|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Audits und Revisionen"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300024 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Audits und Revisionen" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc80519984)

[Dokumentenhistorie 3](#_Toc80519985)

[Inhaltsverzeichnis 4](#_Toc80519986)

[Allgemeine Festlegungen 6](#_Toc80519987)

[Ziel / Zweck 6](#_Toc80519988)

[Geltungsbereich 6](#_Toc80519989)

[Zuständigkeiten 6](#_Toc80519990)

[Genehmigungs- und Änderungsverfahren 7](#_Toc80519991)

[Aufbau des Dokuments 7](#_Toc80519992)

[Sicherheitsrichtlinie „Audits und Revisionen" 8](#_Toc80519993)

[Basismaßnahmen 8](#_Toc80519994)

[Definition von Verantwortlichkeiten (DER.3.1.A1) 8](#_Toc80519995)

[Vorbereitung eines Audits oder einer Revision (DER.3.1.A2) 8](#_Toc80519996)

[Durchführung eines Audits (DER.3.1.A3) 8](#_Toc80519997)

[Durchführung einer Revision (DER.3.1.A4) 8](#_Toc80519998)

[Standardmaßnahmen 8](#_Toc80519999)

[Integration in den Informationssicherheitsprozess (DER.3.1.A5) 9](#_Toc80520000)

[Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas (DER.3.1.A6) 9](#_Toc80520001)

[Erstellung eines Auditprogramms (DER.3.1.A7) 9](#_Toc80520002)

[Erstellung einer Revisionsliste (DER.3.1.A8) 9](#_Toc80520003)

[Auswahl eines geeigneten Audit- oder Revisionsteams (DER.3.1.A9) 9](#_Toc80520004)

[Erstellung eines Audit- oder Revisionsplans (DER.3.1.A10) 9](#_Toc80520005)

[Kommunikation und Verhalten während der Prüfungen (DER.3.1.A11) 10](#_Toc80520006)

[Durchführung eines Auftaktgesprächs (DER.3.1.A12) 10](#_Toc80520007)

[Sichtung und Prüfung der Dokumente (DER.3.1.A13) 10](#_Toc80520008)

[Auswahl von Stichproben (DER.3.1.A14) 10](#_Toc80520009)

[Auswahl von geeigneten Prüfmethoden (DER.3.1.A15) 10](#_Toc80520010)

[Ablaufplan der Vor-Ort-Prüfung (DER.3.1.A16) 10](#_Toc80520011)

[Durchführung der Vor-Ort-Prüfung (DER.3.1.A17) 11](#_Toc80520012)

[Durchführung von Interviews (DER.3.1.A18) 11](#_Toc80520013)

[Überprüfung des Risikobehandlungsplans (DER.3.1.A19) 11](#_Toc80520014)

[Abschlussbesprechung (DER.3.1.A20) 11](#_Toc80520015)

[Auswertung der Prüfungen (DER.3.1.A21) 11](#_Toc80520016)

[Erstellung eines Auditberichts (DER.3.1.A22) 11](#_Toc80520017)

[Dokumentation der Revisionsergebnisse (DER.3.1.A23) 12](#_Toc80520018)

[Abschluss des Audits oder der Revision (DER.3.1.A24) 12](#_Toc80520019)

[Nachbereitung und Einleitung vom Follow-up (DER.3.1.A25) 12](#_Toc80520020)

[Überwachen und Anpassen des Auditprogramms (DER.3.1.A26) 12](#_Toc80520021)

[Aufbewahrung und Archivierung von Unterlagen zu Audits und Revisionen (DER.3.1.A27) 13](#_Toc80520022)

[Maßnahmen bei erhöhtem Schutzbedarf 13](#_Toc80520023)

[Sicherheitsüberprüfung der Auditoren (DER.3.1.A28 - CI) 13](#_Toc80520024)

# Allgemeine Festlegungen

## Ziel / Zweck

Audits und Revisionen sind grundlegend für jedes erfolgreiche Managementsystem für Informationssicherheit (ISMS). Nur wenn etablierte Sicherheitsmaßnahmen und -prozesse regelmäßig daraufhin überprüft werden, ob diese noch wirksam, vollständig, angemessen und aktuell sind, lässt sich der Gesamtzustand der Informationssicherheit der <Institution> beurteilen. Audits und Revisionen sind somit ein Werkzeug, um ein angemessenes Sicherheitsniveau festzustellen, zu erreichen und aufrechtzuerhalten. Durch Audits und Revisionen ist es möglich, Sicherheitsmängel und Fehlentwicklungen zu erkennen und entsprechende Gegenmaßnahmen zu ergreifen.

Als Audit wird eine systematische, unabhängige Prüfung von Aktivitäten und deren Ergebnissen bezeichnet. Dabei wird geprüft, ob definierte Anforderungen wie Normen, Standards oder Richtlinien eingehalten werden. In einer Revision wird untersucht, ob Dokumente, Zustände, Gegenstände oder Vorgehensweisen korrekt, wirksam und angemessen sind. Im Gegensatz zum Audit muss die Revision nicht unbedingt unabhängig erfolgen. Zudem kann die Revision im Sinne einer Wartung auch bereits die Nachbesserung umfassen.

Diese Sicherheitsrichtlinie definiert Anforderungen an Audits und Revisionen mit dem Ziel, die Informationssicherheit in der <Institution> zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und Sicherheitsmaßnahmen und -prozesse zu optimieren. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines DER.3.1 "Audits und Revisionen" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Audits und Revisionen“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Audits und Revisionen"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Definition von Verantwortlichkeiten (DER.3.1.A1)

In der <Institution> werden Mitarbeitende als Verantwortliche für die Planung und Initiierung von Audits und Revision benannt, bei denen zukünftige Interessenkonflikte aufgrund einzelner Rollen vermieden werden. Die Verantwortlichen für Audits und Revisionen überwachen, dass die erhobenen und abgestimmten Ergebnisse durchgeführter Audits und Revisionen entsprechend ihrer Priorität bearbeitet werden.

### Vorbereitung eines Audits oder einer Revision (DER.3.1.A2)

Vor einem Audit oder einer Revision werden Prüfgegenstände und Prüfungsziele festgelegt sowie die betroffenen Ansprechpartner unterrichtet. Abhängig vom Untersuchungsgegenstand wird das betroffene Department über das geplante Audit oder die geplante Revision informiert.

### Durchführung eines Audits (DER.3.1.A3)

Bei der Durchführung eines Audits wird geprüft, ob die Anforderungen aus Richtlinien, Normen, Standards oder weiteren regulatorischen und rechtlichen Vorgaben erfüllt sind. Die Anforderungen sind in der <Institution> bekannt. Ein Audit beinhaltet immer eine Dokumentenprüfung sowie eine Vor-Ort-Prüfung. Beim Vor-Ort-Audit wird sichergestellt, dass die Auditoren niemals selbst aktiv in IT-Systeme eingreifen und auch keine Handlungsanweisungen zu Änderungen am Prüfgegenstand erteilen.

Sämtliche Auditergebnisse werden schriftlich dokumentiert und in einem Auditbericht zusammengefasst. Der Auditbericht wird zeitnah dem verantwortlichen Ansprechpartner innerhalb der <Institution> übermittelt.

### Durchführung einer Revision (DER.3.1.A4)

Bei der Durchführung einer Revision wird geprüft, ob die Anforderungen vollständig, korrekt, angemessen und aktuell umgesetzt sind. Festgestellte Abweichungen werden (sofern möglich) sofort korrigiert. Die jeweiligen Revisionen werden mit einer Änderungsverfolgung dokumentiert.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Integration in den Informationssicherheitsprozess (DER.3.1.A5)

Regelmäßige Audits und Revisionen sind ein fester Bestandteil des Sicherheitsprozesses und werden durch diesen initiiert. Es wird sichergestellt, dass die Ergebnisse der Audits und Revisionen in das ISMS zurückfließen und zu dessen Verbesserung beitragen. Darüber hinaus werden für die durchgeführten Audits und Revisionen, die Ergebnisse sowie die Aktivitäten zur Mängelbeseitigung und Qualitätsverbesserung in den regelmäßigen Bericht des <Informationssicherheitsbeauftragter> an die Geschäftsführung aufgenommen.

### Definition der Prüfungsgrundlage und eines einheitlichen Bewertungsschemas (DER.3.1.A6)

Es sind eine einheitliche Prüfgrundlage für Audits und ein einheitliches Bewertungsschema für die Bewertung der Umsetzung von Anforderungen festgelegt und dokumentiert.

### Erstellung eines Auditprogramms (DER.3.1.A7)

Es wird ein Auditprogramm für mehrere Jahre aufgestellt, das alle durchzuführenden Audits und Revisionen erfasst. Für das Auditprogramm sind Ziele definiert, die sich insbesondere aus den Zielen der <Institution> sowie den Informationssicherheitszielen ableiten. Für unvorhergesehene Ereignisse werden Reserven in der jährlichen Ressourcenplanung vorgesehen. Das Auditprogramm unterliegt einem eigenen kontinuierlichen Verbesserungsprozess.

### Erstellung einer Revisionsliste (DER.3.1.A8)

Es sollten eine oder mehrere Revisionslisten gepflegt werden, die den aktuellen Stand der Revisionsobjekte sowie die geplanten Revisionen dokumentieren.

### Auswahl eines geeigneten Audit- oder Revisionsteams (DER.3.1.A9)

Es wird für jedes Audit beziehungsweise für jede Revision ein geeignetes Team zusammengestellt. Dabei wird ein leitender Auditor (Auditteamleiter) bzw. leitender Revisor benannt, der die Gesamtverantwortung für die Durchführung der Audits beziehungsweise der Revisionen trägt.

Die Größe des Audit- bzw. Revisionsteams entspricht hierbei immer dem Prüfbereich. Es werden zusätzlich Kompetenzanforderungen der Prüfthemen sowie die Größe und örtliche Verteilung des Prüfbereichs berücksichtigt. Die Mitglieder des Audit- bzw. Revisionsteams werden nach angemessener Qualifikation ausgewählt. Die Neutralität des Auditteams und die Unabhängigkeit der Revisoren werden sichergestellt. Sofern externe Dienstleister als Auditoren oder Revisoren eingesetzt werden, werden diese auf ihre Unabhängigkeit überprüft und zur Verschwiegenheit verpflichtet. Im Falle, dass der Auftraggeber das Informationssicherheitsmanagementteam ist, muss der Audit-Plan auch mit der Geschäftsführung abgestimmt werden.

### Erstellung eines Audit- oder Revisionsplans (DER.3.1.A10)

Vor einem Audit oder einer größeren Revision erstellt der Auditteamleiter bzw. leitende Revisor einen Audit- bzw. Revisionsplan. Bei Audits ist der Auditplan Teil des abschließenden Auditberichts. Der Auditplan wird während eines gesamten Audits fortgeschrieben und bei Bedarf angepasst. Kleinere Revisionen werden anhand der Revisionsliste geplant. Es werden genügend Ressourcen für das Audit- bzw. Revisionsteam vorgesehen.

### Kommunikation und Verhalten während der Prüfungen (DER.3.1.A11)

Es werden klare Regelungen dafür aufgestellt, wie das Audit- beziehungsweise Revisionsteam und die Mitarbeitenden der <Institution> miteinander Informationen austauschen dürfen. So wird durch geeignete Maßnahmen sichergestellt, dass die bei einem Audit ausgetauschten Informationen auch vertraulich und integer bleiben. Personen, die das Audit begleiten, dürfen die Prüfungen nicht beeinflussen. Zudem werden sie zur Vertraulichkeit verpflichtet.

### Durchführung eines Auftaktgesprächs (DER.3.1.A12)

Es ist ein Auftaktgespräch zwischen dem Auditteam beziehungsweise dem Revisionsteam und den betroffenen Ansprechpartnern durchzuführen. Dabei werden das Audit- beziehungsweise Revisionsverfahren erläutert, die Rahmenbedingungen der Vor-Ort-Prüfung abgestimmt und durch die jeweiligen Verantwortlichen bestätigt.

### Sichtung und Prüfung der Dokumente (DER.3.1.A13)

Die Dokumentenprüfung im Rahmen von Audits erfolgt anhand der im Prüfplan festgelegten Anforderungen. Alle relevanten Dokumente werden daraufhin geprüft, ob sie aktuell, vollständig und nachvollziehbar sind. Die Ergebnisse der Dokumentenprüfung werden dokumentiert und fließen in die Vor-Ort-Prüfung ein, soweit dies sinnvoll ist.

### Auswahl von Stichproben (DER.3.1.A14)

Das Auditteam wählt die Stichproben für die Vor-Ort-Prüfung risikoorientiert aus und begründet dies nachvollziehbar in dokumentierter Form. Wird das Audit auf der Basis von Baustein-Zielobjekten und Maßnahmen durchgeführt, werden diese anhand eines vorher definierten Verfahrens ausgewählt. Bei der Auswahl von Stichproben werden auch die Ergebnisse vorangegangener Audits berücksichtigt.

### Auswahl von geeigneten Prüfmethoden (DER.3.1.A15)

Das Auditteam benutzt für die jeweils zu prüfenden Sachverhalte geeignete Methoden, z. B. Interviews oder Dokumentenprüfungen. Außerdem wird darauf geachtet, dass alle Prüfungen verhältnismäßig sind.

### Ablaufplan der Vor-Ort-Prüfung (DER.3.1.A16)

Gemeinsam mit den Ansprechpartnern erarbeitet das Auditteam den Ablaufplan für die Vor-Ort-Prüfung. Die Ergebnisse werden im Auditplan dokumentiert.

### Durchführung der Vor-Ort-Prüfung (DER.3.1.A17)

Zu Beginn der Vor-Ort-Prüfung führt das Auditteam ein Eröffnungsgespräch mit den Verantwortlichen der betroffenen Institution, des Bereichs oder der Organisationseinheit durch. Danach werden alle im Prüfplan festgelegten Anforderungen mit den vorgesehenen Prüfmethoden überprüft. Weicht eine ausgewählte Stichprobe vom dokumentierten Status ab, wird die Stichprobe bedarfsorientiert erweitert, bis der Sachverhalt geklärt ist. Nach der Prüfung führt das Auditteam ein Abschlussgespräch, in dem kurz die Ergebnisse ohne Bewertung sowie die weitere Vorgehensweise dargestellt werden. Das Gespräch wird protokolliert.

### Durchführung von Interviews (DER.3.1.A18)

Die Interviews erfolgen strukturiert. Fragen werden knapp, präzise und leicht verständlich formuliert. Zudem werden möglichst geeignete Fragetechniken eingesetzt.

### Überprüfung des Risikobehandlungsplans (DER.3.1.A19)

Das Auditteam prüft, ob die verbleibenden Restrisiken für den Informationsverbund angemessen und tragbar sind. Außerdem wird geprüft, ob sie verbindlich durch die Geschäftsführung getragen werden. Maßnahmen, die grundlegend zur Informationssicherheit der gesamten <Institution> beitragen, fließen nicht in die Risikoübernahme ein.

Der Auditor verifiziert stichprobenartig, ob beziehungsweise wie weit die im Risikobehandlungsplan festgelegten Maßnahmen umgesetzt sind.

### Abschlussbesprechung (DER.3.1.A20)

Das Auditteam führt mit den jeweiligen Verantwortlichen der auditierten Institution, des Bereichs oder der Organisationseinheit eine Abschlussbesprechung durch. Darin werden die vorläufigen Auditergebnisse dargelegt und die weiteren Tätigkeiten vorgestellt.

### Auswertung der Prüfungen (DER.3.1.A21)

Nach der Vor-Ort-Prüfung werden die erhobenen Informationen weiter konsolidiert und ausgewertet. Nachdem die eventuell nachgeforderten Dokumentationen und zusätzlichen Informationen ausgewertet wurden, sind die geprüften Maßnahmen endgültig zu bewerten. Um die nachgeforderten Dokumentationen bereitzustellen, wird ein ausreichendes Zeitfenster gewährt. Dokumente, die bis zum vereinbarten Enddatum nicht eingegangen sind, werden als nicht existent gewertet.

### Erstellung eines Auditberichts (DER.3.1.A22)

Das Auditteam überführt die gewonnenen Ergebnisse in einen nachvollziehbar dokumentierten Auditbericht. Die Ergebnisse des Audits werden den Verantwortlichen in einer Präsentation erläutert.

Die geprüfte Institution, der Bereich oder die Organisationseinheit stellt sicher, dass alle betroffenen Stellen innerhalb einer angemessenen Frist die für sie wichtigen und notwendigen Passagen des Auditberichts erhalten.

### Dokumentation der Revisionsergebnisse (DER.3.1.A23)

Die Revisionsergebnisse werden einheitlich dokumentiert.

### Abschluss des Audits oder der Revision (DER.3.1.A24)

Nach dem Audit beziehungsweise der Revision sind alle relevanten Dokumente, Datenträger und IT-Systeme zurückzugeben oder zu vernichten. Wie vorzugehen ist, ist mit den Zielobjektverantwortlichen abzustimmen. Aufbewahrungspflichten aus gesetzlichen oder anderen verbindlichen Anforderungen sind hierbei entsprechend zu berücksichtigen. Der <Informationssicherheitsbeauftragter> veranlasst nach Abschluss des Audits oder der Revision die Deaktivierung oder Löschung aller für das Audit- oder Revisionsteam genehmigten Zugriffe.

Mit den Auditoren beziehungsweise Revisoren wird vereinbart,

* Wie mit den Ergebnissen umzugehen ist.
* Dass die Auditergebnisse nicht ohne Genehmigung der geprüften Institution, des Bereichs oder der Organisationseinheit an andere Institutionen, Bereiche oder Organisationseinheiten weitergeleitet werden dürfen.

### Nachbereitung und Einleitung vom Follow-up (DER.3.1.A25)

Die im Auditbericht oder bei einer Revision festgestellten Abweichungen oder Mängel werden in einer angemessenen Zeit abgestellt. Zu diesem Zweck erfolgt eine Priorisierung zur Behebung der Abweichungen und Mängel nach Umsetzbarkeit, verfügbaren Ressourcen und Wichtigkeit. Damit sich der Umsetzungsstatus leicht nachvollziehen lässt, sind die durchzuführenden Korrekturmaßnahmen inklusive Zeitpunkt und Zuständigkeiten zu dokumentieren. Auch abgeschlossene Korrekturmaßnahmen sind zu dokumentieren. Dafür besteht im ISMS bereits ein etabliertes zu nutzenden Verfahren. Bei schwerwiegenden Abweichungen oder Mängel überprüft das Audit- bzw. Revisionsteam, ob die Korrekturmaßnahmen durchgeführt wurden.

Für die Umsetzung und die terminliche Verfolgung ist, abhängig von den festgestellten Abweichungen oder Mängel das Informationssicherheitsmanagementteam oder die jeweils zuständige Führungskraft verantwortlich.

### Überwachen und Anpassen des Auditprogramms (DER.3.1.A26)

Das Auditprogramm wird kontinuierlich überwacht und angepasst, sodass Termine, Auditziele, Auditinhalte und die Auditqualität eingehalten werden. Mithilfe der bestehenden Anforderungen an das Auditprogramm und mit den Ergebnissen der durchgeführten Audits wird überprüft, ob das Auditprogramm angemessen ist. Bei Abweichungen von der erforderlichen Angemessenheit wird das Auditprogramm angepasst.

### Aufbewahrung und Archivierung von Unterlagen zu Audits und Revisionen (DER.3.1.A27)

Auditprogramme sowie Unterlagen zu Audits und Revisionen werden entsprechend den gesetzlichen und weiteren regulatorischen Anforderungen nachvollziehbar und revisionssicher abgelegt und aufbewahrt. Dabei wird sichergestellt, dass lediglich berechtigte Personen auf Auditprogramme und Unterlagen (insbesondere Auditberichte) zugreifen können. Nach Ablauf der Archivierungsfristen werden die Auditprogramme und Unterlagen sicher vernichtet.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Sicherheitsüberprüfung der Auditoren (DER.3.1.A28 - CI)

Sobald die Auditoren auf besonders schützenswerte Informationen zugreifen müssen, werden von der <Institution> im Rahmen der Auditvorbereitung Nachweise über ihre Integrität und Reputation eingefordert.