Ein weit verbreiteter Irrglaube besteht darin, dass im Rahmen der Abschlussbesprechung vom Lead-Auditor mitgeteilt wird, ob das Auditergebnis mit positiv endete oder nicht. Der Lead-Auditor übersendet jedoch die Unterlagen zusammen mit seiner Empfehlung an den Zertifizierungsausschuss der Zertifizierungsgesellschaft, welcher dann nach Sichtung aller Unterlagen und ggf. nach Rücksprache mit dem Kunden entscheidet, ob der Empfehlung des leitenden Auditors gefolgt werden kann oder nicht.

Obwohl die Auditoren bei ihren Feststellungen in der Regel sehr sorgfältig arbeiten, kann es durchaus vorkommen, dass die Kundenorganisation eine andere Sichtweise hat und man sich auf der Abschlussbesprechung nicht auf eine gemeinsame Bewertung einigen kann. In solchen Fällen hat der KRITIS Betreiber dann natürlich die Möglichkeit, sich im Rahmen einer Beschwerde an die Zertifizierungsgesellschaft zu wenden.

ABSCHLIESSENDES FAZIT

Zusätzliche Prüfungen führen in der Regel immer erst einmal zu einem monetären Mehraufwand und einer zusätzlichen zeitlichen Mehrbelastung. Dies führt zu Beginn zu einer geringen Akzeptanz. Abgesehen davon, dass es zu einer gesetzlichen Anforderung keine Alternativen gibt, wird man in der Regel aber schnell feststellen, dass die Implementierung und Zertifizierung eines ISMS nach ISO 27001 immer ein Zugewinn ist.

VGB PowerTech e. V.

Deilbachtal 173
45257 Essen
Telefon 0201 8128-205
Telefax 0201 8128-321
E-mail: iso27001@vgb.org
www.vgb.org

KSG Kraftwerks - Simulator - Gesellschaft mbH
GfS Gesellschaft für Simulatorschulung mbH

Deilbachtal 173
45257 Essen
Telefon 0201 4862-121
Telefax 0201 4862-404
E-mail: iso27001@simulatorzentrum.de
www.simulatorzentrum.de

Zertifizierung von KRITIS Betreibern der Energiewirtschaft nach ISO 27001 in Verbindung mit dem IT-Sicherheitskatalog gemäß §11 EnWG

Warum muss mein Unternehmen zertifiziert werden?
Was sind die Grundlagen der Zertifizierung?
Wie läuft eine Zertifizierung ab?

UNSER ANGEBOT AN DIE VGB-MITGLIEDER

- 28. Juni 2017
  kostenlose Info-Veranstaltung zum Thema
  „Implementierung von Managementsystemen nach ISO 27001 für Kritis-Betreiber der Energiewirtschaft."
- Ab 2. Halbjahr 2017
  IT-Beratung und Auditierung ISO 27001 mit Unterstützung eines renommierten Lead-Auditors für die Energiebranche.

GESETZLICHE VORGESCHICHTE

2011 hat die Bundesregierung mit der Cybersicherheitsstrategie den Grundstein für mehr Sicherheit im Cyberraum gelegt. Die digitale Agenda des Jahres 2014 bereitete daraufhin den Weg für das im Juli 2015 in Kraft getretene **IT-Sicherheitsgesetz** (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme), welches im Bereich der kritischen IT-Infrastrukturen (Energie- und Wasserversorgung, Gesundheitswesen, Finanzwesen, Telekommunikation u.a.) dafür sorgt, dass ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen nicht auftritt. Die 1. Verordnung zur Bestimmung kritischer Infrastrukturen (**Kritis-VO**) trat hiernach am 3. Mai 2016 in Kraft. Die 2. Verordnung wird im Frühjahr 2017 in Kraft treten.

Eine Pflicht zur Umsetzung der IT-Sicherheit nach dem Stand der Technik sowie eine Pflicht zur Überprüfung der Absicherung durch Dritte im Rahmen eines Audits ist durch **§11 EnWG** durch den IT-Sicherheitskatalog vorgeschrieben. Abhängig von verschiedenen Kriterien betrifft diese Pflicht:

- Energieversorgungsnetze
- Energieanlagen
- Genehmigungsinhaber nach §§ 6,7 oder 9 AtomG

Durch Unternehmen, die Dienstleistungen im Bereich der Regelleistung erbringen oder erbringen möchten, werden durch die Übertragungsnetzbetreiber umfangreiche Vorgaben in Form der „Mindestanforderungen an die Informationstechnik des Anbieters für die Erbringung von Regelleistung“ definiert. Dabei kann im Rahmen der Präqualifikation durch die Übertragungsnetzbetreiber gefordert werden, dass seitens des Regelleistungsanbieters ein Nachweis der ISO27001 Zertifizierung gemäß den Vorgaben des IT-Sicherheitsgesetzes und in Anlehnung an den IT-Sicherheitskatalog vorgelegt werden muss. Aktuelle Anforderungen der deutschen Übertragungsnetzbetreiber in der Fassung vom 28.04.2016 fordern dies bis zum 31.01.2018.

BIS WANN MUSS DIE KRITIS-VO UMGESETZT SEIN

Die Pflicht zur Einhaltung von IT-Sicherheitsstandards, zu denen Betreiber Kritischer Infrastrukturen verpflichtet werden, ist in §11 Absatz 1 des EnWG festgelegt. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen, in den auch die Bestimmung der Frist aufgenommen wird. Die Veröffentlichung des Sicherheitskatalogs wird derzeit für Q2/2017 erwartet. Die Frist wird voraussichtlich 2 Jahre ab Veröffentlichung betragen.

PRÜFUNGSGRUNDLAGEN

Die Prüfungen werden im Rahmen von Zertifizierungsverfahren durchgeführt, d.h. die Zertifizierungen werden „nur“ von Zertifizierungsgesellschaften durchgeführt, welche von der Deutschen Akkreditierungsgesellschaft DAkkS (Infos unter www.dakks.de) vorher akkreditiert sind. Grundlage hierfür ist die **ISO/IEC 17021-1:2015**.

Bei der Prüfung der Unternehmen des Energiesektors wenden die akkreditierten Zertifizierungsgesellschaften folgende Normen an:

- **ISO 27001:2013** eigentliche Zertifizierungsgrundlage
- **ISO 27006:2015** Besondere Anforderungen für Zertifizierungsgesellschaften, die Informationssicherheitsmanagementsysteme (ISMS) zertifizieren
- **ISO TR 27019** Leitfaden für das ISMS von Steuerungssystemen der Energieversorgung auf Grundlage der ISO 27002
- **ISO 19011:2011** Leitfaden zur Durchführung von internen und externen Audits

AUDITDAUER UND AUDITUMFANG

Ein Auditverfahren besteht aus einer Erstzertifizierung, einem ersten Überwachungsaudit nach (spätestens) zwölf Monaten und einem zweiten Überwachungsaudit nach (circa) vierundzwanzig Monaten. Durch das so genannte Rezertifizierungsverfahren nach (circa) 36 Monaten erfolgt dann ein weiterer dreijähriger Zertifizierungszyklus.

Für die Auditdauer gelten die Vorgaben von Anhang B der ISO/IEC 27006:2015. Dabei ist die Formel zur Ermittlung der Auditdauer gemäß **ISO/IEC 27006:2015 Anhang B.3.4** auf die besondere Situation des KRITIS Betreiber im Energiesektor abzustellen. In Abweichung zu ISO 27006:2015 ist eine Reduzierung der Auditdauer um maximal 10 Prozent zulässig. Die Standarddauer für die Erstzertifizierung ist aus dem nachfolgenden Auszug aus der folgenden Tabelle zu entnehmen:

VZÄ	Audittage	VZÄ	Audittage
1-10	5	176-275	14
11-15	6	276-425	15
16-25	7	426-625	16,5
26-45	8,5	626-875	17,5
46-65	10	876-1175	18,5
66-85	11	1176-1550	19,5
86-125	12	1551-2025	21
126-175	13	2026-2675	22

Hinweise: VZÄ = Mitarbeiter-Vollzeitäquivalente; ein Audittag umfasst eine reine Auditzeit von acht Zeitstunden (ohne Pausen und eventuelle Fahrzeiten)

Die Anzahl der zu auditierenden Standorte bestimmt sich wie folgt aus **Abschnitt 9.1.5.1. der ISO/IEC 27006:2015**:

Erstzertifizierung: Quadratwurzel aller Standorte

Überwachungsaudit: Quadratwurzel aller Standorte x 0,6

Rezertifizierungsaudit: Quadratwurzel aller Standorte x 0,8

DIE STATIONEN EINES AUDITVERFAHRENS

Alles beginnt mit der Auswahl der „richtigen“ Zertifizierungsgesellschaft und des richtigen leitenden Auditors.

Hieran schließt sich die **Auditplanung** an, d.h. die organisatorische Abstimmung zwischen KRITIS – Betreiber und dem Lead-Auditor der Zertifizierungsgesellschaft. Im Rahmen der Auditplanung werden abgestimmt:

- Geltungsbereich
- Termine
- Interviewpartner
- Standorte
- Prüfbereiche

Das Erstzertifizierungsaudit besteht aus einem Audit der Stufe 1 sowie einem Audit der Stufe 2, bei allen weiteren Auditformen entfällt i.d.R. Stufe 1.

Das Audit der Stufe 1 hat folgende Ziele:

- Auditierung der Managementsystemdokumentation
- Beurteilung standortspezifischer Bedingungen
- Statusbewertung des Kunden
- Informationsabstimung zum Geltungsbereich, der Prozesse, der Standorte, gesetzlicher und behördlicher Aspekte etc.
- Zuteilung der Ressourcen für Stufe 2
- Schwerpunktbildung für das Audit der Stufe 2
- Beurteilung der Managementsystembewertung und des internen Audits

Zum Ende der Auditstufe 1 wird dem Kunden in einer Abschlussbesprechung mitgeteilt, ob es mit Stufe 2 weitergehen kann oder nicht.

Das Audit der Stufe 2 hat das Ziel, die Umsetzung einschließlich der Wirksamkeit des Managementsystems zu bewerten. Hierzu setzen die Auditoren Auditchecklisten ein, mit denen Normforderung und Umsetzung in der Realität verglichen werden. Es empfiehlt sich, diese Auditchecklisten im Vorhinein von der Zertifizierungsgesellschaft anzufordern, um die Denkart des Zertifizierers zu kennen.

Im Rahmen des Audits kann es dann natürlich vorkommen, dass Normanforderung und Umsetzung nicht übereinstimmen. In der Regel wird dann vom Lead-Auditor eine Empfehlung gegeben oder eine **Feststellung** (in der Regel in der Klassifizierung als Einzelabweichung oder Abweichung) getroffen. Der Kunde muss nun eine Ursachenanalyse betreiben, eine Korrekturmaßnahme ableiten sowie durchführen und die Zertifizierungsgesellschaft muss die Wirksamkeit der Korrekturmaßnahme abschließend bewerten.

So wie zu Beginn des Audits eine Eröffnungsbesprechung durchgeführt wird, wird zum Ende des Audits eine Abschlussbesprechung durchgeführt.