Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage der ISO/IEC 27006

Stand: 16. November 2017

**Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen**

Referate 606 (Strom) und 607 (Gas)

Tulpenfeld 4
53113 Bonn
Tel.: +49 228 14-0
Fax: +49 228 14-5966
E-Mail: it-sicherheitskatalog@bnetza.de

Inhaltsverzeichnis

1 Allgemeines

Die Zukunft der Energieversorgung ist in zunehmendem Maße von einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig. Die Unterstützung durch diese Technologie bringt viele Vorteile, mit der wachsenden Abhängigkeit von diesen Systemen gehen jedoch auch Risiken für die Versorgungssicherheit einher. Um die Vorteile moderner IKT auch in Zukunft sicher nutzen zu können, ist es wichtig, einen angemessenen Schutz gegen Bedrohungen für IKT-Systeme, die für einen sicheren Netzbetrieb notwendig sind, zu etablieren. Dies soll u. a. durch den von der Bundesnetzagentur am 12. August 2015 veröffentlichten IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG) erreicht werden, dessen Anforderungen von allen Strom- und Gasnetzbetreibern in Deutschland bis zum 31. Januar 2018 umzusetzen sind.

Der Nachweis über die Umsetzung der Anforderungen des IT-Sicherheitskatalogs erfolgt durch die Zertifizierung und Vorlage des Zertifikats bei der Bundesnetzagentur. Seitens der Bundesnetzagentur sind über die Zertifizierung hinaus keine weiteren Prüfungen oder Nachweise vorgesehen. Daher ist es notwendig, ein einheitliches, gleichbleibend hohes und vergleichbares Qualitätsniveau der Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG sicherzustellen. Dies soll über die Akkreditierung der Zertifizierungsstellen bei der Deutschen Akkreditierungsstelle (DAkkS) gewährleistet werden.

Die Anforderungen, deren Erfüllung eine Zertifizierungsstelle für eine Akkreditierung nachweisen muss, richten sich nach diesem Konformitätsbewertungsprogramm. Wenn Zertifizierungsstellen eine Akkreditierung für die Zertifizierung des IT-Sicherheitskatalogs beantragen, wird die Umsetzung der Vorgaben im Rahmen des Begutachtungs- und Akkreditierungsverfahrens der DAkkS überprüft.

2 Grundlage für das Konformitätsbewertungsprogramm

Die Grundlage für die Zertifizierung ist der IT-Sicherheitskatalog der Bundesnetzagentur gemäß § 11 Absatz 1a EnWG.

Für die Zertifizierung gelten folgende Konkretisierungen:

1. Das Risikomanagement der Organisation gemäß Abschnitt 6.1.3 und 8 der DIN ISO/IEC 27001 muss auch sämtliche Maßnahmen der ISO/IEC 27019:2017 berücksichtigen, d. h. der Begriff „Anhang A“ in Abschnitt 6.1.3 ist als „Anhang A sowie sämtliche Maßnahmen der ISO/IEC 27019:2017“ zu verstehen.[1] Die in den Normen[2] genannten Maßnahmen sind also nicht zwingend vollständig umzusetzen, aber im Rahmen des Risikomanagements vollständig auf ihre Relevanz zu prüfen.[3]

2. Sofern Teile des zu zertifizierenden Informationssicherheits-Managementsystems (ISMS) nicht unter den Geltungsbereich der ISO/IEC 27019:2017 fallen (z. B. solche Systeme, die zwar in der Leitstelle Informationen für Schaltentscheidungen bereitstellen, aber technisch nicht mit den unter die ISO/IEC 27019:2017 fallenden Systemen verbunden sind), gilt für diese Teile die ISO/IEC 27019:2017 nicht, d. h. insoweit gilt insbesondere Nr. 1 nicht.

3 Anforderungen an die Zertifizierungsstellen

Die ISO/IEC 27006 legt als internationale Norm ergänzend zur ISO/IEC 17021-1 die Anforderungen an Zertifizierungsstellen fest, die ISMS auditieren und zertifizieren. Sie gilt auch für die Akkreditierung der Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG. Das bedeutet, die nach dieser Anleitung akkreditierten Zertifizierungsstellen müssen die Anforderungen der ISO/IEC 27006 sowie der ISO/IEC 17021-1 in der jeweils durch die DAkkS für gültig erklärten Fassung erfüllen, soweit das vorliegende Dokument keine hiervon abweichenden Regelungen enthält.

Die Zertifizierungsstellen sind verpflichtet, der Bundesnetzagentur eine Liste der Unternehmen, die ein Zertifikat erhalten haben, zu übermitteln. Die Liste ist jeweils zum 30. Juni und zum 31. Dezember eines Jahres elektronisch im XLSX-Dateiformat an die E-Mail-Adresse it-sicherheitskatalog@bnetza.de zu übermitteln. Die Liste muss dem Format gemäß Tabelle 1 entsprechen.

---

[1] Hierbei ist darauf zu achten, dass analog zu den Maßnahmen im Anhang A der DIN ISO/IEC 27001 bei den aus der ISO/IEC 27019:2017 stammenden Maßnahmen das Wort "sollte" durch "muss" bzw. "ist" zu ersetzen ist.

[2] Soweit deutsche Übersetzungen der ISO/IEC-Normen in ihrer jeweils aktuellen Fassung noch nicht vorliegen, sind die jeweils aktuellen ISO/IEC-Normen selbst zu berücksichtigen.

[3] Hierbei ist zu beachten, dass die ISO/IEC 27006 keine Vorgehensweise für das Risikomanagement vorgibt. So ist z. B. auch die Anwendung des IT-Grundschutzes des BSI möglich, sofern dabei die Anforderungen des IT-Sicherheitskatalogs eingehalten werden.

Tabelle 1: Liste der zertifizierten Netzbetreiber

Netzbetreiber-nummer	Zertifikats-nummer	Unternehmensbezeichnung	Gegenstand der Zertifizierung	Datum des Zertifikats	Ablaufdatum des Zertifikats
10012340	1345xyz	Musterstadt Netz GmbH	Stromnetz	01.01.2017	31.12.2019
10045609	14412tt4	Gemeindew erke Kleinstadt GmbH	Strom- und Gasnetz	01.01.2017	31.12.2019

Die auszustellende Zertifizierungsurkunde hat dem als Anlage 1 beigefügten Muster zu entsprechen.[4]

Die Zertifizierungsstelle hat innerhalb eines Zertifizierungszyklus stichprobenartig alle im Rahmen der Risikoeinschätzung mindestens als "hoch" eingestuften Anwendungen, Systeme und Komponenten mindestens einmal zu auditieren.

Die Zertifizierungsstelle muss für einen Informationsaustausch unter den von ihr beschäftigten Auditoren sorgen. Hierzu gehört auch ein mindestens einmal jährlich stattfindender Erfahrungsaustausch.

Die Zertifizierungsstelle muss die von ihr zertifizierten Organisationen auf eine rechtzeitige Einleitung des Rezertifizierungsverfahrens hinweisen.

Die Zertifizierungsstelle ist verpflichtet, das Zertifikat zu jeder Zeit während der Gültigkeitsdauer auszusetzen oder zurückzunehmen, wenn sie Kenntnis davon erlangt, dass die Zertifizierungsvoraussetzungen bei einem Netzbetreiber vorübergehend oder dauerhaft nicht mehr vorliegen. Das Zertifikat ist z. B. auszusetzen, wenn die antragstellende Organisation notwendige Korrekturmaßnahmen während der vereinbarten Frist nicht durchgeführt hat. Die Zertifizierungsstelle muss die Bundesnetzagentur unverzüglich über die Aussetzung bzw. Rücknahme des Zertifikats mit E-Mail an it-sicherheitskatalog@bnetza.de informieren. Sofern die Bundesnetzagentur ihrerseits Kenntnis davon erlangt, dass die Zertifizierungsvoraussetzungen bei einem Netzbetreiber vorübergehend oder dauerhaft nicht mehr vorliegen, leitet sie diese Information an die betreffende Zertifizierungsstelle weiter.

4 Anforderungen an die Auditoren

Abschnitt 7.1 der ISO/IEC 27006:2015 definiert die grundlegenden Anforderungen an die Auditoren, welche auch im Rahmen dieser Akkreditierungsanleitung gelten. Zusätzlich zu den dort genannten Anforderungen müssen alle Auditoren eine von der Bundesnetzagentur anerkannte Schulung zu den Grundlagen der leitungsgebundenen Energieversorgung mit Strom und Gas erfolgreich absolvieren. Die erfolgreiche Teilnahme an der Schulung ist am Schulungsende im Rahmen einer Prüfung nachzuweisen und wird bei Bestehen durch den Schulungsanbieter schriftlich bestätigt. Die Bundesnetzagentur veröffentlicht eine Liste der anerkannten Schulungen auf ihrer Internetseite.

Die Schulung muss einschließlich Prüfung mindestens sechs Tage umfassen und mindestens die folgenden Inhalte abdecken:

[4] Vgl. Beschluss "B SK IT-IS-DS 10/2017" des DAkkS-Sektorkomitees Informationstechnik - Informationssicherheit - Datenschutz.

- Rechtliche Rahmenbedingungen und Anforderungen in der Energiewirtschaft (insbesondere Unbundling),
- Technische Grundlagen der Strom- und Gasversorgung,
- Grundlagen für den Netzbetrieb,
- Netzsteuerung, Dispatching

und als Schulungsschwerpunkt

- IT-Kritische Infrastrukturen für den Netzbetrieb - Scope des ISMS nach IT-Sicherheitskatalog.

Die detaillierten Schulungsinhalte und deren zeitliche Gewichtung werden zwischen der Bundesnetzagentur und dem Schulungsanbieter im Rahmen der Anerkennung abgestimmt, um ein einheitliches Schulungsniveau sicherzustellen.

Für die Prüfung des Geltungsbereichs des ISMS (Scope) und der Risikoeinschätzung gemäß IT-Sicherheitskatalog muss das Audit-Team einen Fachexperten hinzuziehen. Der Fachexperte soll das Audit-Team bei der Einschätzung, ob alle für den Netzbetrieb notwendigen Systeme, Komponenten und Anwendungen im Scope erfasst sind und die Risikoeinschätzung korrekt durchgeführt worden ist, beraten. Die Beratung während des Audits erfordert die Anwesenheit des Fachexperten und dessen Austausch mit dem Auditteam beim Netzbetreiber vor Ort. Dafür muss er insbesondere über fundiertes Wissen und Erfahrungen in den von der o. g. Schulung umfassten Themenbereichen verfügen. Der Fachexperte muss neben einem ingenieur- oder naturwissenschaftlichen (Fach-)Hochschulstudium mindestens drei Jahre einschlägige Berufserfahrung in der leitungsgebundenen Energieversorgung[5] nachweisen. Die Unterstützung durch einen Fachexperten kann entfallen, sofern ein Mitglied des Audit-Teams bereits mindestens fünf Mal zusammen mit einem Fachexperten im Rahmen von Audits zur Zertifizierung des IT-Sicherheitskatalogs gemäß § 11 Absatz 1a EnWG die Risikoeinschätzung und den Scope des ISMS eines Netzbetreibers beurteilt hat. Erfüllt ein Mitglied des Audit-Teams selbst die Anforderungen an die Qualifikation des Fachexperten, so ist es dem Fachexperten gleichgestellt.

5 Auditumfang

Die Anforderungen der ISO/IEC 27006 sowie der ISO/IEC 17021-1 bezüglich der Auditdauer und der Wahl von Stichproben sowie der entsprechenden DAkkS-Regeln gelten, ergänzt um die folgenden Anforderungen.

1. Nicht dauerhaft besetzte Betriebsstätten sind durch geeignete Gruppenbildung zusammenzufassen. Bei der Gruppenbildung ist die Relevanz der Standorte für das Gesamtnetz sowie die Möglichkeit der Ferneinwirkung über IKT auf diesen Standort zu berücksichtigen.

2. Eine Betriebsstätte, die Teil des Scopes ist, gilt als Standort im Sinne der ISO/IEC 27006:2015 Abschnitt 9.1.5.1, sofern sie zumindest an regulären Arbeitstagen mit Personal besetzt ist.

[5] Es ist nicht erforderlich, dass der Fachexperte die mindestens dreijährige Berufserfahrung in einem Anstellungsverhältnis bei einem leitungsgebundenen Energieversorgungsunternehmen erworben hat. Es genügt auch, wenn die notwendige Berufserfahrung außerhalb eines solchen Anstellungsverhältnisses erworben wurde, sofern die berufliche Tätigkeit geeignet war, vergleichbare Fachkenntnisse über die leitungsgebundene Energieversorgung aufzubauen.

3. Es ist zulässig, bei der Auditierung eine Stichprobe der Standorte zu wählen. Hierbei sind die Vorgaben der ISO/IEC 27006:2015 Abschnitt 9.1.5.1 zu beachten. Zusätzlich sind im Rahmen der Audits von jeder Gruppe der nicht dauerhaft besetzten Betriebsstätten, die Teil des Scopes sind, je Zertifizierungszyklus mindestens zwei Betriebsstätten auf die Umsetzung der zutreffenden Maßnahmen der ISO/IEC 27019:2017 zu auditieren.

4. Ergänzend zu den Vorgaben der ISO/IEC 27006:2015 Abschnitt 9.1.5.1 ist bei der Wahl der Stichproben darauf zu achten, dass in der Gesamtheit der Stichproben eine gute netztopologische Abdeckung erzielt wird, also auch geographisch möglichst viele Teile des Scopes berücksichtigt werden.

5. Die Gesamtheit der Stichproben richtet sich nach folgenden Formeln:

- beim Erstzertifizierungsaudit: $Stichprobe = \sqrt{Alle\ Standorte}$
- beim Rezertifizierungsaudit: $Stichprobe = 0{,}8\ x\ \sqrt{Alle\ Standorte}$
- beim Überwachungsaudit: $Stichprobe = 0{,}6\ x\ \sqrt{Alle\ Standorte}$

Die so ermittelte Stichprobe ist auf die jeweils nächste ganze Zahl aufzurunden.

6. Für die Auditdauer gelten die Vorgaben von Anhang B der ISO/IEC 27006:2015. Die Formel zur Ermittlung der Auditdauer gemäß ISO/IEC 27006:2015 Anhang B.3.4 ist auf die besondere Situation der Netzbetreiber hin anzupassen, wobei neben den Standorten auch die Anzahl der nicht dauerhaftbesetzten Betriebsstätten zu berücksichtigen ist. In Abweichung zu ISO/IEC 27006:2015 Anhang B.3.5 ist eine Reduzierung der Auditdauer um höchstens 10 Prozent zulässig.

6 Übergangsregelung

Der IT-Sicherheitskatalog nach § 11 Absatz 1a EnWG verweist u. a. auf die DIN ISO/IEC TR 27019 (DIN SPEC 27019) in der jeweils geltenden Fassung. Soweit deutsche Übersetzungen der ISO-Normen in ihrer jeweils aktuellen Fassung noch nicht vorliegen, sind die jeweils aktuellen ISO-Normen selbst zu berücksichtigen.

Die bisherige ISO/IEC TR 27019:2013 wurde überarbeitet und im Oktober 2017 durch die ISO/IEC 27019:2017 ersetzt.

Für die Berücksichtigung der überarbeiteten Fassung im Rahmen der Zertifizierungsprozesse gilt folgende Übergangsregelung:

Audits zur Erst- oder Rezertifizierung und Überwachungsaudits im Rahmen des IT-Sicherheitskatalogs gemäß § 11 Absatz 1a EnWG haben spätestens ab dem 01.01.2021 verpflichtend unter Berücksichtigung der ISO/IEC 27019:2017 bzw. – sofern bis zu diesem Zeitpunkt vorliegend – unter Berücksichtigung der entsprechenden deutschen Übersetzung (DIN) zu erfolgen. Bei Audits zur Erst- oder Rezertifizierung und Überwachungsaudits kann bis zum 31.12.2020 alternativ die bisherige DIN ISO/IEC TR 27019:2015-03; DIN SPEC 27019:2015-03 berücksichtigt werden.

ANLAGE 1

Zertifikat

Die < KBS > bescheinigt hiermit,

dass das Informationssicherheits-Managementsystem (ISMS)

für den Geltungsbereich

< Betreiberspez. Bezeichnung>

(entsprechend dem Geltungsbereich des IT-Sicherheitskatalogs gem. §11 Absatz 1a EnWG (08/2015))

für den Antragsteller

<Netzbetreiber>

<Adresse>

Sparte Strom, Netzbetreibernummer (BNetzA): xxxxxxxx

Sparte Gas, Netzbetreibernummer (BNetzA): yyyyyyyy

auf Grundlage des Statements of Applicability,

Version <xx> vom <xx.xx.20xx>

die Anforderungen des folgenden Regelwerks erfüllt:

IT-Sicherheitskatalog gem. § 11 Absatz 1a EnWG (08/2015)

Zertifikats-ID: <xyz>

<LOGO, z.B.>

Letzter Audittag: <xx.xx.201x> Datum Zertifikat: <xx.xx.xxxx> gültig bis: <xx.xx.xxxx>

Siegel und Unterschrift mit Bezeichnung der Funktion – (Zertifizierungsstelle)