SECJUR

WHITEPAPER
2026

ISO 27001 · INDUSTRIE & FERTIGUNG

ISO 27001 in der Fertigung: *Schutz für Produktion und Know-how.*

Die Industrie ist das Herz der deutschen Wirtschaft und ein bevorzugtes Ziel von Angreifern. Mit Industrie 4.0 wächst die vernetzte Produktion, OEM-Kunden geben ihre Sicherheitsanforderungen über die Lieferkette weiter, und Industriespionage zielt auf wertvolle Konstruktionsdaten. ISO 27001 ist der anerkannte Nachweis, dass ein Unternehmen Produktion und Wissen im Griff hat, und zugleich die Basis für TISAX in der Automobilbranche. Dieses Whitepaper zeigt, wo die Schwachstellen liegen und wie ein passendes ISMS entsteht.

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

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In der Industrie schützt Sicherheit *Produktion und Vorsprung.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 ist er freiwillig. Für Industrie und Fertigung ist er trotzdem fast unverzichtbar: OEM-Kunden verlangen den Nachweis über die Lieferkette, in der Automobilbranche meist als TISAX, das direkt auf ISO 27001 aufbaut. Das Zertifikat belegt, dass Produktion, Konstruktionsdaten und Kundendaten geschützt sind.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der Büro-IT und Produktionstechnik gleichermaßen absichert, von der Konstruktion bis zur Fertigungslinie.

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 mehreren Seiten. Große Hersteller und OEMs geben ihre Sicherheitsanforderungen an Zulieferer weiter und verlangen den Nachweis vertraglich. Zugleich erfasst NIS2 Teile des verarbeitenden Gewerbes, etwa die Herstellung von Maschinen, Fahrzeugen, Elektronik und Medizinprodukten, und ein ISO-27001-ISMS deckt diese Pflichten weitgehend mit ab.

Hinzu kommt die Bedrohungslage. Ransomware und Industriespionage treffen die Industrie hart, weil ein Produktionsstillstand sofort teuer wird und Konstruktionswissen einen jahrelangen Vorsprung bedeutet. Dieses Whitepaper ordnet ein, was die Norm verlangt, welche Risiken bestehen und wie der Weg zur Zertifizierung aussieht.

WOFÜR SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: OEM-Kunden fordern TISAX oder ein Zertifikat, Sie fallen unter NIS2, oder Sie wollen Konstruktionsdaten und Verfahren vor Spionage schützen. Trifft eines zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: ISO 27001 ist die Basis, auf der TISAX und ein Großteil von NIS2 aufsetzen. Ein einmal aufgebautes ISMS trägt mehrere Nachweise zugleich, statt für jede Anforderung von vorn zu beginnen.

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, Basis auch für TISAX in der Automobil-Lieferkette.

BRANCHENKONTEXT

Die vernetzte Fabrik ist *Chance und Angriffsfläche.*

Industrie 4.0 verbindet Konstruktion, Produktion und Lieferkette zu einem digitalen System. Das steigert die Effizienz und macht Fertigungsunternehmen zugleich verwundbar. OEM-Kunden und Gesetzgeber verlangen deshalb nachweisbare Sicherheit, und ISO 27001 liefert sie.

Im Maschinenbau steckt das Kapital in den Daten: *Konstruktion, Verfahren, Rezeptur.*

INDUSTRIE 4.0 VERNETZT DIE PRODUKTION

Aus isolierten Maschinen wird eine vernetzte Fabrik. Manufacturing-Execution-Systeme (MES), speicherprogrammierbare Steuerungen (SPS), SCADA, IIoT-Sensorik und digitale Zwillinge verbinden Konstruktion, Fertigung und Wartung in Echtzeit. ERP und Engineering-Systeme hängen direkt am Produktionsnetz.

Diese Vernetzung bringt Produktivität und Angriffsfläche zugleich. Wo früher isolierte Steuerungstechnik lief, treffen heute IT und Betriebstechnik aufeinander, und genau dort entstehen die kritischen Punkte.

DIE OEM-LIEFERKETTE GIBT DEN TAKT VOR

Große Hersteller kaufen nicht ohne Prüfung. Zulieferer durchlaufen Lieferantenprüfungen mit umfangreichen Sicherheitsfragebögen, und in der Automobilbranche ist TISAX faktisch Pflicht, um gelistet zu bleiben. TISAX baut direkt auf den Anforderungen der ISO 27001 auf.

Wer ISO 27001 umsetzt, schafft damit zugleich die Grundlage für TISAX und beantwortet einen Großteil der Fragebögen mit einem Dokument. Statt jede Anfrage einzeln zu bearbeiten, legt der Zulieferer den anerkannten Nachweis vor.

NIS2 UND DIE BEDROHUNGSLAGE

NIS2 erfasst Teile des verarbeitenden Gewerbes, von Maschinen- und Fahrzeugbau bis zu Elektronik und Medizinprodukten. Zugleich zählen Ransomware und Industriespionage zu den größten Bedrohungen, gerade für die exportstarken Hidden Champions mit wertvollem Know-how.

WAS AUF DEM SPIEL STEHT

Es geht um Produktionsausfälle mit Vertragsstrafen, um den Verlust von Konstruktionswissen an Wettbewerber und um die Listung beim OEM. In einer Branche, die von Präzision und Zuverlässigkeit lebt, ist Sicherheit ein Wettbewerbsfaktor.

HERAUSFORDERUNGEN

Warum ISO 27001 in der Industrie *besonders fordert.*

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

IT TRIFFT PRODUKTIONSTECHNIK

Neben klassischer IT steuern operative Systeme die Fertigung: SPS, SCADA, MES und Maschinensteuerungen. Vieles ist über Jahrzehnte gewachsen, läuft auf älteren Ständen und darf im laufenden Betrieb nicht einfach abgeschaltet werden.

Die Risikoanalyse muss IT und OT gemeinsam betrachten, ohne die Verfügbarkeit der Linie zu gefährden. Kompensierende Maßnahmen wie Netzsegmentierung und strenge Zugänge (Annex A 8.20 bis 8.23) schützen, wo ein Update nicht möglich ist.

SCHUTZ DES KONSTRUKTIONSWISSENS

Konstruktionsdaten, Verfahren und Patente sind das Kapital vieler Industrieunternehmen. Sie liegen in CAD-, PLM- und Engineering-Systemen und werden mit Partnern geteilt. Genau darauf zielt Industriespionage.

Strenge Zugriffskontrolle, Verschlüsselung und Klassifizierung von Informationen (Annex A 5.12, 8.2 bis 8.5, 8.24) sind hier zentral, ebenso die Absicherung des Datenaustauschs mit Entwicklungspartnern.

VERFÜGBARKEIT DER PRODUKTION

Ein Produktionsstopp ist teuer und reißt Liefertermine. Anders als in der Büro-IT steht in der Fertigung die Verfügbarkeit weit oben. Eine Maßnahme, die eine Anlage destabilisiert, ist keine Option.

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

GLOBALE STANDORTE UND LIEFERKETTEN

Fertigung verteilt sich oft auf mehrere Werke und ein dichtes Netz aus Zulieferern und Dienstleistern mit Fernwartungszugängen. Jeder Standort und jeder Partner erweitert die Angriffsfläche. Lieferantensteuerung und einheitliche Vorgaben (Annex A 5.19 bis 5.23) werden zur Daueraufgabe.

DÜNNE IT-DECKE IM MASCHINENBAU

Viele mittelständische Hersteller haben kleine IT-Teams ohne eigene Sicherheitsfunktion, der Fachkräftemangel verschärft das. Die Norm verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle (Kap. 5 und 7), nicht Heldentaten Einzelner. Werkzeuge, die führen und dokumentieren, machen den Unterschied.

BEDROHUNGSLAGE & RISIKEN

Wo die Industrie *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an vernetzter Produktionstechnik, an wertvollem Konstruktionswissen und an einer tief verzweigten Lieferkette. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE STOPPT DIE FERTIGUNG

Der häufigste und teuerste Ernstfall. Werden ERP, MES oder Steuerungssysteme verschlüsselt, steht die Produktion. Aufträge platzen, Liefertermine reißen, Vertragsstrafen drohen, und der Wiederanlauf zieht sich oft über Tage. Getestete Backups, Segmentierung und ein eingeübter Notfallplan (Annex A 8.13, 5.29, 8.20 bis 8.23) entscheiden über die Dauer des Stillstands und damit über den Schaden.

2 · INDUSTRIESPIONAGE UND IP-DIEBSTAHL

Der gefährlichste Angriff auf den Vorsprung. Werden Konstruktionsdaten, Verfahren oder Patente abgegriffen, ist der Wettbewerbsvorteil von Jahren dahin, oft unbemerkt. Hoch entwickelte Angreifer zielen gezielt auf CAD- und PLM-Systeme. Strenge Zugriffskontrolle, Verschlüsselung und Klassifizierung (Annex A 5.12, 8.2 bis 8.5, 8.24) schützen dieses Kapital.

3 · SABOTAGE DER PRODUKTIONSTECHNIK

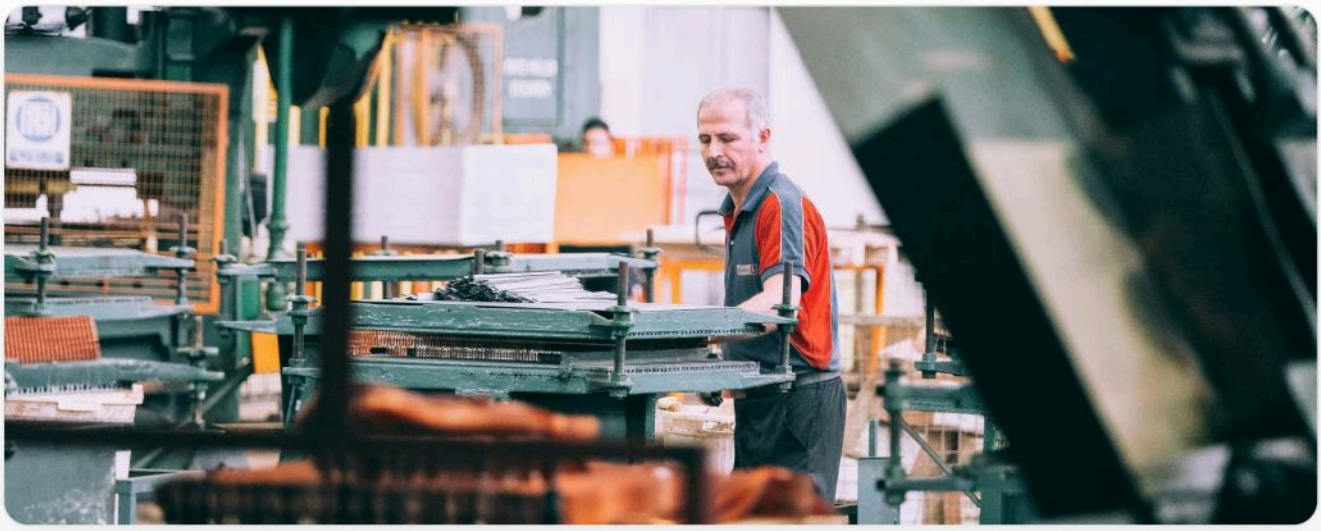
Werden SPS, SCADA oder MES manipuliert, drohen nicht nur Ausfälle, sondern auch Qualitätsmängel und Gefahren für die Anlagensicherheit. Manipulierte Parameter können ganze Chargen unbrauchbar machen. Trennung von IT und OT sowie überwachte Zugänge (Annex A 8.20 bis 8.23) sind hier zentral.

4 · ANGRIFFE ÜBER DIE LIEFERKETTE

Zulieferer, Maschinenhersteller und Wartungsdienste mit Fernzugängen sind ein beliebter Umweg ins Werk. Ein kompromittierter Partner oder ein manipuliertes Update wird zum Einfallstor. Lieferantensteuerung mit klaren Anforderungen und abgesicherte Fernwartung (Annex A 5.19 bis 5.23) begrenzen das Risiko.

5 · VERNETZTE MASCHINEN UND FERNWARTUNG

IIoT-Geräte und fernwartbare Anlagen sind oft nur leicht gesichert und dauerhaft erreichbar. Jeder dieser Zugänge ist ein möglicher Einstieg in das Produktionsnetz. Starke Authentifizierung, abgesicherte Fernzugänge und Protokollierung (Annex A 8.2, 8.5, 8.15) 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, aus denen risikobasiert ausgewählt wird. 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 OEM-Kunden und Aufsicht und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

In der Fertigung ist der Zuschnitt entscheidend. Ein klarer Scope, etwa Entwicklung und Produktion an einem Standort, hält die Zertifizierung schlank und auditierbar und passt zugleich zum TISAX-Scope. 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). Aus dem Qualitätsmanagement nach ISO 9001 ist diese Leitungsverantwortung vielen Betrieben vertraut.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Das Unternehmen legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken über IT und Produktionstechnik 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 der 93 Maßnahmen begründet, ob sie gilt.

OT-Sicherheit, Schutz des Konstruktionswissens und Lieferkette stehen dabei fast immer oben auf der Liste.

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 Fertigung stehen Netzsegmentierung, Zugriffskontrolle, Informationsklassifizierung und Lieferantensteuerung 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). Wer ISO 9001 betreibt, kennt diese Schleife bereits und kann sie übertragen.

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 aus dem Qualitätsmanagement, statt bei null zu beginnen. Realistisch sind je nach Reife und Anlagenlandschaft sechs bis zwölf Monate bis zum Audit.

Ein ISMS nach ISO 27001 ist die Basis für TISAX und einen Großteil von NIS2. *Ein Aufbau, mehrere Nachweise.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope eng schneiden: welcher Standort, welche Entwicklung und Produktion, welche Systeme. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und lässt sich zugleich am TISAX-Scope ausrichten.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. Wo ein Qualitätsmanagement besteht, lässt sich gut daran anknüpfen.

3 · RISIKEN IN IT UND OT ANALYSIEREN

Assets erfassen, von CAD und PLM über ERP und MES bis zu den Maschinensteuerungen. Risiken gemeinsam für IT und Produktionstechnik bewerten, Verfügbarkeit und IP-Schutz besonders gewichten und die Erklärung zur Anwendbarkeit erstellen.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Netzsegmentierung, Zugriffskontrolle, Schutz der Konstruktionsdaten und abgesicherte Fernwartung. 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. Für Betriebe mit ISO-9001-Erfahrung ist dieser Schritt vertrautes Terrain.

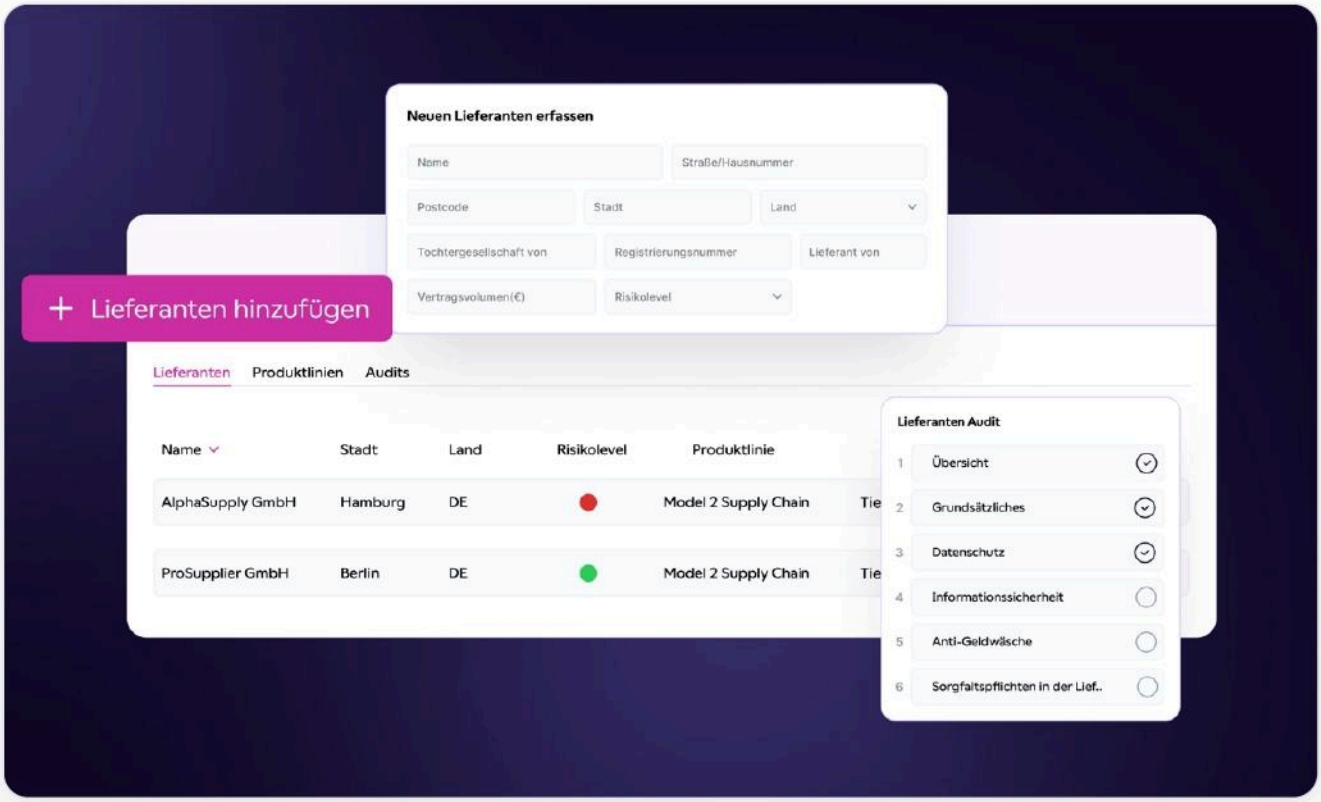
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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 bildet die Basis für eine TISAX-Bewertung.

WIE SECJUR ES EINFACH MACHT

Vom Kunden- und Gesetzesdruck zur *auditbereiten Umsetzung.*

Das Digital Compliance Office (DCO) führt Industrieunternehmen durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse über IT und Produktion, Maßnahmen, interne Audits und Nachweise an einem Ort, als Basis auch für TISAX und NIS2. 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 Büro-IT und Produktionstechnik gemeinsam betrachtet und jede Maßnahme nachvollziehbar begründet und priorisiert.

Lieferanten & TISAX

Lieferantensteuerung und Nachweise für die OEM-Lieferkette, mit ISO 27001 als Basis, auf der eine TISAX-Bewertung direkt aufsetzt.

Audit & Frameworks

Revisionssichere Dokumentation und ein voller Audit-Trail, der zugleich TISAX und einen Großteil von NIS2 trägt.

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 die Produktion stillsteht.

EIN AUFBAU, MEHRERE NACHWEISE

Weil ISO 27001 die Basis für TISAX bildet und sich mit NIS2 überschneidet, 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.*

Industrieunternehmen, Zulieferer, Maschinenbauer und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Industrie:

„Wir konnten wie geplant *neue OEM-Projekte erlangen und so den Unternehmensumsatz steigern.* Die Plattform ist super hilfreich und unsere Ansprechpartnerin unterstützt uns stets kompetent."

Steffen Brureiner
Projektleiter IT
KLEINER STANZTECHNIK
CoCREATE THE FUTURE

REFERENZEN AUS INDUSTRIE, MASCHINENBAU UND FERTIGUNG

BAUMANN · oetinger aluminium · Bitzer · STEYRMOTORS · DUO PLAST · SWT STAHLWERK THÜRINGEN

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, von ISO 27001 bis TISAX.

WARUM INDUSTRIEUNTERNEHMEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und der Branchentiefe. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen, die IT und Produktionstechnik gemeinsam denken und ISO 27001 wie TISAX bedienen. Das Team bleibt an der Fertigung, das ISMS entsteht parallel.

Nachweise entstehen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass IT, Produktion und Qualitätssicherung 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 Produktion absichert, sein Konstruktionswissen schützt und in jeder OEM-Prüfung souverän auftritt. Genau das sichert Listungen und Vorsprung.

Weil dieselbe Struktur ISO 27001, TISAX 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.

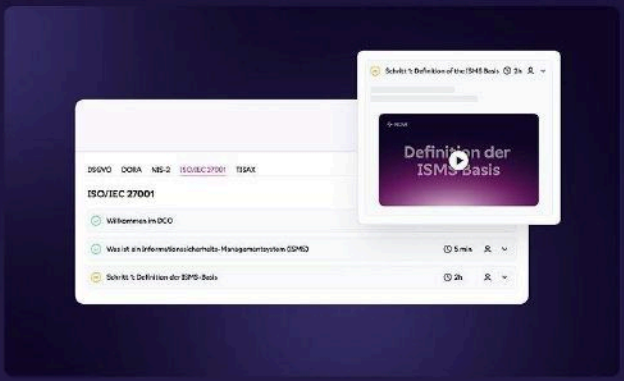
SECJUR

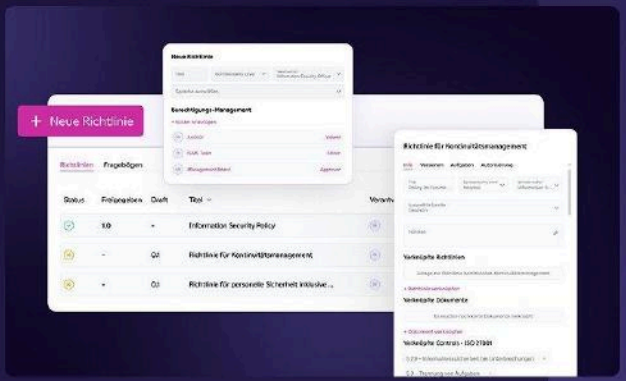
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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:

“Wir konnten wie geplant neue OEM-Projekte erlangen und so den Unternehmensumsatz steigern. Die Plattform ist super hilfreich und unsere Ansprechpartnerin unterstützt uns stets kompetent.”

Steffen Brureiner
Projektleiter IT

KLEINER STANZTECHNIK
CoCREATE THE FUTURE

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

SWT STAHLWERK THÜRINGEN · OTTO DÖRNER · oetinger aluminium · FEDDERSEN · STEYRMOTORS

www.secjur.com