



ISO 27001 · VER- & ENTSORGUNG

ISO 27001 für Stadtwerke: *Schutz, der nie Pause macht.*

Wasser, Abwasser, Strom, Wärme und Abfall: Die kommunale Ver- und Entsorgung hält das Gemeinwesen am Laufen und gehört zur kritischen Infrastruktur. Ihre Prozessleittechnik ist zunehmend vernetzt, KRITIS-Betreiber müssen ihre Sicherheit regelmäßig nachweisen, und NIS2 erweitert den Kreis der verpflichteten Betriebe deutlich. Dieses Whitepaper zeigt, warum ISO 27001 das passende Fundament ist, wo die größten Schwachstellen in IT und Anlagentechnik liegen und wie ein ISMS entsteht, das die Versorgung nicht gefährdet.

ISO 27001

NIS2

KRITIS

B3S

DSGVO

MADE & HOSTED
IN GERMANY

In der Ver- und Entsorgung ist Sicherheit *Schutz der Versorgung.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). In der kommunalen Ver- und Entsorgung ist er mehr als freiwillig: Wasser, Abwasser, Abfall und Energie zählen zur kritischen Infrastruktur, und KRITIS-Betreiber müssen ihre Vorkehrungen regelmäßig nach dem Stand der Technik nachweisen, häufig über ein ISMS nach ISO 27001 oder einen branchenspezifischen Sicherheitsstandard (B3S).

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

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 Pflichtenrahmen verdichtet sich. Neben der KRITIS-Nachweispflicht erweitert NIS2 den Kreis

der erfassten Betriebe erheblich, auch kleinere Ver- und Entsorger fallen nun häufiger darunter. Verlangt werden Risikomanagement, Meldepflichten und Lieferkettensicherheit, und die Leitung trägt die Verantwortung.

Zugleich ist die Bedrohungslage ernst. Versorger zählen zu den bevorzugten Zielen von Ransomware und staatlich gesteuerten Angreifern, weil ein Ausfall die Bevölkerung unmittelbar trifft. Dieses Whitepaper ordnet die Pflichten ein, beschreibt die branchentypischen Risiken und zeigt einen realistischen Weg zur Zertifizierung.

WEN ES BETRIFFT

Gefordert sind Betreiber kritischer Anlagen in Wasser, Abwasser, Abfall und Energie über die KRITIS-Nachweispflicht, ein wachsender Kreis weiterer Ver- und Entsorger über NIS2 sowie Stadtwerke im Querverbund, die mehrere dieser Sparten bündeln. 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 Anlagentechnik, 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.

AKTUELLE FASSUNG

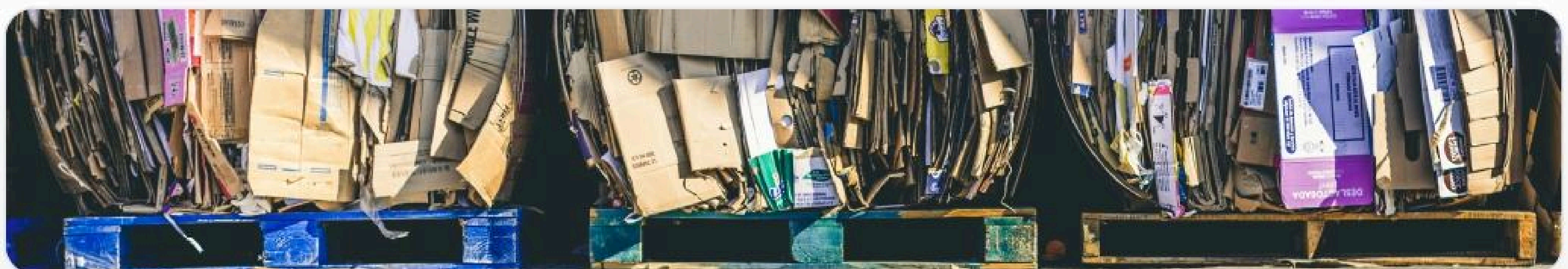
2022

Seit dem 31.10.2025 zählt allein die Fassung von 2022, die Version von 2013 ist ausgelaufen.

KONTROLLEN

93

Maßnahmen im Annex A, ergänzbar um branchenspezifische Standards (B3S, ISO 27019).



Die Versorgung ist *kritische Infrastruktur vor Ort*.

Kein Ausfall ist im Alltag so spürbar wie der von Wasser, Strom oder Wärme. Genau deshalb sind kommunale Ver- und Entsorger reguliert wie kaum eine Branche und zugleich ein lohnendes Ziel. ISO 27001 ist hier nicht nur Nachweis, sondern Schutz der Daseinsvorsorge.

Fällt das Wasserwerk aus, steht nicht eine Firma still, *sondern eine ganze Stadt*.

VERNETZTE ANLAGEN, VIELE SPARTEN

Stadtwerke und kommunale Betriebe steuern ihre Anlagen über Prozessleittechnik und SCADA: Wasserwerke, Pumpstationen, Kläranlagen, Fernwärmenetze, Müllheizkraftwerke. Daneben laufen Abrechnung, Kundenportale und Verwaltung über klassische IT. Im Querverbund bündelt ein Versorger oft mehrere dieser Sparten unter einem Dach.

Diese Vernetzung verbessert den Betrieb und vergrößert die Angriffsfläche zugleich. Wo IT und Anlagentechnik aufeinandertreffen, entstehen die kritischen Punkte, und sie betreffen nicht nur Daten, sondern die Versorgung selbst.

EIN DICHTER PFLICHTENRAHMEN

Wasser, Abwasser, Abfall und Energie sind KRITIS-Sektoren. Betreiber kritischer Anlagen müssen ihre Sicherheit regelmäßig nach dem Stand der Technik nachweisen, üblicherweise über ein ISMS nach ISO 27001 oder einen

branchenspezifischen Sicherheitsstandard wie den B3S Wasser oder Abwasser.

NIS2 erweitert diesen Kreis deutlich. Auch Betriebe unterhalb der bisherigen KRITIS-Schwellen fallen nun häufiger unter die Pflichten. Maßgeblich sind Sektor und Größe, nicht das Selbstbild des Betriebs.

EINE ERNSTE BEDROHUNGSLAGE

Versorgungsinfrastruktur ist ein strategisches Ziel. Neben Ransomware greifen auch staatlich gesteuerte Akteure gezielt Versorger an, um Druck auszuüben oder zu sabotieren. Das BSI bewertet die Lage für KRITIS anhaltend als angespannt.

WAS AUF DEM SPIEL STEHT

Es geht um Versorgungssicherheit, um Umwelt- und Gesundheitsschutz und um das Vertrauen der Bürgerinnen und Bürger. Ein Angriff auf die Prozessleittechnik kann Versorgung unterbrechen oder die Abwasserbehandlung stören, mit Folgen weit über die IT hinaus.



Warum ISO 27001 in der Versorgung *besonders fordert.*

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

IT UND PROZESSLEITTECHNIK ZUGLEICH

Anders als reine Verwaltungen müssen Versorger auch ihre Anlagentechnik absichern: SCADA, Fernwirktechnik und Steuerung von Wasserwerken, Pumpen und Kläranlagen. Diese Systeme haben lange Lebenszyklen, lassen sich kaum patchen und dürfen im Betrieb nicht einfach abgeschaltet werden.

Die Risikoanalyse muss IT und Anlagentechnik gemeinsam betrachten. Branchenspezifische Standards wie der B3S und, im Energiebereich, ISO 27019 ergänzen die ISO 27001 um passende Maßnahmen.

VERSORGUNGSSICHERHEIT HAT VORRANG

In der Büro-IT steht oft Vertraulichkeit zuerst. In der Anlagentechnik ist die Verfügbarkeit überlebenswichtig, denn die Versorgung darf nicht abreißen. Eine Sicherheitsmaßnahme, die eine Steuerung destabilisiert, ist keine Option.

Maßnahmen müssen schützen, ohne den Betrieb zu stören. Wiederanlaufpläne, Redundanzen und ein geübter Notbetrieb (Annex A 5.29, 5.30, 8.13) sind hier besonders wichtig.

GEWACHSENE, LANGLEBIGE ANLAGEN

Komponenten in Wasserwerken und Netzen sind oft Jahrzehnte im Einsatz und stammen aus einer Zeit ohne Cybersicherheit. 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.

QUERVERBUND UND SCOPE

Stadtwerke bündeln Strom, Wasser, Wärme und teils Abfall und Verkehr in einem Haus. Das erschwert den Zuschnitt des ISMS: Der Geltungsbereich muss die kritischen Sparten klar erfassen, ohne sich zu verzetteln. Ein durchdachter Scope (Kap. 4.3) ist hier der wichtigste Hebel.

KNAPPE KOMMUNALE IT

Viele Betriebe haben kleine IT-Teams ohne eigene Sicherheitsfunktion, der Fachkräftemangel und kommunale Haushalte verschärfen das. Die Norm verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die führen und dokumentieren, machen den Unterschied.



Wo die Versorgung *konkret angreifbar ist.*

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

1 · ANGRIFF AUF DIE PROZESSLEITTECHNIK

Der gefährlichste Ernstfall. Gelingt es Angreifern, in die Steuerung von Wasserwerken, Pumpen oder Kläranlagen einzudringen, drohen Versorgungsunterbrechungen oder gestörte Abwasserbehandlung mit Gefahren für Gesundheit und Umwelt. Strikte Trennung von IT und Anlagentechnik, Netzsegmentierung und überwachte Zugänge (Annex A 8.20 bis 8.23) sind die entscheidenden Schutzlinien.

2 · RANSOMWARE LEGT DEN BETRIEB LAHM

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

3 · STAATLICH GESTEUERTE ANGREIFER

Versorger 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 Vorfalprozess (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 in die Anlagen. Ein kompromittierter Hersteller oder ein manipuliertes Update wird zum Einfallstor. Lieferantensteuerung und abgesicherte Fernwartung (Annex A 5.19 bis 5.23) sind deshalb zentral.

5 · BÜRGERDATEN UND ABRECHNUNG

Versorger verwalten die Daten und Bankverbindungen Hunderttausender Haushalte. Ein Abfluss aus dem Abrechnungs- oder Kundenportal ist ein schwerer DSGVO-Vorfall und beschädigt das Vertrauen der Bürger. Verschlüsselung und strenge Zugriffskontrolle (Annex A 8.24, 8.2 bis 8.5) schützen diese Daten.



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, ergänzt um branchenspezifische Standards. Fünf Bausteine bilden den Kern.

KONTEXT UND GELTUNGSBEREICH (KAP. 4)

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

Gerade im Querverbund ist der Zuschnitt entscheidend. Der Scope muss die kritischen Sparten und ihre Anlagen klar abdecken, von der Leitstelle bis zur Fernwirktechnik. Ein zu weit gefasster Geltungsbereich ist der häufigste vermeidbare Fehler.

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). KRITIS-Betreiber benennen zudem eine Kontaktstelle gegenüber dem BSI.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Der Betrieb legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken über IT und Anlagentechnik 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 begründet, ob sie gilt.

Verfügbarkeit, Schutz der Prozessleittechnik und Lieferkette stehen dabei fast immer oben auf der Liste.

BETRIEB UND MASSNAHMEN (KAP. 8, ANNEX A, B3S)

Die ausgewählten Maßnahmen werden umgesetzt und gelebt. Der Annex A liefert 93 Maßnahmen in vier Gruppen, branchenspezifische Standards wie der B3S Wasser ergänzen sie um passende Vorgaben für die Anlagentechnik. Netzsegmentierung, Zugriffskontrolle und Business Continuity 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). Diese Schleife deckt sich mit der regelmäßigen KRITIS-Nachweispflicht.



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 die KRITIS-Nachweispflicht und NIS2 zugleich. *Ein Aufbau, mehrere Pflichten.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die kritischen Sparten schneiden: Wasser, Abwasser, Energie, Abfall, samt Leitstellen und zugehöriger IT. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und für die Nachweise gegenüber der Aufsicht.

2 · FÜHRUNG, LEITLINIE, KONTAKTSTELLE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, stellt Ressourcen bereit und benennt die nötigen Rollen, einschließlich der KRITIS-Kontaktstelle gegenüber dem BSI.

3 · RISIKEN IN IT UND OT ANALYSIEREN

Assets erfassen, von der Verwaltung über Leitstellen bis zur Fernwirktechnik der Anlagen. Risiken gemeinsam für IT und Anlagentechnik bewerten, Verfügbarkeit besonders gewichten und die Erklärung zur Anwendbarkeit 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.

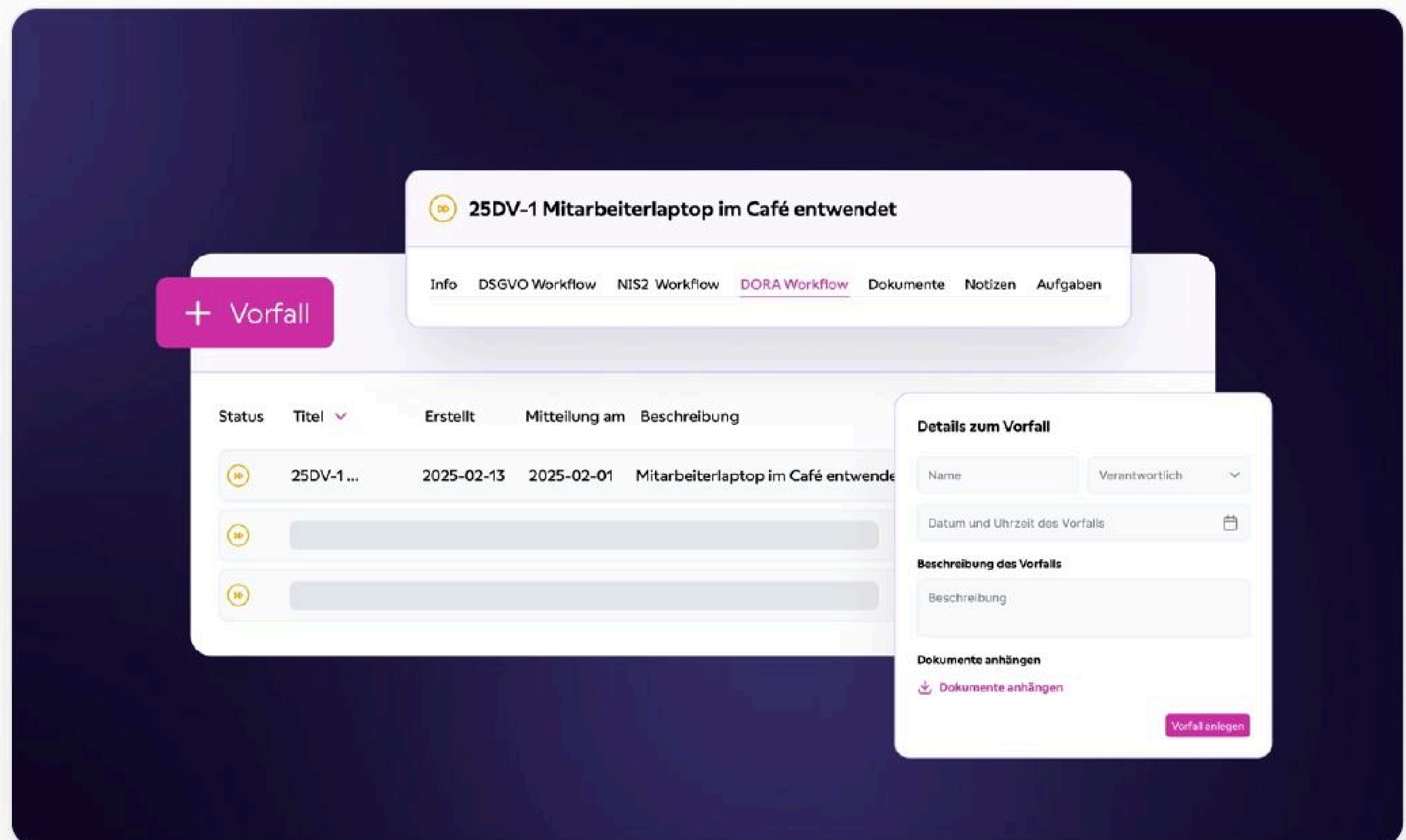
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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 es stützt zugleich die KRITIS-Nachweise.



Von der Pflicht zur *auditbereiten Umsetzung*.

Das Digital Compliance Office (DCO) führt Stadtwerke und kommunale Ver- und Entsorger durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse über IT und Anlagentechnik, Maßnahmen, 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. Betriebe berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Risiko & Resilienz

Geführte Risikoanalyse über IT und Prozessleittechnik und ein strukturierter Umgang mit Vorfällen und Wiederanlauf, damit die Versorgung im Ernstfall trägt.

Lieferanten & Fernwartung

Lieferantensteuerung und Nachweise für Anlagenhersteller und Wartungsdienste, genau dort, wo Fernzugänge und Annex A 5.19 bis 5.23 hinschauen.

KRITIS-Nachweis & Audit

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

SO LÄUFT DIE EINFÜHRUNG

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

EIN AUFBAU, MEHRERE PFLICHTEN

Weil sich KRITIS-Nachweis, 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.*

Stadtwerke, Versorger, Energieunternehmen und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Ver- und Entsorgung:

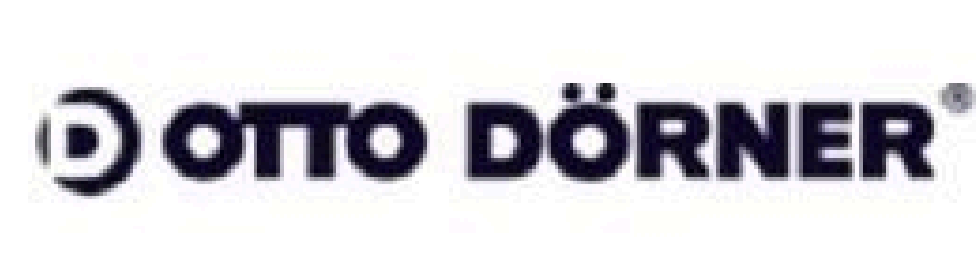
ISMS-Aufbau für die Stadtwerke *Kamp-Lintfort & Nienburg/Weser.*

Die Stadtwerke Kamp-Lintfort und die Stadtwerke Nienburg/Weser haben frühzeitig erkannt, dass Informationssicherheit nicht nur eine regulatorische Pflicht ist, sondern auch ein entscheidender Wettbewerbsfaktor für die Energieversorgung von morgen.

Mit SECJUR fiel die Wahl auf eine automatisierte, praxisnahe Lösung, die von erfahrenen Experten eng begleitet wird. Ziel war es, ein vollumfängliches ISMS nach ISO 27001 aufzubauen und die Stadtwerke gleichzeitig auch auf die kommenden NIS2-Anforderungen vorzubereiten.

Mit dem ISMS demonstrieren die Stadtwerke Kamp-Lintfort und Nienburg/Weser beispielhaft, wie kommunale Versorger heute schon Verantwortung für die Informationssicherheit übernehmen, und sich mit SECJUR zukunftssicher aufstellen.

REFERENZEN AUS STADTWERKEN, VERSORGUNG UND ENERGIE



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 VERSORGER SECJUR WÄHLEN

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

Nachweise entstehen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus Leitsystemen und Verwaltung, sodass Betrieb und Sicherheit an einer Quelle arbeiten statt an parallelen

Tabellen. So bleibt der Aufwand auch im Querverbund mit mehreren Sparten planbar.

MEHR ALS EIN ZERTIFIKAT

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

Weil dieselbe Struktur ISO 27001, KRITIS-Nachweis und NIS2 gemeinsam bedient, deckt ein Projekt mehrere Pflichten zugleich ab. Das senkt den Aufwand und hält den Betrieb gegenüber Aufsicht, Kommune und Bürgern jederzeit nachweisfähig.

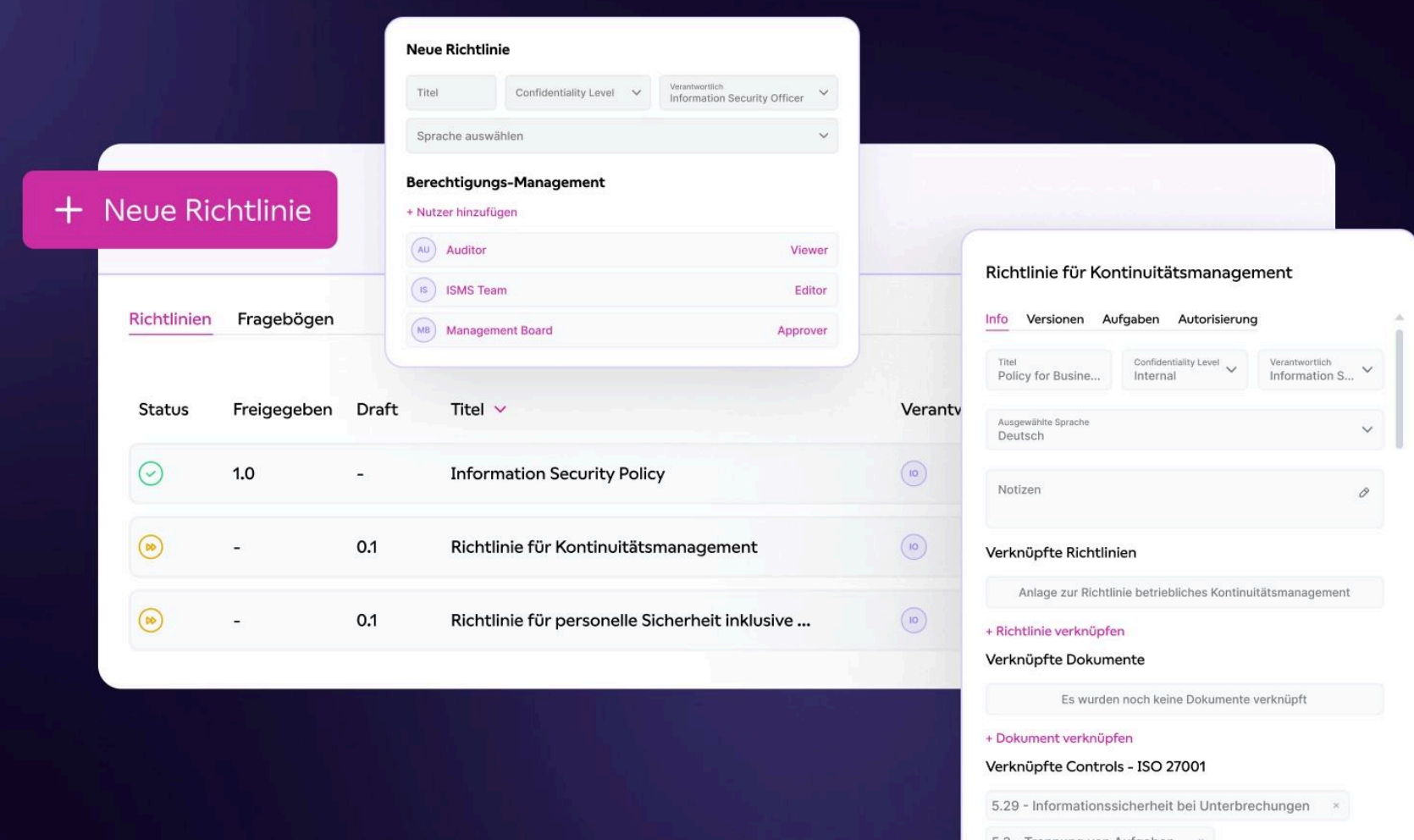
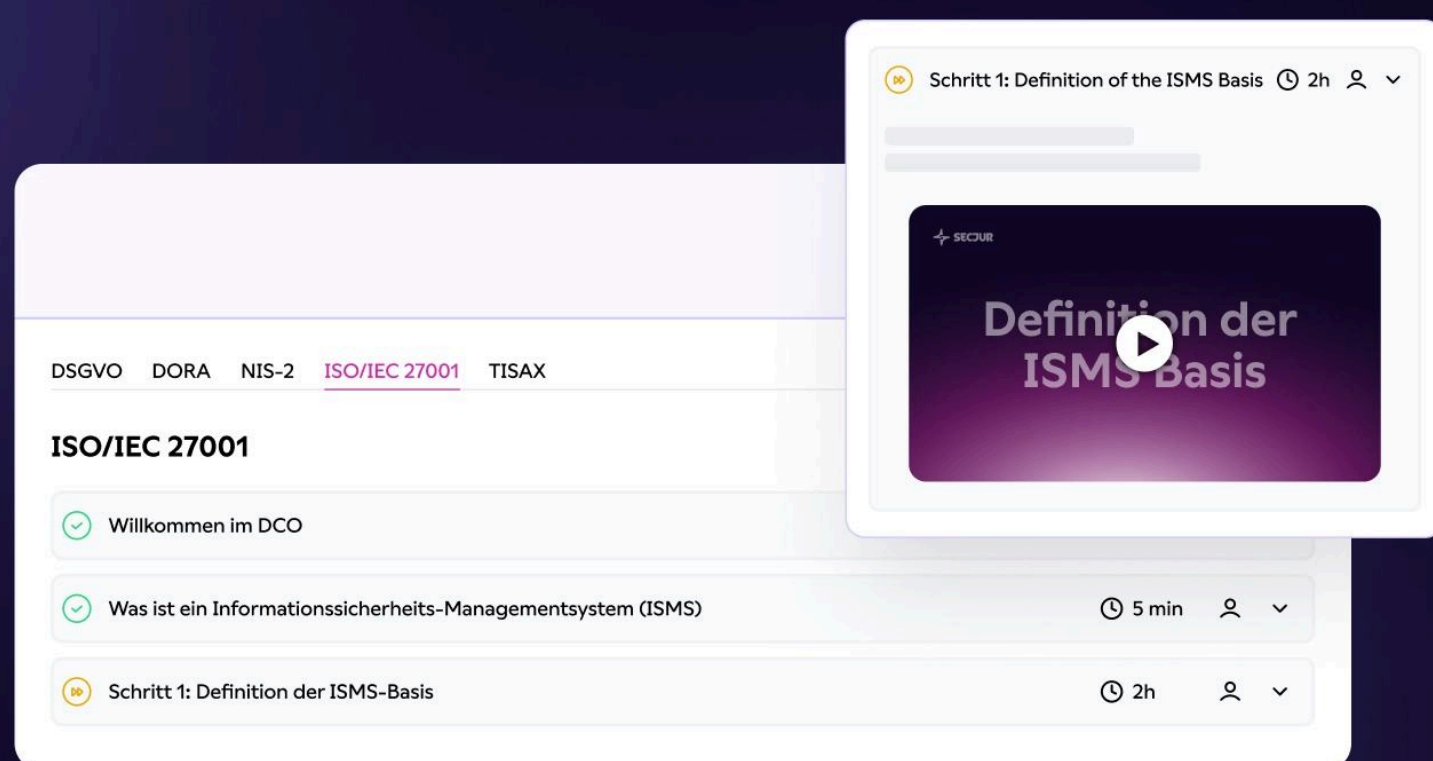


Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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:

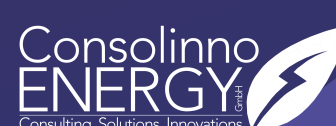
Dank SECJUR konnten wir schnell ein hochwertiges ISMS aufbauen, wie uns auch in den Zertifizierungsaudits bestätigt wurde. Unser zugewiesener Berater hat uns stets kompetent unterstützt – als wäre er ein Teil der Firma. Freuen uns auf die weitere Zusammenarbeit!



Stefan Gregori
Chief Information
Security Officer



FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR



www.secjur.com