Kriterienkatalog und Vorgehensweise zur Auditierung und Zertifizierung nach „IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG“

datenschutz cert GmbH

Version 1.1

Inhaltsverzeichnis

Kriterienkatalog und Vorgehensweise zur Auditierung und Zertifizierung nach „IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG“

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
1.0	08.02.2017		Finalisierung	Dr. Maseberg
1.1	08.09.2017		Umbenennung von Preaudit auf Stage 1-und Site Visit auf Stage 2-Audit	Dr. Maseberg

Dokumenten-Überwachungsverfahren

Status: final	Prozess-/Dokumentbesitzer: Dr. Maseberg	Version: 1.1

1. Anforderungen des IT-Sicherheitskatalogs

Der „IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz“ (IT-Sicherheitskatalog) der Bundesnetzagentur (BNetzA) [IT-SichKat] stellt Anforderungen an Netzbetreiber hinsichtlich einer sicheren IT-Infrastruktur für den Netzbetrieb. Der IT-Sicherheitskatalog fordert von Netzbetreibern ein Informationssicherheits-Managementsystem, das den Anforderungen

--- von ISO/IEC 27001 und

--- ISO/IEC 27019 sowie

--- ergänzenden Anforderungen aus dem IT-Sicherheitskatalog

genügt, und dass durch ein Zertifikat einer akkreditierten Zertifizierungsstelle belegt ist.

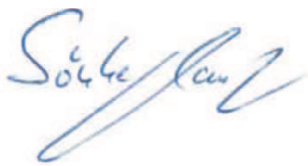
Bzgl. der Akkreditierung dieser Zertifizierungsstelle ist zwischen Deutscher Akkreditierungsstelle (DAkkS) und Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Bundesnetzagentur, BNetzA) das folgende Konformitätsbewertungsprogramm abgestimmt worden:

> Bundesnetzagentur, „Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006“, 13.04.2016.

Die datenschutz cert GmbH auditiert und zertifiziert Informationssicherheits-Managementsysteme für Netzbetreiber, die den Anforderungen des IT-Sicherheitskatalogs und des zugehörigen Konformitätsbewertungsprogramm genügen. Die datenschutz cert GmbH ist – um diese Zertifikate ausstellen zu dürfen – bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO/IEC 27006 akkreditierte Zertifizierungsstelle.

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

Bremen, den 08. September 2017

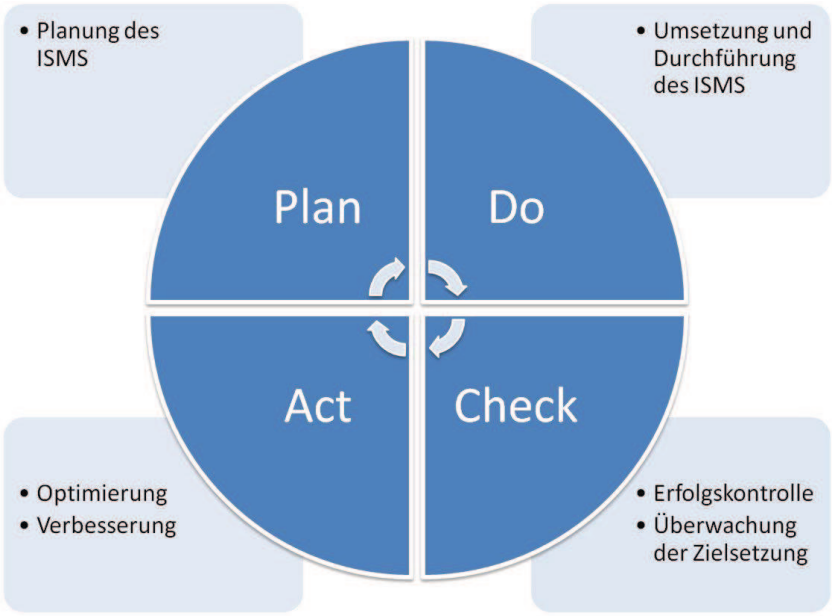


Dr. Sönke Maseberg
datenschutz cert GmbH

2. ISO/IEC 27001 als Basis

2.1 Prozessorientierte Vorgehensweise

Die Norm ISO/IEC 27001 stellt einen prozessorientierten Ansatz eines Managementsystems zur Umsetzung und kontinuierlichen Verbesserung von Informationssicherheit in den Vordergrund. Das Informationssicherheits-Managementsystem (ISMS) wird dabei als Prozess über einen PDCA (Plan, Do, Check, Act)-Zyklus wie folgt organisiert:



2.1.1 Planung des ISMS

Zur Einführung eines Informationssicherheits-Managementsystems (ISMS) sind zunächst Sicherheitspolitik, -ziele, -prozesse und -verfahren festzulegen und konkret zu planen. Genutzt werden dazu insbesondere die Ausführungen der Norm ISO/IEC 27002, in denen die Maßnahmen und Maßnahmenziele – die sogenannten Controls und Control Objectives – aus ISO/IEC 27001 ausführlich dargestellt werden.

2.1.2 Einbeziehung von ISO/IEC 27019 und vom IT-Sicherheitskatalog

Ferner können weitere Normen herangezogen und über das Statement of Applicability (SOA) in das ISMS eingebunden werden – in diesem Fall ISO/IEC 27019 und der IT-Sicherheitskatalog.

2.1.3 Umsetzen und Durchführen des ISMS

Die festgelegten Sicherheitspolitiken, -ziele, -prozesse und -verfahren werden entsprechend umgesetzt und dokumentiert.

2.1.4 Überprüfen des ISMS

Die umgesetzten Maßnahmen werden anhand der definierten Vorgaben überprüft; die Ergebnisse werden an das Management rückgekoppelt.

2.1.5 Verbessern des ISMS

Basierend auf den Prüfergebnissen werden Verbesserungsmaßnahmen formuliert und diese zwecks kontinuierlicher Verbesserung des ISMS priorisiert und umgesetzt.

2.2 Dokumentation des ISMS

Die Dokumentation des Informationssicherheits-Managements (ISMS) umfasst neben den Nachweisen zur Umsetzung typischerweise die folgenden Dokumente:

- Darstellung des ISMS insgesamt samt Prozessdarstellung zum Management der Informationssicherheit;
- Geltungsbereich des ISMS;
- Netzstrukturplan;
- Darstellung der IT-Infrastruktur (IT-Strukturanalyse) mit Schutzbedarfsfeststellung – etwa in einem Sicherheitskonzept samt weiterführender Dokumente –;
- Sicherheitsleitlinie/Managementvorgaben;
- Risikoanalyse;
- Statement of Applicability (SOA), in der dargestellt ist, welche Anforderungen im ISMS umgesetzt werden sollen; Basis sind Controls aus ISO/IEC 27019 und dem IT-Sicherheitskatalog, aber auch andere Regelwerke können hier referenziert werden.

3. Kriterienkatalog

Für eine Auditierung und Zertifizierung nach „IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz“ stellen die folgenden Standards den Kriterienkatalog dar:

- ISO/IEC 27001;
- ISO/IEC 27019;
- ergänzende Anforderungen aus dem „IT-Sicherheitskatalog gem. § 11 Absatz 1a EnWG“;
- ergänzende Anforderungen aus dem „Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006“.

4. Auditierungs- und Zertifizierungsprozess

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

Dabei wird ein zwei-stufiges Zertifizierungsverfahren eingesetzt:

--- Der bei der datenschutz cert GmbH lizenzierte Auditor prüft die Konformität eines Informationssicherheits-Managementsystems gegen das jeweilige Regelwerk und erstellt einen Auditreport.

--- Die Zertifizierungsstelle prüft den Auditreport, insbesondere um eine Vergleichbarkeit zwischen den Audits sicherstellen zu können.

4.1 Laufzeiten

Jedes Zertifizierungsverfahren besteht aus folgenden 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 Zertifikates

4.2 Erst-Zertifizierung

Das Erst-Zertifizierungsaudit spaltet sich auf in:

--- Vorbereitung;

--- Stage 1-Audit;

--- Stage 2-Audit.

4.2.1 Vorbereitung

Im Rahmen der Vorbereitung stellt die Organisation dem Auditor die für das Stage 1-Audit benötigten Referenzdokumente zur Verfügung.

4.2.2 Stage 1-Audit

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 wird der Zeitplan und das weitere Audit abgestimmt; dazu werden Aspekte identifiziert, die beim Audit besonders berücksichtigt werden sollen.

--- Um sicherzustellen, dass die gemäß Statement of Applicability normierten Anforderungen zum Stage 2-Audit entsprechend geprüft werden können, prüft der Auditor, ob alle anwendbaren Anforderungen der Norm entsprechend dokumentiert sind. Darüber hinaus wird festgestellt, ob die Umsetzung den Anforderungen an ein ISMS mit vollständigem Plan-Do-Check-Act (PDCA)-Zyklus genügt.

--- In diesem Kontext findet insbesondere eine Prüfung der internen Audits und der Managementbewertungen statt.

--- Letztendlich werden stichpunktartig Aspekte der Norm geprüft, um festzustellen, ob das ISMS zertifizierungsfähig ist.

4.2.3 Stage 2-Audit

Beim nachfolgenden Stage 2-Audit wird schließlich vor Ort die Wirksamkeit des Managementsystems zur Umsetzung der Anforderungen aus den jeweiligen Regelwerken geprüft und bewertet:

--- Für jeden anwendbaren Aspekt der Norm prüft der Auditor, wie lt. Dokumentation dieser Aspekt der Norm umgesetzt werden soll. Dabei sichtet der Auditor die Dokumentation und prüft sie auf Vollständigkeit, Plausibilität und Nachvollziehbarkeit zu den Anforderungen an ein ISMS mit vollständigem PDCA-Zyklus.

--- Für jeden anwendbaren Aspekt des Regelwerks prüft der Auditor beim Stage 2-Audit den Umsetzungsgrad der in der Dokumentation angegebenen Maßnahmen.

--- Zudem prüft und bewertet der Auditor das ISMS dahingehend, ob die Anforderungen an ein ISMS mit vollständigem PDCA-Zyklus umgesetzt werden.

--- Etwaige Abweichungen werden aufgenommen, und mit der Organisation wird ein Zeitraum zur Beseitigung vereinbart.

--- Der Auditor erstellt final einen ausführlichen Auditreport.

4.2.4 Zertifizierung

Zur Zertifizierung trifft die Zertifizierungsstelle auf Grundlage des Auditreports sowie weiterer relevanter Informationen final die Entscheidung, ob das ISMS normkonform betrieben wird und erteilt dann ein gültiges Zertifikat: Dieses Zertifikat bescheinigt der Organisation, dass das ISMS für den im Zertifikat ausgewiesenen Geltungsbereich den Anforderungen des Regelwerks „IT-Sicherheitskatalog gem. §11 Abs. 1a EnWG“ angemessen genügt.

4.3 Überwachungsaudit

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

4.4 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 und zusätzlich die kontinuierliche Wirksamkeit des Managementsystems feststellen soll.

4.5 Sonstige Audits

Darüber hinaus können sonstige Audits durchgeführt werden, etwa bei signifikanten Änderungen am zertifizierten ISMS oder Erweiterungen/Einschränkungen des Geltungsbereichs ("Scope"). Darüber hinaus können kurzfristig angekündigte Audits aufgrund von Beschwerden durchgeführt werden.

4.6 Zertifikatsliste

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

Ferner übermittelt die datenschutz cert GmbH die Zertifikatsliste halbjährlich an die BNetzA.

4.7 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.

4.8 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.

4.9 Kosten und Gebühren

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

Für die Zertifizierung veranschlagt die datenschutz cert GmbH Kosten in Höhe von 3.900,-- Euro zzgl. gesetzlicher Umsatzsteuer von derzeit 19 %. 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 international gültigen Zertifikats, sofern das ISMS 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. Als Orientierung bietet sich die für alle akkreditierten Zertifizierungsstellen bindende Norm ISO/IEC 27006 an, in der Richtwerte für die Audittage vor Ort angegeben werden. Zu beach-

ten ist, dass diese Werte in der Tabelle für die Audittage vor Ort nur einen Anhaltspunkt darstellen und dass der Aufwand für die Vor- und Nachbereitung, den ausführlichen Auditreport sowie das Projektmanagement zusätzlich zu berücksichtigen sind. Da diese Werte nur einen Anhaltspunkt bieten können, 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.

4.10 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.

4.11 AGB und Sonderbedingungen

Im Falle eines Vertragsschlusses gelten ausschließlich unsere Allgemeinen Geschäftsbedingungen sowie unsere „Sonderbedingungen für Dienstleistungen im Rahmen von Auditierungen und Zertifizierungen“, die Sie unter https://www.datenschutz-cert.de/ueber-uns/agb.html abrufen können.

5. 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:
  - 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.

6. 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.

6.1 Leitlinien

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

6.1.1 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 Kriterienwerk. 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.

6.1.2 Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

6.1.3 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 Ver-

traulichkeit zu und gehen der Sache nach. Wir informieren Sie über den Stand der Untersuchung sowie den Abschluss.

6.1.4 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 cert-ifizierte" Produkte und Prozesse etablieren und für unsere Kunden einen Mehrwert zu einem besseren Datenschutz darstellen und dass unser Zertifikat eine entsprechende Anerkennung genießt.

6.2 Akkreditierungen

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 ISO/IEC 20000-1 und ETSI TS-Normen.

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.

Die datenschutz cert GmbH ist bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) akkreditiert als Zertifizierungsstelle für den Bereich „IT-Sicherheitskatalog gem. § 11 Absatz 1a Energiewirtschaftsgesetz“.

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) zertifiziert.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) akkreditiert und ist danach berechtigt, Evaluierungen gemäß Common Criteria (CC) durchzuführen.

Die datenschutz cert GmbH ist bei der Bundesnetzagentur anerkannte Prüf- und Bestätigungsstelle gemäß Signaturgesetz.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-/ ISO 27001-Auditoren und IS-Revisoren.

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

Die datenschutz cert GmbH ist darüber hinaus als Gutachter des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein akkreditiert. Die Akkreditierung gilt sowohl für den Bereich Technik als auch für den Bereich Recht. Die Auditoren sind zudem anerkannte EuroPriSe Experten für Recht und Technik.

6.3 Kontakt

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen
Tel.: 0421.69 66 32-50
Fax: 0421.69 66 32-51
E-Mail: office@datenschutz-cert.de
Internet: www.datenschutz-cert.de