PPI – Platvoet Performance Intelligence

WHITEPAPER

NIS2 vs. ISO 27001

Gemeinsamkeiten, Unterschiede

und integrierte Umsetzung

NIS2 ist seit Dezember 2025 in Deutschland geltendes Recht — ohne Übergangsfrist. ISO 27001 ist der etablierte internationale Standard für Informationssicherheits-Managementsysteme. Wer beides zusammen denkt, spart erheblichen Aufwand und schafft ein robusteres Sicherheitsfundament als mit isolierten Compliance-Programmen. Dieses Whitepaper zeigt, wo beide Rahmenwerke überlappen, wo echte Lücken entstehen und wie ein integriertes ISMS beide Anforderungen effizient abdeckt.

Autor	Ralf Platvoet, Diplom-Ökonom
Organisation	PPI – Platvoet Performance Intelligence
Stand	Juni 2026 (NIS2UmsuCG in Kraft seit 06.12.2025; ISO 27001:2022)
Umfang	ca. 22 Seiten
Themenbereich	Cyber-Compliance · Informationssicherheit · ISMS

platvoet.org

Executive Summary

Zwei Regelwerke dominieren derzeit die Informationssicherheits-Agenda europäischer Organisationen: Die **NIS2-Richtlinie**, seit Dezember 2025 durch das NIS2UmsuCG in deutsches Recht überführt, und **ISO 27001:2022**, der international anerkannte Standard für Informationssicherheits-Managementsysteme. Beide verfolgen das gleiche übergeordnete Ziel — Informationssicherheitsrisiken systematisch zu managen und die Widerstandsfähigkeit gegen Cyberangriffe zu stärken. Dennoch unterscheiden sie sich fundamental in Rechtscharakter, Anwendungsbereich, Detaillierungstiefe und Nachweisanforderungen.

Die gute Nachricht: Wer bereits nach ISO 27001:2022 zertifiziert ist, hat einen erheblichen Vorsprung bei der NIS2-Umsetzung. Studien und Praxiserfahrungen zeigen, dass ein reifes ISMS nach ISO 27001 zwischen 70 und 80 Prozent der NIS2-Anforderungen bereits abdeckt. Die schlechte Nachricht: Die verbleibenden 20 bis 30 Prozent sind kein formaler Rest — sie enthalten einige der operativ anspruchsvollsten Anforderungen: strikte Meldepflichten, persönliche Geschäftsführerhaftung und Lieferkettenanforderungen, die über klassische ISMS-Logik hinausgehen.

Dieses Whitepaper bietet ein systematisches Mapping beider Rahmenwerke, identifiziert die echten Lücken und beschreibt, wie ein integriertes ISMS beide Anforderungen effizient und ohne Doppelstruktur abdeckt.

Kernaussagen

- NIS2 ist seit 06.12.2025 in Deutschland geltendes Recht (NIS2UmsuCG) — keine Übergangsfrist.
- ISO 27001:2022 deckt 70–80 % der NIS2-Anforderungen ab — aber nicht alle.
- Die kritischen Lücken: Meldepflichten (24 h), persönliche Geschäftsführerhaftung, Lieferkettenanforderungen.
- Ein integriertes ISMS ist effizienter als zwei parallele Compliance-Programme.
- Rund 29.500 Unternehmen in Deutschland sind von NIS2 betroffen — viele davon ohne ISO-27001-Basis.

1. Die beiden Rahmenwerke im Überblick

Bevor ein Vergleich möglich ist, müssen die grundlegenden Charakteristika beider Rahmenwerke verstanden werden — denn sie sind in ihrer Grundlogik verschieden, auch wenn sie das gleiche Sicherheitsproblem adressieren.

NIS2 / NIS2UmsuCG	ISO/IEC 27001:2022
Rechtscharakter: EU-Richtlinie, nationales Recht (NIS2UmsuCG)	Rechtscharakter: Internationaler Standard (ISO/IEC)
Verbindlichkeit: Gesetzliche Pflicht — kein Opt-in	Verbindlichkeit: Freiwillig — außer bei vertraglicher Pflicht
In Kraft (DE): 06. Dezember 2025	Aktuelle Version: ISO 27001:2022 (Oktober 2022)
Zielgruppe: ~29.500 Unternehmen in 18 Sektoren	Zielgruppe: Alle Organisationen weltweit
Größenschwelle: ≥ 50 MA oder ≥ 10 Mio. € Umsatz	Größenschwelle: Keine — skalierbar für KMU bis Konzern
Nachweis: BSI-Registrierung, Meldepflichten, Audits	Nachweis: Zertifizierung durch akkreditierte Stellen
Zertifizierung: Nicht möglich — NIS2 ist kein Standard	Zertifizierung: Möglich und international anerkannt
Sanktionen: bis 10 Mio. € oder 2 % Weltumsatz	Sanktionen: Keine direkt — Vertragsstrafen möglich
Verantwortung: Persönliche Haftung der Geschäftsführung	Verantwortung: Organisatorische Verantwortung (Top Management)
Fokus: Resilienz kritischer Sektoren, gesellschaftliche Schutzwirkung	Fokus: Systematisches ISMS, risikobasierter Ansatz

2. NIS2 und NIS2UmsuCG: Was gilt seit Dezember 2025?

2.1 Adressatenkreis und Sektoren

NIS2 unterscheidet zwei Kategorien betroffener Einrichtungen — mit unterschiedlichen Anforderungsniveaus und Sanktionsrahmen:

Kategorie	Kriterien	Sektoren (Beispiele)	Max. Bußgeld
Besonders wichtige Einrichtungen	≥ 250 MA oder ≥ 50 Mio. € Umsatz in Hochrisikoektoren	Energie, Verkehr, Banken, Gesundheit, Trinkwasser, digitale Infrastruktur	10 Mio. € oder 2 % Weltumsatz
Wichtige Einrichtungen	≥ 50 MA oder ≥ 10 Mio. € Umsatz in weiteren Sektoren	Post, Abfallentsorgung, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Dienste	7 Mio. € oder 1,4 % Weltumsatz

2.2 Die zehn Mindestmaßnahmen nach § 30 BSIG

NIS2 definiert in Art. 21 der Richtlinie (umgesetzt in § 30 BSIG-neu) mindestens zehn technische und organisatorische Maßnahmen, die alle betroffenen Einrichtungen implementieren müssen:

1. Risikoanalyse und Sicherheit der Informationssysteme
2. Bewältigung von Sicherheitsvorfällen (Incident Management)
3. Aufrechterhaltung des Betriebs, Backup-Management, Krisenmanagement, Business Continuity
4. Sicherheit der Lieferkette (Supply Chain Security)
5. Sicherheitsmaßnahmen beim Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
7. Grundlegende Cyberhygiene und Schulungen zur Cybersicherheit
8. Kryptografie und Verschlüsselung
9. Personalsicherheit, Zugriffskontrolle und Asset-Management
10. Verwendung von Multi-Faktor-Authentifizierung (MFA)

2.3 Meldepflichten: Der operative Kern von NIS2

Die Meldepflichten sind einer der operativ anspruchsvollsten Aspekte von NIS2 — und gleichzeitig der, der unmittelbar nach Inkrafttreten gilt. Der dreistufige Meldeprozess nach § 32 NIS2UmsuCG sieht vor:

Stufe	Frist	Inhalt	Meldekanal
Frühwarnung	Innerhalb 24 Stunden nach Kenntnis	Erster Hinweis auf erheblichen Vorfall; Art und Ausmaß (soweit bekannt)	BSI-Meldeportal (MIP)
Erstmeldung	Innerhalb 72 Stunden	Bewertung: erheblicher Vorfall? Ersteinschätzung Auswirkungen, Kompromittierungsindikator	BSI-Meldeportal (MIP)
Abschlussbericht	Innerhalb eines Monats	Vollständige Beschreibung, Ursachenanalyse, Gegenmaßnahmen, grenzüberschreitende Auswirkungen	BSI-Meldeportal (MIP)

Wann ist ein Vorfall meldepflichtig?

Ein 'erheblicher Sicherheitsvorfall' liegt nach § 32 NIS2UmsuCG vor, wenn er (a) erhebliche Betriebsstörungen oder finanzielle Verluste verursacht hat oder verursachen kann, oder (b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden betroffen hat oder betreffen kann. Die Formulierung 'verursachen kann' ist wichtig: Ein Vorfall muss noch keinen Schaden verursacht haben, um meldepflichtig zu sein. Das Schadenspotenzial reicht aus.

2.4 Geschäftsführerhaftung

Eine der gravierendsten Neuerungen von NIS2 gegenüber NIS1 und gegenüber ISO 27001: Die Geschäftsführung haftet persönlich für die Einhaltung der NIS2-Pflichten. § 38 BSIG-neu verpflichtet Leitungsorgane, Risikomanagementmaßnahmen aktiv zu billigen, ihre Umsetzung zu überwachen und regelmäßig an Schulungen zur Cybersicherheit teilzunehmen. Eine reine Delegation an IT oder externe Dienstleister enthaftet nicht.

Im Unterschied dazu: ISO 27001 fordert 'Commitment des Top-Managements' — aber die persönliche Haftbarkeit ist in der Norm selbst nicht verankert. Sie entsteht erst durch nationales Recht, und NIS2 setzt genau diesen Hebel.

3. ISO 27001:2022: Was der Standard leistet

3.1 Struktur und Logik des ISMS

ISO 27001 definiert die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS). Die Norm ist nach der High-Level-Structure (HLS / Annex SL) aufgebaut — der gleichen Grundstruktur wie ISO 9001 (Qualität), ISO 14001 (Umwelt) oder ISO 22301 (Business Continuity). Das ermöglicht die Integration mehrerer Managementsysteme.

Der Kern der Norm: Ein risikobasierter PDCA-Zyklus (Plan–Do–Check–Act), der Organisationen dazu bringt, Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten, zu behandeln und kontinuierlich zu verbessern. Die Version 2022 führte 11 neue Kontrollen ein und reorganisierte die Anhang-A-Kontrollen von 14 auf 4 Themencluster (Organisatorisch, Personell, Physisch, Technologisch).

ISO 27001:2022 Hauptkapitel	Inhalt
Kap. 4 — Kontext	Organisationskontext, interessierte Parteien, Anwendungsbereich des ISMS
Kap. 5 — Führung	Leitungscommitment, Informationssicherheitspolitik, Rollen und Verantwortlichkeiten
Kap. 6 — Planung	Risikobeurteilung und -behandlung, Informationssicherheitsziele
Kap. 7 — Unterstützung	Ressourcen, Kompetenz, Bewusstsein, Kommunikation, Dokumentation
Kap. 8 — Betrieb	Operative Planung, Risikobeurteilung und -behandlung in der Praxis
Kap. 9 — Leistungsbewertung	Überwachung, Messung, internes Audit, Managementbewertung
Kap. 10 — Verbesserung	Nichtkonformitäten, Korrekturmaßnahmen, kontinuierliche Verbesserung
Anhang A — Kontrollen	93 Kontrollen in 4 Clustern (Organisatorisch, Personell, Physisch, Technologisch)

3.2 Stärken und Grenzen von ISO 27001

ISO 27001 bietet drei entscheidende Stärken, die NIS2-Compliance vorbereiten — und hat gleichzeitig blinde Flecken, die für NIS2-pflichtige Organisationen relevant sind:

Stärken von ISO 27001	Grenzen gegenüber NIS2
✓ Systematischer, risikobasierter Ansatz — genau was NIS2 fordert	✗ Keine gesetzliche Bindewirkung — NIS2 schafft Rechtspflicht
✓ Vollständige ISMS-Struktur: Governance, Prozesse, Kontrollen	✗ Meldepflichten nicht spezifiziert (24h/72h/1 Monat fehlen)
✓ Zertifizierbar — internationaler Vertrauensnachweis	✗ Persönliche Geschäftsführerhaftung nicht adressiert

✓ Skalierbar für alle Unternehmensgrößen ✓ HLS-Kompatibilität: Integration mit ISO 22301, ISO 9001 möglich ✓ Anhang A deckt breite Kontrollenlandschaft ab (93 Kontrollen) ✓ Etablierte Audit- und Rezertifizierungszyklen	✗ Lieferkettensicherheit weniger operativ als NIS2 Art. 21d ✗ Sektorspezifische Anforderungen nicht abgedeckt ✗ Registrierung beim BSI kein ISO-27001-Thema ✗ KRITIS-spezifische Sonderanforderungen fehlen

4. NIS2 × ISO 27001: Das Mapping

Die folgende Mapping-Tabelle zeigt, welche NIS2-Anforderungsbereiche (Art. 21 NIS2 / § 30 BSIG) durch ISO-27001:2022-Kontrollen abgedeckt werden — und wo echte Lücken verbleiben. Farbcodierung: ■ **Vollständig/weitgehend abgedeckt** · ■ **Teilweise abgedeckt** · ■ **Lücke — zusätzlicher Aufwand nötig**.

NIS2-Anforderungsbereich	ISO 27001:2022 Kontrollen	Deckungsgrad
Risikoanalyse & Informationssystemsicherheit	Kap. 6.1, 8.2, 8.3; A.5.1–5.37	● **Vollständig abgedeckt**
Vorfallmanagement (intern)	A.5.24–5.28 (Incident Management)	● **Weitgehend abgedeckt**
Business Continuity & Backup	A.5.29–5.30; A.8.13–8.14	◑ **Teilweise — NIS2 konkreter bei Krisenmanagement**
Kryptografie & Verschlüsselung	A.8.24 (Kryptografieregeln)	● **Weitgehend abgedeckt**
Personalsicherheit & Schulung	A.6.1–6.8; A.6.3 (Awareness)	◑ **Teilweise — NIS2 fordert GF-Schulung explizit**
Zugangskontrolle & Asset-Management	A.5.9–5.15; A.8.2–8.3	● **Weitgehend abgedeckt**
Multi-Faktor-Authentifizierung (MFA)	A.8.5 (Sichere Authentifizierung)	● **Abgedeckt**
Lieferkettensicherheit	A.5.19–5.22 (Lieferantenbeziehungen)	◑ **Teilweise — NIS2 fordert tiefere vertragliche Integration**
Sicherheit in Entwicklung & Beschaffung	A.8.25–8.32 (Sichere Entwicklung)	● **Weitgehend abgedeckt**
Wirksamkeitsbewertung von Maßnahmen	Kap. 9.1 (Überwachung & Messung)	● **Abgedeckt**
Meldepflichten (24h/72h/1 Monat)	Nicht spezifiziert in ISO 27001	○ **Lücke — kein ISO-27001-Äquivalent**
BSI-Registrierung	Nicht adressiert	○ **Lücke — rein regulatorische Pflicht**
Persönliche Geschäftsführerhaftung	Kap. 5 (Leadership) — prinzipiell	○ **Lücke — keine Haftungsregelung in der Norm**
Sektorspezifische Anforderungen (KRITIS)	Nicht adressiert	○ **Lücke — sektorales Zusatzrecht notwendig**

Fazit des Mappings

ISO 27001:2022 deckt die methodischen und technisch-organisatorischen Anforderungen von NIS2 weitgehend ab. Die verbleibenden Lücken sind klar lokalisiert: Meldepflichten, BSI-Registrierung, Geschäftsführerhaftung und sektorspezifische

Anforderungen. Diese Lücken sind nicht durch ISMS-Optimierung zu schließen — sie erfordern zusätzliche operative Prozesse und rechtliche Governance.

5. Die echten Lücken: Was ISO 27001 nicht abdeckt

Das Mapping zeigt, wo die kritischen Lücken liegen. Dieser Abschnitt beschreibt, was Organisationen konkret tun müssen, um diese Lücken zu schließen — auch wenn sie bereits ISO-27001-zertifiziert sind.

Lücke 1 — Meldepflichten nach § 32 NIS2UmsuCG

ISO 27001 fordert Incident-Management-Prozesse (A.5.24–5.28) — aber keine behördliche Meldepflicht mit konkreten Fristen. Die NIS2-Meldepflicht ist qualitativ anders: Sie erfordert eine operative 24/7-Bereitschaft, vordefinierte Eskalationspfade zur BSI-Kommunikation und ein funktionierendes Klassifikationssystem für 'erhebliche Vorfälle'.

Was zu tun ist: Incident-Response-Prozesse auf die dreistufige Meldepflicht ausrichten, BSI-Meldeportal (MIP) einrichten und testen, 24/7-Erreichbarkeit sicherstellen, interne Klassifikationsmatrix für meldepflichtige Vorfälle entwickeln.

Lücke 2 — Persönliche Geschäftsführerhaftung (§ 38 BSIG)

ISO 27001 Kapitel 5 fordert Leitungscommitment — aber keine persönliche Haftbarkeit. § 38 BSIG-neu geht deutlich weiter: Geschäftsführer müssen Risikomanagementmaßnahmen aktiv billigen (nicht nur genehmigen), deren Umsetzung überwachen und regelmäßig selbst geschult werden. Delegation enthaftet nicht.

Was zu tun ist: Formalen Beschluss der Geschäftsführung zur NIS2-Compliance dokumentieren, regelmäßige Schulungen der GF zu Cybersicherheitsthemen mit Nachweis, Berichterstattungsstruktur GF ↔ CISO/IT-Sicherheit formalisieren.

Lücke 3 — BSI-Registrierung

Alle NIS2-pflichtigen Einrichtungen müssen sich beim BSI registrieren. Das BSI-Meldeportal (MIP) ist seit dem 6. Januar 2026 in Betrieb. Die Registrierungsfrist für besonders wichtige Einrichtungen lief bis zum 6. März 2026. Wer sich noch nicht registriert hat, riskiert unmittelbares Sanktionsrisiko.

Was zu tun ist: Prüfen, ob NIS2-Pflicht besteht und welcher Kategorie die Einrichtung zuzuordnen ist. Registrierung im BSI-MIP nachholen. Kontaktdaten für den 24/7-Sicherheitskontakt hinterlegen.

Lücke 4 — Lieferkettensicherheit (Art. 21d NIS2)

ISO 27001 A.5.19–5.22 adressiert Lieferantenbeziehungen — aber auf einem prinzipienbasierten Level. NIS2 Art. 21d geht tiefer: Es fordert eine systematische Bewertung der Sicherheitspraktiken und Vertragsbedingungen aller wesentlichen Lieferanten, die Berücksichtigung von Sicherheitslücken und bekannten Angreifertaktiken und die vertragliche Verankerung von Sicherheitsanforderungen.

Was zu tun ist: Lieferantenbewertung um NIS2-spezifische Sicherheitskriterien erweitern, Vertragsmuster mit NIS2-konformen Sicherheitsklauseln aktualisieren, kritische Lieferanten nach NIS2-Kriterien klassifizieren.

6. Das integrierte ISMS: Beide Rahmenwerke effizient kombinieren

Ein integriertes ISMS, das NIS2 und ISO 27001 gleichzeitig abdeckt, ist kein Parallelkonstrukt — es ist ein erweitertes ISO-27001-ISMS mit NIS2-spezifischen Ergänzungen. Das Grundprinzip: ISO 27001 liefert die Struktur, Methodik und Dokumentationssystematik. NIS2 ergänzt die gesetzlich vorgeschriebenen Mindestmaßnahmen, Meldepflichten und Governance-Anforderungen.

6.1 Das Architekturprinzip: Keine Doppelstrukturen

Der häufigste Fehler bei der Doppel-Compliance: Zwei separate Programme — eines für ISO-27001-Zertifizierung, eines für NIS2-Compliance — mit eigenen Dokumenten, eigenen Prozessen, eigenen Verantwortlichkeiten. Das Ergebnis: doppelter Aufwand, inkonsistente Sicherheitskultur, Konflikte zwischen Anforderungen.

Das Alternativmodell: Ein einziges ISMS, das beide Anforderungssets als Quellen behandelt. ISO 27001 ist der strukturelle Rahmen. NIS2-Anforderungen werden als zusätzliche Anforderungen in dieselben Prozesse, Dokumente und Kontrollen integriert.

Integrationsarchitektur auf einen Blick

ISMS-Kerndokumente (ISO 27001): Informationssicherheitspolitik, Risikobeurteilung, Statement of Applicability (SoA)

→ NIS2-Erweiterung: SoA um NIS2-Mindestmaßnahmen ergänzen; explizit NIS2-Referenzen einarbeiten

Incident Management (ISO 27001: A.5.24–28): Interner Prozess für Vorfallidentifikation und -behandlung

→ NIS2-Erweiterung: Meldeprozess 24h/72h/1 Monat als eigenständigen Workflow integrieren

Lieferantenmanagement (ISO 27001: A.5.19–22): Risikobasierte Lieferantenbewertung

→ NIS2-Erweiterung: NIS2-Sicherheitskriterien in Lieferantenbewertungsmatrix aufnehmen

Leadership (ISO 27001: Kap. 5): Top-Management-Commitment

→ NIS2-Erweiterung: GF-Schulungsnachweis, formaler GF-Beschluss, Haftungsdokumentation

6.2 Implementierungsreihenfolge für unterschiedliche Ausgangssituationen

Ausgangssituation	Empfohlene Reihenfolge	Typischer Aufwand

ISO 27001 zertifiziert (aktuell)	1. NIS2-Gap-Analyse · 2. Lücken schließen (Meldung, GF, Register) · 3. SoA erweitern · 4. Interne Audits anpassen	3–6 Monate
ISO 27001 in Aufbau, NIS2-pflichtig	1. NIS2-Sofortmaßnahmen (Registrierung, Meldeprozess) · 2. ISMS integriert aufbauen · 3. Zertifizierung anstreben	9–18 Monate
Kein ISMS, NIS2-pflichtig	1. NIS2-Pflichtmaßnahmen sofort (Registrierung, GF-Governance, Meldeprozess) · 2. ISMS nach ISO 27001 strukturiert aufbauen	12–24 Monate
ISO 27001 geplant, kein NIS2	ISO 27001 vollständig implementieren — NIS2-Abdeckung als Mehrwert kommunizieren	9–18 Monate

6.3 Die fünf Integrationsschritte

11. Gap-Analyse: NIS2-Anforderungen gegen bestehende ISMS-Kontrollen abgleichen — Mapping-Tabelle (Kapitel 4) als Ausgangspunkt nutzen.
12. NIS2-Sofortmaßnahmen: BSI-Registrierung, Meldeprozess und GF-Governance haben keine Übergangsfrist — prioritär umsetzen.
13. ISMS-Erweiterung: Statement of Applicability um NIS2-Referenzen ergänzen; Risikobewertung um NIS2-spezifische Bedrohungsszenarien erweitern.
14. Dokumentation konsolidieren: Ein einziges Dokumentenset, das beide Anforderungsquellen abdeckt — keine Parallelstrukturen.
15. Audit-Strategie: Interne Audits um NIS2-Compliance-Checks erweitern; ISO-Zertifizierungsaudit und NIS2-Nachweise aufeinander abstimmen.

7. Integrierter Readiness-Check

Der folgende Check ermöglicht eine erste Einschätzung des Umsetzungsstands für NIS2 und ISO 27001 im integrierten Ansatz. Bewerten Sie jede Aussage mit: ✓ umgesetzt · △ teilweise · ✗ fehlt.

Block A — NIS2-Pflichtmaßnahmen

Aussage	✓ / △ / ✗
BSI-Registrierung ist abgeschlossen.	
Meldeprozess für erhebliche Vorfälle (24h/72h/1 Monat) ist operativ erprobt.	
Klassifikationsmatrix für meldepflichtige Vorfälle ist definiert.	
Geschäftsführung hat NIS2-Risikomanagementmaßnahmen formell gebilligt.	
Geschäftsführung wurde zu Cybersicherheitsthemen geschult (nachweisbar).	
Lieferantenbewertung deckt NIS2-Sicherheitskriterien ab.	

Block B — ISO 27001 ISMS

Aussage	✓ / △ / ✗
Ein formales ISMS nach ISO 27001 ist dokumentiert und betrieben.	
Risikobeurteilung und -behandlung sind aktuell und vollständig.	
Statement of Applicability (SoA) ist vorhanden und aktuell.	
Internes Audit-Programm läuft regelmäßig.	
ISO-27001-Zertifizierung besteht oder ist in Vorbereitung.	

Block C — Integration

Aussage	✓ / △ / ✗
NIS2-Anforderungen sind explizit im SoA / ISMS-Dokumentenset referenziert.	
Ein einziges Incident-Response-Prozess deckt ISO-interne und NIS2-Meldepflicht ab.	
Es gibt kein paralleles NIS2-Compliance-Programm neben dem ISMS.	
Interne Audits prüfen sowohl ISO-27001- als auch NIS2-Compliance.	

Auswertung (max. 15 × ✓)

13–15 × ✓: Hohe Integrationsreife — laufende Optimierung und Audit-Vorbereitung.

9–12 × ✓: Mittlere Reife — Lücken gezielt schließen; NIS2-Sofortmaßnahmen priorisieren.

5–8 × ✓: Erhebliche Lücken — strukturiertes Programm mit externem Support empfohlen.

< 5 × ✓: Kritischer Rückstand — sofortige Maßnahmen nötig, besonders BSI-Registrierung und Meldeprozess.

8. Fazit: Integration als strategische Entscheidung

NIS2 und ISO 27001 sind keine Alternativen — sie sind komplementär. ISO 27001 gibt Organisationen das methodische Handwerkszeug, das NIS2-Compliance strukturierbar und auditierbar macht. NIS2 gibt ISO-27001-ISMS die rechtliche Verbindlichkeit und die Operativität, die viele ISMS-Implementierungen bisher nicht hatten.

Die strategische Entscheidung für ein integriertes ISMS ist auch eine wirtschaftliche: Zwei parallele Compliance-Programme kosten mehr — in Ressourcen, Zeit und Aufmerksamkeit der Führung — als ein gut strukturiertes, erweitertes ISMS. Und sie produzieren häufig inkonsistente Sicherheitskulturen, weil Teams unterschiedliche Anforderungsquellen bedienen, anstatt ein gemeinsames Sicherheitsverständnis zu entwickeln.

Für Organisationen, die noch kein ISMS betreiben und von NIS2 betroffen sind: Der Aufbau eines ISO-27001-konformen ISMS ist der effizienteste Weg zur NIS2-Compliance — nicht nur für heute, sondern als strukturelle Investition in eine langfristig regulierungsfähige Sicherheitsarchitektur.

Drei Prioritäten für Compliance-Verantwortliche

1. NIS2-Sofortmaßnahmen jetzt umsetzen: BSI-Registrierung, Meldeprozess und GF-Governance dulden keinen Aufschub — sie gelten seit Dezember 2025.
2. Gap-Analyse vor Investitionsentscheidungen: Wer nicht weiß, welche 20–30 % fehlen, investiert möglicherweise in die falschen Bereiche.
3. Ein ISMS, zwei Anforderungsquellen: Integrierte Strukturen sind robuster, effizienter und auditfähiger als parallele Compliance-Programme.

Quellen & Weiterführende Dokumente

- Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates (NIS2-Richtlinie), 27.12.2022
- NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), in Kraft seit 06.12.2025 (BGBl. I)
- ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection
- ISO/IEC 27002:2022 — Information security controls (Leitfaden zu Anhang A)
- BSI: NIS2-Umsetzung, BSI-Meldeportal (MIP), bsi.bund.de
- ENISA: NIS2-Implementierungsleitfaden und Mapping zu Cybersicherheitsrahmenwerken
- SECJUR: NIS2 und ISO 27001 — Mapping, Lücken und Strategie, Mai 2026
- Viehoff Consult: NIS2 vs. ISO/IEC 27001, Dezember 2025
- OpenKRITIS: NIS2-Umsetzungsgesetz Deutschland — Rechtsrahmen und Anforderungen
- DataGuard: NIS2-ISO-27001-Mapping, 2025/2026

Über den Autor

Ralf Platvoet ist Diplom-Ökonom und Inhaber von PPI – Platvoet Performance Intelligence. Er berät Organisationen zu Cyber-Compliance (NIS2, DORA, EU Cyber Resilience Act, ISO 27001), Strategic Portfolio Management und PMO-Advisory. Sein Beratungsschwerpunkt liegt auf der Verknüpfung regulatorischer Anforderungen mit strategischer Steuerungsfähigkeit — für Industrieunternehmen, IT-Dienstleister und Finanzorganisationen.

Weitere Whitepapers, interaktive Tools und Ressourcen: **platvoet.org**

Haftungsausschluss