CISIS12®-Kriterienkatalog

datenschutz cert GmbH
Version 1.1

datenschutz cert

Inhaltsverzeichnis

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	24.03.2022		Erstellung	Mühlhause
1.1	09.06.2022	Anforderungen an einen Auditreport; Anerkennungen und Akkreditierungen	Präzisierung der Angaben	Mühlhause

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentbesitzer	Version
Final	Matthias Mühlhause	1.1

Anforderungen an CISIS12®

CISIS12® vormals ISIS12 hat sich als Standard für Informationssicherheit für öffentliche Einrichtungen, Verwaltung sowie kleinen und mittleren Unternehmen (KMU's) etabliert. Informationssicherheit ist hierbei mehr als die reine IT: Ganzheitlich werden alle Aspekte zur Informationssicherheit betrachtet, die zum „Funktionieren" eines Unternehmens oder einer Behörde notwendig sind.

Die datenschutz cert GmbH auditiert und zertifiziert CISIS12®-konforme Informationssicherheits-Managementsysteme und erteilt CISISI12-Zertifikate: Diese Zertifikate bescheinigen einer Institution, dass sie ein Informationssicherheits-Managementsystem nach CISIS12® vom IT-Sicherheitscluster e.V. eingeführt und umgesetzt hat.

Die datenschutz cert GmbH ist dazu beim IT-Sicherheitscluster e.V. gemäß CISIS12® anerkannte Zertifizierungsstelle.

Das vorliegende Dokument beschreibt den Auditierungs- und Zertifizierungsprozess und ist ein Extrakt aus dem vollständigen Zertifizierungsschema der datenschutz cert GmbH.

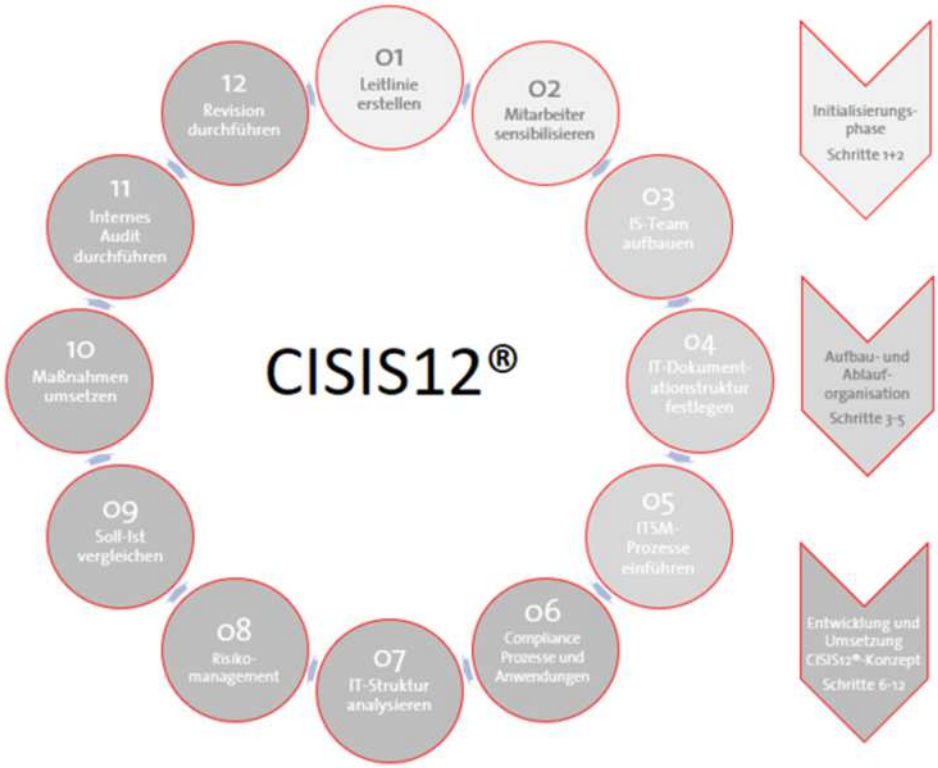
Bremen, den 24.03.2022

Dr. Sönke Maseberg
Geschäftsführer
datenschutz cert GmbH

CISIS12®

Informationssicherheit in 12 Schritten

Der Standard für ein Informationssicherheits-Managementsystem nach CISIS12® sieht 12 Schritte vor, die in drei Phasen – Initialisierungsphase, Beschäftigten Sensibilisierung und Entwicklung und Umsetzung der CISIS12®-Konzeption – eingeteilt sind.



Phase I Initialisierungsphase

In dieser Phase erstellen Sie eine Leitlinie zur Informationssicherheit und sensibilisieren Ihre Mitarbeiter.

Schritt 1 – Leitlinie

Die Leitlinie für Informationssicherheit (ISL) ist das zentrale strategische Dokument der Organisationsleitung bei der Einführung, Etablierung, Umsetzung und kontinuierlichen Verbesserung der Informationssicherheit. Sie gehört zu den ersten wesentlichen Elementen für den Aufbau eines ISMS. Die Leitlinie muss auf die Organisation bezogen sein und die Formulierungen den Gepflogenheiten der Organisation entsprechen.

Schritt 2 – Beschäftigten Sensibilisierung

Die Beschäftigten sind der wesentlichste Erfolgsfaktor und unverzichtbarer Bestandteil bei der Einführung, Etablierung und Umsetzung eines ISMS in einer Organisation. Dabei geht es einerseits um das Verständnis für Maßnahmen im Rahmen der Informationssicherheit, die unter Umständen gewohnte Arbeitsabläufe für die Beschäftigten aufwendiger gestalten. Es geht aber auch darum, den Beschäftigten die Risiken, die aus verschiedensten Angriffen entstehen können, bewusst zu machen und sie auf diese Herausforderungen in ihrem Arbeitsalltag vorzubereiten.

Phase II Aufbau- und Ablauforganisation

Diese Phase dient der Festlegung der Aufbau- und Ablauforganisation.

Schritt 3 – Informationssicherheitsteam

Die erfolgreiche Einführung eines ISMS kann nur gelingen, wenn sich ein Spezialisten Team dauerhaft mit dieser Aufgabe beschäftigt. Dafür müssen von der Organisationsleitung die entsprechenden Rollen und Verantwortlichkeiten für den Aufbau, die Aufrechterhaltung und die kontinuierliche Verbesserung benannt und die dafür erforderlichen Ressourcen bereitgestellt werden. Dabei sollte darauf geachtet werden, dass die Verantwortlichkeiten dieser Rollen klar geregelt sind und nach Möglichkeit eine Funktionstrennung vorgenommen wird.

Schritt 4 – Dokumentation

Die IT-Dokumentation ist die notwendige Basis, um die IT-Services und die Informationssicherheit zu steuern. Eine IT-Dokumentation zeichnet sich durch Vollständigkeit, Übersichtlichkeit, Verständlichkeit, Strukturiertheit, Korrektheit, Nachvollziehbarkeit, Integrität/Authentizität (z.B. Änderungshistorie) und Objektivität aus.

Schritt 5 – IT-Servicemanagement

Das IT-Servicemanagement ist die Gesamtheit aller Maßnahmen und Methoden, die nötig sind, um eine bestmögliche Unterstützung der Geschäftsprozesse durch die IT-Organisation zu erreichen. In Abhängigkeit von der Größe einer Organisation ist auch die Menge der IT-Services zu sehen, die zur Optimierung der jeweiligen Geschäftsziele benötigt werden. Die Geschäftsprozesse der Organisation sind in einem Servicemanagementhandbuch (IT-SMHB) zu dokumentieren.

Phase III Entwicklung und Umsetzung CISIS12®-Konzept

Schritte 6 - 12

Die letzte Phase umfasst schließlich die Entwicklung und Umsetzung des Konzepts

Schritt 6 – Compliance, Prozesse und Anwendungen

Der Begriff „Compliance“ umfasst die Beachtung aller gesetzlichen Regelungen, Richtlinien und weiterer Anforderungen, die für eine Organisation wesentlich sind. Darüber hinaus bedeutet er auch die Schaffung organisatorischer Vorkehrungen durch die Organisation (Governance), um die Einhaltung von gesetzlichen und selbstdefinierten Richtlinien zu gewährleisten.

Schritt 7 – IT-Struktur

Die IT-Struktur stellt die notwendige Basis für die Geschäftsprozesse der Organisation dar. Daher müssen die für diese Prozesse notwendigen IT-Strukturen und Assets identifiziert und klassifiziert werden. Eine aktuelle Übersicht dokumentiert diese IT-Strukturen und Assets einschließlich des zugehörigen Eigentümers (Asset-Owner)

Schritt 8 – Risikomanagement

Der Betrieb von IT-Strukturen, Diensten und Anwendungen beinhaltet Risiken, unabhängig davon, ob man sie selbst betreibt oder im Outsourcing von Partnern betreiben lässt. Zusammen mit der Einhaltung von rechtlichen und vertraglichen Anforderungen an die Organisation, ergibt sich somit die Herausforderung eines Governance-, Risk- und Compliancemanagements.

Schritt 9 – Soll-Ist-Vergleich

Alle Maßnahmen, die als Ergebnis der Analyse von IT-Strukturen, Assets und IT-gestützter Geschäftsprozesse und Zuordnung entsprechender Schutzbedarfe an z.B. IT-Systemen automatisiert mit einem Tool oder mit Hilfe einer Liste entstehen, müssen auf tatsächliche Umsetzung hin ausgewertet werden. Dieser Vergleich kann schon als Teil des Reifegrades der Implementierung eines ISMS verstanden werden.

Schritt 10 – Maßnahmenumsetzung

Die aus dem Soll-Ist-Vergleich umzusetzenden Maßnahmen müssen konsolidiert, priorisiert, budgetiert und terminiert werden. Im Rahmen des Managementreports, der internen Audits oder im Rahmen des Vortragsrechts des Informationssicherheitsbeauftragten muss die Umsetzungsplanung der Maßnahmen zeitnah der Organisationsleitung zur Entscheidung vorgelegt werden.

Schritt 11 – Internes Audit

Der Demingkreis oder PDCA-Zyklus verbindet alle Managementsysteme als ein gleichbleibendes Element. Inhärent mit dieser Anforderung geht einher, dass der kontinuierliche Verbesserungsprozess ermöglicht werden muss.

Schritt 12 – Revision

Die Bedeutung des zwölften Schritts des Managementsystems CISIS12® darf nicht vernachlässigt werden, da es die andauernde und nachhaltige Implementierung sichert. Kontinuität und die Unterstützung der Organisationsleitung und deren steuernde Eingriffe werden über die Revision fortwährend gewährleistet.

Vorteile einer CISIS12®-Zertifizierung

Allein durch das Etablieren eines Informationssicherheits-Managementsystem nach CISIS12® werden die internen Prozesse und Verfahren besser und effizienter. Da ein etabliertes Informationssicherheits-Managementsystem kaum Mehraufwand bedeutet, können durch ein funktionierendes Informationssicherheits-Managementsystem Effizienzgewinne erzielt werden. Steigern lässt sich dies erfahrungsgemäß durch eine unabhängige Begutachtung und Zertifizierung.

Unternehmen, die den Schutz von sensiblen Daten ernst nehmen und selbst auferlegte Sicherheitsstandards umsetzen wollen oder aber auch, um den rechtlichen Anforderungen des Gesetzgebers zu genügen, wird mit einem Informationssicherheits-Managementsystem nach CISIS12® der Einstieg in die Zertifizierung geboten.

Nicht zu unterschätzen sind die positiven Effekte, die Reputation betreffend, um Geschäftspartnern einen verantwortungsvollen Umgang mit Informationen und auch personenbezogenen Daten widerzuspiegeln und nicht zuletzt die Möglichkeit, die Zertifizierung für das Marketing zu nutzen.

Daneben erleichtert die CISIS12®-Zertifizierung einem Unternehmen, sich zu einem späteren Zeitpunkt auf Basis von ISO/IEC 27001 oder IT-Grundschutz zertifizieren zu lassen. CISIS12® ist daher ein Fundament, auf dem die Informationssicherheit eines Unternehmens aufgebaut ist.

Warum datenschutz cert GmbH?

Über 12 Jahre Erfahrung in der Prüfung und Zertifizierung von Informationssicherheit und Datenschutz. Wir sind anerkannte CISIS12®-Zertifizierungsstelle mit lizensierten, qualifizierten und zugelassen CISIS12®-Auditoren. Außerdem sind wir bei der DAkkS als Zertifizierungsstelle für ISO/IEC 27001 akkreditiert, verfügen über BSI-lizenzierte IT-Grundschutz-Auditoren und sind beim BSI anerkannter IT-Sicherheitsdienstleister für Penetrationstests.

Auditierungs- und Zertifizierungsprozess

In diesem Abschnitt wird dargestellt, wie die datenschutz cert GmbH ein Informationssicherheits-Managementsystem nach CISIS12® auditiert und zertifiziert. Abschließend wird der Life-Cycle eines CISIS12®-Zertifikates illustriert.

Dabei wird ein zweistufiges Zertifizierungsverfahren eingesetzt:

- Der bei der datenschutz cert GmbH lizenzierte Auditor prüft die Konformität eines Informationssicherheits-Managementsystem nach CISIS12® und erstellt einen Audit-report.
- Die Zertifizierungsstelle prüft den Auditreport, insbesondere um eine Vergleichbarkeit zwischen den Audits sicherstellen zu können.

Zertifizierung Anfrageformular

Vom Antragssteller ist das von der Zertifizierungsstelle zur Verfügung gestellte Anfrageformular vollständig zu befüllen und zuzusenden. Diese Angaben sind wesentlich für die weitere Bearbeitung inkl. Angebotserstellung und Auditplanung.

Laufzeiten

Jedes Zertifizierungsverfahren besteht ausfolgenden Phasen:

- Erst-Zertifizierung;
- 1. Überwachungsaudit (1 Jahr nach Erst-Zertifizierung);
- 2. Überwachungsaudit (2 Jahre nach Erst-Zertifizierung);
- Re-Zertifizierung (3 Jahre nach Erst-Zertifizierung).

Nachfolgend ist in Abbildung 1 der Lebenszyklus eines Zertifikates dargestellt.

Abbildung 1 Lebenszyklus eines CISIS12-Zertifikates

Erst-Zertifizierung

Das Erst-Zertifizierungsaudit spaltet sich auf in:

- Vorbereitung;
- Stage 1-Audit;
- Stage 2-Audit.

Vorbereitung

Im Rahmen der Vorbereitung stellt die Organisation dem Auditor die für das Stage 1-Audit benötigten Referenzdokumente zur Verfügung – typischerweise umfasst dies

- eine Darstellung des Informationssicherheits-Managementsystem nach CISIS12® insgesamt samt
- Darstellung der Umsetzung von Sicherheitsmaßnahmen aus den festgelegten Bausteinen und zutreffenden Wahl-Bausteinen Schicht 1 und 2 sowie 3 oder 4.

In der Regel findet nur eine Begutachtung eines Standortes (Zentrale) des Unternehmensverbundes statt. Bei mehreren Standorten wird neben der Zentrale nur eine Auditierung vor Ort an einem Standort durchgeführt. Die weiteren Standorte werden

dann bei den anstehenden Überwachungsaudits gemäß einem erstellten Prüfplan überprüft.

Die Überwachung von mehreren Standorten (Multi-Site Verfahren) wird durch eine repräsentative Stichprobe durchgeführt. Die Höhe der Stichprobe sowie die Anzahl wird von der Zertifizierungsstelle, auf Basis anerkannter Regeln vgl. auch [27006, Abschnitt 9.1.5.1.2] und DAkkS-Vorgabe [IAF MD 1]) festgelegt.

Stage 1-Audit

Der Auditor prüft vor Ort, ob die Zertifizierungsfähigkeit des Informationsverbundes prinzipiell, durch Einsicht in die Dokumente, gegeben ist. Hierzu werden dem Auditor die in einer Liste „Übergabe der Referenzdokumente“ aufgeführten Referenzdokumente zur Verfügung gestellt.

Beim Stage 1-Audit wird eine Sichtung der Referenzdokumente und einer Kurz-Beurteilung vor Ort durchgeführt:

- Ziel des Treffens vor Ort ist es, sich und den Standort sowie die standortspezifischen Bedingungen kennenzulernen. Des Weiteren werden der Zeitplan und das weitere Audit abgestimmt; dazu werden Aspekte identifiziert, die beim Audit besonders berücksichtigt werden sollen.
- Um sicherzustellen, dass die gemäß Standard geforderten Anforderungen zum Stage 2-Audit entsprechend geprüft werden können, prüft der Auditor, ob alle anwendbaren Anforderungen des Standards entsprechend dokumentiert sind.
- Letztendlich werden stichpunktartig Aspekte des Standards geprüft, um festzustellen, ob das des Informationssicherheits-Managementsystem nach CISIS12® zertifizierungsfähig ist.

Stage 2-Audit

Bei der Umsetzungsprüfung werden die Kontrollfragen der CISIS12®-Schritte 1-11 untersucht. Der Auditor überzeugt sich von der wirksamen Umsetzung dieser elf Schritte und dokumentiert dies in seinem Auditreport.

Zudem hat der Auditor hat die wirksame Umsetzung von Sicherheitsmaßnahmen aus fünf Bausteinen zu prüfen. Die Bausteine werden vom Auditor nach einem Stichprobenverfahren aus den Baustein- und Maßnahmenkatalog ausgewählt.

Beim nachfolgenden Stage 2-Audit, in der Regel im Anschluss zum Stage 1, wird schließlich vor Ort die Wirksamkeit des Managementsystems zur Umsetzung des Standards aus CISIS12® geprüft und bewertet:

- Für jeden anwendbaren Aspekt des Standards prüft der Auditor, wie lt. Dokumentation dieser Aspekt der des Standards umgesetzt werden soll. Dabei sichtet der Auditor die Dokumentation und prüft sie auf Vollständigkeit, Plausibilität und Nachvollziehbarkeit zu den Anforderungen an ein Informationssicherheits-Managementsystem nach CISIS12®.
- Für jeden anwendbaren Aspekt des Standards CISIS12® prüft der Auditor beim Stage 2-Audit den Umsetzungsgrad der in der Dokumentation angegebenen Maßnahmen zu den drei Phasen und 12 Schritten.

- Der Reifegrad wird aufgenommen, und mit der Organisation wird ein Zeitraum zur Beseitigung eventueller Abweichungen vereinbart.
- Der Auditor erstellt final einen ausführlichen Auditreport.

Zertifizierung

Zur Zertifizierung trifft die Zertifizierungsstelle auf Grundlage des Auditreports sowie weiterer relevanter Informationen final die Entscheidung, ob das Informationssicherheits-Managementsystem konform nach CISIS12® betrieben wird und erteilt dann ein gültiges CISIS12®-Zertifikat: Dieses Zertifikat bescheinigt der Organisation, dass das Informationssicherheits-Managementsystem nach CISIS12® für das im Zertifikat ausgewiesene Unternehmen und einbezogene Standorte den Anforderungen des Standards CISIS12® angemessen genügt.

Überwachungsaudit

Nach Erteilung des Zertifikats ist jährlich ein Überwachungsaudit zur Aufrechterhaltung des Zertifikats durchzuführen, in denen die Wirksamkeit des Informationssicherheits-Managementsystem nach CISIS12® vor Ort überprüft wird.

Re-Zertifizierung

Nach Ablauf des (i.d.R.) drei Jahre gültigen Zertifikats kann ein Re-Zertifizierungsaudit durchgeführt werden, dass sich im Wesentlichen an der Erst-Zertifizierung orientiert.

Sonstige Audits

Darüber hinaus können sonstige Audits durchgeführt werden, etwa bei signifikanten Änderungen am zertifizierten Informationssicherheits-Managementsystem nach CISIS12® oder Erweiterungen/Einschränkungen des Geltungsbereichs z.B. Standorte. Darüber hinaus können kurzfristig angekündigte Audits aufgrund von Beschwerden durchgeführt werden.

Übernahme von Zertifikaten

Die datenschutz cert GmbH bietet die Zertifizierung eines Informationssicherheits-Managementsystem nach CISIS12®, für welches bereits ein CISIS12®-Zertifikat existiert, ebenfalls an. Im Rahmen einer Übernahme kann eine bestehende CISIS12®-Zertifizierung übernommen werden. Die Zertifikatslaufzeit orientiert sich dabei an der Restlaufzeit des bestehenden Zertifikats.

Zertifikatsliste

Eine Liste unserer erteilten Zertifizierungen kann abgerufen werden unter: http://www.datenschutz-cert.de/zertifikatslisten/. Aus der Liste sind der Antragsteller, der Geltungsbereich, die Zertifikats-ID sowie die Gültigkeit der Zertifizierung ersichtlich.

Entzug, Aussetzen oder Einschränken eines Zertifikates

Das Zertifikat wird entzogen, wenn der Antragsteller nachhaltig gegen die Zertifizierungsvoraussetzungen verstößt. Ein solcher Verstoß liegt insbesondere vor, wenn

- der zertifizierte Untersuchungsgegenstand in der beschriebenen Weise verändert wurde und der Anbieter keine Prüfung ermöglicht,
- im Rahmen der Prüfung nicht die für die Vergabe des Zertifikats erforderlichen Voraussetzungen erfüllt werden,
- der Antragsteller aufgrund drohender oder eingetretener Insolvenz einen zuverlässigen Geschäftsbetrieb nicht mehr aufrechterhalten kann oder
- die Zertifizierungskosten nicht spätestens innerhalb von 4 Wochen nach Abschluss der Zertifizierung gegenüber der Zertifizierungsstelle beglichen werden.

Die Zertifizierungsstelle teilt dem Antragsteller die Gründe des Zertifikatsentzugs mit. Im Falle des Entzuges wird das über die Zertifikatsliste online unter www.datenschutz-cert.de veröffentlichte Zertifikat auf den Status als entzogen gesetzt und spätestens nach 4 Wochen aus der Liste entfernt. Der Entzug des Zertifikates kann auch anderweitig veröffentlicht werden.

Ferner kann die datenschutz cert GmbH Zertifikate aussetzen, wenn eine wesentliche Anforderung des Regelwerkes nicht erfüllt wird (max. Aussetzung: 6 Monate), oder einschränken, wenn für diesen ausgeschlossenen Teil wesentliche Anforderung des Regelwerkes nicht erfüllt werden (Einschränkung des Geltungsbereiches). Im Anschluss an eine Aussetzung erfolgt entweder die Behebung unter Berücksichtigung entsprechender Nachweise (mit Wiederherstellung) oder die Zurückziehung des Zertifikates.

Ablauf eines Zertifikates

Soweit das Zertifikat nach Ablauf der Gültigkeit entfällt, hat der Anbieter dafür zu sorgen, dass das Logo und sämtliche Hinweise auf eine gültige Zertifizierung aus den genutzten Medien unverzüglich entfernt werden.

Kosten und Gebühren

Kosten fallen einerseits für die Auditierung, andererseits für die Zertifizierung an.

Für die Zertifizierung veranschlagt die datenschutz cert GmbH Kosten/ Gebühren. Die einmaligen Zertifizierungskosten gelten für die gesamte Laufzeit des Zertifikats (i.d.R. drei Jahre) und umfassen

- Prüfbegleitung des Auditors durch die Zertifizierungsstelle;
- Ausstellung des gültigen Zertifikats, sofern das eines Informationssicherheits-Managementsystem nach CISIS12® zertifizierungsfähig ist, in deutscher Sprache;
- Darstellung Ihres Zertifikats in der Zertifikatsliste unter www.datenschutz-cert.de;
- Übergabe Ihres Zertifikats.

Neben den Zertifizierungskosten fallen Kosten für die Auditierung an, wobei der Aufwand für die Auditierung stark von der Komplexität des Untersuchungsgegenstands und der Anzahl der Mitarbeiter im Geltungsbereich abhängt, sprechen Sie uns für ein konkretes Angebot bitte einfach an!

Jährliche Überwachungsaudits zur Aufrechterhaltung mit dem Auditor werden separat berechnet; alternativ können wir diese gerne in die Kalkulation aufnehmen, so dass wir Ihnen ein Angebot zur Auditierung und Zertifizierung über die gesamte Laufzeit des Zertifikats unterbreiten können.

Anfrageformular

Sofern Sie Interesse an einer Zertifizierung haben, sprechen Sie uns bitte an! Sie können auch das Anfrageformular ausfüllen, das die für uns wichtigen Angaben enthält. Das Anfrageformular können Sie herunterladen unter: http://www.datenschutz-cert.de.

AGB und KBO

Im Falle eines Vertragsschlusses gelten ausschließlich unsere Allgemeinen Geschäftsbedingungen (AGB) sowie unsere Konformitätsbewertungsordnung (KBO), die Sie unter https://www.datenschutz-cert.de/ueber-uns/agb.html abrufen können.

Anforderungen an einen Auditreport

Ein Auditreport zur Vorlage bei der Zertifizierungsstelle muss inhaltlich mindestens zu folgenden Aspekten Stellung beziehen:

- Organisatorische und formale Angaben zum Audit:
  - das mit der Auditierung angestrebte Zertifikat;
  - untersuchte Organisation, Name, Anschrift, Standort;
  - genaue Bezeichnung des Untersuchungsgegenstands, Abgrenzung zu den nicht auditierten Bereichen;
  - Auditoren (Recht/Technik), Name, Anschrift;
  - Zeitraum der Auditierung;
- Angewandte Methodik: z.B. Prüfung von Dokumenten des Auftraggebers, Führung von Mitarbeitergesprächen, Durchführung von Stichproben vor Ort (Site Visit) oder Plausibilitätstests;
- Grundlagen der Auditierung:
  - Audit Kriterien und Prüfgrundlage der IT-Sicherheitscluster e. V. Vorgaben mit Nennung des Versionsstandes zu CISIS12®;
  - eingesehene Dokumente;
  - befragte Abteilungen/Arbeitsbereiche/Unternehmensorgane;
  - Gegenstand der Stichproben;
  - Ortsbesichtigung, Standort, Adresse, Dauer, Teilnehmer;

- Erklärung der Auditoren zur Unabhängigkeit und Unparteilichkeit;
- Kurzdarstellung des Untersuchungsgegenstands;
- Zusammenstellung des für den konkreten Auditgegenstand anwendbaren Prüfkriterien/Anforderungen;
- Auditergebnisse:
  - Prüfung und Bewertung aller Prüfpunkte des Kriterienkatalogs;
- Votum des Auditors mit:
  - Zusammenfassung der Auditergebnisse / Management Summary;
  - Vorschlag an die Zertifizierungsstelle.

Über die datenschutz cert GmbH

Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.

Die datenschutz cert GmbH ist ein Unternehmen der datenschutz nord-Gruppe. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der datenschutz nord Gruppe sind inhabergeführt.

Leitlinien

Die datenschutz cert GmbH bietet Konformitätsbewertungen unter folgenden grundsätzlichen Leitlinien an:

Unabhängigkeit und Unparteilichkeit

Wir sind unabhängig und unparteilich. Es gilt das übergeordnete Interesse und die vorrangige Pflicht, Auditierungen, Evaluierungen, Zertifizierungen und Bestätigungen entsprechend den Vorgaben frei von internen und externen kommerziellen, finanziellen und sonstigen Zwängen durchzuführen. Maßstab ist das jeweilige Kriterien Werk. Zudem führen wir keinerlei Beratung durch.

Wir haben einen "Ausschuss zur Sicherstellung der Unparteilichkeit der datenschutz cert GmbH" (Ausschuss) etabliert, mit dem die grundsätzlichen Regelungen zur Unabhängigkeit und Unparteilichkeit der Zertifizierungstätigkeiten diskutiert und durchgeführte Zertifizierungsprozesse auf ihre Unabhängigkeit hin überprüft werden.

Zur Gewährleistung der Unabhängigkeit und Unparteilichkeit unserer erteilten Zertifikate setzen wir für den Auditierungs- und Zertifizierungsprozess darüber hinaus regelmäßig externe Fachbegutachter ein.

Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

Offenheit und Transparenz

Wir sind offen und transparent hinsichtlich unserer Tätigkeiten, d.h.

- wir kommunizieren klar und unmissverständlich, was und nach welchen Regeln geprüft und zertifizieren wird;
- unsere Zertifikate und Auditreports sind klar und verständlich formuliert;
- wir veröffentlichen die zugrundeliegenden Regelwerke – sofern nicht durch Copyright geschützt;
- wir benennen klar, wofür wir akkreditiert sind;
- wir lassen uns selber regelmäßig auditieren;
- wir sind offen für alle Anfragen und Beschwerden: Wenn Sie Fragen zu einem von uns erteilten Zertifikat haben oder potentiell den Missbrauch eines Zertifikats vermuten: Bitte sprechen Sie uns an. Wir sichern Ihnen Vertraulichkeit zu und gehen der Sache nach. Wir informieren Sie über den Stand der Untersuchung sowie den Abschluss.

Datenschutz

Wir kommen aus dem Datenschutz. Jede Art von Konformitätsprüfung wird – im Rahmen des jeweiligen Untersuchungsgegenstands – unter den besonderen Aspekten des Datenschutzes beleuchtet. Dadurch stellen wir sicher, dass die von uns geprüften und bewerteten IT-Produkte und -Systeme den Anforderungen des Datenschutzes genügen.

Unser Anspruch ist, dass sich "datenschutz zertifizierte" Produkte und Prozesse etablieren und für unsere Kunden einen Mehrwert zu einem besseren Datenschutz darstellen und dass unser Zertifikat eine entsprechende Anerkennung genießt.

Anerkennungen und Akkreditierungen

Die datenschutz cert GmbH ist beim IT-Sicherheitscluster e.V. anerkannte CISIS12®-Zertifizierungsstelle.

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO/IEC 27006 akkreditierte Zertifizierungsstelle und darf danach international gültige Zertifikate für ISO/IEC 27001-konforme Informationssicherheits-Managementsysteme (ISMS) erteilen. Die Akkreditierung der DAkkS umfasst ferner das Regelwerk „IT-Sicherheitskatalog“.

Ferner ist die datenschutz cert GmbH bei der DAkkS für Produkte und Dienstleistungen gemäß ISO/IEC 17065 akkreditiert und darf danach Zertifikate für Vertrauensdienste gemäß eIDAS erteilen.

Auditoren der datenschutz cert GmbH sind beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Auditoren für die TR-03109-6 (Smart Meter Gateway Administratoren) sowie BSI TR-03145 (Secure CA Operation) zertifiziert.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

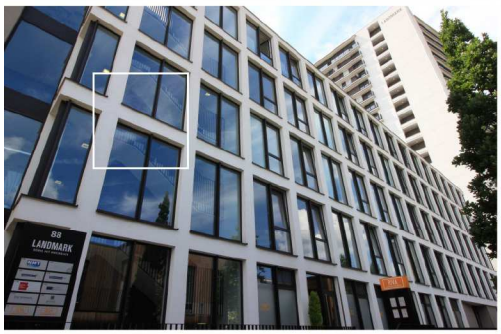
Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG) sowie Konformitätsbewertungsstelle nach eIDAS.

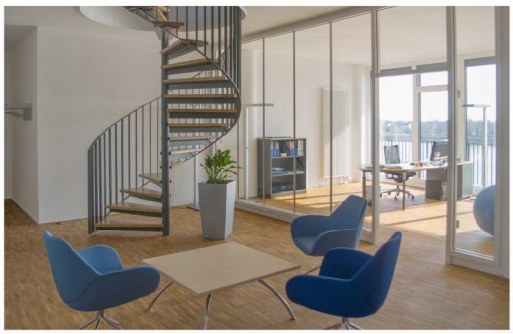
Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren und IS-Revisoren. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.

Ferner ist die datenschutz cert GmbH beim BSI anerkannter IT-Sicherheitsdienstleister für Penetrationstest.

Auditoren der datenschutz cert GmbH sind zudem anerkannte EuroPriSe Experten für Recht und Technik.

Aufgrund der Akkreditierung bei der DAkkS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a-Verfahren die Rolle der „prüfenden Stelle“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer für § 8a BSIG anerkannt.









datenschutz cert GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: 0421 69 66 32 50

Standort Offenbach am Main
Mainstraße 143
63065 Offenbach am Main
Tel.: 069 87 00 783 580

office@datenschutz-cert.de
www.datenschutz-cert.de

datenschutz cert