WHITEPAPER

NIS2 und ISO 27001

Cyber Compliance im Mittelstand

Regulatorische Pflicht, integriertes ISMS und ein praxisorientierter Weg zur Umsetzung

NIS2 ist seit Dezember 2025 in Deutschland geltendes Recht — ohne Übergangsfrist. ISO 27001 ist der etablierte internationale Standard für Informationssicherheits-Managementsysteme. Für den Mittelstand entscheidet sich hier, ob Cybersecurity als isolierte Pflichtübung oder als integrierter Baustein der Unternehmensführung behandelt wird. Dieses Whitepaper ordnet NIS2, ISO 27001 sowie die angrenzenden Regelwerke DORA und Cyber Resilience Act ein und zeigt einen konkreten Umsetzungspfad.

Autor	Ralf Platvoet, Diplom-Ökonom
Organisation	PPI – Platvoet Performance Intelligence
Stand	Juli 2026 (NIS2UmsuCG in Kraft seit 06.12.2025; ISO 27001:2022; DORA seit 17.01.2025; CRA seit 10.12.2024)
Themenbereich	Cyber-Compliance · Informationssicherheit · ISMS · Mittelstand

platvoet.org

Executive Summary

Zwei Regelwerke bestimmen aktuell die Cybersecurity-Agenda mittelständischer Unternehmen in Deutschland: die NIS2-Richtlinie, seit dem 6. Dezember 2025 durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) geltendes Recht, und ISO/IEC 27001:2022, der international anerkannte Standard für Informationssicherheits-Managementsysteme (ISMS). Beide verfolgen dasselbe Ziel — Informationssicherheitsrisiken systematisch zu managen und die Widerstandsfähigkeit gegen Cyberangriffe zu stärken —, unterscheiden sich jedoch fundamental in Rechtscharakter, Verbindlichkeit und Nachweisanforderungen.

Rund 29.500 Unternehmen in Deutschland fallen unter NIS2 — viele davon mittelständische Betriebe ohne etabliertes ISMS. Die gute Nachricht: Wer bereits nach ISO 27001:2022 zertifiziert ist, hat einen erheblichen Vorsprung. Ein reifes ISMS deckt Studien zufolge 70 bis 80 Prozent der NIS2-Anforderungen bereits ab. 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.

Für Finanzunternehmen und deren IKT-Dienstleister tritt mit DORA (Digital Operational Resilience Act) ein drittes, sektorspezifisches Regelwerk hinzu, das als Lex specialis gegenüber NIS2 gilt. Hersteller vernetzter Produkte müssen zusätzlich den EU Cyber Resilience Act beachten. Für die überwiegende Mehrheit der Mittelstandsunternehmen bleibt die zentrale Aufgabe jedoch dieselbe: ein integriertes ISMS aufbauen, das NIS2-Pflichten und ISO-27001-Struktur in einem einzigen Compliance-Fundament vereint.

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 Stunden), persönliche Geschäftsführerhaftung, Lieferkettenanforderungen und BSI-Registrierung.

Ein integriertes ISMS ist effizienter und robuster als zwei parallele Compliance-Programme.

DORA und der Cyber Resilience Act ergänzen das Bild für Finanzsektor bzw. Produkthersteller — mit eigenen, spezifischen Pflichten.

1. Warum Cyber-Compliance jetzt Chefsache ist

1.1 Der regulatorische Druck wächst

Digitale Transformation erweitert grundlegend die Angriffsfläche eines Unternehmens. Cloud-Migration, mobile Arbeitsformen, IoT-Einsatz und digitale Kundenkanäle schaffen jeweils neue Sicherheitsrisiken, die systematisch adressiert werden müssen. Gleichzeitig hat der Gesetzgeber auf europäischer Ebene in kurzer Folge mehrere Regelwerke geschaffen, die Cybersecurity von einer freiwilligen Best Practice zu einer gesetzlichen Pflicht mit persönlicher Verantwortung der Geschäftsführung machen.

Für den deutschen Mittelstand ist besonders die NIS2-Richtlinie relevant: Sie erweitert den Kreis betroffener Unternehmen erheblich gegenüber der Vorgängerregelung und erfasst nun auch viele Betriebe, die sich bislang nicht als kritische Infrastruktur verstanden haben.

1.2 Drei Regelwerke, ein gemeinsamer Nenner

Neben NIS2 prägen zwei weitere EU-Regelwerke die Cyber-Compliance-Landschaft: DORA für den Finanzsektor und der Cyber Resilience Act (CRA) für Hersteller vernetzter Produkte. Alle drei Regelwerke lassen sich mit einem gemeinsamen Fundament adressieren, wenn dieses systematisch nach ISO 27001 aufgebaut ist.

Regelwerk	Zielgruppe	Seit wann verbindlich	Verhältnis zu ISO 27001
NIS2 / NIS2UmsuCG	~29.500 Unternehmen in 18 Sektoren, ≥ 50 MA oder ≥ 10 Mio. € Umsatz	06.12.2025 (Deutschland)	70–80 % durch ein reifes ISMS abgedeckt
DORA (EU 2022/2554)	Finanzsektor: Banken, Versicherer, Wertpapierfirmen, Zahlungsinstitute + kritische IKT-Drittanbieter	17.01.2025	Komplementär; Anforderungen gehen über ISO 27001 hinaus, Lex specialis gegenüber NIS2
Cyber Resilience Act (EU 2024/2847)	Hersteller, Importeure und Händler von Produkten mit digitalen Elementen	10.12.2024 (schrittweise bis 12/2027)	Produktbezogen; ergänzt ein organisationsweites ISMS um Produktsicherheitsanforderungen
ISO/IEC 27001:2022	Alle Organisationen weltweit, freiwillig (skalierbar)	Aktuelle Version seit Oktober 2022	Strukturelles Fundament für NIS2-, DORA- und CRA-Compliance

Der Rest dieses Whitepapers konzentriert sich auf die für den Mittelstand wichtigste Kombination — NIS2 und ISO 27001 — und ordnet DORA sowie den CRA dort ein, wo sie für spezifische Unternehmenstypen zusätzlich relevant werden (Kapitel 6).

2. Die NIS2-Richtlinie im Überblick

2.1 Was ist NIS2?

NIS2 (Network and Information Security Directive 2, Richtlinie (EU) 2022/2555) ist die überarbeitete Fassung der ersten NIS-Richtlinie von 2016. Sie trat im Januar 2023 in Kraft und wurde in Deutschland durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) zum 6. Dezember 2025 in nationales Recht überführt — ohne Übergangsfrist. Ziel der Richtlinie ist ein hohes gemeinsames Cybersecurity-Niveau in der EU durch einheitliche Anforderungen an Risikomanagement, Incident Reporting und Unternehmensführung.

2.2 Wer ist betroffen?

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 Hochrisikosektoren	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

2.3 Die zehn Mindestmaßnahmen

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

- Risikoanalyse und Sicherheit der Informationssysteme
- Bewältigung von Sicherheitsvorfällen (Incident Management)
- Aufrechterhaltung des Betriebs, Backup-Management, Krisenmanagement, Business Continuity
- Sicherheit der Lieferkette (Supply Chain Security)
- Sicherheitsmaßnahmen beim Erwerb, der Entwicklung und Wartung von Netz- und Informationssystemen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Grundlegende Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrollen und Asset-Management
- Verwendung von Multi-Faktor-Authentifizierung (MFA)

2.4 Meldepflichten: der operative Kern von NIS2

Die Meldepflichten sind einer der operativ anspruchsvollsten Aspekte von NIS2. Der dreistufige Meldeprozess nach § 32 NIS2UmsuCG sieht vor:

Stufe	Frist	Inhalt
Frühwarnung	Innerhalb 24 Stunden nach Kenntnis	Erster Hinweis auf erheblichen Vorfall; Art und Ausmaß (soweit bekannt)
Erstmeldung / Zwischenbericht	Innerhalb 72 Stunden	Ersteinschätzung der Auswirkungen, Kompromittierungsindikatoren
Abschlussbericht	Innerhalb eines Monats	Vollständige Beschreibung, Ursachenanalyse, Gegenmaßnahmen, grenzüberschreitende Auswirkungen

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. Entscheidend: Ein Vorfall muss noch keinen Schaden verursacht haben, um meldepflichtig zu sein — das Schadenspotenzial reicht aus.

2.5 Geschäftsführerhaftung

Eine der gravierendsten Neuerungen von NIS2 gegenüber der Vorgängerrichtlinie 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. Bei Verstößen drohen persönliche Haftung und zeitweiser Ausschluss von Führungspositionen.

3. ISO 27001:2022 als Fundament

3.1 Struktur und Logik des ISMS

ISO 27001 definiert die Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) und 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 ist 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.

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 (37), Personell (8), Physisch (14), Technologisch (34)

3.2 Stärken und Grenzen von ISO 27001 gegenüber NIS2

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	✗ Lieferkettensicherheit weniger operativ als NIS2 Art. 21d
✓ HLS-Kompatibilität: Integration mit ISO 22301, ISO 9001 möglich	✗ Sektorspezifische Anforderungen (KRITIS) nicht abgedeckt
✓ Anhang A deckt breite Kontrollenlandschaft ab (93 Kontrollen)	✗ Registrierung beim BSI kein ISO-27001-Thema

3.3 Geschäftlicher Nutzen für den Mittelstand

Über die reine Compliance hinaus liefert ISO 27001 messbaren wirtschaftlichen Wert. Organisationen, die ein reifes ISMS betreiben, berichten von deutlich weniger Sicherheitsvorfällen, schnellerer Einhaltung von Datenschutzanforderungen und besserem Zugang zu Ausschreibungen, die eine Zertifizierung voraussetzen.

Nutzendimension	Typischer Effekt	Wert für das Unternehmen
Risikoreduktion	50–60 % weniger Sicherheitsvorfälle	Geringeres Schadensrisiko
Marktzugang	Relevant für ca. 70 % der Enterprise-Ausschreibungen	Neue Umsatzchancen
Kundenvertrauen	25–35 % höheres Vertrauen bei Kunden und Partnern	Markenschutz
Versicherung	10–20 % niedrigere Cyber-Versicherungsprämien	Direkte Kosteneinsparung

Die Zertifizierung erfordert typischerweise 9 bis 12 Monate von der Initiierung bis zum Zertifikat, mit vollem Return on Investment innerhalb von 18 bis 24 Monaten.

4. NIS2 × ISO 27001: Das Mapping

Die folgende Tabelle zeigt, welche NIS2-Anforderungsbereiche (Art. 21 NIS2 / § 30 BSIG) durch ISO-27001:2022-Kontrollen abgedeckt werden — und wo echte Lücken verbleiben.

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

NIS2-Anforderungsbereich	ISO 27001:2022 Kontrollen	Deckungsgrad
Persönliche Geschäftsführerhaftung	Kap. 5 (Leadership) — nur 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

Dieser Abschnitt beschreibt, was Mittelstandsunternehmen konkret tun müssen, um die im Mapping identifizierten 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, deren Umsetzung überwachen und sich regelmäßig selbst schulen lassen. Delegation enthaftet nicht.

Was zu tun ist: Formalen Beschluss der Geschäftsführung zur NIS2-Compliance dokumentieren, regelmäßige Schulungen der Geschäftsführung zu Cybersicherheitsthemen mit Nachweis, Berichterstattungsstruktur Geschäftsführung ↔ 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 sowie 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. Einordnung für Finanzunternehmen und Produkthersteller: DORA und der Cyber Resilience Act

Für die meisten Mittelstandsunternehmen ist die Kombination aus NIS2 und ISO 27001 ausreichend, um das eigene Compliance-Fundament zu beschreiben. Zwei Sondergruppen benötigen jedoch zusätzliche Aufmerksamkeit: Finanzunternehmen und ihre IKT-Dienstleister (DORA) sowie Hersteller vernetzter Produkte (Cyber Resilience Act).

6.1 DORA — Digital Operational Resilience Act für den Finanzsektor

DORA (Verordnung (EU) 2022/2554) ist seit dem 17. Januar 2025 vollumfänglich verbindlich und schafft einen einheitlichen Rechtsrahmen für die digitale operationale Resilienz im Finanzsektor. Er gilt für rund 20 Kategorien von Finanzunternehmen — Banken, Versicherer, Wertpapierfirmen, Zahlungsinstitute und weitere — sowie für IKT-Drittdienstleister, die als kritisch eingestuft werden (Critical Third-Party Providers, CTPPs).

DORA strukturiert seine Anforderungen in fünf Säulen: IKT-Risikomanagement, IKT-Vorfallmanagement & Meldepflichten, Testen der digitalen Betriebsstabilität (inklusive Threat-Led Penetration Testing), IKT-Drittparteienrisikomanagement und Informationsaustausch. Wie bei NIS2 trägt das Leitungsorgan — Vorstand und Aufsichtsrat — persönliche und nicht delegierbare Verantwortung für das IKT-Risikomanagement.

Entscheidend für Finanzunternehmen: DORA gilt als Lex specialis gegenüber NIS2 — das bedeutet, NIS2-Anforderungen sind für Finanzinstitute durch DORA vollständig abgedeckt. Eine separate NIS2-Implementierung ist für den Finanzsektor nicht erforderlich, sofern DORA vollständig umgesetzt ist. Gegenüber ISO 27001 gehen DORA-Anforderungen deutlich hinaus, insbesondere beim IKT-Informationsregister, den Drittparteienanforderungen und den verpflichtenden Resilienztests.

Für wen ist DORA relevant?

Kreditinstitute, Versicherungsunternehmen, Wertpapierfirmen, Zahlungs- und E-Geld-Institute, zentrale Gegenparteien und Krypto-Dienstleister (soweit MiCA-pflichtig).

IKT-Drittdienstleister, die kritische Funktionen für Finanzunternehmen erbringen (Cloud-Anbieter, Rechenzentren, Kernsoftware) — diese werden bei Einstufung als CTPP direkt von den europäischen Aufsichtsbehörden (EBA, EIOPA, ESMA) beaufsichtigt.

6.2 EU Cyber Resilience Act — Sicherheit für vernetzte Produkte

Der Cyber Resilience Act (CRA, Verordnung (EU) 2024/2847) ist die erste EU-Verordnung, die ein Mindestniveau an Cybersecurity für alle vernetzten Produkte auf dem EU-Markt festlegt. Er trat am 10. Dezember 2024 in Kraft und wird schrittweise bis Dezember 2027 vollständig anwendbar. Anders als NIS2 und DORA richtet sich der CRA nicht an Organisationen, sondern an Produkte: von Smartphones und Smart-Home-Geräten über Software und Cloud-Services bis zu industriellen Steuerungssystemen.

Der CRA verlangt einen Lebenszyklus-Ansatz — Hersteller müssen Sicherheit von Design bis End-of-Life gewährleisten, darunter sichere Standardkonfigurationen, Schwachstellenmanagement über mindestens fünf Jahre und eine Meldepflicht für aktiv ausgenutzte Schwachstellen binnen 24 Stunden ab dem 11. September 2026.

Für Mittelstandsunternehmen, die selbst vernetzte Hard- oder Software entwickeln oder vertreiben, kommt der CRA als zusätzliche, produktbezogene Compliance-Ebene zum organisationsweiten ISMS hinzu. Ein bestehendes ISO-27001-ISMS erleichtert die CRA-Umsetzung strukturell, deckt die produktspezifischen Anforderungen aus Annex I der Verordnung jedoch nicht automatisch ab.

Regelwerk	Bezugsebene	Betroffen ist Ihr Unternehmen, wenn …
NIS2	Organisation	Sie in einem der 18 kritischen Sektoren tätig sind und die Größenschwellen erreichen
DORA	Organisation (Finanzsektor)	Sie ein Finanzunternehmen sind oder kritische IKT-Dienste für solche erbringen
Cyber Resilience Act	Produkt	Sie Produkte mit digitalen Elementen herstellen, importieren oder vertreiben

7. 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.

7.1 Keine Doppelstrukturen

Der häufigste Fehler bei der Doppel-Compliance: Zwei separate Programme — eines für die ISO-27001-Zertifizierung, eines für die 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.

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.

7.2 Implementierungsreihenfolge nach Ausgangssituation

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-Bezug	ISO 27001 vollständig implementieren — NIS2-Abdeckung als Mehrwert kommunizieren	9–18 Monate

7.3 Die fünf Integrationsschritte

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

7.4 Zeitlicher Rahmen für die ISO-27001-Zertifizierung

Der Aufbau eines vollständigen ISMS bis zur Zertifizierung folgt typischerweise sechs Phasen und dauert insgesamt 9 bis 12 Monate:

Phase	Wichtigste Aktivitäten	Dauer
Initiierung	Executive Sponsorship, Scope-Definition, Gap-Analyse	4–6 Wochen
Risikobewertung	Asset-Inventar, Bedrohungsidentifikation, Risikobewertung	6–8 Wochen
Dokumentation	Richtlinien, Verfahren, Kontrollen, Statement of Applicability	8–12 Wochen
Implementierung	Kontrollen ausrollen, Schulung, Monitoring, Nachweissammlung	12–16 Wochen
Internes Audit	Interne Audits, Management-Review, Korrekturmaßnahmen	4–6 Wochen
Zertifizierung	Stage-1- & Stage-2-Audits, Feststellungen beheben, Zertifizierung	6–8 Wochen

8. 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 einziger 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.

9. 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 einem 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 Mittelstandsunternehmen, die noch kein ISMS betreiben und von NIS2 betroffen sind, gilt: 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, die auch DORA- oder CRA-Anforderungen als zusätzliche Bausteine aufnehmen kann, sobald diese relevant werden.

Drei Prioritäten für Compliance-Verantwortliche im Mittelstand

1. NIS2-Sofortmaßnahmen jetzt umsetzen: BSI-Registrierung, Meldeprozess und Geschäftsführungs-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, mehrere Anforderungsquellen: Integrierte Strukturen sind robuster, effizienter und auditfähiger als parallele Compliance-Programme — und bilden zugleich das Fundament, falls DORA oder der Cyber Resilience Act künftig relevant werden.

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)
- Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (DORA), 14.12.2022
- Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates (Cyber Resilience Act)
- Finanzmarktdigitalisierungsgesetz (FinmadiG), in Kraft seit 27.12.2024
- BSI: NIS2-Umsetzung, BSI-Meldeportal (MIP), bsi.bund.de
- BSI: Informationen zum Cyber Resilience Act, bsi.bund.de/EN/Themen/Cyber_Resilience_Act
- BaFin: DORA-Übersicht und Aufsichtsmitteilungen, bafin.de/dora
- ENISA: NIS2-Implementierungsleitfaden und Mapping zu Cybersicherheitsrahmenwerken
- EBA / EIOPA / ESMA: Regulatory Technical Standards (RTS) und Implementing Technical Standards (ITS) zu DORA, 2024
- IBM Security: Cost of a Data Breach Report
- SECJUR: NIS2 und ISO 27001 — Mapping, Lücken und Strategie, Mai 2026
- 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 den Mittelstand, Industrieunternehmen, IT-Dienstleister und Finanzorganisationen.

Weitere Whitepapers, interaktive Tools und Ressourcen: platvoet.org

Haftungsausschluss

Dieses Whitepaper dient ausschließlich allgemeinen Informationszwecken und stellt keine Rechts- oder Compliance-Beratung dar. Die Anforderungen aus NIS2, ISO 27001, DORA und dem Cyber Resilience Act sowie deren nationale Umsetzung unterliegen laufenden Konkretisierungen durch BSI, ENISA, BaFin und Gerichte. Für die individuelle Compliance-Beurteilung empfehlen wir die Einbindung qualifizierter Rechts- und Compliance-Berater.

