SECJUR

WHITEPAPER
2026

ISO 27001 · GESUNDHEIT & VERSORGUNG

ISO 27001 im Gesundheitswesen: *Sicherheit schützt Patienten.*

Im Gesundheitswesen ist Informationssicherheit längst eine Frage der Patientensicherheit. Vernetzte Medizingeräte, digitale Patientenakten und die Telematikinfrastruktur verbinden alles miteinander, und ein Ransomware-Angriff kann eine Klinik in den Notbetrieb zwingen. Krankenhäuser sind kritische Infrastruktur, §75c SGB V verlangt den Stand der Technik, und NIS2 erfasst die Branche. Dieses Whitepaper zeigt, warum ISO 27001 das passende Fundament ist, wo die größten Schwachstellen liegen und wie ein ISMS entsteht, das den Betrieb nicht gefährdet.

ISO 27001 | NIS2 | KRITIS | B3S | DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Im Gesundheitswesen ist Sicherheit *Patientensicherheit.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Im Gesundheitswesen ist er mehr als freiwillig: §75c SGB V verpflichtet Krankenhäuser, angemessene Vorkehrungen nach dem Stand der Technik zu treffen, häufig nachgewiesen über den branchenspezifischen Sicherheitsstandard B3S oder ein ISMS nach ISO 27001. Für KRITIS-Häuser ist der regelmäßige Nachweis Pflicht.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der Verwaltung, klinische Systeme und vernetzte Medizintechnik gleichermaßen absichert, und der im Ernstfall den Betrieb aufrechterhält.

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 Pflichtenrahmen ist dicht. Neben §75c SGB V und dem B3S Krankenhaus erfasst NIS2 weite Teile des Gesundheitssektors und verlangt Risikomanagement, Meldepflichten und Lieferkettensicherheit. Die Leitung trägt die Verantwortung und haftet für die Umsetzung.

Zugleich ist die Bedrohungslage akut. Kliniken gehören zu den am häufigsten von Ransomware getroffenen Einrichtungen, weil der Druck zur schnellen Wiederherstellung dort am größten ist. Dieses Whitepaper ordnet die Pflichten ein, beschreibt die branchentypischen Risiken und zeigt einen realistischen Weg zur Zertifizierung.

WEN ES BETRIFFT

Mehrere Gruppen sind gefordert: Krankenhäuser über §75c SGB V und, ab den Schwellen, über KRITIS, große Einrichtungen und Dienstleister über NIS2, sowie MedTech-Hersteller, die Kliniken Sicherheit nachweisen müssen. Kommt eines davon in Frage, führt am ISMS kein Weg vorbei.

Die folgenden Seiten liefern die Grundlage: den Branchenkontext, die konkreten Risiken in IT und Medizintechnik, die Anforderungen der Norm und eine Roadmap, die im Klinikbetrieb funktioniert.

WELTWEIT ZERTIFIZIERT

70.000+

Organisationen sind nach ISO 27001 zertifiziert, mit klar steigender Tendenz.

FÜR KRANKENHÄUSER

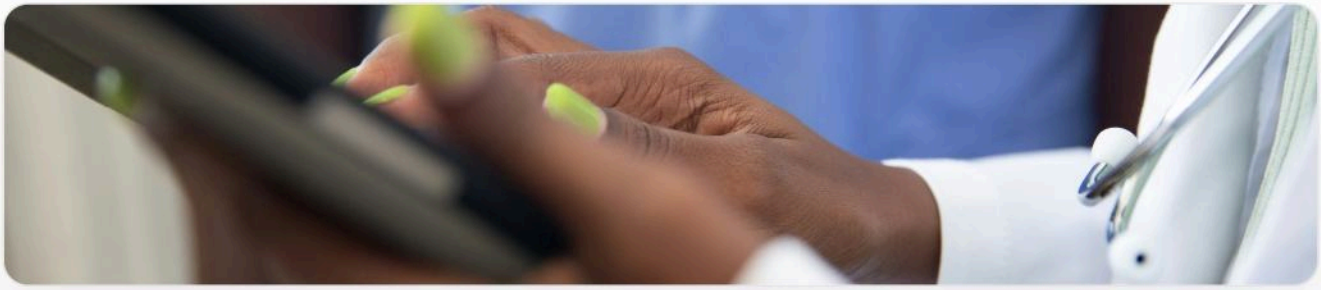
§75c

SGB V verlangt angemessene Vorkehrungen nach dem Stand der Technik (B3S / ISO 27001).

KONTROLLEN

93

Maßnahmen im Annex A, in vier Gruppen von organisatorisch bis technisch.



BRANCHENKONTEXT

Die Versorgung hängt *am Netz und an den Daten.*

Moderne Medizin ist digital. Patientenakten, Diagnostik, Medizingeräte und die Telematikinfrastruktur sind eng vernetzt, und ein Ausfall trifft unmittelbar die Versorgung. Genau deshalb ist das Gesundheitswesen reguliert wie kaum eine Branche und zugleich ein bevorzugtes Ziel. ISO 27001 macht die Sicherheit nachweisbar.

Fällt das Klinik-IT-System aus, geht es nicht um Daten, *sondern um Behandlung.*

EINE DURCHDIGITALISIERTE VERSORGUNG

Krankenhausinformationssysteme (KIS), elektronische Patientenakte, Labor- und Radiologiesysteme, vernetzte Medizingeräte und die Telematikinfrastruktur bilden eine durchgehende digitale Kette. Befunde, Medikation und Vitaldaten fließen in Echtzeit zwischen Stationen, Praxen und Diensten.

Diese Vernetzung verbessert die Versorgung und vergrößert die Angriffsfläche zugleich. Wo IT und Medizintechnik aufeinandertreffen, entstehen die kritischen Punkte, und sie betreffen nicht nur Daten, sondern den Behandlungsbetrieb selbst.

EIN DICHTER PFLICHTENRAHMEN

Das Gesundheitswesen ist mehrfach reguliert. §75c SGB V verlangt von Krankenhäusern Vorkehrungen nach dem Stand der Technik, üblicherweise über den B3S Krankenhaus oder ein ISMS nachgewiesen. Häuser ab den KRITIS-Schwellen müssen regelmäßig Nachweise erbringen, und NIS2 erweitert den Kreis der erfassten Einrichtungen deutlich.

Hinzu kommt der Datenschutz: Gesundheitsdaten sind nach Art. 9 DSGVO eine besondere Kategorie mit erhöhten Anforderungen. Ein ISMS bündelt diese Pflichten in einem System, statt sie einzeln zu verwalten.

KLINIKEN IM VISIER

Krankenhäuser zählen zu den häufigsten Ransomware-Zielen. Angreifer wissen, dass eine Klinik nicht tagelang stillstehen kann, und erhöhen so den Druck zur Zahlung. Mehrere Häuser mussten nach Angriffen Operationen verschieben und sich von der Notfallversorgung abmelden.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als Daten: um Behandlungsfähigkeit, Patientensicherheit und Menschenleben. Ein Ausfall der Systeme kann Diagnosen verzögern und Eingriffe gefährden. Sicherheit ist hier unmittelbar Teil der Versorgungsqualität.

HERAUSFORDERUNGEN

Warum ISO 27001 im Gesundheitswesen *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Branche. Der Aufwand ist es nicht. Fünf Eigenheiten des Gesundheitswesens machen die Umsetzung anspruchsvoller als anderswo, und für jede gibt es einen pragmatischen Umgang.

VERNETZTE MEDIZINGERÄTE

Vom Beatmungsgerät bis zum MRT sind Medizingeräte heute vernetzt, haben aber lange Lebenszyklen und laufen oft auf veralteten Betriebssystemen. Hersteller schränken Updates ein, und ein Gerät lässt sich nicht im laufenden Betrieb neu starten.

Die Risikoanalyse muss diese Geräte einbeziehen, ohne ihre Verfügbarkeit zu gefährden. Kompensierende Maßnahmen wie Netzsegmentierung und strenge Zugänge (Annex A 8.20 bis 8.23) schützen, wo ein Patch nicht möglich ist.

VERFÜGBARKEIT RETTET LEBEN

In der Büro-IT steht oft Vertraulichkeit zuerst. In der Klinik ist Verfügbarkeit überlebenswichtig, denn Systeme müssen rund um die Uhr laufen. Eine Sicherheitsmaßnahme, die ein klinisches System destabilisiert, ist keine Option.

Maßnahmen müssen deshalb schützen, ohne den Betrieb zu stören. Wiederanlaufpläne, Redundanzen und ein geübter Notbetrieb (Annex A 5.29, 5.30, 8.13) sind hier besonders wichtig.

HÖCHSTES SCHUTZNIVEAU FÜR DATEN

Gesundheitsdaten sind nach Art. 9 DSGVO besonders geschützt. Ein Abfluss ist nicht nur ein Vertrauensbruch, sondern kann hohe Bußgelder und Erpressung nach sich ziehen. Verschlüsselung, strenge Zugriffskontrolle und Protokollierung (Annex A 8.24, 8.2 bis 8.5) sind hier nicht optional.

SCHICHTBETRIEB UND FLUKTUATION

Kliniken arbeiten im Schichtbetrieb mit vielen Beschäftigten, Wechseldiensten und externem Personal. Zugänge müssen schnell vergeben und ebenso schnell wieder entzogen werden. Sauberes On- und Offboarding und rollenbasierte Rechte (Annex A 5.15, 5.18, 6.5) sind eine Daueraufgabe.

BUDGET- UND PERSONALDRUCK

Das Gesundheitswesen arbeitet unter Kosten- und Personaldruck, eigene Sicherheitsfunktionen sind selten üppig besetzt. Die Norm verlangt aber Struktur und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die führen und dokumentieren, machen hier den Unterschied.

BEDROHUNGSLAGE & RISIKEN

Wo das Gesundheitswesen *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an vernetzter Medizintechnik, an höchst sensiblen Daten und an einer Versorgung, die keinen Stillstand verträgt. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE ZWINGT IN DEN NOTBETRIEB

Der gefährlichste Ernstfall. Werden KIS und klinische Systeme verschlüsselt, fällt die Einrichtung auf Stift und Papier zurück, Operationen werden verschoben und die Notaufnahme meldet sich ab. Hier geht es unmittelbar um Patientensicherheit. Getestete Backups, Segmentierung und ein eingeübter Notfallplan (Annex A 8.13, 5.29, 8.20 bis 8.23) entscheiden, wie schnell der Betrieb zurückkehrt.

2 · KOMPROMITTIERTE MEDIZINGERÄTE

Vernetzte, schlecht gepatchte Geräte sind ein Einfallstor und im schlimmsten Fall selbst manipulierbar. Ein verändertes Gerät oder ein über das Medizingerätenetz verbreiteter Angriff gefährdet Diagnose und Therapie. Strikte Trennung der Gerätenetze und überwachte Zugänge (Annex A 8.20 bis 8.23) sind hier zentral.

3 · DIEBSTAHL VON PATIENTENDATEN

Gesundheitsdaten sind auf dem Schwarzmarkt besonders wertvoll und für Erpressung geeignet. Ein Abfluss von Diagnosen, Befunden und Stammdaten ist ein schwerer DSGVO-Vorfall nach Art. 9 mit hohem Bußgeldrisiko. Verschlüsselung und strenge Zugriffskontrolle (Annex A 8.24, 8.2 bis 8.5) schützen diesen Datenschatz.

4 · ANGRIFFE ÜBER DIE LIEFERKETTE

Gerätehersteller, Wartungsdienste und IT-Dienstleister mit Fernzugängen sind ein beliebter Umweg ins Kliniknetz. Ein kompromittierter Partner oder ein manipuliertes Update wird zum Einfallstor. Lieferantensteuerung und abgesicherte Fernwartung (Annex A 5.19 bis 5.23) begrenzen dieses Risiko.

5 · INSIDER UND OFFENE ZUGÄNGE

Im Schichtbetrieb mit hoher Fluktuation bleiben Zugänge ausscheidender oder externer Kräfte leicht offen, Rechte häufen sich an. Ein vergessenes Konto wird zum Risiko. Rollenbasierte Rechte, sauberes Offboarding und Protokollierung (Annex A 5.15, 5.18, 8.15) schließen diese Lücke.

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. Die Einrichtung bestimmt internen und externen Kontext, die Erwartungen wichtiger Parteien wie Patienten, Kostenträger und Aufsicht und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Im Gesundheitswesen ist der Zuschnitt entscheidend. Der Scope sollte die versorgungskritischen Systeme abdecken, von KIS bis zur vernetzten Medizintechnik. 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 unter Budgetdruck ist der sichtbare Rückhalt der Leitung entscheidend.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Die Einrichtung legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet ihre Risiken von der Verwaltung bis zur Medizintechnik 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.

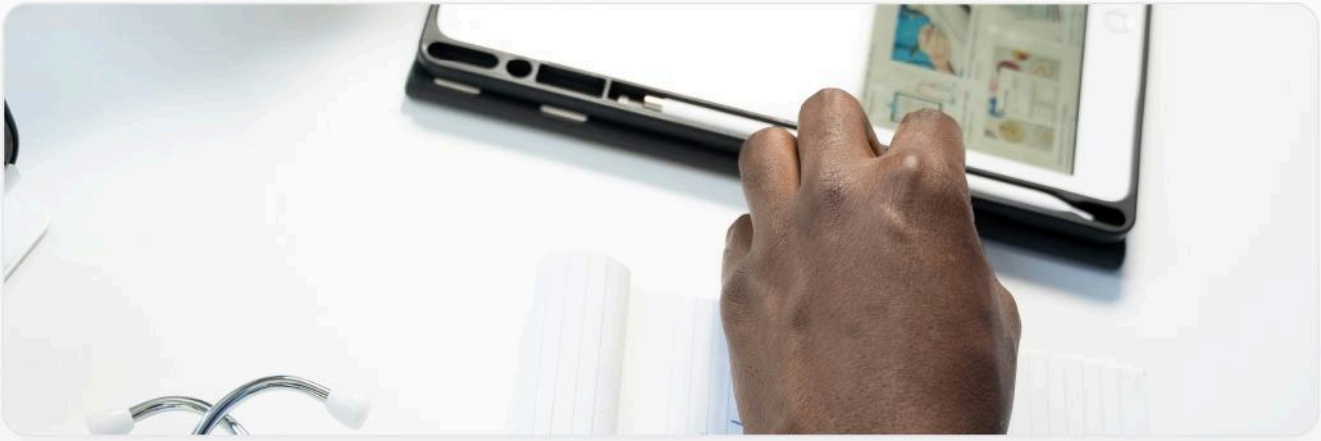
Verfügbarkeit, Schutz von Gesundheitsdaten und Medizingerätesicherheit stehen dabei fast immer oben auf der Liste.

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 Gesundheitswesen stehen Business Continuity, Netzsegmentierung, Zugriffskontrolle 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). Diese Schleife deckt sich mit den wiederkehrenden Nachweisen, die KRITIS und §75c SGB V verlangen.



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 und Gerätelandschaft sechs bis zwölf Monate bis zum Audit.

Ein ISMS nach ISO 27001 erfüllt §75c SGB V und einen Großteil von NIS2 zugleich. *Ein Aufbau, mehrere Pflichten.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope auf die versorgungskritischen Bereiche schneiden: KIS, klinische Systeme, Medizintechniknetze und zugehörige IT. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und für die Nachweise gegenüber der Aufsicht.

2 · FÜHRUNG UND LEITLINIE

Die Geschäftsführung verabschiedet die Sicherheitsleitlinie, benennt eine verantwortliche Person und stellt Ressourcen bereit. Der sichtbare Rückhalt der Leitung ist gerade im Klinikbetrieb entscheidend.

3 · RISIKEN IN IT UND MEDIZINTECHNIK ANALYSIEREN

Assets erfassen, von der Verwaltung über KIS bis zu den vernetzten Geräten. Risiken gemeinsam für IT und Medizintechnik bewerten, Verfügbarkeit und Datenschutz besonders gewichten und die Erklärung zur Anwendbarkeit erstellen.

4 · MASSNAHMEN UMSETZEN

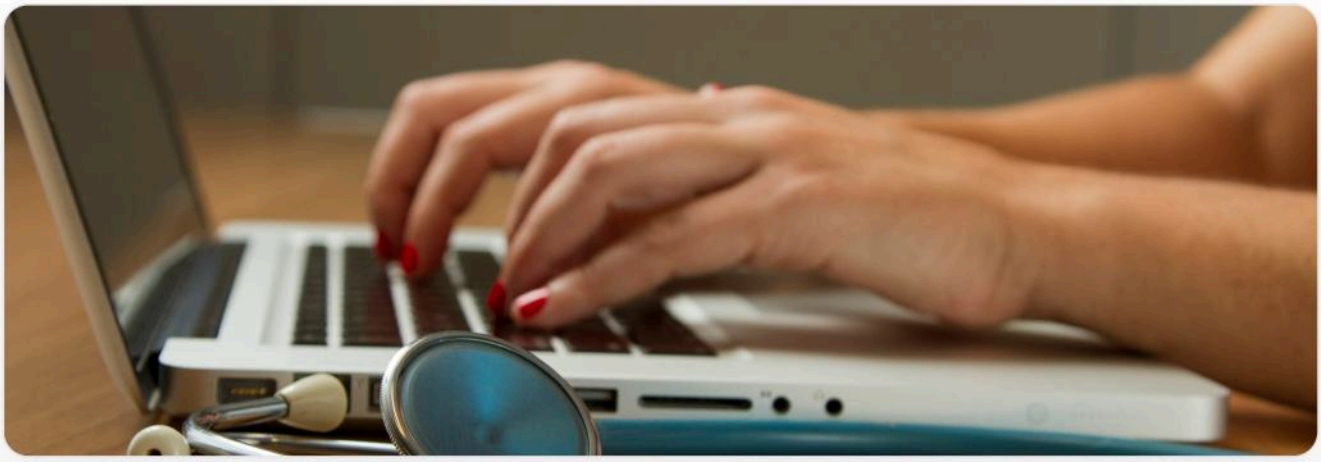
Die ausgewählten Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Netzsegmentierung der Gerätenetze, Backup, Zugriffskontrolle und abgesicherte Fernwartung. Jede Maßnahme so festhalten, dass sie im Audit und vor der Aufsicht Bestand hat.

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

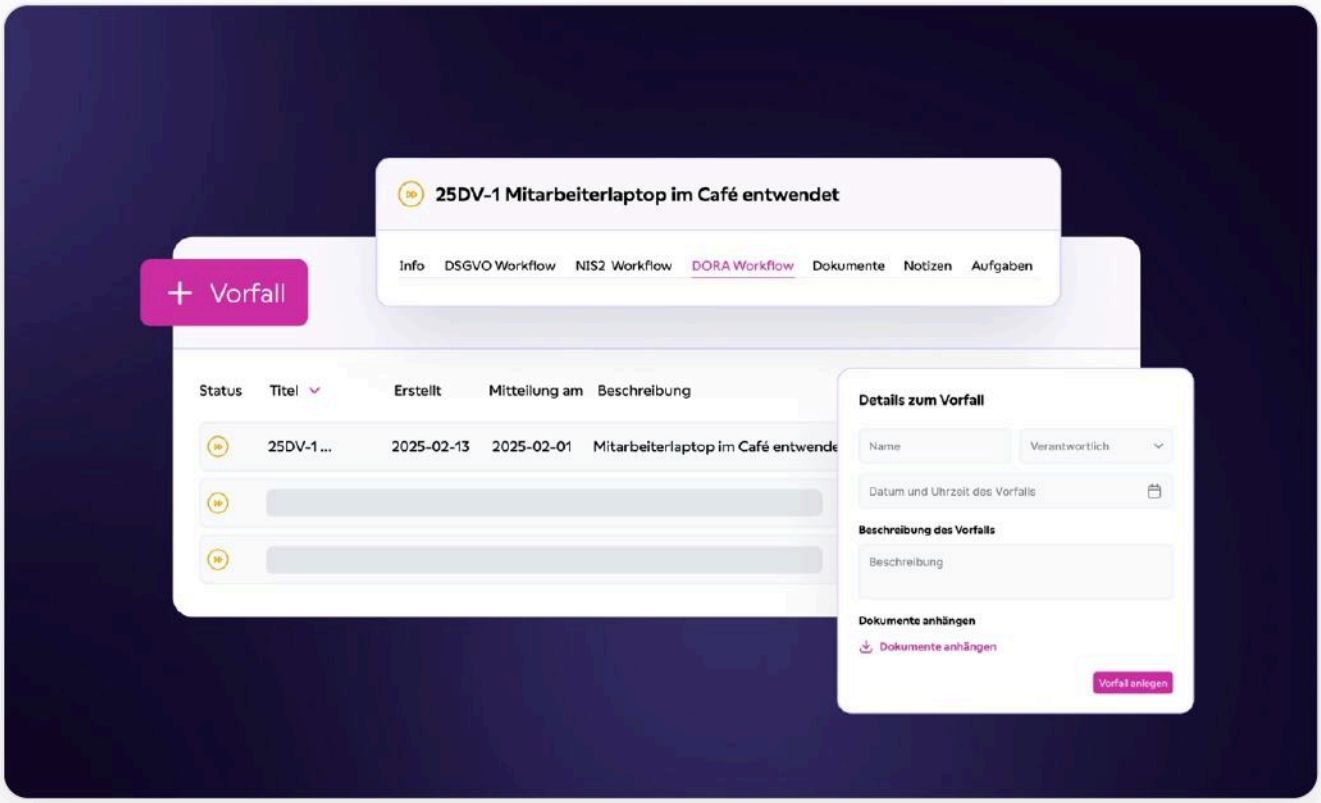
Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung (Stage 2). Danach folgt das Zertifikat, gültig für drei Jahre mit jährlichen Überwachungsaudits, und es stützt zugleich die Nachweise nach §75c SGB V und KRITIS.



WIE SECJUR ES EINFACH MACHT

Von der Pflicht zur *auditbereiten Umsetzung.*

Das Digital Compliance Office (DCO) führt Gesundheitseinrichtungen durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse über IT und Medizintechnik, 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. Einrichtungen berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Risiko & Resilienz

Geführte Risikoanalyse über IT und Medizintechnik und ein strukturierter Umgang mit Vorfällen und Wiederanlauf, damit der Betrieb auch im Ernstfall trägt.

Lieferanten & Fernwartung

Lieferantensteuerung und Nachweise für Gerätehersteller und Wartungsdienste, genau dort, wo Fernzugänge und Annex A 5.19 bis 5.23 hinschauen.

Audit & Aufsicht

Revisionssichere Dokumentation und ein voller Audit-Trail, mit dem Zertifizierungsaudit und die Nachweise nach §75c SGB V und KRITIS gelingen.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist strukturiert. 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, ohne dass der Versorgungsbetrieb gefährdet wird.

EIN AUFBAU, MEHRERE PFLICHTEN

Weil sich §75c SGB V, ISO 27001 und NIS2 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegen muss.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Kliniken, Gesundheitsdienstleister, MedTech-Unternehmen und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem Gesundheitswesen:

Erfolgreicher ISMS-Aufbau *für den MD Nordrhein.*

Der Medizinische Dienst Nordrhein hat früh erkannt, dass Informationssicherheit ein zentrales Zukunftsthema ist, nicht nur wegen NIS2, sondern auch, um das Unternehmen langfristig sicher aufzustellen. Deshalb fiel die Entscheidung auf SECJUR, um ein ISMS nach ISO 27001 für das gesamte Unternehmen aufzubauen.

Mit 1.500 Mitarbeitenden an acht Standorten setzt der Medizinische Dienst Nordrhein gemeinsam mit SECJUR auf eine automatisierte, praxisnahe Lösung, die durch unsere Experten eng begleitet wird.

So wird der MD Nordrhein nicht nur erfolgreich nach ISO 27001 zertifiziert, sondern zugleich optimal auf die NIS2-Verpflichtungen vorbereitet, ein Beispiel für effiziente und nachhaltige Informationssicherheit im Gesundheitswesen.

Medizinischer Dienst Nordrhein

REFERENZEN AUS GESUNDHEIT, PFLEGE UND MEDTECH

VIDEOCLINIC · St. Bernhard Hospital · HOMECARE die Altenpflege · Medizinischer Dienst Nordrhein · AllDent Zahnzentrum · URSAPHARM

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 GESUNDHEITSEINRICHTUNGEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und der Branchentiefe. Statt monatelanger Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen, die IT und Medizintechnik gemeinsam denken. Das Team bleibt bei der Versorgung, das ISMS entsteht parallel.

Weil dieselbe Struktur auch §75c SGB V und die NIS2-Pflichten bedient, deckt ein Projekt mehrere Anforderungen gleichzeitig ab. Das senkt den Aufwand und macht den Fortschritt jederzeit sichtbar, für die Leitung wie für die Aufsicht.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat und der Nachweis nach §75c SGB V, sondern eine Einrichtung, die ihre Risiken kennt und im Ernstfall handlungsfähig bleibt. Genau das schützt die Versorgung und die Patienten.

Und weil das DCO die Nachweise laufend aktuell hält, bleibt die Einrichtung auch nach dem Audit auskunftsfähig, gegenüber Aufsicht, Partnern und der eigenen Geschäftsführung. Informationssicherheit wird damit zur Routine statt zum Projekt.

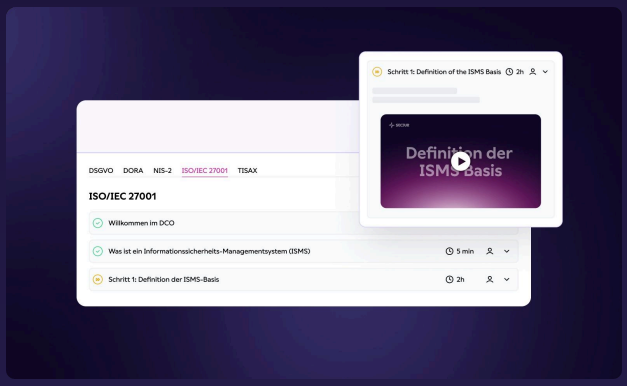
SECJUR

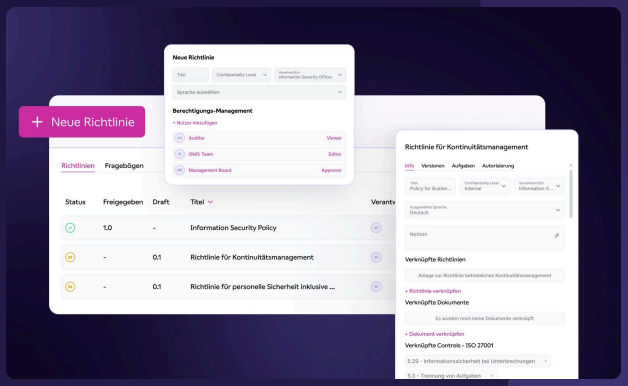
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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 automatisierten Compliance

"Als Einrichtung im Gesundheitswesen mussten wir NIS2 verlässlich und prüfungssicher umsetzen. Mit SECJUR haben wir Risikoanalyse, Dokumentation und Behördennachweise zentral abgebildet, ohne unser Tagesgeschäft auszubremsen."

Anonym

Leitung IT-Sicherheit, Gesundheitswesen

VIDEOCLINIC GSK EvoCare. St. Bernhard HOSPITAL HOMECARE die Alltagshelfer viluavitartis

www.secjur.com