Bundesnetzagentur

Konformitätsbewertungsprogramm

zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog (für Anlagenbetreiber)

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

Stand: 12. Januar 2023

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen

Referat 627

Tulpenfeld 4
53113 Bonn
Tel.: +49 228 14-0
Fax: +49 228 14-8872
E-Mail: info@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 sicherheitsrelevante IKT-Systeme im Energiesektor zu etablieren. Dabei haben die Strom- und Gasnetze eine herausragende Bedeutung.[1] Nicht weniger wichtig ist aber auch der sichere Betrieb bestimmter Energieanlagen, wie beispielsweise größerer Erzeugungsanlagen. Letzterer soll unter anderem durch den von der Bundesnetzagentur am 19. Dezember 2018 veröffentlichten IT-Sicherheitskatalog gemäß § 11 Absatz 1bEnergiewirtschaftsgesetz (EnWG) erreicht werden. Dessen Anforderungen sind von allen Betreibern von Energieanlagen[2] in Deutschland, die als Kritische Infrastruktur im Sinne der BSI-Kritisverordnung[3] gelten, bis zum 31. März 2021 umzusetzen.

Der Nachweis über die Umsetzung der Anforderungen des IT-Sicherheitskatalogs erfolgt durch die Zertifizierung und Vorlage des Zertifikats bei der Bundesnetzagentur. Dabei ist es notwendig, ein einheitliches, gleichbleibend hohes und vergleichbares Qualitätsniveau der Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1b 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 dem vorliegenden 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.

---

[1] Vgl. IT-Sicherheitskatalog für Netze nach § 11 Abs. 1a EnWG (https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.html) und das zugehörige Konformitätsbewertungsprogramm für die Akkreditierung von Zertifizierungsstellen (https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/Konformitaetsbewertungsprogramm.html).

[2] Vgl. § 3 Nr. 15 Energiewirtschaftsgesetz: https://www.gesetze-im-internet.de/enwg_2005/__3.html.

[3] Vgl. Anhang 1 zur Verordnung: https://www.gesetze-im-internet.de/bsi-kritisv/anhang_1.html.

2 Grundlage für das Konformitätsbewertungsprogramm

Die Grundlage für die Zertifizierung ist der IT-Sicherheitskatalog der Bundesnetzagentur gemäß § 11 Absatz 1b EnWG. Darüber hinaus gelten die im Folgenden aufgeführten Normen[4]:

- DIN EN ISO/IEC 17011
- DIN EN ISO/IEC 17021
- DIN EN ISO/IEC 27001
- ISO/IEC 27006
- DIN EN ISO/IEC 27019

Für die Zertifizierung gelten folgende Konkretisierungen:

1. Das Risikomanagement der Organisation gemäß Abschnitt 6.1 und 8 der DIN EN ISO/IEC 27001 muss auch sämtliche Maßnahmen der DIN EN ISO/IEC 27019 berücksichtigen, das heißt der Begriff „Anhang A“ in Abschnitt 6.1.3 ist als „Anhang A sowie sämtliche Maßnahmen der DIN EN ISO/IEC 27019“ zu verstehen. Die in den Normen genannten Maßnahmen sind also nicht zwingend vollständig umzusetzen, aber im Rahmen des Risikomanagements vollständig auf ihre Relevanz zu prüfen.[5]

2. Sofern Teile des zu zertifizierenden Informationssicherheits-Managementsystems (ISMS) nicht unter den Geltungsbereich der DIN EN ISO/IEC 27019 fallen[6], gilt für diese Teile die DIN EN ISO/IEC 27019 nicht, das heißt insoweit gilt insbesondere Nr. 1 nicht.

Die Auditierung und Zertifizierung für dieses Konformitätsbewertungsprogramm der Bundesnetzagentur ist in jedem Fall getrennt von Auditierungen und Zertifizierungen für andere Normen – wie zum Beispiel DIN EN ISO 9001, DIN EN ISO/IEC 27001 – zu betrachten und zu dokumentieren sofern der Geltungsbereich maßgeblich abweicht. Die im Konformitätsbewertungsprogramm genannten Normen gelten jeweils in ihrer aktuellen Fassung, es sei denn das Konformitätsbewertungsprogramm legt abweichende Regelungen fest. In diesen Fällen hat das Konformitätsbewertungsprogramm Vorrang.

3 Anforderungen an das Akkreditierungsverfahren

Die Akkreditierung erfolgt nach der DIN EN ISO/IEC 17021-1. Ergänzend gelten hierfür alle verpflichtenden Dokumente des International Accreditation Forum (IAF) außer sie sind durch dieses Konformitätsbewertungsprogramm oder die zur Anwendung kommenden Normen ausgeschlossen.

Wenn Zertifizierungsstellen eine Akkreditierung für die Zertifizierung des IT-Sicherheitskatalogs gemäß § 11 Abs. 1b EnWG beantragen, wird die Umsetzung der Vorgaben im Rahmen des Begutachtungs- und

---

[4] 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.

[5] 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.

[6] Ein Beispiel hierfür sind solche Systeme, die zwar in der Leitstelle Informationen für Schaltentscheidungen bereitstellen, aber technisch nicht mit den unter die DIN EN ISO/IEC 27019 fallenden Systemen verbunden sind.

Akkreditierungsverfahrens der DAkkS überprüft. Hierfür sind alle aktuell geltenden Regeln der DAkkS gültig. Ergänzend sind folgende Regelungen zu beachten:

3.1 Geschäftsstellenbegutachtung

Im Rahmen der Geschäftsstellenbegutachtung während der Akkreditierung der Zertifizierungsstelle sind bei Überwachung und Wiederholungsbegutachtung mindestens 20% der durchgeführten Zertifizierungsverfahren als Stichprobe durch die Begutachtenden der DAkkS zu prüfen. Sollten bei Erstakkreditierung bereits Zertifizierungsverfahren bearbeitet worden sein, werden diese im Rahmen der Geschäftsstellenbegutachtung ebenfalls geprüft.

3.2 Durchführung von Witness-Audits

Das Durchführen eines Audits (Witness-Audit) ist eine Tätigkeit, die von der DAkkS gemäß DIN EN ISO/IEC 17011 ausgeführt werden muss. Die DAkkS behält sich dabei vor, festzulegen, welches Personal beziehungsweise welche Tätigkeiten im Zertifizierungsprozess einem Witnessing zu unterziehen sind. Der Umfang des erforderlichen Witnessing im Rahmen des Begutachtungsverfahrens wird durch die DAkkS nach folgenden Grundsätzen festgelegt:

- Für die Erst- und Wiederholungsbegutachtung einer Zertifizierungsstelle muss je Geltungsbereich mindestens ein Witness-Audit durchgeführt werden.
- Bei der anschließenden Überwachung der Akkreditierung im 5-jährigen Akkreditierungszyklus müssen Witness-Audits proportional zur Anzahl der für diese Norm ausgestellten Zertifikate und der durchgeführten Audittage erfolgen. Hierfür sind der DAkkS in Vorbereitung auf die Überwachungsbegutachtung die Anzahl der ausgestellten Zertifikate und die durchgeführten Audittage des Vorjahres zu melden. Im Akkreditierungszyklus zur Überwachung ist mindestens ein Witness-Audit zur Kompetenzfeststellung durchzuführen.

Witness-Audits dürfen in Abhängigkeit von weiteren Befunden und risikoorientierter Betrachtung jederzeit angeordnet werden.

4 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 1b 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 dieses Konformitätsbewertungsprogramm 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 und soll alle durch die jeweilige Zertifizierungsstelle bis zu diesem Zeitpunkt zertifizierten Unternehmen enthalten (fortlaufende Liste). Liegen zum letzten Übermittlungsstichtag keine Änderungen vor, ist dennoch

eine Meldung abzugeben. Die Liste muss dem Format gemäß Tabelle 1 entsprechen. Abgelaufene und ausgesetzte Zertifikate sind in der Tabelle gesondert hervorzuheben.

Tabelle 1: Liste der zertifizierten Anlagenbetreiber

Marktstammdaten-registernummer (MaStR-Nr.)	Zertifikats-ID	Anlagenbetreiber	Datum des Zertifikats	Ablaufdatum des Zertifikats
ABRxxxxxxxxxxxx	1345xyz	Gasspeicher GmbH	31.03.2021	30.03.2024
ABRxxxxxxxxxxxx	14412tt4	Kraftwerksbetreiber GmbH	31.03.2021	30.03.2024

Die auszustellende Zertifizierungsurkunde (Zertifikat) hat nach Layout, Aufbau und Inhalt dem als Anlage 1 beigefügten Muster zu entsprechen. Das Zertifikatsmuster muss vorab zur Prüfung bei der DAkkS eingereicht werden.

Die Zertifizierungsstelle hat innerhalb eines Zertifizierungszyklus 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 Auditorinnen und Auditoren sorgen. Hierzu gehört auch ein mindestens einmal jährlich stattfindender Erfahrungsaustausch. Die Auditorinnen und Auditoren müssen immer auf dem aktuellen Stand der Anforderungen und der Technik sein, um die Aufrechterhaltung der Kompetenz sicherzustellen. Hierbei sollte der Großteil der Veranstaltung (>70%) zur Wissensvermittlung dienen.

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 Betreiber einer Energieanlage vorübergehend oder dauerhaft nicht mehr vorliegen. Das Zertifikat ist zum Beispiel 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 per E-Mail an IT-Sicherheitskatalog@BNetzA.de informieren. Sofern die Bundesnetzagentur ihrerseits Kenntnis davon erlangt, dass die Zertifizierungsvoraussetzungen bei einem Anlagenbetreiber vorübergehend oder dauerhaft nicht mehr vorliegen, leitet sie diese Information an die betreffende Zertifizierungsstelle weiter.

Die Zertifizierungsstelle muss mindestens eine Fachexpertin / einen Fachexperten für die im IT-Sicherheitskataloge gemäß § 11 Abs. 1b EnWG genannten Anlagenkategorien nachweisen können, um in um in dem Bereich akkreditiert werden zu können

5 Anforderungen an die Auditorinnen und Auditoren

Abschnitt 7.1 der DIN ISO/IEC 27006 definiert die grundlegenden Anforderungen an die Auditorinnen und Auditoren, welche auch im Rahmen dieser Akkreditierungsanleitung gelten. Zusätzlich zu den dort genannten Anforderungen müssen alle Auditorinnen und Auditoren eine von der Bundesnetzagentur anerkannte Schulung zu den Grundlagen der Erzeugung und leitungsgebundenen Versorgung mit Strom und Gas („Vollschulung“) erfolgreich absolvieren.[7] Auditorinnen und Auditoren, die bereits in der Vergangenheit die Schulung nach dem Konformitätsbewertungsprogramm vom 12.08.2015 zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG („IT-Sicherheitskatalog für Netze“) erfolgreich absolviert haben, sind auch weiterhin dafür qualifiziert, um als Auditorin / Auditor im Rahmen der Zertifizierungsverfahren gemäß § 11 Absatz 1a EnWG tätig zu sein. Die erfolgreiche Teilnahme an der Vollschulung ist am Schulungsende im Rahmen einer Prüfung nachzuweisen und wird bei Bestehen durch den Schulungsanbieter schriftlich bestätigt. Das Bestehen der Vollschulung qualifiziert die Teilnehmerinnen und Teilnehmer für die Tätigkeit als Auditorinnen und Auditoren im Bereich der Zertifizierungsverfahren gemäß der IT-Sicherheitskataloge nach § 11 Absatz 1a EnWG sowie §11 Absatz 1b EnWG

Die Vollschulung muss einschließlich Prüfung mindestens fünf Tage umfassen und mindestens die folgenden Inhalte abdecken:

- Rechtliche Rahmenbedingungen in der Energiewirtschaft (insbesondere Entflechtung) und relevante Regelwerke,
- Technische Grundlagen der Erzeugung und der leitungsgebundenen Versorgung mit Strom und Gas,
- Grundlagen des Netzbetriebs und der Netzsteuerung,
- Grundlagen des Anlagenbetriebs und der Anlagensteuerung
- und als Schulungsschwerpunkt
- IT-Infrastrukturen für den Netzbetrieb - Scope des ISMS nach IT-Sicherheitskatalog § 11 Abs. 1a EnWG,
- IT-Infrastrukturen für den Anlagenbetrieb – Scope des ISMS nach IT-Sicherheitskatalog § 11 Abs. 1b EnWG.

Die Aufbauschulung muss einschließlich Prüfungen mindestens zwei Tage umfassen und die folgenden Inhalte abdecken:

- Rechtliche Rahmenbedingungen und relevante Regelwerke für die Stromerzeugung und die Gasförderung,

[7] Die in diesem Konformitätsbewertungsprogramm festgelegten Schulungsanforderungen gelten nicht für Begutachtende der Akkreditierungsstelle. Für diese gelten die festgelegten Kompetenzanforderungen der DAkkS.

- Grundlagen zu den verschiedenen Energieanlagenkategorien[8] und deren Besonderheiten,
- Grundlagen des Anlagenbetriebs und der Anlagensteuerung.
- und als Schulungsschwerpunkt
- IT-Infrastrukturen für den Anlagenbetrieb – Scope des ISMS nach IT-Sicherheitskatalog für Betreiber von Energieanlagen.

Die Bundesnetzagentur veröffentlicht eine Liste der anerkannten Schulungen auf ihrer Internetseite. Die detaillierten Schulungsinhalte sowohl der Vollschulung als auch der Aufbauschulung und deren zeitliche Gewichtung werden zwischen der Bundesnetzagentur und dem Schulungsanbieter im Rahmen der Anerkennung abgestimmt, um ein einheitliches Schulungsniveau sicherzustellen.

Die Zertifizierungsstellen haben zusätzlich sicherzustellen, dass alle von ihr eingesetzten Auditorinnen und Auditoren regelmäßig, spätestens jedoch alle 3 Jahre ausgehend von der bestandenen Auditorenschulung, an einer zweitägigen einschlägigen Fortbildungsveranstaltung über mindestens zehn Zeitstunden mit Bezug zum Thema IT-Sicherheit im Energiesektor teilnehmen. Diese Anforderung gilt auch dann als erfüllt, wenn eine Auditorin /ein Auditor an einem von einem externen Veranstalter organisierten Erfahrungsaustausch mit anderen Branchenvertretern teilnimmt, bei dem ein themenbezogener Wissenstransfer zu aktuellen Themen rechtlicher, organisatorischer oder technischer Art ermöglicht wird.

Für die Prüfung des Geltungsbereichs des ISMS (Scope) und der Risikoeinschätzung gemäß IT-Sicherheitskatalog muss das Audit-Team eine Fachexpertin / einen Fachexperten hinzuziehen. Die Fachexpertin / der Fachexperte berät das Audit-Team bei der Einschätzung, ob alle für den Anlagenbetrieb notwendigen Systeme, Komponenten und Anwendungen im Scope erfasst sind und die Risikoeinschätzung korrekt durchgeführt worden ist. Die Beratung des Auditteams durch die Fachexpertin / den Fachexperten im Rahmen der Audits zur Erstzertifizierung (Stufe 1 und 2), Rezertifizierung und bei den Überwachungsaudits erfordert die dauerhafte Anwesenheit der Fachexpertin / des Fachexperten während des jeweiligen Audits beim Anlagenbetreiber vor Ort. Dafür muss sie / er insbesondere über fundiertes Wissen und Erfahrungen in den von der oben genannten Schulung umfassten Themen im Bereich Anlagenbetrieb verfügen. Die Fachexpertin / der Fachexperte muss über eine ingenieurs- oder naturwissenschaftliche beziehungsweise technische oder handwerkliche Qualifikation in einem für diese Tätigkeit relevantem Gebiet mindestens auf dem DQR-Niveau 6[9] verfügen. Zusätzlich müssen mindestens drei Jahre einschlägige Berufserfahrung mit Bezug zur leitungsgebundenen Energieversorgung[10] nachgewiesen werden, innerhalb welcher sie / er sich vertiefte Kenntnisse über die zum Anwendungsbereich des IT-Sicherheitskatalogs gehörenden Energieanlagenkategorien und deren IT-Systeme angeeignet hat. Der Auditbericht, an dem die Fachexpertin /

---

[8] Vgl. Anhang 1, Teil 3, Nr. 1.1.1. bis 1.1.4, Nr. 2.1.1 und Nr. 2.1.2 BSI-Kritisverordnung.

[9] https://www.dqr.de/content/2336.php.

[10] Es ist nicht erforderlich, dass die Fachexpertin / 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 und die dazu eingesetzten IT-Systeme aufzubauen. Reine Beratungstätigkeiten sind nur eingeschränkt als erforderliche Berufserfahrung geeignet und können somit nur zum Teil anerkannt werden. Näheres wird im Einzelfall durch die DAkkS geprüft.

der Fachexperte beteiligt war, muss von der Fachexpertin / dem Fachexperten ebenfalls unterschrieben werden.

Die Unterstützung durch eine Fachexpertin / einen Fachexperten kann entfallen, sofern alle Mitglieder des Audit-Teams jeweils mindestens fünf Mal zusammen mit einer Fachexpertin / einem Fachexperten im Rahmen von Audits zur Zertifizierung des IT-Sicherheitskatalogs gemäß § 11 Abs. 1b EnWG die Risikoeinschätzung und den Scope des ISMS eines Anlagenbetreibers beurteilt hat.[11] Die Audits bei den Anlagenbetreibern der Kategorien Strom und Gas sind differenziert zu betrachten. Eine Addition der beiden Kategorien zum Erhalt der erforderlichen fünf Begleitungen ist nicht möglich.

Erfüllt eine Auditorin / ein Auditor selbst die Anforderungen an die Qualifikation der Fachexpertin / des Fachexperten, so kann die initiale fünfmalige Begleitung für diese Auditorin / diesen Auditor entfallen. Auditorinnen / Auditoren, die nicht die Anforderungen als Fachexpertin / Fachexperte erfüllen erreichen auch bei ausreichender Begleitung durch die Fachexpertin / den Fachexperten nicht den Status der Fachexpertin / des Fachexperten. Sie dürfen lediglich alleine auditieren und sind nicht mehr auf die Unterstützung der Fachexpertin / des Fachexperten angewiesen.

Die Fachexpertin / der Fachexperte selbst kann als Auditorin / Auditor in Zertifizierungsverfahren nach IT-Sicherheitskatalog gem. § 11 Abs. 1b EnWG tätig sein, sofern alle Voraussetzungen für die Arbeit als Auditorin / Auditor erfüllt sind und die Qualifikationen, welche für den Status der Fachexpertin / des Fachexperten notwendig sind nachgewiesen werden können. Da die Fachexpertin / der Fachexperte die Schulungsinhalte der Auditorenschulung mit dem vorhandenen Wissen bereits abdeckt, kann diese entfallen.

6 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 Abschnitt 9.1.5.1, sofern sie zumindest an regulären Arbeitstagen mit Personal besetzt ist.

3. Jeder Standort muss anhand der Vorgaben aus Tabelle B1 der ISO/IEC 27006 grundsätzlich einzeln kalkuliert werden, um eine Ausgangsgröße der zu erbringenden Auditzeit zu ermitteln.

4. Es ist zulässig, bei der Auditierung eine Stichprobe der Standorte zu wählen. Hierbei sind die Vorgaben der DIN ISO/IEC 17021, die ISO/IEC 27006 Abschnitt 9.1.5.1 und des IAF MD 1:2018 („Verbindliches IAF

[11] Audits aus Zertifizierungsverfahren für den IT-Sicherheitskatalog nach § 11 Absatz 1b EnWG („IT-Sicherheitskatalog für Energieanlagen“) bleiben dabei unberücksichtigt.

Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten“) 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 DIN EN ISO/IEC 27019 zu auditieren.

5. Für die Auditdauer gelten die Vorgaben von Anhang B der ISO/IEC 27006.[12] Die Formel zur Ermittlung der Auditdauer gemäß ISO/IEC 27006 Anhang B.3.4 ist auf die besondere Situation der Anlagenbetreiber hin anzupassen, wobei neben den Standorten auch die Anzahl der nicht dauerhaftbesetzten Betriebsstätten zu berücksichtigen ist. In Abweichung zu ISO/IEC 27006 Anhang B.3.5 ist eine Reduzierung der Auditdauer um höchstens 10 Prozent zulässig.

7 Übergangsregelung

Der IT-Sicherheitskatalog nach § 11 Absatz 1b EnWG verweist unter anderem auf die DIN EN ISO/IEC 27001, die DIN EN ISO/IEC 27002 und die DIN EN ISO/IEC 27019 in der jeweils geltenden Fassung. 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.

Sofern die genannten Normen künftig aktualisiert werden, gilt für die Berücksichtigung der aktualisierten Fassungen im Rahmen der Zertifizierungsprozesse folgende Übergangsregelung:

Audits zur Erst- oder Rezertifizierung und Überwachungsaudits im Rahmen des IT-Sicherheitskatalogs gemäß § 11 Absatz 1b EnWG haben spätestens nach Ablauf von zwei Jahren seit deren Veröffentlichung verpflichtend auf Basis der aktualisierten Fassungen zu erfolgen. Bei Audits zur Erst- oder Rezertifizierung und Überwachungsaudits können bis zu diesem Zeitpunkt daher alternativ auch die zuvor geltenden Fassungen berücksichtigt werden. Dies muss eindeutig aus dem Auditplan hervorgehen und mit dem Kunden schriftlich vereinbart worden sein.

Für die Überarbeitung der ISO/IEC 27001 und ISO/IEC 27002 zum Jahreswechsel 2021/2022 ist zusätzlich zur Übergangsregelung zu beachten, dass eine kompatible Version der ISO/IEC 27019 vermutlich erst im Jahr 2024/2025 erscheinen wird. Aus diesem Grund wurde ein Mapping[13] zwischen den aktualisierten ISO Normen 27001 & 27002, sowie der 27019:2020 durch die Bundesnetzagentur publiziert, das bis zur Veröffentlichung der aktualisierten Version der ISO/IEC 27019 im Jahr 2024/2025, entsprechend der Übergangsregelung, genutzt werden muss.

[12] Die Verteilung der Auditzeiten auf die verschiedenen Standorte ist nach den Anforderungen der ISO/IEC 27006 zulässig.

[13] https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/start.html.

Anlagen

Zertifikat

Die <KBS> bescheinigt hiermit,

dass das Informationssicherheits-Managementsystem (ISMS)

für den Geltungsbereich[14]

<Betreiberspezifische Bezeichnung>

(entsprechend dem Geltungsbereich des IT-Sicherheitskatalogs gem. § 11 Absatz 1b EnWG (12/2018))

für den Antragsteller

<Name des Antragstellers>

<Adresse>

Marktstammdatenregisternummer <xxxxxxxx>[15]

auf Grundlage des Statements of Applicability,

Version <xx> vom <xx.xx.xxxx>

die Anforderungen des folgenden Regelwerks erfüllt:

Zertifikats-ID: <xxx>

IT-Sicherheitskatalog gem. § 11 Absatz 1b EnWG (12/2018)

<LOGO, z.B.>

Letzter Audittag:	<xx.xx.xxxx>
Zertifizierungsdatum:	<xx.xx.xxxx>
Ausstellungsdatum:	<xx.xx.xxxx>
gültig bis:	<xx.xx.xxxx>

Siegel und Unterschrift mit Bezeichnung der Funktion – (Zertifizierungsstelle)

---

[14] Aus dem jeweiligen Geltungsbereich muss hervorgehen, welche Aufgabe der Antragsteller wahrnimmt, wie zum Beispiel den Betrieb, oder die Betriebsführung einer Energieanlage. Alle für den Geltungsbereich relevanten Energieanlagen sind im Anhang zu benennen.

[15] Die Marktstammdatennummer ist aufzuführen, sofern es sich beim Antragsteller nicht um einen Betriebsführer handelt.

Zertifikatsanhang

Zertifikats-ID: <xxx>

Liste der Energieanlagen[16]:

Name des Anlagenbetreibers der jeweiligen Einheit laut MaStR: <xxx>

Marktstammdatenregisternummer des Anlagenbetreibers der jeweiligen Einheit laut MaStR:

<xxxxxxxx> Einheit 1:

<Energieanlagenbezeichnung laut MaStR>

<Adresse>

MaStR-Nr. der jeweiligen Einheit: <SEExxxxxxxxxxxx bzw. GEExxxxxxxxxxxx>

Energieträger laut MaStR: <xxx>

Netto-Nennleistung [MW] der jeweiligen Einheit laut MaStR[17]: <xxx>

MaStR-Nr. der Stromerzeugungslokation: <SELxxxxxxxxxxxx>

[16] Bei mehreren Energieanlagen sind diese mit den oben gefragten Angaben untereinander aufzulisten.

[17] Diese Angabe ist nur für Stromerzeugungseinheiten erforderlich.

Impressum

Herausgeber

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

Tulpenfeld 4

53113 Bonn

Bezugsquelle | Ansprechpartner

Tulpenfeld 4

53113 Bonn

IT-Sicherheitskatalog@bnetza.de

www.bundesnetzagentur.de

Tel. +49 228 14-0

Fax +49 228 14-5966

Stand

Januar 2023

Text

Referat 627