



# Zertifizierung nach IT-Sicherheitskatalog

Im August 2015 hat die Bundesnetzagentur (BNetzA) den IT-Sicherheitskatalog auf der Grundlage von § 11 Abs. 1a des Energiewirtschaftsgesetzes (EnWG) veröffentlicht. Durch diesen sind Strom- und Gasnetzbetreiber verpflichtet, die Anforderungen des IT-Sicherheitskatalogs zu erfüllen. Hierdurch sind sie aufgefordert ein Informationssicherheits-Managementsystem (ISMS) gemäß der DIN ISO/IEC 27001 aufzubauen und zertifizieren zu lassen. Durch die Veröffentlichung ergeben sich Fragen für Unternehmen: Welche Änderungen gibt es? Was muss beachtet werden?

## **SICHERE NETZBETRIEBE MIT EINER IT-SICHERHEITS-KATALOG-ZERTIFIZIERUNG**

Mit einer Zertifizierung nach IT-Sicherheitskatalog gewährleisten Netzbetreiber einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme. Dieser Schutz dient nicht nur

der eigenen Technologie, sondern auch der Sicherstellung der Energieversorgung der Bevölkerung. Da unsere Gesellschaft in hohem Maße von deren Funktionalität abhängig ist, würde das öffentliche Leben ohne Strom und Gas innerhalb kürzester Zeit zum Erliegen kommen und lebensnotwendige Dienstleistungen könnten nicht erbracht werden.

## VERANTWORTLICHKEIT FÜR DIE UMSETZUNG DES IT-SICHERHEITSKATALOGS

Verantwortlich für die Umsetzung des IT-Sicherheitskatalogs ist der eingetragene Betreiber des Strom- oder Gasnetzes. Das gilt auch für den Fall, dass der Netzbetreiber Anwendungen, Systeme oder Komponenten durch externe Dienstleister betreiben lässt. Durch entsprechende vertragliche Vereinbarungen muss er sicherstellen, dass der beauftragte Dienstleister sich an die vorgegebenen Anforderungen des IT-Sicherheitskatalogs hält. Wird von einem Strom- oder Gasnetzbetreiber keines der vom IT-Sicherheitskatalog erfassten Systeme betrieben, handelt es sich also um Systeme ohne Gefährdungspotential, besteht keine Umsetzungspflicht und es ist keine Zertifizierung nötig. Allerdings muss diese Situation mit einem begründeten Nachweis belegt werden.

## ZIELE DES IT-SICHERHEITSKATALOGS

Der IT-Sicherheitskatalog hat zum Ziel, die Verfügbarkeit und Integrität der zu schützenden Systeme und Daten sicherzustellen und die Vertraulichkeit der verarbeiteten Informationen in Bezug auf den sicheren Netzbetrieb zu gewährleisten. Die Ziele werden im IT-Sicherheitskatalog dabei wie folgt beschrieben:

- **Sicherung:** IT- und Kommunikationstechnik, die den Netzbetrieb sicherstellen, sollen geschützt sein
- **Verfügbarkeit:** Systeme und Daten sollen auf Verlangen einer berechtigten Einheit zugänglich und nutzbar sein
- **Integrität:** Richtigkeit und Vollständigkeit der verarbeiteten Daten und korrekte Funktionsweise der Systeme
- **Vertraulichkeit:** Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse

## VORTEILE EINER ZERTIFIZIERUNG NACH IT-SICHERHEITSKATALOG

Mit einer Zertifizierung nach IT-Sicherheitskatalog erfüllen Sie nicht nur alle notwendigen Anforderungen sondern sichern sich auch Wettbewerbsvorteile:



Erfüllung der Anforderungen des IT-Sicherheitskatalogs gem. § 11 Abs. 1a EnWG



Erhalt eines gesetzlich vorgeschriebenen Zertifikats



Sicherstellung Ihrer zu schützenden Systeme und Daten



Prozessverbesserung und Produktivitätssteigerung



Reduzierung der Haftungsrisiken



Wettbewerbsvorteil



Imagesteigerung in der Öffentlichkeit und bei Geschäftspartnern



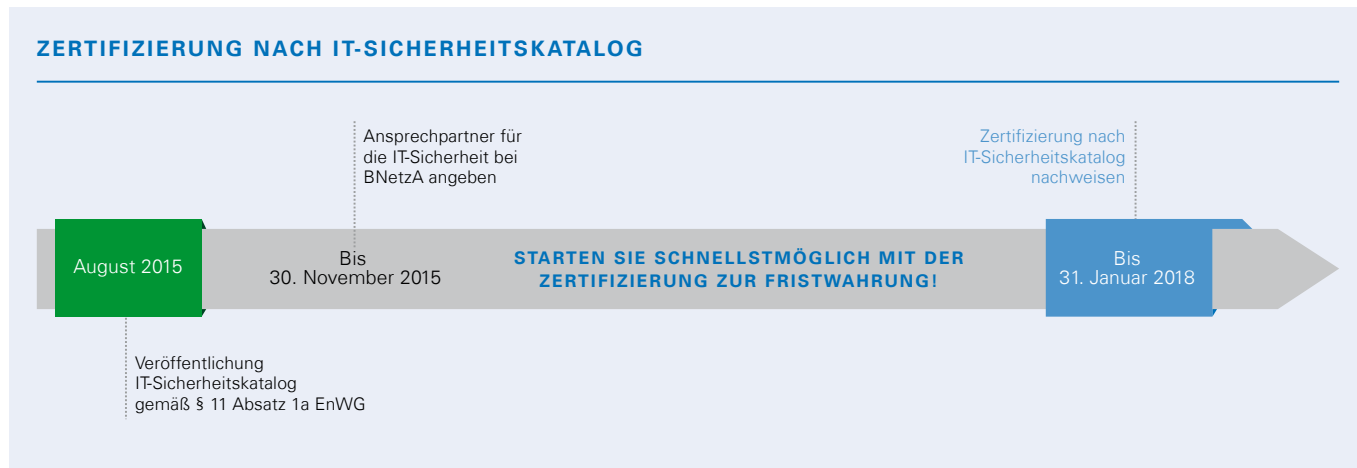
Erfüllung der Kundenerwartungen

## EINZUHALTENDE FRISTEN

Seit dem 30. November 2015 muss der Bundesnetzagentur vom Energienetzbetreiber ein Ansprechpartner für die IT-Sicherheit angegeben werden, der für die Kommunikation bei auftretenden Sicherheitsvorfällen zuständig ist. Das Formular für die Übermittlung der Daten finden Sie

auf der [Seite der Bundesnetzagentur](#).

Bis spätestens 31. Januar 2018 muss die erfolgreiche Umsetzung der Anforderungen mit einer Zertifizierung nachgewiesen werden. Diese muss in Form einer Kopie des Zertifikats der Bundesnetzagentur vorliegen.



Beginnen Sie so früh wie möglich mit dem Zertifizierungsprozess, um die Frist der Bundesnetzagentur zu wahren.

**Wir empfehlen Ihnen die vorgelagerte Bestandsaufnahme mit einzubinden. Sprechen Sie uns an! Wir informieren Sie gern.**

## GELTUNGBEREICH DES IT-SICHERHEITSKATALOGS

Der IT-Sicherheitskatalog umfasst alle Anwendungen, Systeme und Komponenten, die für den sicheren Netzbetrieb nötig sind. Enthalten sind EDV- und Telekommunikations-Systeme, welche bei einem Ausfall direkt oder indirekt die Netzwerksicherheit gefährden. Auch wenn

relevante Anwendungen, Systeme und Komponenten nicht direkt vom Netzbetreiber betrieben werden, muss die Einhaltung der im IT-Sicherheitskatalog definierten Standards durch Vereinbarungen vom Netzbetreiber sichergestellt werden.

# Ablauf unserer IT-Sicherheitskatalog-Zertifizierung

Profitieren Sie von der langjährigen Erfahrung unserer Experten und lassen Sie sich durch uns nach dem Standard des IT-Sicherheitskatalogs zertifizieren.

## 1. Bestandsaufnahme (optional)

Vor Ort erfassen unsere Auditoren zunächst den Ist-Zustand. Es wird untersucht, in welchem Maße die Inhalte des IT-Sicherheitskatalogs bereits umgesetzt sind.

## 2. Zertifizierungsaudit Stufe 1 (Dokumentenprüfung)

Das Audit-Team prüft, inwieweit die Dokumentation den Anforderungen des IT-Sicherheitskatalogs entspricht. Das Team (Auditoren und Fachexperte) definiert und grenzt die Betriebsanforderungen ab. Dies geschieht in der Regel mit Ihnen und den Beratern gemeinsam.

## 3. Zertifizierungsaudit Stufe 2 (Prüfung der Umsetzung)

Unsere Auditoren prüfen mit aktiver Begleitung und Unterstützung eines Fachexperten die Umsetzung der festgelegten Schutzziele und die Vorgaben des IT-Sicherheitskatalogs. Wurden alle Kriterien erfüllt, erhält Ihr Unternehmen das Zertifikat.

## 4. Zertifikatserteilung

Nach erfolgreichem Zertifizierungsverfahren erhält Ihr Unternehmen das Zertifikat gem. IT-Sicherheitskatalog. Es bescheinigt, dass die Anforderungen des IT-Sicherheitskatalogs gem. § 11 Abs. 1a EnWG erfüllt sind. Darüber hinaus wird Ihr Unternehmen in unsere öffentliche Online-Zertifikatsdatenbank [Certipedia](#) aufgenommen und Sie können mit dem TÜV Rheinland

Siegel für Ihr zertifiziertes Qualitätsmanagement werben. Weitere Informationen in „[Werben mit TÜV Rheinland](#)“.

## 5. Jährliche Überwachungsaudits

Unsere jährlichen Überwachungsaudits unterstützen Sie dabei die Normanforderungen nachhaltig zu erfüllen.

## 6. Re-Zertifizierung

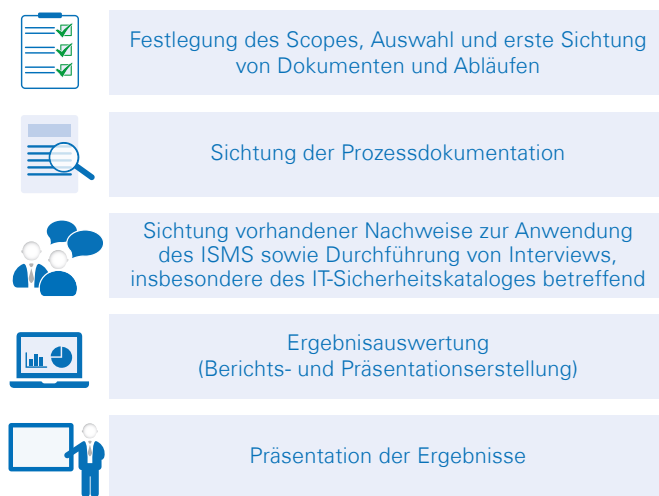
Mit der Re-Zertifizierung vor Ablauf von drei Jahren setzen Sie Ihren kontinuierlichen Verbesserungsprozess dauerhaft fort und dokumentieren Ihr Engagement gegenüber Partnern und Kunden.



## ABLAUF UND VORTEILE EINER BESTANDSAUFNAHME

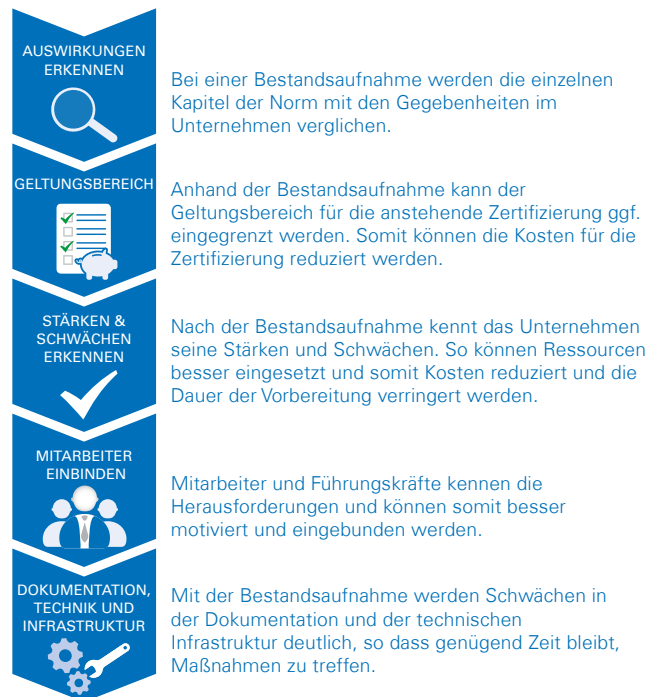
Wir empfehlen Ihnen sehr den Zertifizierungsprozess mit der optionalen Bestandsaufnahme zu beginnen. Diese bereitet Sie optimal auf die Zertifizierung vor und spart somit Zeit und Kosten. Die Bestandsaufnahme durchläuft fünf Schritte von der Sichtung Ihrer Dokumente bis zur Präsentation der Ergebnisse.

### ABLAUF EINER BESTANDSAUFNAHME



Durch die Bestandsaufnahmen vereinfachen Sie Ihren Zertifizierungsprozess, sparen Kosten ein und können notwendige Maßnahmen schneller und zielgerichteter umsetzen. Unseren Experten stehen Ihnen als kompetente Ansprechpartner zur Seite.

### VORTEILE EINER VORGELAGERTEN BESTANDSAUFNAHME



**SIE MÖCHTEN SICH ZERTIFIZIEREN LASSEN ODER HABEN WEITERE FRAGEN? UNSERE EXPERTEN STEHEN IHNEN MIT EINEM KOSTENFREIEN INFORMATIONSGESPRÄCH ZUR VERFÜGUNG. SPRECHEN SIE UNS HIERZU GERNE AN!**

Quelle: Bundesnetzagentur

[ONLINE KONTAKT](#)

TÜV Rheinland Group  
TÜV Rheinland Cert GmbH  
Am Grauen Stein  
51105 Köln  
Tel. +49 800 888 2378  
Fax. +49 800 888 3296  
tuvcert@de.tuv.com  
www.tuv.com/it-sicherheitskatalog



 **TÜVRheinland®**  
Genau. Richtig.