ISO 27001 · NIS2

Sechs Dinge zwischen den Audits

Das Zertifikat gilt drei Jahre, die Nachweise dahinter oft nur eines. Diese sechs Aufgaben fallen zwischen zwei Audits am häufigsten unbemerkt aus. Keine ist groß. Gefährlich werden sie, weil niemand merkt, dass sie liegen bleiben.

1 Zugriffsrechte prüfen

Wer hat noch Zugang, der ihn nicht mehr braucht? Ehemalige Beschäftigte, Rollenwechsel, Dienstleisterkonten und Administratorrechte sind die typischen Funde.

BEZUG	TURNUS (EMPFEHLUNG)	NACHWEIS
ISO 27001 A.5.18 · NIS2 Art. 21 (2) i	halbjährlich, privilegierte Konten vierteljährlich	Prüfprotokoll mit Datum, Prüfer und entzogenen Rechten

- [ ] Liste aller Systeme mit Rechtevergabe aktuell
- [ ] Prüfung durch die fachlich verantwortliche Person, nicht nur durch die IT

2 Kritische Lieferanten neu bewerten

Ein Dienstleister, der vor einem Jahr unkritisch war, betreibt heute vielleicht Ihre Cloud. NIS2 macht die Sicherheit in der Lieferkette ausdrücklich zur Pflicht.

BEZUG	TURNUS (EMPFEHLUNG)	NACHWEIS
ISO 27001 A.5.19–A.5.22 · NIS2 Art. 21 (2) d	jährlich und bei wesentlichen Änderungen	Bewertung je Lieferant, Zertifikate mit Gültigkeitsdatum

- [ ] Lieferantenliste mit Kritikalität vorhanden
- [ ] Ablaufende Zertifikate der Lieferanten im Blick

3 Schulungen für neue und bestehende Beschäftigte

Neue Kolleginnen und Kollegen werden oft vergessen, weil die jährliche Schulung schon gelaufen ist. NIS2 nimmt ausdrücklich auch die Geschäftsleitung in die Pflicht.

BEZUG	TURNUS (EMPFEHLUNG)	NACHWEIS
ISO 27001 A.6.3 · NIS2 Art. 20 (2), Art. 21 (2) g	beim Eintritt und jährlich	Teilnahmeliste mit Datum und Inhalt

- [ ] Eintritte seit der letzten Schulung erfasst
- [ ] Schulung der Geschäftsleitung dokumentiert

neonotu GmbH · Edelsbergstraße 8 · 80686 München · Amtsgericht München HRB 313206 · USt-IdNr. DE339131149
Geschäftsführer Armin Haller · Sightadel ist eine Marke der neonotu GmbH · www.sightadel.com

4 Wiederherstellung von Backups testen

Ein Backup, das nie zurückgespielt wurde, ist eine Annahme. Erst der Test zeigt, ob Daten vollständig und in vertretbarer Zeit wiederkommen.

BEZUG	TURNUS (EMPFEHLUNG)	NACHWEIS
ISO 27001 A.8.13 · NIS2 Art. 21 (2) c	mindestens jährlich je kritischem System	Testprotokoll mit Dauer und Ergebnis

- [ ] Kritische Systeme und Wiederanlaufziele festgelegt
- [ ] Abweichungen aus dem Test als Maßnahme erfasst

5 Internes Audit und Managementbewertung

Beide sind Pflichtbestandteile des Managementsystems und werden gern ins letzte Quartal vor dem Überwachungsaudit geschoben, wo dann die Zeit fehlt.

BEZUG	TURNUS (EMPFEHLUNG)	NACHWEIS
ISO 27001 Kap. 9.2 und 9.3	jährlich, mit festem Termin	Auditbericht, Protokoll der Managementbewertung

- [ ] Auditprogramm für das laufende Jahr steht
- [ ] Ergebnisse und Entscheidungen der Leitung protokolliert

6 Risiken fortschreiben

Neue Systeme, neue Lieferanten, neue Bedrohungen: Eine Risikobewertung vom Zertifizierungsaudit beschreibt nach einem Jahr ein anderes Unternehmen.

BEZUG	TURNUS (EMPFEHLUNG)	NACHWEIS
ISO 27001 Kap. 6.1.2 und 8.2 · NIS2 Art. 21 (1)	jährlich und bei wesentlichen Änderungen	aktualisierte Risikobewertung mit Datum und Behandlungsplan

- [ ] Änderungen seit der letzten Bewertung gesammelt
- [ ] Risikoeigentümer haben die Bewertung bestätigt

Damit nichts davon liegen bleibt

In Sightadel bekommt jede dieser Aufgaben einen Turnus, eine zuständige Person und einen Nachweis mit Ablaufdatum. Die Erinnerung kommt, solange noch Zeit ist, und ein Nachweis zählt für jede Anforderung, der er dient, über ISO 27001, NIS2, DORA und weitere Frameworks.

sightadel.com

Die Turnusangaben sind Empfehlungen aus der Praxis, keine Vorgaben der Normen. Keine Rechtsberatung. Stand Oktober 2026.