MSzert

2017

Zertifizierung gemäß ISO/IEC 27001

IT-Sicherheitskatalog nach§ 11 Abs. 1a EnWG

18.01.2017

Einleitung

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

Zum Nachweis, dass die Anforderungen des IT-Sicherheitskatalogs erfüllt werden, hat die Bundesnetzagentur gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein eigenes Zertifikat erarbeitet und auf der Internetseite der Bundesnetzagentur veröffentlicht.

Das Zertifikat basiert dabei im Wesentlichen auf dem bereits existierenden Zertifikat bzw. Zertifizierungsschema zur ISO/IEC 27001 und ergänzt diese um die zusätzlichen Anforderungen des IT-Sicherheitskatalogs.

Des Weiteren wurde der Anwendungsbereich (Scope) spezifiziert, um sicherzustellen, dass die einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme von der Zertifizierung erfasst sind.

Ob der Standard eingehalten wird, kann von unabhängigen Auditoren überprüft und durch ein ISO/IEC 27001-Zertifikat nach außen dokumentiert werden – etwa um gesetzlichen Anforderungen nachzukommen oder den Erwartungen Ihrer Kunden zu genügen.

Die ISO/IEC 27001 ist der internationale Standard für Informationssicherheitsmanagementsysteme. Dadurch werden Prozesse in einer Organisation etabliert, um Informationssicherheit dauerhaft zu gewährleisten.

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
Customer-Management

Dipl.-Ing. Stefan Oehm
Leiter Zertifizierungsstelle

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

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

E-Mail: mszert@mszert.de

Gesetzliche Vorgaben für KRITIS

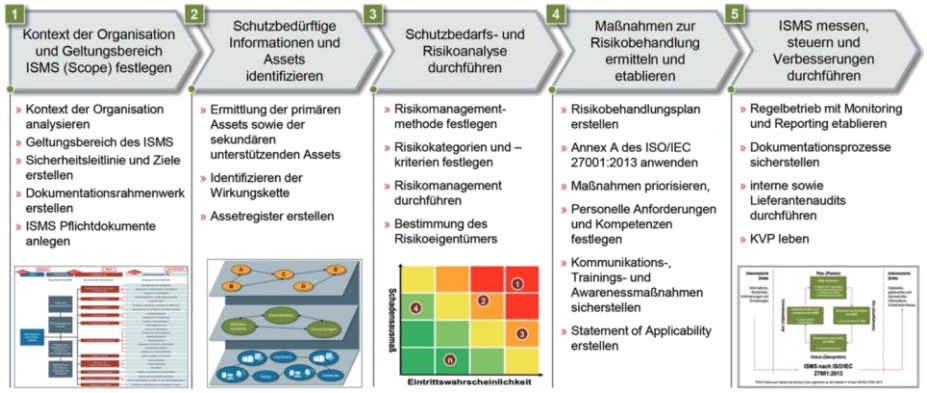
Mit dem IT-Sicherheitsgesetz und dem IT-Sicherheitskatalog hat der Gesetzgeber Vorgaben für Betreiber Kritischer Infrastrukturen (KRITIS) und Netzbetreiber erlassen. Hintergrund ist, dass zunehmend IT-Infrastrukturen wichtige Versorgungsbereiche durchdringen. So gewinnt Informationstechnik und deren 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 27001:2013 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

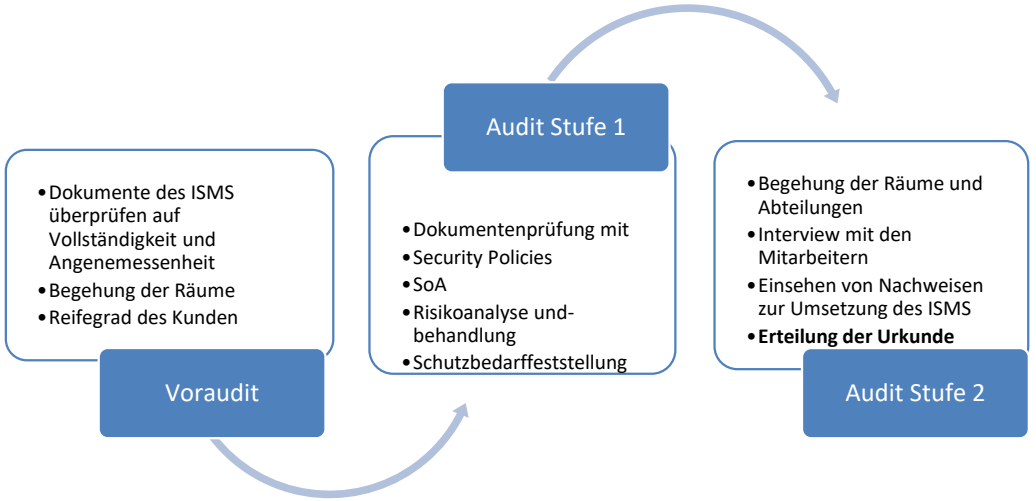
Ein Informationssicherheits-Managementsystem kann sich über mehrere Standorte oder sogar juristische Personen verteilen. So ist es möglich, einen kompletten Unternehmensverbund zu zertifizieren und dabei Synergieeffekte sinnvoll zu nutzen. Voraussetzung ist dabei, dass alle Einheiten unter einem zentralen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

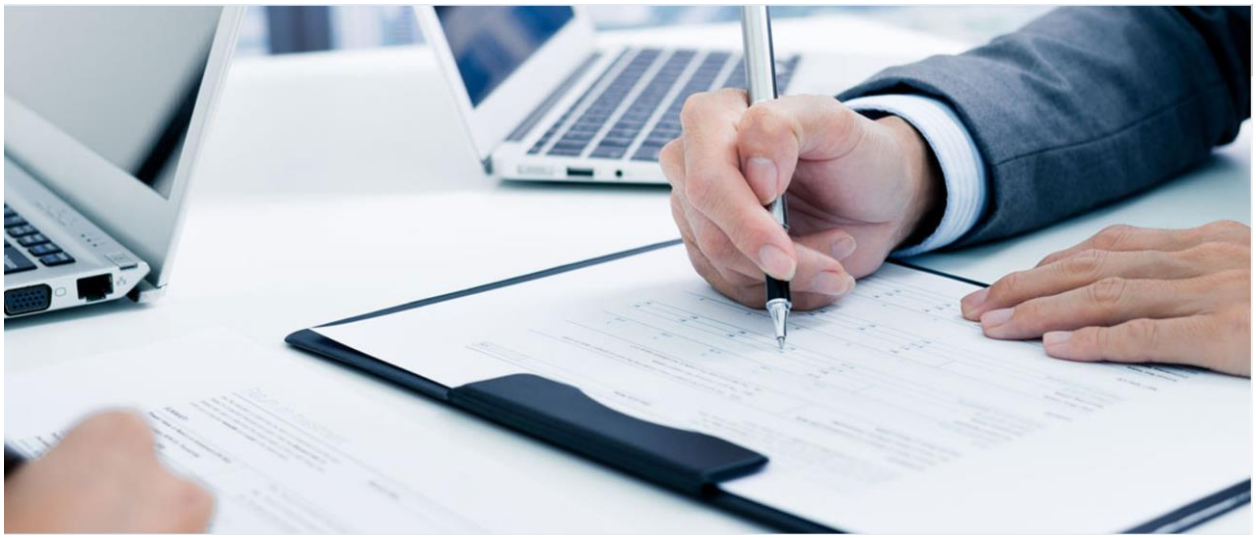
Durch ein gemeinsames Audit aller Einheiten sparen Sie Zeit und Ressourcen, sowohl bei der Vorbereitung als auch bei der Zertifizierung Ihres ISMS gemäß ISO/IEC 27001.

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

Ihre Ansprechpartner

Wirt.-Ing. Thomas Welsch
Customer-Management

Dipl.-Ing. Stefan Oehm
Leiter Zertifizierungsstelle

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

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

E-Mail: mszert@mszert.de