Häufig gestellte Fragen zur Zertifizierung nach dem IT-Sicherheitskatalog

FAQ

IT-Sicherheitskatalog

DEKRA Alles im grünen Bereich

Sie möchten eine effiziente und stabile digitale Netzsteuerung in Ihrem Unternehmen etablieren? In unseren FAQs haben wir die häufigsten Fragen und Antworten zur Zertifizierung nach dem IT-Sicherheitskatalog für Sie zusammengefasst.

1. Was ist der IT-Sicherheitskatalog gemäß § 11 Absatz 1b EnWG der Bundesnetzagentur (BNetzA)?

Die Zunahme der dezentralen Stromerzeugung, sowohl durch erneuerbare Energien als auch durch Privathaushalte mit eigener Stromerzeugung, erhöht die Anforderungen an die digitale Netzwerksteuerung erheblich.

Um Netzwerkverantwortlichen eine optimale Grundlage für den Betrieb eines effizienten und stabilen Netzsystems bieten zu können, ist jedoch der permanente Austausch großer Datenmengen in Echtzeit notwendig.

Dabei sind vor allem stabile und sichere Informations- und Kommunikationstechnologien (IKT) von Bedeutung. Um dies zu gewährleisten, hat die Regierung zahlreiche Gesetze und Verordnungen verabschiedet, die dafür sorgen, dass die IKTs der Unternehmen angemessen vor Bedrohungen geschützt werden. Speziell für Strom- und Gasnetzbetreiber wurde der IT-Sicherheitskatalog (IT-SiKat) entwickelt, der das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz) um zusätzliche Anforderungen ergänzt.

2. Was sind die Anforderungen des IT-Sicherheitskatalogs?

Als Mindeststandard fordert der IT-Sicherheitskatalog von Unternehmen das Betreiben eines geeigneten Informationsmanagementsystems (ISMS) gemäß ISO 27001, welches um spezifische Faktoren der Netzsteuerung gemäß ISO 27019 erweitert werden muss. Der Nachweis hierfür ist über eine entsprechende Zertifizierung zu erbringen. Des Weiteren ist der Bundesnetzagentur eine Kontaktstelle für IT-Sicherheit mitzuteilen.

3. Für wen gilt der IT-Sicherheitskatalog?

Der IT-Sicherheitskatalog der Bundesnetzagentur gilt für alle Betreibenden eines Energieversorgungsnetztes im Bereich Strom und Gas, unabhängig von ihrer Größe oder der Anzahl der belieferten Kunden und Kundinnen.

4. Wie sorgt der IT-Sicherheitskatalog für mehr Sicherheit?

Das Ziel des IT-Sicherheitskatalogs ist es, einen stabilen und sicheren Netzbetrieb zu gewährleisten, indem wichtige Informations- und Telekommunikationstechnologien der Energiebetreibenden angemessen vor Bedrohungen geschützt werden.

Folgende Schutzziele werden hierfür im IT- Sicherheitskatalog definiert:

- Gewährleistung der Vertraulichkeit der Informationen, die mit den betrachteten Systemen verarbeitetet wurden
- Sicherstellung der Verfügbarkeit der zu schützenden Daten und Systeme
- Sicherstellung der Integrität der verarbeiteten Informationen und Systeme

5. Ist eine Zertifizierung nach BSI Grundschutz oder ISO 27001 ausreichend?

Nein. Diese Zertifizierungen allein sind nicht ausreichend, da sie die spezifischen Anforderungen für Energiebetreibende unberücksichtigt lassen. Unsere Sachverständigen informieren Sie hierzu gern.

6. Welche Vorteile hat eine Zertifizierung durch DEKRA für mein Unternehmen?

Mit unserer Zertifizierung nach dem IT-Sicherheitskatalog bieten wir Ihnen eine Vielzahl von Vorteilen:

- Erfüllung der gesetzlich vorgeschriebenen Norm
- Minimierung von Haftungsrisiken
- Schutz vor unberechtigten Zugriffen auf Ihre Informations- und Telekommunikationssysteme
- Steigerung der Produktivität durch optimierte Prozesse
- Verbesserung des Unternehmensimages nach außen
- Stärkung der Vertrauenswürdigkeit bei allen Beteiligten

7. Muss ich auch Teile meines Systems zertifizieren lassen, die durch externe Dritte betrieben werden?

Ja. Sie tragen die Verantwortung für all Ihre Anwendungen, Systeme und Komponenten, die vom IT-Sicherheitskatalog betroffen sind, auch wenn diese von externen Dritten betrieben werden. Dies bezieht sich auf den Betrieb aller Systeme und Anlagen mit Gefährdungspotential, Anschluss an das Leitsystem oder das Internet.

Sie vereinbaren in diesem Fall mit Ihren externen Dienstleistungsunternehmen vertraglich, dass diese sich an die Sicherheitsvorschriften gemäß des IT-Sicherheitskatalogs halten.

8. Wie läuft die Zertifizierung meines Unternehmens ab?

1. **Geltungsbereich des ISMS definieren**
   Erstellung eines Maßnahmenplans auf der Grundlage eines (selbst durchgeführten) internen Audits und des Geltungsbereichs. Sowie anschließende Erstellung einer Anwendbarkeitserklärung zum Annex A der ISO 27001 und den Forderungen der ISO 27019 durch die Kunden und Kundinnen.

2. **Audit**
   Durchführung des Zertifizierungsaudits, bei dem die Anforderungen aus der ISO 27001, Anforderungen aus dem IT-Sicherheitskatalog und aus der ISO 27019 überprüft werden

3. **Auditbericht**
   Dokumentation des Audits und Bewertung des Managementsystems

4. **Zertifikat**
   Nach erfolgreich abgeschlossener Zertifizierung erhalten Sie Ihr Zertifikat (mit maximal drei Jahren Laufzeit)

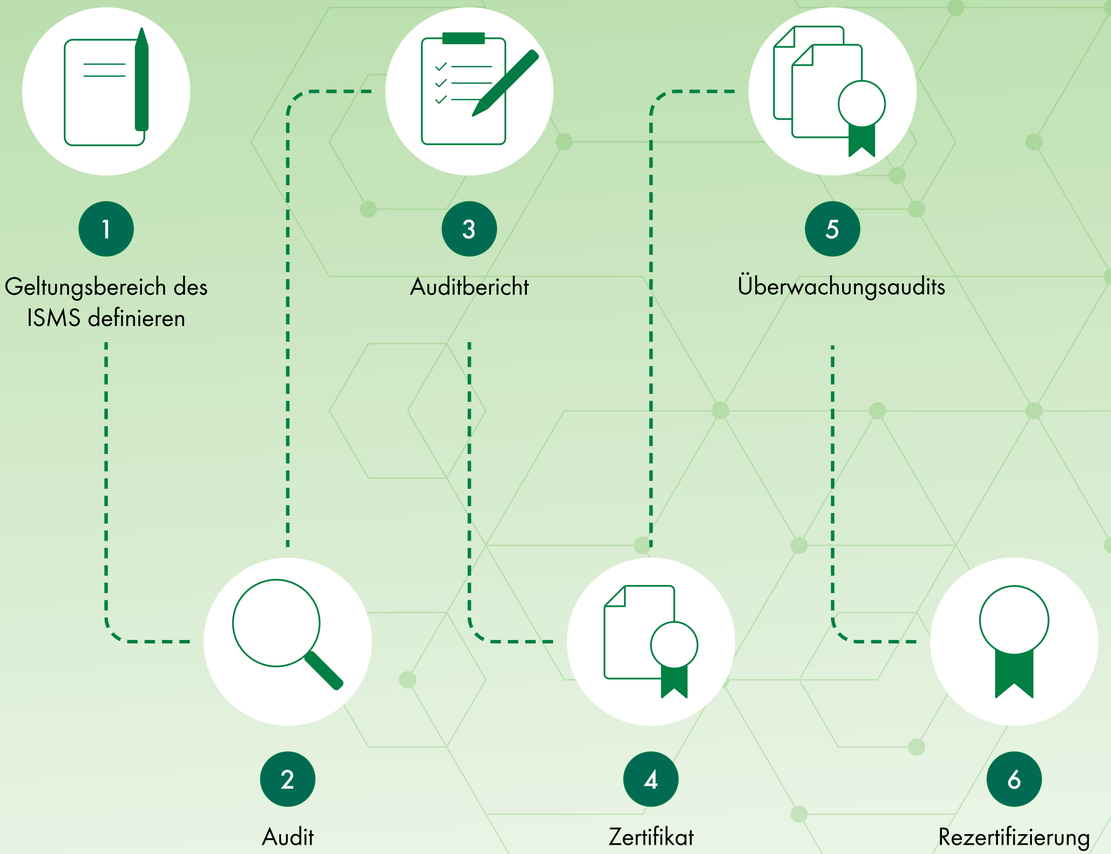
5. **Überwachungsaudits**
   Alle 12 Monate findet ein Überwachungsaudit statt

6. **Rezertifizierung**
   Vor Ablauf von drei Jahren nach der Erstzertifizierung werden im Rezertifizierungsaudit die Schritte 2 bis 6 wiederholt

Sie haben weitere Fragen zur Zertifizierung nach dem IT-Sicherheitskatalog? Dann kontaktieren Sie uns!

→ Kontaktieren Sie uns!

Erfolgreich zur
Zertifizierung
nach ***IT-Sicherheitskatalog***



Wünschen Sie weitere Informationen?
Besuchen Sie unsere Website:

dekra-certification.de