SECJUR

WHITEPAPER
2026

ISO 27001 · LOGISTIK & TRANSPORT

ISO 27001 in der Logistik: *Sicherheit, die den Warenfluss schützt.*

Verlader und Auftraggeber prüfen ihre Dienstleister immer genauer, und ein Stillstand in der IT legt heute den physischen Warenfluss lahm. ISO 27001 ist der Nachweis, dass ein Logistikunternehmen seine Systeme und die Daten seiner Kunden im Griff hat. Dieses Whitepaper zeigt, warum sich der Standard für Speditionen, Lager- und Transportbetriebe lohnt, wo die größten Schwachstellen liegen und wie ein ISMS entsteht, ohne den laufenden Betrieb auszubremsen.

ISO 27001 | NIS2 | TISAX® | ISO 9001 | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Sicherheit ist in der Logistik *zum Auftragskriterium geworden.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 ist er kein Gesetz, sondern freiwillig. Genau das macht ihn für die Logistik wertvoll: Ein Zertifikat ist ein unabhängiger Nachweis, dass ein Betrieb seine Disposition, seine Lagersysteme und die Daten seiner Verlader schützt. In Ausschreibungen und Rahmenverträgen wird dieser Nachweis immer öfter zur Bedingung.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der dafür sorgt, dass der Warenfluss auch dann weiterläuft, wenn ein System ausfällt oder ein Angriff erfolgt.

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 Druck kommt von zwei Seiten. Verlader und Industriekunden geben ihre eigenen Sicherheitsanforderungen über die Lieferkette weiter und verlangen den Nachweis vertraglich. Zugleich erfasst NIS2 weite Teile des Verkehrssektors, und ein ISO-27001-ISMS deckt einen Großteil dieser gesetzlichen Pflichten gleich mit ab.

Hinzu kommt die Bedrohungslage. Ransomware zählt zu den größten Risiken für die deutsche Wirtschaft, und Logistik ist ein lohnendes Ziel, weil Stillstand sofort teuer wird. Dieses Whitepaper ordnet ein, was die Norm verlangt, welche Risiken die Branche konkret trägt und wie der Weg zur Zertifizierung aussieht.

WOFÜR SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: Sie verlieren Ausschreibungen mangels Zertifikat, Ihre Auftraggeber schicken Sicherheitsfragebögen, oder Sie fallen ohnehin unter NIS2. Trifft eines davon zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Der Standard ist verhältnismäßig. Er schreibt kein Konzern-Schutzniveau vor, sondern eines, das zur Größe und zum Risiko des Betriebs passt. Ein schlankes, sauber geführtes ISMS reicht für die Zertifizierung aus.

WELTWEIT ZERTIFIZIERT

70.000+

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

AKTUELLE FASSUNG

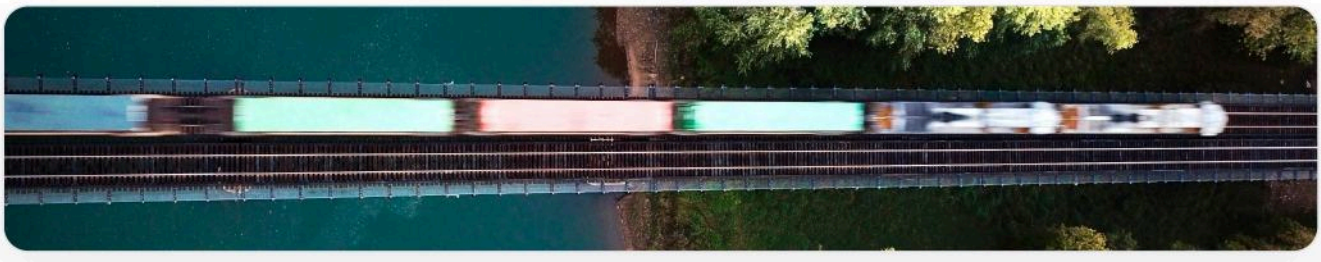
2022

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

KONTROLLEN

93

Maßnahmen im Annex A, in vier Gruppen von organisatorisch bis technisch.



BRANCHENKONTEXT

Die Logistik ist *das Nervensystem der Wirtschaft.*

Kaum eine Branche ist so vernetzt und so zeitkritisch wie die Logistik. Genau das macht sie für Angreifer attraktiv und für Auftraggeber zum Prüffall. ISO 27001 macht die Sicherheit eines Betriebs nachweisbar, statt sie nur zu behaupten.

Wenn das Transportmanagementsystem steht, steht der Warenfluss. *Stunden entscheiden, nicht Tage.*

ZWANZIG JAHRE DIGITALISIERUNG

Was früher Telefon, Fax und Papierfrachtbrief war, läuft heute über vernetzte Systeme. Transportmanagement (TMS), Lagerverwaltung (WMS), Telematik in der Flotte, automatisierte Hochregallager, Sendungsverfolgung und elektronischer Datenaustausch (EDI) bilden eine durchgehende digitale Kette vom Auftrag bis zur Auslieferung.

Hinzu kommen Zollanbindungen wie ATLAS und Buchungsplattformen. Jede dieser Schnittstellen ist Effizienzgewinn und Angriffsfläche zugleich. Was den Betrieb schnell macht, macht ihn auch verwundbar.

AUFTRAGGEBER PRÜFEN GENAUER

Große Verlader und Industriekunden kaufen Logistik nicht mehr ohne Prüfung. Bevor ein Konzern einen Dienstleister in seine Lieferkette lässt, durchläuft dieser eine Lieferantenprüfung mit langen Sicherheitsfragebögen. ISO 27001 beantwortet einen Großteil davon mit einem einzigen Dokument.

Ohne Zertifikat wird aus der Ausschreibung ein Prüfmarathon, und manche Vergabe ist von vornherein verloren. Mit Zertifikat steht der Betrieb auf der Auswahlliste, statt vorab auszuscheiden. Sicherheit wird so vom Kostenposten zum Vertriebsargument.

DIE NIS2-VERBINDUNG

Der Verkehrssektor fällt weitgehend unter NIS2. Wer ein ISMS nach ISO 27001 betreibt, erfüllt damit einen Großteil der gesetzlichen Pflichten aus dem NIS2-Umsetzungsgesetz, etwa Risikomanagement, Lieferkettensicherheit und Notfallvorsorge. Ein Aufbau, zwei Ergebnisse.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als IT-Ausfall: gerissene Liefertermine, Vertragsstrafen, abwandernde Verlader und ein beschädigter Ruf. In einem Markt, der von Zuverlässigkeit lebt, ist Sicherheit längst ein Wettbewerbsfaktor.

HERAUSFORDERUNGEN

Warum ISO 27001 in der Logistik *besonders fordert.*

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

ZEITKRITIKALITÄT OHNE PUFFER

Ein Maschinenbauer kann die Produktion drei Tage anhalten. Ein Logistiker kann das nicht. Fällt das TMS oder WMS aus, stoppen Disposition, Kommissionierung und Verladung sofort. Just-in-time-Zusagen platzen innerhalb von Stunden.

Für das ISMS heißt das: Die Wiederanlaufzeiten betriebsnaher Systeme müssen kurz sein, mit getesteten Backups und einem belastbaren Notfallplan. Die Norm verlangt genau diese Vorsorge (Annex A 5.29, 5.30, 8.13).

GEWACHSENE IT- UND OT-LANDSCHAFT

Neben klassischer IT steuern operative Systeme den physischen Betrieb: Telematik, Lagerautomatik, Tor- und Rampensteuerung, Scanner und Förderanlagen. Vieles davon ist über Jahre gewachsen, läuft auf älteren Ständen und war nie für offene Vernetzung gedacht.

Diese Übergänge zwischen OT und IT sind der wunde Punkt der Branche und verdienen in der Risikoanalyse nach Kap. 6 besondere Aufmerksamkeit.

TIEFE SUBUNTERNEHMER-NETZE

Speditionen arbeiten mit Frachtführern, Lagerpartnern, Zollagenten und IT-Dienstleistern. Jeder Zugang ist ein möglicher Einstiegspunkt. Die Norm verlangt Sicherheit in der Lieferantenbeziehung (Annex A 5.19 bis 5.23), also Anforderungen an Dienstleister und deren Nachweis. In einem fragmentierten Markt ist das harte, dauerhafte Arbeit, aber genau hier liegt der größte Hebel.

DÜNNE MARGEN, SAISONSPITZEN

Die Branche arbeitet mit knappen Margen, Budget für Sicherheit ist selten üppig. Hier hilft das Prinzip der Verhältnismäßigkeit: Maßnahmen müssen zur Größe und zum Risiko passen, nicht zum Konzernmaßstab. Zugleich treffen Angriffe in Spitzenzeiten besonders hart, wenn alles unter Volllast läuft und das Team weniger wachsam ist.

DÜNNE IT-DECKE

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

BEDROHUNGSLAGE & RISIKEN

Wo Logistik *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an konkreten Systemen und an einem Netz aus Partnern, das ein einzelner Betrieb kaum allein kontrolliert. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE STOPPT DEN WARENFLUSS

Der häufigste Ernstfall. Wird das TMS oder WMS verschlüsselt, lässt sich nicht mehr disponieren, kommissionieren oder verladen. Der Betrieb fällt auf manuellen Notbetrieb zurück, Sendungen stauen sich, Termine reißen. Getestete Backups und ein eingeübter Notfallplan (Annex A 8.13, 5.29) entscheiden, ob der Stillstand Stunden oder Tage dauert.

2 · ANGRIFFE ÜBER DIE LIEFERKETTE

Angreifer nutzen den schwächsten Partner als Tür. Ein kompromittierter Frachtführer, Lagerpartner oder Software-Dienstleister wird zum Einfallstor in das eigene Netz. Genau hier setzt die Lieferantensteuerung nach Annex A 5.19 bis 5.23 an, mit Mindestanforderungen und deren Überprüfung. Verlader fordern diesen Nachweis zunehmend selbst ein.

3 · OT- UND TELEMATIK-KOMPROMITTIERUNG

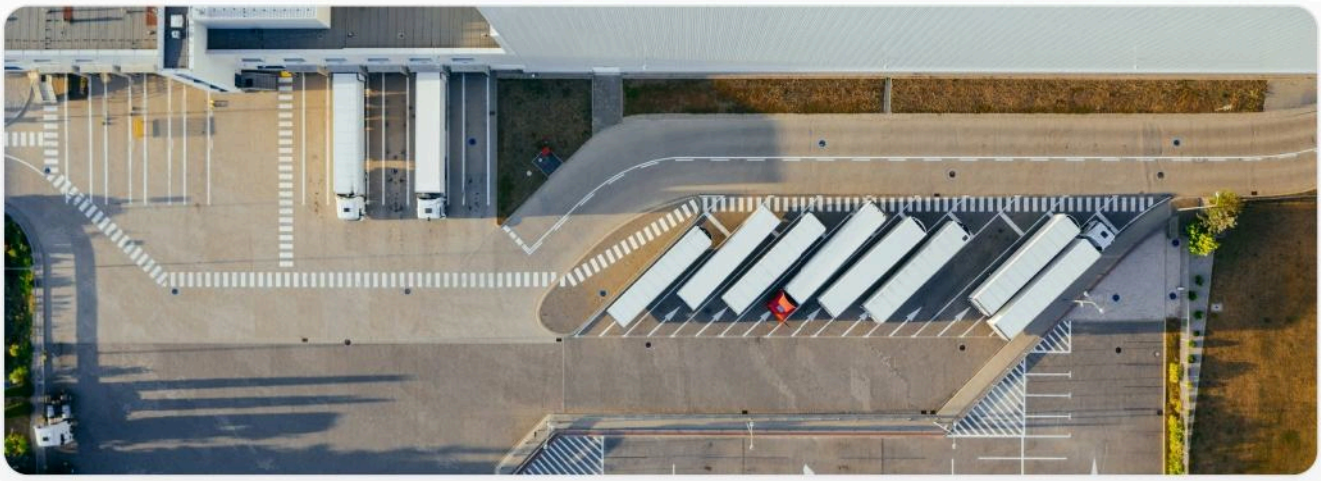
Flotten-Telematik, Lagerautomatik und Steueranlagen sind angreifbar, wenn sie offen vernetzt und selten gepatcht sind. Manipulierte Standortdaten oder lahmgelegte Förderanlagen wirken unmittelbar auf den physischen Betrieb. Anders als klassische IT lassen sich solche Anlagen selten einfach neu starten, ohne den Betrieb zu unterbrechen.

4 · DIEBSTAHL SENSIBLER DATEN

Sendungsdaten, Zolldokumente, Tarife und Kundendaten fließen permanent zwischen Systemen und über EDI-Schnittstellen. Ein Abfluss ist nicht nur ein DSGVO-Vorfall, sondern kostet Vertrauen bei Verladern und kann Wettbewerber begünstigen. Verschlüsselung und Zugriffskontrolle (Annex A 8.24, 8.2 bis 8.5) sind hier die zentralen Hebel.

5 · FRACHTBETRUG UND SCHWACHE ZUGÄNGE

Überlastangriffe auf Track-and-Trace-Portale legen den Kundenkontakt lahm. Frachtbetrug mit gefälschten Lieferadressen, untergeschobenen Aufträgen oder manipulierten Rechnungen verursacht direkten Schaden. Multifaktor-Authentifizierung und saubere Rechtevergabe (Annex A 5.17, 8.5) verhindern einen Großteil davon und kosten wenig.



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, aus denen risikobasiert ausgewählt wird. 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 Verlader und Aufsicht und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Für Logistiker ist der Zuschnitt entscheidend. Ein klarer Scope, etwa Disposition, Lager und die zugehörige IT, hält die Zertifizierung schlank und auditierbar. 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). Das deckt sich mit der persönlichen Leitungsverantwortung, die auch NIS2 verlangt.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Der Betrieb legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken von TMS bis OT 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 der 93 Maßnahmen begründet, ob sie gilt.

Genau hier zahlt sich Verhältnismäßigkeit aus. Nicht jede Maßnahme passt zu jedem Betrieb, aber jede Auswahl muss nachvollziehbar sein.

BETRIEB UND MASSNAHMEN (KAP. 8, ANNEX A)

Die ausgewählten Maßnahmen werden umgesetzt und gelebt. Der Annex A gliedert sie in vier Gruppen: 37 organisatorische, 8 personenbezogene, 14 physische und 34 technische Maßnahmen. In der Logistik stehen Lieferantensteuerung, Notfallvorsorge, Zugriffskontrolle und physische Sicherheit der Lagerstandorte 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 will der Auditor sehen: nicht Perfektion, sondern einen gelebten Kreislauf.

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 drei bis sechs Monate bis zum Audit.

Ein ISMS nach ISO 27001 deckt zugleich einen Großteil von NIS2 ab. *Ein Aufbau, zwei Ergebnisse.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope eng schneiden: welche Standorte, welche Systeme, welche Prozesse. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und der wirksamste Hebel, um den Aufwand niedrig zu halten.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. Dieser Schritt ist schnell erledigt, wenn die Leitung dahintersteht.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von TMS und WMS über Telematik bis zu den OT/IT-Übergängen. Risiken bewerten, Lücken sichtbar machen und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse trennt das Wichtige vom Nebensächlichen und macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Backup, Zugriffskontrolle, Multifaktor-Anmeldung und Lieferantenanforderungen. Jede Maßnahme so festhalten, dass sie im Audit 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.

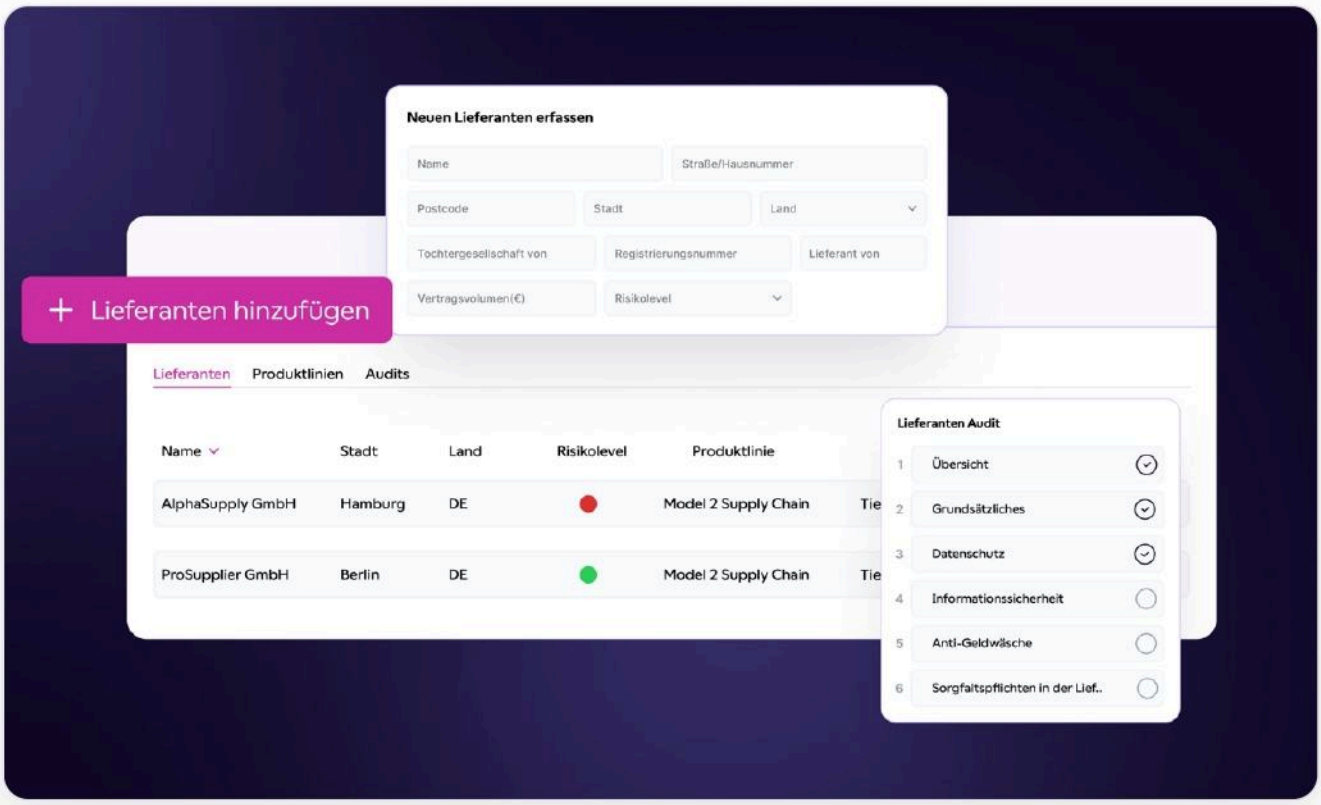
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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. ISO 27001 ist damit kein Projekt mit Enddatum, sondern ein dauerhafter Prozess.

WIE SECJUR ES EINFACH MACHT

Vom ersten Scope zum *zertifizierten ISMS.*

Das Digital Compliance Office (DCO) führt Logistikbetriebe durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse, Lieferantensteuerung, 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 & SoA

Geführte Risikoanalyse über TMS, WMS und OT/IT-Übergänge und eine Erklärung zur Anwendbarkeit, die jede Maßnahme nachvollziehbar begründet.

Lieferanten & Lieferkette

Lieferantenbewertung und Nachweise für Frachtführer, Lager- und IT-Partner, genau dort, wo Verlader und Annex A 5.19 bis 5.23 hinschauen.

Nachweise & Audit

Revisionssichere Dokumentation, internes Audit und ein voller Audit-Trail, mit dem das Zertifizierungsaudit zur Formsache wird.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. 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 in Wochen statt in Quartalen, ohne dass der Betrieb stillsteht.

EIN AUFBAU, ZWEI ERGEBNISSE

Weil ISO 27001 und NIS2 sich weitgehend überschneiden, deckt das DCO beide zugleich ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, von Microsoft 365 bis zur Cloud, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegen muss.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Industrieunternehmen, Logistiker, Energieversorger und digitale Dienstleister erfüllen mit dem DCO ihre Sicherheitsanforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Logistik:

„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 LOGISTIK UND ANGRENZENDEN BRANCHEN

OTTO DÖRNER · SVG · orbit · bm bahndienste · HADAG

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 LOGISTIKER SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen, die zum Betrieb passen statt zum Konzern. Das Team bleibt beim Tagesgeschäft, das ISMS entsteht parallel.

Nachweise entstehen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass IT, Betrieb und Disposition an einer Quelle arbeiten statt an parallelen Tabellen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Betrieb, der seine Risiken kennt, seine Lieferkette im Griff hat und in der nächsten Ausschreibung souverän auftritt. Genau das gewinnt Aufträge und hält Verlader.

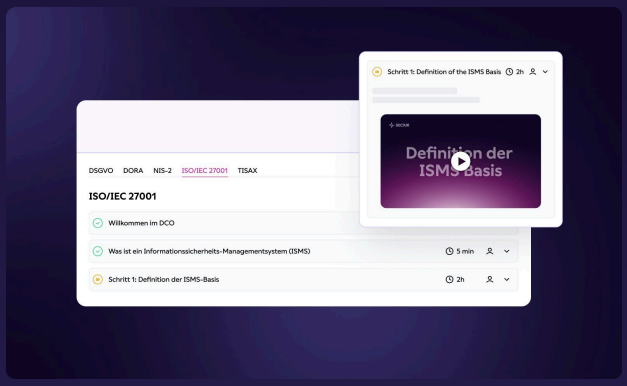
Weil dieselbe Struktur ISO 27001 und die NIS2-Pflichten gemeinsam bedient, deckt ein Projekt mehrere Anforderungen ab. Das senkt den Aufwand und hält den Betrieb auch nach dem Audit jederzeit nachweisfähig.

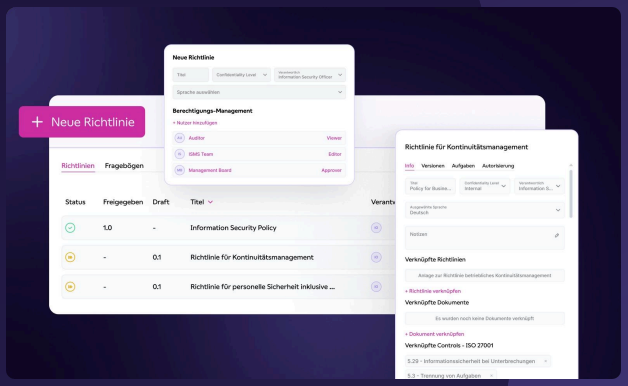
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

CONSOLINNO energy

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

OTTO DÖRNER® · SVG · HEADWAY headwaylogistic gmbh · bm bahndienste · HADAG

www.secjur.com