



Kriterienkatalog und Vorgehensweise zur Zertifizierung gemäß ISO/IEC 27001

datenschutz cert GmbH
Version 1.10

Inhaltsverzeichnis

| | |
|---|----|
| 1. Einleitung..... | 4 |
| 2. ISO/IEC 27001 | 5 |
| 2.1. Prozessorientierte Vorgehensweise..... | 5 |
| 2.2. Dokumentation des ISMS | 6 |
| 2.3. Vorteile einer ISO/IEC 27001-Zertifizierung..... | 6 |
| 3. Kriterienkatalog..... | 7 |
| 4. Auditierungs- und Zertifizierungsprozess | 8 |
| 4.1. Laufzeiten | 8 |
| 4.2. Erst-Zertifizierung..... | 9 |
| 4.3. Überwachungsaudit | 11 |
| 4.4. Re-Zertifizierung | 11 |
| 4.5. Sonstige Audits..... | 11 |
| 4.6. Anerkennung existierender Zertifikate..... | 11 |
| 4.7. Zertifikatsliste | 11 |
| 4.8. Entzug, Aussetzen oder Einschränken eines Zertifikates | 11 |
| 4.9. Ablauf eines Zertifikates | 12 |
| 4.10. Kosten und Gebühren..... | 12 |
| 4.11. Anfrageformular..... | 13 |
| 4.12. AGB und KBP | 13 |
| 5. Über die datenschutz cert GmbH..... | 14 |
| 5.1. Leitlinien..... | 14 |
| 5.2. Anerkennungen und Akkreditierungen | 15 |

Historie

| Version | Datum | Grund der Änderung | Geändert durch |
|---------|------------|---------------------|--------------------|
| 1.0-1.9 | | | |
| 1.10 | 18.02.2025 | Format aktualisiert | Dr. Sönke Maseberg |

Dokumenten-Überwachungsverfahren

| Status | Prozess-/Dokumentenbesitzer | Version |
|--------|-----------------------------|---------|
| final | Dr. Sönke Maseberg | 1.10 |

1. Einleitung

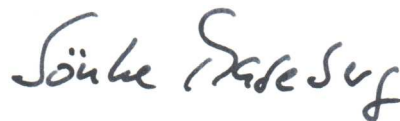
ISO/IEC 27001 hat sich international als Standard für Informationssicherheit in Unternehmen und Behörden etabliert. Informationssicherheit ist hierbei mehr als die reine IT: Ganzheitlich werden alle Aspekte zur Informationssicherheit betrachtet, die zum „Funktionieren“ eines Unternehmens oder einer Behörde notwendig sind. Dies umfasst neben technisch-organisatorischen Maßnahmen beispielsweise auch eine Risikoanalyse, in der die jeweils relevanten Bedrohungen analysiert werden.

Geprüft und zertifiziert wird dabei ein Informationssicherheits-Managementsystem (Information Security Management System – ISMS), welches prozessorientiert alle für einen ausgewiesenen Geltungsbereich einer Institution relevanten Werte zur Informationssicherheit umfasst.

Die datenschutz cert GmbH auditiert und zertifiziert ISO/IEC 27001-konforme Informationssicherheits-Managementsysteme und erteilt international gültige ISO/IEC 27001-Zertifikate: Diese Zertifikate bescheinigen einer Institution, dass das ISMS für den im Zertifikat ausgewiesenen Geltungsbereich den Anforderungen der internationalen Norm ISO/IEC 27001 angemessen genügt. Die datenschutz cert GmbH ist – um diese international gültigen 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 18.02.2025



Dr. Sönke Maseberg
Geschäftsführer
datenschutz cert GmbH

2. ISO/IEC 27001

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:

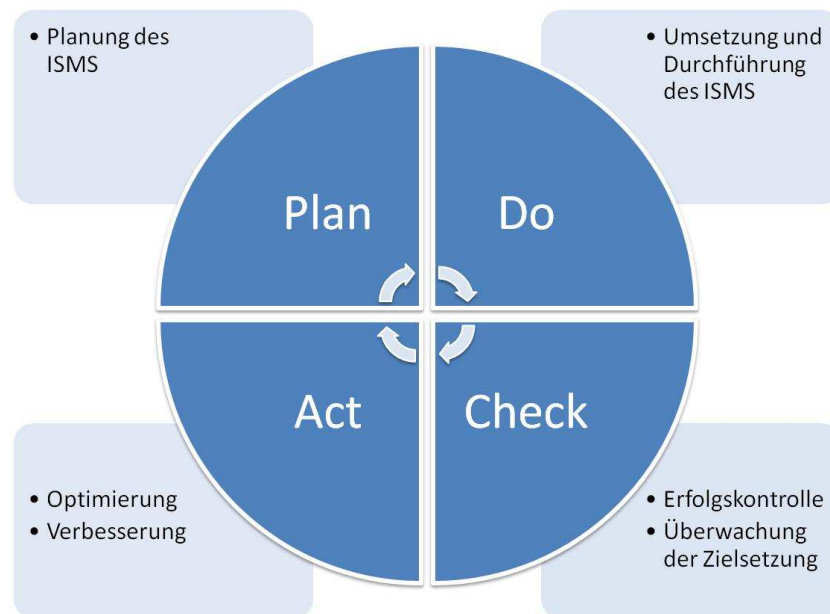


Abbildung 1 PDCA-Zyklus

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. Ferner können weitere Normen herangezogen und über das Statement of Applicability (SOA) in das ISMS eingebunden werden – etwa um die Umsetzung sektorspezifischer Anforderungen nachweisen zu können.

2.1.2. Umsetzen und Durchführen des ISMS

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

2.1.3. Überprüfen des ISMS

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

2.1.4. 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;
- 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 typischerweise Controls aus ISO/IEC 27002, aber auch andere Regelwerke können hier referenziert werden.

2.3. Vorteile einer ISO/IEC 27001-Zertifizierung

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

Durch den ganzheitlichen Ansatz und die Prozessorientierung erhält die Organisation einen guten Überblick über die Informationssicherheit in ihrem Verantwortungsbereich. Sie kann damit das „Maß“ ihrer Informationssicherheit messen und steuern – was auch ihr Haftungsrisiko verringern kann.

Mit einem zertifizierten ISMS können sich Organisationen vom Wettbewerb absetzen oder in einen reglementierten Markt eintreten, der die Vorlage eines ISO/IEC 27001-Zertifikats verlangt.

Da sich Märkte und Anforderungen bewegen und immer häufiger den Nachweis zu bestimmten Standards fordern, sind Organisationen mit einem international anerkannten ISO/IEC 27001-Zertifikat bestens gerüstet, auch in Zukunft neue Anforderungen schnell zu erfüllen und die Einhaltung nachzuweisen.

3. Kriterienkatalog

Für eine ISO/IEC 27001-Auditierung und -Zertifizierung stellt die internationale Norm ISO/IEC 27001 den Kriterienkatalog dar.

4. Auditierungs- und Zertifizierungsprozess

Zunächst wird in diesem Abschnitt vorgestellt, wie die datenschutz cert GmbH ein Informationssicherheits-Managementsystem (ISMS) auditiert und zertifiziert.

4.1. Laufzeiten

Jedes Zertifikat ist (i.d.R.) drei Jahre gültig. Jedes Zertifizierungsverfahren besteht aus den folgenden Phasen:

- Erst-Zertifizierung;
- 1. Überwachungsaudit (max. 12 Monaten nach Zertifikatserteilung);
- 2. Überwachungsaudit (max. 24 Monaten nach Zertifikatserteilung);
- Re-Zertifizierung (max. 36 Monaten nach Zertifikatserteilung).

Es wird ein zweistufiges Zertifizierungsverfahren eingesetzt:

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



4.2. Erst-Zertifizierung

Das Erst-Zertifizierungsaudit spaltet sich auf in

- Vorbereitung,
- Stage 1-Audit und
- Stage 2-Audit,

woran sich dann die Zertifizierung anschließt, sofern das Auditteam die Zertifizierung empfiehlt.

4.2.1. Vorbereitung

Im Rahmen der Vorbereitung stellen Sie der Zertifizierungsstelle die vollständige ISMS-Referenzdokumentation zur Verfügung, dies umfasst insbesondere

- eine Darstellung des ISMS insgesamt samt Prozessdarstellung zum Management der Informationssicherheit,
- eine Darstellung der IT-Infrastruktur samt Netzstrukturplan mit Schutzbedarfsfeststellung und Übersichten über alle Assets,
- die Risikoanalyse,
- das Statement of Applicability (SOA), in der Sie darstellen, welche Anforderungen in Ihrem ISMS umgesetzt werden, sowie
- alle Leitlinien, Richtlinien, Policies und Arbeitsanweisungen, aus denen Ihre Umsetzung der normativen Vorgaben ersichtlich wird.

Beachten Sie bitte, dass es aufgrund behördlicher Vorgaben erforderlich ist, dass Ihre vollständige Referenzdokumentation sowie sämtliche Nachweise der Zertifizierungsstelle vorliegen.

4.2.2. Stage 1-Audit

Das Stage 1-Audit besteht aus einer Sichtung der Referenzdokumente und einer Kurz-Beurteilung vor Ort:

- Ziel des Treffens vor Ort ist es, sich und den Standort und standortspezifische Bedingungen kennenzulernen. Des Weiteren werden der Zeitplan und das weitere Audit mit Ihnen 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 und dokumentiert 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.
- Darüber hinaus werden stichpunktartig Aspekte der Norm geprüft

Im Ergebnis soll durch das Stage 1-Audit festgestellt werden, ob das Zertifizierungsverfahren mit dem Stage 2-Audit fortgeführt werden kann.

Das Stage 1-Audit findet typischerweise nur bei Erst-Zertifizierungsverfahren Anwendung.

4.2.3. Stage 2-Audit

Das Ziel des Stage 2-Audits ist es, die Umsetzung einschließlich der Wirksamkeit Ihres Informationssicherheits-Managementsystems hinsichtlich der Konformität zum Regelwerk zu beurteilen.

Das Audit besteht aus der Dokumentenprüfung sowie dem Vor-Ort-Audit (Site Visit):

- Für jeden Aspekt der Norm prüft und dokumentiert der Auditor, wie Sie lt. Dokumentation diesen Aspekt der Norm umsetzen. 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 Aspekt der Norm ISO/IEC 27001 prüft der Auditor beim Stage 2-Audit den Umsetzungsgrad der in der Dokumentation angegebenen Maßnahmen und dokumentiert die Ergebnisse der Prüfung im Auditreport. Dazu nimmt der Auditor entsprechende objektive Nachweise auf.
- Zudem prüft und bewertet der Auditor Ihr ISMS dahingehend, ob die Anforderungen an ein ISMS mit vollständigem PDCA-Zyklus umgesetzt werden.
- Etwaige Abweichungen werden aufgenommen; dazu gibt es vier Abstufungen:
 1. Anforderungen der Norm sind erfüllt;
 2. Anforderungen der Norm sind erfüllt, es besteht jedoch Verbesserungspotential (Verbesserungspotential);
 3. Abweichung von mind. einer Normanforderung, die in ihrer Geringfügigkeit die Funktionsfähigkeit des ISMS insgesamt nicht in Frage stellt (Nebenabweichung/ Minor Non-Conformities);
 4. Abweichung von einer Normanforderung, die grundsätzlich die Funktionsfähigkeit des ISMS in Frage stellt (Hauptabweichung/ Major Non-Conformities).

Bei Nebenabweichungen kann das Zertifikat mit Auflagen erteilt werden; hierzu wird eine Frist zur Umsetzung vereinbart, und es sind entsprechende Unterlagen nachzureichen.

Bei Hauptabweichungen ist ein Nachaudit notwendig mit entsprechender Dokumentenprüfung und erneutem Site Visit. Auch hierzu wird mit Ihnen ein Zeitraum zur Beseitigung festgelegt.

Die Auditierung wird strikt unabhängig von jeglicher Beratung durchgeführt.

4.2.4. Zertifizierung

Auf Grundlage des Auditreports sowie weiterer relevanter Informationen und Nachweise trifft die Zertifizierungsstelle final die Entscheidung, ob das ISMS Norm-konform betrieben wird und erteilt dann ein Zertifikat: Dieses Zertifikat bescheinigt dem

Antragsteller, dass das ISMS für den im Zertifikat ausgewiesenen Geltungsbereich den Anforderungen des Regelwerks angemessen genügt.

Auditierung und Zertifizierung werden strikt unabhängig voneinander durchgeführt.

4.3. Überwachungsaudit

Nach Erteilung Ihres Zertifikats ist jährlich ein Überwachungsaudit zur Aufrechterhaltung des Zertifikats durchzuführen, in denen die Wirksamkeit Ihres Informations-sicherheits-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, das sich im Wesentlichen an der Erst-Zertifizierung orientiert und zusätzlich die kontinuierliche Wirksamkeit Ihres 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. Anerkennung existierender Zertifikate

Die datenschutz cert GmbH bietet die Zertifizierung eines ISMS, für welches bereits ein IT-Grundschutz-Zertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) existiert, mit einem ISO/IEC 27001-Zertifikat unter Anerkennung des ISO/IEC 27001 / IT-Grundschutz-Zertifikats an. Vorteile:

- internationale Anerkennung;
- die ISO/IEC 27001-Zertifizierung wird zu günstigeren Konditionen angeboten: Es ist zwar keine Abweichung vom Auditprozess gemäß ISO/IEC 27006 möglich, aber eine deutliche Verringerung des Zeitaufwands, da diejenigen Aspekte, die bereits vollumfänglich durch IT-Grundschutz im Rahmen des IT-Grundschutz-Audits vor Ort überprüft wurden, nicht noch einmal geprüft werden.

4.7. Zertifikatsliste

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

4.8. 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.

4.9. 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.

4.10. 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 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 beachten 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.

4.11. 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>.

4.12. AGB und KBP

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.

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 DSN Group. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der DSN Group 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 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.

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 zertifiziert 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 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.

5.2. Anerkennungen und 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. Darüber hinaus umfasst die DAkKS-Akkreditierung das Regelwerk „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“ für Strom- und Gasnetzbetreiber sowie das Regelwerk „IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG“ für Energieanlagenbetreiber.

Ferner ist die datenschutz cert GmbH bei der DAkKS für Produkte und Dienstleistungen gemäß ISO/IEC 17065 akkreditiert und darf danach als Konformitätsbewertungsstelle Vertrauensdienste gemäß eIDAS prüfen und bewerten. Die Akkreditierung gem. ISO/IEC 17065 umfasst auch Videosprechstunden (ips-VSS-IT).

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 und IT-Sicherheitsdienstleister beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschatz-Auditoren und IS-Revisionen. 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-Grundschatz-Verfahren durchführt.

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

Aufgrund der Akkreditierung bei der DAkKS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a BSIG/KRITIS-VO-Verfahren die Rolle der „prüfenden Stelle“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer für § 8a BSIG anerkannt; dies umfasst auch die Prüfung von Systemen zur Angriffserkennung (SZA).



datenschutz
■ ■ ■ cert

datenschutz cert GmbH

Hauptsitz Bremen

Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: +49 421 69 66 32-550

Standort Offenbach

Mainstraße 143
63065 Offenbach am Main
Tel.: +49 69 870 07 83-580

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