SECJUR

WHITEPAPER
2026

ISO 27001 · LEBENSMITTEL & ERNÄHRUNG

ISO 27001 für Lebensmittel: *Sicherheit bis ins Regal.*

Die Lebensmittelbranche ist hochautomatisiert und eng mit dem Handel verzahnt. Genau das macht sie verwundbar: Ein IT-Ausfall stoppt die Produktion, und verderbliche Ware wartet nicht. Der Lebensmitteleinzelhandel verlangt von seinen Lieferanten zunehmend nachweisbare Sicherheit, und NIS2 erfasst die Branche ab bestimmten Schwellen. Dieses Whitepaper zeigt, warum ISO 27001 für Hersteller und Verarbeiter sinnvoll ist, wo die größten Schwachstellen liegen und wie ein ISMS entsteht, das zur Branche passt.

ISO 27001 · NIS2 · IFS · ISO 9001 · DSGVO

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

In der Lebensmittelbranche schützt Sicherheit *die Lieferfähigkeit.*

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits-Managementsysteme (ISMS). Anders als NIS2 ist er freiwillig. Für Lebensmittelhersteller ist er der Nachweis, dass Produktion, Rezepturen und die Daten der Handelspartner geschützt sind. In Lieferantenprüfungen des Einzelhandels wird dieser Nachweis zunehmend verlangt, ähnlich wie es IFS und BRC für die Lebensmittelsicherheit längst tun.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der IT und Produktionstechnik gleichermaßen absichert. Die aus IFS und BRC bekannte Audit-Kultur ist dabei ein echter Vorsprung.

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 zwei Seiten. Der Lebensmitteleinzelhandel gibt seine Sicherheitsanforderungen über die Lieferkette weiter und verlangt den Nachweis vertraglich. Zugleich erfasst NIS2 die Produktion, Verarbeitung und den Vertrieb von Lebensmitteln ab bestimmten Schwellen, und ein ISO-27001-ISMS deckt einen Großteil dieser Pflichten mit ab.

Hinzu kommt die Bedrohungslage. Ransomware zählt zu den größten Risiken für die Wirtschaft, und in der Lebensmittelproduktion wird ein Stillstand sofort teuer, weil verderbliche Ware und enge Lieferfenster keinen Aufschub dulden. 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: Der Handel schickt Sicherheitsfragebögen oder fordert das Zertifikat, Sie fallen unter NIS2, oder Sie wollen Rezepturen und Rückverfolgbarkeitsdaten verlässlich schützen. Trifft eines zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Der Standard ist verhältnismäßig und knüpft an bekannte Audit-Strukturen an. 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.

BRANCHENKONTEXT

Die Lebensmittelbranche läuft *auf Termin und Vertrauen.*

Vom Wareneingang bis ins Regal ist die Lebensmittelproduktion ein eng getakteter, digital gesteuerter Prozess. Verderbliche Ware und feste Lieferfenster lassen keinen Stillstand zu, und der Handel verlangt von seinen Lieferanten nachweisbare Sicherheit. ISO 27001 macht diese Sicherheit prüfbar.

Verderbliche Ware kennt keine Geduld. *Steht die Produktion, ist die Charge verloren.*

AUTOMATISIERT VON DER LINIE BIS ZUM ERP

Moderne Lebensmittelbetriebe steuern ihre Produktion über vernetzte Systeme: ERP und Warenwirtschaft, Manufacturing-Execution-Systeme (MES), Abfüll- und Verpackungsanlagen, Kühl- und Lagertechnik sowie die elektronische Anbindung an den Handel über EDI. Rückverfolgbarkeit verlangt zudem lückenlose Daten von der Charge bis zur Auslieferung.

Diese durchgehende Digitalisierung schafft Effizienz und Angriffsfläche zugleich. Wo IT und Produktionstechnik zusammentreffen, entstehen die kritischen Punkte.

DER HANDEL GIBT DEN TAKT VOR

Der Lebensmitteleinzelhandel ist mächtig und anspruchsvoll. Wer als Lieferant gelistet bleiben will, muss liefern, was der Handel fordert, und das umfasst zunehmend Informationssicherheit. Sicherheitsfragebögen und Lieferantenprüfungen sind aus dem Qualitätsbereich längst bekannt und greifen nun auch auf die IT über.

ISO 27001 beantwortet einen Großteil dieser Anforderungen mit einem einzigen Dokument. Statt jeden Fragebogen einzeln zu bearbeiten, legt der Hersteller den anerkannten Nachweis vor und bleibt verlässlicher Partner.

DIE NIS2-VERBINDUNG

NIS2 erfasst die Produktion, Verarbeitung und den Vertrieb von Lebensmitteln ab bestimmten Schwellen. Wer ein ISMS nach ISO 27001 betreibt, erfüllt damit einen Großteil der NIS2-Pflichten, etwa Risikomanagement, Lieferkettensicherheit und Notfallvorsorge. Ein Aufbau, zwei Ergebnisse.

WAS AUF DEM SPIEL STEHT

Es geht um mehr als IT: verlorene Chargen, gerissene Liefertermine, Vertragsstrafen und ausgelistete Produkte. Hinzu kommen wertvolle Rezepturen und die Integrität der Rückverfolgbarkeit, die für die Lebensmittelsicherheit unverzichtbar ist. Sicherheit schützt hier das Kerngeschäft.

HERAUSFORDERUNGEN

Warum ISO 27001 in der Lebensmittelbranche *besonders fordert.*

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

ZEITKRITIKALITÄT UND VERDERBLICHE WARE

Anders als in vielen Industrien lässt sich ein Produktionsstopp nicht einfach nachholen. Steht die Linie, verdirbt Ware, Kühlketten reißen, und feste Lieferfenster des Handels platzen. Der Druck zur schnellen Wiederherstellung ist enorm.

Für das ISMS heißt das: kurze Wiederanlaufzeiten, getestete Backups und ein belastbarer Notfallplan (Annex A 8.13, 5.29, 5.30). Genau diese Vorsorge verlangt die Norm.

IT TRIFFT PRODUKTIONSTECHNIK

Neben klassischer IT steuern operative Systeme den Betrieb: MES, Abfüllanlagen, Kühl- und Fördertechnik. Vieles ist über Jahre gewachsen, läuft auf älteren Ständen und darf im Betrieb nicht einfach unterbrochen werden.

Diese Übergänge zwischen Produktionstechnik und IT verdienen in der Risikoanalyse nach Kap. 6 besondere Aufmerksamkeit. Kompensierende Maßnahmen wie Netzsegmentierung schützen, wo ein Update nicht möglich ist.

DÜNNE MARGEN, HOHE VOLUMINA

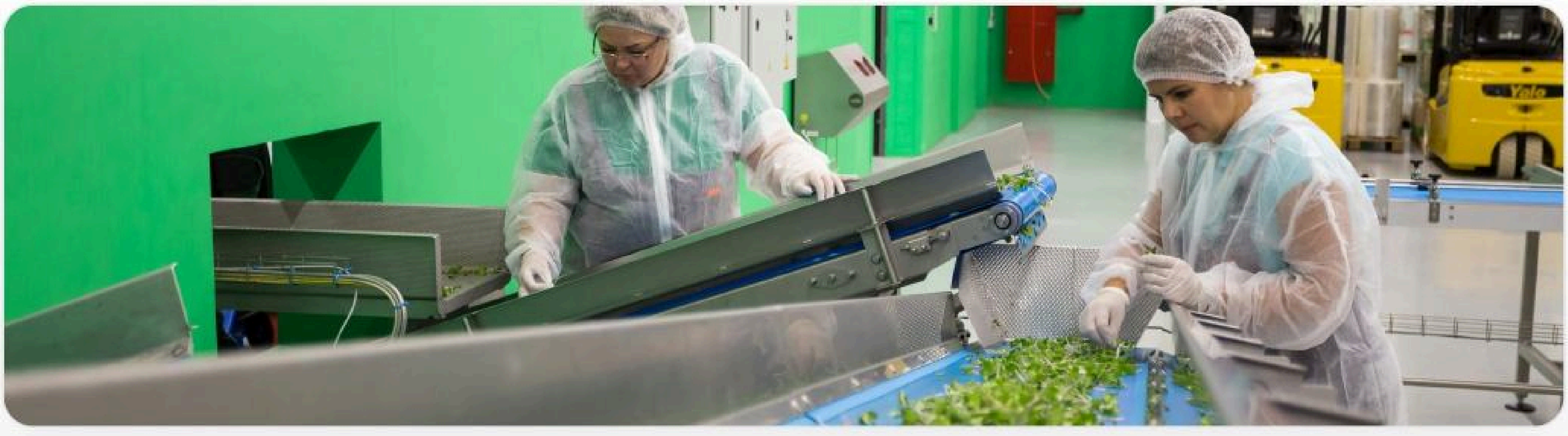
Die Branche arbeitet mit knappen Margen und großen Mengen. Budget für Sicherheit ist selten üppig. Hier hilft das Prinzip der Verhältnismäßigkeit: Maßnahmen richten sich nach Größe und Risiko, nicht nach Konzernmaßstab. So bleibt die Investition überschaubar und der Nutzen, vermiedene Ausfälle und gehaltene Listungen, messbar.

AUDIT-KULTUR ALS VORSPRUNG

Anders als viele Branchen kennt die Lebensmittelproduktion strenge Audits längst, etwa nach IFS oder BRC. Dokumentation, Rückverfolgbarkeit und Korrekturmaßnahmen sind vertraut. Diese Kultur lässt sich auf das ISMS übertragen und verkürzt den Weg zur Zertifizierung spürbar.

DÜNNE IT-DECKE

Viele Hersteller 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 führen und dokumentieren, machen hier den Unterschied.



BEDROHUNGSLAGE & RISIKEN

Wo die Lebensmittelbranche *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an einer eng getakteten, automatisierten Produktion, an wertvollen Rezepturen und an der engen Anbindung an den Handel. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE STOPPT DIE PRODUKTION

Der häufigste und teuerste Ernstfall. Werden ERP, MES oder Steuerungssysteme verschlüsselt, steht die Linie. Verderbliche Ware verdirbt, Kühlketten sind gefährdet, und feste Lieferfenster des Handels reißen. Getestete Backups und ein eingeübter Notfallplan (Annex A 8.13, 5.29) entscheiden, ob der Stillstand Stunden oder Tage dauert, und damit über den Schaden.

2 · ANGRIFFE ÜBER DIE LIEFERKETTE

Angreifer nutzen den schwächsten Partner als Tür. Ein kompromittierter Zulieferer, Logistiker 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. Der Handel fordert denselben Nachweis zunehmend auch vom Hersteller selbst ein.

3 · MANIPULATION DER PRODUKTIONSTECHNIK

Werden MES, Rezeptursteuerung oder Kühltechnik manipuliert, drohen nicht nur Ausfälle, sondern im Extremfall Risiken für die Lebensmittelsicherheit, etwa durch veränderte Mischungsverhältnisse oder unterbrochene Kühlung. Trennung von IT und OT sowie strenge Zugänge (Annex A 8.20 bis 8.23) sind hier zentral.

4 · DIEBSTAHL VON REZEPTUREN UND DATEN

Rezepturen, Verfahren und Konditionen mit dem Handel sind das Kapital vieler Hersteller. Werden sie abgegriffen, ist der Wettbewerbsvorsprung dahin. Verschlüsselung und strenge Zugriffskontrolle (Annex A 8.24, 8.2 bis 8.5) schützen dieses Wissen vor Abfluss und Wettbewerb.

5 · INTEGRITÄT DER RÜCKVERFOLGBARKEIT

Rückverfolgbarkeit ist gesetzlich gefordert und für Rückrufe überlebenswichtig. Werden Chargen- und Herkunftsdaten verfälscht oder gelöscht, ist im Ernstfall kein sauberer Rückruf möglich. Schutz der Datenintegrität, Protokollierung und Backups (Annex A 8.10 bis 8.13) sichern diese Nachweiskette.

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 Handel und Aufsicht und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

In der Lebensmittelbranche ist der Zuschnitt entscheidend. Ein klarer Scope, etwa Produktion samt zugehöriger IT und Anbindung an den Handel, 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). Aus dem Qualitätsmanagement ist diese Verantwortung der Leitung vielen Betrieben bereits vertraut.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Das Unternehmen legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet seine Risiken von der IT bis zur Produktionstechnik 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, OT-Sicherheit 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. In der Lebensmittelproduktion stehen Business Continuity, Zugriffskontrolle, physische Sicherheit 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 ist aus IFS und BRC bereits vertraut und lässt sich direkt übertragen.

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 aus dem Qualitätsmanagement, statt bei null zu beginnen. Realistisch sind je nach Reife drei bis sechs Monate bis zum Audit.

Wer IFS und BRC kennt, kennt die Audit-Logik. *ISO 27001 baut darauf auf.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope eng schneiden: welcher Standort, welche Produktion, welche Systeme. 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. Wo bereits ein Qualitätsmanagement besteht, lässt sich daran gut anknüpfen.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von ERP und MES über Kühl- und Abfülltechnik bis zur Anbindung an den Handel. Risiken bewerten, Verfügbarkeit und Datenintegrität besonders gewichten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten Hebeln beginnen: Backup, Zugriffskontrolle, Netztrennung von Produktion und IT sowie 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. Für Betriebe mit IFS- oder BRC-Erfahrung ist dieser Schritt vertrautes Terrain.

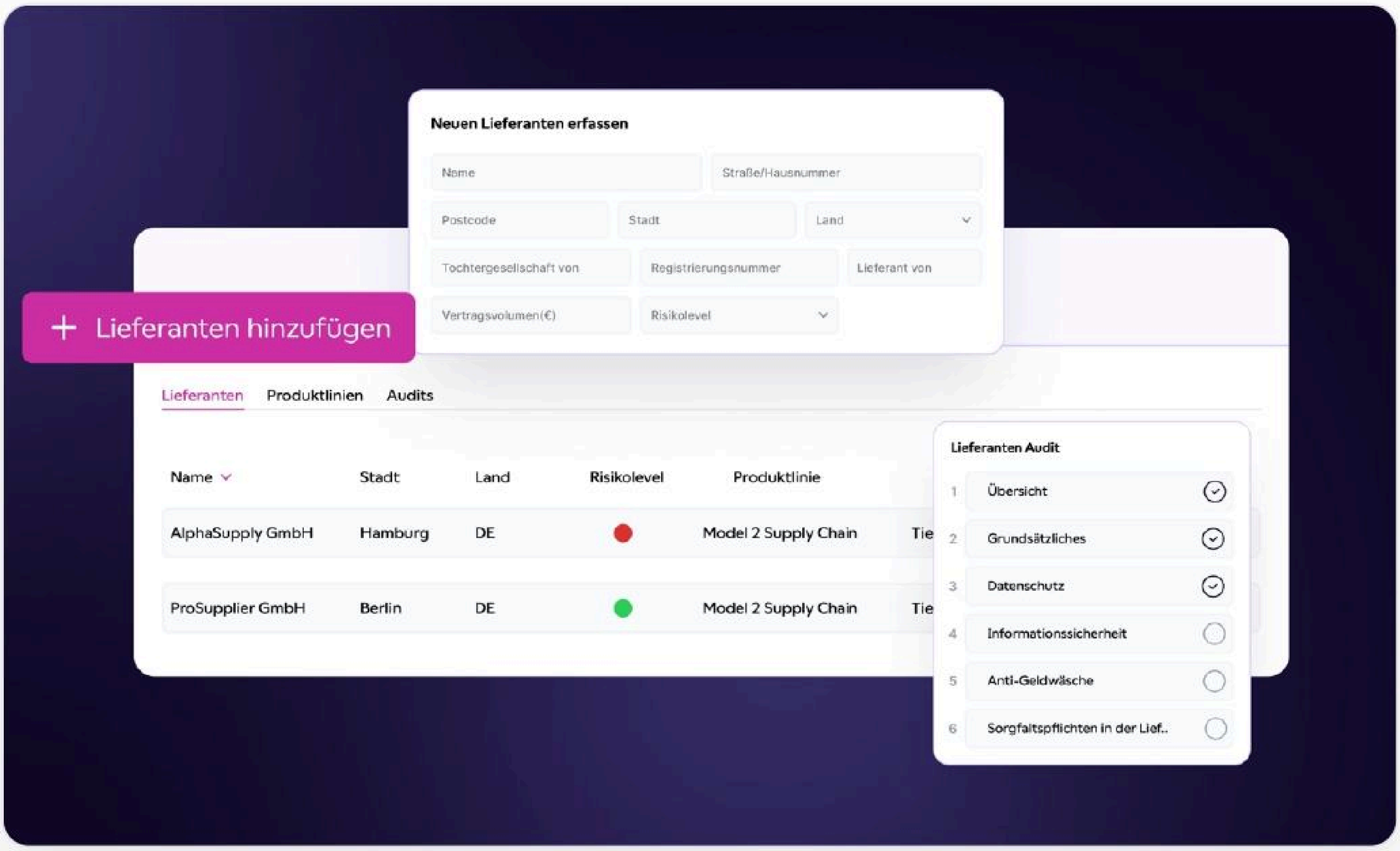
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

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.

WIE SECJUR ES EINFACH MACHT

Vom Kunden- und Gesetzesdruck zur *auditbereiten Umsetzung.*

Das Digital Compliance Office (DCO) führt Lebensmittelbetriebe durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse über IT und Produktion, 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 & Produktion

Geführte Risikoanalyse, die Verwaltung und Produktionstechnik gemeinsam betrachtet und jede Maßnahme nachvollziehbar begründet und priorisiert.

Lieferanten & Handel

Lieferantenbewertung und revisionssichere Nachweise, genau dort, wo der Einzelhandel 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, sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegen muss.

VERTRAUEN & ERGEBNISSE

Über 500 Unternehmen *arbeiten mit SECJUR.*

Lebensmittelhersteller, Industrieunternehmen, Logistiker und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus der Lebensmittelbranche:

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

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

REFERENZEN AUS LEBENSMITTEL, INDUSTRIE UND HANDEL

PETER KÖLLN · Trolli · Nordzucker · yfood · demeter · STERNWYWIOL Gruppe

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 LEBENSMITTELBETRIEBE SECJUR WÄHLEN

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 an der Produktion, 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 ERP, MES und Co., sodass das ISMS aktuell bleibt, ohne dass jemand Tabellen pflegt.

Weil derselbe Unterbau ISO 27001, NIS2 und die Erwartungen aus IFS und BRC zugleich trägt, zahlt eine bekannte Audit-Kultur direkt auf die Zertifizierung ein, statt getrennt abgearbeitet zu werden.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern ein Betrieb, der seine Produktion absichert, seine Rezepturen schützt und in der nächsten Lieferantenprüfung des Handels souverän auftritt. Genau das sichert Listungen und Lieferfähigkeit.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Vorteil: Sicherheitsfragebögen des Handels sind in Stunden beantwortet, Audits verlieren ihren Schrecken, und Kunden sehen belegt, dass ihre Ware zuverlässig kommt.

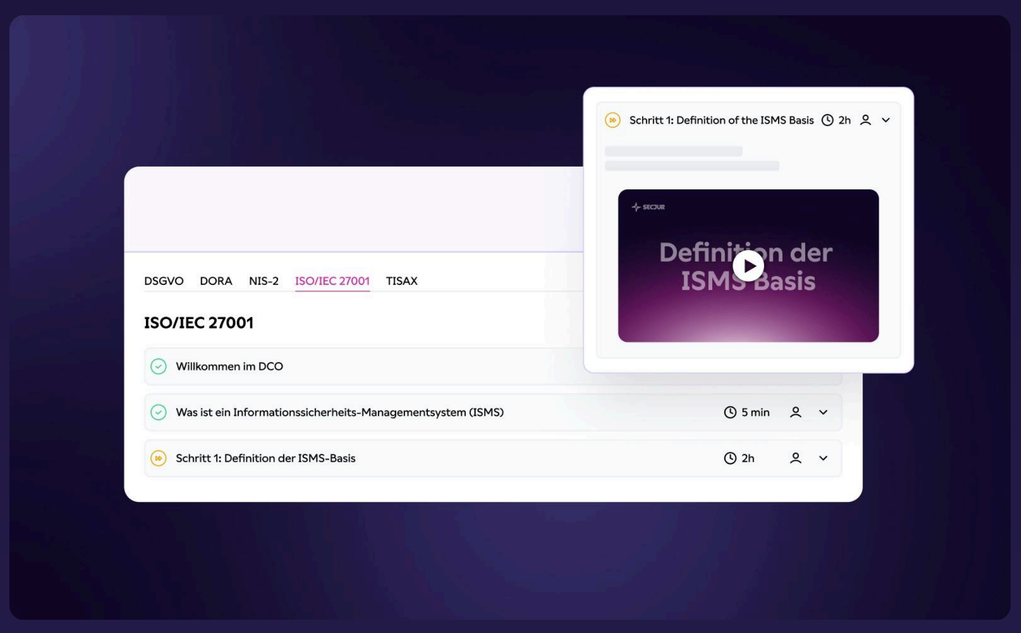
So wird aus einer Pflicht ein dauerhafter Schutz von Charge, Liefertermin und Ruf, der mit jeder neuen Anlage und jedem Handelspartner an Bedeutung gewinnt.

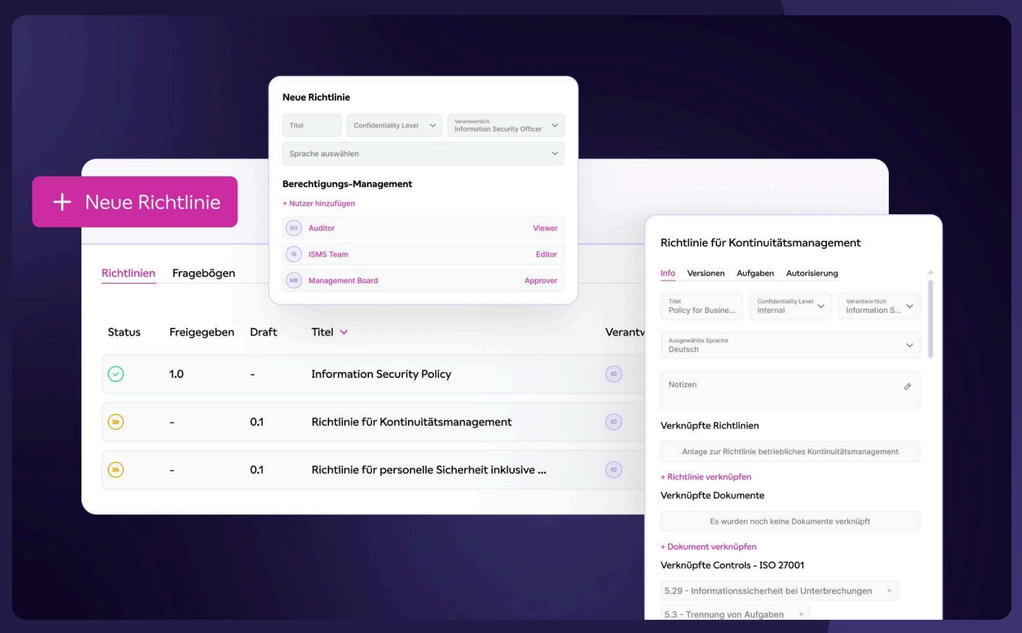
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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

yfood® Trolli PETER KÖLLN demeter Nordzucker STERNWYWIOL Gruppe

www.secjur.com