SECJUR

WHITEPAPER
2026

NIS2 · INDUSTRIE, MASCHINENBAU & FERTIGUNG

# NIS2 in Industrie & 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. Das NIS2-Umsetzungsgesetz erfasst zudem weite Teile des verarbeitenden Gewerbes. Dieses Whitepaper zeigt, welche Pflichten gelten, wo die größten Schwachstellen in IT und Produktionstechnik liegen und wie ein ISMS entsteht, das NIS2, TISAX und die OEM-Anforderungen zugleich bedient.

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

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

# In der Industrie schützt Sicherheit Produktion und Vorsprung.

## DAS WICHTIGSTE IN KÜRZE

Das NIS2-Umsetzungsgesetz (NIS2UmsuCG) ist am 6. Dezember 2025 in Kraft getreten und novelliert das BSI-Gesetz. Eine Übergangsfrist gibt es nicht. NIS2 erfasst Teile des verarbeitenden Gewerbes, etwa die Herstellung von Maschinen, Fahrzeugen und Kfz-Teilen, Elektronik und Medizinprodukten.

Für Industrie und Fertigung ist NIS2 dabei nur ein Treiber von mehreren. OEM-Kunden verlangen den Sicherheitsnachweis über die Lieferkette, in der Automobilbranche meist als TISAX, das direkt auf ISO 27001 aufbaut. Maßgeblich sind Sektor und Größe: Wer 50 Beschäftigte oder 10 Millionen Euro erreicht, ist im erfassten Sektor eine wichtige Einrichtung, große Hersteller sind besonders wichtig. Ein ISMS nach ISO 27001 deckt diese Pflichten weitgehend gemeinsam ab. Anders als das frühere KRITIS-Recht knüpft NIS2 an Sektor und Größe an, wodurch deutlich mehr Betriebe erfasst werden. Wer die Prüfung sauber dokumentiert, schützt die Geschäftsführung im Zweifel vor Haftung.

## WARUM JETZT HANDELN

Der Druck kommt von mehreren Seiten. Große Hersteller und OEMs geben ihre Sicherheitsanforderungen an Zulieferer weiter und verlangen den Nachweis vertraglich. Parallel läuft die NIS2-Pflicht mit Registrierung und Meldewegen, die BSI-Frist endete am 31. Juli 2026.

Hinzu kommt die Bedrohungslage. Ransomware und Industriespionage treffen die Industrie hart, weil ein Produktionsstillstand sofort teuer wird und Konstruktionswissen einen jahrelangen Vorsprung bedeutet. Ein Vorfall trifft hier nicht nur die IT, sondern sofort Liefertermine und Listungen. Wer den Nachweis früh aufbaut, begegnet OEM-Kunden und Aufsicht aus einer Position der Stärke.

## EIN AUFBAU, MEHRERE NACHWEISE

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. Es sichert Büro-IT und Produktionstechnik gleichermaßen, von der Konstruktion bis zur Fertigungslinie.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken in IT und Produktionstechnik, die Pflichten aus dem Gesetz und eine Roadmap, die im Fertigungsbetrieb funktioniert. So bleibt die knappe IT-Kapazität an der Fertigung, statt in Formularen zu versickern. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht im Betrieb.

BETROFFEN

**29.500**

Unternehmen in 18 Sektoren fallen unter NIS2, Teile des verarbeitenden Gewerbes darunter.

OEM-STANDARD

**TISAX**

In der Automobil-Lieferkette faktisch Pflicht, direkt auf ISO 27001 aufbauend.

BUSSGELD

**10 Mio €**

Bis zu 10 Mio. Euro bei besonders wichtigen, bis zu 7 Mio. bei wichtigen Einrichtungen.

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.

## 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, speicherprogrammierbare Steuerungen, 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. Schon ein Blick auf die Übergänge zwischen ERP und Maschinennetz zeigt, wo die dringendsten Lücken liegen.

### 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. Wer den Nachweis früh vorlegt, bleibt im Vergabeprozess ein bevorzugter Partner.

### 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. Gerade der Mittelstand unterschätzt oft, wie attraktiv sein Spezialwissen für Angreifer ist.

### 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.

Ein sauberer Nachweis wird damit zum Vertriebsargument. Er sichert Aufträge und macht aus einer Pflicht einen Vorsprung gegenüber Wettbewerbern, die den Nachweis erst noch aufbauen müssen. Ein einziger längerer Stillstand kann eine ganze Auftragsplanung durcheinanderbringen.

HERAUSFORDERUNGEN

# Warum NIS2 in der Industrie besonders fordert.

Die Anforderungen gelten unabhängig von der Branche, der Aufwand ist es nicht. Sechs 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. Netzsegmentierung und strenge Zugänge schützen, wo ein Update nicht möglich ist. Genau dafür ist die getrennte Betrachtung von Büro- und Produktionsnetz der wirksamste erste Schritt.

### 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 sind hier besonders wichtig. Ein zweiter, getrennter Datenstand verkürzt den Wiederanlauf erheblich.

### 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 sind hier zentral, ebenso die Absicherung des Datenaustauschs mit Entwicklungspartnern. Wer weiß, wo die wertvollsten Daten liegen, kann sie zuerst und am stärksten schützen.

### 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 werden zur Daueraufgabe. Einheitliche Mindeststandards über alle Werke hinweg verhindern, dass ein schwaches Glied die ganze Kette gefährdet.

### DÜNNE IT-DECKE IM MASCHINENBAU

Viele mittelständische Hersteller haben kleine IT-Teams ohne eigene Sicherheitsfunktion, der Fachkräftemangel verschärft das. NIS2 verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die führen und dokumentieren, machen den Unterschied.

### AUDIT-KULTUR AUS ISO 9001

Anders als manche Branche kennt die Fertigung strenge Audits längst, etwa aus ISO 9001. Dokumentation, interne Audits und Korrekturmaßnahmen sind vertraut. Diese Kultur lässt sich auf das ISMS übertragen und verkürzt den Weg zur NIS2-Konformität spürbar.

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, vom Netz getrennte Backups, Segmentierung und ein eingeübter Notfallplan entscheiden über die Dauer des Stillstands und damit über den Schaden. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit. Ein aktueller Notfallplan legt vorab fest, wer was entscheidet.

### 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 schützen dieses Kapital. Eine Klassifizierung der Daten sorgt dafür, dass die sensibelsten Informationen am stärksten geschützt sind. Auffällige Zugriffe fallen nur auf, wenn sie protokolliert werden.

### 3 · SABOTAGE DER PRODUKTIONSTECHNIK

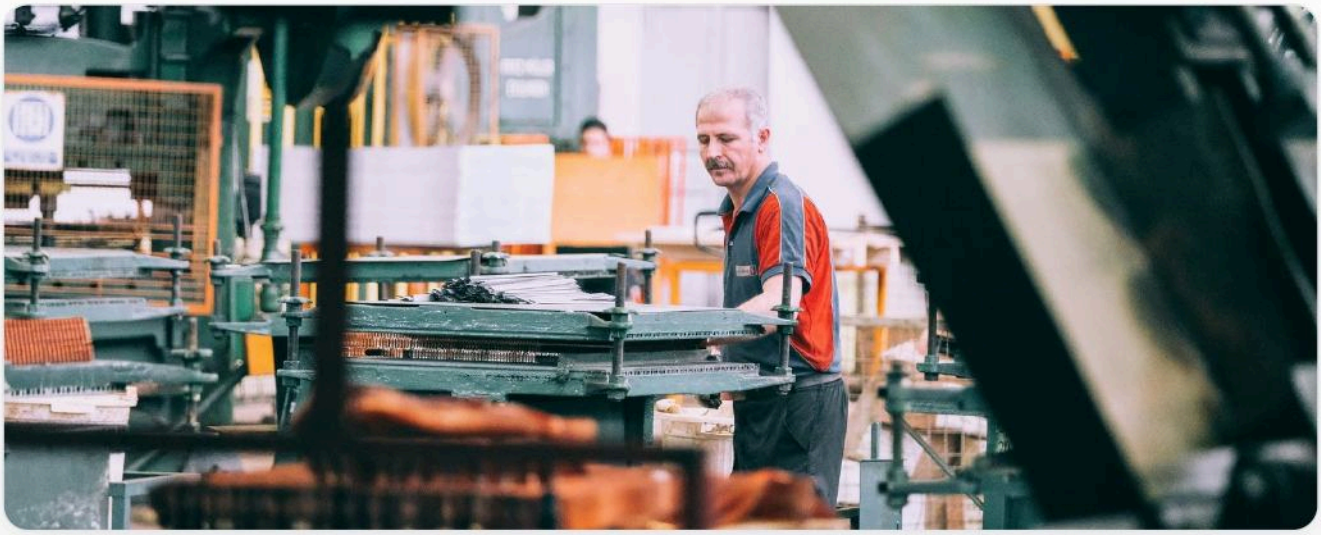
Werden SPS, SCADA oder MES manipuliert, drohen nicht nur Ausfälle, sondern auch Qualitätsmängel und Gefahren für die Anlagensicherheit. Manipulierte Parameter können ganze Chargen unbrauchbar machen. Die Trennung von IT und OT sowie überwachte Zugänge sind hier zentral und schützen zugleich Produkt und Mensch. Eine kontinuierliche Überwachung der Steuerungen erkennt Manipulationen, bevor sie Schaden anrichten.

### 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 nach §30 mit klaren Anforderungen und abgesicherte Fernwartung begrenzen das Risiko. Ein aktuelles Verzeichnis aller Fernwartungszugänge macht die Kette überhaupt erst überblickbar.

### 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 lückenlose Protokollierung begrenzen dieses Risiko. Feste Zeitfenster und eine Mehrfaktor-Anmeldung begrenzen, was über einen Fernzugang möglich ist.



REGULATORISCHE PFLICHTEN

# Was das Gesetz konkret verlangt.

Fünf Paragraphen bilden den Kern, den jeder betroffene Betrieb kennen muss: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

## §28 · BETROFFENHEIT UND REGISTRIERUNG

Wichtige Einrichtung ist, wer ab 50 Beschäftigte oder mehr als 10 Mio. Euro erreicht, besonders wichtig ab 250 Beschäftigte oder mehr als 50 Mio. Euro. Maßgeblich ist die Zugehörigkeit zu einem erfassten Sektor, etwa Maschinenbau, Fahrzeugbau, Elektronik oder Medizinprodukte. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal, die Einstufung nimmt der Betrieb selbst vor und begründet sie schriftlich. Im Zweifel hilft eine kurze rechtliche Einschätzung. Wer wartet, riskiert, im entscheidenden Moment ohne Nachweis dazustehen.

## §30 · DIE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Verlangt werden angemessene Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, Zugriffskontrolle, Kryptografie und Multifaktor-Authentifizierung. Produktions- und Betriebstechnik gehören ausdrücklich dazu. Wer bereits ein ISMS nach ISO 27001 oder ein TISAX-Label betreibt, hat den Großteil abgedeckt und setzt NIS2 als Erweiterung um, nicht als zweites Projekt. Entscheidend ist, dass jede Maßnahme nicht nur existiert, sondern nachweisbar gelebt und regelmäßig überprüft wird.

## §32 · MELDEFRISTEN

Bei einem erheblichen Sicherheitsvorfall gilt eine gestufte Meldepflicht an das BSI: Frühwarnung binnen 24 Stunden, Meldung mit erster Bewertung binnen 72 Stunden, Abschlussbericht binnen eines Monats. Steht die Fertigung still, zählt jede Stunde, und die Uhr läuft ab Kenntnis. Nur ein vorab geübter Prozess hält diese Fristen. Ein vorbereitetes Meldeformular und klare Zuständigkeiten sparen im Ernstfall wertvolle Minuten.

## §38 · LEITUNG HAFTET PERSÖNLICH

Die Geschäftsführung muss die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Die Verantwortung ist nicht delegierbar, auch nicht an den externen IT-Dienstleister. Aus dem Qualitätsmanagement ist diese Leitungsverantwortung vielen Betrieben vertraut. Das dokumentierte Engagement ist im Ernstfall zugleich ein Nachweis gelebter Sorgfalt. Regelmäßige, kurze Schulungen der Leitung sind ausdrücklich Teil dieser Pflicht.

## §65 · SANKTIONEN UND VERHÄLTNISMÄSSIGKEIT

Verstöße kosten bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen, bis zu 7 Mio. Euro oder 1,4 % bei wichtigen Einrichtungen. Zugleich gilt die Verhältnismäßigkeit: geschuldet ist ein Schutzniveau, das zu Größe und Risiko passt. Ein dokumentierter, gelebter Prozess ist im Prüffall die beste Verteidigung. Wer Lücken kennt und plant, wird selbst bei einem Vorfall milder bewertet als ein untätiger Betrieb.

UMSETZUNG IN DER PRAXIS

# In sechs Schritten mit Augenmaß NIS2-konform.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene Strukturen aus dem Qualitätsmanagement, statt bei null zu beginnen. Realistisch führt der Weg je nach Reife und Anlagenlandschaft in einigen Monaten zu einem auditbereiten Stand.

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

### 1 · BETROFFENHEIT UND GELTUNGSBEREICH

Sektor und Schwellenwerte prüfen, auch die Rolle als Zulieferer, und die Einstufung dokumentieren. 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 · BEIM BSI REGISTRIEREN

Unternehmenskonto anlegen, im BSI-Portal registrieren, Kontaktstellen benennen. Wer die Frist versäumt hat, holt den Schritt umgehend nach, um Bußgelder zu vermeiden. Die benannte Kontaktstelle ist zugleich der Draht zum BSI im Ernstfall.

### 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. Eine gute Analyse macht den Aufwand planbar.

### 4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Netzsegmentierung, Zugriffskontrolle, Schutz der Konstruktionsdaten und abgesicherte Fernwartung. Jede Maßnahme so festhalten, dass sie im Audit Bestand hat. Vieles lässt sich in vorhandenen Systemen direkt aktivieren und zentral vorgeben. So wirkt jede Maßnahme sofort im ganzen Betrieb.

### 5 · MELDEPROZESS AUFBAUEN

Die 24-Stunden-Meldekette an das BSI einrichten, Zuständigkeiten klären und den Notfallplan testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen. Eine Übung pro Jahr zeigt, wo der Ablauf zwischen Produktion und IT noch hakt.

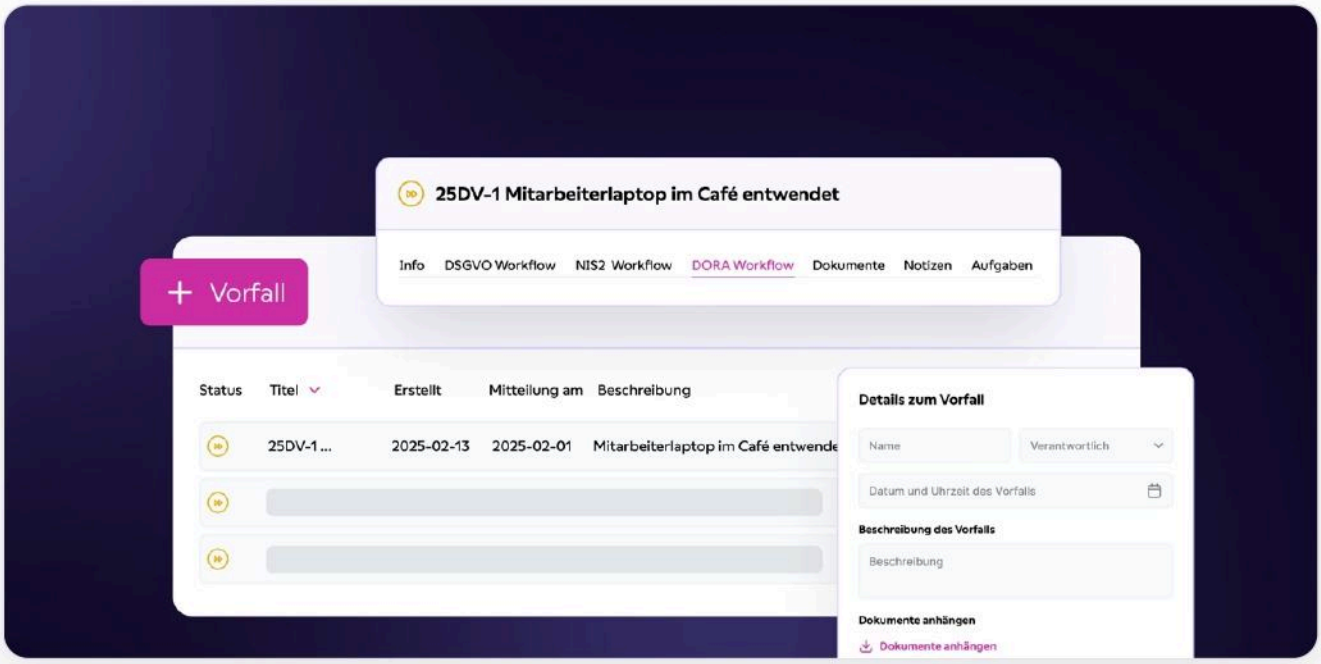
### 6 · PRÜFEN, NACHWEISEN, VERBESSERN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Für Betriebe mit ISO-9001-Erfahrung ist diese Schleife vertrautes Terrain. Wer sie einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung und eine TISAX-Bewertung. Der Aufwand von heute trägt so gleich mehrere Nachweise von morgen.

WIE SECJUR ES EINFACH MACHT

# Vom Pflichtenrahmen zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) führt Industrieunternehmen durch NIS2, TISAX und ISO 27001 zugleich: Risiken in IT und Produktionstechnik, Maßnahmen, Meldeprozess und Nachweise an einem Ort. Statt monatelanger Beratung arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Teams berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.




### IT und Produktion

Eine Risikoanalyse, die Büro-IT, Konstruktion und Produktionstechnik zusammen denkt, mit Vorlagen, die den Fertigungsbetrieb kennen.

### Vorfall & Meldung

Strukturiertes Incident-Management mit der 24-Stunden-Meldekette an das BSI, inklusive Fristenverfolgung (24h / 72h / 1 Monat) und Bericht.

### ISO 27001 & TISAX

NIS2, ISO 27001 und TISAX laufen auf einem ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt mehrfach.

## SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank. Sie legen den Geltungsbereich fest, das DCO führt durch jede Anforderung, und wo eine Expertin nötig ist, schalten wir sie zu. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereiter Nachweis in Wochen statt in Quartalen, ohne dass die Fertigung stehen bleibt.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets in IT und Produktion sowie bestehende Maßnahmen ab und leitet daraus die offenen Punkte ab. Jeder Schritt ist mit einer Vorlage hinterlegt, sodass niemand vor einem leeren Blatt sitzt.

Wo es schnell gehen muss, arbeitet das Team die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar. Der Fortschritt bleibt jederzeit sichtbar, für die IT ebenso wie für die Fertigung.

## EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, ISO 27001 und TISAX 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 pflegt.

Für einen Hersteller heißt das weniger Doppelarbeit. Der NIS2-Nachweis, die ISO-27001-Zertifizierung und die TISAX-Bewertung entstehen aus demselben Aufbau, statt in getrennten Projekten.

Und weil die Belege aktuell bleiben, ist der Betrieb für die nächste OEM-Prüfung oder das nächste Überwachungsaudit vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Vorteil.

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

REFERENZEN AUS INDUSTRIE, MASCHINENBAU UND FERTIGUNG

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

AUDIT-ERFOLG
**100%**
Erfolgsquote in bisherigen Zertifizierungsaudits.

ZEITERSPARNIS
**50%**
Weniger Aufwand gegenüber klassischer Beratung.

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

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, 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.

Wo Fachwissen für IT und OT fehlt, schalten sich Expertinnen und Experten gezielt zu, statt ein dauerhaftes Beratungsmandat zu verlangen. Das hält die Kosten im Rahmen und die Kontrolle im Haus, gerade bei mittelständischen Herstellern.

Und die Plattform denkt in der Realität eines Fertigungsbetriebs. Sie priorisiert die Maßnahmen mit der größten Wirkung und schützt, ohne die Verfügbarkeit der Linie zu gefährden.

## 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.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Wettbewerbsvorteil. OEM-Fragebögen sind in Stunden beantwortet, Audits verlieren ihren Schrecken, und Kunden sehen belegt, dass ihr Zulieferer zuverlässig liefert.

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.

So wird aus einer Pflicht ein dauerhafter Schutz von Produktion, Wissen und Vorsprung, der mit jeder neuen Anlage und jedem OEM-Projekt an Bedeutung gewinnt.

SECJUR

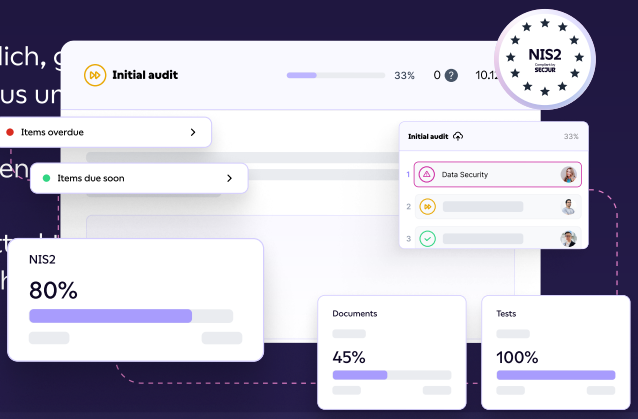
# Mit SECJUR zu 100 % NIS2-Compliance

Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, g
Transparenz über Ihren Compliance-Status ur
eine belastbare Grundlage für regulator
und anspruchsvolle Kundenanforderungen




Für unsere Bestandskunden bieten wir att
Konditionen, um frühzeitig Klarheit zu sch
NIS2-Readiness planbar umzusetzen.

→ **Jetzt informieren**

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**

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

www.secjur.com