SECJUR

WHITEPAPER
2026

ISO 27001 · SOFTWARE & IT-CONSULTING

ISO 27001 für IT-Dienstleister: *Ihr Vertrauen ist Ihr Produkt.*

Software-Häuser, IT-Berater und Managed-Service-Provider arbeiten täglich in den Systemen und Daten ihrer Kunden. Genau dieses Vertrauen verlangt einen Nachweis. Auftraggeber prüfen ihre IT-Dienstleister inzwischen härter als jeden anderen Lieferanten, und ISO 27001 ist der anerkannte Beweis, dass die Informationssicherheit sitzt. Dieses Whitepaper zeigt, warum der Standard für IT-Dienstleister fast zur Geschäftsgrundlage wird und wie ein zertifizierungsreifes ISMS entsteht.

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

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Für IT-Dienstleister ist Sicherheit *die Geschäftsgrundlage.*

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 IT-Dienstleister ist er jedoch fast verpflichtend, weil sie privilegierten Zugang zu Kundensystemen und sensiblen Daten haben. Das Zertifikat ist der unabhängige Nachweis, dass dieser Zugang sicher verwaltet wird.

Ein ISMS ist dabei kein reines IT-Thema, auch wenn die Kunden ausgerechnet IT-Profis sind. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der zeigt, dass ein Dienstleister seine eigenen Versprechen einhält und nicht nur die Sicherheit anderer berät.

Weltweit sind über 70.000 Organisationen nach ISO 27001 zertifiziert, mit deutlich steigender Tendenz, und IT-Dienstleister stellen einen großen Anteil davon. 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 ist im IT-Markt besonders direkt. Auftraggeber machen das Zertifikat zur Ausschreibungsbedingung, und als Auftragsverarbeiter oder Sub-Dienstleister geben Kunden ihre eigenen Pflichten aus DSGVO und NIS2 vertraglich weiter. Wer in die Lieferkette eines regulierten Kunden gehört, muss liefern, was dieser nachweisen muss.

Hinzu kommt: Ein IT-Dienstleister ist ein attraktives Ziel, weil ein einziger Angriff über ihn gleich viele seiner Kunden trifft. Dieses Whitepaper ordnet ein, was die Norm verlangt, welche Risiken die Branche konkret trägt und wie der Weg zur Zertifizierung aussieht.

WOFÜR SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: Ausschreibungen verlangen das Zertifikat, Kunden schicken Auftragsverarbeitungsverträge und Sicherheitsfragebögen, oder Ihre Kunden fallen unter NIS2 und reichen die Pflichten weiter. Trifft eines zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Als IT-Dienstleister bringen Sie technisch viel mit. Häufig fehlt nur die Struktur drumherum, also Dokumentation, Prozesse und Nachweise. Genau die liefert ein schlankes ISMS.

WELTWEIT ZERTIFIZIERT

70.000+

Organisationen sind nach ISO 27001 zertifiziert, IT-Dienstleister mit großem Anteil.

AKTUELLE FASSUNG

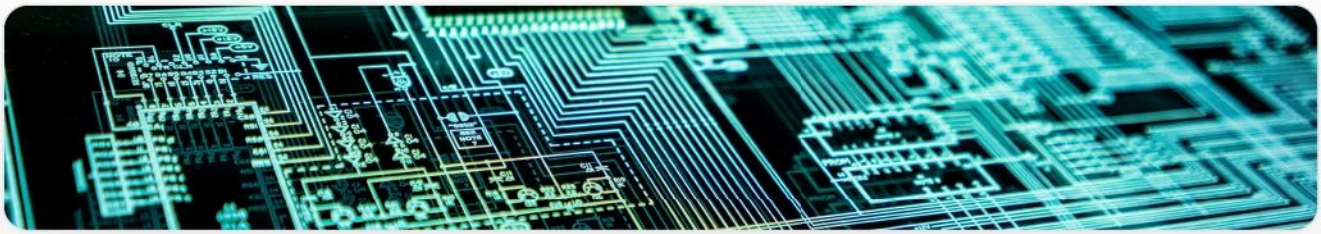
2022

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

Wer fremde Systeme betreut, *muss die eigenen beherrschen.*

Software-Häuser, IT-Berater und Managed-Service-Provider sitzen an einer besonders sensiblen Stelle: Sie haben Zugang zu allem. Genau deshalb prüfen Auftraggeber sie strenger als andere. ISO 27001 macht die eigene Sicherheit nachweisbar, statt sie nur zu versprechen.

Ein IT-Dienstleister verkauft Vertrauen. *ISO 27001 macht es prüfbar.*

PRIVILEGIERTER ZUGANG ZU ALLEM

Managed-Service-Provider verwalten die Infrastruktur ihrer Kunden, Software-Häuser verarbeiten deren Produktivdaten, Berater bekommen Administratorrechte für die Projektdauer. Kein anderer Lieferant kommt den Kronjuwelen eines Unternehmens so nah.

Dieser Zugang ist das Geschäftsmodell und das Risiko zugleich. Auftraggeber wissen das und verlangen Gewissheit, dass der Dienstleister diesen Zugang sauber verwaltet, protokolliert und absichert. Ein Zertifikat liefert diese Gewissheit auf einen Blick.

DAS ZERTIFIKAT ALS VERTRIEBSHEBEL

Im IT-Markt ist ISO 27001 vom Bonus zur Bedingung geworden. Öffentliche und große private Auftraggeber setzen es in Ausschreibungen voraus, und ohne Zertifikat fällt ein Anbieter oft schon in der Vorauswahl heraus.

Der Standard beantwortet zudem einen Großteil der Sicherheitsfragebögen, die im Vertrieb ohnehin kommen, mit einem einzigen Dokument. Statt jede Anfrage neu zu bearbeiten, legt der Dienstleister den anerkannten Nachweis vor und verkürzt seinen Vertriebszyklus.

DIE EIGENE ROLLE IN DER LIEFERKETTE

IT-Dienstleister sind selbst ein kritisches Glied in der Lieferkette ihrer Kunden. Über DSGVO-Auftragsverarbeitung und NIS2-Lieferkettenpflichten reichen regulierte Auftraggeber ihre Anforderungen vertraglich weiter. Ein ISMS nach ISO 27001 ist die strukturierte Antwort darauf und deckt NIS2 weitgehend mit ab.

WAS AUF DEM SPIEL STEHT

Für einen IT-Dienstleister ist Reputation alles. Ein Vorfall, der über ihn zu seinen Kunden durchschlägt, zerstört Vertrauen bei vielen auf einmal und ist im engen Markt kaum wiedergutzumachen. Sicherheit ist hier kein Kostenposten, sondern die Lizenz zum Geschäft.

HERAUSFORDERUNGEN

Warum ISO 27001 IT-Dienstleister *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Branche. Bei IT-Dienstleistern liegt die Hürde selten in der Technik, sondern an anderer Stelle. Fünf Eigenheiten machen die Umsetzung speziell.

TECHNIK STARK, STRUKTUR DÜNN

IT-Dienstleister beherrschen Firewalls, Verschlüsselung und Monitoring oft besser als ihre Kunden. Was fehlt, ist die Struktur drumherum: dokumentierte Richtlinien, nachvollziehbare Prozesse und der Nachweis der Wirksamkeit (Kap. 5 bis 9).

Der Auditor prüft nicht, ob ein Tool gut ist, sondern ob es geregelt, dokumentiert und überprüft eingesetzt wird. Genau diese Formalisierung des ohnehin Vorhandenen ist die eigentliche Arbeit.

MANDANTENTRENNUNG

Wer viele Kunden gleichzeitig betreut, muss deren Daten und Zugänge sauber trennen. Eine Vermischung ist nicht nur ein Sicherheits-, sondern auch ein Vertrauensproblem. Die Norm verlangt klare Zugriffskontrolle und Trennung von Umgebungen (Annex A 5.15, 8.3, 8.31), gerade im Multi-Mandanten-Betrieb.

PRIVILEGIERTE ZUGÄNGE IM GRIFF

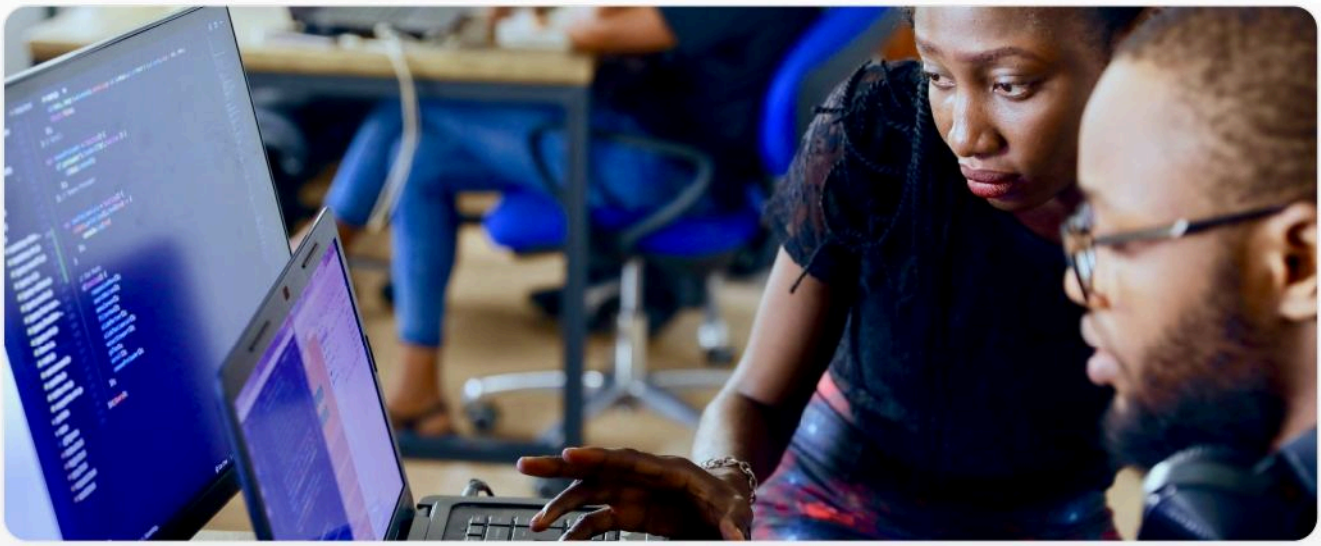
Administrator- und Fernzugänge zu Kundensystemen sind das größte Pfund und das größte Risiko. Sie müssen streng vergeben, protokolliert und nach Projektende wieder entzogen werden. Privileged-Access-Management und Protokollierung (Annex A 8.2, 8.15, 8.18) stehen für IT-Dienstleister besonders im Fokus.

TEMPO UND VERTEILTE TEAMS

Projektgeschäft, Remote-Arbeit und schnelle Teamwechsel erschweren ein sauberes On- und Offboarding. Werden Zugänge nicht konsequent entzogen, sammeln sich verwaiste Berechtigungen an. Geregelte Prozesse (Annex A 5.18, 6.5) halten diese Lücke klein.

EIGENE LIEFERKETTE AUS SAAS

IT-Dienstleister nutzen selbst zahlreiche Cloud- und SaaS-Dienste, über die wiederum Kundendaten laufen. Jeder ist ein Sub-Dienstleister im Sinne der Norm (Annex A 5.19 bis 5.23). Ohne Übersicht über diese Kette bleibt die Risikoanalyse unvollständig.



BEDROHUNGSLAGE & RISIKEN

Wo IT-Dienstleister *konkret angreifbar sind.*

Die Risiken hängen am privilegierten Zugang und an der Rolle als Multiplikator: Wer einen IT-Dienstleister trifft, trifft viele seiner Kunden. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · SUPPLY-CHAIN-ANGRIFF ÜBER DEN DIENSTLEISTER

Der Albtraum der Branche. Angreifer kompromittieren einen IT-Dienstleister, um über dessen Zugänge oder Software-Updates gleich in die Netze vieler Kunden zu gelangen. Der Schaden vervielfacht sich und trifft das Vertrauen ins Mark. Strenge Zugriffskontrolle, getrennte Umgebungen und sichere Entwicklung (Annex A 8.3, 8.25 bis 8.31) sind hier zentral.

2 · MISSBRAUCH PRIVILEGIERTER ZUGÄNGE

Administrator- und Fernzugänge sind das lohnendste Ziel. Werden Zugangsdaten abgegriffen oder nach Projektende nicht entzogen, steht Angreifern die Kundenumgebung offen. Privileged-Access-Management, Mehrfaktor-Anmeldung und lückenlose Protokollierung (Annex A 8.2, 8.5, 8.15) schließen diese Tür.

3 · DATENABFLUSS AUS KUNDENPROJEKTEN

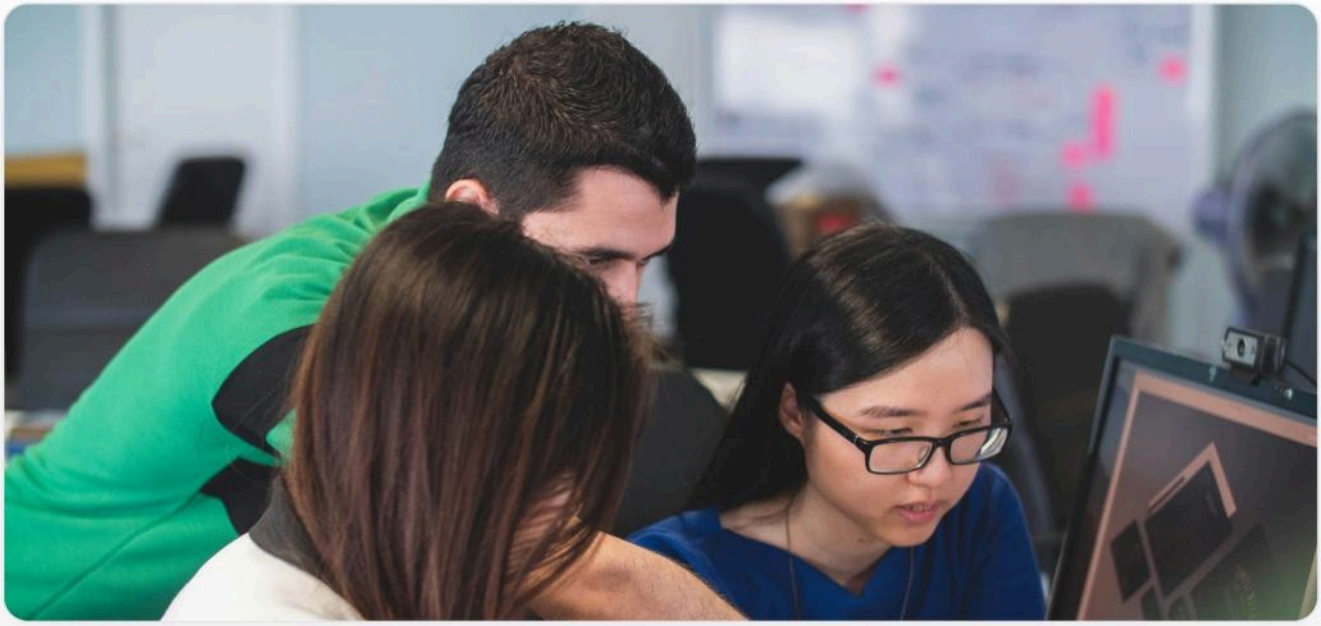
IT-Dienstleister verarbeiten fremde Produktiv- und Personendaten. Ein Abfluss ist zugleich ein DSGVO-Vorfall des Kunden und ein Vertrauensbruch. Verschlüsselung, saubere Mandantentrennung und Zugriffskontrolle (Annex A 8.24, 8.3, 5.15) begrenzen den Schaden.

4 · SCHWACHSTELLEN IM EIGENEN CODE

Wer Software entwickelt, liefert mit jeder Schwachstelle auch ein Einfallstor an seine Kunden aus. Sichere Entwicklung, Code-Prüfung und getrennte Test- und Produktivumgebungen (Annex A 8.25 bis 8.31) sind für Software-Häuser keine Kür, sondern Pflicht.

5 · PHISHING UND RANSOMWARE

Auch IT-Profis werden Opfer von Phishing, und ein Ransomware-Vorfall im eigenen Haus legt nicht nur den Dienstleister, sondern auch die betreuten Kunden lahm. Awareness, Mehrfaktor-Anmeldung und getestete Backups (Annex A 6.3, 5.17, 8.13) gehören zu den wirksamsten Maßnahmen.



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

Für IT-Dienstleister ist der Zuschnitt entscheidend. Der Scope sollte die Dienstleistungen abdecken, die Kunden tatsächlich prüfen, also Betrieb, Entwicklung oder Beratung samt zugehöriger Systeme. 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). Gerade weil Kunden auf Verlässlichkeit achten, muss die Spitze das Thema sichtbar tragen.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Der Dienstleister legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken rund um Kundenzugänge und Daten 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.

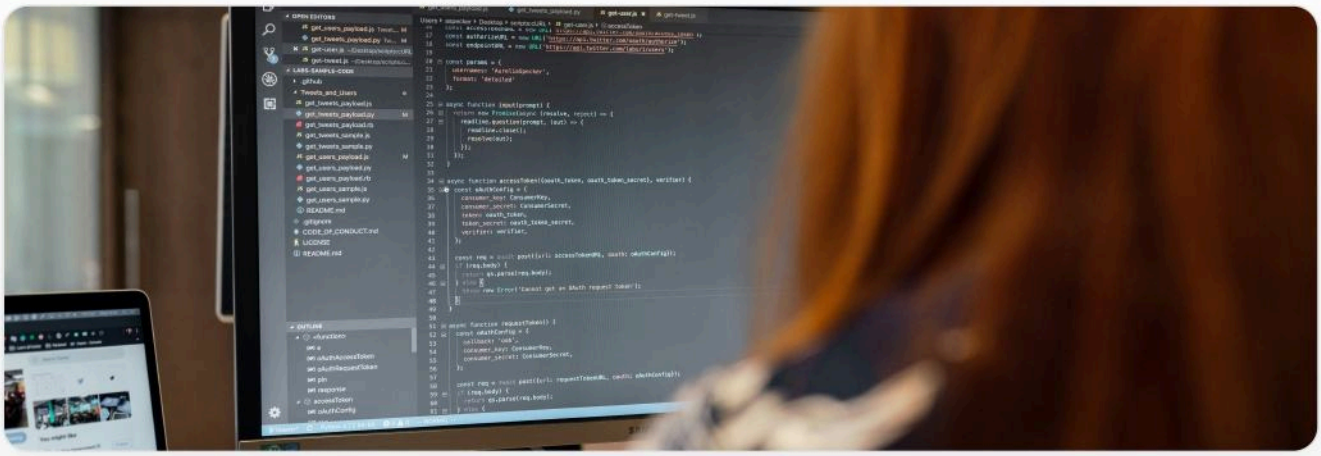
Privilegierte Zugänge, Mandantentrennung und Lieferkette stehen dabei für IT-Dienstleister fast immer oben auf der Liste.

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. Im IT-Geschäft stehen Zugriffs- und Privileged-Access-Management, sichere Entwicklung und Lieferantensteuerung 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 die starke Technikbasis von IT-Dienstleistern, statt bei null zu beginnen. Realistisch sind je nach Reife drei bis sechs Monate bis zum Audit.

Die Technik steht meist schon. *ISO 27001 macht sie nachweisbar und verkaufbar.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die Dienstleistungen schneiden, die Kunden prüfen. 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. In kleinen, technikgetriebenen Teams ist dieser Schritt schnell erledigt.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von Kundenzugängen über die eigene Entwicklungs- und Betriebsumgebung bis zu den genutzten SaaS-Diensten. Risiken bewerten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse priorisiert nach Risiko und macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

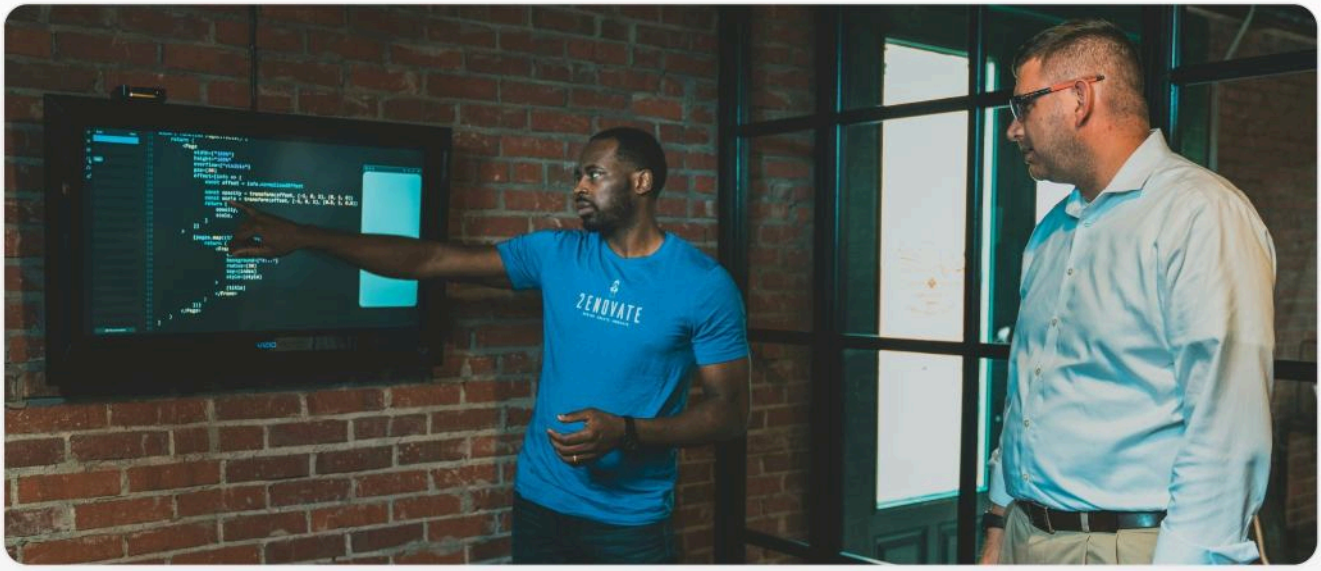
Die ausgewählten Annex-A-Maßnahmen einführen und vor allem dokumentieren. Die Technik ist oft da, der Nachweis fehlt. Privileged-Access-Management, Mandantentrennung, sichere Entwicklung und Lieferantenanforderungen zuerst.

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

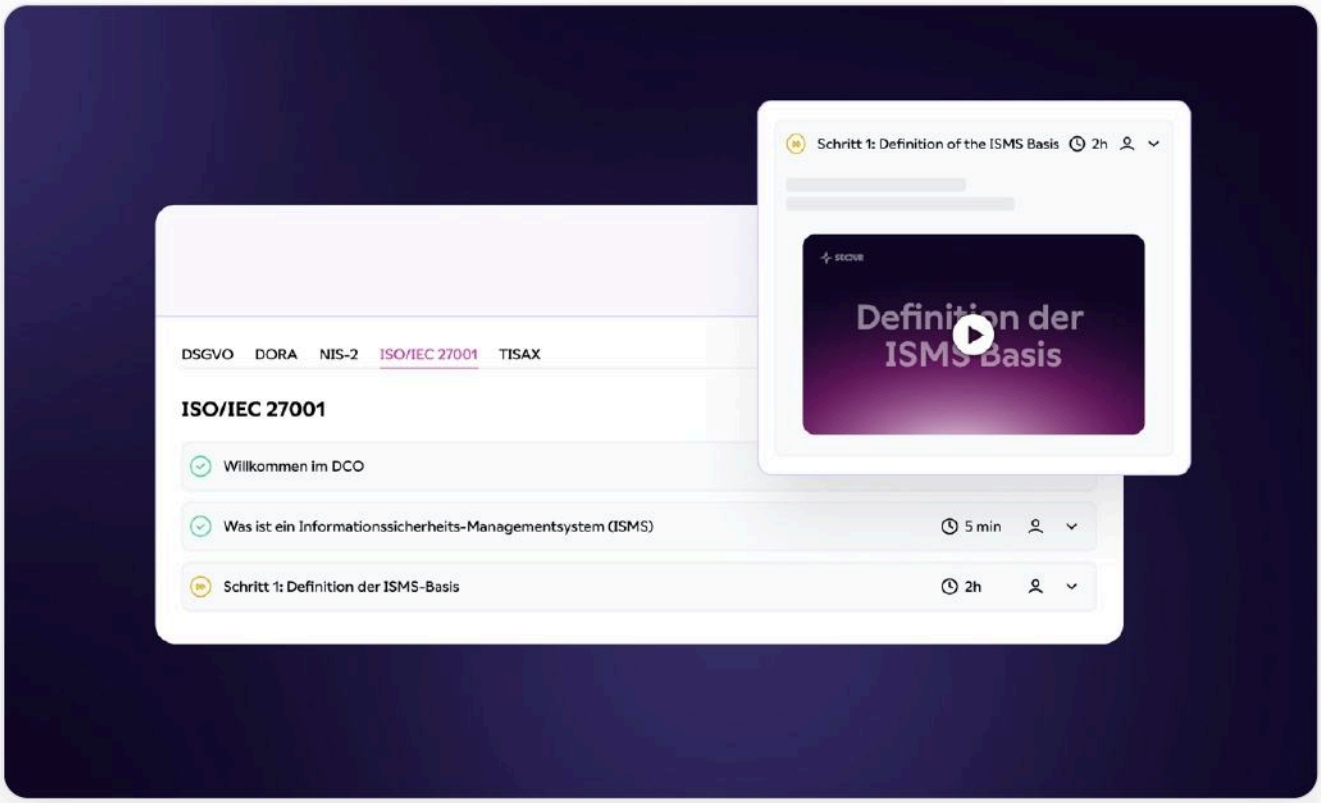
Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung (Stage 2). Danach folgt das Zertifikat, gültig für drei Jahre mit jährlichen Überwachungsaudits. Wer SOC 2 oder NIS2 ergänzt, baut auf demselben Fundament auf.



WIE SECJUR ES EINFACH MACHT

Von der starken Technik zum *zertifizierten ISMS.*

Das Digital Compliance Office (DCO) führt IT-Dienstleister 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 formalisiert die vorhandene Technik zu auditfähigen Prozessen, ohne dass Sie das Rad neu erfinden.

Zugänge & Lieferkette

Module für Zugriffskontrolle, Privileged-Access und Lieferantensteuerung, genau die Punkte, die Auftraggeber und Annex A 5.19 bis 5.23 bei IT-Dienstleistern prüfen.

Mehrere Frameworks

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

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 wird aus vorhandener Technik in Wochen ein auditbereites ISMS, statt in Quartalen.

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 im Projektgeschäft aktuell bleibt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Software-Häuser, Managed-Service-Provider, IT-Berater und digitale Dienstleister erfüllen mit dem DCO ihre Sicherheitsanforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem IT-Umfeld:

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

René Schlüß
Founder & Managing Director, reanmo

reanmo

REFERENZEN AUS SOFTWARE, IT-CONSULTING UND MANAGED SERVICES

deepset · Masterplan.com · think-cell · WatchGuard · statista · team internet.

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 IT-DIENSTLEISTER 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 Kundenprojekt, 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. Über 60 Integrationen holen Belege direkt aus den Systemen, mit denen ohnehin gearbeitet wird, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Weil derselbe Unterbau ISO 27001, SOC 2 und die Anforderungen aus Auftragsverarbeitungsverträgen zugleich trägt, skaliert das System mit jedem neuen Kunden mit, statt bei jeder Ausschreibung von vorn zu beginnen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Dienstleister, der seine Zugänge im Griff hat, seine Lieferkette steuert und in jeder Ausschreibung souverän auftritt. Genau das gewinnt Aufträge und hält Kunden.

Ein gelebtes ISMS macht Sicherheit vom lästigen Fragebogen zum Verkaufsargument: Kundenaudits sind in Stunden beantwortet, Sicherheitsprüfungen verlieren ihren Schrecken, und Auftraggeber sehen belegt, dass ihre Daten in verlässlichen Händen liegen.

So wird aus einer Pflicht ein dauerhafter Wettbewerbsvorteil, der die Position in Ausschreibungen stärkt und das Vertrauen der Kunden langfristig sichert.

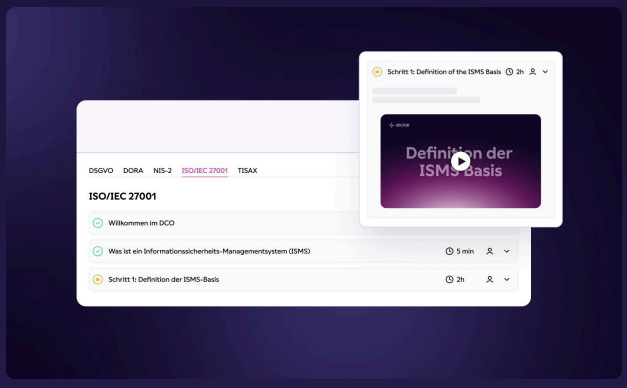
SECJUR

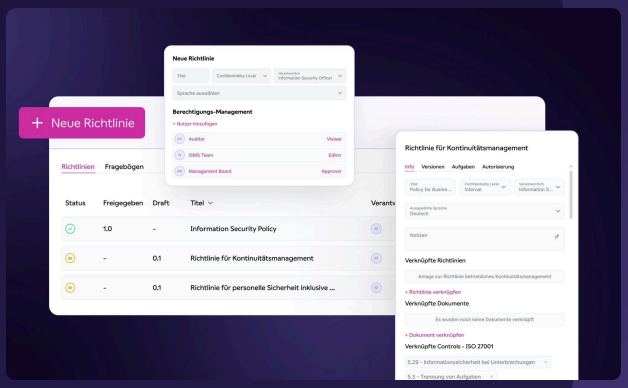
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

deepset · Masterplan.com · team internet. · think-cell · statista · WatchGuard

www.secjur.com