SECJUR

WHITEPAPER
2026

ISO 27001 · IT-SYSTEMHÄUSER & MANAGED SERVICES

ISO 27001 für Systemhäuser: *Ihre Kunden vertrauen Ihnen ihre IT an.*

IT-Systemhäuser beschaffen, integrieren und betreiben die IT ihrer Kunden, oft mit vollem administrativem Zugriff und über Managed Services aus der Ferne. Genau dieser Zugang macht sie zum lohnenden Ziel und zum Prüffall. Öffentliche Auftraggeber verlangen ISO 27001 als Eignungskriterium, Hersteller koppeln Partnerprogramme an Sicherheitsnachweise, und regulierte Kunden geben ihre Pflichten weiter. Dieses Whitepaper zeigt, warum der Standard zur Geschäftsgrundlage wird und wie ein belastbares ISMS entsteht.

ISO 27001 | NIS2 | BSI-Grundschutz | SOC 2 | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Wer die IT anderer betreibt, *muss die eigene beherrschen.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 ist er freiwillig. Für IT-Systemhäuser ist er trotzdem fast verpflichtend, weil sie privilegierten Zugang zu den Systemen vieler Kunden haben und diese Verantwortung nachweisen müssen. Das Zertifikat belegt, dass dieser Zugang sicher verwaltet wird.

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

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 Systemhausgeschäft besonders direkt. Öffentliche Auftraggeber setzen ISO 27001 als Eignungskriterium in Vergabeverfahren voraus, Hersteller knüpfen höhere Partnerstufen an Sicherheitsnachweise, und Kunden, die selbst unter NIS2 fallen, geben ihre Pflichten über die Lieferkette weiter.

Hinzu kommt: Ein Systemhaus ist ein attraktives Ziel, weil ein einziger Angriff über seine Fernwartungswerkzeuge gleich viele 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: Sie bewerben sich um öffentliche Aufträge, Sie betreiben Managed Services mit Fernzugriff auf Kundensysteme, oder Ihre Hersteller- und Großkunden fordern Nachweise. Trifft eines zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Als Systemhaus 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

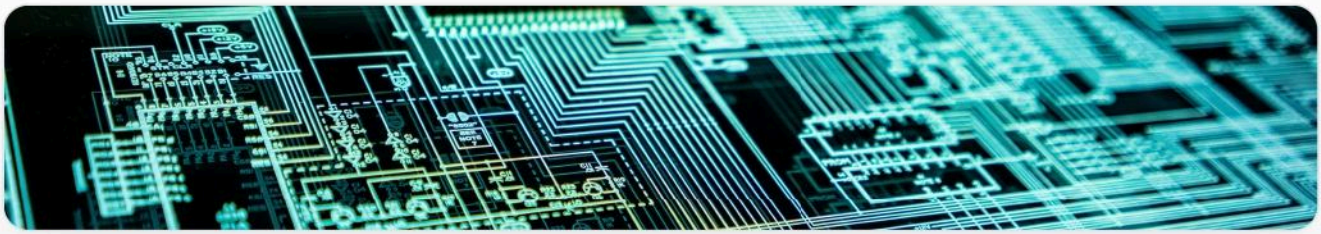
2022

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

Das Systemhaus ist *der Generalschlüssel zur Kunden-IT.*

IT-Systemhäuser beschaffen Hardware und Software, bauen Netzwerke und betreiben die IT ihrer Kunden, vom Mittelstand bis zur öffentlichen Hand. Mit diesem Zugang kommt Verantwortung, und Auftraggeber verlangen dafür einen Nachweis. ISO 27001 liefert ihn.

Ein einziges Fernwartungswerkzeug öffnet Hunderte Kundennetze. *Das ist Chance und Gefahr zugleich.*

BESCHAFFEN, INTEGRIEREN, BETREIBEN

Systemhäuser decken die gesamte Kette ab: Beratung, Beschaffung von Hard- und Software, Integration, Migration und der laufende Betrieb über Managed Services. Viele Kunden geben ihre IT vollständig in diese Hände, inklusive administrativer Zugänge und Fernwartung.

Diese Tiefe ist das Geschäftsmodell und das Risiko zugleich. Wer die IT vieler Kunden betreut, bündelt deren Schwachstellen und wird selbst zum sensibelsten Punkt in deren Sicherheit.

ÖFFENTLICHE VERGABE UND HERSTELLER

Im Geschäft mit der öffentlichen Hand ist ISO 27001 häufig ein Eignungskriterium: Ohne Zertifikat ist eine Teilnahme an vielen Ausschreibungen gar nicht möglich. Zugleich koppeln Hersteller wie die großen Plattform- und Netzwerkanbieter höhere Partnerstufen zunehmend an Sicherheitsnachweise.

ISO 27001 beantwortet zudem einen Großteil der Sicherheitsfragebögen privater Großkunden mit einem einzigen Dokument. Statt jede Anfrage neu zu bearbeiten, legt das Systemhaus den anerkannten Nachweis vor und qualifiziert sich für größere Aufträge.

TEIL DER LIEFERKETTE DER KUNDEN

Systemhäuser sind 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 und deckt NIS2 weitgehend mit ab.

WAS AUF DEM SPIEL STEHT

Für ein Systemhaus ist Reputation alles. Ein Vorfall, der über die eigene Infrastruktur zu den Kunden durchschlägt, zerstört Vertrauen bei vielen auf einmal und ist im engen Markt kaum wiedergutzumachen. Sicherheit ist hier die Lizenz zum Geschäft.

HERAUSFORDERUNGEN

Warum ISO 27001 Systemhäuser *besonders fordert.*

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

TECHNIK STARK, STRUKTUR DÜNN

Systemhäuser beherrschen Firewalls, Backup 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 Werkzeug gut ist, sondern ob es geregelt, dokumentiert und überprüft eingesetzt wird. Genau diese Formalisierung des ohnehin Vorhandenen ist die eigentliche Arbeit.

FERNWARTUNG ALS KRITISCHER PUNKT

Managed Services laufen über zentrale Fernwartungs- und Monitoring-Werkzeuge, die Zugriff auf viele Kundennetze bündeln. Wird ein solches Werkzeug kompromittiert, steht Angreifern die gesamte Kundenbasis offen.

Diese Werkzeuge verdienen härtesten Schutz: Mehrfaktor-Anmeldung, strenge Rechtevergabe und lückenlose Protokollierung (Annex A 8.2, 8.5, 8.15) sind hier Pflicht, nicht Kür.

MANDANTENTRENNUNG

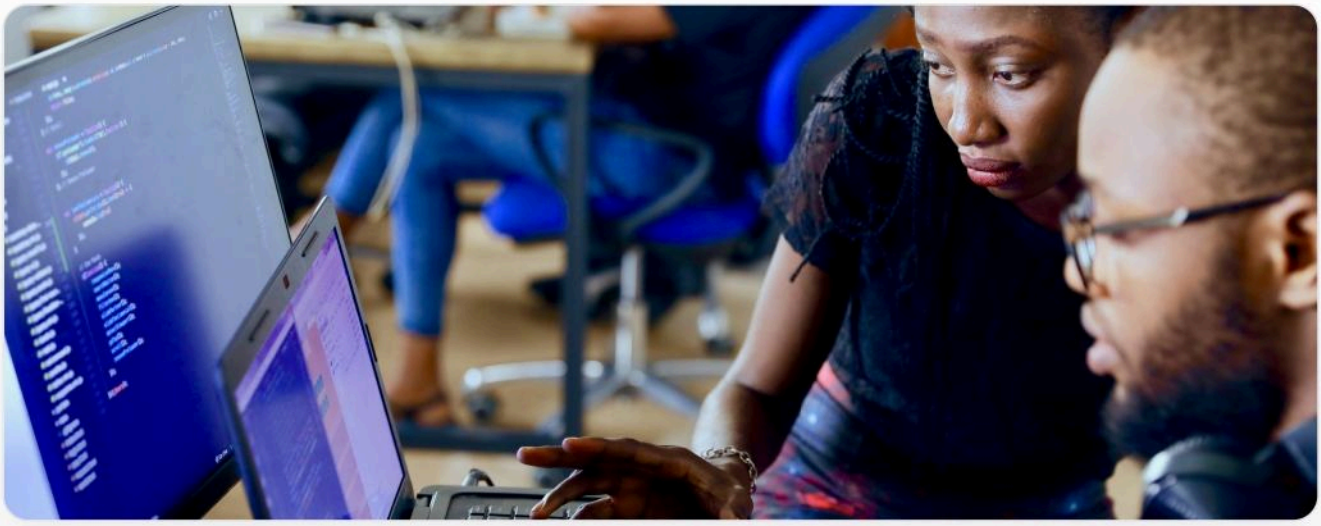
Wer viele Kunden gleichzeitig betreut, muss deren Systeme, Daten und Zugänge sauber trennen. Eine Vermischung ist nicht nur ein Sicherheits-, sondern auch ein Vertrauensproblem. Die Norm verlangt klare Zugriffskontrolle und Trennung von Umgebungen (Annex A 5.15, 8.3, 8.31).

BESCHAFFUNG UND LIEFERKETTE

Systemhäuser liefern Hard- und Software aus Distribution und von Herstellern aus. Manipulierte Geräte oder kompromittierte Updates können über das Systemhaus zum Kunden gelangen. Lieferantensteuerung und sichere Beschaffung (Annex A 5.19 bis 5.23) gehören deshalb in den Kern des ISMS.

TECHNIKER UND FLUKTUATION

Technikerteams wechseln, arbeiten im Außeneinsatz und beim Kunden und tragen weitreichende Rechte. Werden Zugänge nicht konsequent vergeben und wieder entzogen, sammeln sich gefährliche Berechtigungen an. Sauberes On- und Offboarding (Annex A 5.18, 6.5) hält diese Lücke klein.



BEDROHUNGSLAGE & RISIKEN

Wo Systemhäuser *konkret angreifbar sind.*

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

1 · ANGRIFF ÜBER DAS FERNWARTUNGSWERKZEUG

Der Albtraum der Branche. Kompromittieren Angreifer das zentrale Monitoring- und Fernwartungswerkzeug, gelangen sie über dessen Zugänge gleich in die Netze vieler Kunden und können dort breit Schadsoftware ausrollen. Der Schaden vervielfacht sich. Härtung, Mehrfaktor-Anmeldung und Protokollierung dieser Werkzeuge (Annex A 8.2, 8.5, 8.15, 8.9) sind die zentrale Schutzlinie.

2 · MISSBRAUCH PRIVILEGIERTER ZUGÄNGE

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

3 · KOMPROMITTIERTE LIEFERUNG

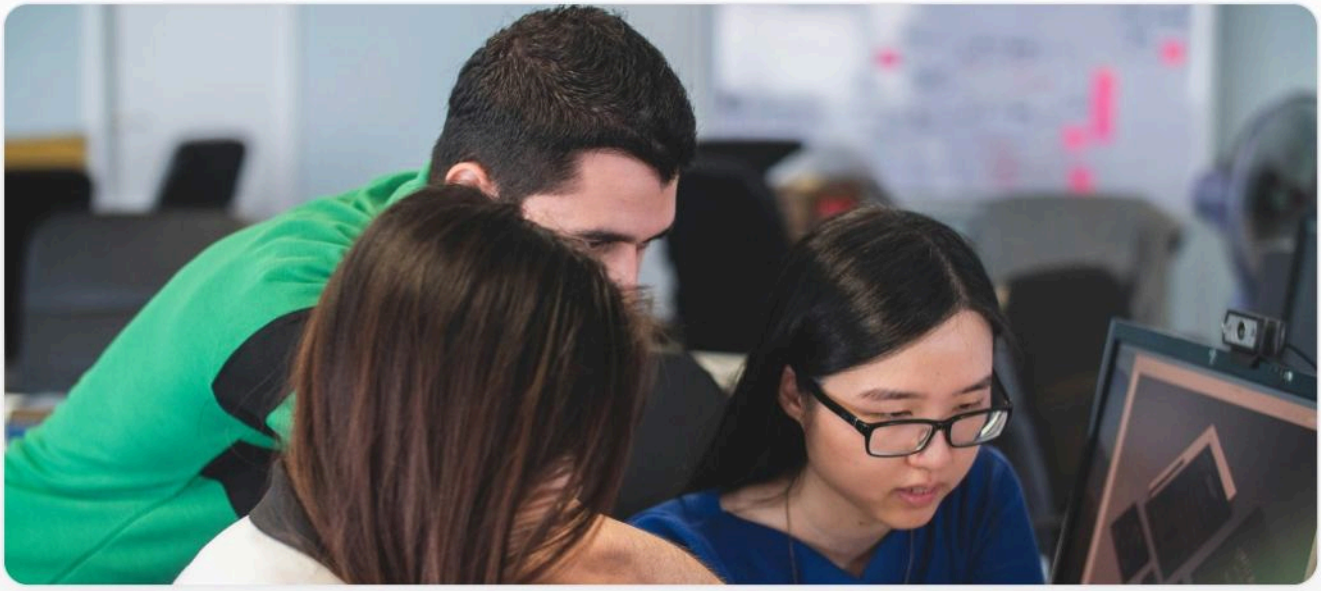
Über die Beschaffung können manipulierte Hardware oder mit Schadsoftware versehene Images und Updates zum Kunden gelangen. Das Systemhaus wird so ungewollt zum Überträger. Sichere Beschaffung, Prüfung von Lieferungen und Lieferantensteuerung (Annex A 5.19 bis 5.23, 8.30) begrenzen dieses Risiko.

4 · DATENABFLUSS ÜBER MANDANTEN

Systemhäuser verwalten Daten und Konfigurationen vieler Kunden nebeneinander. Eine schwache Mandantentrennung kann dazu führen, dass ein Vorfall bei einem Kunden auf andere übergreift oder Daten vermischt werden. Strikte Trennung und Zugriffskontrolle (Annex A 5.15, 8.3) sind hier entscheidend.

5 · RANSOMWARE IM EIGENEN HAUS

Auch IT-Profis werden Opfer von Phishing, und ein Ransomware-Vorfall im Systemhaus legt nicht nur den eigenen Betrieb, sondern auch die betreuten Kunden lahm. Awareness, Mehrfaktor-Anmeldung und getestete, getrennte Backups (Annex A 6.3, 8.5, 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. Das Systemhaus bestimmt internen und externen Kontext, die Erwartungen wichtiger Parteien wie Auftraggeber und Hersteller und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Der Scope sollte die Dienstleistungen abdecken, die Kunden prüfen, also insbesondere Managed Services, Fernwartung und Betrieb 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. Das Systemhaus legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken rund um Fernwartung, Kundenzugänge und Beschaffung 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.

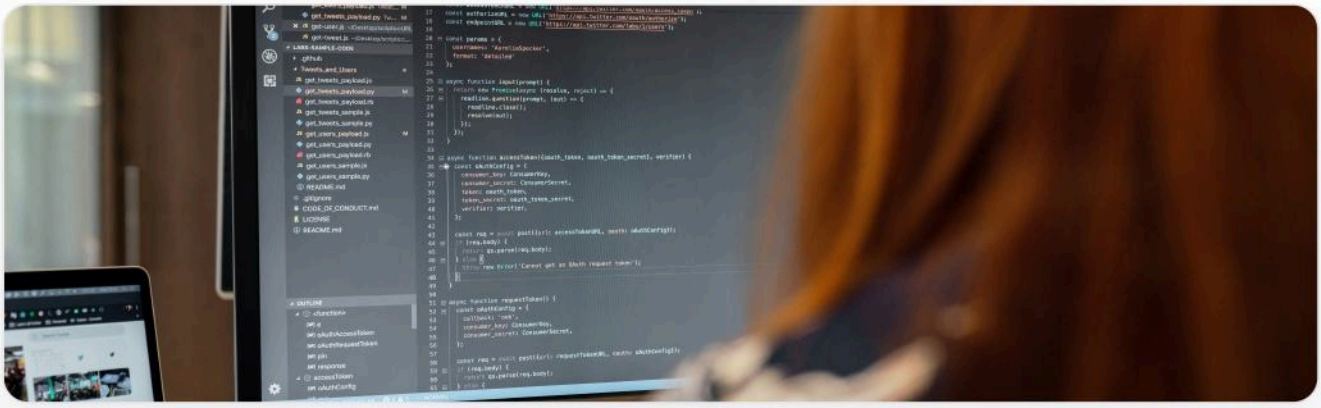
Privilegierte Zugänge, Mandantentrennung und Lieferkette stehen dabei fast immer oben auf der Liste.

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 Systemhaus stehen Zugriffs- und Privileged-Access-Management, sichere Beschaffung 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 Systemhäusern, 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 vergabefähig.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die Dienstleistungen schneiden, die Kunden und Vergabestellen prüfen: Managed Services, Fernwartung, Betrieb. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und hält den Aufwand niedrig.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. In technikgetriebenen Teams ist dieser Schritt schnell erledigt, wenn die Spitze dahintersteht.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von den Fernwartungswerkzeugen über die eigene Infrastruktur bis zur Beschaffung. Risiken bewerten, privilegierte Zugänge und Lieferkette besonders gewichten und die Erklärung zur Anwendbarkeit erstellen.

4 · MASSNAHMEN UMSETZEN

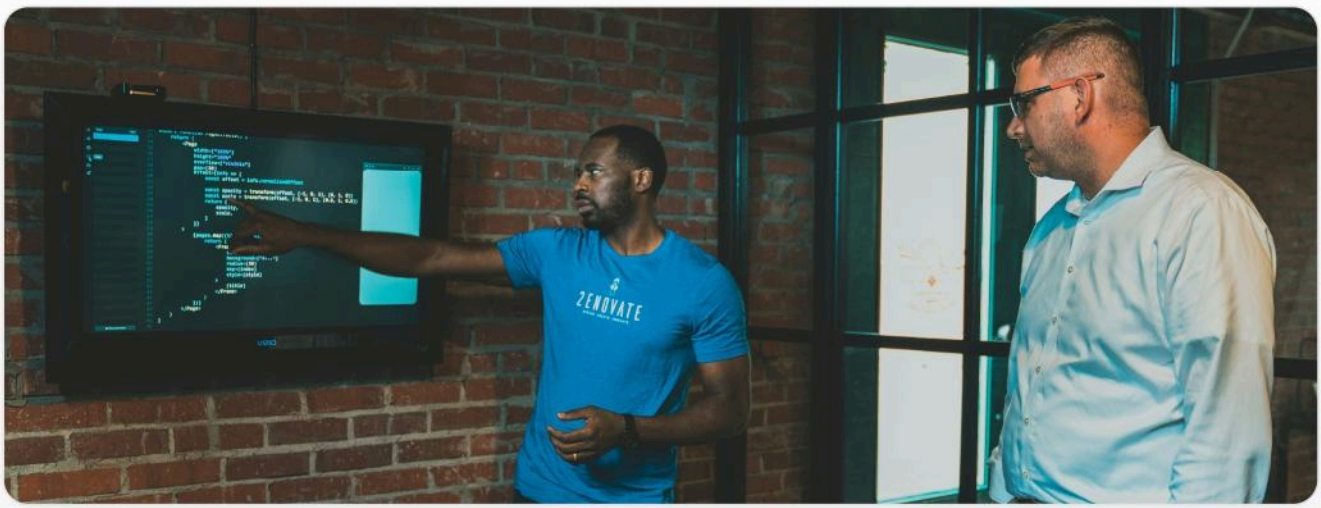
Die ausgewählten Annex-A-Maßnahmen einführen und vor allem dokumentieren. Die Technik ist oft da, der Nachweis fehlt. Privileged-Access-Management, Mandantentrennung, sichere Beschaffung und getrennte Backups zuerst.

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 für Vergabeprüfungen.

6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

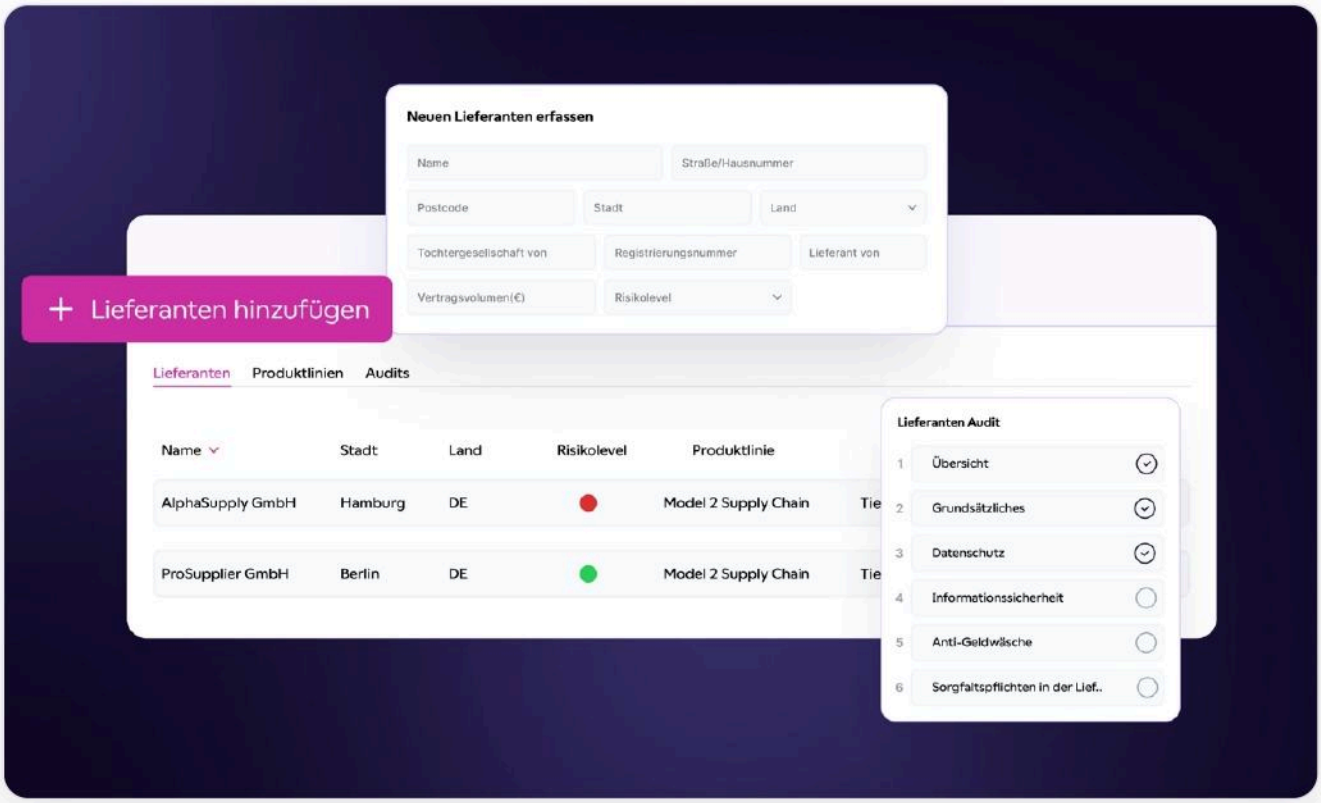
Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung (Stage 2). Danach folgt das Zertifikat, gültig für drei Jahre mit jährlichen Überwachungsaudits, und es öffnet die Tür zu öffentlichen Vergaben und höheren Partnerstufen.



WIE SECJUR ES EINFACH MACHT

Von der starken Technik zum *zertifizierten ISMS.*

Das Digital Compliance Office (DCO) führt IT-Systemhäuser 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. Unternehmen berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Zugänge & Fernwartung

Module für Privileged-Access, Mandantentrennung und die Härtung der Fernwartungswerkzeuge, genau die Punkte, die ein Systemhaus absichern muss.

Beschaffung & Lieferkette

Lieferantensteuerung und sichere Beschaffung für Hardware, Software und Distribution, dort, wo Annex A 5.19 bis 5.23 hinschaut.

Vergabe & Nachweise

Revisionssichere Dokumentation und ein voller Audit-Trail, mit dem öffentliche Vergaben und Hersteller-Partnerstufen erreichbar werden.

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, NIS2 und der BSI-Grundschutz weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, von Microsoft 365 bis zu den Fernwartungswerkzeugen, sodass das ISMS aktuell bleibt.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Systemhäuser, Managed-Service-Provider, IT-Dienstleister und digitale Anbieter erfüllen mit dem DCO ihre Sicherheitsanforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem Systemhausumfeld:

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

René Schlüß
Founder & Managing Director, reanmo

reanmo

REFERENZEN AUS IT-SYSTEMHÄUSERN UND MANAGED SERVICES

deepset · Masterplan.com · think-cell · WatchGuard · statista · ti 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 SYSTEMHÄUSER 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 im Kundengeschäft, das ISMS entsteht parallel.

Nachweise entstehen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass Betrieb, Projekte und Security an einer Quelle arbeiten statt an parallelen Tabellen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Systemhaus, das seine Zugänge im Griff hat, seine Beschaffung steuert und sich für öffentliche Aufträge qualifiziert. Genau das gewinnt Ausschreibungen und hält Kunden.

Weil dieselbe Struktur ISO 27001 und angrenzende Nachweise wie SOC 2 gemeinsam bedient, deckt ein Projekt mehrere Kundenanforderungen ab. Das senkt den Aufwand und hält das Systemhaus auch nach dem Audit jederzeit nachweisfähig.

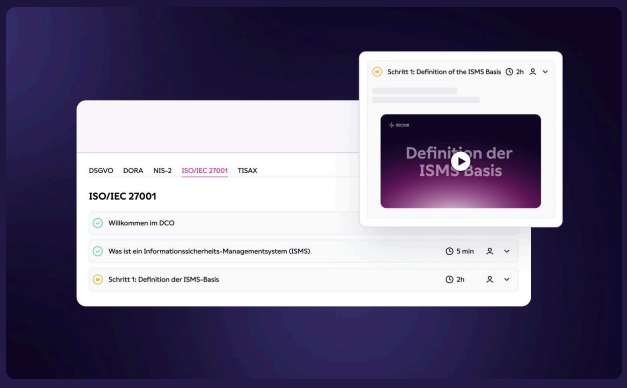
SECJUR

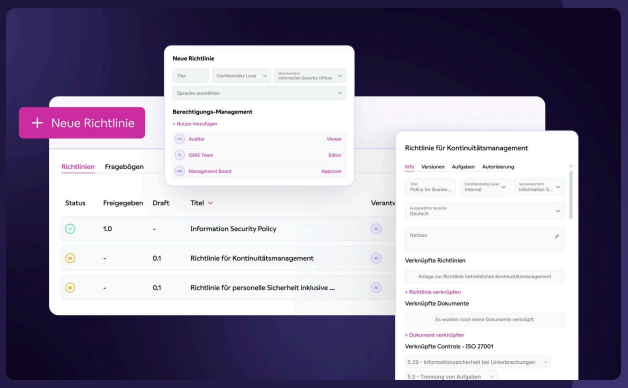
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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