MSzert 2020

Zertifizierung gemäß ISO/IEC 27001

IT-Sicherheitskatalog nach§ 11 Abs. 1a EnWG

© MSzert GmbH
06.01.2020

Aktuelle Anforderungen für Netzbetreiber

Der IT-Sicherheitskatalog verpflichtete Strom- und Gasnetzbetreiber zur Umsetzung IT-sicherheitstechnischer Mindeststandards. Kernforderung war die Etablierung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 sowie dessen Zertifizierung bis zum 31. Januar 2018.

Dies bedeutet, dass der zweite Zyklus für die Wiederholungsaudits zum Nachweis der nächsten 3 Jahre beginnt.

Das Zertifikat basiert dabei im Wesentlichen auf dem bereits existierenden IT-Sicherheitskatalog bzw. Zertifizierungsschema zur ISO/IEC 27001. Wichtig ist, dass bei zukünftigen Re-Zertifizierungen das für Zertifizierungsstellen relevante aktuelle Konformitätsbewertungsprogramm umgesetzt werden muss.

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.

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.

Vorteile Ihres ISO/IEC 27001-Zertifikates

- ✓ **Erfüllung gesetzlicher Anforderungen, z.B.:**
  - IT-Sicherheitsgesetz
  - IT-Sicherheitskatalog
  - TR-03109 / Messstellenbetriebsgesetz
  - Energiewirtschaftsgesetz
  - MaRisk
- ✓ **Erfüllung der Erwartung Ihrer Kunden**
- ✓ **Prozessverbesserung und damit Produktivitätssteigerung**
- ✓ **Informationssicherheit**
- ✓ **Datenschutz**
- ✓ **Haftungsreduktion**
- ✓ **Synergien zu anderen Managementprozessen, z.B.:**
  - ISO 9001
  - ISO 50001
  - ISO/IEC 20000-1

Ansprechpartner

Wirt.-Ing. Thomas Welsch
Leiter Zertifizierungsstelle

Dipl.-Ing. Stefan Oehm
Geschäftsführung

Telefon: +49 (0)6833 900 895-0

Telefax: +49 (0)6833 900 895-19

E-Mail: mszert@mszert.de

Gesetzliche Vorgaben für KRITIS

Mit dem IT-Sicherheitsgesetz und dem IT-Sicherheitskatalog hat der Gesetzgeber Vorgaben für Betreiber Kritischer Infrastrukturen (KRITIS) und Netzbetreiber erlassen. Hintergrund ist, dass zunehmend IT-Infrastrukturen wichtige Versorgungsbereiche durchdringen. So gewinnt Informationstechnik und deren Sicherheit an Stellenwert – besonders für die wichtige Verfügbarkeit.

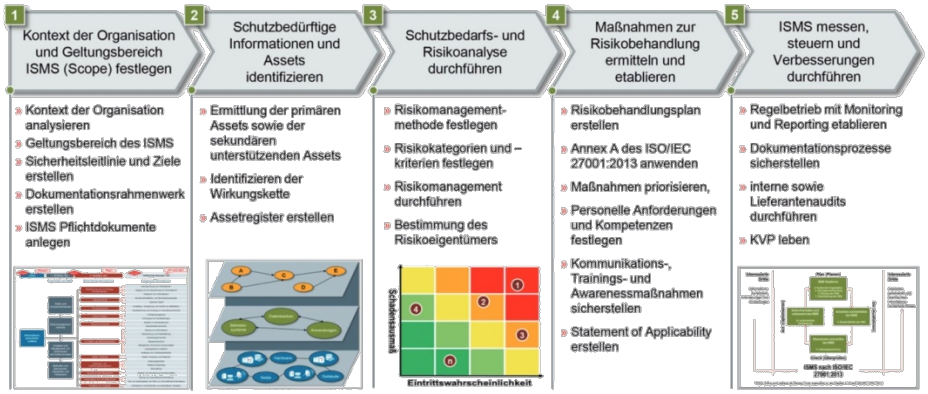
Umsetzung und Projektierung

Da die ISO 27001 für Organisationen jeder Art und Größe anwendbar ist (vgl. ISO/ IEC 27001 Kap. 1), sind branchenspezifische Vorgaben daher prinzipiell höher zu priorisieren, da sie individuelle Gegebenheiten und Voraussetzungen betrachten.

Zudem unterscheiden sich bspw. die Sicherheitsanforderungen des Energiesektors fundamental von denen anderer Branchen. Speziell bei den Steuerungsnetzen steht die Verfügbarkeit der IT-Service an oberster Stelle, um die Stromversorgung zu gewährleisten.

In der ISO 27001 ist explizit vorgesehen, dass erforderliche Schutzmaßnahmen neben dem mitgelieferten Annex A auch explizit aus anderen Quellen verwendet werden dürfen. Dieses eröffnet die Möglichkeit, die erforderlichen branchenspezifischen Standards und Regelungen im Kontext des ISMS entsprechend mitzuberücksichtigen. Auch bei einer Zertifizierung (siehe ISO 27001, Kap. 6.1.3 b) können Maßnahmen nach Bedarf gestaltet oder vorgefertigte Maßnahmen aus anderen Quellen gewählt werden.

Folglich können in der Praxis über diesen Weg die vorgeschlagenen Empfehlungen und Maßnahmen aus der DIN SPEC 27019 (DIN SPEC 27019 – Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung) im ISMS ergänzend berücksichtigt werden, sollten aber im Rahmen des Risikobehandlungsplans dann mit einer Quellenangabe gekennzeichnet werden, um die Nachvollziehbarkeit zu gewährleisten.



Weitere anzuwendende Normen

ISO/IEC 27001 stellt die Basisnorm für weitere branchenspezifische Anforderungen dar, etwa:

- ISO/IEC 27011 für Telekommunikationsunternehmen,
- ISO/IEC 27017 für IT-Sicherheit in der Cloud,
- ISO/IEC 27018 für Datenschutz in der Cloud,
- ISO/IEC 27019 für die Energiewirtschaft,
- ISO 27799 für das Gesundheitswesen,

Gerne informieren wir Sie, wie diese branchenspezifischen Anforderungen in eine ISO/IEC 27001-Zertifizierung integriert werden können.

Multi-Site: Zertifizierung eines ISMS an mehreren Standorten

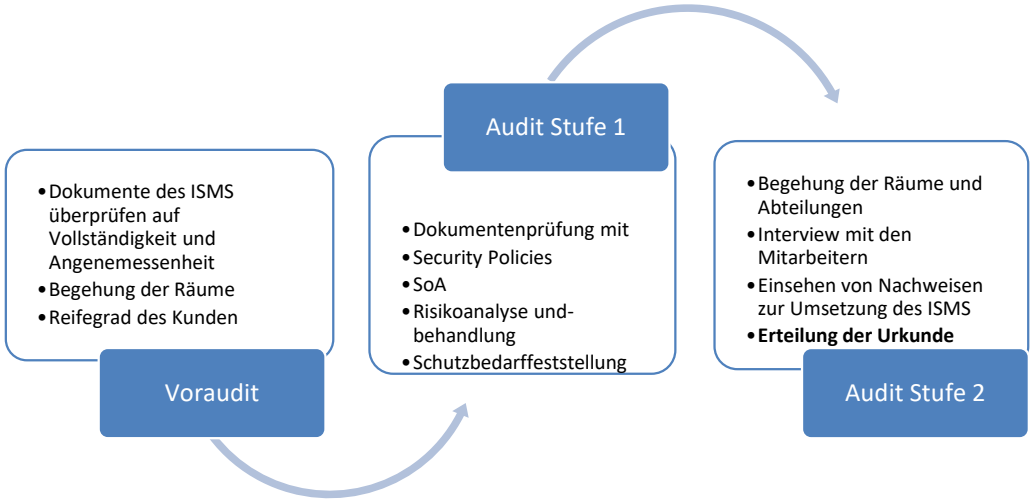
Ein Informationssicherheits-Managementsystem kann sich über mehrere Standorte oder sogar juristische Personen verteilen. So ist es möglich, einen kompletten Unternehmensverbund zu zertifizieren und dabei Synergieeffekte sinnvoll zu nutzen. Voraussetzung ist dabei, dass alle Einheiten unter einem zentralen Managementsystem interagieren und gesteuert werden, wobei einzelne Tätigkeiten sich auf die Unternehmenseinheiten verteilen lassen.

Durch ein gemeinsames Audit aller Einheiten sparen Sie Zeit und Ressourcen, sowohl bei der Vorbereitung als auch bei der Zertifizierung Ihres ISMS gemäß ISO/IEC 27001.

Aufwand und Ablauf der Auditierung

Der Umfang der Auditierung orientiert sich an der für alle akkreditierten Zertifizierungsstellen bindenden Norm ISO/IEC 27006. Hier werden in Abhängigkeit der Größe des ISMS (Anzahl der Mitarbeiter im Geltungsbereich) folgende Vorgaben genannt.

Anzahl der Mitarbeiter im Geltungsbereich	1 - 10	11 - 25	26 - 45	46 - 65	66 - 85	86 - 125	...
Anzahl der Tage für die Auditierung vor Ort	5	7	8,5	10	11	12	...



MSzert

Zum Nollenberg 16
66780 Rehlingen-Siersburg
www.mszert.de

Telefon: +49 (0)6833 900 895-0

Telefax: +49 (0)6833 900 895-19

E-Mail: mszert@mszert.de

Ihre Ansprechpartner

Wirt.-Ing. Thomas Welsch
Leiter Zertifizierungsstelle

Dipl.-Ing. Stefan Oehm
Geschäftsführung

Re-Zertifizierung gemäß den Anforderungen des IT-Sicherheitskataloges:

Sehr geehrte Damen und Herren,

wir betreiben zentrale und dezentrale Anwendungen, Systeme und Komponenten im Geltungsbereich des vorliegenden IT-Sicherheitskatalogs, die für einen sicheren Netzbetrieb notwendig sind.

Betroffen sind hiervon alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte. Darunter fallen z. B. Messeinrichtungen an Trafo- oder Netzkoppelstationen.

Wir möchten im Rahmen der Zertifizierung nach §11 EnWG / IT-Sicherheitskatalog:

- ☐ Informationsgespräch / Vor-Ort Termin
- ☐ Zusendung weiterer Informationen
- ☐ Angebot zur Zertifizierung nach dem IT-Sicherheitskatalog der BNetzA
- ☐ Durchführung eines optionalen Check-Ups durch einen erfahrenen ISMS-Auditor
- ☐ Durchführung der Zertifizierung durch MSzert GmbH

Kontaktdaten:

Ansprechpartner ISMS: _____

Telefon: _____

Mail: _____