SEQIFY

FACT PAPER

NIS2 & Cyberrisiko Management mit SEQIFY

Wie SEQIFY Sie bei der Umsetzung der NIS2-Richtlinie unterstützt – konkret, verständlich, umsetzbar.

NIS2 & ISO 27001: Was wird gefordert?

Mit der EU-Richtlinie NIS2 rücken Cybersicherheit und Risikomanagement stärker denn je in den Fokus der Unternehmensführung. Unternehmen müssen nachweislich **sicherstellen**, dass sie Risiken erkennen, bewerten und behandeln – systematisch, dokumentiert und kontinuierlich.
Auch ISO 27001, als international etablierter Standard für Informationssicherheitsmanagement (ISMS), fordert ein strukturiertes Vorgehen in den Bereichen Assetmanagement, Zugriffskontrolle, Vorfallmanagement und kontinuierliche Verbesserung.

Was beide Regelwerke verbindet:

- Klare **Verantwortlichkeiten** auf Managementebene
- Nachvollziehbares Risikomanagement **über alle Systeme hinweg**
- **Dokumentierte** Maßnahmen und Wirksamkeitskontrolle
- Fokus auf **Prävention**, Resilienz und Reaktionsfähigkeit

Für viele Unternehmen bedeutet das, dass neue Prozesse und technische Transparenz geschaffen werden muss - und sich das Thema Cybersicherheit als Führungsaufgabe etabliert.

§ NIS2

§ 32. (1) Wesentliche und wichtige Einrichtungen haben geeignete und verhältnismäßige technische, operative und organisatorische **Risikomanagementmaßnahmen** (...) **umzusetzen**, um die Risiken für die Sicherheit der Netz- und Informationssysteme (...) zu beherrschen und die Auswirkungen von Cybersicherheitsvorfällen (...) zu verhindern oder möglichst gering zu halten.

Quelle Gesetzesentwurf Ö

Herausforderungen in der Praxis

Risikomanagement

Fehlendes Gesamtbild, Messbarkeit von Maßnahmen schwierig, Nachweise fehlen

Assetmanagement

Unvollständige Erfassung aller Assets, Kritikalität unklar, inaktive Accounts verzerren Gesamtbild

Zugriffsmanagement

Unstrukturierte Rollen/Rechte-Vergabe, veraltete Konten bleiben bestehen, Anomalien bleiben unerkannt

IT-Betrieb & Wartung

Update-Prozesse nicht nach Priorität, Insellösungen, zentrales Monitoring fehlt

Warum ein ganzheitliches ISMS mehr ist als ein Sicherheitskonzept

Ein Informationssicherheits-Managementsystem (ISMS) ist die Grundlage für wirksame, kontinuierliche Cybersicherheit. Auditor:innen prüfen nicht nur, ob Maßnahmen existieren, sondern ob sie **wirksam**, **nachvollziehbar** und **aktuell** sind.

Gefragt ist ein klares Risikobild:

- Wo bestehen Risiken?
- Welche sind akzeptiert?
- Was wurde wie behandelt?

Für das Management zählt: Haftung wird reduziert, wenn **Pflichten nachweislich wahrgenommen**, **Entscheidungen belegt** und **Risiken aktiv gesteuert** werden. Genau hier setzt SEQIFY an – mit Monitoring, Dokumentation und einem strukturierten Überblick über Risiken, Maßnahmen und Verantwortlichkeiten.

NIS 2 & SEQiFY

SEQIFY deckt die zentralen Anforderungen der NIS2-Richtlinie praxisnah und automatisiert ab. Hier ein Überblick über die konkreten Teilbereiche:

1. Leitungsorgane

Rollen & Verantwortlichkeiten
SEQiFY ermöglicht die Übersicht über Risiken und deren Managementstatus. Ein Managementreview ist integrierbar, sodass das Berichtswesen gegenüber der Leitungsebene unterstützt wird.

2. Sicherheitsrichlinen

Richtlinien, Aufgaben & Verantwortlichkeiten
SEQIFY ersetzt keine formalen Richtlinien, unterstützt aber ihre Umsetzung effektiv:
Rollen, Zuständigkeiten und Maßnahmen werden innerhalb der Plattform klar zugeordnet und dokumentiert – so entsteht Transparenz, wer wofür verantwortlich ist. Das erleichtert sowohl die operative Umsetzung als auch den Nachweis gegenüber Auditor:innen.

NIS 2 & SEQiFY

3. Risikomanagement

Ein wirksames Risikomanagement ist das Herzstück jeder NIS2-Strategie. SEQIFY unterstützt Unternehmen dabei, Risiken nicht nur zu erfassen, sondern sie systematisch zu bewerten, zu steuern und nachweisbar zu dokumentieren – vollständig integriert in den Arbeitsalltag und auditfähig aufbereitet.

Risikoerkennung & -bewertung
Automatisierte Identifikation und Bewertung von Risiken für Assets, Anwendungen und Cloud-Dienste. Alle Bewertungen sind zentral einsehbar.

Risikobehandlung
Klare Handlungsempfehlungen, Maßnahmenverfolgung und revisionssichere Dokumentation – inklusive Risikoakzeptanz.

Wirksamkeitskontrolle
Nachvollziehbare Erfolgskontrolle durch Score-Veränderungen bei Maßnahmenumsetzung.

Vorgabenüberwachung
Echtzeit-Transparenz zur Einhaltung sicherheitsrelevanter Anforderungen (z.B. Update- und Patch-Status).

Rechtliche Anforderungen
Unterstützung bei der Überprüfung der Umsetzung gesetzlicher und vertraglicher Pflichten.

Darstellung & Reporting
Übersichtliches Risikobild mit Managementstatus, integrierbarer Managementreview - Unterstützung des Berichtswesens gegenüber Leitungsebene

NIS 2 & SEQiFY

4. Verwaltung von Vermögenswerten

Eine vollständige und aktuelle Übersicht über alle digitalen Assets ist Voraussetzung für jede Form der Risiko- und Sicherheitsbewertung. SEQIFY unterstützt Unternehmen dabei, Assets systemübergreifend zu identifizieren, zu klassifizieren und regelkonform zu verwalten – auch in dynamischen IT-Umgebungen.

Inventarisierung & Klassifikation
SEQIFY bietet eine systemübergreifende Übersicht und Klassifikation der relevanten Assets – von Servern über Anwendungen bis hin zu Benutzerkonten

Asset Management & Rückführung
Die Plattform bietet eine aktuelle Übersicht über den Status von Assets - von der Nutzung bis zu Rückgabe/Löschung – insbesondere in Bezug auf Cloud-Anwendungen und mobile Endgeräte – gemäß geltender Vorgaben.

5. Personalwesen

Im Kontext der Cybersicherheit ist das Austrittsmanagement ein kritischer Faktor: Verbliebene Zugänge oder nicht zurückgegebene Assets stellen ein erhebliches Risiko dar. SEQIFY unterstützt Unternehmen dabei, den Offboarding-Prozess revisionssicher und regelkonform zu gestalten.

Austrittsmanagement
SEQIFY macht die Rücknahme und Löschung von Benutzerkonten und digitalen Assets transparent – konform zu internen Vorgaben und regulatorischen Anforderungen.

NIS 2 & SEQiFY

6. Cybersicherheitsbewusstsein und Schulungen

Schulungen & Awareness
Mit Integration von Awareness-Tools wird aufgezeigt, welche Schulungen durch wen durchgeführt wurden - oder fehlen.

Cyberhygiene
Transparenz über Patch-Status, Updates und inaktive Nutzerkonten (z. B. „Ghost User“).

7. Sicherheit in der Lieferkette

Lieferantenmanagement
Das zentrale Dashboard liefert eine Übersicht über Hard- und Softwarelieferanten, Cyberrisk-Ratings (z. B. KSV1870), Zertifizierungen und deren Gültigkeit.

8. Zugriffssteuerung

Benutzerübersicht & Logins
SEQIFY stellt eine zentrale Übersicht über Benutzer, Gruppenberechtigungen, Login-Verhalten und Standort der Logins bereit. Auch fehlerhafte oder verdächtige Anmeldeversuche werden erfasst.

Ein vollumfängliches Berechtigungsmanagement ist nicht enthalten – SEQIFY liefert eine solide Grundlage zur Identifikation kritischer Zugriffsmuster und Bereinigungsbedarfe.

NIS 2 & SEQiFY

9. IT-Betrieb & Wartung

SEQIFY unterstützt zentrale Aufgaben der technischen Sicherheit – insbesondere in den Bereichen Patchmanagement, Schwachstellenerkennung und Softwarekontrolle.

Patch- & Konfigurationsmanagement
Übersicht über Update- und Lizenzstatus. Teilweise Integration bei Mobile Devices, sonst über externe Tools.

Vulnerability Management
Identifikation und Darstellung relevanter Schwachstellen (z. B. CVEs) auf System- und Applikationsebene.

Unautorisierte Software
Schnellübersicht über verdächtige oder nicht autorisierte Anwendungen als Grundlage für weitere Prüfungen.

NIS 2 & SEQiFY

10. Kryptographie

Verschlüsselung
SEQIFY dokumentiert den Einsatz von Festplattenverschlüsselung. Eine umfassende Kryptostrategie oder Schlüsselverwaltung ist nicht enthalten.

11. Informations-sicherheitsvorfälle

Vorfallmanagement
Erkennung fehlerhafter Logins, präventive Hinweise und Übersicht zur Reaktionsfähigkeit bei sicherheitsrelevanten Vorfällen sind gegeben.

12. Betriebskontinuität & Krisenmanagement

Unterstützung
Unterstützung durch präventive Maßnahmen (z.B. Softwareupdates, Monitoringaktivitäten)

13. Physische & umgebungsbezogene Sicherheit

Physische Zutritte & Schutzmaßnahmen
Funktionen zur Kontrolle physischer Zutritte oder baulicher Schutzmaßnahmen sind in SEQIFY nicht enthalten.

Überblick

Bereich	SEQIFY-Unterstützung	NIS 2	ISO 27001
1. Rollen & Verantwortlichkeiten	Überblick über Risiken und Status; integriertes Management-Review	Art. 21, i	A.5.1, A.5.3, A.5.4
2. Sicherheitsrichtlinien	Keine Richtlinienpflege, aber klare Rollen- und Maßnahmenzuordnung in der Risikoübersicht.	Art. 21, a, i	A.5.1, A.5.2, A.5.4, A.5.31
3. Risikomanagement	Automatisierte Erkennung, Bewertung, Maßnahmenverfolgung, Wirksamkeitskontrolle und Nachweise.	Art. 21, a,f	A.5.7, A.5.30, A.8.2, A.5.35
4. Assetmanagement	Systemübergreifende Inventarisierung und Klassifikation; Dokumentation von Rückgaben	Art. 21, i	A.5.9 – A.5.11, A.7.9, A.7.10, A.7.14
5. Personalwesen	Dokumentierte Rücknahme & Löschung von Benutzerkonten bei Austritten.	Art. 21, i	A.6.1 – A.6.5, A.6.7
6. Awareness & Cyberhygiene	Überblick über Schulungen, Patch-Status, Benutzerleichen und technische Sicherheitslücken.	Art. 21, g	A.6.3, A.7.7, A.5.15 – A.5.18, A.8.8 – A.8.9
7. Lieferkettensicherheit	Zentrales Dashboard für Lieferanten, Cyberrisk-Ratings, Zertifikate und Ablaufdaten.	Art. 21, d	A.5.19 – A.5.23
8. Zugriffssteuerung	Übersicht über Benutzer, Logins, Gruppenrechte (kein vollständiges Berechtigungsmanagment).	Art. 21, i,j	A.5.15 – A.5.18, A.8.3 – A.8.5
9. IT-Betrieb & Wartung	Transparenz zu Updates, Lizenzen, Konfigurationen und Schwachstellen (z. B. CVEs).	Art. 21, e,f	A.8.8 – A.8.23, A.5.37
10. Kryptographie	Dokumentation der Festplattenverschlüsselung; keine tiefere Kryptostrategie.	Art. 21, h	A.8.24 – A.8.25
11. Vorfallmanagement	Erkennung fehlerhafter Logins, Prävention und Übersicht zur Reaktionsfähigkeit bei Vorfällen.	Art. 21, b	A.5.24 – A.5.28, A.6.8, A.8.15 – A.8.17
12. Betriebskontinuität	Unterstützung durch präventive Maßnahmen wie Monitoring und Update-Kontrolle.	Art. 21, c	A.5.29 – A.5.30, A.8.6, A.8.13 – A.8.14
13. Physische Sicherheit	Keine Abdeckung physischer Zutritte oder umgebungsbezogener Schutzmaßnahmen.	/	A.7.1 – A.7.10, A.7.12 – A.7.14

NIS 2 & SEQiFY

SEQIFY deckt die zentralen Anforderungen der NIS2-Richtlinie praxisnah und automatisiert ab – von **Risikomanagement** über **Asset- und Benutzerübersicht** bis hin zur **Nachweisführung** für Auditor:innen.

- Risiko-erkennung
- Maßnahmen-steuerung
- Nachverfolgung
- Nachweis / Audit