SECJUR

WHITEPAPER
2026

ISO 27001 · SCALE-UPS & WACHSTUM

ISO 27001 für Scale-ups: *Sicherheit, die mit dem Wachstum Schritt hält.*

In der Startup-Phase war Sicherheit Nebensache, jetzt ist sie eine Voraussetzung für die nächste Stufe. Große Enterprise-Deals, internationale Märkte und Late-Stage-Investoren verlangen den Nachweis nach ISO 27001. Dieses Whitepaper zeigt, wie ein wachsendes Unternehmen seine über Jahre gewachsene, oft informelle Sicherheit in ein zertifiziertes ISMS überführt, ohne die Geschwindigkeit zu verlieren, die es groß gemacht hat.

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

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Wachstum bringt Sicherheit *an die Belastungsgrenze.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 oder die DSGVO ist er freiwillig. Für ein Scale-up ist er der Beweis, dass die Sicherheit mit dem Unternehmen mitgewachsen ist und nicht in der Garage stehen geblieben. In großen Deals und bei internationalen Kunden wird dieser Beweis zur Voraussetzung.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der Sicherheit von einzelnen Köpfen löst und in die Organisation einbettet. Genau das brauchen Unternehmen, deren Team sich jährlich verdoppelt.

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

In der Wachstumsphase wird Sicherheit nicht einfacher, sondern komplexer. Was im kleinen Team mündlich geregelt war, muss jetzt dokumentiert, verteilt und kontrolliert werden. Je später das geschieht, desto größer die Sicherheitsschuld, die ein Scale-up vor sich herschiebt.

Zugleich steigt der Einsatz. Enterprise-Verträge werden größer, internationale Ausschreibungen kommen hinzu, und spätestens in einer Series-C-Runde oder beim Exit prüft die Due Diligence die Sicherheit genau. Dieses Whitepaper ordnet ein, was die Norm verlangt, welche Risiken im Wachstum entstehen und wie der Weg zur Zertifizierung realistisch aussieht.

WOFÜR SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: Ihre Deals werden größer und die Sicherheitsprüfungen härter, Sie expandieren international, oder Sie bereiten eine späte Finanzierungsrunde oder einen Exit vor. Trifft eines davon zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Der Standard ist skalierbar und lässt sich mit SOC 2 oder NIS2 kombinieren. Ein einmal aufgebautes ISMS trägt mehrere Nachweise zugleich, statt für jeden Markt 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, in vier Gruppen von organisatorisch bis technisch.

BRANCHENKONTEXT

Im Wachstum wird Vertrauen *zur Voraussetzung.*

Ein Scale-up bewegt sich in einer anderen Liga als ein junges Startup. Die Kunden sind größer, die Märkte internationaler, die Erwartungen höher. ISO 27001 macht die Sicherheit nachweisbar, die diese Liga voraussetzt.

Was im Startup im Kopf der Gründer lag, *muss im Scale-up dokumentiert sein.*

ENTERPRISE-DEALS IM GROSSEN STIL

Mit der Größe der Kunden wächst die Tiefe der Prüfung. Wo ein erster Pilotkunde noch pragmatisch war, schickt ein Großkonzern strukturierte Sicherheitsfragebögen, verlangt Audits und macht das Zertifikat zur Vergabebedingung. Bei sechs- und siebenstelligen Vertragswerten ist die Sicherheitsprüfung kein Nebenschauplatz mehr.

ISO 27001 beantwortet einen Großteil dieser Fragen mit einem einzigen Dokument und verkürzt so den ohnehin längeren Vertriebszyklus großer Deals spürbar. Der Nachweis liegt bereits vor, statt für jeden Kunden neu erarbeitet zu werden.

INTERNATIONALE EXPANSION

Sobald ein Unternehmen über die Landesgrenze hinaus verkauft, trifft es auf Kunden, denen deutsche Eigenheiten nichts sagen. ISO 27001 dagegen ist weltweit anerkannt und spricht eine Sprache, die ein Einkäufer in London, New York oder Singapur versteht.

Für viele internationale Ausschreibungen ist das Zertifikat schlicht das Eintrittsticket. Ohne den anerkannten Nachweis bleibt ein Anbieter außen vor, unabhängig von der Qualität des Produkts.

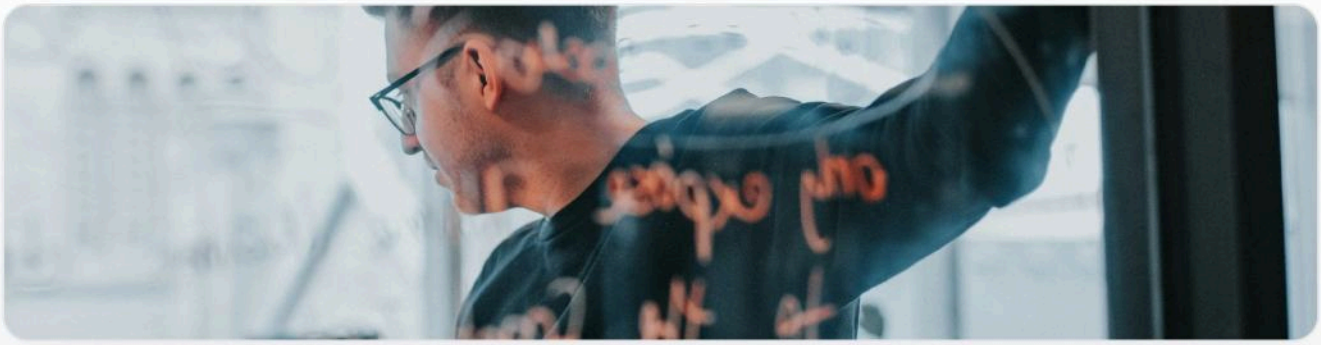
INVESTOREN UND EXIT

In späten Finanzierungsrunden, bei einer Übernahme oder vor einem Börsengang wird Informationssicherheit zum harten Prüfpunkt der Due Diligence. Käufer und Investoren wollen wissen, ob Risiken beherrscht sind und kein Vorfall die Bewertung gefährdet.

Ein etabliertes ISMS beschleunigt die Prüfung und stützt die Bewertung. Sein Fehlen wird zum Findings-Punkt, der Verhandlungsmacht kostet.

WAS AUF DEM SPIEL STEHT

Mit der Reichweite wächst der Schaden. Ein Vorfall trifft jetzt eine große Kundenbasis auf einmal, und der Reputationsschaden skaliert mit. In dieser Phase ist Sicherheit kein Kostenposten, sondern der Schutz von allem, was bereits aufgebaut wurde.



HERAUSFORDERUNGEN

Warum ISO 27001 Scale-ups *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Größe. Der Aufwand verlagert sich im Wachstum aber. Fünf Eigenheiten der Scale-up-Phase machen die Umsetzung speziell, und für jede gibt es einen pragmatischen Umgang.

AUFGELAUFENE SICHERHEITSSCHULD

In der Startup-Phase wurde Sicherheit oft improvisiert: geteilte Zugänge, gewachsene Rechte, Wissen in wenigen Köpfen. Im Wachstum rächt sich das. Diese Schuld muss aufgearbeitet werden, während der Betrieb auf Hochtouren läuft.

Die Norm gibt dafür einen Rahmen. Risikoanalyse und Erklärung zur Anwendbarkeit (Kap. 6) machen sichtbar, wo die größten Lücken liegen, und priorisieren die Aufarbeitung nach Risiko statt nach Bauchgefühl.

ORGANISATION IN BEWEGUNG

Ein Scale-up stellt schnell ein, gründet Teams, eröffnet Standorte. Jede dieser Bewegungen schafft neue Zugänge und neue Verantwortlichkeiten. On- und Offboarding (Annex A 6.1 bis 6.5) wird vom Randthema zur ständigen Aufgabe.

Ohne klare, wiederholbare Prozesse verliert eine wachsende Organisation den Überblick, wer worauf Zugriff hat. Genau dort schaut der Auditor besonders genau hin.

MEHRERE FRAMEWORKS ZUGLEICH

Wer international verkauft, sieht sich oft mit mehreren Anforderungen konfrontiert: ISO 27001 in Europa, SOC 2 im US-Geschäft, NIS2 als gesetzliche Pflicht. Getrennt aufgesetzt vervielfacht das den Aufwand. Ein gemeinsames ISMS als Fundament trägt alle drei, weil sich die Maßnahmen weitgehend überschneiden.

TOOL- UND LIEFERANTEN-SPRAWL

Mit dem Wachstum vervielfachen sich SaaS-Dienste, Cloud-Konten und Dienstleister. Jeder verarbeitet Daten, jeder ist ein Lieferant im Sinne der Norm (Annex A 5.19 bis 5.23). Ohne ein gepflegtes Verzeichnis dieser Landschaft bleibt die Risikoanalyse unvollständig und die Lieferkette ein blinder Fleck.

SICHERHEIT WIRD ZUR FUNKTION

Was eine Person nebenbei gemacht hat, muss jetzt eine Rolle oder ein kleines Team übernehmen. Die Norm verlangt benannte Verantwortung, Kompetenz und Wirksamkeitskontrolle (Kap. 5 und 7). Werkzeuge, die führen und dokumentieren, überbrücken die Phase, in der die eigene Sicherheitsfunktion erst entsteht.

BEDROHUNGSLAGE & RISIKEN

Wo Scale-ups *konkret angreifbar sind.*

Mit dem Wachstum wächst die Angriffsfläche schneller als die Schutzmaßnahmen. Die Risiken hängen an einer komplexer werdenden Organisation und an einem Datenbestand, der jetzt viele Kunden auf einmal betrifft. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · DATENPANNE MIT GROSSER REICHWEITE

Der teuerste Ernstfall. Wo ein junges Startup einen Kunden gefährdet, trifft ein Scale-up bei einem Vorfall Hunderte oder Tausende auf einmal. Der Schaden an Vertrauen und Ruf skaliert mit der Reichweite. Verschlüsselung, Zugriffskontrolle und Protokollierung (Annex A 8.2 bis 8.5, 8.24) sind im Audit ein zentraler Nachweis.

2 · VERLORENER GROSSAUFTRAG

Ein konkretes Geschäftsrisiko. Scheitert das Unternehmen an der Sicherheitsprüfung eines großen Kunden, steht jetzt ein sechs- oder siebenstelliger Auftrag auf dem Spiel. Ohne ISO 27001 zieht sich jede Prüfung, und manche endet vorzeitig. Das Zertifikat verschiebt das Gespräch vom Ob zur Umsetzung.

3 · INSIDER- UND OFFBOARDING-RISIKO

Bei hoher Fluktuation und schnellem Wachstum bleiben Zugänge ausscheidender Mitarbeiter offen, Rechte häufen sich an. Ein vergessenes Konto wird zum Einfallstor. Sauberes Offboarding und regelmäßige Rechteprüfung (Annex A 5.18, 6.5) schließen diese Lücke, die mit der Teamgröße automatisch wächst.

4 · RISIKO AUS DER LIEFERKETTE

Die Zahl der Dienstleister und SaaS-Anbindungen steigt mit dem Wachstum stark. Ein kompromittierter Anbieter wird zum Einstieg in das eigene Netz. Lieferantensteuerung mit Mindestanforderungen und deren Überprüfung (Annex A 5.19 bis 5.23) ist hier der wirksamste Hebel.

5 · CLOUD-KOMPLEXITÄT UND SCHWACHE ZUGÄNGE

Mit mehreren Cloud-Konten, Umgebungen und Teams steigt das Risiko von Fehlkonfigurationen und uneinheitlichen Zugängen. Sichere Konfiguration, Multifaktor-Authentifizierung und ein zentrales Identitätsmanagement (Annex A 8.9, 5.17, 8.5) bringen die Kontrolle zurück, die im schnellen Wachstum verloren geht.

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

Für Scale-ups ist der Zuschnitt entscheidend. Ein klarer Scope, der die Kernprodukte und ihre Infrastruktur abdeckt und Standorte bewusst einbezieht oder ausschließt, hält die Zertifizierung beherrschbar. Ein zu weiter 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). Im Scale-up heißt das, die entstehende Sicherheitsfunktion sichtbar zu mandatieren, statt sie nur geschehen zu lassen.

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, die für jede der 93 Maßnahmen begründet, ob sie gilt.

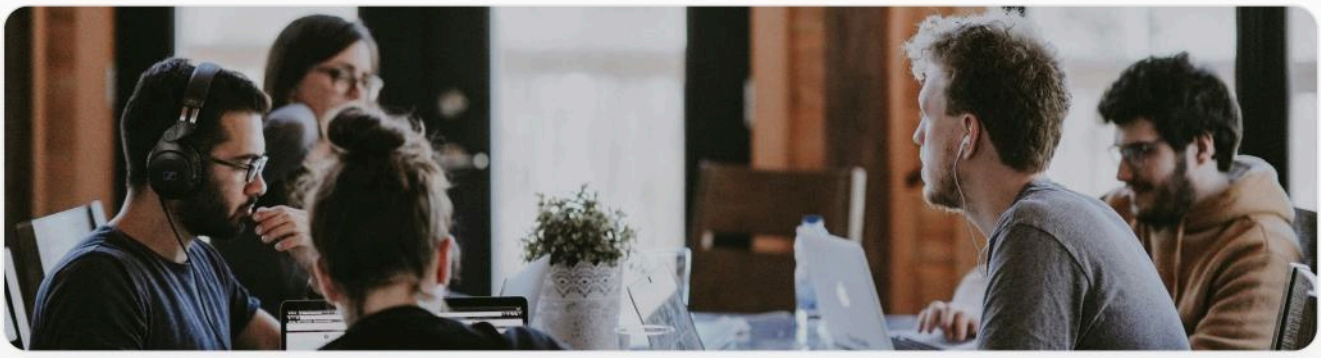
Genau hier zahlt sich Verhältnismäßigkeit aus und genau hier wird die Sicherheitsschuld aus der Frühphase sichtbar und planbar.

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 Wachstumsphase stehen Identitätsmanagement, Offboarding, 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 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 ISMS, das einmal steht, trägt ISO 27001, SOC 2 und NIS2 zugleich. *Ein Fundament, mehrere Nachweise.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope bewusst schneiden: welche Produkte, welche Systeme, welche Standorte. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und der wirksamste Hebel, um den Aufwand beherrschbar zu halten.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, mandatiert die Sicherheitsfunktion und stellt Ressourcen bereit. Dieser Schritt setzt das Signal, dass Sicherheit jetzt Teil der Organisation ist.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von Repositories über SaaS-Dienste bis zur Multi-Cloud. Risiken bewerten, die aufgelaufene Sicherheitsschuld sichtbar machen und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse priorisiert nach Risiko und macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Identitätsmanagement, Offboarding, Zugriffskontrolle 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.

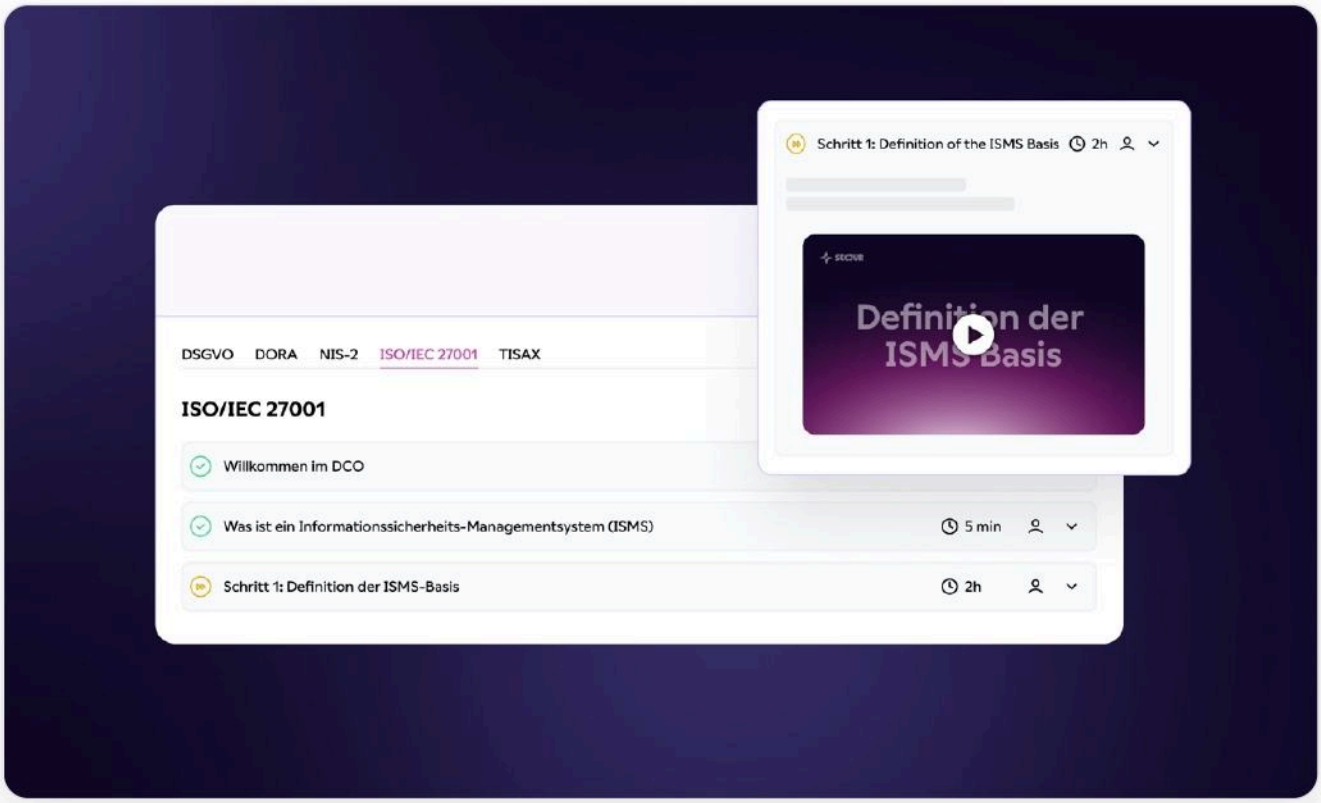
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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. Wer SOC 2 oder NIS2 ergänzt, baut auf demselben Fundament auf.

WIE SECJUR ES EINFACH MACHT

Vom gewachsenen Chaos zum *zertifizierten ISMS.*

Das Digital Compliance Office (DCO) führt wachsende Unternehmen durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse, Maßnahmen, interne Audits und Nachweise an einem Ort, mehrere Frameworks parallel. 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 und arbeitet die Sicherheitsschuld aus der Frühphase strukturiert ab, ohne Vorwissen vorauszusetzen.

Mehrere Frameworks

ISO 27001, SOC 2 und NIS2 laufen auf einem gemeinsamen ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt dreimal.

Nachweise & Audit

Revisionssichere Dokumentation, internes Audit und ein voller Audit-Trail, der auch der Due Diligence von Investoren standhält.

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, während das Unternehmen weiter skaliert.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich ISO 27001, SOC 2 und NIS2 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, von Microsoft 365 bis zur Cloud, sodass das ISMS auch bei hohem Tempo aktuell bleibt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

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

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

René Schlüß
Founder & Managing Director, reanmo

reanmo

REFERENZEN AUS DEM SCALE-UP- UND TECH-UMFELD

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

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 WACHSENDE UNTERNEHMEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen, die mehrere Frameworks zugleich bedienen. Das Team bleibt beim Produkt, das ISMS entsteht parallel.

Der digitale Compliance-Officer (DCO) bündelt Richtlinien, Aufgaben und Nachweise an einem Ort und verteilt Verantwortlichkeiten automatisch an die richtigen Personen. Was sonst in Tabellen und E-Mail-Threads zerfranst, wird nachvollziehbar und auditfest dokumentiert, ohne zusätzliche Stelle im Team.

Weil derselbe Unterbau ISO 27001, SOC 2 und NIS2 zugleich trägt, skaliert das System mit jeder neuen Anforderung mit, statt bei jedem Markteintritt von vorn zu beginnen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Unternehmen, das seine Risiken kennt, seine Lieferkette steuert und in jeder Due Diligence souverän auftritt. Genau das gewinnt große Deals und stützt die nächste Bewertung.

Ein gelebtes ISMS macht Sicherheit vom Vertriebshindernis zum Argument: Fragebögen sind in Stunden beantwortet, Audits verlieren ihren Schrecken, und Kunden wie Investoren sehen belegt, dass Wachstum und Sorgfalt zusammenpassen.

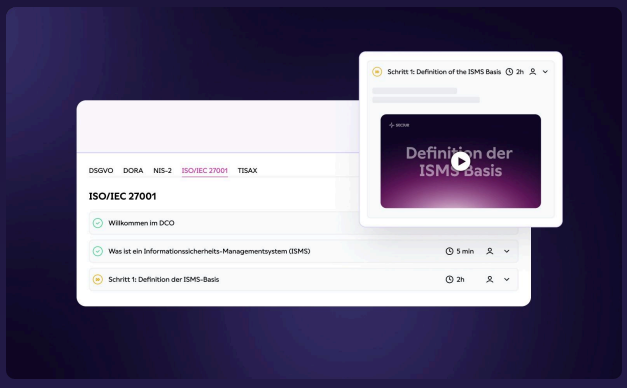
Damit wird aus einem Pflichtnachweis ein dauerhafter Wettbewerbsvorteil, der mit jedem Jahr an Wert gewinnt, statt nur einmal abgehakt zu werden.

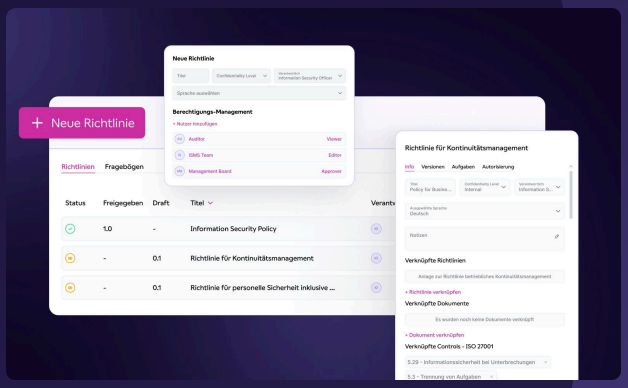
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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° · yfood · deepset · Tomorrow · AllDent Zahnzentrum

www.secjur.com