CISIS12

(ISIS12 V3.0)

Compliance und Informationssicherheit in zwölf 12 Schritten

Auditschema

I Dokumentinformationen

Dokument

Beschreibung	CISIS12-Auditschema
Version:	1.1
Version vom:	01.06.2021
Freigabe durch:	Sandra Wiesbeck
Status:	Final, Öffentlich

Zielgruppe

Zielgruppe	IT-Sicherheitscluster, CISIS12-Nutzer, CISIS12-Berater, Hochschulen
Zugehörige Dokumentationen	CISIS12-Norm, CISIS12 Baustein- und Maßnahmenkatalog CISIS12 Handbuch

Entwicklerteam

Frank Müller	Entwurf und Inhalt
Frank Moses	Lektorat

Änderungsnachweis

Version	Änderung	durch	gültig ab
1.0	CISIS12 Veröffentlichung	IT-Sicherheitscluster	01.06.2021

II Inhaltsverzeichnis

III Abbildungsverzeichnis

1 Einleitung

Im vorliegenden Auditierungsschema werden zur Bestätigung der Konformität des CISIS12-Managementsystems die Anforderungen an das Audit das Prüfungsteam beschrieben.
Im Auditierungsschema werden die Voraussetzungen und die grundsätzliche Vorgehensweise für eine CISIS12-Zertifizierung beschrieben. Dadurch haben die geprüften Organisationen die Möglichkeit, ihre Maßnahmen und Ergebnisse bei der Umsetzung der CISIS12-Norm innerhalb und außerhalb ihrer Organisation nachzuweisen.
Mit der Erteilung des CISIS12-Zertifikats wird bestätigt, dass die Organisation nachfolgenden Anforderungen genügt:

- Informationssicherheit wird in einem definierten Prozess gelebt,
- ein funktionierendes Management der Informationssicherheit ist vorhanden und
- ein definiertes Sicherheitsniveau ist zum Auditzeitpunkt erreicht.

Prüfgrundlagen des Verfahrens sind:

- CISIS12-Norm
- CISIS12-Handbuch
- CISIS12-Katalog

2 Zielgruppe

Dieses Dokument richtet sich vor allem an Auditoren und Auditteams, die ein unabhängige Prüfung in einer Organisation durchführen, um die Konformität des Managementsystems für Informationssicherheit gemäß der CISIS12-Norm zu bestätigen. Informationssicherheitsbeauftragte (ISB) und CISIS12-Berater können sich einen Überblick darüber verschaffen, welche Prüfungsanforderungen durch die Auditoren gestellt werden und welche Referenzen notwendig sind.

3 Überblick über den Zertifizierungsprozess

3.1 Prozessablauf

Der Prozess startet mit der Antragstellung zu einem Zertifizierungsaudit bei einem anerkannten Zertifizierungsdienstleister. Das Audit erfolgt gemäß den Anforderungen zur Auditierung Managementsystemen auf Basis der ISO EN 19011. Damit wird sichergestellt, dass die Audits effektiv und systematisch durchgeführt werden. Die ISO EN 19011 enthält unter anderem Auditprinzipien, die Steuerung eines Auditprogramms, Die Durchführung von Audits sowie die Beurteilung der Kompetenz derer, die in den Auditprozess einbezogen sind. Sie wurde an die High-Level-Struktur von Management-Normen angepasst, verbunden mit einer Harmonisierung der Begriffe.

Abbildung 1: Zertifizierungsprozess

Auf der Grundlage der Dokumenten- und Umsetzungsprüfung bewertet das Auditteam die Konformität des CISIS12-Managementsystems. Nachbesserungen sind erforderlich, wenn bestimmte

Anforderungen aus den Prüfgrundlagen zwar umgesetzt worden sind, die Umsetzung und Wirksamkeit jedoch Mängel oder Lücken aufweist. Diese Nachbesserungen führen nicht zu einem Nicht-Bestehen eines Zertifizierungsaudits. Allerdings müssen die Nachbesserungen bis zu den vereinbarten Terminen abgestellt werden.

3.2 Arten der Auditierung

Ein Erst-Zertifizierungsaudit betrachtet den gesamten Informationssicherheitsprozess innerhalb des Geltungsbereichs sowie die Überprüfung der Umsetzung der Anforderungen im Rahmen einer Stichprobenprüfung auf der Basis von Bausteinen aus dem CISIS12-Katalog. Im Rahmen eines Voraudits kann ein Auditteam sich einen Überblick über den Informationssicherheitsprozess der Organisation verschaffen.

Die Aufrechterhaltung der Informationssicherheit wird mit einem jährlich durchzuführenden Überwachungsaudit geprüft.

Ein Zertifikat kann durch eine Re-Zertifizierung um drei Jahre verlängert werden. Das Auditteam 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 Geltungsbereiches seit dem letzten Audit ergeben haben.

Jedes Audit umfasst zwei Phasen: eine Dokumentenprüfung und eine Umsetzungsprüfung. Die Ergebnisse werden immer in einem Auditbericht zusammengefasst.

3.3 Auditvoraussetzungen

Voraussetzung für ein Audit ist die entsprechende Antragstellung bei einem für die CISIS12-Norm zugelassenen Zertifizierungsgesellschaft. Auf Basis des Antrags wird der zu berücksichtigende zeitliche Aufwand für das Audit ermittelt und dokumentiert. Die wesentliche Bemessungsgrundlage für den zeitlichen Aufwand ergibt sich in erster Linie aus der jeweiligen Organisationsgröße und dabei sind bis zu drei Standorten inkludiert. Bei einer größeren Anzahl von Standorten sind die Audittage mit den Zertifizierungsgesellschaften zu klären.

Bezeichnung	Beschäftigte	Erstaudit	Überwachungsaudit
Kleine Organisationen	1-25	1,5 Audittage[1]	1 Audittag
Mittlere Organisationen	25-150	2 Audittage	1 Audittag
Größere Organisationen	150-250	3 Audittage	1,5 Audittage
Große Organisationen	ab 250	4 Audittage	2 Audittage

Abbildung 2: Auditaufwand in Tagen

Die Einführung eines Informationssicherheitsmanagementsystems auf Basis CISIS12 muss abgeschlossen sein. Das bedeutet, dass alle zwölf Schritte einmal durchlaufen sind, bevor eine Auditierung erfolgen kann.

[1] davon 0,5 Tage Dokumentenprüfung vorab, dann 1 Tag vor Ort

Für das Audit sind die jeweils aktuellen Versionen der Prüfgrundlagen zu verwenden, Übergangsfristen sind dabei entsprechend zu beachten. Vor Beginn des Audits ist das Auditteam verpflichtet zu prüfen, ob die jeweils aktuell gültigen Versionen verwendet wurden.

Die Referenzdokumente:

1. Informationssicherheitsleitlinie
2. Schulungs- und Sensibilisierungskonzept
3. Dokumente bzgl. der Rollenbenennung der Informationssicherheitsteam
4. Betriebshandbuch
5. Netzplan
6. Notfallhandbuch
7. IT-Servicemanagementhandbuch
8. Prozesssteckbriefe
9. Schutzbedarfsfeststellung
10. Sicherheitskonzept
11. Umsetzungsplan
12. Managementbericht
13. Revision mit internem Auditbericht und ggf. Zertifizierungsauditbericht
14. Richtlinie zum Risikomanagement und
15. Risikobehandlungsplan

bilden die Grundlage für das Audit. Sie sind wesentlich für den Informationssicherheitsprozess nach CISIS12. Das Auditteam kann darüber hinaus während des Audits weitere Dokumente und Aufzeichnungen einsehen.

Die Referenzdokumente werden, wie andere wesentliche Dokumente, Bestandteil des Auditberichts.

4 Auditprinzipien

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 Zertifizierungsgesellschaft als auch die auditierte Organisation müssen dem Auditteam bei ihrem Vorgehen vertrauen können.

- **Fachkompetenz**: Das Auditteam übernimmt nur solche Aufgaben, für die es das erforderliche Wissen, Können und die entsprechende Erfahrung hat, und setzt diese/s bei der Durchführung seiner Arbeit ein. Es verbessert kontinuierlich seine Fachkenntnisse sowie die Effektivität und Qualität seiner 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**: Das Auditteam hat die Pflicht, sowohl der zu auditierenden Organisation als auch der Zertifizierungsgesellschaft 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 das Auditteam zu seinen Schlussfolgerungen kommt.

- **Objektivität und Sorgfalt**: Das Auditteam 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.

5 Der Auditprozess

Jedes Audit setzt sich grundsätzlich aus zwei einander ergänzenden Phasen zusammen. Die eine Phase umfasst zunächst die Prüfung der vom Antragsteller vorgelegten Dokumente. Die andere Phase bewertet die Umsetzung und Wirksamkeit der Maßnahmen, die sich aus den vorgelegten Dokumenten ergeben. Hierbei wird innerhalb des festgelegten Geltungsbereichs die praktische Umsetzung der in den Dokumenten dokumentierten Sicherheitsmaßnahmen auf ihre Vollständigkeit, Korrektheit und Wirksamkeit hin überprüft.

Für jedes Audit ist vom Auditteam ein Auditbericht zu erstellen, der alle Auditergebnisse enthält. Dabei ist darauf zu achten, dass die entsprechenden Kontrollfragen aller zwölf Schritte beantwortet werden müssen und weitere Feststellungen des Auditteams aus Beobachtungen, Interviews, weiteren Dokumenten und Nachweisen angemessen beachtet werden.

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

Der Auditbericht muss auf der Basis des Musters für Auditberichte in der jeweils gültigen Version erstellt werden. (Siehe Anhang A – Prüfschema Excel Tabelle)

5.1 Erstellung eines Auditplans

Zur Vorbereitung auf die Vor-Ort-Prüfung muss das Auditteam einen Auditplan erstellen. Das bedeutet, dass das Auditteam die erforderlichen Themen benennt, damit die zu auditierende Organisation die Interviewpartner rechtzeitig benennen kann.

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

- Bei der Erst-/Re-Zertifizierung werden mindestens 6 Bausteine auditiert, darunter zwingend die Bausteine B2.010 Gesamtverantwortung und B5.050 Serverraum.
- Bei den beiden Überwachungsaudits werden jeweils zwingend der Baustein B2.060 Aufbau einer Sicherheitsorganisation 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.
- Das Auditteam kann die Stichprobe erweitern.
- Der Baustein B2.300 Outsourcing (Nutzung) wird zwingend auditiert, sofern Outsourcing-Dienstleister im Geltungsbereich eingebunden sind.

Welche Zielobjekte konkret auditiert werden, sollte der zu auditierenden Organisation nach Möglichkeit vorab nicht mitgeteilt werden.

Sollten sich während der Zertifikatslaufzeit wesentliche Änderungen ergeben (z. B. Änderung im Geltungsbereich, neue bekannte Risikoklasse, neue Risikobehandlungen) sollten diese Änderungen vorranging in einem Überwachungsaudit betrachtet werden.

5.2 Phase Dokumentenprüfung

Die erste Phase dient dazu, dass das Auditteam ein ausreichendes Verständnis für den Geltungsbereich erlangt und feststellt, ob die Konzeption der Informationssicherheitsstruktur des Geltungsbereiches gemäß den Vorgaben und Maßnahmen der Prüfgrundlagen schlüssig und sinnvoll ist. Das Auditteam prüft dabei insbesondere, ob die Zertifizierungsfähigkeit des Geltungsbereiches grundsätzlich gegeben ist.

Damit das Auditteam ein ausreichendes Verständnis des Geltungsbereiches gewinnen kann, kann es sinnvoll sein, einen Teil der Dokumentenprüfung bereits vorab durchzuführen. In einigen Fällen ist die Einsichtnahme von Dokumenten auch aus Vertraulichkeitsgründen nur vor Ort möglich.

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

5.3 Phase Umsetzungsprüfung

Es ist wichtig, dass innerhalb des Geltungsbereiches das Managementsystem für Informationssicherheit 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. Das Auditteam prüft auf Basis der vorgelegten Dokumente die Umsetzung durch Interviews und Beobachtungen in der zu auditierenden Organisation, um sich von der Effektivität und der Effizienz des ISMS zu überzeugen.

Bei der Umsetzungsprüfung wird für jeden gewählten Baustein überprüft, ob der im CISIS12+-Verfahren festgestellte und dokumentierte Umsetzungsstatus durch die in diesem Baustein enthaltenen Anforderungen angemessen umsetzt wurde.

Die Umsetzungsprüfung beinhaltet auch Besichtigungen (bspw. Baustein B5.050 Serverraum als verpflichtender Baustein) oder auch Vorführungen (bspw. Demonstration der CMDB in DocuSnap). Über Interviews soll sich das Audit-Team davon überzeugen, dass sich die Regelungen zur Informationssicherheit der Organisation den Mitarbeitern bekannt sind und gelebt werden.

Zusätzlich wird die Umsetzung von ausgewählten Maßnahmen aus dem „Schritt 6 – Risikomanagement“ überprüft.

Zudem muss sichergestellt sein, dass die in „Schritt 7 – IT-Struktur analysieren“ aufgeführten Eigenschaften der IT-Assets 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 das Audit-Team nachvollziehbar dokumentiert sein.

5.4 Behandlung von Auditergebnissen

Sowohl in der Phase der Dokumentenprüfung als auch in der Phase der Umsetzungsprüfung kann es zu Feststellungen kommen, die nicht der CISIS12 - Norm entsprechen (Abweichungen). Diese Feststellungen führen zu verschiedenen Arten der Behandlung.

- Empfehlungen:
  Empfehlungen oder Verbesserungsmöglichkeiten[2] gefährden nicht die Erteilung oder die Aufrechterhaltung des Zertifikats. Es sind Feststellungen, wie die Effizienz und Effektivität des ISMS verbessert werden kann. Die Organisation muss sich mit diesen Feststellungen nachweislich spätestens bis zum nächsten Audit beschäftigen, sie aber nicht unbedingt annehmen.

- Nebenabweichungen:
  Eine Nebenabweichung gefährdet nicht die Erteilung oder Aufrechterhaltung des Zertifikats. Mehrere Nebenabweichungen können aber zu einer Hauptabweichung führen. Bei einer Nebenabweichung wird ein Mangel festgestellt, der dazu führt, dass die Anforderungen der CISIS12 - Norm nicht angemessen umsetzt werden, das ISMS aber insgesamt funktioniert. Bei Nebenabweichungen wird der Organisation eine der Abweichung entsprechende Frist zur Behebung gesetzt. Dafür wird durch das Audit-Team ein Maßnahmenplan erstellt. Die Organisation muss diesen Maßnahmenplan akzeptieren und innerhalb der gesetzten Frist umsetzen. Eine Fristverletzung führt automatisch zu einer Hauptabweichung. Nebenabweichungen werden über ein Formular (Anhang B – Nebenabweichung) dokumentiert.

- Hauptabweichung
  Eine Hauptabweichung ermöglicht keine Erteilung oder Aufrechterhaltung des Zertifikats. Bei einer Hauptabweichung wird ein Mangel festgestellt, ohne dessen Behebung nicht sichergestellt werden kann, dass das ISMS effektiv und effizient funktioniert bzw. die Gesamtsicherheit innerhalb des Geltungsbereiches nicht (mehr) gegeben ist. Eine Hauptabweichung beendet den Auditprozess. Nach der Behebung der Hauptabweichung muss der Zertifizierungsprozess erneut gestartet werden.

Empfehlungen und Nebenabweichungen, die bereits während des Audits abgearbeitet werden, sind dennoch in den Auditbericht mit aufzunehmen.

Das Audit-Team bewertet die Ergebnisse über ein Reifegrad-Modell (siehe Anhang A -Prüfschema Exceltabelle).

Das Reifegrad-Modell basiert auf dem CMMI-Modell[3]. CMMI ist ein Prozessmodell, mit dem sich die Qualität von Produkt-Entwicklungsprozessen in Unternehmen beurteilen und verbessern lässt. Das Modell basiert auf 5 Reifegraden. Die Reifegrade orientieren sich an nachfolgender Tabelle:

Reifegrad	**Umsetzung der CISIS12 - Norm**
0	Die Umsetzung ist für die Organisation nicht relevant
1	Es ist keine Umsetzung erfolgt

[2] Verbesserungsmöglichkeiten oder Empfehlungen werden auch auch als OFI (engl. opportunity for improvement) bezeichnet

[3] Das Software Engineering Institute (SEI) der Carnegie Mellon University hat CMMI als Nachfolger des dort ebenfalls entwickelten CMM (Capability Maturity Model) beschrieben (www.sei.cmu.edu/cmmi)

2	Die Umsetzung erfolgt teilweise
3	Die Umsetzung ist erfolgt
4	Die Umsetzung ist regelmäßig und angemessen erfolgt
5	Die Umsetzung ist regelmäßig optimal erfolgt, angemessen und nachgewiesen

Der Reifegrad 1 führt automatisch zu einer Hauptabweichung. Bei den Reifegraden 2 und 3 ist zu prüfen, ob Nebenabweichungen vorliegen. Sollte eine Umsetzung mit dem Reifegrad 4 bewertet werden, sind lediglich Empfehlungen zu geben. Der Reifegrad 5 zeigt einen optimalen Prozess, der alle Anforderungen der Norm ohne Einschränkungen erfüllt.

6 Erstellung des Auditberichts

Das Audit-Team erstellt für das Audit einen Auditbericht, der alle Auditergebnisse enthält. Der Bericht dient den jeweiligen Zertifizierungsstellen als Grundlage für die Erteilung des Zertifikats bzw. für die Rezertifizierung. Im Falle eines Überwachungsaudits dient der Auditbericht als Grundlage für die Aufrechterhaltung des Zertifikats. Im Auditbericht gibt das Audit-Team zu dem Ergebnis des Audits ein Votum ab.

7 Zertifikatserteilung

Die endgültige Zertifikatserteilung erfolgt über eine Zertifizierungsgesellschaft auf Basis des vorgelegten Auditberichts. Nachdem der Auditbericht vom Audit-Team an die Zertifizierungsstelle übermittelt wurde, entscheidet die Zertifizierungsstelle über die Erteilung bzw. Aufrechterhaltung des Zertifikats. Mit der Entscheidung über die Zertifikatserteilung wird der auditierten Organisation auch der Auditbericht übermittelt.

Für den Fall, das ein Maßnahmenplan erstellt werden muss, der Voraussetzung zur Zertifikatserteilung ist, kann die Erteilung des Zertifikats erst erfolgen, wenn die erfolgreiche Umsetzung der Maßnahmen durch das Audit-Team bestätigt wurde. Die Bestätigung kann erst erfolgen, wenn sich das Audit-Team durch entsprechende Vorlage von Dokumenten oder vor Ort überzeugt hat, dass die erforderlichen Maßnahmen wirksam umgesetzt wurden.

8 Überwachungsaudit

Ein erteiltes Zertifikat ist mit jährlichen Überwachungsaudits verbunden.

Ein Überwachungsaudit dient der Überwachung der für das Zertifikat nachgewiesenen Informationssicherheit im laufenden Betrieb des Geltungsbereichs und hat jedoch 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 Audit-Team erstellt und bei der jeweiligen Zertifizierungsstelle vorgelegt werden. Nur im Falle der Einhaltung der Anforderungen gemäß der CISIS12 - bleibt das erteilte Zertifikat gültig. Es erfolgt keine Neuausstellung der Zertifikatsurkunde oder des Zertifizierungsreports.

Für das Überwachungsaudit sind von Organisation eine Zusammenstellung der wesentlichen Änderungen seit dem letzten Audit und der letzte Bericht des internen Audits bereitzustellen. Zusätzlich erfolgt eine Fortschreibung der von der Institution erstellten Liste der Referenzdokumente. Aufgrund dieser Zusammenstellung verschafft sich das Audit-Team einen Überblick über die Änderungen im Geltungsbereich im Vergleich zum vorherigen Audit. Die Referenzdokumente sind keiner vollumfänglichen Prüfung zu unterziehen, es sind nur geänderte Dokumente zu prüfen.

Stellt das Audit-Team bei seiner Prüfung gravierende Änderungen am Geltungsbereich fest und ist die Organisation ihrer Anzeigepflicht gegenüber der Zertifizierungsstelle nicht nachgekommen, informiert das Audit-Team die Zertifizierungsstelle hierüber. Die Zertifizierungsstelle 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 Revisionen/Audits durchgeführt und bei erkannten Mängeln Korrekturmaßnahmen ergriffen wurden
- dass die Organisationsleitung regelmäßig über den Stand der Informationssicherheit informiert wurde und diese bewertet hat,
- dass die seit der vorhergehenden Auditierung unveränderten Komponenten des Geltungsbereichs weiterhin die Anforderungen gemäß der CISIS12 - Norm erfüllen,
- dass neue Bausteine, die im Rahmen der regelmäßigen Aktualisierung des CISIS - Katalogs hinzugekommen sind, im Geltungsbereich korrekt berücksichtigt worden sind,
- dass neue oder aktualisierte Anforderungen der CISIS12 - Norm im Geltungsbereich angemessen umgesetzt sind,
- dass durch den Wegfall von Komponenten seit der vorhergehenden Auditierung die Informationssicherheit des Geltungsbereichs nicht beeinträchtigt wird,
- dass die Informationssicherheit des Geltungsbereichs durch Veränderungen in übergeordneten Aspekten, beispielsweise Änderungen der Organisationsstruktur, nicht beeinträchtigt wird.

9 Re-Zertifizierungsaudit

Eine Re-Zertifizierung setzt einen erneuten Antrag voraus.
Mit der Re-Zertifizierung wird der auditierten Organisation bescheinigt, dass die Voraussetzungen für die Erfüllung einer CISIS12 - Zertifizierung 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 5 beschrieben ist.