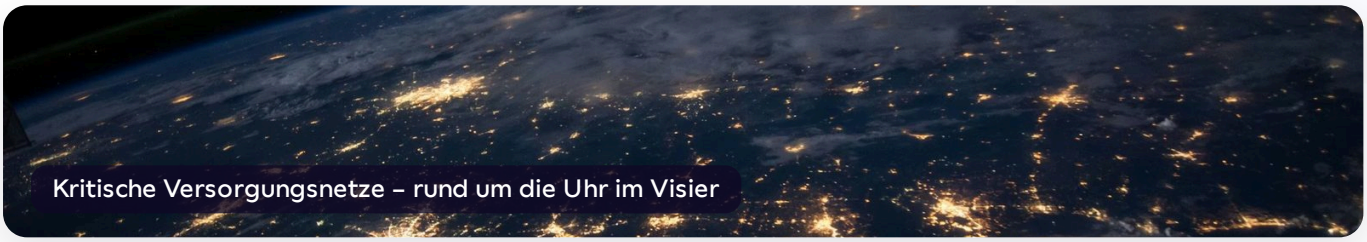
SECJUR

ISO 27001 für die Energiewirtschaft

Der Readiness-Check für Versorger und Energie-Dienstleister — von der Scope-Definition bis zur Zertifizierungsreife.

Für Energieunternehmen ist Informationssicherheit längst kein reines IT-Thema mehr, sondern eine Frage der Versorgungssicherheit. Steigende Bedrohungen für OT- und Leitsysteme, regulatorischer Druck durch **NIS2 und das KRITIS-Dachgesetz** sowie Anforderungen von Netzbetreibern, Stadtwerken und Industriekunden treffen oft auf schlanke Teams. **ISO/IEC 27001** liefert hier den anerkannten Rahmen, um Sicherheit strukturiert nachzuweisen — und schafft gleichzeitig die Grundlage, um regulatorische Pflichten effizient mit abzudecken.



Kritische Versorgungsnetze – rund um die Uhr im Visier

Wann ISO 27001 für Energieunternehmen entscheidend wird:

TREIBER 01

Regulatorischer Druck

NIS2 und das KRITIS-Dachgesetz verlangen ein belastbares Risikomanagement für Energie-Einrichtungen. Ein ISO-27001-ISMS deckt einen Großteil dieser Pflichten strukturiert ab und macht den Nachweis gegenüber Behörden deutlich einfacher.

TREIBER 02

OT- und Leitsysteme

Steuerungs- und Netzleittechnik ist ein attraktives Angriffsziel. ISO 27001 zwingt zur sauberen Erfassung dieser Assets, ihrer Risiken und Schutzmaßnahmen — und verbindet die oft getrennten Welten von IT und OT in einem gemeinsamen Steuerungsrahmen.

TREIBER 03

Anforderungen aus der Lieferkette

Netzbetreiber, Stadtwerke und Industriekunden prüfen ihre Dienstleister zunehmend per Sicherheitsfragebogen und Audit-Recht. Ein Zertifikat ersetzt viele dieser Einzelnachweise und beschleunigt Ausschreibungen und Onboardings spürbar.

TREIBER 04

Leitungsverantwortung

Mit NIS2 rückt die Geschäftsführung persönlich in die Pflicht: Risikomaßnahmen müssen freigegeben und überwacht werden. Ein ISMS schafft die Governance-Struktur, mit der die Leitung diese Verantwortung nachweisbar wahrnimmt.

NIS2-Synergie

ein ISO-27001-ISMS deckt zentrale NIS2-Risikomaßnahmen strukturiert mit ab

IT + OT

ein gemeinsamer Steuerungsrahmen für Büro-IT und Netzleittechnik statt zweier Silos

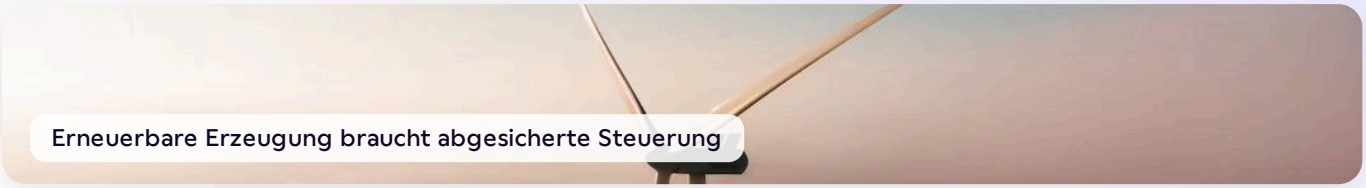
Ein Zertifikat

ersetzt zahllose Sicherheitsfragebögen aus der Energie-Lieferkette

SECJUR

Der Readiness-Check: Schritt 1–6

Die Basis eines zertifizierungsreifen ISMS für Energieversorger und Energie-Dienstleister.



SCHRITT 01

Anwendungsbereich definieren

- [ ] Standorte, Gesellschaften und Geschäftsprozesse abgrenzen
- [ ] IT- und OT-/Leitsysteme bewusst in den Scope einbeziehen
- [ ] Externe Dienstleister und Rechenzentren berücksichtigen
- [ ] Schnittstellen zu NIS2- und KRITIS-Pflichten festhalten
- [ ] Scope-Dokument schriftlich festhalten und freigeben

SCHRITT 02

Asset- und Risikoinventar

- [ ] Informations- und OT-Assets vollständig erfassen
- [ ] Verantwortliche je Asset benennen
- [ ] Schutzbedarf nach Vertraulichkeit, Integrität, Verfügbarkeit
- [ ] Bedrohungen und Schwachstellen je Asset bewerten
- [ ] Risiken nach einheitlicher Methodik priorisieren

SCHRITT 03

Leitungsmandat sichern

- [ ] Geschäftsführung formal als ISMS-Verantwortliche einbinden
- [ ] Informationssicherheitsleitlinie verabschieden
- [ ] ISMS-Rollen und Verantwortlichkeiten festlegen
- [ ] Sicherheitsziele messbar definieren
- [ ] Ressourcen und Budget freigeben

SCHRITT 04

Risikobehandlung planen

- [ ] Behandlungsoption je Risiko wählen (reduzieren, übertragen, akzeptieren)
- [ ] Maßnahmen aus Annex A ableiten und zuordnen
- [ ] Statement of Applicability erstellen und begründen
- [ ] Maßnahmenplan mit Terminen und Owern aufsetzen
- [ ] Restrisiken durch die Leitung freigeben lassen

SCHRITT 05

Technische & organisatorische Maßnahmen

- [ ] Zugriffs- und Berechtigungskonzepte umsetzen
- [ ] Netzsegmentierung zwischen IT und OT etablieren
- [ ] Härtung, Patch- und Schwachstellenmanagement einführen
- [ ] Monitoring, Logging und Backups absichern
- [ ] Lieferanten- und Dienstleistersteuerung verankern

SCHRITT 06

Vorfallsmanagement aufbauen

- [ ] Erkennungs- und Reaktionsprozesse definieren
- [ ] Meldewege inkl. NIS2-Fristen abbilden
- [ ] Eskalation und Notfallrollen festlegen
- [ ] Notfall- und Wiederanlaufpläne dokumentieren
- [ ] Vorfälle üben und Lessons Learned auswerten

SECJUR

Der Readiness-Check: Schritt 7–11

Von der Umsetzung zum bestätigten Zertifikat — und wie sich der Weg dorthin verkürzen lässt.

SCHRITT 07

Awareness & Schulung

- [ ] Mitarbeitende und OT-Personal regelmäßig schulen
- [ ] Rollenbasierte Inhalte für kritische Funktionen
- [ ] Leitungsebene gemäß NIS2 qualifizieren
- [ ] Phishing- und Notfallübungen durchführen
- [ ] Schulungsnachweise dokumentieren

SCHRITT 08

Dokumentation komplettieren

- [ ] Richtlinien, Verfahren und Nachweise zusammenführen
- [ ] Lenkung von Dokumenten und Aufzeichnungen sicherstellen
- [ ] Versionierung, Freigaben und Zugriffe regeln
- [ ] Nachweise prüfbar und auffindbar ablegen
- [ ] Aufbewahrungsfristen festlegen

SCHRITT 09

Internes Audit

- [ ] Auditprogramm und -umfang planen
- [ ] ISMS gegen die Normanforderungen prüfen
- [ ] Abweichungen und Korrekturmaßnahmen erfassen
- [ ] Wirksamkeit der Maßnahmen belegen
- [ ] Auditberichte der Leitung vorlegen

SCHRITT 10

Managementbewertung

- [ ] Leitung bewertet ISMS-Leistung und Ziele
- [ ] Audit-, Risiko- und Vorfallsergebnisse einbeziehen
- [ ] Verbesserungen und Ressourcen beschließen
- [ ] Änderungen am Scope prüfen
- [ ] Ergebnisse nachvollziehbar dokumentieren

SCHRITT 11

Zertifizierungsaudit

- [ ] Zertifizierungsstelle auswählen und beauftragen
- [ ] Stufe-1- und Stufe-2-Audit vorbereiten
- [ ] Nachweise für Auditor:innen bereitstellen
- [ ] Festgestellte Abweichungen abarbeiten
- [ ] Zertifikat erlangen und Folgezyklen einplanen

BESCHLEUNIGER

Plattformgestützt statt im Eigenbau

- [ ] Controls, Risiken und Nachweise zentral im Dashboard
- [ ] Vorlagen und Workflows für jeden Schritt
- [ ] Expert:innen-Begleitung von Scope bis Audit
- [ ] Audit-Readiness jederzeit auf Knopfdruck
- [ ] NIS2- und ISO-Pflichten in einem System abdecken

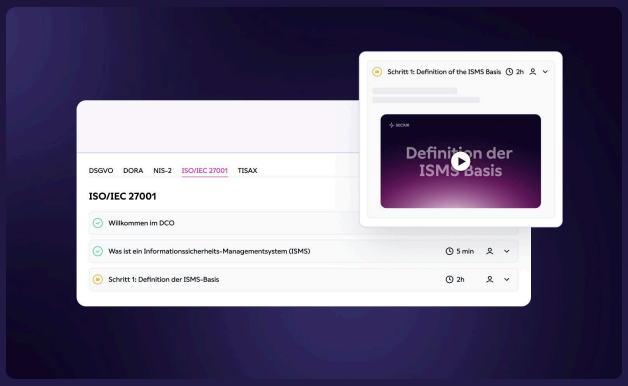
SECJUR

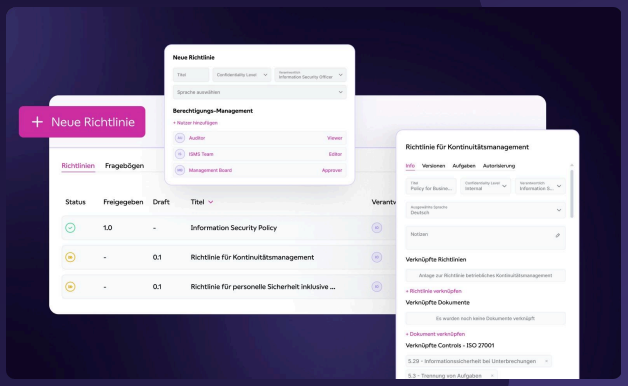
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

Mit der **SECJUR Automatisierungsplattform** und unseren **TÜV-zertifizierten Expert:innen** setzen Sie ISO 27001 in Rekordzeit um:

- Automatisierte Erstellung und Verwaltung Ihres ISMS
- Integriertes Risikomanagement & Lieferantenbewertungen
- Audit-Readiness auf Knopfdruck

Damit sparen Sie hunderte Stunden Aufwand – und sichern sich den entscheidenden Wettbewerbsvorteil bei großen Kundenprojekten.





Mit SECJUR zu Informationssicherheitszertifizierungen:

Dank SECJUR konnten wir schnell ein hochwertiges ISMS aufbauen, wie uns auch in den Zertifizierungsaudits bestätigt wurde. Unser zugewiesener Berater hat uns stets kompetent unterstützt - als wäre er ein Teil der Firma. Freuen uns auf die weitere Zusammenarbeit!

Stefan Gregori
Chief Information Security Officer

CONSOLINNO energy

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

1KOMMA5° · Stadtwerke Kamp-Lintfort · Consolinno Energy · Stadtwerke Nienburg Energie · Changing Cities · CUBOS

www.secjur.com