SECJUR

WHITEPAPER
2026

ISO 27001 · LUFTFAHRT & VERTEIDIGUNG

ISO 27001 in der Verteidigung: *Sicherheit als Eintrittskarte.*

Kaum eine Branche verlangt mehr Vertraulichkeit als Luftfahrt und Verteidigung. Aufträge von Generalunternehmern, Bundeswehr und NATO-Partnern setzen nachweisbare Informationssicherheit voraus, der Umgang mit Verschlusssachen und der Geheimschutz stellen hohe Anforderungen, und staatliche Angreifer haben es gezielt auf sicherheitsrelevantes Know-how abgesehen. ISO 27001 ist die kommerzielle Basis, auf der diese Anforderungen aufsetzen. Dieses Whitepaper zeigt, warum der Standard zur Geschäftsgrundlage wird und wie ein belastbares ISMS entsteht.

ISO 27001 | Geheimschutz | NIS2 | TISAX® | Exportkontrolle

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In Luftfahrt und Verteidigung ist Sicherheit *die Lizenz zum Auftrag.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). In Luftfahrt und Verteidigung ist er selten freiwillig: Generalunternehmer und öffentliche Auftraggeber setzen ihn in Ausschreibungen voraus, und er bildet die kommerzielle Grundlage, auf der Geheimschutz und der Umgang mit Verschlusssachen aufbauen. Das Zertifikat belegt, dass ein Unternehmen sensible Informationen sicher beherrscht.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der Informationsklassifizierung, Personalsicherheit, Zugriffskontrolle und den Schutz der Fertigung umfasst.

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. Generalunternehmer geben ihre Sicherheitsanforderungen über die Lieferkette weiter und verlangen den Nachweis vertraglich. Öffentliche Vergaben setzen ISO 27001 oft als Mindestanforderung. Zugleich fallen Zulieferer und Dienstleister je nach Tätigkeit unter NIS2, und der Umgang mit Verschlusssachen verlangt geprüfte Vorkehrungen.

Hinzu kommt eine besonders ernste Bedrohungslage. Verteidigungs- und Luftfahrttechnologie ist ein bevorzugtes Ziel staatlich gesteuerter Angreifer, die gezielt und langfristig vorgehen. 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: Ausschreibungen von Primes oder Behörden fordern das Zertifikat, Sie verarbeiten Verschlusssachen oder exportkontrollierte Informationen, oder Sie wollen sicherheitsrelevantes Know-how 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 Geheimschutz, TISAX und ein Großteil von NIS2 aufsetzen. Ein einmal aufgebautes ISMS trägt mehrere Anforderungen zugleich.

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 Geheimschutz und TISAX in der Lieferkette.

BRANCHENKONTEXT

Hier ist Vertraulichkeit *keine Option, sondern Pflicht.*

Luftfahrt und Verteidigung arbeiten mit den sensibelsten Informationen überhaupt: Konstruktionsdaten, Verschlusssachen und exportkontrolliertem Wissen. Auftraggeber und Staat verlangen nachweisbare Sicherheit, und ISO 27001 liefert das Fundament dafür.

Ein abgeflossenes Konstruktionsdetail ist hier kein Datenleck, *sondern ein Sicherheitsvorfall mit Tragweite.*

HÖCHSTE GEHEIMHALTUNG, LANGE PROGRAMME

Luftfahrt- und Verteidigungsprogramme laufen über Jahrzehnte und verarbeiten Konstruktions-, Test- und Einsatzdaten von hohem Schutzbedarf. Vieles ist als Verschlusssache eingestuft, etwa VS-NfD, und unterliegt dem staatlichen Geheimschutz mit eigenen, geprüften Anforderungen.

ISO 27001 ist die kommerzielle Basis darunter. Es schafft die Struktur aus Klassifizierung, Zugriffskontrolle und Nachweis, auf der die besonderen Geheimschutzpflichten aufsetzen.

DIE LIEFERKETTE DER GENERALUNTERNEHMER

Große Hersteller und Systemhäuser kaufen nicht ohne Prüfung. Zulieferer durchlaufen strenge Lieferantenprüfungen, und ISO 27001 ist dabei häufig die Mindestanforderung, um überhaupt gelistet zu werden. In angrenzenden Bereichen kommt TISAX hinzu, das auf denselben Anforderungen aufbaut.

Wer ISO 27001 umsetzt, beantwortet einen Großteil der Sicherheitsfragebögen mit einem Dokument und schafft die Grundlage für weitergehende Geheimschutz- und Programmanforderungen.

EXPORTKONTROLLE UND NATIONALITÄT

Verteidigungsgüter und Technologien unterliegen strenger Exportkontrolle. Der Zugriff auf bestimmte Informationen muss nach Nationalität und Berechtigung beschränkt werden. Das verlangt eine fein granulierte Zugriffssteuerung, wie sie die Norm in Annex A vorsieht.

WAS AUF DEM SPIEL STEHT

Es geht um nationale Sicherheit, den Schutz von Soldaten und einen Technologievorsprung von strategischem Wert. Ein Vorfall kann Programme gefährden, Zulassungen kosten und das Vertrauen von Auftraggeber und Staat dauerhaft beschädigen.

HERAUSFORDERUNGEN

Warum ISO 27001 in dieser Branche *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Branche. In Luftfahrt und Verteidigung kommen jedoch besondere Auflagen hinzu. Fünf Eigenheiten machen die Umsetzung anspruchsvoll, und für jede gibt es einen klaren Umgang.

UMGANG MIT VERSCHLUSSSACHEN

Eingestufte Informationen verlangen mehr als guten Willen: definierte Klassifizierungsstufen, getrennte Verarbeitung, dokumentierte Weitergabe und geprüfte Vorkehrungen. Das geht über die übliche Büro-IT deutlich hinaus.

ISO 27001 liefert mit Informationsklassifizierung und Handhabung (Annex A 5.12, 5.13, 5.14) den Rahmen, in den sich die besonderen Geheimschutzanforderungen einfügen.

PERSONALSICHERHEIT

Wo sensible Informationen verarbeitet werden, zählt die Zuverlässigkeit der Menschen. Sicherheitsüberprüfungen, klare Rollen und ein sauberes Onboarding und Offboarding sind Pflicht, gerade bei wechselnden Projektteams und Subunternehmern.

Die Norm adressiert das mit Personalsicherheit über den gesamten Beschäftigungszyklus (Annex A 6.1 bis 6.6), von der Überprüfung bis zur Rückgabe von Werten und Rechten.

GRANULARE, EXPORTKONFORME ZUGRIFFE

Nicht jeder darf alles sehen. Zugriffe müssen nach Programm, Berechtigung und teils Nationalität streng getrennt werden, um Exportkontrolle und Geheimhaltung einzuhalten. Eine grobe Rechtevergabe genügt nicht.

Rollenbasierte Zugriffskontrolle, das Prinzip der minimalen Rechte und lückenlose Protokollierung (Annex A 5.15, 5.18, 8.2 bis 8.5) sind hier zentral.

LANGE LEBENSZYKLEN UND FERTIGUNG

Wie in der Industrie laufen Fertigung und Prüfstände auf Systemen mit sehr langen Lebenszyklen, die sich kaum patchen lassen. Diese Technik muss geschützt werden, ohne den Betrieb zu stören. Netzsegmentierung und kompensierende Maßnahmen (Annex A 8.20 bis 8.23) sind der Weg.

STAATLICHE ANGREIFER

Die Gegenseite ist oft kein Gelegenheitstäter, sondern ein gut ausgestatteter, staatlich gesteuerter Akteur mit langem Atem. Das verlangt kontinuierliche Überwachung, Angriffserkennung und einen geübten Vorfallprozess (Annex A 8.16, 5.24 bis 5.27), nicht nur Basisschutz.

BEDROHUNGSLAGE & RISIKEN

Wo Luftfahrt und Verteidigung *konkret angreifbar sind.*

Die Risiken sind selten Zufall. Sie richten sich gezielt gegen sensibles Wissen, gegen die Lieferkette und gegen die Fertigung. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · GEZIELTE SPIONAGE DURCH STAATEN

Der gefährlichste Angriff. Hoch entwickelte, staatlich gesteuerte Akteure nisten sich oft monatelang unbemerkt ein, um Konstruktions-, Test- und Einsatzdaten abzuschöpfen. Der Schaden ist strategisch und oft erst spät erkennbar. Kontinuierliche Überwachung, Angriffserkennung und strenge Zugriffskontrolle (Annex A 8.16, 5.24 bis 5.27, 8.2 bis 8.5) sind die zentralen Schutzlinien.

2 · ABFLUSS VON VERSCHLUSSSACHEN

Werden eingestufte Informationen offengelegt, ist das kein gewöhnlicher Datenschutzvorfall, sondern ein Sicherheitsvorfall mit nationaler Tragweite, der Programme und Zulassungen gefährdet. Klassifizierung, getrennte Verarbeitung und Verschlüsselung (Annex A 5.12, 5.13, 8.24) schützen diese Informationen.

3 · ANGRIFFE ÜBER DIE LIEFERKETTE

Die Lieferkette ist tief und international. Ein kompromittierter Zulieferer oder ein manipuliertes Bauteil oder Update wird zum Einstieg in Programme und Netze. Lieferantensteuerung mit harten Anforderungen und Nachweisen (Annex A 5.19 bis 5.23) ist hier nicht Kür, sondern Pflicht.

4 · SABOTAGE VON FERTIGUNG UND PRÜFUNG

Werden Fertigungs- oder Prüfsysteme manipuliert, drohen nicht nur Ausfälle, sondern verdeckte Qualitätsmängel an sicherheitskritischen Bauteilen. Trennung von IT und OT sowie überwachte Zugänge (Annex A 8.20 bis 8.23) sind hier entscheidend.

5 · INSIDER UND PERSONALRISIKEN

Bei hochsensiblen Informationen ist der Mensch ein zentraler Faktor, ob durch Anwerbung, Nachlässigkeit oder offene Zugänge nach dem Ausscheiden. Sicherheitsüberprüfungen, das Prinzip der minimalen Rechte und sauberes Offboarding (Annex A 6.1 bis 6.6, 5.18) 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 Auftraggeber und Behörden und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

In dieser Branche ist der Zuschnitt besonders heikel. Der Scope muss die programmkritischen und eingestuften Bereiche klar abdecken, ohne sich zu verzetteln. 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). Häufig ist zudem ein Sicherheitsbevollmächtigter für den Geheimschutz zu benennen.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Das Unternehmen legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken rund um eingestufte Informationen, Lieferkette und Fertigung 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.

Klassifizierung, Personalsicherheit und Zugriffskontrolle 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 dieser Branche stehen Informationsklassifizierung, Personalsicherheit, Zugriffskontrolle und physische Sicherheit besonders 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 den wiederkehrenden Prüfungen, die Auftraggeber und Geheimschutz verlangen.

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 Geheimschutzanforderungen sechs bis zwölf Monate bis zum Audit.

Ein ISMS nach ISO 27001 ist die Basis für Geheimschutz, TISAX und NIS2. *Ein Fundament, mehrere Anforderungen.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die programmkritischen und eingestuften Bereiche schneiden: Entwicklung, Fertigung, zugehörige IT. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und für die Nachweise gegenüber Auftraggebern.

2 · FÜHRUNG, LEITLINIE, SICHERHEITSROLLEN

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, stellt Ressourcen bereit und benennt die nötigen Sicherheitsrollen, einschließlich der Funktionen für den Geheimschutz, wo eingestufte Informationen verarbeitet werden.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von Konstruktions- und Programmdaten über die Fertigung bis zur Lieferkette. Risiken bewerten, Vertraulichkeit und Spionageabwehr besonders gewichten und die Erklärung zur Anwendbarkeit erstellen.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Informationsklassifizierung, granulare Zugriffskontrolle, Personalsicherheit und Netzsegmentierung. 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.

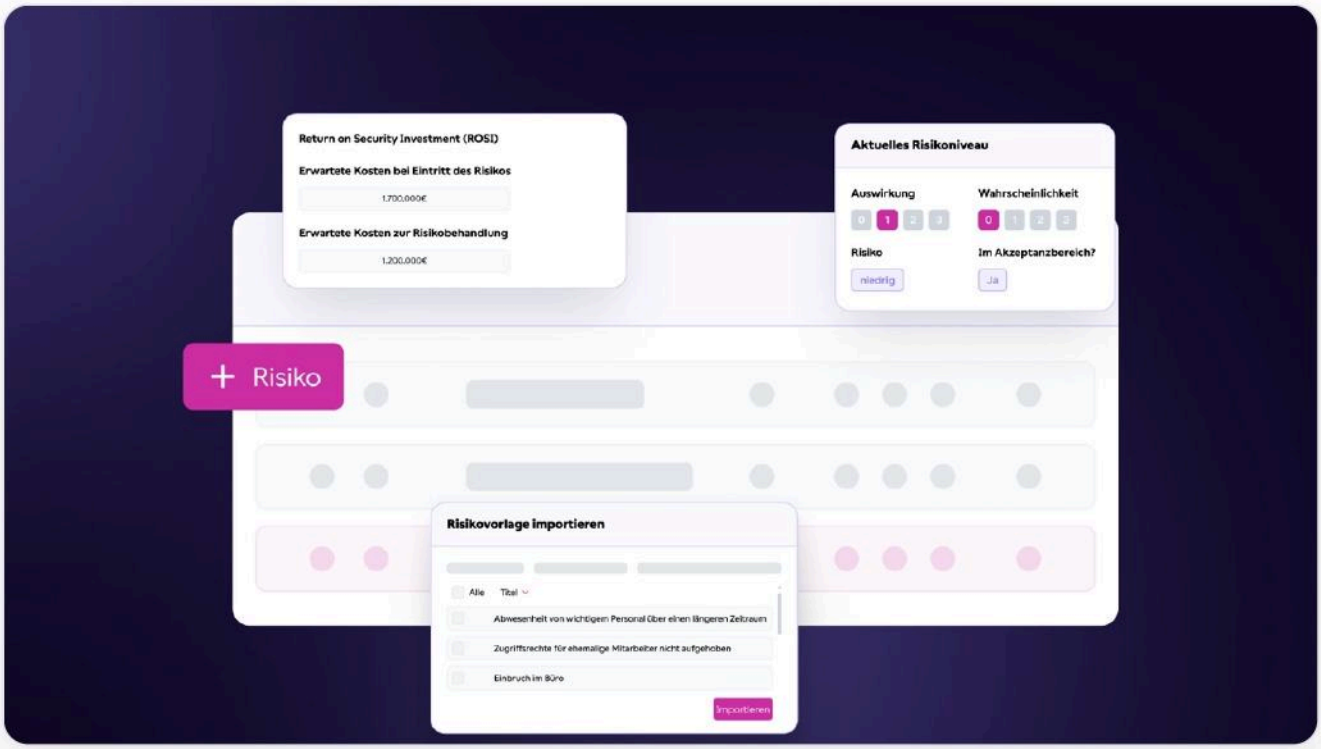
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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, und es bildet die Basis für Geheimschutz- und Programmanforderungen.

WIE SECJUR ES EINFACH MACHT

Von der Auftragsanforderung zur *auditbereiten Umsetzung.*

Das Digital Compliance Office (DCO) führt Luftfahrt- und Verteidigungsunternehmen durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse, Klassifizierung, Personalsicherheit, Lieferantensteuerung und Nachweise an einem Ort, als Basis auch für Geheimschutz, 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 & Spionageabwehr

Geführte Risikoanalyse mit Fokus auf Vertraulichkeit, eingestufte Informationen und gezielte Angreifer, jede Maßnahme nachvollziehbar begründet.

Zugriff & Personal

Module für granulare, exportkonforme Zugriffskontrolle, Personalsicherheit und Klassifizierung, genau dort, wo Geheimschutz und Annex A hinschauen.

Lieferanten & Audit

Lieferantensteuerung und ein voller Audit-Trail, der zugleich die Anforderungen von Primes, Geheimschutz und 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 belastbares, auditbereites ISMS, das auch strengen Auftraggeberprüfungen standhält.

AUS DEUTSCHLAND, EIN FUNDAMENT FÜR VIELE PFLICHTEN

Alle Daten liegen in Deutschland, der Betrieb ist selbst nach ISO 27001 zertifiziert. Weil ISO 27001 die Basis für Geheimschutz, TISAX und NIS2 bildet, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass das ISMS aktuell bleibt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Luftfahrt- und Verteidigungsunternehmen, Industriebetriebe, Zulieferer und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Branche:

„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 LUFTFAHRT, VERTEIDIGUNG UND INDUSTRIE

STEYRMOTORS · airsphere · BECKHOFF New Automation Technology · Harmattan AI · TELESPAZIO a LEONARDO and THALES company · CIRCUS GROUP

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 DIE BRANCHE SECJUR WÄHLT

Der Reiz liegt in der Geschwindigkeit und der Tiefe. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen für Klassifizierung, Personalsicherheit und Zugriffskontrolle. Das Team bleibt am Programm, das ISMS entsteht parallel.

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

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Unternehmen, das eingestufte Informationen beherrscht, seine Lieferkette steuert und in jeder Auftraggeberprüfung souverän auftritt. Genau das sichert Programme und Vertrauen.

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

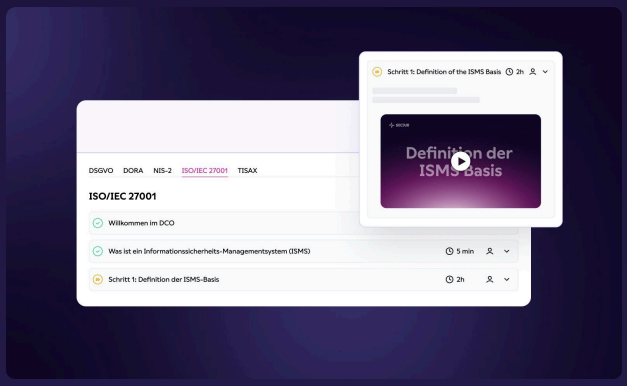
SECJUR

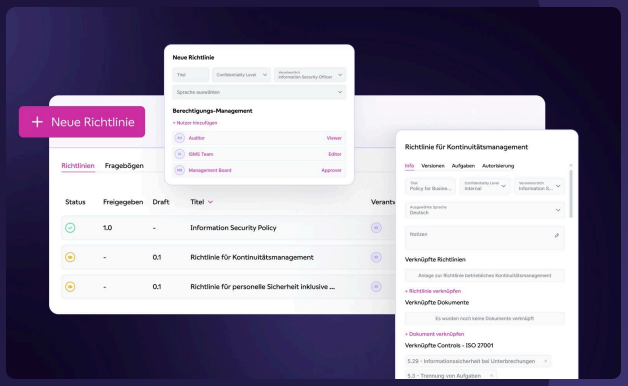
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

STEYRMOTORS · CIRCUS GROUP · BECKHOFF New Automation Technology · Harmattan AI · TELESPAZIO a LEONARDO and THALES company · airsphere

www.secjur.com