GRASP
German GRC

NIS2 PLAYBOOK INKL. CHECKLIST

NIS2 im Mittelstand: Das Playbook für Organisation, Tempo und Nachweise

Einführung

Dass Sie dieses Playbook angefragt haben, lässt nur zwei Schlüsse zu: Entweder wissen Sie bereits, dass Sie von NIS2 betroffen sind oder Sie vermuten es. In beiden Fällen ist dieses Playbook Ihr Startpunkt, denn *machen ist besser als wollen*.

NIS2 ist ein bisschen wie eine neue Verkehrsordnung. Allerdings tauscht niemand die Schilder aus. Betroffene Unternehmen müssen selbst prüfen, ob sie auf dieser Straße fahren dürfen. Sind Sie NIS2-pflichtig, beginnt ein klarer Parcours: **Registrierung**, Meldewege festzurren, Verantwortlichkeiten klären, Risiken steuern, Nachweise führen.

Dieses Playbook zeigt, wie Sie das elegant und praxistauglich organisieren. Ganz ohne Bürokratie-Marathon, aber mit genug Struktur, um vor Prüfern und Management zu bestehen.

Bedenken Sie außerdem: Die Behörden sehen bei NIS2 eine persönliche Haftung der Geschäftsführung vor. Daher sollte Cybersicherheit als integraler Bestandteil der Unternehmensstrategie betrachtet werden und nicht als nachgelagerte oder an die IT ausgelagerte Funktion. NIS2 ist Chef-Sache.

Das bedeutet auch, dass Ihre Geschäftsführung Hilfe annehmen sollte. Etwa Beratungsdienstleitungen oder zumindest Awareness-Schulungen. Man erwartet von der Geschäftsführung, dass sie sich bestens mit dem Thema NIS2 auskennt.

Tipp: Falls Sie doch noch unsicher sind: Prüfen Sie die Schwellenwerte genau. Viele produzierende Unternehmen und Dienstleister fallen erstmals unter den Geltungsbereich. Die Realität: Viele Organisationen sind noch nicht vorbereitet. Mit diesem Playbook erhöhen Sie die Chance, frühzeitig compliant und nachweisfähig zu werden.

Wenn Sie mehr über uns erfahren wollen, besuchen Sie **grasp-grc.com**.

Was sind die Herausforderungen und Chancen von NIS2?

Die Umsetzung ist anspruchsvoll. Besonders bei mehreren Standorten und Ländern mit unterschiedlichen Behörden und Meldewegen. Falls Sie in der Vergangenheit schon Strukturen für Incident-Management, Risikosteuerung und Nachweise aufgebaut haben – wunderbar. Sie sollten diese aber zumindest aktualisieren und ausbauen.

Ein kritischer Punkt ist die Supply-Chain-Security: Verträge und Lieferantenprüfungen sind enger zu verzahnen. Im produzierenden Gewerbe verlangen Schnittstellen zwischen Betriebstechnologie (Operational Technology, OT) und Informationstechnik (IT) besondere Aufmerksamkeit.

Gleichzeitig bietet NIS2 Chancen: Wer früh startet, stärkt die Cyber-Resilienz, reduziert Haftungsrisiken und schafft Wettbewerbsvorteile durch nachvollziehbare Sicherheit. Ein Plus für Kunden, Partner und Investoren.

So gehen Sie konkret vor

1. **Betroffenheit klären (sicher ist sicher):** Selbsttest starten (Essential, Important oder aktuell nicht im Anwendungsbereich).
2. **Governance aktivieren:** Steuerungsgremium einberufen. Charter und RASCI freigeben.
3. **Meldefähigkeit sicherstellen:** Incident-SOPs (24 h/72 h/30 Tage) finalisieren. Tabletop in 60 Minuten üben.
4. **Risiko und Business Continuity starten:** Risikoregister mit Top-10 füllen. BIA in 3–5 Schlüsselbereichen beginnen.
5. **KPI-Regelkreis etablieren:** Monatsreport mit Zielen MTTR < 8 Stunden, Patch-SLA ≥ 95 %, BIA-Abdeckung ≥ 60 %.
6. **Excel oder dezidierte NIS2-Software?** Checkliste ausfüllen. Bei Upgrade-Triggern auf Software wechseln (Automationen, Audit-Trail, Rollen, Mehr-Standort).

1. Betroffenheit klären (sicher ist sicher):

Zur Sicherheit: Sind Sie überhaupt im Scope? Das BSI stellt den verbindlichsten Selbstcheck. Unter diesem Link finden Sie ihn: **BSI Betroffenenprüfung**

Hintergrund: Von NIS1 zu NIS2

Die erste NIS-Richtlinie (2016) betraf vor allem kritische Infrastrukturen. Mit NIS2 wird der Kreis deutlich erweitert: 18 Sektoren, aufgeteilt in wesentliche Einrichtungen (Essential Entities) und wichtige Einrichtungen (Important Entities).

- **Wesentliche Einrichtungen:** in der Regel ab 250 Mitarbeitenden oder > 50 Mio. € Umsatz
- **Wichtige Einrichtungen:** in der Regel ab 50 Mitarbeitenden oder > 10 Mio. € Umsatz

2. Governance aktivieren

Wer macht was? Das minimalistische Aufbauteam

Den Takt gibt ein monatlich tagendes NIS2-Steuerungsgremium vor:
- Geschäftsführung
- Leitung Informationssicherheit (Chief Information Security Officer, CISO) und BCM
- Leitungen aus IT und OT sowie Rechtsabteilung/Compliance.

Das Gremium stimmt Prioritäten, Budgets, akzeptierte Risikohöhe und Berichtsfreigaben ab. In den Fachbereichen benennen Sie Risikoverantwortliche (Risk Owner), die Risiken ins Register eintragen, Maßnahmen planen und den Fortschritt berichten. Die Rechtsabteilung behält zuständige Behörden und Meldekanäle im Blick, besonders, wenn mehrere EU-Länder betroffen sind. Das BCM führt die Business-Impact-Analyse, erstellt BCP und IT-DR und verankert die Verantwortung bewusst im Fachbereich, nicht nur in der IT.

Artefakte für den Start
- Sicherheitsleitlinie
- RASCI-Matrix (Responsible, Accountable, Support, Consulted, Informed)
- Risikoregister plus Behandlungsplan
- Standardarbeitsanweisungen für Sicherheitsvorfälle (Incident-SOPs)
- Unterlagen zu BIA/BCP/IT-DR
- Lieferanten-Due-Diligence (Risikoprüfung kritischer Dienstleister)
- Reporting-Kalender

Die vier Säulen des Betriebssystems Ihrer NIS2-Organisation

Vier Zahnräder tragen alles, was Sie tun: Risikomanagement, Verantwortung der Leitung (Corporate Accountability), Meldepflichten, Betriebsfähigkeit (Business Continuity). Wenn diese greifen, läuft der Rest deutlich eleganter.

1. Risikomanagement: Vom Bauchgefühl zur Prioritätenliste

Erfassen Sie Risiken dort, wo Arbeit passiert: in Prozessen, Anwendungen, Standorten, Lieferketten. Bewerten Sie Auswirkung und Wahrscheinlichkeit auf einer einfachen Skala (z. B. 1–5), planen Sie Maßnahmen mit verantwortlichen Personen und verbindlichen Terminen. Beginnen Sie mit Bereichen mit dem höchsten Risiko. Entscheidend ist nicht die perfekte Zahl, sondern der Takt: monatlich Status aktualisieren und berichten.

Praktisch bedeutet das: Bevor Sie Maßnahmen ergreifen, müssen Sie die relevanten Risiken systematisch ermitteln und bewerten: Wo entstehen heute Ausfälle, Datenverluste oder Angriffsflächen? Welche Prozesse und Assets sind kritisch, welche Lieferanten „single point of failure"? Erst wenn Eintrittswahrscheinlichkeit und Auswirkung pro Risiko eingeschätzt sind, wählen Sie wirksam passende Gegenmaßnahmen – sonst schießen Sie leicht an den wahren Ursachen vorbei.

Auf dieser Basis starten Sie mit schnellen, risikogerechten Maßnahmen: Wenn die Analyse etwa ein hohes Risiko seitlicher Bewegung von Angreifern zeigt, segmentieren Sie das Netz. Wenn die Folgen eines Datenverlusts kritisch sind, testen Sie konsequent Ihre Backups und Wiederherstellungszeiten. Wenn Fehlkonfigurationen die Verfügbarkeit bedrohen, prüfen Sie Änderungen zuerst in der Testumgebung. Wenn die Abhängigkeit von einem Anbieter groß ist, sichern Sie einen zweiten Lieferanten. Vergeben Sie klare Zuständigkeiten mit Terminen und prüfen Sie den Fortschritt monatlich (Kennzahlen, Statusberichte). So sinken die größten, zuvor identifizierten Risiken sichtbar und nachweisbar – mit Fokus auf das, was Ihre Organisation wirklich gefährdet.

2. Corporate Accountability: Das ist Chefsache, keine Fußnote

Die Geschäftsleitung braucht Klarheit, Takt, Nachweise. Richten Sie einen Monatsbericht ein (Risiken, Maßnahmen, Kennzahlen) und kurze Pflichtschulungen für Führungskräfte. Freigaben werden im Report dokumentiert. Das schafft Aufmerksamkeit und Tempo.

3. Reportings

Bauen Sie eine kleine Meldefabrik: Vorlagen, Freigabepfade, Behördenkontakte. Wenn etwas passiert, müssen alle wissen, wer was wann freigibt und wo gemeldet wird – national wie international. Üben Sie das quartalsweise in 60 Minuten (Tabletop).

4. Business Continuity: Was zählt, wenn's brennt

Starten Sie mit einer knappen Business-Impact-Analyse (BIA) für die wichtigsten Prozesse:

- Wie lange dürfen Sie ausfallen (Recovery Time Objective, RTO)?
- Wie alt dürfen Ihre Daten sein (Recovery Point Objective, RPO)?

Daraus entstehen Business-Continuity-Pläne (BCP), IT-Desaster-Recovery-Pläne (IT-DR) und praktische Workarounds. Ein Wiederherstellungstest pro Jahr gehört zur Grundhygiene.

Betriebssystem für NIS2

3. Meldefähigkeit sicherstellen

Pflichten und Sanktionen:
Das dreistufige Melderegime

Sobald ein Sicherheitsvorfall auftritt, müssen Sie diesen zwingend melden. Meldepflichtige Sicherheitsvorfälle nach NIS-2 betreffen „besonders wichtige“ und „wichtige“ Einrichtungen sowie Betreiber kritischer Anlagen. Diese Unternehmen müssen erhebliche Vorfälle unverzüglich an das BSI melden.

Dabei ist wichtig: Schnelligkeit geht vor Vollständigkeit. Nach Registrierung in der gemeinsamen Meldestelle von BSI und BBK können berechtigte Personen der Einrichtung (oder beauftragte Dienstleister) melden. Das BSI bestätigt den Eingang spätestens nach 24 Stunden, stellt bei Bedarf Rückfragen, leitet Informationen zur Lagebewertung weiter, warnt ggf. Dritte in auf das Notwendigste reduzierter Form.

Wo?
Meldungen laufen heute bereits über das Melde- und Informationsportal (MIP) des BSI. Das ist erreichbar unter dem offiziellen BSI-Portal (Login/Registrierung), und es wird auch für NIS-2 genutzt bzw. weiterentwickelt: **LINK**

Wann und wie?
1. Innerhalb von 24 Stunden (Frühwarnung)
2. Nach 72 Stunden (Zwischenbericht)
3. Innerhalb von 30 Tagen Abschlussbericht (Ursache, Maßnahmen).

Und wenn Sie es verheimlichen?
Bei Verstößen drohen Bußgelder (wesentliche Einrichtungen bis 10 Mio. € oder 2 % Umsatz, wichtige Einrichtungen bis 7 Mio. € oder 1,4 %). Neu ist, dass Geschäftsführungen bei Pflichtverletzungen temporär von Führungsfunktionen ausgeschlossen werden können.

Praxis-Tipp:
Legen Sie jetzt Meldewege und Vorlagen fest. Im Ernstfall zählt jede Minute.

Der 90-Tage-Plan: Von null auf auditfähig (light)

Tage 0–30 **Grundlage legen (Outcomes)**

- Stellen Sie das Steuerungsgremium zusammen. Geben Sie Charter und RASCI frei → Governance steht.
- Erfassen Sie zuständige Behörden und Meldekanäle je Land → Kontaktliste komplett.
- Legen Sie die Risiko-Methodik fest, legen Sie ein Risikoregister an. Bewerten Sie die Top-10-Risiken → Register live.

Tage 31–60 **Meldefähigkeit und Resilienz (Outcomes)**

- Finalisieren Sie die Meldekommunikation (Schritt-für-Schritt für 24 h / 72 h / 30 Tage). Klären Sie Freigaben → Meldung geübt.
- Starten Sie die BIA in 3–5 Schlüsselbereichen. Definieren Sie Workarounds → BCM-Fähigkeit sichtbar.
- Identifizieren Sie kritische Anbieter. Starten Sie eine Due-Diligence (light) → Transparenz steigt.

Tage 61–90 **Nachweis und Takt (Outcomes)**

- Etablieren Sie den Monatsreport ans Management (Risiken, Maßnahmen, KPIs) → Regelkreis aktiv.
- Setzen Sie eine Tabletop-Übung an (60–90 Min.). Terminieren Sie einen Wiederherstellungstest → Praxisnachweis geplant.
- Konsolidieren Sie die 6–12-Monats-Roadmap (Lücken schließen, Lieferanten-Kontrollen ausrollen) → Plan fix.

4. Risikomanagement und Business Continuity starten

NIS2-Kern: Risikomanagement

Ziel ist es, Risiken systematisch zu erkennen, zu bewerten und so zu behandeln, dass der Betrieb sicher und regelkonform bleibt.

- **Risikobewertung:** Sie identifizieren relevante Risiken und schätzen Eintrittswahrscheinlichkeit sowie Auswirkungen unter Ihren konkreten Rahmenbedingungen.
- **Risikobehandlung:** Sie entscheiden, welche Maßnahmen Sie ergreifen (vermeiden, vermindern, übertragen oder akzeptieren), in welchem Umfang und bis wann.
- **Risikoaggregation:** Sie führen alle Risiken zusammen, um Trends, Häufungen und Prioritäten zu erkennen.
- **Risikoregister:** Sie pflegen eine zentrale Liste aller wesentlichen Risiken inklusive Bewertung, Maßnahmen, Verantwortlichen und Terminen – für Steuerung und Nachverfolgung.
- **Risikoüberwachung:** Sie überwachen regelmäßig die Wirksamkeit der Maßnahmen und aktualisieren die Bewertungen.
- **Risikokommunikation:** Sie berichten verständlich an alle relevanten Stakeholder (Management, IT, Fachbereiche), damit Entscheidungen fundiert getroffen werden.

Damit Ihr Betrieb läuft: Business Continuity Management (BCM)

BCM stellt sicher, dass Ihre kritischen Leistungen auch bei Störungen schnell wieder verfügbar sind.

- **Kritische Prozesse & Ressourcen:** Sie legen fest, welche Prozesse geschäftskritisch sind und welche IT, Personen und Standorte benötigt werden.
- **Ziele für Wiederanlauf:** Sie definieren klare Zielzeiten (RTO/RPO) und berücksichtigen Abhängigkeiten.
- **Strategien & Notfallpläne:** Sie nutzen praxisnahe Playbooks für typische Szenarien (z. B. Ransomware, Lieferantenausfall, Standortstörung) – mit Rollen, Entscheidungen und Kommunikationswegen.
- **Übungen & Tests:** Sie führen regelmäßige Tabletop-Übungen und Wiederherstellungstests durch, um Lücken früh zu erkennen.
- **Integration mit Risikomanagement:** Sie lassen Erkenntnisse aus Incidents und Tests ins Risikoregister zurückfließen; Maßnahmen werden priorisiert und nachgehalten.
- **Kontinuierliche Verbesserung:** Sie halten Ihr BCM über Lessons Learned, KPI-Reviews und regelmäßige Updates aktuell und wirksam.

5. KPI-Regelkreis etablieren

Alltagstauglich steuern: Rhythmus und Kennzahlen

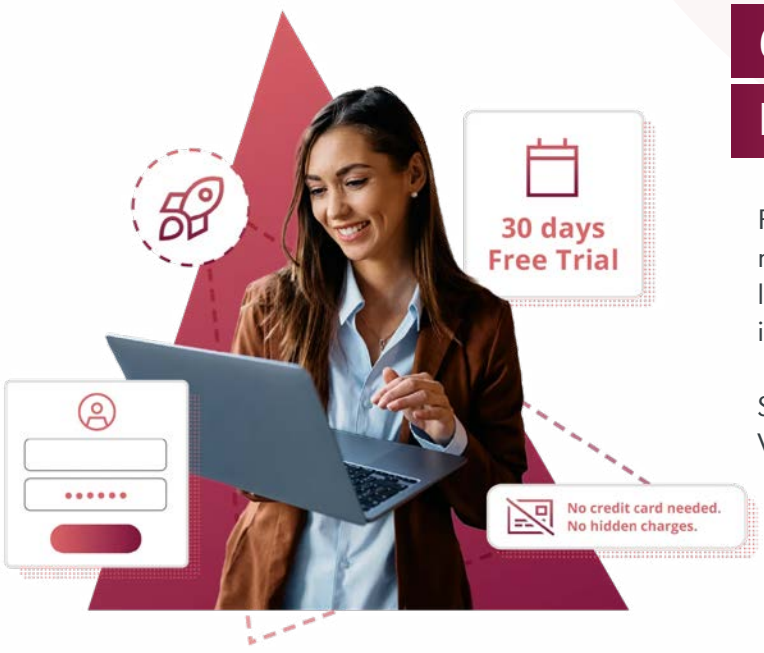
Kadenzen: wöchentlich 30-min-Sync Risiko/Incidents, monatlich Steering-Report, quartalsweise Übung/DR-Test plus Lieferanten-Review.

KPIs mit Start-Schwellenwerten:

- Mean Time to Detect/Recover (MTTD/MTTR) – **Ziel** nach Übung: MTTR < 8 Stunden
- Patch-SLA-Quote – **Ziel:** mindestens 95 % sicherheitsrelevante Updates fristgerecht
- Offene Hochrisiken – **Ziel:** minus 50 % in 90 Tagen (gegen Baseline Monat 1)
- BIA-Abdeckung – **Ziel:** mindestens 60 % der kritischen Prozesse in 90 Tagen
- Anteil geprüfter kritischer Lieferanten – **Ziel:** mindestens 70 % mit Due-Diligence in 6 Monaten

Mehrere Länder oder Einheiten

Koordinieren Sie Behördenkontakte zentral, passen Sie Vorlagen lokal an. Eine einheitliche Meldefabrik (Templates, Checklisten, Freigaben) spart Zeit. Dabei bleiben juristische Feinheiten je Land möglich. Für Konzerne: globales Grundmuster, lokale Add-ons.



6. Excel oder dezidierte NIS2-Software?

Falls Sie an dieser Stelle unsicher sind, ob Sie all das mit einer Excel-Liste auf dem SharePoint machen wollen, oder doch eine dezidierte NIS2-Software sinnvoll ist – füllen Sie unsere Checkliste aus.

Sie können **GRASP German GRC** auch als Free Trial-Version ausprobieren.