ISIS12-Kriterienkatalog

datenschutz cert GmbH
Version 1.3

datenschutz cert

Inhaltsverzeichnis

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	16.07.2020		Ersterstellung	MM SM
1.1	23.07.2020	Kap. 2	Anpassung mit Graphik	MM
1.2	10.08.2020		Redaktionelle Änderungen nach Rückmeldung vom IT-Sicherheitscluster e. V.	MM
1.3	07.12.2021		Aktualisierung AGB und KBO	HH

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentbesitzer	Version
Final	Matthias Mühlhause	1.3

1. Anforderungen an ISIS12

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 ISIS12-konforme Informationssicherheits-Managementsysteme und erteilt ISISI12-Zertifikate: Diese Zertifikate bescheinigen einer Institution, dass sie ein Informationssicherheits-Managementsystem nach ISIS12 vom IT-Sicherheitscluster e.V. eingeführt und umgesetzt hat.

Die datenschutz cert GmbH ist dazu beim IT-Sicherheitscluster e.V. gemäß ISIS12 anerkannte Zertifizierungsstelle.

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

Bremen, den 16.07.2020

Dr. Sönke Maseberg
Geschäftsführer
datenschutz cert GmbH

2. ISIS12

2.1. Informationssicherheit in 12 Schritten

Der Standard für ein Informationssicherheits-Managementsystem nach ISIS12 sieht 12 Schritte vor, die in drei Phasen – Initialisierungsphase, Festlegung der Aufbau- und Ablauforganisation sowie Entwicklung und Umsetzung der ISIS12-Konzeption – eingeteilt sind.

Schritt 1 Leitlinie erstellen

Schritt 1 beschäftigt sich mit der Erstellung einer Unternehmensleitlinie für Informationssicherheit. Die Unternehmensleitlinie ist das zentrale Strategiepapier. Darin werden die Informationssicherheitsziele sowie die daraus abgeleiteten und abzuleitenden Konzepte und Maßnahmen festgehalten. Die Mitarbeiter müssen zur Einhaltung und Umsetzung von der Unternehmensleitung motiviert werden. Zu berücksichtigen sind insbesondere auch die unternehmensspezifischen Sicherheitsziele wie z.B. Reduzierung der Kosten im Schadensfall oder Aufrechterhaltung der Produktionsfähigkeit.

Schritt 2 Mitarbeiter sensibilisieren

In Schritt 2 stehen die Mitarbeiter und Führungskräfte im Mittelpunkt. Auf allen Organisationsebenen muss die Notwendigkeit des Projekts kommuniziert werden. In einem speziellen ISIS12-Vortrag sollen alle Mitarbeiter über den ISIS12-Workflow und die spezifische Bedeutung der Informationssicherheit für das Unternehmen hingewiesen werden. Neben dem Erhalt eines schriftlichen Exemplars der Leitlinie für Informationssicherheit sollen die Mitarbeiter regelmäßig über Neuerungen informiert werden.

Schritt 3 Informationssicherheitsteam aufbauen

Schritt 3 beschreibt den Aufbau, die Zusammensetzung, die Aufgaben und Pflichten des Informationssicherheitsteams. Leiter ist der Informationssicherheitsbeauftragte (ISB), der auch für die Einführung des ISIS12 Prozesses verantwortlich ist. Die Berichterstattung erfolgt direkt an die Unternehmens- bzw. Behördenleitung.

Schritt 4 IT-Dokumentationsstruktur festlegen

Schritt 4 beschäftigt sich mit einer zielführenden IT-Dokumentation. Absolut wichtig ist die Aktualität der Dokumente, die der IT-Verantwortliche kontinuierlich kontrollieren muss. Um Änderungen nachzuvollziehen, ist eine Versionierung der Dokumente erforderlich.

Schritt 5 IT-Service-Management-Prozess einführen

In Schritt 5 erfolgt die Implementierung von drei fundamentalen IT-Service-Managementprozessen: Wartung, Änderung und Störungsbeseitigung. Wird im Rahmen einer Wartung eine Änderung nötig, wird diese über den Änderungsprozess eingesteuert. Final wird der Störungsbeseitigungsprozess definiert.

Schritt 6 Kritische Applikationen identifizieren

Mit Schritt 6 beginnt die operative Phase des ISIS12 Vorgehensmodells. Dabei werden nur unternehmenskritische Anwendungen identifiziert und bewertet. Diesen werden jeweils drei Schutzbedarfskategorien, bezogen auf die Grundwerte „Vertraulichkeit, Integrität und Verfügbarkeit“, zugeordnet.

Schritt 7 IT-Struktur analysieren

Nach der Lokalisierung kritischer Applikationen steht in Schritt 7 die Definition des Informationsverbunds im Mittelpunkt. In diesem werden die technischen, personellen, organisatorischen und infrastrukturellen Objekte, die für die Verarbeitung von Informationen im Unternehmen benötigt werden, zusammengefasst.

Schritt 8 Sicherheitsmaßnahmen modellieren

Bei Schritt 8 erfolgt die Zuordnung der empfohlenen Sicherheitsmaßnahmen zu den in Schritt 7 ermittelten Objekten. Die Bausteine, die für den gesamten Informationsverbund anzuwenden sind, lauten: Universale Aspekte, Infrastruktur, IT-Systeme /

Netze und Anwendungen. Diesen Bausteinen werden die IT-Objekte zugeordnet, z.B. gehören Gebäude und Serverraum zur Infrastruktur.

Schritt 9 Soll-Ist vergleichen

In Schritt 9 soll mit dem Soll-Ist-Vergleich ein Überblick über den Umsetzungsgrad der in Schritt 8 geforderten Maßnahmen gegeben werden. Die Erhebung kann durch die vom ISB ernannten verantwortlichen Spezialisten im Unternehmen durchgeführt werden. Die hierfür von der ISIS12-Software erstellten Erhebungsbögen können im größeren Kreis oder in Einzelinterviews abgearbeitet werden.

Schritt 10 Umsetzung planen und Umsetzung

In Schritt 10 wird ein Maßnahmenkatalog erzeugt und konsolidiert. Die umzusetzenden Maßnahmen werden priorisiert und zusammen mit einer Kostenabschätzung der Geschäftsleitung als Vorschlag präsentiert. Nach Festlegung der Umsetzungsreihenfolge der Maßnahmen werden diese umgesetzt.

Schritt 11 Internes Audit

In Schritt 11 werden die konsolidierten, genehmigten und umgesetzten Sicherheitsmaßnahmen überprüft, wie gut diese umgesetzt und den Vorgaben entsprechen.

Schritt 12 Revision

Mit dem Abschluss des Schrittes 11 fordert die ISIS12-Software zur Eingabe eines Revisionstermins für eine oder mehrere Maßnahmen auf. Die gescannte Revisionsliste wird in Schritt 12 erzeugt.

2.2. Vorteile einer ISIS12-Zertifizierung

Allein durch das Etablieren eines Informationssicherheits-Managementsystem nach ISIS12 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 ISIS12 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 ISIS12-Zertifizierung einem Unternehmen, sich zu einem späteren Zeitpunkt auf Basis von ISO/IEC 27001 oder IT-Grundschutz zertifizieren zu

lassen. ISIS12 ist daher ein Fundament, auf dem die Informationssicherheit eines Unternehmens aufgebaut ist.

2.3. Warum datenschutz cert GmbH?

Über 12 Jahre Erfahrung in der Prüfung und Zertifizierung von Informationssicherheit und Datenschutz. Wir sind anerkannte ISIS12-Zertifizierungsstelle mit lizensierten, qualifizierten und zugelassen ISIS12-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.

3. Auditierungs- und Zertifizierungsprozess

In diesem Abschnitt wird dargestellt, wie die datenschutz cert GmbH ein Informationssicherheits-Managementsystem nach ISIS12 auditiert und zertifiziert. Abschließend wird der Life-Cycle eines ISIS12-Zertifikates illustriert.

Dabei wird ein zweistufiges Zertifizierungsverfahren eingesetzt:

- Der bei der datenschutz cert GmbH lizenzierte Auditor prüft die Konformität eines Informationssicherheits-Managementsystem nach ISIS12 und erstellt einen Auditreport.
- Die Zertifizierungsstelle prüft den Auditreport, insbesondere um eine Vergleichbarkeit zwischen den Audits sicherstellen zu können.

3.1. 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.

3.2. 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 ISIS12-Zertifikates

3.3. Erst-Zertifizierung

Das Erst-Zertifizierungsaudit spaltet sich auf in:

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

3.3.1. 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 ISIS12 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 eines erstellten Prüfplans 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.

3.3.2. 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 ISIS12 zertifizierungsfähig ist.

3.3.3. Stage 2-Audit

Bei der Umsetzungsprüfung werden die Kontrollfragen der ISIS12-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 folgenden Regeln gewählt:

- aus Schicht 1 den Baustein 1.1 und zwei Bausteine nach Wahl des Auditors;
- aus Schicht 2 den Baustein 2.3 und einen Baustein nach Wahl des Auditors;
- aus Schicht 3-4 zwei Bausteine nach Wahl des Auditors.

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 ISIS12 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 ISIS12.

- Für jeden anwendbaren Aspekt des Standards ISIS12 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.

3.3.4. Zertifizierung

Zur Zertifizierung trifft die Zertifizierungsstelle auf Grundlage des Auditreports sowie weiterer relevanter Informationen final die Entscheidung, ob das Informationssicherheits-Managementsystem konform nach ISIS12 betrieben wird und erteilt dann ein gültiges ISIS12-Zertifikat: Dieses Zertifikat bescheinigt der Organisation, dass das Informationssicherheits-Managementsystem nach ISIS12 für das im Zertifikat ausgewiesene Unternehmen und einbezogene Standorte den Anforderungen des Standards ISIS12 angemessen genügt.

3.4. Überwachungsaudit

Nach Erteilung des Zertifikats ist jährlich ein Überwachungsaudit zur Aufrechterhaltung des Zertifikats durchzuführen, in denen die Wirksamkeit des Informationssicherheits-Managementsystem nach ISIS12 vor Ort überprüft wird.

3.5. 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.

3.6. Sonstige Audits

Darüber hinaus können sonstige Audits durchgeführt werden, etwa bei signifikanten Änderungen am zertifizierten Informationssicherheits-Managementsystem nach ISIS12 oder Erweiterungen/Einschränkungen des Geltungsbereichs z.B. Standorte. Darüber hinaus können kurzfristig angekündigte Audits aufgrund von Beschwerden durchgeführt werden.

3.7. Übernahme von Zertifikaten

Die datenschutz cert GmbH bietet die Zertifizierung eines Informationssicherheits-Managementsystem nach ISIS12, für welches bereits ein ISIS12-Zertifikat existiert, ebenfalls an. Im Rahmen einer Übernahme kann eine bestehende ISIS12-Zertifizierung übernommen werden. Die Zertifikatslaufzeit orientiert sich dabei an der Restlaufzeit des bestehenden Zertifikats.

3.8. 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.

3.9. 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.

3.10. 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.

3.11. 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 ISIS12 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.

3.12. 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.

3.13. 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.

4. 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 ISIS12 Handbuch und Katalog mit Nennung des Versionsstandes;

    - 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.

5. 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.

5.1. Leitlinien

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

5.1.1. 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.

5.1.2. Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

5.1.3. 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.

5.1.4. 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.

5.2. Anerkennungen und Akkreditierungen

Die datenschutz cert GmbH ist beim IT-Sicherheitscluster e.V. anerkannte ISIS12-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 gemäß § 11 Abs. 1a EnWG“.

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.

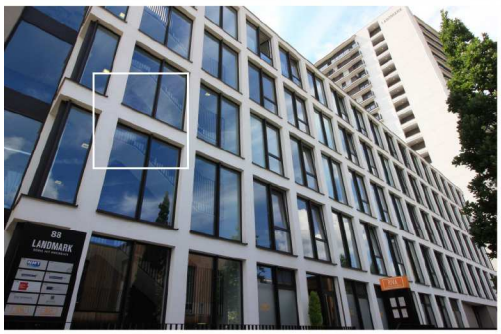
Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG) sowie Konformitätsbewertungsstelle nach eIDAS.

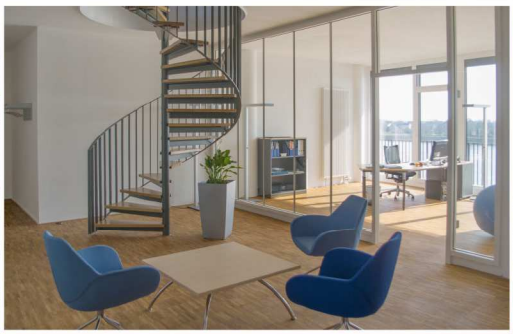
Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren und IS-Revisoren. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.

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