formulierung in Kapitel 4.3 bezüglich Anzahl der zu prüfenden Bausteine
2.2	23.04.2019	BSI	Ergänzung in Kapitel 4.5 zu der Umsetzung von Basis-Anforderungen und Kapitel 4 zur Berücksichtigung von Abweichungen und Empfehlungen aus vorherigen Audits.
2.3	23.12.2019	BSI	Ergänzung in Kapitel 4.3 zur Bausteinprüfung, in Kapitel 4.3.1 zur Anzahl der Begutachtung der Standorte und in Kapitel 6 zum Überwachungsaudit.
2.4	31.01.2023	BSI	Überführung in aktuelles Dokumentenlayout, Kleinere Präzisierungen und Anpassungen.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-62 22
E-Mail: gs-zert-pruef@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Vorwort

Für die Bestätigung der Konformität eines Managementsystems für Informationssicherheit (ISMS) gemäß der ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz werden im Auditierungsschema die Anforderungen an die Prüfungshandlung des Auditteamleiters und der Mitglieder des Auditteams beschrieben.

Die grundsätzliche Vorgehensweise und die Voraussetzungen für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz werden im Zertifizierungsschema beschrieben. ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz geben Institutionen die Möglichkeit, ihre Bemühungen um Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen unter Anwendung der IT-Grundschutz-Methodik nach innen und außen zu dokumentieren.

Mit der Vergabe eines Zertifikats wird der Institution bescheinigt, dass

- Informationssicherheit ein anerkannter Wert ist,
- ein funktionierendes IS-Management vorhanden ist und außerdem
- zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau erreicht wurde.

Prüfgrundlage des Verfahrens sind:

- DIN ISO/IEC 27001: „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“
- BSI-Standard 200-1: „Managementsystem für Informationssicherheit ISMS“
- BSI-Standard 200-2: „IT-Grundschutz-Methodik“
- BSI-Standard 200-3: „Risikoanalyse auf Basis von IT-Grundschutz“
- IT-Grundschutz-Kompendium

1.2 Adressatenkreis

Dieses Dokument richtet sich vor allem an Auditteamleiter, die ein unabhängiges Audit in einer Institution durchführen, um die Konformität eines Managementsystems für Informationssicherheit (ISMS) gemäß ISO 27001 auf der Basis von IT-Grundschutz zu bestätigen. Verantwortliche für die Informationssicherheit können sich einen Überblick darüber verschaffen, welche Prüfanforderungen bei einem Audit gestellt werden und welche Referenzdokumente zur Verfügung gestellt werden müssen.

1.3 Literaturverzeichnis

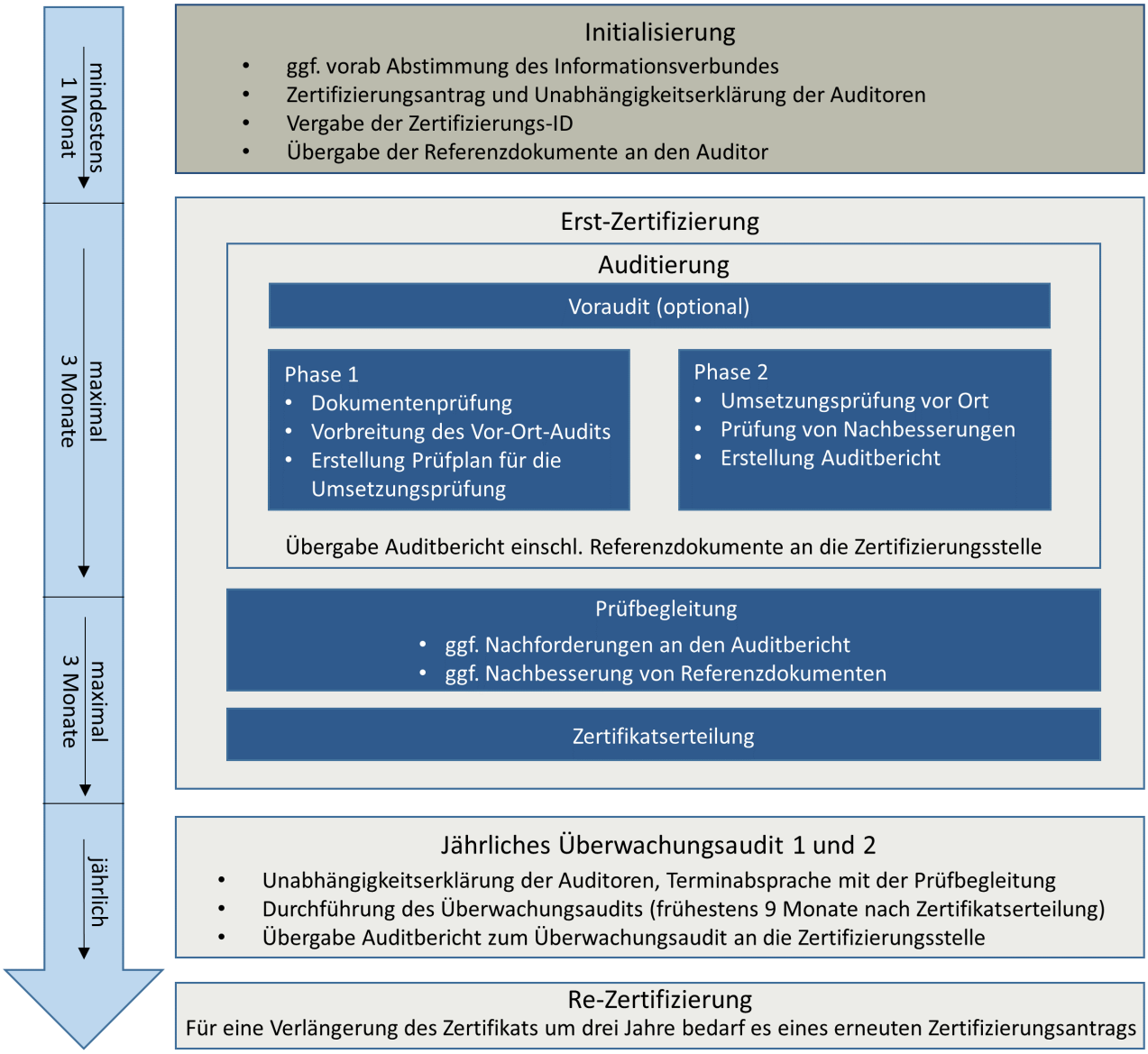
Bezeichnung	Beschreibung
27001	ISO/IEC 27001: „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Management – Anforderungen“, 2022
200-1	Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-1 „Managementsysteme für Informationssicherheit (ISMS), Version 1.0, Oktober 2017
200-2	Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-2 „IT-Grundschutz-Methodik“, Version 1.0, Oktober 2017
200-3	Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3 „Risikoanalyse auf der Basis von IT-Grundschutz“, Version 1.0, Oktober 2017

Bezeichnung	Beschreibung
ITGSK	Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, jährlich neu
OUTS	Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Methodik im Kontext von Outsourcing“, Version 2.2, Dezember 2019

2 Überblick über das Zertifizierungsverfahren

2.1 Der Ablauf des Prozesses

Erst nach erfolgreicher Initialisierung des Zertifizierungsprozesses durch die Stellung eines Zertifizierungsantrags und Prüfung der Unabhängigkeitserklärungen aller Mitglieder des Auditteams, kann ein Audit begonnen und durchgeführt werden.



Auf der Grundlage einer Dokumentenprüfung (siehe Kapitel 4.1 Phase 1 des Audits: Dokumentenprüfungen) bereiten sich die Mitglieder des Auditteams auf die Vor-Ort-Prüfung (siehe Kapitel 4.2 Vorbereitung des Vor-Ort-Audits) vor, bevor das Auditteam die konkrete Umsetzung der Anforderung vor Ort überprüft (siehe Kapitel 4.4 Phase 2: Umsetzungsprüfung vor Ort). Werden Defizite festgestellt, muss die Institution Nachbesserungen durchführen (siehe Kapitel 4.6 Nachbesserungen), damit der Auditteamleiter ein positives Gesamtvotum (siehe Kapitel 4.8 Gesamtvotum für die Erteilung eines Zertifikats) abgeben kann. Nach Abgabe des Auditberichts an die Prüfbegleitung der Zertifizierungsstelle des BSI kann diese noch Nachforderungen (siehe Kapitel 4.9 Nachforderungen) an den Auditbericht gegenüber dem Auditteamleiter oder den Antragsteller haben. Nach positiver Abnahme des Auditberichts kann ein Zertifikat erteilt werden.

2.2 Arten der Auditierung

Ein **Erst-Zertifizierungsaudit** betrachtet den gesamten Sicherheitsprozess eines Informationsverbundes sowie die Überprüfung der Umsetzung der Anforderungen im Rahmen einer Stichprobenprüfung auf der Basis von Bausteinen aus dem IT-Grundschutz-Kompendium. Hierbei kann sich der Auditteamleiter mit dem Auditteam im Rahmen eines Voraudits einen Überblick über den Informationsverbund verschaffen.

Die Aufrechterhaltung der Sicherheit wird mit einem jährlich durchzuführenden **Überwachungsaudit** geprüft.

Ein Zertifikat kann durch eine **Re-Zertifizierung** um drei Jahre verlängert werden. Der Auditteamleiter greift für das Re-Zertifizierungsaudit auf die Ergebnisse der Auditierungen der vorhergehenden Zertifizierung (Audit für das Erst-Zertifizierungsverfahren sowie die Überwachungsaudits) zurück und berücksichtigt bei der Prüfung auch die Veränderungen, die sich innerhalb des Informationsverbundes seit dem letzten Audit ergeben haben.

Jedes Audit umfasst zwei Phasen: eine Dokumentenprüfung und eine Vor-Ort-Prüfung. Die Ergebnisse werden immer in einem Auditbericht zusammengefasst.

2.3 Voraussetzungen aus Seiten des Antragstellers

Für jedes Audit stellt eine Institution die erforderlichen Referenzdokumente bereit. Zusätzlich sind vom Antragsteller in einer zusammenfassenden Übersicht der Stand der jeweiligen Referenzdokumente sowie wesentliche Änderungen gegenüber dem letzten Audit aufzuzeigen.

Voraussetzung für die Zertifizierung und Auditierung ist die Umsetzung der Standard- oder Kernabsicherung der IT-Grundschutz-Methodik. Grundlage dafür ist die aktuelle Version der Prüfungsgrundlage für Zertifizierungen nach ISO 27001 auf der Basis von IT-Grundschutz in der die gültigen Versionen und Übergangsfristen festgelegt sind. Für jedes Verfahren muss die aktuelle Edition des IT-Grundschutz-Kompendiums verwendet werden, da zum Auditbeginn durch den Auditteamleiter geprüft wird, ob gültige Versionen verwendet wurden.

Folgende Referenzdokumente bilden die Grundlage für die Zertifizierung und müssen vom Antragsteller dem Auditteamleiter und der Prüfbegleitung des BSI zur Verfügung gestellt werden:

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

Der Auditteamleiter kann darüber hinaus während des Vor-Ort-Audits weitere Dokumente und Aufzeichnungen einsehen.

Die Referenzdokumente sind Bestandteil des Auditberichts. Sollten zusätzliche Dokumente erstellt worden sein, die zur Prüfung relevant sind, sind diese ebenfalls in der aktuellen Fassung dem Auditteamleiter vorzulegen und können bei Bedarf Gegenstand des Auditberichts werden.

3 Berufsethik

Die Auditierung stützt sich auf eine Reihe von Prinzipien. Diese machen das Audit zu einem wirksamen und zuverlässigen Werkzeug. Um Vertrauen in eine objektive Prüfung zu schaffen, ist die Einhaltung der Berufsethik notwendig. Dies ist eine Voraussetzung für nachvollziehbare, wiederholbare und vergleichbare Auditergebnisse, um eine nachfolgende Zertifizierung zu ermöglichen.

Die Berufsethik umfasst folgende Prinzipien:

- **Ethisches Verhalten**: Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Daten zu finden sind, sind die Vertraulichkeit der Informationen und der diskrete Umgang mit den Ergebnissen des Audits eine wichtige Arbeitsgrundlage. Sowohl die Zertifizierungsstelle des BSI als auch die auditierte Institution müssen dem Auditteamleiter und dem Auditteam in ihrem Vorgehen vertrauen können.
- **Fachkompetenz**: Die Mitglieder des Auditteams übernehmen nur solche Aufgaben, für die sie das erforderliche Wissen, Können und die entsprechende Erfahrung haben, und setzen diese/s bei der Durchführung ihrer Arbeit ein. Sie verbessern kontinuierlich ihre Fachkenntnisse sowie die Effektivität und Qualität ihrer Arbeit.
- **Vertrauenswürdigkeit**: Da im Umfeld der Informationssicherheit oft sensible Geschäftsprozesse und Informationen zu finden sind, ist die Vertraulichkeit der während eines Audits erlangten Informationen und der diskrete Umgang mit den Auskünften und Ergebnissen der Prüfung eine wichtige Arbeitsgrundlage. Informationen dürfen nicht ohne entsprechende Befugnis offengelegt werden, es sei denn, es bestehen dazu rechtliche oder berufliche Verpflichtungen.
- **Sachliche Darstellung**: Ein Auditteamleiter hat die Pflicht, sowohl der zu auditierenden Institution als auch der Zertifizierungsstelle wahrheitsgemäß und genau über die Untersuchungsergebnisse zu berichten. Dazu gehört die wahrheitsgemäße und nachvollziehbare Darstellung des Sachverhaltes in den Feststellungen und Voten im Auditbericht. Die Prüfungsergebnisse des Audits müssen (bei unverändertem Sachstand) wiederholbar sein.
- **Nachweise und Nachvollziehbarkeit**: Die rationale Grundlage, um zu zuverlässigen und nachvollziehbaren Schlussfolgerungen und Ergebnissen zu kommen, ist eine eindeutige und folgerichtige Dokumentation der Sachverhalte erforderlich. Hierzu gehört auch die dokumentierte und nachvollziehbare Methodik, mit der der Auditor zu seinen Schlussfolgerungen kommt.
- **Objektivität und Sorgfalt**: Ein Auditteamleiter hat ein Höchstmaß an sachverständiger Qualität und Sorgfalt beim Zusammenführen, Bewerten und Weitergeben von Informationen über geprüfte Aktivitäten oder Geschäftsprozesse zu zeigen. Die Beurteilung aller relevanten Umstände hat mit Ausgewogenheit zu erfolgen und darf nicht durch eigene Interessen oder durch Dritte beeinflusst werden.

4 Der Auditprozess

Jedes Audit setzt sich grundsätzlich aus zwei getrennten, aufeinander aufbauenden Phasen zusammen. Die erste Phase umfasst zunächst die Prüfung der vom Antragsteller eingereichten Referenzdokumente. In der zweiten Phase schließt sich eine Vor-Ort-Prüfung des Informationsverbundes durch das Auditteam an. Hierbei wird im realen Informationsverbund die praktische Umsetzung der in den Referenzdokumenten dokumentierten Sicherheitsmaßnahmen auf ihre Vollständigkeit, Korrektheit und Wirksamkeit hin überprüft.

Für jedes Audit ist vom Auditteamleiter ein Auditbericht zu erstellen, der alle Prüfergebnisse enthält. In Anlehnung an die Aufteilung eines Audits in zwei Phasen ist der Auditbericht ebenfalls in zwei Schritten zu erstellen: zunächst dokumentiert der Auditbericht die Auditergebnisse für die erste Phase des Auditprozesses (Dokumentenprüfung), anschließend sind die Auditergebnisse der zweiten Phase (Vor-Ort-Prüfung) zu ergänzen.

Abweichungen und Empfehlungen aus vorangegangenen IT-Grundschutz-Audits sind im Rahmen des kontinuierlichen Verbesserungsprozesses zu berücksichtigen und auditieren.

Hinweis: Die Erläuterungen zum Auditprozess gelten sowohl für das Erst- als auch Re-Zertifizierungsaudit sowie für die beiden Überwachungsaudits. Abweichend hiervon gestaltet sich das Voraudit.

Der Auditbericht muss auf der Basis des Musters für Auditberichte in der jeweils gültigen Version erstellt werden.

4.1 Phase 1 des Audits: Dokumentenprüfung

Die erste Phase dient dazu, dass der Auditteamleiter ein ausreichendes Verständnis für den Informationsverbund erlangt und feststellt, ob die Konzeption der Sicherheitsstruktur des Informationsverbundes gemäß der Vorgehensweise des BSI-Standards 200-2 schlüssig und sinnvoll ist. Der Auditor prüft insbesondere, ob die Zertifizierungsfähigkeit des Informationsverbundes grundsätzlich gegeben ist.

Damit der Auditteamleiter ein ausreichendes Verständnis des Informationsverbundes gewinnen kann, kann es sinnvoll sein, einen Teil der Dokumentenprüfung bei der auditierenden Institution durchzuführen. In einigen Fällen ist die Einsichtnahme von Dokumenten auch aus Vertraulichkeitsgründen nur vor Ort möglich.

Festgestellte Abweichungen und Empfehlungen in den Referenzdokumenten teilt der Auditteamleiter dem Antragsteller mit einer angemessenen Frist zur Behebung mit. Der Antragsteller bekommt somit die Gelegenheit, festgestellt Abweichungen und Empfehlungen bereits vor der zweiten Phase des Audits zu beheben.

Alle Abweichungen und Empfehlungen aus der Dokumentenprüfungen müssen im Auditbericht dokumentiert werden. Dies gilt auch dann, wenn die Abweichungen und Empfehlungen bereits vor der zweiten Phase des Audits behoben wurden.

4.2 Vorbereitung des Vor-Ort-Audits

Der Auditteamleiter erhält durch die Dokumentenprüfung einen umfassenden Einblick in die zu auditerende Institution. Nach dieser Prüfung sollte der Auditor prüfen, ob die Fachkenntnisse des Auditteams ausreichend sind. Es können Sektor und Baustein spezifische Fachkenntnisse für die Auditierung nötig sein, die das Auditteam zum Zeitpunkt der Anmeldung für die Zertifizierung nicht ausreichend erfüllt. Dann muss der Auditteamleiter das Auditteam durch Auditoren oder Fachexperten erweitern. Die Anpassung des Auditteams muss rechtzeitig der Zertifizierungsstelle des BSI mitgeteilt werden. Die Unabhängigkeitserklärungen müssen rechtzeitig vor dem Vor-Ort-Audit an die Zertifizierungsstelle des BSI übersendet und von dieser freigegeben werden.

Nach der Dokumentenprüfung besteht für den Auditteamleiter die Möglichkeit, den Auditierungsprozess abzubrechen, wenn ein Abschluss der Auditierung mit einem positiven Votum ausgeschlossen erscheint. Dies ist beispielsweise dann der Fall, wenn die Dokumentation zum ISMS gravierende Defizite aufweist oder bei der Institution nicht die Bereitschaft erkennbar ist, beim Zertifizierungsaudit aktiv mitzuwirken. Die Zertifizierungsstelle des BSI muss hiervon informiert werden.

4.3 Erstellung eines Auditplans für die Vor-Ort-Prüfung

Zur Vorbereitung auf die Vor-Ort-Prüfung muss der Auditteamleiter einen Auditplan erstellen. Das bedeutet, dass der Auditteamleiter aus den Ergebnissen der Dokumentenprüfung die erforderlichen Themen benennt, damit die zu auditierende Institution die Interviewpartner rechtzeitig benennen kann.

Für die Vorbereitung der Vor-Ort-Prüfung gelten die folgenden Vorgaben:

- Bei der Erst-/Re-Zertifizierung werden mindestens 6 Bausteine auditiert, darunter zwingend der Baustein ISMS.1 Sicherheitsmanagement.
- Bei den beiden Überwachungsaudits werden jeweils zwingend der Baustein ISMS.1 Sicherheitsmanagement und mindestens 2 weitere Bausteine auditiert.
- Über die Zertifikatslaufzeit gilt:
    - Es werden alle modellierten Schichten mit mindestens je einem Baustein überprüft.
    - Es werden mindestens 12 Bausteine auditiert.
    - Es werden mindestens 10% der modellierten Bausteine auditiert.
    - Der Auditteamleiter kann die Stichprobe erweitern.
    - Der Baustein ISMS.1 (Sicherheitsmanagement) wird zwingend bei jedem Audit geprüft.
    - Der Baustein OPS.2.1 Outsourcing für Kunden bzw. OPS.2.3 Nutzung von Outsourcing wird zwingend auditiert, sofern Outsourcing-Dienstleister im Informationsverbund eingebunden sind.
- Der Auditteamleiter wählt die Bausteine Risiko-orientiert aus und begründet die Auswahl.
- Der Auditteamleiter wählt zu den Bausteinen die Zielobjekte aus und begründet die Auswahl.
- Es werden 5 Maßnahmen der Risikoanalyse auditiert. Der Auditteamleiter muss seine Auswahl begründen.

Beispiel: Auswahl der Bausteine für einen kompletten Audit-Zyklus

Erst-/Re-Zertifizierung:

1. ISMS.1 Sicherheitsmanagement
2. ORP.4 Identitäts- und Berechtigungsmanagement
3. CON.3 Datensicherungskonzept
4. OPS.1.1.1 Allgemeiner IT-Betrieb
5. NET.3.2 Firewall
6. INF.2 Rechenzentrum sowie Serverraum
7. SYS.1.1 Allgemeiner Server (erweiterte Stichprobe/risikoorientierte Prüfung)
8. SYS.1.2.3 Windows Server (erweiterte Stichprobe/risikoorientierte Prüfung)

1. Überwachungsaudit:

1. ISMS.1 Sicherheitsmanagement
2. OPS.2.3 Nutzung von Outsourcing
3. DER.2.2 Vorsorge für die IT-Forensik
4. OPS.1.1.3 Patch- und Änderungsmanagement (erweiterte Stichprobe/risikoorientierte Prüfung)

2. Überwachungsaudit:

1. ISMS.1 Sicherheitsmanagement
2. APP.5.3 Allgemeiner E-Mail-Client und –Server
3. APP.5.2 Microsoft Exchange und Outlook
4. ORP.3 Sensibilisierung und Schulung zur Informationssicherheit (erweiterte Stichprobe/risikoorientierte Prüfung)

Welche Zielobjekte konkret auditiert werden, sollte der zu auditierenden Institution nach Möglichkeit vorab nicht mitgeteilt werden. Sofern eine Änderung der Bausteinwahl erforderlich oder sinnvoll ist, muss eine plausible Begründung vorliegen.

Sollten sich während der Zertifikatslaufzeit neue Risiken ergeben (z. B. Änderung im Informationsverbund, neue bekannte Risikoklasse, neue Risikobehandlungen) sollten diese Änderungen vor einem Vor-Ort-Audit zwischen dem Auditteamleiter und der Prüfbegleitung der Zertifizierungsstelle des BSI bewertet werden. Die zu Beginn der Zertifikatslaufzeit getroffene Auswahl kann aufgrund veränderter Rahmenbedingungen nachträglich und begründet angepasst werden.

4.3.1 Begutachtung der Standorte es Informationsverbundes

Die Mindestanzahl an Standorten (Stichprobe), die pro Audit zu begehen sind, berechnet sich wie folgt:

- **Erst-Zertifizierungsaudit:** Quadratwurzel aus der Anzahl der Standorte, gerundet auf die höhere Anzahl.
- **Überwachungsaudit:** Quadratwurzel aus der Anzahl der Standorte, multipliziert mit dem Faktor 0,6, gerundet auf die höhere Anzahl.
- **Re-Zertifizierungsaudit:** analog zum Erst-Zertifizierungsaudit, sollte sich das ISMS in den letzten drei Jahren als effektiv erwiesen haben, berechnet sich die Mindestanzahl an Standorten durch die Quadratwurzel aus der Anzahl der Standorte, multipliziert mit dem Faktor 0,8, gerundet auf die höhere Anzahl.

Beispiel: Ein Informationsverbund besteht auch 18 Standorten, somit ergibt sich pro Audit folgende Mindestanzahl an Standorten, die zu begehen sind:

- **Erst-Zertifizierungsaudit:** 5
- **Überwachungsaudit:** 3
- **Re-Zertifizierungsaudit:** 5, bei effektivem ISMS 4

Die Vorgaben richten sich nach IAF MD 1 - Verbindliches IAF-Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten (DAkkS 71 SD 6 013).

Die ausgewählten Standorte werden im Auditbericht bereits beim Erst-/Re-Zertifizierungsverfahren über die Zertifikatslaufzeit hinweg für eine Begutachtung vor Ort geplant. Diese Planung darf aufgrund veränderter Rahmenbedingungen begründet angepasst werden.

Abweichungen von der beschriebenen Vorgehensweise bei der Auswahl von Standorten (z. B. die vollständige Begutachtung aller Standorte, wenn diese mehr drei umfassen) sind zulässig, müssen jedoch vorher mit der Zertifizierungsstelle des BSI abgestimmt werden.

4.3.2 Outsourcing

Sind Teile des Informationsverbundes ausgelagert (sogenanntes Outsourcing), ist die Auditierung auf der Basis der ergänzenden Bestimmungen zum Auditierungsschema durch das Dokument „IT-Grundschutz im Kontext von Outsourcing“ vorzunehmen.

4.4 Phase 2 des Audits: Umsetzungsprüfung vor Ort

Es ist wichtig, dass das Managementsystem für Informationssicherheit des Informationsverbundes wirksam und effektiv ist, gelebt und weiterentwickelt wird. Dazu gehört auch, dass alle wichtigen Prozesse des Informationsverbundes dokumentiert sind, und nach diesen Prozessen verfahren wird. Der Auditteamleiter prüft die Sicherheitsleitlinie und andere Dokumente und führt intensive Gespräche mit den Mitarbeitern der zu auditierenden Institution, ums ich von der Effektivität und der Effizienz des ISMS zu überzeugen.

Bei der Vor-Ort-Prüfung wird für jeden gewählten Baustein durch Inspektion des jeweiligen Zielobjekts überprüft, ob der im IT-Grundschutz-Check festgestellte und dokumentierte Umsetzungsstatus die in diesem Baustein enthaltenen Anforderungen angemessen umsetzt. Für den Fall, dass es zu einem Baustein Umsetzungshinweise gibt, sollten diese gesichtet und überprüft werden, ob die Anforderungen mit diesen oder gleichwertigen Sicherheitsmaßnahmen umgesetzt wurden. Es sollten keine schwächeren Mechanismen umgesetzt werden.

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

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

Bei Anforderungen, die die Institution als entbehrlich gekennzeichnet hat, muss die Begründung für den Auditteamleiter nachvollziehbar dokumentiert sein.

4.5 Übernahme von Risiken durch das Management (Realisierungsplan)

Für Anforderungen, die nicht oder noch nicht vollständig umgesetzt wurden, bedarf es eines Realisierungsplans (siehe hierzu BSI-Standard 200-2). Die bestehenden Risiken bis zur vollständigen Umsetzung der Anforderungen müssen für das Management transparent dargestellt werden. Darüber hinaus müssen im Realisierungsplan auch solche Risiken dokumentiert werden, für die das Management eine Risiko-Übernahme oder einen Risiko-Transfer (siehe hierzu BSI-Standard 200-3) beschlossen hat.

Die Übernahme von Risiken muss vom Management durch Unterschrift oder elektronische Freigabe bestätigt werden.

Sind zum Zeitpunkt der Auditierung IT-Grundschutz-Anforderungen des Realisierungsplans noch nicht oder nur teilweise umgesetzt, entscheidet der Auditteamleiter, ob eine Zertifizierung zu diesem Zeitpunkt möglich ist. Der Auditteamleiter muss Risiko orientiert den Gesamtkontext des Informationsverbundes und der kritischen Geschäftsprozesse betrachten. Teilanforderungen mit dem Modalverb MUSS, also solche Teilanforderungen, die grundlegend zur Informationssicherheit der gesamten Institution beitragen, dürfen nicht in die Risiko-Übernahme einfließen. Voraussetzungen für eine ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz ist, dass alle Teilanforderungen mit dem Modalverb MUSS umgesetzt sind. Dies gilt sowohl für Basis- als auch für Standard-Anforderungen.

Anforderungen können nur dann als „Entbehrlich“ gekennzeichnet werden, wenn die Erfüllung in der vorgeschlagenen Art nicht notwendig ist. Wenn z. B. eine Anforderung im betrachteten Informationsverbund nicht relevant ist (z. B. weil Dienste nicht aktiviert wurden) oder durch Alternativmaßnahmen behandelt wurde (vgl BSI-Standard 200-2). Der Umsetzungsstatus „entbehrlich“ kann nicht dazu genutzt (oder verwendet) werden, um zu begründen, warum eine eigentlich zu erfüllende Anforderung ganz bewusst nicht erfüllt wird. Wird eine Anforderung gewollt nicht erfüllt (beispielsweise aus wirtschaftlichen Gründen), dann ist der Umsetzungsstatus auf „nein“ zu setzen, wodurch die Anforderung automatisch in den Realisierungsplan aufgenommen wird, ggf. mit dem Hinweis, dass die

Umsetzung dieser Anforderung nicht vorgesehen ist. Im Realisierungsplan wird die Anforderung behandelt wie eine Anforderung, die nicht oder nicht vollständig umgesetzt ist: Die durch die fehlende Umsetzung entstehenden Risiken sind zu bewerten und der Leitungsebene transparent darzustellen. Die Leitungsebene muss die entstehenden Risiken tragen und dies durch Unterschrift oder elektronischer Freigabe bestätigen.

4.6 Nachbesserungen während des Audits

Sowohl bei der Sichtung der Referenzdokumente als auch bei der Inspektion vor Ort werden in manchen Fällen Abweichungen und Empfehlungen ausgesprochen werden. Diese müssen sachgerecht behoben und dokumentiert werden. Dabei gibt es verschiedene Stufen der Behandlung von Abweichungen und Empfehlungen:

- Der Auditteamleiter hat die Möglichkeit, **Empfehlungen** an die Institution auszusprechen. Diese sind nicht bindend, erhöhen aber die Effektivität und Effizienz des ISMS. Empfehlungen sind z. B. Verbesserungsvorschläge, die im Rahmen der kontinuierlichen Verbesserung der Prozesse umgesetzt werden sollten, zumindest jedoch zu prüfen sind. Die Empfehlungen werden mit einer Frist zur Prüfung versehen. Die Nichtbeachtung der Prüfung einer Empfehlung kann nach der Entscheidung des Auditteamleiters oder der Prüfbegleitung der Zertifizierungsstelle des BSI zu einer geringfügigen Abweichung führen.
- **Geringfügige Abweichungen** sind Mängel, bei denen IT-Grundschutz-Anforderungen nicht angemessen umgesetzt werden, das ISMS aber insgesamt funktioniert. Eine Abweichung ist also dann geringfügig, wenn einzelne Aspekte einer Anforderung nicht (ausreichend) umgesetzt wurden, aber das wesentliche Ziel der Anforderung realisiert ist. Eine Ausstellung des Zertifikats kann unter Umständen trotzdem erfolgen. Mehrere geringfügige Abweichungen können zusammen eine schwerwiegende Abweichung darstellen. Die Anzahl der geringfügigen Abweichungen für die Erteilung eines Zertifikats muss in jedem Einzelfall bewertet werden.
- **Schwerwiegende Abweichungen** sind Mängel, ohne deren Behebung nicht sichergestellt werden kann, dass das Informationssicherheitsmanagementsystem effektiv und effizient funktioniert oder die Sicherheit des Informationsverbundes erheblich gefährdet ist. Ein solcher Mangel kann vorliegen, wenn IT-Grundschutz-Anforderungen nicht oder in wesentlichen Teilen nicht umgesetzt sind. Bei Vorliegen von schwerwiegenden Abweichungen ist die Ausstellung oder Aufrechterhaltung eines Zertifikats nicht möglich.

Der Auditteamleiter entscheidet bei Abweichungen, ob es sich um geringfügige oder schwerwiegende Abweichungen handelt. Jede ausgesprochene Abweichung oder Empfehlung wird mit einer angemessenen Bearbeitungsfrist in die Liste eingetragen.

Der Auditteamleiter beginnt die Liste der Abweichungen und Empfehlungen bereits während der Dokumentenprüfung. Im Anschluss an die Dokumentenprüfung überreicht der Auditteamleiter die Liste der Abweichungen und Empfehlungen dem Ansprechpartner der zu auditierenden Institution, so dass diese die Möglichkeit erhalten, bis zum Vor-Ort-Audit die ersten Abweichungen und Empfehlungen zu beheben.

Während des Vor-Ort-Audits prüft der Auditteamleiter, ob bereits Abweichungen und Empfehlungen auf der Dokumentenbasis behoben wurden und dokumentiert diesen Status in der Liste der Abweichungen und Empfehlungen.

Abweichungen und Empfehlungen, die während des Vor-Ort-Audits festgestellt werden, ergänzt der Auditteamleiter in der Liste der Abweichungen und Empfehlungen.

Die Liste der Abweichungen und Empfehlungen wird für den Informationsverbund fortgeschrieben. Dies ist vor allem bei der Vergabe der Nummern zu berücksichtigen.

4.7 Erstellung des Auditberichts

Für jedes Audit wird vom Auditteamleiter ein Auditbericht erstellt, der alle Prüfergebnisse enthält. Es muss immer die gültige Version des Muster-Auditberichts verwendet werden. Die Inhalte aus dem Bericht dürfen nicht verändert werden. Die Ausfüllhilfe im Anhang des Auditberichts muss beachtet werden.

Im Falle eines Erst- oder Re-Zertifizierungsaudits dient der Auditbericht der Zertifizierungsstelle des BSI als Grundlage für die Erteilung des Zertifikats. Ein Auditbericht im Rahmen eines Überwachungsaudits bildet für die Zertifizierungsstelle des BSI die Grundlage für die Aufrechterhaltung eines erteilten Zertifikats. Der Auditbericht muss der Zertifizierungsstelle des BSI unterschrieben in Papierform sowie in elektronischer Form zur Verfügung gestellt werden.

4.8 Gesamtvotum

Grundlage für die Entscheidung über die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Einschätzung des Auditteamleiters, ob der betrachtete Informationsverbund die jeweiligen Anforderungen erfüllt.

Das Gesamtvotum ist vom Auditteamleiter mit Datum zu unterschreiben.

4.9 Nachforderungen

Die Prüfbegleitung der Zertifizierungsstelle des BSI empfängt den Auditbericht mit den erforderlichen Referenzdokumenten in verschlüsselter Form. Die Prüfbegleitung prüft den Auditbericht und kann bei Bedarf Nachforderungen an den Auditteamleiter oder an die auditierte Institution benennen.

Die Nachforderungen der Prüfbegleitung können zu einer Nachbesserung gegenüber dem Antragsteller führen. Der Auditteamleiter informiert die auditierte Institution entsprechend. Für die Nachbesserung wird der Institution einmalig Gelegenheit zur Beseitigung der Defizite gegeben. Der Auditteamleiter dokumentiert die Nachbesserung im Auditbericht und bewertet diese im entsprechenden Kapitel des Auditberichts. Die Prüfbegleitung kann gegenüber dem Auditteamleiter mehrmals Nachforderungen stellen.

Hat die auditierte Institution bezüglich festgestellter Abweichungen und Empfehlungen eine andere Auffassung als der Auditteamleiter kann der Auditteamleiter sich schriftlich bei der Zertifizierungsstelle oder Prüfbegleitung des BSI zu den dokumentierten Abweichungen und Empfehlungen äußern. Der Kommentar wird der Institution vorgelegt und in die Liste der Abweichungen und Empfehlungen im Auditbericht übernommen. Der Prüfbegleitung oder der Zertifizierungsstelle obliegt die Entscheidung, ob die Abweichung behoben werden muss und innerhalb welcher Frist dies geschehen soll.

Kommt es zu Nachforderungen seitens der Prüfbegleitung, sind diese vom Auditteamleiter innerhalb der in der Kommentierung benannten Frist zu beheben. Sollte absehbar sein, dass die benannte Frist nicht eingehalten werden kann, muss der Auditteamleiter unverzüglich Kontakt mit der Prüfbegleitung aufnehmen und eine Fristverlängerung begründet beantragen.

4.10 Zertifikatserteilung und Aufrechterhaltung

Sobald der Auditbericht zu einem Erst- oder Re-Zertifizierungsaudit in vollständiger Fassung bei der Zertifizierungsstelle des BSI vorliegt, prüft die Zertifizierungsstelle den Auditbericht auf Einhaltung aller Vorgaben des vorliegenden Auditierungsschema. Die Prüfung gegen das Auditierungsschema erfolgt mit der Zielsetzung, ein einheitliches Niveau aller Zertifizierungen und die Vergleichbarkeit von einzelnen Zertifizierungsaussagen zu gewährleisten. Analog verhält es sich bei Überwachungsaudits mit dem Ziel der Aufrechterhaltung eines erteilten Zertifikats.

5 Voraudit

Beim sogenannten Voraudit kann der Auditor gezielt einzelne Aspekte auswählen und stichprobenartig vor Ort und anhand der Referenzdokumente prüfen. Außer intensiven Gesprächen mit dem Antragsteller hat der Auditteamleiter die Möglichkeit, sich Dokumente, Prozesse und Implementierungen anzusehen, um einen Eindruck davon zu bekommen, ob ein Zertifizierungsaudit prinzipiell zu einem positiven Ergebnis führen könnte.

5.1 Umfang des Voraudits

Das Voraudit darf in Summe nicht mehr als ein Dritte der Gesamtzeit für das Zertifizierungsaudit in Anspruch nehmen. Das Voraudit darf nicht dem Zweck dienen, die Institution auf später geprüft Aspekte vorzubereiten, indem Prüfungen wiederholt werden.

5.2 Dokumentation des Voraudits

Alle Prüfungen, die der Auditteamleiter während des Voraudits durchführt, müssen im Auditbericht dokumentiert werden. Hierzu gehört auch der Umfang des Voraudits mit den geprüften Aspekten, Ergebnissen und Feststellungen.

Hinweis: Wenn der Auditteamleiter ein Voraudit durchführt, ist es sinnvoll, unter anderem die Prüfpunkte zu:

- Aktualität der Dokumente
- Leitlinie zur Informationssicherheit
- Referenzdokumente
- Nachvollziehbarkeit der Abgrenzung des Informationsverbundes und
- Wirksamkeit des ISMS

schon zu diesem Zeitpunkt durchzuführen oder anzureißen.

5.3 Verschiebung des Audits

Kommt der Auditteamleiter nach dem Voraudit zu der Empfehlung, das Audit um eine von ihm festgesetzte Zeit zu verschieben, so teilt er dieses der zu auditierenden Institution schriftlich mit. Folgt die Institution der Entscheidung des Auditteamleiters, wird die Fortführung des Audits an einem späteren Zeitpunkt fortgesetzt. Ein erneutes Voraudit ist nicht möglich. Die Zertifizierungsstelle des BSI wird über die Verschiebung des Audits schriftlich informiert.

6 Überwachungsaudits

Ein erteiltes Zertifikat ist mit jährlichen Überwachungsaudits verbunden, das von einem beim BSI zertifizierten Auditteamleiter für ISO 27001-Zertifizierungen auf der Basis von IT-Grundschutz durchgeführt werden muss.

Ein Überwachungsaudit dient der Überwachung der für das Zertifikat nachgewiesenen Informationssicherheit im laufenden Betrieb des Informationsverbundes und hat einen deutlich geringeren Umfang als das Zertifizierungsaudit. Das Überwachungsaudit soll nachweisen, dass das ISMS aktiv ist und weiterentwickelt wird.

Der Auditbericht zu einem Überwachungsaudit muss vom Auditteamleiter erstellt und bei der Prüfbegleitung des BSI vorgelegt werden. Nur im Falle der Einhaltung der Anforderungen gemäß der Standard- oder Kern-Absicherung des BSI-Standards 200-2 und des IT-Grundschutz-Kompendiums bleibt das erteilte Zertifikat gültig. Es erfolgt keine Neuausstellung der Zertifikatsurkunde oder des Zertifizierungsreports.

Ein Überwachungsaudit erfolgt analog zur Vorgehensweise, die in Kapitel 4 beschrieben ist, jedoch mit folgenden Einschränkungen:

- Ein Voraudit ist nicht möglich.
- Es wird der „Muster-Auditbericht im Rahmen der Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz“ gemäß den gültigen Prüfgrundlagen verwendet, der auch bei Zertifizierungsaudits/Rezertifizierungsaudits verwendet wird, es sind jedoch nur die jeweils relevanten Kapitel auszufüllen.
- Für das Überwachungsaudit ist von der Institution eine Zusammenstellung der wesentlichen Änderungen seit dem Audit bereitzustellen. Zusätzlich erfolgt eine Fortschreibung der von der Institution erstellten Liste der Referenzdokumente. Aufgrund dieser Zusammenstellung verschafft sich der Auditteamleiter einen Überblick über die Änderungen im Informationsverbund im Vergleich zum vorherigen Audit. Die Referenzdokumente sind keiner vollumfänglichen Prüfung zu unterziehen, es sind nur geänderte Dokumente zu prüfen. Die Kapitel 3.2 bis 3.8 des Muster-Auditberichts sind entsprechend nicht vollumfänglich zu bearbeiteten. Die Stichprobendokumentation der Strukturanalyse (Kapitel 3.3.8. im Muster-Auditbericht) entfällt entsprechend bzw. ist nur auf die geänderten Dokumente anzuwenden.
- Der Bausteins ISMS.1 wird vollständig auditiert, Schwerpunkt wird dabei auf die Aspekte Aufrechterhaltung der Informationssicherheit und Management-Berichte zur Informationssicherheit gelegt.
- Stellt der Auditteamleiter bei seiner Prüfung gravierende Änderungen am Informationsverbund fest und ist die Institution ihrer Anzeigepflicht gegenüber dem BSI nicht nachgekommen, informiert der Auditteamleiter die Zertifizierungsstelle des BSI hierüber. Die Zertifizierungsstelle des BSI entscheidet über das weitere Vorgehen und behält sich in diesem Falle vor, das Zertifikat zurückzuziehen.

Durch das Überwachungsaudit soll sichergestellt werden,

- dass das Managementsystem für Informationssicherheit weiterhin wirksam und angemessen ist,
- dass Sicherheitsrevisionen durchgeführt und bei erkannten Mängeln Korrekturmaßnahmen ergriffen wurden
- dass die Leitungsebene regelmäßig über den Stand der Informationssicherheit informiert wurde und diese bewertet hat,

- dass die seit der vorhergehenden Auditierung unveränderten Komponenten des Informationsverbundes weiterhin die Anforderungen gemäß dem BSI-Standard 200-2 und dem IT-Grundschutz-Kompendium erfüllen,
- dass neue Bausteine, die im Rahmen der regelmäßigen Aktualisierung des IT-Grundschutz-Kompendiums hinzugekommen sind, in der Modellierung des Informationsverbundes korrekt berücksichtigt sind,
- dass neue oder aktualisierte Anforderungen des IT-Grundschutz-Kompendiums im vorliegenden Informationsverbund angemessen umgesetzt sind,
- dass durch den Wegfall von Komponenten seit der vorhergehenden Auditierung die Informationssicherheit des Informationsverbundes nicht beeinträchtigt wird,
- dass die Informationssicherheit des Informationsverbundes durch Veränderungen in übergeordneten Aspekten, beispielsweise Änderungen der Organisationsstruktur, nicht beeinträchtigt wird.

7 Re-Zertifizierungsaudit

Eine Re-Zertifizierung setzt einen erneuten Antrag voraus.

Mit der Re-Zertifizierung wird der auditierten Institution bescheinigt, dass die Voraussetzungen für die Erfüllung einer ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz weiterhin vorliegen.

Die Auditaktivitäten unterscheiden sich grundsätzlich nicht von denen eines Erst-Zertifizierungsaudits, von daher erfolgt ein Re-Zertifizierungsaudit analog zur Vorgehensweise, die in Kapitel 4 beschrieben ist, jedoch mit den folgenden Einschränkungen:

- Ein Voraudit ist nicht möglich.
- Bei der Auswahl von Stichproben sind redundante Prüfungen zu den vorhergehenden Audits nur in begründeten und mit der Zertifizierungsstelle des BSI abgestimmten Ausnahmefällen zulässig.