



ISO 27001 • MITTELSTAND

ISO 27001 im Mittelstand: *Sicherheit als Chefsache.*

Der deutsche Mittelstand ist erfolgreich, vernetzt und damit angreifbar geworden. Große Kunden geben Sicherheitsanforderungen über die Lieferkette weiter, Cyber-Versicherer verlangen nachweisbare Schutzmaßnahmen, und Ransomware trifft Hidden Champions genauso wie Konzerne. ISO 27001 ist der anerkannte Nachweis, dass ein Unternehmen seine Daten und sein Know-how im Griff hat. Dieses Whitepaper zeigt, wie der Mittelstand ein ISMS aufbaut, das zur eigenen Größe passt.

ISO 27001

NIS2

TISAX®

ISO 9001

DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Cybersicherheit ist im Mittelstand *zur Chefsache geworden.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 ist er kein Gesetz, sondern freiwillig. Für den Mittelstand ist er der Nachweis, dass ein Unternehmen seine Produktion, seine Konstruktionsdaten und die Daten seiner Kunden schützt. In Rahmenverträgen und Lieferantenprüfungen wird dieser Nachweis immer öfter verlangt.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der das Wissen aus den Köpfen einzelner Mitarbeiter in die Organisation überführt. Genau das schützt einen Betrieb, dessen Stärke oft an langjährigen Schlüsselpersonen hängt.

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. Große Kunden, oft Konzerne und OEMs, geben ihre

Sicherheitsanforderungen über die Lieferkette weiter und verlangen den Nachweis vertraglich. Cyber-Versicherer prüfen vor Abschluss die Schutzmaßnahmen, und der Verkehrs-, Energie- und Industriesektor fällt zunehmend unter NIS2, das ein ISMS weitgehend miterfüllt.

Hinzu kommt die Bedrohungslage. Ransomware zählt zu den größten Risiken für die deutsche Wirtschaft, und der Mittelstand ist ein bevorzugtes Ziel, weil Schutzlücken und Zahlungsfähigkeit hier oft zusammentreffen. 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: Ihre Kunden schicken Sicherheitsfragebögen oder fordern das Zertifikat, Ihr Versicherer verlangt Nachweise, oder Sie fallen unter NIS2. Trifft eines davon zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Der Standard ist verhältnismäßig. Er schreibt kein Konzern-Schutzniveau vor, sondern eines, das zur Größe und zum Risiko des Betriebs 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.



Der Mittelstand ist *das Rückgrat und ein Ziel.*

Hidden Champions, Familienunternehmen und spezialisierte Zulieferer tragen die deutsche Wirtschaft. Ihre Stärke, tiefe Integration in Wertschöpfungsketten und wertvolles Know-how, macht sie zugleich zum lohnenden Ziel. ISO 27001 macht die Sicherheit nachweisbar, die dieser Stand voraussetzt.

Ein erfolgreicher Mittelständler hat etwas zu schützen: *sein Wissen, seine Lieferfähigkeit, seinen Ruf.*

GEWACHSEN UND VERNETZT

Die IT im Mittelstand ist über Jahrzehnte gewachsen. Bewährte Systeme im eigenen Haus treffen auf neue Cloud-Dienste, ERP- und Produktionssysteme sind eng verzahnt, und der Datenaustausch mit Kunden und Lieferanten läuft längst digital. Diese Vernetzung schafft Effizienz und Angriffsfläche zugleich.

Anders als ein Startup kann ein gewachsener Betrieb nicht auf der grünen Wiese bauen. Er muss Bestehendes absichern, ohne die laufende Produktion zu stören. Genau darin liegt die eigentliche Aufgabe.

DRUCK AUS DER LIEFERKETTE

Große Kunden kaufen nicht mehr ohne Prüfung. Konzerne und OEMs geben ihre Sicherheitsanforderungen an Zulieferer weiter und verlangen den Nachweis, oft als ISO 27001 oder, in der Automobilbranche, als TISAX. Ohne Zertifikat geraten langjährige Lieferbeziehungen ins Wanken.

ISO 27001 beantwortet einen Großteil der Sicherheitsfragebögen mit einem einzigen Dokument. Statt jede Anfrage einzeln zu bearbeiten, legt der Betrieb den anerkannten Nachweis vor und bleibt gesetzter Lieferant.

VERSICHERER UND GESETZ

Cyber-Versicherer prüfen vor Abschluss zunehmend die Schutzmaßnahmen und verlangen ein Mindestniveau, das sich an Standards wie ISO 27001 orientiert. Parallel erfasst NIS2 weite Teile von Industrie, Energie und Verkehr. Ein ISMS deckt beides ab und spart Doppelarbeit.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als IT: gestohlene Konstruktionsdaten und Rezepturen, ein Produktionsstillstand mit Vertragsstrafen, der Verlust eines Großkunden und ein beschädigter Ruf, der über Generationen aufgebaut wurde. Sicherheit ist hier Schutz des Lebenswerks.



HERAUSFORDERUNGEN

Warum ISO 27001 im Mittelstand *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Größe. Der Aufwand ist es nicht. Fünf Eigenheiten mittelständischer Betriebe machen die Umsetzung speziell, und für jede gibt es einen pragmatischen Umgang.

GEWACHSENE, HETEROGENE IT

Neben moderner Software laufen oft ältere Systeme weiter, die für die Produktion unverzichtbar, aber nie für offene Vernetzung gedacht waren. Sie lassen sich nicht einfach abschalten oder patchen, ohne den Betrieb zu unterbrechen.

Die Norm verlangt keine Radikalkur, sondern eine Risikoanalyse (Kap. 6), die diese Altlasten bewertet und angemessen absichert. Kompensierende Maßnahmen wie Netztrennung schützen, wo ein Update nicht möglich ist.

DÜNNE IT- UND SECURITY-DECKE

Viele Betriebe haben kleine IT-Teams ohne eigene Sicherheitsfunktion, und der Fachkräftemangel verschärft das. Die Norm verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle (Kap. 5 und 7), nicht Heldentaten Einzelner.

Werkzeuge, die durch die Anforderungen führen und dokumentieren, ersetzen hier ein Stück weit das fehlende Spezialwissen und halten den Aufwand klein.

WISSEN IN WENIGEN KÖPFEN

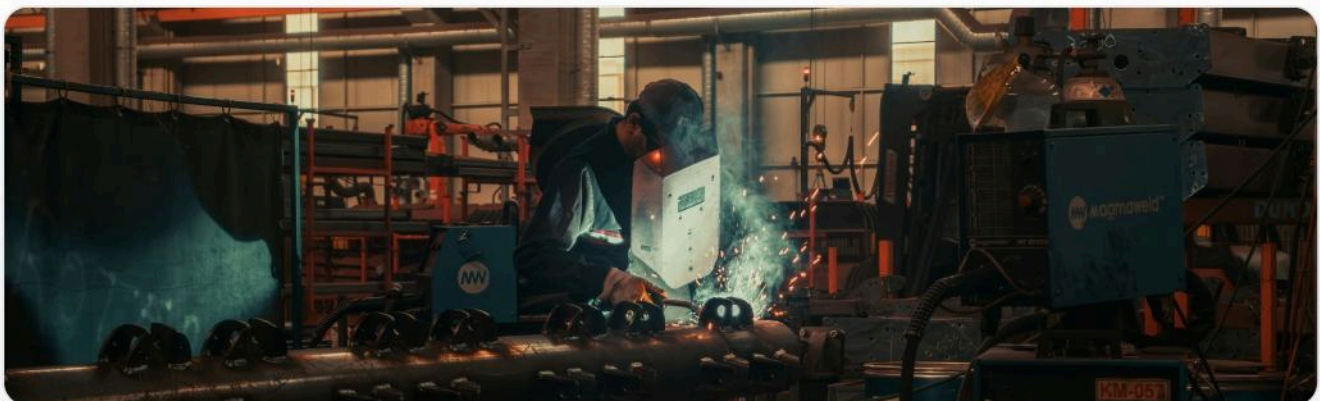
In gewachsenen Betrieben steckt entscheidendes Wissen oft bei langjährigen Mitarbeitern, manchmal beim Inhaber selbst. Fällt diese Person aus, fehlen Zugänge und Überblick zugleich. Dokumentierte Prozesse und geregelte Zugänge (Annex A 5.9 bis 5.11) machen den Betrieb unabhängiger und sichern die Nachfolge.

INVESTITIONSDENKEN STATT PROJEKTDENKEN

Der Mittelstand investiert gern in Maschinen, deren Nutzen sichtbar ist. Sicherheit wirkt dagegen abstrakt. Hier hilft die Verhältnismäßigkeit der Norm: Maßnahmen richten sich nach Größe und Risiko, nicht nach Konzernmaßstab. So bleibt die Investition überschaubar und der Nutzen, gewonnene Aufträge und vermiedene Ausfälle, messbar.

SCHEU VOR BÜROKRATIE

Viele Geschäftsführer fürchten Aktenberge und Stillstand. Ein gut geführtes ISMS ist das Gegenteil: schlank, gelebt und auf das Wesentliche reduziert. Ein überladenes System, das niemand pflegt, besteht kein Audit. Ein schlankes, das im Alltag funktioniert, schon.



Wo der Mittelstand *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an gewachsenen Systemen, an wertvollem Know-how und an einem Netz aus Kunden und Lieferanten. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE LEGT DIE PRODUKTION LAHM

Der häufigste Ernstfall. Werden zentrale Systeme verschlüsselt, steht die Produktion, Aufträge platzen, Vertragsstrafen drohen. Für einen Betrieb, der termingerecht liefern muss, ist das existenzbedrohend. Getestete Backups und ein eingeübter Notfallplan (Annex A 8.13, 5.29) entscheiden, ob der Stillstand Stunden oder Wochen dauert.

2 · DIEBSTAHL VON KNOW-HOW

Der Schatz vieler Mittelständler sind Konstruktionsdaten, Rezepturen und Verfahren. Wird dieses Wissen abgegriffen, sei es durch Angreifer oder über Industriespionage, ist der Wettbewerbsvorsprung von Jahren verloren. Verschlüsselung und strenge Zugriffskontrolle (Annex A 8.24, 8.2 bis 8.5) schützen das Kapital des Unternehmens.

3 · ANGRIFFE ÜBER DIE LIEFERKETTE

Angreifer nutzen den schwächsten Partner als Tür. Ein kompromittierter Lieferant oder IT-

Dienstleister wird zum Einfallstor. Genau hier setzt die Lieferantensteuerung nach Annex A 5.19 bis 5.23 an, mit Mindestanforderungen und deren Überprüfung. Große Kunden fordern denselben Nachweis vom Mittelstand selbst ein.

4 · RISIKO SCHLÜSSELPERSON

Wenn Zugänge, Wissen und Verantwortung bei wenigen langjährigen Personen liegen, wird ihr Ausfall zum Risiko. Geregelte Zugänge, Vertretungen und ein sauberes Offboarding (Annex A 5.18, 6.5) machen den Betrieb unabhängiger und sichern Kontinuität über Generationen.

5 · PHISHING UND SCHWACHE ZUGÄNGE

Angreifer zielen auf den einfachsten Weg hinein, und das sind meist Zugangsdaten. Geteilte Passwörter und fehlende Mehrfaktor-Anmeldung sind 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.



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. Der Betrieb bestimmt internen und externen Kontext, die Erwartungen wichtiger Parteien wie Kunden und Versicherer und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Für den Mittelstand ist der Zuschnitt entscheidend. Ein klarer Scope, etwa die Produktion samt zugehöriger IT an einem Standort, 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 zu (Kap. 5.1 bis 5.3). Im inhabergeführten Betrieb ist dieser Rückhalt schnell gegeben, wenn die Spitze dahintersteht.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Der Betrieb legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken von der Altanlage bis zur Cloud 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 zählt sich Verhältnismäßigkeit aus. Nicht jede Maßnahme passt zu jedem Betrieb, aber jede Auswahl muss nachvollziehbar 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. Im Mittelstand stehen Zugriffskontrolle, Backup, Lieferantensteuerung und der Schutz der Produktions-IT 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.



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 nach ISO 27001 erfüllt zugleich einen Großteil von NIS2. *Ein Aufbau, zwei Ergebnisse.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope eng schneiden: welcher Standort, welche Systeme, welche Prozesse. 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 Ressourcen bereit. Im inhabergeführten Betrieb ist dieser Schritt schnell erledigt, wenn die Spitze dahintersteht.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von der Produktions-IT über das ERP bis zur Cloud. 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: Backup, Zugriffskontrolle, Multifaktor-Anmeldung 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.

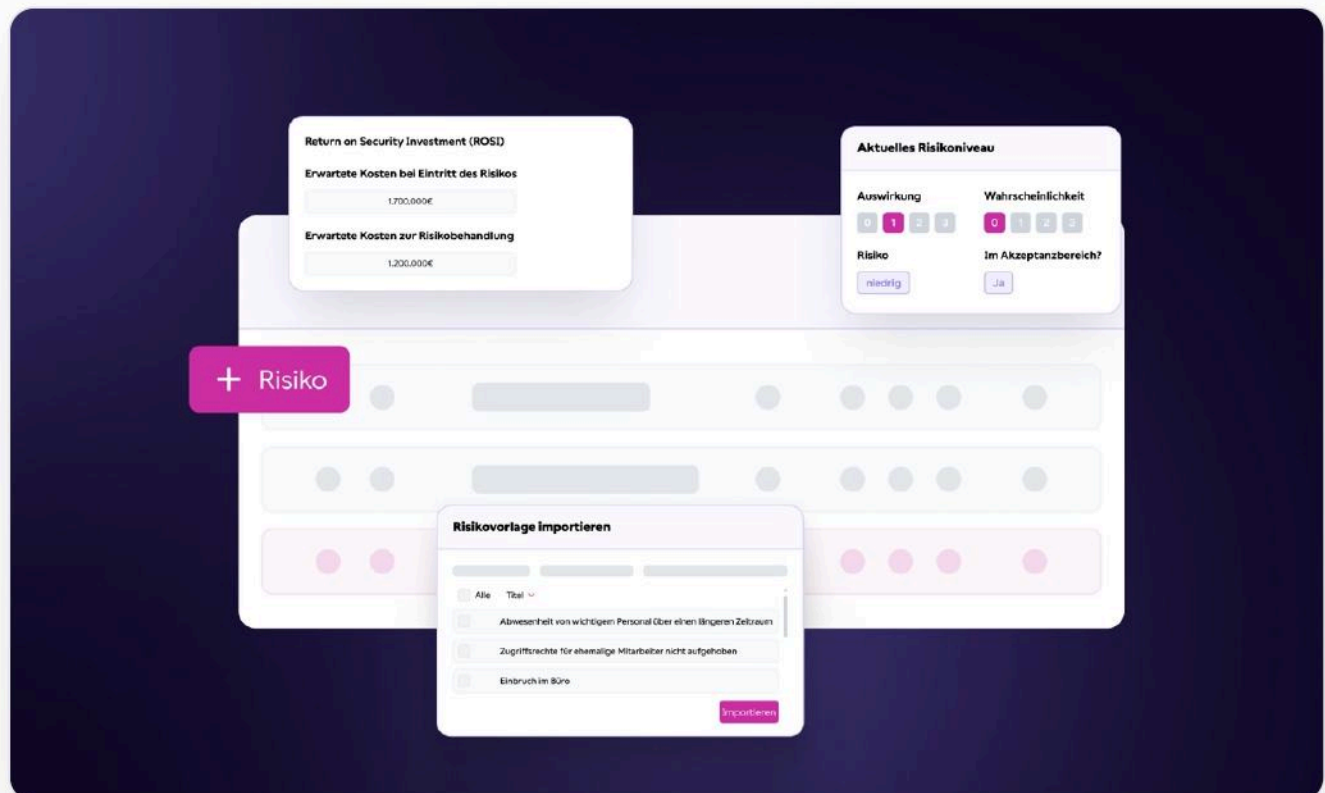
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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. ISO 27001 ist damit kein Projekt mit Enddatum, sondern ein dauerhafter Prozess.



Vom Gesetzes- und Kundendruck zur *auditbereiten* Umsetzung.

Das Digital Compliance Office (DCO) führt mittelständische Betriebe 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. Betriebe berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Risiko & SoA

Geführte Risikoanalyse von der Altanlage bis zur Cloud und eine Erklärung zur Anwendbarkeit, die jede Maßnahme nachvollziehbar begründet und priorisiert.

Lieferanten & Nachweise

Lieferantenbewertung und revisionssichere Dokumentation, genau dort, wo große Kunden und Annex A 5.19 bis 5.23 hinschauen.

Audit & NIS2

Voller Audit-Trail für die Zertifizierung, und weil sich ISO 27001 und NIS2 überschneiden, ist die gesetzliche Pflicht gleich mit abgedeckt.

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, ohne dass die Produktion stillsteht.

AUS DEUTSCHLAND, EIN AUFBAU FÜR ZWEI PFLICHTEN

Alle Daten liegen in Deutschland, der Betrieb ist selbst nach ISO 27001 zertifiziert. Weil sich ISO 27001 und NIS2 überschneiden, deckt das DCO beide zugleich ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, so dass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegen muss.

Über 500 Unternehmen *arbeiten mit SECJUR.*

Familienunternehmen, Zulieferer, Industriebetriebe und digitale Dienstleister erfüllen mit dem DCO ihre Sicherheitsanforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem Mittelstand:

„Mit SECJUR lassen sich alle NIS2-Anforderungen auf einer Plattform umsetzen. Dadurch konnten wir *innen einer Woche* ein zentrales, skalierbares Richtlinienensystem für die NIS2 aufbauen.“



Dipl.-Ing. Michael Dohr
Manager IT Security,
Nordzucker



REFERENZEN AUS DEM MITTELSTAND UND DER INDUSTRIE



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 DER MITTELSTAND SECJUR WÄHLT

Der Reiz liegt in der Geschwindigkeit und der Verhältnismäßigkeit. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen, die zum Betrieb passen statt zum Konzern. Das Team bleibt beim Tagesgeschäft, 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-Verläufen zerfranst, wird auditfest dokumentiert, ohne dass eine eigene Sicherheitsabteilung nötig ist.

Weil derselbe Unterbau ISO 27001, NIS2 und TISAX zugleich trägt, wächst das System mit

jeder neuen Kundenanforderung mit, statt bei jeder Prüfung von vorn zu beginnen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Betrieb, der seine Risiken kennt, sein Know-how schützt und in der nächsten Lieferantenprüfung souverän auftritt. Genau das sichert Aufträge und das Lebenswerk.

Ein gelebtes ISMS macht Sicherheit vom lästigen Fragebogen zum Verkaufsargument: Prüfungen sind in Stunden beantwortet, Audits verlieren ihren Schrecken, und große Kunden sehen belegt, dass ihr Zulieferer verlässlich ist.

So wird aus einer Pflicht ein dauerhafter Wettbewerbsvorteil, der die Lieferfähigkeit absichert und das über Generationen aufgebaute Vertrauen schützt.

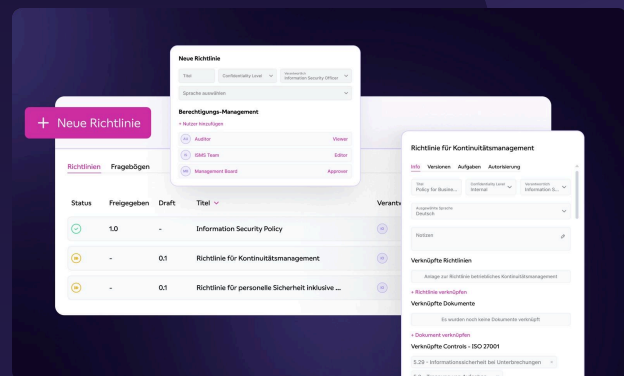
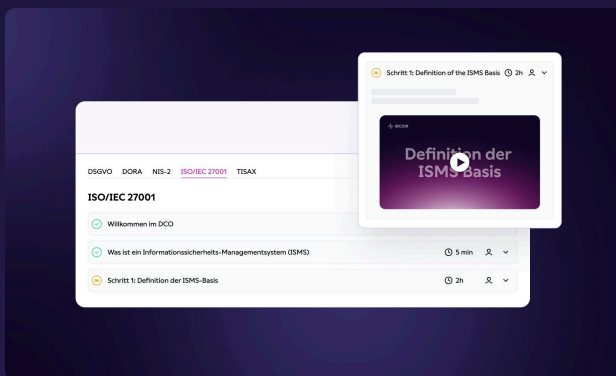


Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 automatisierten Compliance

"Mit SECJUR lassen sich alle NIS2-Anforderungen auf einer Plattform umsetzen. Dadurch konnten wir binnen einer Woche ein zentrales, skalierbares Richtliniensystem für die NIS2"



Dipl. Ing. Michael Dohr
Manager IT Security



Nordzucker

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR



Nordzucker

PETER KÖLLN



www.secjur.com