SECJUR

WHITEPAPER
2026

NIS2 · LUFTFAHRT, VERTEIDIGUNG & AEROSPACE

NIS2 in Luftfahrt & 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, und staatliche Angreifer haben es gezielt auf sicherheitsrelevantes Know-how abgesehen. Der Luftverkehr fällt direkt unter NIS2, die Luft-, Raumfahrt- und Verteidigungsindustrie über das verarbeitende Gewerbe und die Lieferkette. Dieses Whitepaper zeigt, welche Pflichten gelten, wie NIS2, Geheimschutz und Exportkontrolle zusammenspielen und wie ein belastbares ISMS entsteht.

NIS2 | ISO 27001 | Geheimschutz | TISAX® | Exportkontrolle

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In Luftfahrt und Verteidigung ist Sicherheit die Lizenz zum Auftrag.

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. Der Luftverkehr, von Luftfahrtunternehmen über Flughäfen bis zum Flugverkehrsmanagement, zählt ausdrücklich zu den erfassten Bereichen.

Für die Luft-, Raumfahrt- und Verteidigungsindustrie entsteht die Betroffenheit über das verarbeitende Gewerbe, etwa die Herstellung von Luft- und Raumfahrzeugen, und über die Lieferkette der Generalunternehmer. Rein hoheitliche Aufgaben der nationalen Verteidigung können von NIS2 ausgenommen sein, die kommerzielle Industrie und ihre Zulieferer sind es nicht. Ein ISMS nach ISO 27001 deckt einen Großteil dieser Pflichten mit ab und bildet zugleich die Basis, auf der Geheimschutz und der Umgang mit Verschlusssachen aufsetzen. Wer die Einstufung sauber dokumentiert, schafft Klarheit und schützt die Leitung im Zweifel vor Haftung.

WARUM JETZT HANDELN

Der Druck kommt von mehreren Seiten. Generalunternehmer geben ihre Sicherheitsanforderungen über die Lieferkette weiter, öffentliche Vergaben setzen ISO 27001 oft als Mindestanforderung, und die NIS2-Registrierungsfrist beim BSI endete am 31. Juli 2026.

Hinzu kommt eine besonders ernste Bedrohungslage. Verteidigungs- und Luftfahrttechnologie ist ein bevorzugtes Ziel staatlich gesteuerter Angreifer, die gezielt und langfristig vorgehen. Ein Vorfall trifft hier nicht nur die IT, sondern ganze Programme und Zulassungen. Wer den Nachweis früh aufbaut, bleibt für Generalunternehmer ein gelisteter Partner.

EIN FUNDAMENT, MEHRERE ANFORDERUNGEN

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. Es umfasst Informationsklassifizierung, Personalsicherheit, Zugriffskontrolle und den Schutz der Fertigung.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken rund um eingestufte Informationen und Lieferkette, die Pflichten aus dem Gesetz und eine Roadmap, die im Programmbetrieb funktioniert. So bleibt die knappe Kapazität am Programm, statt in Formularen zu versickern. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht im Betrieb.

LUFTVERKEHR

NIS2

Luftfahrtunternehmen, Flughäfen und Flugverkehrsmanagement fallen direkt unter NIS2.

INDUSTRIE

§30

Aerospace- und Verteidigungsindustrie über verarbeitendes Gewerbe und Lieferkette erfasst.

BUSSGELD

10 Mio €

Bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes bei besonders wichtigen Einrichtungen.

BRANCHENKONTEXT

Hier ist Vertraulichkeit keine Option, sondern Pflicht.

Luftfahrt und Verteidigung arbeiten mit den sensibelsten Informationen überhaupt: Konstruktionsdaten, Verschlusssachen und exportkontrolliertem Wissen. Auftraggeber, Staat und mit NIS2 nun auch das Gesetz verlangen nachweisbare Sicherheit.

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 und die NIS2-Maßnahmen gemeinsam aufsetzen. Schon die saubere Klassifizierung der Bestände zeigt, wo der Schutz zuerst greifen muss.

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 erfüllt zugleich die Lieferkettenpflicht, die auch NIS2 nach §30 verlangt. Wer den Nachweis früh vorlegt, verkürzt jede Lieferantenprüfung erheblich.

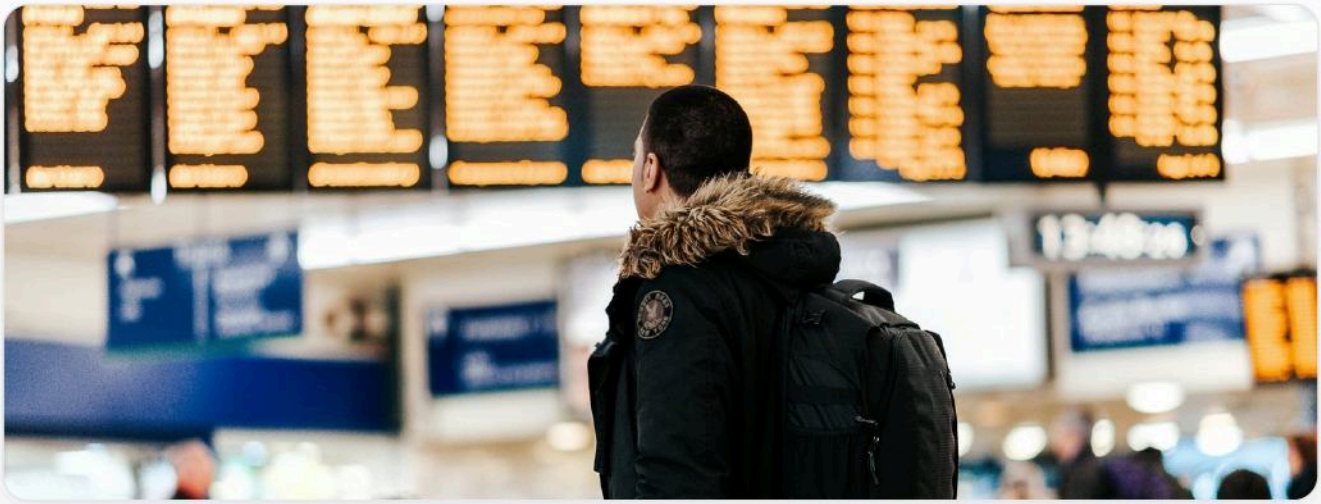
EXPORTKONTROLLE UND NATIONALITÄT

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 im Annex A vorsieht und NIS2 als Zugriffskontrolle einfordert.

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.

Ein belastbarer Nachweis ist deshalb weit mehr als eine Formalie. Er ist die Eintrittskarte in Programme und die Voraussetzung, um gelistet zu bleiben. Ein einziger Abfluss kann den Vorsprung von Jahren zunichtemachen.



HERAUSFORDERUNGEN

Warum NIS2 in dieser Branche besonders fordert.

Die Anforderungen gelten unabhängig von der Branche. In Luftfahrt und Verteidigung kommen jedoch besondere Auflagen hinzu. Sechs 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 den Rahmen, in den sich die besonderen Geheimschutz- und NIS2-Anforderungen einfügen. Eine klare Kennzeichnung jeder Information ist die Grundlage jeder weiteren Maßnahme.

PERSONALSICHERHEIT

Wo sensible Informationen verarbeitet werden, zählt die Zuverlässigkeit der Menschen. Sicherheitsüberprüfungen, klare Rollen und ein sauberes On- und Offboarding sind Pflicht, gerade bei wechselnden Projektteams und Subunternehmern. Die Norm adressiert das mit Personalsicherheit über den gesamten Beschäftigungszyklus, von der Überprüfung bis zur Rückgabe von Werten und Rechten. Ein automatisierter Rechteentzug beim Ausscheiden verhindert, dass Zugänge offen bleiben.

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 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 sind der Weg. Ein eigenes, getrenntes Fertigungsnetz hält den Schaden im Ernstfall lokal.

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, wie ihn auch die NIS2-Meldepflicht voraussetzt, nicht nur Basisschutz. Regelmäßige Übungen zeigen, ob die Angriffserkennung im Ernstfall wirklich greift.

ZWEI REGIME, EIN AUFBAU

Geheimschutz, Exportkontrolle und NIS2 stellen ähnliche Fragen an Klassifizierung, Zugänge und Nachweise. Wer sie getrennt bearbeitet, pflegt vieles doppelt. Ein gemeinsames ISMS bündelt die Anforderungen und hält die Nachweise über alle Regime hinweg konsistent.

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 sind die zentralen Schutzlinien. Wer Zugriffe lückenlos protokolliert, erkennt solche stillen Angriffe überhaupt erst. Eine strikte Trennung der Programme begrenzt, wie weit ein Angreifer kommt.

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 schützen diese Informationen und stützen zugleich die NIS2-Meldepflicht. Ein aktuelles Verzeichnis aller eingestuften Bestände ist die Grundlage jeder Kontrolle. Verschlüsselung schützt die Daten auch dann, wenn sie das Haus verlassen.

3 · ANGRIFFE ÜBER DIE LIEFERKETTE

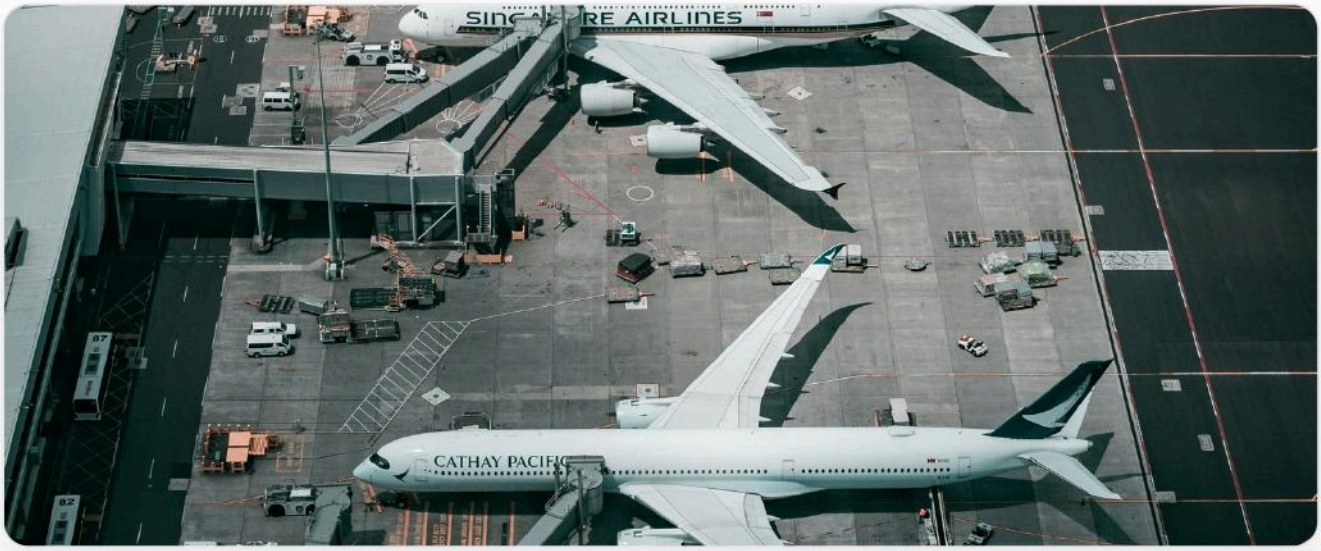
Die Lieferkette ist tief und international. Ein kompromittierter Zulieferer oder ein manipuliertes Bauteil oder Update wird zum Einstieg in Programme und Netze. Lieferantensteuerung mit harten Anforderungen und Nachweisen nach §30 ist hier nicht Kür, sondern Pflicht. Ein aktuelles Verzeichnis aller Zulieferer und Zugänge macht die Kette überhaupt erst überblickbar. Wer seine Schnittstellen sauber führt, besteht die Prüfungen der Generalunternehmer ohne Hektik.

4 · SABOTAGE VON FERTIGUNG UND PRÜFUNG

Werden Fertigungs- oder Prüfsysteme manipuliert, drohen nicht nur Ausfälle, sondern verdeckte Qualitätsmängel an sicherheitskritischen Bauteilen. Die Trennung von IT und OT sowie überwachte Zugänge sind hier entscheidend und schützen Programm wie Betrieb. Eine kontinuierliche Überwachung erkennt Manipulationen, bevor fehlerhafte Teile das Werk verlassen. Ein sicherer Rückfallmodus schützt im Zweifel Produkt und Programm.

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 begrenzen dieses Risiko. Ein Vier-Augen-Prinzip bei kritischen Vorgängen senkt das Risiko zusätzlich. Eine lückenlose Protokollierung macht ungewöhnliche Zugriffe früh sichtbar.



REGULATORISCHE PFLICHTEN

Was das Gesetz konkret verlangt.

NIS2 steht in dieser Branche neben Geheimschutz, Exportkontrolle und TISAX. Fünf Bausteine muss jede betroffene Einrichtung kennen: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

§28 · BETROFFENHEIT UND REGISTRIERUNG

Der Luftverkehr zählt zum Sektor Verkehr, die Aerospace- und Verteidigungsindustrie zum verarbeitenden Gewerbe, häufig als wichtige, große Betriebe als besonders wichtige Einrichtungen. Rein hoheitliche Verteidigungsaufgaben können ausgenommen sein, die kommerzielle Industrie ist erfasst. Die Registrierung läuft über das Unternehmenskonto und das BSI-Portal, die Einstufung nimmt der Betrieb selbst vor. 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. Informationsklassifizierung, Personalsicherheit und der Schutz der Fertigung gehören dazu. Wer bereits ein ISMS nach ISO 27001 oder ein TISAX-Label betreibt, hat den Großteil abgedeckt und setzt NIS2 als Erweiterung um. 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. Neben der BSI-Meldung können Geheimschutz- und Programmmeldewege greifen. 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. Häufig ist zudem ein Sicherheitsbevollmächtigter für den Geheimschutz zu benennen. Die Verantwortung ist nicht delegierbar. Das dokumentierte Engagement der Leitung 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 Einrichtungen. Weit schwerer wiegt hier oft der Verlust von Programmen und Zulassungen. 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, statt bei null zu beginnen. Realistisch führt der Weg je nach Reife und Geheimschutzanforderungen in einigen Monaten zu einem auditbereiten Stand.

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

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Prüfen, ob die Einrichtung als Luftverkehr, als Industriebetrieb oder über die Lieferkette unter NIS2 fällt, 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 und Aufsicht.

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. Registrierung und Kontaktstellen für das BSI gehören ebenfalls in diesen Schritt.

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. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Mit den wirksamsten Hebeln beginnen: Informationsklassifizierung, granulare Zugriffskontrolle, Personalsicherheit und Netzsegmentierung. Jede Maßnahme so festhalten, dass sie im Audit und vor Auftraggebern Bestand hat. Vieles lässt sich in vorhandenen Systemen zentral vorgeben. Zentrale Vorgaben verhindern, dass jedes Programm eigene Wege geht.

5 · MELDEPROZESS AUFBAUEN

Die 24-Stunden-Meldekette an das BSI einrichten, mit den Geheimschutz- und Programmmeldewegen verzahnen und den Vorfallprozess testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen. Eine Übung pro Jahr zeigt, wo es noch hakt.

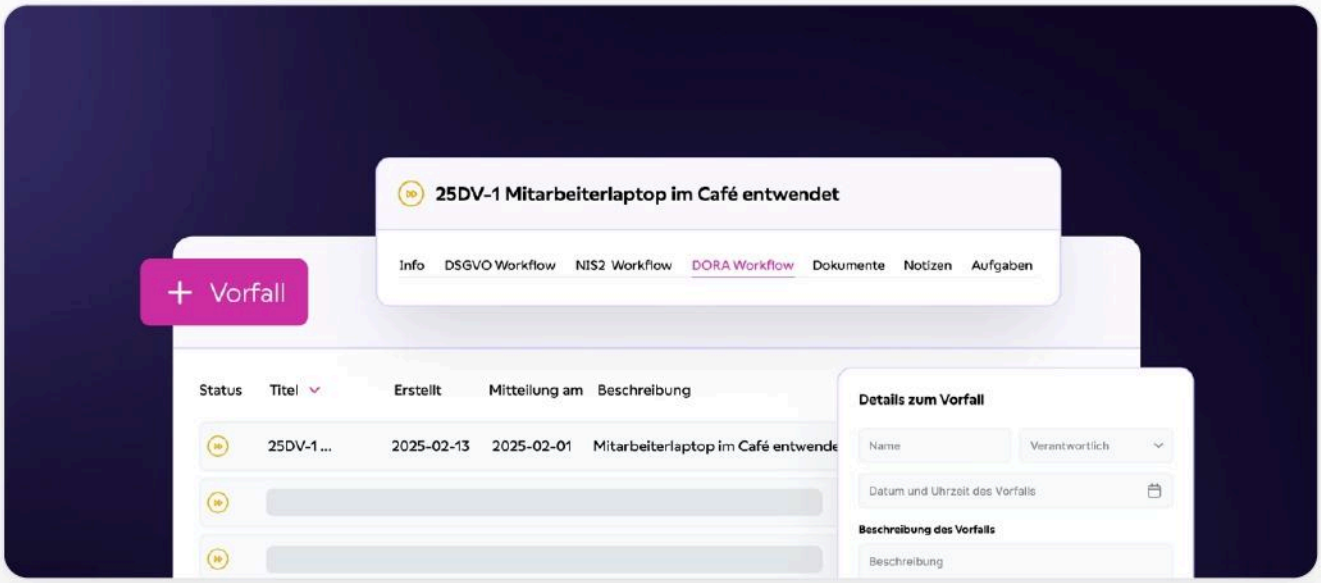
6 · PRÜFEN, NACHWEISEN, VERBESSERN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Diese Schleife deckt sich mit den wiederkehrenden Prüfungen, die Auftraggeber und Geheimschutz verlangen. Wer sie einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung.

WIE SECJUR ES EINFACH MACHT

Vom Pflichtenrahmen zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) führt Luftfahrt- und Verteidigungsunternehmen durch NIS2, Geheimschutz-Vorbereitung und ISO 27001 zugleich: Klassifizierung, Personalsicherheit, Zugriffskontrolle, 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.



Klassifizierung & Zugriff

Module für Informationsklassifizierung, minimale Rechte und granulare, exportkonforme Zugriffskontrolle, genau die Punkte, die Auftraggeber prüfen.

Personal & Lieferkette

Personalsicherheit über den Beschäftigungszyklus und eine Lieferantensteuerung, die die §30-Pflicht und die Prime-Anforderungen gemeinsam bedient.

Mehrere Anforderungen

NIS2, ISO 27001 und TISAX laufen auf einem ISMS, das zugleich die Grundlage für Geheimschutz- und Programmanforderungen bildet.

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 das Programm stehen bleibt.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, eingestufte Bereiche, Assets und 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 IT, Programm und Sicherheitsverantwortliche.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, ISO 27001 und TISAX weitgehend überschneiden und Geheimschutz auf derselben Struktur aufsetzt, 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 ein Unternehmen der Branche heißt das weniger Doppelarbeit. Der NIS2-Nachweis, die ISO-27001-Zertifizierung und die Vorbereitung auf Geheimschutz entstehen aus demselben Aufbau, statt in getrennten Projekten.

Und weil die Belege aktuell bleiben, ist das Unternehmen für die nächste Auftraggeberprüfung 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.

Luftfahrt- und Verteidigungsunternehmen, Zulieferer, Industriebetriebe 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

REFERENZEN AUS LUFTFAHRT, VERTEIDIGUNG UND INDUSTRIE

STEYRMOTORS · airsphere · BECKHOFF New Automation Technology · Harmattan AI · TELESPAZIO · CIRCUS GROUP

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 DIE BRANCHE SECJUR WÄHLT

Der Reiz liegt in der Geschwindigkeit und der Tiefe. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung, 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.

Wo Spezialwissen 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 Zulieferern.

Und die Plattform denkt in der Realität eines Programmbetriebs. Sie priorisiert die Maßnahmen mit der größten Wirkung und schützt eingestufte Informationen, ohne die Fertigung zu stören.

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.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zur Eintrittskarte. Sicherheitsfragebögen sind schneller beantwortet, Audits verlieren ihren Schrecken, und Auftraggeber sehen belegt, dass ihr Partner sensibles Wissen sicher beherrscht.

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

So wird aus einer Pflicht ein dauerhafter Schutz von Wissen, Programm und Vertrauen, der mit jedem neuen Auftrag und jeder Zulassung an Bedeutung gewinnt.

SECJUR

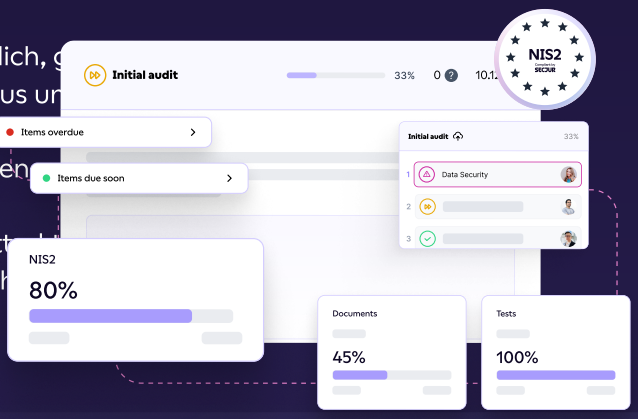
Mit SECJUR zu 100 % NIS2-Compliance

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