SECJUR

WHITEPAPER
2026

ISO 27001 · ENERGIE & VERSORGUNG

ISO 27001 in der Energiebranche: *Sicherheit für die Versorgung.*

Strom-, Gas- und Wärmeversorgung gehören zur kritischen Infrastruktur, und ihre Digitalisierung schreitet mit der Energiewende rasant voran. Für Netzbetreiber ist ein ISMS nach ISO 27001 über den IT-Sicherheitskatalog der Bundesnetzagentur ohnehin faktisch verpflichtend, und NIS2 erfasst weite Teile der Branche. Dieses Whitepaper zeigt, welche Pflichten gelten, wo die größten Schwachstellen in IT und Netzleittechnik liegen und wie ein zertifizierungsreifes ISMS entsteht, ohne die Versorgungssicherheit zu gefährden.

ISO 27001 | ISO 27019 | NIS2 | KRITIS | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In der Energiebranche ist Sicherheit *gesetzlich verankert.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). In der Energiebranche ist er kein freiwilliges Extra: Der IT-Sicherheitskatalog der Bundesnetzagentur nach §11 EnWG verlangt von Strom- und Gasnetzbetreibern ein zertifiziertes ISMS nach ISO 27001, ergänzt um die energiespezifische ISO 27019. Für viele Unternehmen der Branche ist die Zertifizierung damit Pflicht.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der IT und Betriebstechnik gleichermaßen absichert, von der Verwaltung bis zur Netzleittechnik.

Weltweit sind über 70.000 Organisationen nach ISO 27001 zertifiziert, mit deutlich steigender Tendenz. Seit dem 31. Oktober 2025 gilt ausschließlich die Fassung von 2022; die ältere Version :2013 ist mit dem Ende der Übergangsfrist ausgelaufen.

WARUM JETZT HANDELN

Der regulatorische Rahmen verdichtet sich. Neben dem IT-Sicherheitskatalog erfasst NIS2 weite Teile der Energiewirtschaft und verlangt Risikomanagement, Meldepflichten und die Sicherheit der Lieferkette. Wer den Netzbetrieb verantwortet, haftet persönlich für die Umsetzung.

Zugleich ist die Bedrohungslage real. Energieversorger zählen zu den bevorzugten Zielen von Ransomware und staatlich gesteuerten Angreifern, weil ein Ausfall sofort große Wirkung entfaltet. Dieses Whitepaper ordnet die Pflichten ein, beschreibt die branchentypischen Risiken und zeigt einen realistischen Weg zur Zertifizierung.

WEN ES BETRIFFT

Drei Gruppen sind klar gefordert: Strom- und Gasnetzbetreiber über den IT-Sicherheitskatalog, Energieanlagen- und Kraftwerksbetreiber über eigene Kataloge und Schwellen, und nahezu alle größeren Versorger über NIS2. Kommt eines davon in Frage, führt am ISMS kein Weg vorbei.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken in IT und Netzleittechnik, die Anforderungen der Norm und eine Roadmap, die im Versorgungsbetrieb funktioniert.

WELTWEIT ZERTIFIZIERT

70.000+

Organisationen sind nach ISO 27001 zertifiziert, mit klar steigender Tendenz.

FÜR NETZBETREIBER

§11

Der IT-Sicherheitskatalog nach EnWG §11 verlangt ein zertifiziertes ISMS nach ISO 27001.

KONTROLLEN

93

Maßnahmen im Annex A, plus die energiespezifische Erweiterung ISO 27019.

BRANCHENKONTEXT

Die Energieversorgung ist *kritische Infrastruktur.*

Kaum ein Ausfall wirkt so unmittelbar wie der von Strom, Gas oder Wärme. Genau deshalb ist die Energiebranche reguliert wie kaum eine andere und zugleich ein bevorzugtes Ziel. ISO 27001 ist hier nicht nur Nachweis, sondern gesetzlich eingefordertes Fundament.

Fällt das Netz, steht nicht eine Firma still, *sondern eine ganze Region.*

DIE ENERGIEWENDE DIGITALISIERT DAS NETZ

Aus dem zentralen Kraftwerkspark wird ein dezentrales, digital gesteuertes System. Tausende Windräder, Solaranlagen und Speicher speisen ein, Smart Meter und Smart Grids steuern Lastflüsse in Echtzeit, Leitstellen koordinieren das Ganze. Jede neue Schnittstelle erhöht die Flexibilität und die Angriffsfläche zugleich.

Wo früher proprietäre, isolierte Steuerungstechnik lief, treffen heute IT und Betriebstechnik aufeinander. Diese Konvergenz ist der Motor der Energiewende und ihr größtes Sicherheitsthema.

EIN DICHTER PFLICHTENRAHMEN

Die Energiebranche ist mehrfach reguliert. Der IT-Sicherheitskatalog der Bundesnetzagentur nach §11 EnWG verlangt von Netzbetreibern ein zertifiziertes ISMS nach ISO 27001 und ISO 27019. Für Energieanlagen gilt ein eigener Katalog, und über die KRITIS-Regulierung sowie NIS2 kommen weitere Pflichten hinzu.

Maßgeblich ist nicht das Selbstbild, sondern Funktion und Größe. Wer Netze betreibt oder ab den einschlägigen Schwellen Anlagen verantwortet, ist erfasst und muss die Zertifizierung nachweisen, oft gegenüber der Bundesnetzagentur.

EINE GEOPOLITISCHE BEDROHUNGSLAGE

Energieinfrastruktur ist ein strategisches Ziel. Neben Ransomware-Banden greifen staatlich gesteuerte Akteure gezielt Versorger an, um Druck auszuüben oder im Ernstfall zu sabotieren. Das BSI stuft die Lage für KRITIS anhaltend als angespannt ein.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als Daten: Versorgungssicherheit, Anlagensicherheit und am Ende der Schutz von Menschen. Ein erfolgreicher Angriff auf die Netzleittechnik kann Versorgungsunterbrechungen auslösen, deren Schaden weit über die IT hinausreicht.

HERAUSFORDERUNGEN

Warum ISO 27001 in der Energie *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Branche. Der Aufwand ist es nicht. Fünf Eigenheiten der Energieversorgung machen die Umsetzung anspruchsvoller als anderswo, und für jede gibt es einen pragmatischen Umgang.

IT UND BETRIEBSTECHNIK ZUGLEICH

Anders als reine Bürobetriebe müssen Energieunternehmen auch ihre Betriebstechnik absichern: Netzleittechnik, SCADA, Fernwirktechnik und Stationsautomatisierung. Diese Systeme haben lange Lebenszyklen, lassen sich nicht beliebig patchen und dürfen im Betrieb nicht einfach abgeschaltet werden.

Genau dafür ergänzt ISO 27019 die ISO 27001 um energiespezifische Maßnahmen. Die Risikoanalyse muss IT und OT gemeinsam betrachten, ohne die Verfügbarkeit der Steuerung zu gefährden.

VERSORGUNGSSICHERHEIT HAT VORRANG

In der IT gilt oft Vertraulichkeit zuerst. In der Netzleittechnik steht die Verfügbarkeit an erster Stelle, denn die Versorgung darf nicht abreißen. Eine Sicherheitsmaßnahme, die ein Steuerungssystem destabilisiert, ist keine Option.

Maßnahmen müssen deshalb so gewählt werden, dass sie schützen, ohne den Betrieb zu stören. Wiederanlaufpläne und Redundanzen (Annex A 5.29, 5.30, 8.13) sind hier besonders wichtig.

GEWACHSENE, LANGLEBIGE ANLAGEN

Komponenten im Netz sind oft Jahrzehnte im Einsatz und stammen aus einer Zeit, in der Cybersicherheit keine Rolle spielte. Sie lassen sich selten ersetzen und kaum aktualisieren. Kompensierende Maßnahmen wie Netzsegmentierung und strenge Zugänge (Annex A 8.20 bis 8.23) schützen, wo ein Update nicht möglich ist.

DEZENTRALE ANLAGEN UND SMART METER

Mit der Energiewende verteilt sich die Erzeugung auf unzählige Standorte, von der Trafostation bis zur PV-Anlage. Jeder Fernzugang und jedes intelligente Messsystem ist ein möglicher Einstieg. Diese verteilte Angriffsfläche konsequent zu verwalten, ist eine Daueraufgabe.

NACHWEIS GEGENÜBER DER AUFSICHT

Anders als bei einer rein freiwilligen Zertifizierung prüft hier die Bundesnetzagentur. Das Zertifikat und die zugehörige Dokumentation müssen jederzeit belastbar vorliegen. Ein gut geführtes ISMS mit lückenlosem Nachweis ist deshalb kein Selbstzweck, sondern Pflichterfüllung.

BEDROHUNGSLAGE & RISIKEN

Wo die Energiebranche *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an der Netzleittechnik, an einer wachsenden Zahl dezentraler Anlagen und an einer Bedrohungslage, die auch staatliche Akteure umfasst. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · ANGRIFF AUF DIE NETZLEITTECHNIK

Der gefährlichste Ernstfall. Gelingt es Angreifern, in Leitstellen oder Fernwirktechnik einzudringen, können sie im schlimmsten Fall Schaltzustände manipulieren und die Versorgung unterbrechen. Strikte Trennung von IT und OT, Netzsegmentierung und überwachte Zugänge (Annex A 8.20 bis 8.23) sind hier die entscheidenden Schutzlinien, ergänzt um die Maßnahmen der ISO 27019.

2 · RANSOMWARE LEGT DEN BETRIEB LAHM

Auch ohne direkten Zugriff auf die Steuerung trifft Ransomware die Verwaltungs- und Abrechnungssysteme und kann den Betrieb empfindlich stören. Verschlüsselte Leitsysteme oder Kundendatenbanken bedeuten Stillstand und Meldepflicht. Getestete Backups und ein eingeübter Notfallplan (Annex A 8.13, 5.29) entscheiden über die Dauer des Ausfalls.

3 · STAATLICH GESTEUERTE ANGREIFER

Energieversorger sind ein strategisches Ziel. Hoch entwickelte Angreifer nisten sich oft monatelang unbemerkt ein, um im Ernstfall handlungsfähig zu sein. Dagegen helfen kontinuierliche Überwachung, Angriffserkennung und ein geübter Vorfallprozess (Annex A 8.16, 5.24 bis 5.27), wie ihn auch NIS2 verlangt.

4 · ANGRIFFE ÜBER DIE LIEFERKETTE

Steuerungstechnik, Wartungsdienstleister und Fernwartungszugänge sind ein beliebter Umweg ins Netz. Ein kompromittierter Hersteller oder ein manipuliertes Update wird zum Einfallstor. Lieferantensteuerung mit klaren Anforderungen und abgesicherte Fernwartung (Annex A 5.19 bis 5.23) sind deshalb zentral.

5 · VERTEILTE ANLAGEN UND FERNZUGÄNGE

Trafostationen, PV- und Windparks sowie intelligente Messsysteme sind oft nur leicht gesichert und über Fernzugänge erreichbar. Jeder dieser Punkte ist ein möglicher Einstieg in größere Systeme. Starke Authentifizierung, Verschlüsselung und lückenlose Protokollierung (Annex A 8.2, 8.5, 8.24) begrenzen dieses Risiko.

ANFORDERUNGEN DER NORM

Was ISO 27001 *konkret verlangt.*

Die Norm besteht aus zwei Teilen: den Management-Anforderungen in den Kapiteln 4 bis 10, die zertifiziert werden, und dem Annex A mit 93 Sicherheitsmaßnahmen, in der Energie ergänzt um ISO 27019. Fünf Bausteine bilden den Kern.

KONTEXT UND GELTUNGSBEREICH (KAP. 4)

Am Anfang steht die Frage, was geschützt werden soll. Das Unternehmen bestimmt internen und externen Kontext, die Erwartungen wichtiger Parteien wie Aufsicht und Kunden und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

In der Energie ist der Zuschnitt besonders wichtig, weil der IT-Sicherheitskatalog den Netzbetrieb klar umfasst. Der Scope muss die regulierten Systeme abdecken, von der Leitstelle bis zur Fernwirktechnik.

FÜHRUNG UND POLITIK (KAP. 5)

Die Norm macht Sicherheit zur Leitungsaufgabe. Die Geschäftsführung verabschiedet die Informationssicherheitsleitlinie, stellt Ressourcen bereit und weist Rollen zu (Kap. 5.1 bis 5.3). Der IT-Sicherheitskatalog verlangt zudem einen benannten Ansprechpartner für IT-Sicherheit gegenüber der Bundesnetzagentur.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Das Unternehmen legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken über IT und Netzleittechnik hinweg und entscheidet je Risiko über die Behandlung (Kap. 6.1.2 und 6.1.3). Das Ergebnis mündet in die Erklärung zur Anwendbarkeit, die für jede Maßnahme aus Annex A und ISO 27019 begründet, ob sie gilt.

Verfügbarkeit, OT-Sicherheit und Lieferkette stehen dabei fast immer oben auf der Liste.

BETRIEB UND MASSNAHMEN (KAP. 8, ANNEX A, ISO 27019)

Die ausgewählten Maßnahmen werden umgesetzt und gelebt. Der Annex A liefert 93 Maßnahmen in vier Gruppen, ISO 27019 ergänzt sie um energiespezifische Vorgaben für Prozessleit- und Fernwirktechnik. Netzsegmentierung, Zugriffskontrolle, Business Continuity und Lieferantensteuerung stehen im Vordergrund.

BEWERTUNG UND VERBESSERUNG (KAP. 9, 10)

Ein ISMS endet nicht mit der Einführung. Internes Audit und Managementbewertung (Kap. 9.2 und 9.3) prüfen regelmäßig die Wirksamkeit, Korrekturmaßnahmen schließen Lücken (Kap. 10.2). Genau diese Schleife erwarten Zertifizierer und Aufsicht gleichermaßen.

UMSETZUNG IN DER PRAXIS

In sechs Schritten *zum Zertifikat.*

Der Weg zur Zertifizierung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene Strukturen, statt bei null zu beginnen. Realistisch sind je nach Reife und Anlagenlandschaft sechs bis zwölf Monate bis zum Audit.

Ein ISMS nach ISO 27001 erfüllt den IT-Sicherheitskatalog und einen Großteil von NIS2 zugleich. *Ein Aufbau, mehrere Pflichten.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die regulierten Bereiche schneiden: Netzbetrieb, Leitstellen, zugehörige IT und OT. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und entscheidend für die Prüfung durch die Aufsicht.

2 · FÜHRUNG, LEITLINIE, ANSPRECHPARTNER

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, stellt Ressourcen bereit und benennt den Ansprechpartner IT-Sicherheit, den der IT-Sicherheitskatalog gegenüber der Bundesnetzagentur fordert.

3 · RISIKEN IN IT UND OT ANALYSIEREN

Assets erfassen, von der Verwaltung über Leitstellen bis zur Fernwirktechnik. Risiken gemeinsam für IT und Betriebstechnik bewerten, Verfügbarkeit besonders gewichten und die Erklärung zur Anwendbarkeit mit Annex A und ISO 27019 erstellen.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Netzsegmentierung, Zugriffs- und Fernwartungskontrolle, Backup und Angriffserkennung. Jede Maßnahme so festhalten, dass sie im Audit und vor der Aufsicht Bestand hat.

5 · INTERN AUDITIEREN UND BEWERTEN

Vor dem Zertifizierungsaudit prüft ein internes Audit die Wirksamkeit, die Managementbewertung zieht Bilanz. Diese Schleife einmal vollständig zu durchlaufen ist Pflicht und zugleich die beste Generalprobe.

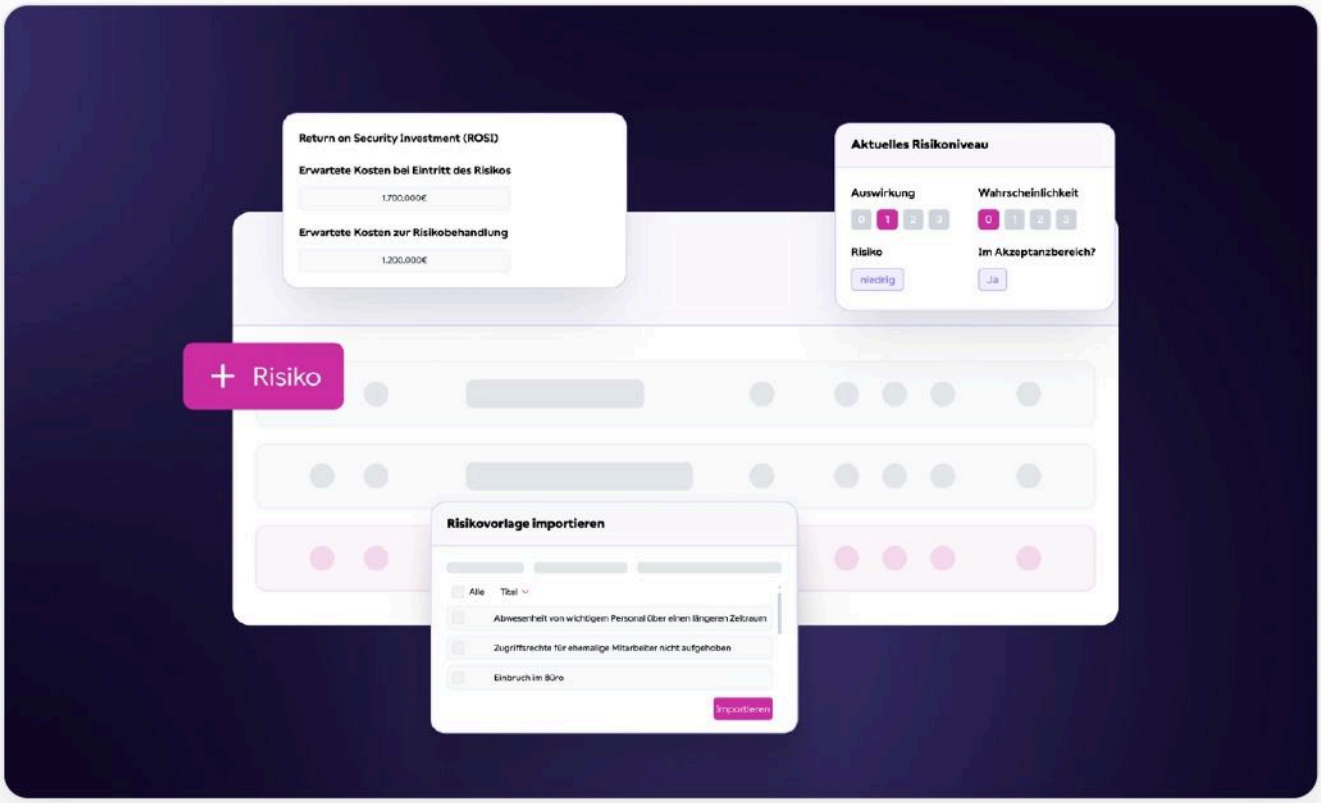
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung (Stage 2). Danach folgt das Zertifikat, gültig für drei Jahre mit jährlichen Überwachungsaudits, und der Nachweis gegenüber der Bundesnetzagentur.

WIE SECJUR ES EINFACH MACHT

Von der Pflicht zur *auditbereiten Umsetzung.*

Das Digital Compliance Office (DCO) führt Energieunternehmen durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse über IT und OT, Maßnahmen nach Annex A und ISO 27019, interne Audits und Nachweise an einem Ort. Statt monatelanger Beratung und einem Dutzend Tabellen arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Unternehmen berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Risiko über IT & OT

Geführte Risikoanalyse, die Verwaltung und Netzleittechnik gemeinsam betrachtet und die Maßnahmen aus Annex A und ISO 27019 nachvollziehbar begründet.

Lieferanten & Fernwartung

Lieferantensteuerung und Nachweise für Hersteller, Wartungsdienstleister und Fernwartungszugänge, genau dort, wo Annex A 5.19 bis 5.23 hinschaut.

Audit & Aufsicht

Revisionssichere Dokumentation und ein voller Audit-Trail, mit dem Zertifizierungsaudit und Nachweis gegenüber der Bundesnetzagentur gelingen.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist strukturiert. Sie legen den Geltungsbereich fest, das DCO führt Sie durch jede Anforderung von ISO 27001 und ISO 27019, und wo eine Expertin nötig ist, ist sie zugeschaltet. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereites ISMS, ohne dass der Netzbetrieb gefährdet wird.

EIN AUFBAU, MEHRERE PFLICHTEN

Weil sich IT-Sicherheitskatalog, ISO 27001 und NIS2 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegen muss.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Energieversorger, Netzbetreiber, Industrieunternehmen und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Energiebranche:

„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

REFERENZEN AUS ENERGIE, VERSORGUNG UND INDUSTRIE

1KOMMA5° · Stadtwerke Zamstetten · Consolinno ENERGY · Stadtwerke Nienburg Energie · Changing Cities · CUBOS

AUDIT-ERFOLG
100%
Erfolgsquote in bisherigen Zertifizierungsaudits.

SCHNELLER
50%
Weniger Aufwand gegenüber klassischer Beratung.

INTEGRATIONEN
60+
Native API-Anbindungen, von Microsoft 365 bis JIRA.

STANDARDS
10+
Frameworks parallel abgedeckt, ohne Doppelarbeit.

WARUM ENERGIEUNTERNEHMEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und in der Branchentiefe. Statt monatelanger Beratung führt ein klarer Pfad durch ISO 27001 und ISO 27019, mit Vorlagen, die IT und Netzleittechnik gemeinsam denken. Das Team bleibt beim Betrieb, das ISMS entsteht parallel.

Der digitale Compliance-Officer (DCO) bündelt Richtlinien, Aufgaben und Nachweise an einem Ort und verteilt Verantwortlichkeiten automatisch an die richtigen Personen. Über 60 Integrationen holen Belege direkt aus den Systemen, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Weil derselbe Unterbau ISO 27001, ISO 27019 und einen Großteil von NIS2 zugleich trägt, ist der IT-Sicherheitskatalog mit einem Aufbau erfüllt, statt in getrennten Projekten abgearbeitet zu werden.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat und der Nachweis gegenüber der Bundesnetzagentur, sondern ein Versorger, der seine Risiken in IT und OT kennt und im Ernstfall handlungsfähig bleibt. Genau das schützt die Versorgung.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Betriebsvorteil: Audits der Aufsicht verlieren ihren Schrecken, Störungen werden schneller beherrscht, und Netzleittechnik wie Verwaltung ziehen an einem Strang.

So wird aus einer Pflicht ein dauerhafter Schutz der Versorgungssicherheit, der mit jeder neuen dezentralen Anlage und jedem Smart Meter an Bedeutung gewinnt.

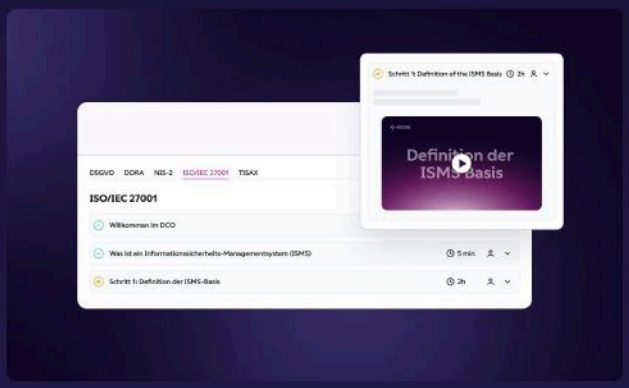
SECJUR

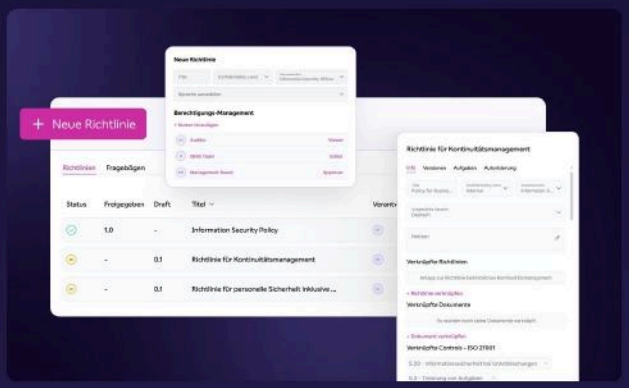
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 Rammelsberg · Consolinno Energy · Stadtwerke Nienburg Energie · Changing Cities · CUBOS

www.secjur.com