

Compliance darf kein Excel-Projekt bleiben.

NETZ EXPERTEN
NXN Compliance OS

ISO 27001, BSI IT-Grundschutz und TISAX verlangen Nachweise, keine Absichten. In vielen Unternehmen entsteht daraus eine Sammlung aus Tabellen, Dokumenten und E-Mail-Ketten, die niemand mehr vollständig überblickt. Und die zweite Hälfte fehlt ganz: ob das Dokumentierte technisch überhaupt noch wirkt.

WORAN ES IN DER PRAXIS SCHEITERT



Excel-Listen

Stand von gestern, drei Versionen im Umlauf.



Word-Dokumente

Richtlinien ohne Freigabe, ohne Historie.



E-Mail-Abstimmung

Entscheidungen, die niemand wiederfindet.



Unklare Zuständigkeit

Jeder Punkt gehört irgendwie allen.



Fehlende Nachweise

Die Maßnahme läuft, der Beleg fehlt.



Nachweise von gestern

Der Screenshot belegt den Stand von letztem Juni.



Unbekannter Ist-Zustand

Was im Netz wirklich läuft, steht in keiner Liste.



Hoher Audit-Aufwand

Wochen Vorbereitung für vorhandene Arbeit.

NXN Compliance OS führt Anforderungen, Maßnahmen, Nachweise und die technische Prüfung in einem System zusammen.

Selbst gehostet, mandantenfähig, revisionssicher – organisatorischer Nachweis und technische Prüfung in einem Werkzeug.

Von der Anforderung zur Umsetzung.

Eine Kette statt sieben Werkzeuge. Jeder Schritt hängt am vorherigen – und bleibt bis zum Audit nachvollziehbar.

DIE KETTE



Anforderung



Gap-Analyse



Risiko



Maßnahme



Verantwortliche Person



Nachweis



Audit

Jedes Glied kennt sein nächstes. Kein Schritt ohne Herkunft.



Frameworks & Kataloge

ISO 27001:2022 mit den Kapiteln 4-10 und Annex A, BSI IT-Grundschutz, TISAX - versioniert, mit Zuordnungen zwischen den Katalogen.



Geführter Modus

Der Durchlauf fragt pro Anforderung, nicht pro Unternehmen. Jede Antwort liefert Einstufung, benötigten Nachweis und Maßnahme mit Aufwand.



Gap-Analyse mit Herkunft

Vorschlag und Aussage bleiben getrennt: erst die menschliche Bestätigung wirkt auf Anwendbarkeitserklärung und Kennzahlen.



Risikomanagement

»Ohne Ihre Maßnahmen 20 (kritisch) → mit Ihren Maßnahmen 6 (mittel)«. Konfigurierbare Matrix, Bewertungshistorie, befristete Risikoakzeptanz.



Aufgaben & Fristen

Aus jeder Maßnahme wird eine Aufgabe mit Zuständigkeit, Frist, benötigtem Nachweis und konkreten Umsetzungsschritten.



Nachweise & Belege

Zentrales Repository mit Freigabe-Workflow und Ablaufdatum. Automatische Sammlung aus angebundenen Systemen und aus den eigenen Prüfläufen.



Erinnerungen

Täglich ein Aufriss an die Zuständigen: ablaufende Nachweise, fällige Aufgaben, überfällige Befunde – und nur, wenn etwas ansteht.



Berichte & Auditoren-Paket

Managementbericht, Kennzahlen, Auditoren-Portal mit begrenztem Zugriff, Exportpaket mit Prüfsummen-Manifest.

DREI GRUNDSÄTZE, DIE DAS SYSTEM DURCHZIEHEN

Vorschlag ist keine Aussage

Was das System vorschlägt, ist gekennzeichnet. Erst die Bestätigung eines Menschen wirkt auf Kennzahlen und Anwendbarkeitserklärung.

Jede Zahl ist herleitbar

Zu jedem Vollständigkeitsgrad gehört die Ausschlussquote und der Weg, auf dem er entstanden ist.

Nichts verschwindet still

Wird ein Plan neu erzeugt, bleibt menschliche Arbeit erhalten; Entfallenes wird als hinfällig markiert statt gelöscht

Prüfen statt behaupten.

Ein Nachweis sagt, was einmal eingerichtet wurde. Er sagt nicht, ob es heute noch so ist. Deshalb hat NXN Compliance OS eine eigene technische Prüfung: Netzwerk-Scan und automatisierte Penetrationstests, deren Ergebnisse direkt an der betroffenen Anforderung landen.



Netzwerk-Scan

Was im Netz wirklich läuft

- ✓ Systeme und Dienste finden – auch die, die auf keiner Liste mehr stehen
- ✓ Offene Ports, erreichbare Dienste, unerwartete Freigaben
- ✓ Veraltete Versionen und bekannte Schwachstellen
- ✓ Fehlkonfigurationen und schwache Verschlüsselung
- ✓ Ablaufende Zertifikate, bevor sie ablaufen
- ✓ Abweichung gegen das eigene Werteinventar



Automatisierte Pentests

Der Angriffsweg, nicht nur die Liste

- ✓ Eigenes Prüfwerkzeug von NetzExperten, kein zugekaufter Scanner-Report
- ✓ Wiederholbare Prüfläufe statt einer Momentaufnahme im Jahresbericht
- ✓ Nachweis der Ausnutzbarkeit statt einer Liste theoretischer Lücken
- ✓ Bericht je Lauf und Verlauf über die Zeit – wurde es besser?
- ✓ Nur gegen freigegebene Ziele, jeder Lauf im Audit-Log

SIE LEGEN FEST: WAS, WIE TIEF, WIE OFT



Umfang

Netzbereiche, einzelne Systeme, Anwendungen, externe Adressen – je Ziel getrennt freigegeben.



Tiefe

Inventar · Schwachstellenprüfung · aktive Prüfung. Jede Stufe ist eine eigene Entscheidung.



Takt

Täglich, wöchentlich, monatlich, quartalsweise – oder vor dem nächsten Audit.



Fenster

Wartungsfenster und Freigabe je Ziel. Nichts läuft ungeplant, nichts läuft unprotokolliert.

Einmal eingerichtet, läuft die Prüfung von selbst weiter – und meldet sich, wenn sich etwas verschlechtert.

WAS AUS EINEM FUND WIRD



Fund



Befund
mit Frist



Risiko



Aufgabe



Nachprüfung



Nachweis

Der Fund wird kein PDF im Ordner, sondern ein Befund mit Frist, ein Risiko im Register und eine Aufgabe bei einer namentlich zuständigen Person. Nach der Nachprüfung hängt der Nachweis an der Anforderung, die er belegt.

Weniger Aufwand. Mehr Transparenz. Bessere Auditfähigkeit.



Zentral

Eine Plattform statt Excel, Word, E-Mail und Dateiablagen. Ein Stand, den alle sehen.



Transparent

Die Geschäftsführung sieht jederzeit den aktuellen Compliance-Status – ohne Nachfrage-Runde.



Nachweisbar

Dokumentation und Nachweise entstehen während der Arbeit, nicht in der Woche vor dem Audit.



Skalierbar

Einmal aufgebaute Prozesse gelten für den nächsten Standard und den nächsten Standort.



DREI KATALOGE, EINE ARBEIT

Drei Kataloge in der Tiefe

ISO 27001, BSI IT-Grundschutz und TISAX – statt zwölf Standards, von denen keiner trägt.

Eine Maßnahme, mehrfach angerechnet

Was Sie einmal einrichten, zählt für jeden Katalog, der es verlangt – ISO, BSI und TISAX zugleich.

Ein Nachweis, ein Ablageort

Der Beleg hängt an der Anforderung, die er belegt. Nicht dreimal in drei Ordnerstrukturen.

BESONDERS INTERESSANT FÜR

Logistik

Industrie

Maschinenbau

Automotive & Zulieferer

Healthcare

Energie

IT-Dienstleister

Kritische Lieferketten

Unternehmen mit ISO-27001-Anforderung

Compliance nicht verwalten. Compliance steuern.

Heute die Zertifizierung. Morgen das gesamte Compliance Management.

NXN Compliance OS ist kein Werkzeug für eine einzelne Norm. Die Kette aus Anforderung, Risiko, Maßnahme und Nachweis bleibt dieselbe – der Katalog wechselt, die technische Prüfung läuft daneben weiter.

HEUTE IM PRODUKT



ISO 27001:2022

Kapitel 4–10 und Annex A, gegen DIN EN ISO/IEC 27001:2024-01 geprüft.



BSI IT-Grundschutz

Katalogstruktur mit Bausteinen und Anforderungen.



TISAX

Katalogstruktur für die Anforderungen der Automobil-Lieferkette.

AUSBAUBAR

DORA

ISO 9001

SOC 2

Lieferanten-Compliance

weitere Kataloge

Bewusste Entscheidung: drei Kataloge in der Tiefe statt zwölf an der Oberfläche. Breite ohne Tiefe hilft bei einer Zertifizierung nicht.

WARUM NETZEXPERTEN



Security by Design

Mandantentrennung, Rollenmodell und revisionssicheres Audit-Log sind Fundament, nicht nachträgliches Feature.



Made for Mittelstand

Pragmatisch statt Enterprise-Komplexität – bedienbar von Menschen, die Compliance nicht in Vollzeit machen.



Technologie und Umsetzung

Nicht nur Software: Einführung, Betrieb und die Sicherheitsarbeit dahinter kommen vom selben Team.



Europäische Datenhoheit

Self-hosted oder Private Cloud. Ihre Nachweise bleiben dort, wo Sie sie haben wollen.

Wo steht Ihr Unternehmen heute?

Ein strukturierter Blick auf den Ist-Stand – organisatorisch und technisch, bevor irgendein Werkzeug eingeführt wird.

Compliance Readiness Check

ISO 27001 Gap-Assessment

Live-Demo

Jetzt
NXN Compliance OS
entdecken!



IMPRESSUM

NetzExperten Unternehmensberatung
GmbH & Co. KG
Engerstr. 90, 47800 Krefeld

KONTAKT

kontakt@netzexperten.net
02151-4547786
www.netzexperten.net



KI BUNDESVERBAND

Allianz für
Cyber-Sicherheit

