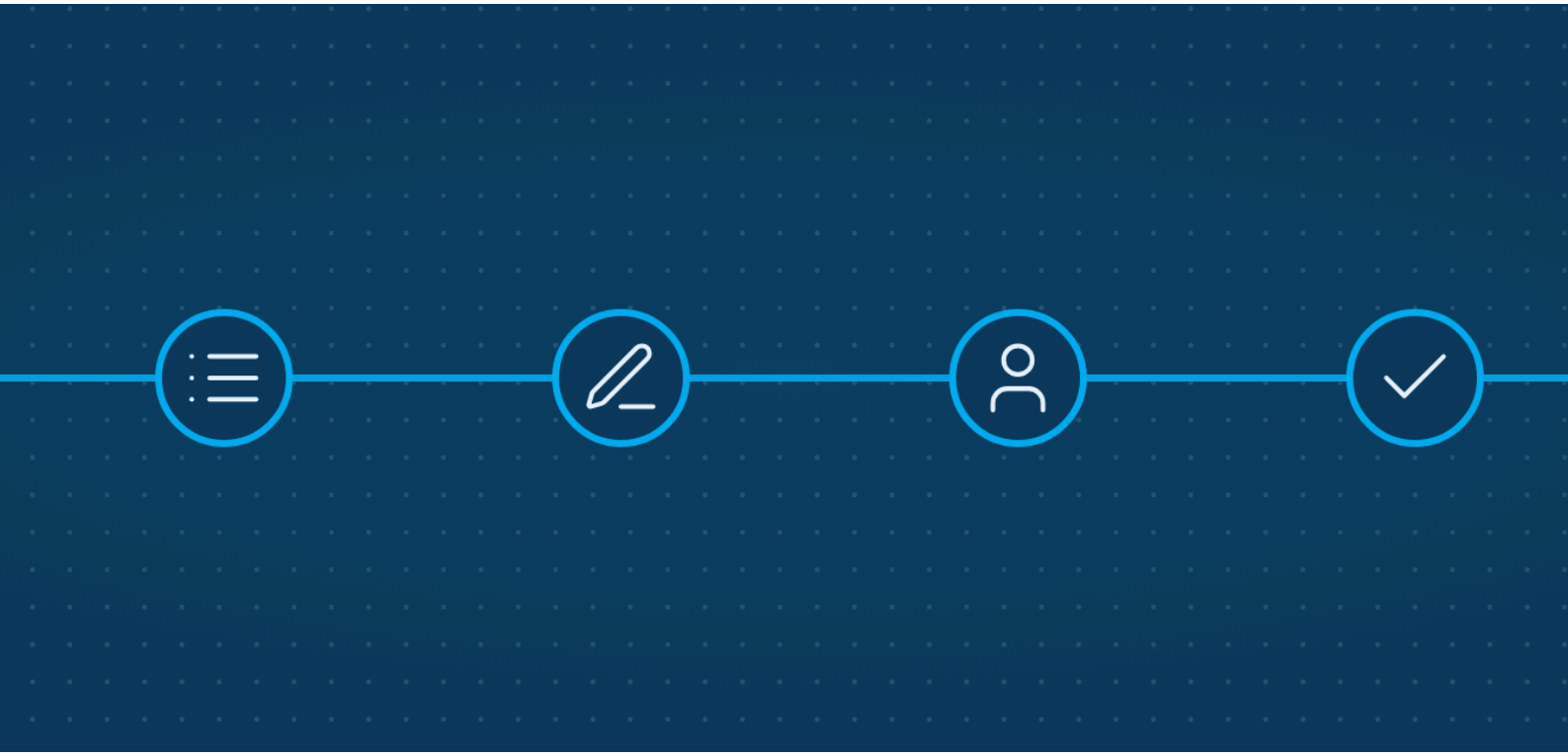
n-komm.
Unser IT Partner

Whitepaper

NIS2 und ISO 27001: Vom Pflichtenkatalog zum gelebten ISMS

Wie Sie Betroffenheit klären, Lücken schließen und Informationssicherheit nachweisbar steuern.



n-komm GmbH · Karlsruhe · Stand November 2026

Auf einen Blick

Wie Sie Betroffenheit klären, Lücken schließen und Informationssicherheit nachweisbar steuern.

- NIS2 ist eine EU-Richtlinie mit Pflichten für Unternehmen bestimmter Sektoren und Größen. ISO 27001 ist eine freiwillige internationale Norm mit Zertifizierung. Wer ein ISMS nach ISO 27001 aufbaut, erfüllt viele Anforderungen von NIS2 bereits.
- Am Anfang steht die Frage, ob NIS2 Ihr Unternehmen betrifft. Entscheidend sind Sektor und Größe; das Ergebnis sollten Sie schriftlich festhalten und rechtlich absichern lassen. Auch nicht betroffene Unternehmen spüren NIS2 oft als Lieferant.
- Eine Gap-Analyse vergleicht Ihren heutigen Stand mit den Anforderungen und ordnet die Lücken nach Risiko und Aufwand. Daraus entsteht ein Maßnahmenplan mit Reihenfolge, Kosten und Verantwortlichen.
- Das ISMS macht Informationssicherheit steuerbar: Risiken systematisch bewerten, Maßnahmen umsetzen, Richtlinien und Prozesse festlegen, Wirksamkeit prüfen. Die Geschäftsleitung muss die Maßnahmen billigen, ihre Umsetzung überwachen und selbst an Schulungen teilnehmen.
- Erhebliche Sicherheitsvorfälle müssen betroffene Unternehmen dem BSI melden, in mehreren Stufen und unter Zeitdruck. Klare Meldewege gehören deshalb vor den Ernstfall. Das Zertifikat nach ISO 27001 vergibt eine unabhängige Zertifizierungsstelle nach einem Audit.

Inhalt

1. Gesetz und Norm: Was NIS2 und ISO 27001 verbindet
2. Schritt 1: Die Betroffenheit klären
3. Schritt 2: Die Gap-Analyse als Fundament
4. Schritt 3: Das ISMS aufbauen und die Geschäftsleitung einbinden
5. Schritt 4: Vorfälle melden und das Zertifizierungsaudit bestehen
6. Wie die n-komm unterstützt
7. Checkliste: Auf dem Weg zum ISMS

01

Gesetz und Norm: Was NIS2 und ISO 27001 verbindet

Lange war IT-Sicherheit für viele Unternehmen freiwillig. Das hat sich geändert: Gesetze, Kunden und Versicherer verlangen heute, dass Unternehmen ihre Informationssicherheit nicht nur betreiben, sondern auch belegen können. Zwei Begriffe fallen dabei besonders oft: NIS2 und ISO 27001. Sie werden häufig in einem Atemzug genannt, sind aber grundverschieden.

NIS2 ist eine europäische Richtlinie für mehr Cybersicherheit. In Deutschland setzt das NIS2-Umsetzungsgesetz sie in nationales Recht um. Sie verpflichtet Unternehmen bestimmter Sektoren und Größen zu Sicherheitsmaßnahmen und Meldungen. Für betroffene Unternehmen ist NIS2 damit Pflicht, nicht Kür.

ISO 27001 ist eine internationale Norm für Informationssicherheit. Sie beschreibt, wie eine Organisation ein Managementsystem für Informationssicherheit aufbaut, kurz ISMS. Ein ISMS ist das Regelwerk aus Zuständigkeiten, Abläufen und Dokumenten, mit dem ein Unternehmen seine Informationssicherheit plant, umsetzt, überprüft und verbessert. Die Norm ist freiwillig, doch viele Kunden verlangen ein Zertifikat von ihren Lieferanten.

Der Zusammenhang liegt im Inhalt: NIS2 sagt, was betroffene Unternehmen erreichen müssen, etwa ein systematisches Risikomanagement, klare Meldewege und die Verantwortung der Geschäftsleitung. ISO 27001 liefert einen erprobten Rahmen dafür, wie sich solche Anforderungen dauerhaft im Unternehmen verankern lassen. Wer ein ISMS nach ISO 27001 aufgebaut hat, erfüllt viele Anforderungen von NIS2 bereits.

Wichtig ist aber auch die Grenze: Ein Zertifikat nach ISO 27001 ersetzt die gesetzlichen Pflichten aus NIS2 nicht. Die Registrierung beim BSI oder die Meldung erheblicher Vorfälle bleiben eigene Aufgaben. NIS2 selbst kennt kein eigenes Zertifikat. Wie die beiden Regelwerke sich unterscheiden, zeigt die Übersicht.

Für die Praxis heißt das: Sie müssen sich nicht zwischen Gesetz und Norm entscheiden. Viele Unternehmen nutzen ISO 27001 als Gerüst, um die Anforderungen aus NIS2 geordnet umzusetzen, und verbinden so Pflicht und Nachweis. Ob am Ende ein Zertifikat steht, ist eine eigene Entscheidung. Sie hängt vor allem davon ab, ob Kunden oder Ausschreibungen es verlangen und welchen Aufwand Sie dafür einplanen wollen.

	NIS2	ISO 27001
Was es ist	EU-Richtlinie, in deutsches Recht umgesetzt	Internationale Norm für Informationssicherheit
Für wen	Unternehmen vieler Branchen, nicht nur große	Alle Organisationen
Verbindlich?	Pflicht für betroffene Unternehmen	Freiwillig, aber von vielen Kunden verlangt
Kern	Risikomanagement, Meldepflichten, Verantwortung der Geschäftsleitung	Managementsystem für Informationssicherheit (ISMS)
Zertifikat	Kein eigenes Zertifikat	Durch eine unabhängige Zertifizierungsstelle

Kurz erklärt: BSI IT-Grundschutz

Neben ISO 27001 gibt es die Methode des Bundesamts für Sicherheit in der Informationstechnik (BSI). Der IT-Grundschutz beschreibt in Bausteinen sehr konkret, wie Sie typische Systeme und Abläufe absichern. Viele Behörden und Kommunen orientieren sich daran. Auf Basis von IT-Grundschutz ist ebenfalls eine Zertifizierung nach ISO 27001 möglich; das Zertifikat vergibt dann das BSI.

02

Schritt 1: Die Betroffenheit klären

Bevor Sie Maßnahmen planen, brauchen Sie eine belastbare Antwort auf die Frage, ob NIS2 Ihr Unternehmen betrifft. Davon hängt ab, welche Pflichten gelten und wie dringend einzelne Schritte sind. Viele Unternehmen sind unsicher, weil die Kriterien auf den ersten Blick abstrakt wirken.

Im Kern geht es um zwei Fragen: Gehört Ihr Unternehmen zu einem der Sektoren, die das Gesetz nennt? Und erreicht es eine bestimmte Größe? Treffen beide zu, gilt Ihr Unternehmen als „wichtige" oder „besonders wichtige Einrichtung" und muss die Pflichten aus NIS2 erfüllen. Einige Einrichtungen sind unabhängig von ihrer Größe erfasst, etwa Betreiber kritischer Anlagen.

Beim Sektor zählt, was Ihr Unternehmen tatsächlich tut, nicht wie es sich selbst bezeichnet. Die Sektoren reichen von Energie, Verkehr, Gesundheit und digitaler Infrastruktur bis zu Teilen des verarbeitenden Gewerbes wie dem Maschinenbau. Auch IT-Dienstleister wie Managed Service Provider und Anbieter von Cloud- und Rechenzentrumsdiensten gehören dazu. NIS2 gilt in vielen Sektoren schon für mittlere Unternehmen.

Bei der Größe kommt es auf die Zahl der Beschäftigten sowie auf Umsatz und Bilanzsumme an. Gehört Ihr Unternehmen zu einer Gruppe, können die Zahlen verbundener Unternehmen eine Rolle spielen. Eine erste Orientierung gibt die Betroffenheitsprüfung auf der Website des BSI.

Gehen Sie die Prüfung strukturiert an und beteiligen Sie die richtigen Personen. Die Geschäftsführung kennt die Tätigkeitsfelder und die Struktur der Gruppe, die Buchhaltung liefert Beschäftigtenzahlen, Umsatz und Bilanzsumme aus dem letzten Jahresabschluss, die IT-Leitung weiß, welche Dienste das Unternehmen für Kunden erbringt. Erst das Zusammenspiel ergibt ein vollständiges Bild.

Halten Sie Ihr Ergebnis und die Begründung schriftlich fest, auch wenn Sie nicht betroffen sind. Bei Zweifeln klären Sie die Frage mit Ihrer Rechtsberatung, denn die Einordnung ist eine rechtliche Bewertung. Prüfen Sie erneut, wenn Ihr Unternehmen wächst, ein neues Geschäftsfeld dazukommt oder sich die Unternehmensgruppe ändert.

Für öffentliche Einrichtungen gelten eigene Regeln. Ob und wie NIS2 für Landesbehörden und Kommunen gilt, regeln die Länder; erste Ansprechpartnerin ist die zuständige Landesbehörde. Einen machbaren Einstieg in die Informationssicherheit bietet dort häufig der BSI IT-Grundschutz mit der Basis-Absicherung.

- Welche Ihrer Tätigkeiten fallen in einen der Sektoren, die das BSI-Gesetz nennt?
- Erreicht Ihr Unternehmen die Größenschwellen bei Beschäftigten oder bei Umsatz und Bilanzsumme?
- Gehört Ihr Unternehmen zu den Einrichtungen, die unabhängig von der Größe erfasst sind?

- Gehört Ihr Unternehmen zu einer Gruppe, deren Zahlen mitzählen können?
- Welche Ihrer Kunden fallen unter NIS2 und werden Nachweise von Ihnen verlangen?

Nicht betroffen, aber trotzdem gefragt

Auch wer selbst nicht unter NIS2 fällt, spürt das Gesetz oft als Lieferant. Betroffene Unternehmen müssen die Sicherheit ihrer Lieferkette prüfen und schicken Fragebögen oder verlangen Nachweise. Ein Zertifikat nach ISO 27001 zeigt, dass Sie Informationssicherheit systematisch steuern.

03

Schritt 2: Die Gap-Analyse als Fundament

Steht fest, welche Anforderungen gelten, folgt die Bestandsaufnahme. Eine Gap-Analyse vergleicht den heutigen Stand Ihrer Informationssicherheit mit den Anforderungen aus NIS2 und, falls Sie eine Zertifizierung anstreben, aus ISO 27001. Das englische Wort „Gap“ steht für Lücke: Die Analyse zeigt, was schon da ist und was fehlt.

Eine gute Gap-Analyse betrachtet Technik und Organisation gleichermaßen. Auf der technischen Seite geht es etwa um Netzwerk, Firewall, Server und Clients, Patchstand, Active Directory, Berechtigungen und Datensicherung, dazu Cloud-Dienste und Microsoft 365. Auf der organisatorischen Seite stehen Zuständigkeiten, Richtlinien, Abläufe für Vorfälle, Schulungen und der Umgang mit Dienstleistern.

Viele Unternehmen sind weiter, als sie denken. Oft gibt es bereits eine funktionierende Datensicherung, einen Endpoint-Schutz oder Regeln für Berechtigungen, nur fehlt die Dokumentation oder die regelmäßige Überprüfung. Die Gap-Analyse macht sichtbar, welche Maßnahmen nur noch nachgewiesen werden müssen und wo tatsächlich etwas fehlt.

Entscheidend ist die Priorisierung. Nicht jede Lücke ist gleich wichtig, und nicht alles lässt sich auf einmal schließen. Ordnen Sie die Lücken nach Risiko und Aufwand: Was schützt Ihr Unternehmen am stärksten, was ist schnell umgesetzt, was braucht einen längeren Vorlauf? Aus dieser Ordnung entsteht der Maßnahmenplan.

Ein Bereich wird in Gap-Analysen leicht übersehen: die Dienstleister. Wer betreut Ihre Server, Ihre Cloud-Dienste, Ihre Fachanwendungen? Welche Zugänge haben diese Firmen, und was ist vertraglich zur Sicherheit vereinbart? NIS2 verlangt ausdrücklich die Absicherung der Lieferkette. Eine Liste der wichtigen Dienstleister mit ihren Zugängen und Zuständigkeiten ist deshalb ein guter erster Schritt.

Ein Maßnahmenplan legt Reihenfolge, Kosten und Verantwortliche fest. Er ist das zentrale Steuerungsinstrument für die folgenden Monate und die Grundlage, auf der die Geschäftsleitung Budget und Personal freigibt. Ein ISO-27001-Projekt muss dabei nicht alles auf einmal leisten: Viele Maßnahmen bringen auch ohne Zertifikat mehr Sicherheit.

Bewährt hat sich ein Vorgehen in Etappen. Zuerst kommen Maßnahmen, die mit überschaubarem Aufwand viel Schutz bringen, etwa aktuelle Updates, eine geschützte Datensicherung und die Mehr-Faktor-Anmeldung für Fernzugänge und Administratorkonten. Parallel beginnt der Aufbau der Organisation mit Zuständigkeiten und Risikobewertung. Größere Vorhaben wie ein zentrales Monitoring oder die Neuordnung von Berechtigungen folgen nach Plan. So sehen Geschäftsleitung und Beschäftigte früh Ergebnisse, und das Projekt behält seinen Schwung.

- Ergebnis 1: eine Zusammenfassung für die Geschäftsleitung, die Stand und größte Risiken verständlich darstellt.

- Ergebnis 2: eine Bewertung je Anforderung, ob sie erfüllt, teilweise erfüllt oder offen ist.
- Ergebnis 3: ein priorisierter Maßnahmenplan mit Reihenfolge, Kosten und Verantwortlichen.

04

Schritt 3: Das ISMS aufbauen und die Geschäftsleitung einbinden

Das ISMS ist der Kern, der aus einzelnen Maßnahmen ein steuerbares Ganzes macht. Es beginnt mit dem Anwendungsbereich: Welche Standorte, Abteilungen, Systeme und Prozesse sollen erfasst werden? Für die Zertifizierung nach ISO 27001 legen Sie diesen Geltungsbereich verbindlich fest. Er sollte groß genug sein, um aussagekräftig zu sein, und klein genug, um ihn beherrschen zu können.

Das Herzstück ist das Risikomanagement. Sie erfassen, welche Informationen und Systeme für Ihr Geschäft wichtig sind, welche Bedrohungen und Schwachstellen bestehen und wie groß das Risiko jeweils ist. Danach entscheiden Sie, wie Sie mit jedem Risiko umgehen: es durch Maßnahmen verringern, es vermeiden, es übertragen oder es bewusst tragen. NIS2 verlangt ebenfalls, Risiken systematisch zu erfassen und geeignete technische, organisatorische und operative Maßnahmen umzusetzen.

Zu diesen Maßnahmen gehören etwa Zugriffskontrollen, Datensicherung, Verschlüsselung und die Absicherung der Lieferkette. ISO 27001 enthält in ihrem Anhang einen Katalog möglicher Maßnahmen. In einer Erklärung zur Anwendbarkeit halten Sie fest, welche davon für Sie gelten, welche nicht und warum. Dieses Dokument ist eine der wichtigsten Grundlagen für das spätere Audit.

Richtlinien und Prozesse machen die Maßnahmen verbindlich. Eine übergeordnete Leitlinie zur Informationssicherheit beschreibt Ziele und Verantwortung; darunter regeln Richtlinien etwa den Umgang mit Passwörtern, Berechtigungen, mobilen Geräten, Datensicherung und Dienstleistern. Gute Richtlinien sind kurz, verständlich und beschreiben, was im Alltag tatsächlich passiert. Ein ISMS, das nur auf dem Papier existiert, besteht kein Audit und schützt auch nicht.

Damit das ISMS nicht neben dem Tagesgeschäft verkümmert, braucht es klare Zuständigkeiten. Üblich ist eine benannte Person, die das ISMS koordiniert, Risiken nachhält und Berichte für die Geschäftsleitung erstellt, häufig als Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter bezeichnet. Diese Rolle braucht Zeit, Rückhalt und einen direkten Draht zur Geschäftsleitung. Die Fachabteilungen bleiben trotzdem für die Risiken in ihren Prozessen verantwortlich.

Auch beim Dokumentieren lohnt Augenmaß. Die Norm verlangt Nachweise, aber keine Papierberge. Was im Alltag gelebt wird, lässt sich oft mit vorhandenen Werkzeugen belegen, etwa mit Tickets, Protokollen, Berechtigungsübersichten oder Berichten aus der Datensicherung. Entscheidend ist, dass Dokumente aktuell sind und jemand für ihre Pflege zuständig ist.

Die Geschäftsleitung spielt dabei eine aktive Rolle. Unter NIS2 muss sie die Maßnahmen billigen, ihre Umsetzung überwachen und selbst an Schulungen teilnehmen. NIS2 macht IT-Sicherheit damit zur Chefsache. Auch ISO 27001 verlangt, dass die oberste Leitung Ziele setzt, Ressourcen bereitstellt und das ISMS regelmäßig bewertet.

Für die Geschäftsleitung bedeutet das vor allem, die richtigen Fragen zu stellen und Entscheidungen bewusst zu treffen. Welche Risiken sind die größten? Welche nehmen wir bewusst in Kauf, und warum? Wie steht es um die Umsetzung des Maßnahmenplans? Ein kurzer, regelmäßiger Bericht zur Informationssicherheit in der Führungsrunde schafft hier Klarheit. Eine Management-Schulung vermittelt, welche Pflichten NIS2 der Geschäftsleitung auferlegt und wie sie die Umsetzung im Unternehmen steuert.

Ein ISMS lebt vom Kreislauf aus Planen, Umsetzen, Prüfen und Verbessern. Interne Audits zeigen, ob die Regeln eingehalten werden; die Managementbewertung zieht Bilanz und setzt neue Schwerpunkte. Technische Tests wie Penetrationstests belegen, ob die Maßnahmen gegen echte Angriffe wirken. Ihre Berichte dienen zugleich als Nachweis gegenüber Auditoren und Kunden.

- Anwendungsbereich festlegen: Standorte, Abteilungen, Systeme und Prozesse.
- Risiken erfassen und bewerten, Entscheidungen zur Behandlung dokumentieren.
- Maßnahmen auswählen und in der Erklärung zur Anwendbarkeit begründen.
- Leitlinie und Richtlinien schreiben, verständlich und alltagstauglich.
- Rollen und Zuständigkeiten benennen, die Geschäftsleitung schulen.
- Beschäftigte regelmäßig sensibilisieren, als fortlaufender Prozess statt einmaliger Schulung.
- Wirksamkeit prüfen: interne Audits, Managementbewertung, technische Tests.

05

Schritt 4: Vorfälle melden und das Zertifizierungsaudit bestehen

Ein Sicherheitsvorfall ist kein Zeitpunkt für Grundsatzfragen. Unter NIS2 müssen betroffene Unternehmen erhebliche Sicherheitsvorfälle dem BSI melden. Die Meldung erfolgt in mehreren Stufen und unter Zeitdruck. Deshalb brauchen Sie klare Abläufe, bevor etwas passiert.

Ein Meldeprozess beantwortet vorab die entscheidenden Fragen: Wer erkennt einen Vorfall, und wer bewertet, ob er erheblich ist? Wer informiert die Geschäftsleitung, wer bereitet die Meldung vor, wer gibt sie ab? Welche Informationen werden gesammelt, und wo werden sie dokumentiert? Je nach Vorfall sind zusätzlich andere Stellen zu informieren, etwa die Datenschutzaufsicht.

Technische Analyse und Meldung greifen ineinander. Die IT oder ein Dienstleister liefert die Analyse, die Dokumentation und einen technischen Vorfallsbericht. Die rechtliche Bewertung und die Meldung selbst bleiben beim Unternehmen und seiner Rechtsberatung. Üben Sie den Ablauf einmal durch, etwa in einer Planübung am Tisch. So zeigen sich Lücken, solange noch kein Druck herrscht.

Nach jedem Vorfall lohnt ein Blick zurück: Was hat funktioniert, wo hat es gehakt, welche Maßnahme hätte den Vorfall verhindert oder früher erkannt? Diese Erkenntnisse fließen in die Risikobewertung und den Maßnahmenplan zurück. So wird aus einem Ernstfall eine Verbesserung des ISMS, wie es auch ISO 27001 vorsieht.

Wer sich nach ISO 27001 zertifizieren lassen will, schließt den Aufbau mit dem Zertifizierungsaudit ab. Das Zertifikat vergibt eine unabhängige Zertifizierungsstelle, nicht der Berater, der beim Aufbau geholfen hat. Das Audit läuft in der Regel zweistufig: Zuerst prüfen die Auditoren, ob die Dokumentation des ISMS vollständig und schlüssig ist. Danach prüfen sie vor Ort oder remote, ob das ISMS im Alltag tatsächlich gelebt wird und wirkt.

Planen Sie das Audit rechtzeitig. Zertifizierungsstellen brauchen Vorlauf, und Ihr ISMS sollte vor dem Audit eine Weile im Betrieb sein, damit es Nachweise aus dem Alltag gibt. Hilfreich ist ein Vorab-Check, der die Unterlagen und einige Abläufe so prüft, wie es die Auditoren später tun. Benennen Sie außerdem für jeden Bereich Ansprechpartner, die im Audit Auskunft geben können.

Gut vorbereitet sind Sie, wenn Anwendungsbereich, Risikobewertung, Erklärung zur Anwendbarkeit und Richtlinien vorliegen, interne Audits und eine Managementbewertung stattgefunden haben und die Beteiligten ihre Rollen kennen. Abweichungen, die im Audit festgestellt werden, sind kein Scheitern: Sie werden dokumentiert und mit Korrekturmaßnahmen behoben. Nach der Zertifizierung prüft die Zertifizierungsstelle in regelmäßigen Überwachungsaudits, ob das ISMS weiter wirkt.

Kurz erklärt: Registrierung beim BSI

Betroffene Unternehmen müssen sich beim BSI registrieren. Wer betroffen ist und sich noch nicht registriert hat, sollte sich zeitnah darum kümmern. Die Registrierung ist aber nur der erste Schritt: Danach zählen Risikomanagement, Schutzmaßnahmen und klare Meldewege.

06

Wie die n-komm unterstützt

Die n-komm GmbH aus Karlsruhe ist seit 2000 IT-Partner für Unternehmen und Verwaltungen, als Familienunternehmen in zweiter Generation. Wir sind selbst nach ISO/IEC 27001 zertifiziert und kennen den Weg zum Zertifikat aus eigener Erfahrung. Die meisten Aufgaben rund um NIS2 und ISO 27001 erledigt unser eigenes Cyber-Security-Team.

Im Erstgespräch klären wir mit Ihnen, welche Regelwerke Sie betreffen können. Die rechtliche Bewertung der Betroffenheit erfolgt mit spezialisierten Partnern; für rechtliche Detailfragen empfehlen wir zusätzlich eine Rechtsberatung. In der Gap-Analyse vergleichen wir Ihren Stand mit den Anforderungen und priorisieren die Lücken nach Risiko und Aufwand. Den Maßnahmenplan legen wir mit Ihnen fest, mit Reihenfolge, Kosten und Verantwortlichen.

Auf Wunsch bauen wir mit Ihnen ein ISMS mit Risikomanagement, Richtlinien und klaren Prozessen auf. Wir bereiten Sie auf das Audit nach ISO 27001 vor, auch auf Basis von IT-Grundschutz, und begleiten Sie durch die Zertifizierung. Das Zertifikat vergibt eine unabhängige Zertifizierungsstelle oder beim IT-Grundschutz das BSI. Wir schulen Ihre Geschäftsleitung zu ihren Pflichten unter NIS2 und helfen bei der Registrierung beim BSI.

Damit Informationssicherheit nicht an der Technik hängen bleibt, trainieren wir auf Wunsch auch Ihre Beschäftigten, mit Security Awareness Trainings als fortlaufendem Prozess. Betrieb und Monitoring Ihrer Sicherheitstechnik können Sie als Managed Security an uns abgeben.

Technische Maßnahmen wie Endpoint-Schutz, Firewalls, Datensicherung und SIEM setzen wir selbst um. Ob sie wirken, prüfen unsere eigenen Pentester mit Penetrationstests und automatisierten Tests; die Berichte dienen als Nachweis. Im Ernstfall analysieren wir den Vorfall und bereiten die Meldung an das BSI mit Ihnen vor. Die Meldung selbst geben Sie ab, und die rechtliche Bewertung bleibt bei Ihnen und Ihrer Rechtsberatung.

Unser Team bringt langjährige Praxis in technischer und organisatorischer Informationssicherheit mit, dazu anerkannte fachliche Qualifikationen. Beratung und Technik kommen so aus einer Hand.

Checkliste: Auf dem Weg zum ISMS

- [ ] Haben Sie geprüft, ob NIS2 Ihr Unternehmen betrifft, und das Ergebnis mit Begründung schriftlich festgehalten?
- [ ] Wissen Sie, welche Ihrer Kunden unter NIS2 fallen und welche Nachweise sie von Ihnen erwarten?
- [ ] Ist Ihr Unternehmen beim BSI registriert, falls es betroffen ist?
- [ ] Liegt eine aktuelle Gap-Analyse vor, die Technik und Organisation abdeckt?
- [ ] Gibt es einen Maßnahmenplan mit Reihenfolge, Kosten und Verantwortlichen?
- [ ] Ist der Anwendungsbereich Ihres ISMS festgelegt?
- [ ] Werden Risiken systematisch erfasst, bewertet und die Entscheidungen dokumentiert?
- [ ] Hat die Geschäftsleitung die Maßnahmen gebilligt und an einer Schulung teilgenommen?
- [ ] Ist festgelegt, wer einen erheblichen Sicherheitsvorfall bewertet, dokumentiert und meldet?
- [ ] Prüfen Sie die Wirksamkeit Ihrer Maßnahmen regelmäßig, etwa mit internen Audits und Penetrationstests?

Welche Regeln gelten für Ihr Unternehmen?

Im kostenlosen Erstgespräch klären wir gemeinsam, welche Regelwerke für Sie gelten und wo Sie stehen. Sie erfahren, welche nächsten Schritte sinnvoll sind. 30 Minuten per Teams oder Telefon, unverbindlich. Dieses Whitepaper ersetzt keine Rechtsberatung.

Kostenloses Erstgespräch vereinbaren

---

n-komm GmbH · Karlsruhe
Tel. +49 721 35 46 00 · info@n-komm.de
n-komm.de/cyber-security/compliance/

n-komm.
Unser IT Partner

Stand November 2026. Dieses Whitepaper gibt einen fachlichen Überblick und ersetzt keine individuelle Beratung und keine Rechtsberatung. © n-komm GmbH