SECJUR

WHITEPAPER
2026

ISO 27001 · STARTUPS & SCALE-UPS

ISO 27001 für Startups: *aus Sicherheit wird Wachstum.*

Für ein junges Unternehmen ist Informationssicherheit kein Bürokratiethema, sondern die Eintrittskarte ins Enterprise-Geschäft. Immer mehr große Kunden und Investoren verlangen ein Zertifikat nach ISO 27001, bevor sie unterschreiben. Dieses Whitepaper zeigt, warum sich der Standard für Startups früh lohnt, wo die typischen Stolpersteine liegen und wie ein junges Team ein zertifizierungsreifes ISMS aufbaut, ohne sein Tempo zu verlieren.

ISO 27001 | SOC 2 | TISAX® | DSGVO | NIS2

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Sicherheit entscheidet, *welche Deals Sie gewinnen.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 oder die DSGVO ist er kein Gesetz, sondern freiwillig. Genau das macht ihn für Startups wertvoll: Ein Zertifikat ist ein unabhängiger Nachweis, dass ein junges Unternehmen seine Daten und die seiner Kunden im Griff hat. Im Vertrieb an größere Kunden 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 Sicherheit auch dann trägt, wenn das Team wächst und einzelne Personen das Unternehmen verlassen.

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

Sicherheit wird im Wachstum nicht einfacher, sondern teurer. Ein Team von fünfzehn Leuten richtet Zugriffsrechte, Backups und klare Prozesse in Wochen ein. Bei hundert Beschäftigten, gewachsener Tool-Landschaft und verteilten Teams wird daraus ein Großprojekt. Früh aufgesetzt, wächst das ISMS mit, statt später nachgerüstet zu werden.

Hinzu kommt der Vertriebsdruck. Enterprise-Einkauf, Sicherheitsfragebögen und die Due Diligence von Investoren fragen das Zertifikat aktiv ab. Ohne Nachweis verzögern sich Abschlüsse oder platzen. Dieses Whitepaper ordnet ein, was die Norm verlangt, welche Risiken Startups konkret tragen und wie der Weg zur Zertifizierung realistisch aussieht.

FÜR WEN SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: Sie verkaufen an größere Unternehmen oder den öffentlichen Sektor, Sie verarbeiten sensible Kunden- oder Personendaten, oder Sie stehen vor einer Finanzierungsrunde. Trifft eines davon zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht für junge Unternehmen: Der Standard ist skalierbar. Er schreibt kein Schutzniveau eines Konzerns vor, sondern eines, das zu Größe und Risiko 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

Vertrauen ist für Startups *die härtere Währung.*

Junge Unternehmen leben von Geschwindigkeit und vom Vertrauen ihrer ersten großen Kunden. Beides gerät in Konflikt, sobald der Vertrieb auf das Enterprise-Segment trifft. ISO 27001 löst diesen Konflikt, indem es Vertrauen nachweisbar macht.

Der erste große Kunde fragt nicht, ob Sie sicher sind. *Er verlangt den Beleg.*

CLOUD-NATIVE UND SCHNELL GEBAUT

Startups arbeiten von Tag eins in der Cloud. Code liegt in Repositories, Kundendaten in SaaS-Diensten, die Infrastruktur kommt von Hyperscalern, und ein Großteil des Teams arbeitet remote. Diese Architektur bringt Tempo, verteilt sensible Daten aber über viele Dienste und Zugänge, die selten zentral kontrolliert werden.

In den ersten Jahren zählt das Produkt, nicht die Dokumentation. Zugriffsrechte wachsen organisch, Tools kommen und gehen, Verantwortlichkeiten sind im Kopf der Gründer statt auf Papier. Das funktioniert, solange das Team klein ist. Mit dem ersten Enterprise-Kunden kippt diese Logik.

DER EINKAUF GROSSER KUNDEN

Große Unternehmen kaufen nicht ohne Prüfung. Bevor ein Konzern eine junge Software in seine Prozesse lässt, durchläuft der Anbieter eine Lieferantenprüfung mit langen Sicherheitsfragebögen. ISO 27001 beantwortet einen Großteil davon mit einem einzigen Dokument.

Ohne Zertifikat wird aus dem Verkaufsgespräch ein Prüfmarathon. Jeder Kunde schickt seinen eigenen Fragebogen, das Startup beantwortet jede Frage neu, und der Abschluss verschiebt sich um Monate. Mit Zertifikat verkürzt sich dieser Teil des Vertriebszyklus spürbar, weil der Nachweis bereits vorliegt.

INVESTOREN SCHAUEN GENAU HIN

Spätestens in der Due Diligence vor einer Finanzierungsrunde wird Informationssicherheit zum Thema. Investoren wollen wissen, ob das Unternehmen seine Daten schützt, gesetzliche Pflichten erfüllt und nicht auf einem Sicherheitsvorfall sitzt, der die Bewertung gefährdet.

Ein etabliertes ISMS ist hier ein Pluspunkt, sein Fehlen ein Risikovermerk. Reife in der Sicherheit signalisiert Reife im Unternehmen.

WAS AUF DEM SPIEL STEHT

Für ein junges Unternehmen ist Reputation das wertvollste Gut und zugleich das fragilste. Ein einziger Datenvorfall beim ersten Referenzkunden kann mehr kosten als jede Zertifizierung. Sicherheit ist deshalb kein Kostenposten, sondern Schutz des eigenen Wachstums.

HERAUSFORDERUNGEN

Warum ISO 27001 Startups *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Unternehmensgröße. Der Aufwand verteilt sich aber anders als im Konzern. Fünf Eigenheiten machen die Umsetzung im Startup speziell, und für jede gibt es einen pragmatischen Umgang.

KEIN SICHERHEITSTEAM

Im Startup gibt es selten eine eigene Sicherheitsfunktion. Sicherheit ist Nebenrolle eines Entwicklers oder landet direkt beim Gründer. Die Norm verlangt jedoch klare Rollen, dokumentierte Prozesse und den Nachweis ihrer Wirksamkeit (Kapitel 5 und 7 der ISO 27001).

Das heißt nicht, dass ein junges Team Vollzeitstellen schaffen muss. Es heißt, dass Verantwortung benannt und die Umsetzung nachvollziehbar dokumentiert wird. Werkzeuge, die durch die Anforderungen führen, ersetzen hier ein Stück weit das fehlende Team.

TEMPO GEGEN DOKUMENTATION

Startups optimieren auf Geschwindigkeit. Ein ISMS bringt zunächst das Gegenteil: Richtlinien, Nachweise, Wiederholung. Wird das zu schwer aufgesetzt, erstickt es die Kultur, die das Unternehmen schnell macht.

Der Ausweg liegt in der Verhältnismäßigkeit. Die Norm erlaubt es ausdrücklich, den Umfang an Größe und Risiko auszurichten (Kapitel 4.3 und 6.1). Ein schlankes, gut geführtes ISMS schlägt ein überladenes, das niemand pflegt.

KNAPPER RUNWAY

Budget und Zeit sind begrenzt, jeder Euro konkurriert mit dem Produkt. Klassische Beratung mit Tagessätzen und monatelangen Projekten passt schlecht zu dieser Realität. Gefragt ist ein Weg, der den Aufwand niedrig hält und das interne Team nur dort bindet, wo seine Entscheidung wirklich nötig ist. Vorlagen und geführte Abläufe sparen hier die teuersten Stunden.

SCHNELLES WACHSTUM

Was heute für zwanzig Personen passt, ist in einem Jahr überholt. Teams verdoppeln sich, neue Tools kommen hinzu, Zugänge vermehren sich. Ein ISMS muss mitwachsen, statt bei jedem Sprung neu erfunden zu werden. Sauberes On- und Offboarding (Annex A 6.1 bis 6.5) wird damit zur Daueraufgabe, nicht zur Einmalaktion. Wer Prozesse von Anfang an wiederholbar anlegt, spart sich den Bruch beim nächsten Wachstumsschub.

TOOL-WILDWUCHS

Ein junges Unternehmen nutzt schnell dutzende SaaS-Dienste. Jeder verarbeitet Daten, jeder ist ein Zugang, jeder ein Lieferant im Sinne der Norm (Annex A 5.19 bis 5.23). Ohne Übersicht über diese Landschaft bleibt die Risikoanalyse unvollständig, und genau dort schaut der Auditor hin. Ein gepflegtes Verzeichnis der Dienste und ihrer Datenflüsse ist deshalb einer der ersten lohnenden Schritte.

BEDROHUNGSLAGE & RISIKEN

Wo Startups *konkret angreifbar sind.*

Die Risiken eines jungen Unternehmens sind selten abstrakt. Sie hängen an wenigen Schlüsselpersonen, einer schnell gewachsenen Cloud und dem Druck, schnell zu liefern. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · DATENPANNE BEIM REFERENZKUNDEN

Der teuerste Ernstfall für ein Startup. Werden Kundendaten abgegriffen oder offengelegt, leidet zuerst das Vertrauen des wichtigsten Kunden, dann der Ruf am Markt. Was ein Konzern wegsteckt, kann ein junges Unternehmen die Existenz kosten. Wirksame Zugriffskontrolle, Verschlüsselung und Protokollierung (Annex A 8.2 bis 8.5, 8.24) senken dieses Risiko deutlich und sind im Audit ein zentraler Nachweis.

2 · GESCHEITERTE SICHERHEITSPRÜFUNG

Ein konkretes Geschäftsrisiko, das oft übersehen wird. Scheitert das Startup an der Lieferantenprüfung eines großen Kunden, ist der Deal weg, unabhängig davon, wie gut das Produkt ist. Ohne ISO 27001 zieht sich jede dieser Prüfungen, und manche enden vorzeitig. Das Zertifikat verschiebt das Gespräch vom Ob zur Umsetzung und macht aus einem Hindernis ein Verkaufsargument.

3 · CLOUD-FEHLKONFIGURATION

Offene Speicher, zu weit gefasste Rechte, vergessene Testumgebungen: Fehlkonfigurationen in der Cloud zählen zu den häufigsten Ursachen für Datenabflüsse. In schnell gebauten Umgebungen ohne klare Standards passieren sie besonders leicht. Die Norm verlangt sichere Konfiguration und Änderungssteuerung (Annex A 8.9, 8.32) als festen Prozess statt als Zufallsergebnis.

4 · RISIKO SCHLÜSSELPERSON

In jungen Teams steckt entscheidendes Wissen oft in wenigen Köpfen, manchmal nur im Gründer. Fällt diese Person aus oder verlässt das Unternehmen, fehlen Zugänge, Wissen und Kontrolle zugleich. Dokumentierte Prozesse, geregelte Zugänge und ein sauberes Offboarding (Annex A 5.9 bis 5.11) machen das Unternehmen unabhängiger von Einzelnen und sind zugleich ein Reifesignal für Investoren.

5 · PHISHING UND SCHWACHE ZUGÄNGE

Angreifer zielen auf den einfachsten Weg hinein, und das sind meist Zugangsdaten. Geteilte Passwörter, fehlende Mehrfaktor-Anmeldung und unklare Rechte sind in jungen Teams verbreitet. Multifaktor-Authentifizierung, ein Passwort-Manager und regelmäßige Awareness (Annex A 5.17, 6.3, 8.5) gehören zu den wirksamsten und günstigsten Maßnahmen überhaupt. Sie kosten wenig und verhindern einen Großteil der typischen Angriffe.

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 Kunden und Investoren und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Für Startups ist der Zuschnitt entscheidend. Ein klar umrissener Scope, etwa das Produkt samt zugehöriger Infrastruktur, 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 und Verantwortlichkeiten zu (Kap. 5.1 bis 5.3). Im Startup heißt das: Die Gründer tragen das Thema sichtbar mit, statt es allein nach unten zu delegieren.

Dazu kommt die Unterstützung im Alltag (Kap. 7): klare Zuständigkeiten, Kompetenz im Team und eine geordnete Lenkung der Dokumente.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Das Unternehmen legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken und entscheidet je Risiko über die Behandlung (Kap. 6.1.2 und 6.1.3). Das Ergebnis mündet in die Erklärung zur Anwendbarkeit (Statement of Applicability), die für jede der 93 Maßnahmen begründet, ob sie gilt.

Genau hier zahlt sich Verhältnismäßigkeit aus. Nicht jede Maßnahme passt zu jedem Startup, aber jede Auswahl muss nachvollziehbar begründet 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. Für junge, cloud-native Teams stehen meist Zugriffskontrolle, Kryptografie, Lieferantensteuerung und sichere Entwicklung 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 funktionierenden, 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 schlankes ISMS, das gelebt wird, schlägt jede dicke Dokumentation, *die niemand öffnet.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope eng schneiden: welches Produkt, welche Systeme, welche Teams. 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 die nötigen Ressourcen bereit. Im Startup ist dieser Schritt schnell erledigt, wenn die Gründer dahinterstehen.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von Code-Repositories über SaaS-Dienste bis zur Cloud-Infrastruktur. 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: Zugriffskontrolle, Mehrfaktor-Anmeldung, Backup 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. Auffälligkeiten lassen sich so vor dem externen Termin in Ruhe abstellen.

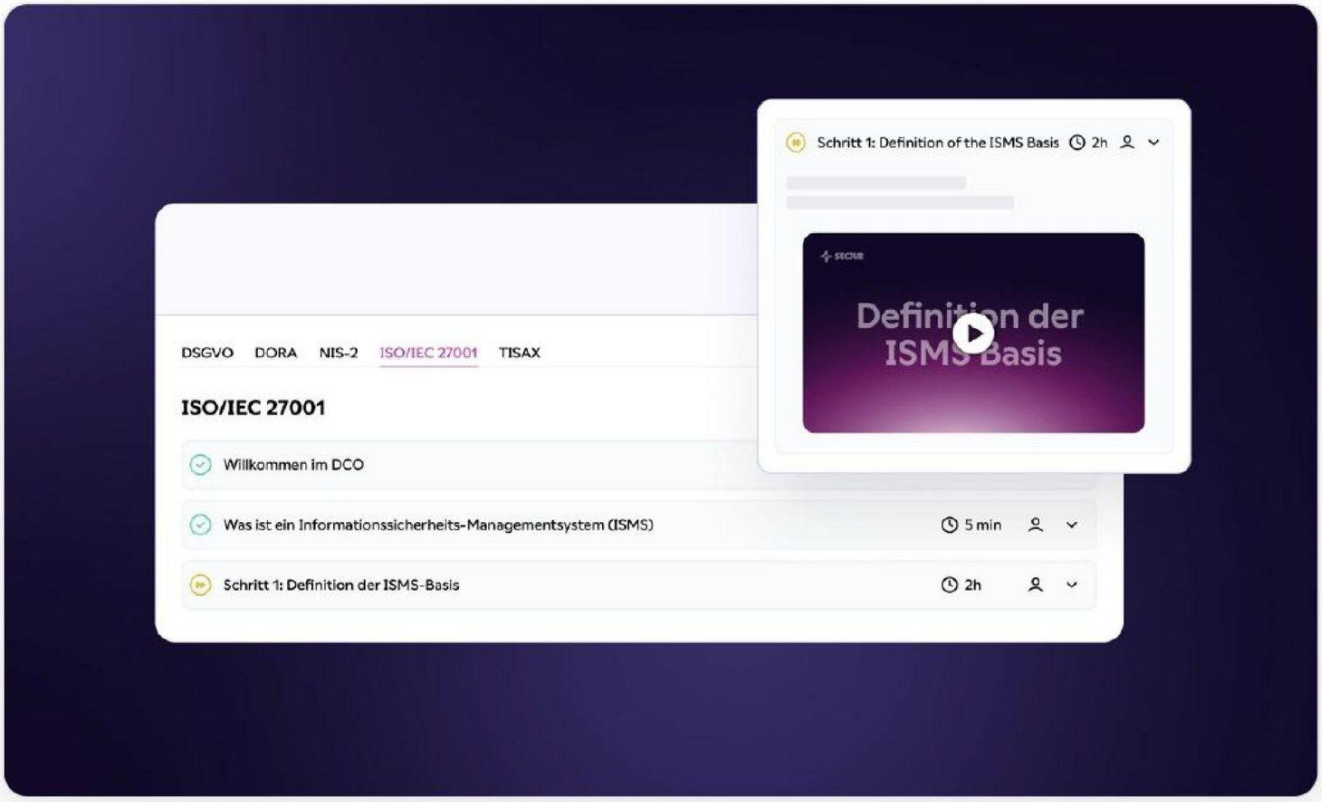
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung vor Ort oder remote (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, der mit dem Unternehmen weiterläuft.

WIE SECJUR ES EINFACH MACHT

Vom ersten Scope zum *zertifizierten ISMS.*

Das Digital Compliance Office (DCO) führt junge Teams durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse, Maßnahmen, 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. Teams berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Geführter Aufbau

Der Navigator führt Schritt für Schritt durch die Kapitel 4 bis 10, von der Leitlinie bis zur Managementbewertung, ohne Vorwissen vorauszusetzen.

Risiko & SoA

Geführte Risikoanalyse und eine Erklärung zur Anwendbarkeit, die jede der 93 Annex-A-Maßnahmen nachvollziehbar begründet und priorisiert.

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.

AUS DEUTSCHLAND, FÜR DEN ERNSTFALL GEBAUT

Alle Daten liegen in Deutschland, der Betrieb ist selbst nach ISO 27001 zertifiziert. Über 60 Integrationen holen Nachweise automatisch aus Ihren bestehenden Tools, 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.*

Vom frühen Startup bis zum etablierten Scale-up erfüllen Unternehmen mit dem DCO ihre Sicherheitsanforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem Startup-Umfeld:

„Dank Kundenvertrauen auf die *Financial-Times-1000-Liste.*"

René Schlüß
Founder & Managing Director, reanmo

reanmo

REFERENZEN AUS DEM STARTUP- UND TECH-UMFELD

Masterplan.com · 1KOMMA5° · Tomorrow · deepset · yfood · vestlane

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 JUNGE UNTERNEHMEN SECJUR WÄHLEN

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

Dazu kommt echte Begleitung: Wo eine Expertin gebraucht wird, ist sie zugeschaltet, und alle Daten liegen in Deutschland. So wird aus einer lästigen Pflichtübung ein geführter Prozess, der auch beim nächsten Wachstumsschub noch trägt.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Unternehmen, das seine Risiken kennt, seine Zugänge im Griff hat und im nächsten Sicherheitsfragebogen souverän auftritt. Genau das öffnet die Tür zu größeren Kunden und zur nächsten Finanzierungsrunde.

Und weil das ISMS gelebt statt abgeheftet wird, bleibt der Betrieb dauerhaft auditbereit: Überwachungsaudits, neue Kundenanforderungen und weitere Frameworks wie SOC 2 lassen sich auf demselben Fundament abbilden, ohne jedes Mal von vorn zu beginnen.

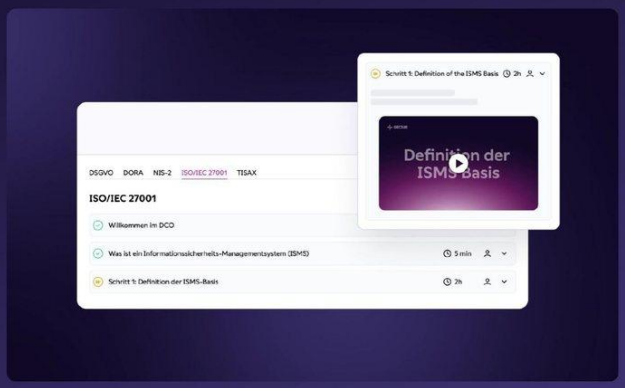
SECJUR

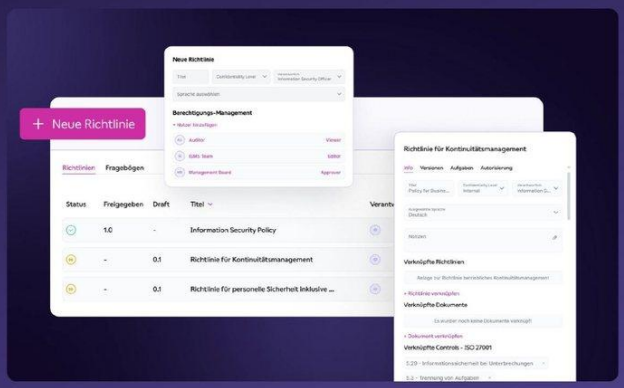
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 zur ISO 27001:

“Dank Kundenvertrauen auf die Financial-Times-1000-Liste”

René Schlüß
Founder & Managing Director, reanmo

reanmo

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

Masterplan.com 1KOMMA5° Tomorrow deepset yfood vestlane

www.secjur.com