ORBIT
IT-SOLUTIONS

Erleben. Vernetzen. Wachsen.
Impulse für Ihr Business von morgen.

EXPERIENCE DAY 2026

Experience Day 2026

Impulse für Ihr Business von morgen.

15:45 Uhr Start Masterclasses	• Vom Wissens-Flaschenhals zum 24/7-Berater: In wenigen Schritten zum eigenen KI-Agenten im Kundenservice	Championshall | Raum 1
	• Infrastruktur mit Rückgrat: Souveränes Datacenter-Management meets Modern Workplace	Salon | Raum 2
	• Schluss mit „Bauchgefühl" & Pipeline-Märchen, wie KI Ihren Vertrieb schonungslos ehrlich macht	Kurt-Brumme-Saal | Raum 3
ca. 16:15 Uhr	• Impuls zu KI-Use Case	
	• Besprechung und Aufbereitung der eingereichten Use Case	
	• danach Pause bis ca. 17:15 Uhr	
17:15 Uhr Start Masterclasses	• Mehr als M365: Der sichere Weg in den KI gestützten Modern Workplace	Championshall | Raum 1
	• Offline arbeiten, live dokumentieren: Das Geheimnis nahtloser Außendienst-Prozesse	Salon | Raum 2
	• NIS2 in der Praxis umsetzen	Kurt-Brumme-Saal | Raum 3
ca. 18:00 Uhr	• Keynote durch Steven Nicolin | Microsoft	Championshall | Raum 1

NIS-2 in der Praxis umsetzen

Erfahrungsbericht & Best Practice

Dr. Uwe Alkemper
Head of Cyber Security

ORBIT IT-SOLUTIONS

Experience Day 2026
Masterclass Session 2

NIS-2 und ORBIT Timeline

A – Inkrafttreten der ersten NIS-Richtlinie (2016)

B – Formales Inkrafttreten der EU NIS-2-Richtlinie (16.01.2023)

C – Zertifiziert NIS-2 Directive Senior Lead Implementer (23.06.2024)

D – Seit 12.07.2024 LinkedIn NIS-Reality-Check zu NIS2UmsuCG

E – Seit 08.08.2024 ORBIT-Blog NIS-2 Pflichten, Umsetzung & Kosten

F – Seit Q3-2024 Durchführung von NIS-2 Gap-Analysen

G – DE NIS2UmsuCG (NIS-2-Umsetzungs- und Cybersicherheitsgesetz)

Seit Q3-2024 Begleitung von Kunden bei Umsetzung von Maßnahmen aus NIS-2 Gap-Analysen

H – Frist für Umsetzung in nationales Recht (17.10.2024)

I – Verkündet und in Kraft getreten (05.12.2025)

J – Ablauf der Frist zur Registrierung (06.03.2026)

NIS-2 begleitet unsere Kunden und damit auch ORBIT seit 18 Monaten

Dr. Uwe Alkemper
Head of Cyber Security
uwe.alkemper@orbit.de
+49 175 7276379

Theorieteil

NIS-2-Umsetzungs- und Cybersicherheitsgesetz (Zahlen, Daten & Fakten)

Beweggründe für die NIS-2 Direktive

Einheitlich hohes Cybersicherheitsniveau in der EU

Stärkung der Resilienz gegen Cyberangriffe

Schutz kritischer Sektoren vor wirtschaftlichen Schäden

Verbindliche Sicherheitsmaßnahmen (z. B. Risiko- & Lieferkettenmanagement)

Verschärfte Meldepflichten bei Sicherheitsvorfällen

Klare Verantwortung und Haftung der Geschäftsführung

NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz

NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz

Einordung und Erfüllungsaufwand

Einordnung

- Referentenentwurf zum Gesetz enthält Folgen für die Wirtschaft
- Zahlen zum Schaden durch Cybercrime
- Budgets für den Erfüllungsaufwand in der Wirtschaft

Erfüllungsaufwand

- Gesamterfüllungsaufwand für die Wirtschaft beträgt 2,3 Mrd. €
- Davon 2,2 Mrd. € einmaliger Aufwand
- 2,8 Mio. € entfallen auf Bürokratie-kosten und Informationspflichten

Der einmalige Aufwand für die Wirtschaft beträgt 2,2 Mrd. € Aufwand

Link zum Referentenentwurf vom 23.6.2025:
https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-RefE_2025.html

Lagebericht

Schadensvolumen laut Studie von Bitkom e. V.

- Ø Cyber-Schaden DE: ~210 Mrd. €/Jahr (Bitkom)
- Ø Schaden pro Unternehmen: ~500.000 €
- Potenzial durch NIS-2: signifikante Reduktion (Modellannahme ~50 %)
- Basis: Unternehmen ≥10 MA (≈444.000)

Der Wert von NIS-2 wird im Mittel mit 250.000 € je Unternehmen beziffert

Größte Bedrohungen in der aktuellen „Zeitenwende“

- Distibuted-Denial-of-Service-Angriffe
- Cyber-Sabotage-Angriffe
- Lieferketten-Angriffe
- Ransomware-Angriffe

Quelle: Referentenentwurf des Bundesministeriums des Innern und für Heimat für das Gesetz zur Umsetzung der NIS-2-Richtlinie vor (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) vom 23. Juni 2025

Quelle: Bitkom, Wirtschaftsschutz 2025 – Schäden durch Cyberangriffe in Deutschland

Erwartete Fallzahlen und Aufwand je Unternehmen

Zum Stichtag am 6. März waren rund 11.500 Einrichtungen (der angenommenen 29.850) beim BSI registriert

Wichtige Unternehmen

21.600 Unternehmen sind vorrausichtlich klassifiziert, davon sind

3.700 (17%) bereits heute gut gegen Cyberangriffe aufgestellt, verbleiben

17.900 wichtige Unternehmen

Aufwand je Unternehmen

1.100 Stunden Zeitaufwand

24.300 € Sachaufwand

Besonders wichtige Unternehmen

8.250 Unternehmen sind vorrausichtlich klassifiziert, davon sind

4.693 Anbieter digitaler Dienste & Betreiber kritischer Anlagen (bereits ohne NIS2 betroffen), verbleiben

3.550 Unternehmen, davon sind

600 (17%) bereits heute gut gegen Cyberangriffe aufgestellt, verbleiben

2.950 Besonders wichtige Unternehmen in der Aufwandkalkulation des Referentenentwurfs

Aufwand je Unternehmen

2.752 Stunden Zeitaufwand

60.700 € Sachaufwand

Quelle: Referentenentwurf des Bundesministeriums des Innern und für Heimat für das Gesetz zur Umsetzung der NIS-2-Richtlinie vor (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) vom 23. Juni 2025

Kosten (Ø) für wichtiges Unternehmen

Summe	Berechnung	Kostenart
57.530 €	1.100 h (52,30 €/h)	Zeitaufwand
24.300 €	24.300 €	Sachkosten
1,668 €	5 x 4 h (58,40 €/h) + 500 €	Schulung Leitende Angestellte
3.630 €	100 x 1 h (36,30 €/h)	Schulung Mitarbeitende
19 €	0,5 h (36,30 €/h)	Registrierung
58 €	1,0 h (58,40 €/h)	Meldung
87.205 €	Gesamtkosten	

65% der Gesamtkosten entfallen demnach auf die „Einführung und Anpassung digitaler Prozessabläufe“

Annahmen (Kalkulation)

- Durchschnittliches wichtiges Unternehmen, mit
- 10 leitende Beschäftigte (50% sind bereits geschult)
- 200 Beschäftigte (50% sind bereits geschult)

Praxisteil

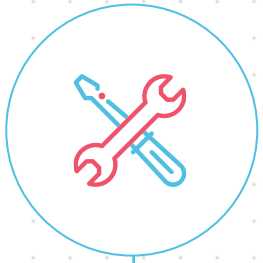
Praktisches Vorgehen und Erfahrungen

Wie sieht ein einfacher Masterplan zu NIS-2 aus?

NIS-2 Betroffenheit

- Kriterien zur Betroffenheit (Sektor, Größe) prüfen (lassen)
- Einstufung als „wichtiges", „besonders wichtiges" oder Kritis-Unternehmen dokumentieren
- Registrierung bei BSI-Portal durchführen

1



NIS-2 Gap-Analyse

- Kick-off / Abschluss-Meeting
- Bereitstellung Austauschplattform
- Dokumentationslage prüfen
- Nachweise prüfen / validieren
- Remote / On-Site Workshop
- Bericht erstellen

2

Abweichungen beheben

- Richtlinien erstellen
- Technische Maßnahmen planen
- Prozesse dokumentieren
- IT-Betrieb (Security) unterstützen

3

Awareness / Schulung

- NIS-2 und Information Security Schulung erstellen
- Mitarbeiterschulung durchführen
- Management briefen

4

NIS-2 ready

5

1 Howto: NIS-2 Betroffenheit prüfen

Betroffenheit prüfen

Quelle: https://betroffenheitspruefung-nis-2.bsi.de/

Begründung (Doku)

z.B. E-Mail

Unternehmensgröße

- Für die NIS-2 Betroffenheit ist die Unternehmensgröße relevant.
- Wenn Sie weniger als 50 Mitarbeitende haben und außerdem Ihr Umsatz- Bilanzvolumen unter 50 Mio. € liegen, dann sind Sie nicht von NIS-2 betroffe
- Dies gilt jeweils für das einzelne Unternehmen (juristische Person) sowie für verbundene Unternehmen.
- Nach unserem Gespräch gehe ich davon aus, dass Ihre Mitarbeiterzahl im Bereich von 50-250 Mitarbeitenden liegt.
- Damit ist das Größenkritierium erfüllt, unabhängig von Umsatz/Bilanzvolumen. D.h. vo der Größe her sind Sie betroffen.

Formale NIS2-Einstufung

- Die Betroffenheit nach NIS-2 ergibt sich auch aus der Zuordnung zu bestimmten Sektoren, die in den Anlagen der Richtlinie definiert sind und unter anderem auf Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU verweisen.
- Nach unserem Gespräch gehe ich davon aus, dass Sie definitiv zu „Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU“ zählen. Zu Ihren Leistungen gehören Rettungsdienst, der Betrieb von Praxen, Vorsorge usw.

Gesamtergebnis der Prüfung

Unter Berücksichtigung der oben genannten Punkte ergibt sich folgende Einschätzung:

- Eines oder mehrere Unternehmen (juristische Person) in Ihrer Gruppe zählen zu den Sektoren von wichtigen und besonders wichtigen Einrichtungen im Bereich „Gesundheit“ des NIS-2 Gesetzes
- Eines oder mehrere dieser Unternehmen haben eine Mitarbeiterzahl von mehr als 50 und weniger als 250 Mitarbeitenden
- Aus unserer Sicht sind diese Tochterunternehmen von der NIS2-Regulierung betroffen und zählen zu der Gruppe der „wichtigen Unternehmen“.
- Wenn die Mitarbeiterzahl über 250 liegt, dann zählen sie zu der Gruppe der „besonders wichtigen Unternehmen.

Ergebnis

- Sektor NIS-2 relevant ✓
- Mitarbeiter / Umsatz / Bilanz ✓
- Wichtiges Unternehmen ✓
- Besonders wichtiges Unt. ✗
- Registrierung erforderlich ✓

1 Howto: Registrierung beim BSI

Unternehmenskonto ELSTER

Wie erstelle ich Mein Unternehmenskonto?

1 **Beantragung**

Beantragen Sie ein oder mehrere ELSTER-Organisationszertifikate unter „Benutzerkonto erstellen". Halten Sie hierfür Ihre betriebliche Steuernummer bereit. Sollten mehrere ELSTER-Organisationszertifikate für mehrere Mitarbeitende beantragt werden, empfiehlt sich die Einrichtung einer Zentralen Stelle.

2 **Aktivierungsdaten per E-Mail**

Sie erhalten sodann die grundlegenden Aktivierungsdaten per E-Mail an die im Antrag hinterlegte E-Mail-Adresse.

3 **Aktivierungsbrief per Post**

Zusätzlich wird ein Aktivierungsbrief per Post an die bei der Steuerverwaltung hinterlegte Unternehmensadresse geschickt. Die Zustellung dauert in der Regel ca. 5 Werktage.

4 **Zertifikatsdatei generieren**

Wenn beides bei der Zentralen Stelle oder dem zuständigen Mitarbeitenden vereint ist, ist den Anweisungen aus der E-Mail innerhalb der dort gesetzten Frist zu folgen, um die Zertifikatsdatei als Download zu erhalten. Diese kann im Anschluss für den Login an digitalen Verwaltungsleistungen genutzt werden.

Quelle: https://info.mein-unternehmenskonto.de/

Anmeldung BSI-Portal

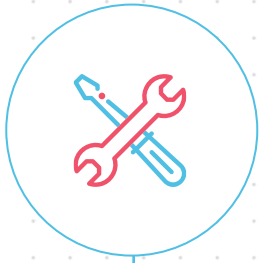
Quelle: https://portal.bsi.bund.de/

Masterplan – Schritt 2

NIS-2 Betroffenheit

- Kriterien zur Betroffenheit (Sektor, Größe) prüfen (lassen)
- Einstufung als „wichtiges", „besonders wichtiges" oder Kritis-Unternehmen dokumentieren
- Registrierung bei BSI-Portal durchführen

1



NIS-2 Gap-Analyse

- Kick-off / Abschluss-Meeting
- Bereitstellung Austauschplattform
- Dokumentationslage prüfen
- Nachweise prüfen / validieren
- Remote / On-Site Workshop
- Bericht erstellen

2

Abweichungen beheben

- Richtlinien erstellen
- Technische Maßnahmen planen
- Prozesse dokumentieren
- IT-Betrieb (Security) unterstützen

3

Awareness / Schulung

- NIS-2 und Information Security Schulung erstellen
- Mitarbeiterschulung durchführen
- Management briefen

4

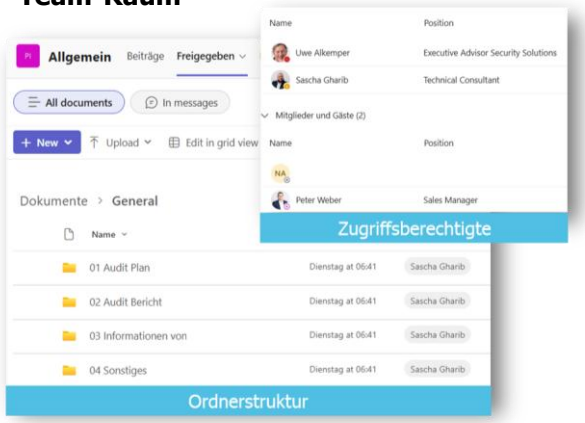
NIS-2 ready

5

2 Standard-Vorgehen Gap-Analyse

Kickoff

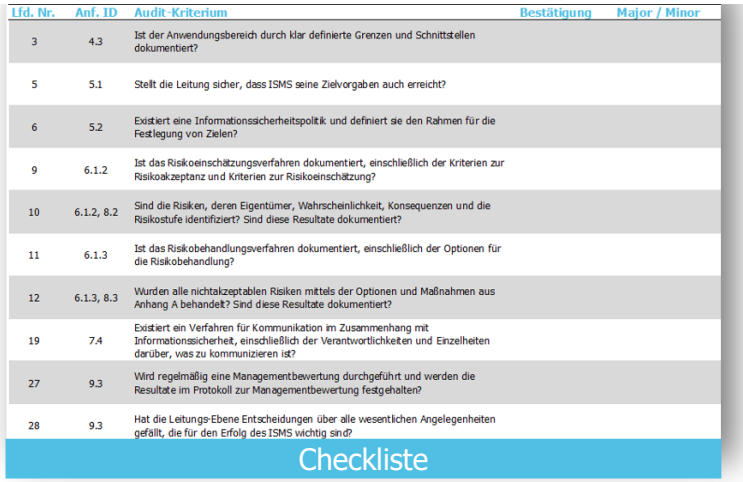
Team-Raum



Zeitplan

Audit

- Dokumente prüfen
- Begehung
- Interviews
- Stichproben / Validierung



Lfd. Nr.	Anf. ID	Audit-Kriterium	Bestätigung	Major / Minor
3	4.3	Ist der Anwendungsbereich durch klar definierte Grenzen und Schnittstellen dokumentiert?		
5	5.1	Stellt die Leitung sicher, dass ISMS seine Zielvorgaben auch erreicht?		
6	5.2	Existiert eine Informationssicherheitspolitik und definiert sie den Rahmen für die Festlegung von Zielen?		
9	6.1.2	Ist das Risikoeinschätzungsverfahren dokumentiert, einschließlich der Kriterien zur Risikoakzeptanz und Kriterien zur Risikoeinschätzung?		
10	6.1.2, 8.2	Sind die Risiken, deren Eigentümer, Wahrscheinlichkeit, Konsequenzen und die Risikostufe identifiziert? Sind diese Resultate dokumentiert?		
11	6.1.3	Ist das Risikobehandlungsverfahren dokumentiert, einschließlich der Optionen für die Risikobehandlung?		
12	6.1.3, 8.3	Wurden alle nichtakzeptablen Risiken mittels der Optionen und Maßnahmen aus Anhang A behandelt? Sind diese Resultate dokumentiert?		
19	7.4	Existiert ein Verfahren für Kommunikation im Zusammenhang mit Informationssicherheit, einschließlich der Verantwortlichkeiten und Einzelheiten darüber, was zu kommunizieren ist?		
27	9.3	Wird regelmäßig eine Managementbewertung durchgeführt und werden die Resultate im Protokoll zur Managementbewertung festgehalten?		
28	9.3	Hat die Leitungs-Ebene Entscheidungen über alle wesentlichen Angelegenheiten gefällt, die für den Erfolg des ISMS wichtig sind?		

Checkliste

Bericht (Erfüllung)

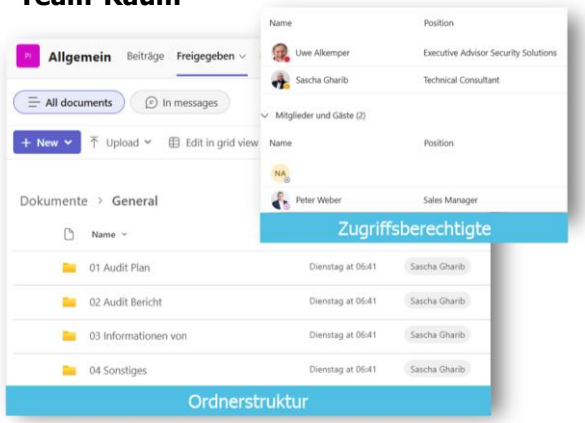
- Erfüllungsgrad (Gaps)
- Handlungsempfehlung (priorisiert)

NIS2 Anforderung	Erfüllungsgrad
3.3. UMGANG MIT SICHERHEITSVORFÄLLEN	0
3.4. AUFRECHTERHALTUNG DES BETRIEBS	0
3.7. KRISENMANAGEMENT	0
3.13. BEWERTUNG DER WIRKSAMKEIT VON RISIKOMANAGEMENTMAßNAHMEN	0
3.16. SICHERHEIT DES PERSONALS	0
3.1. RISIKOANALYSE	1
3.8. SICHERHEIT DER LIEFERKETTE	1
3.9. SICHERHEITSMAßNAHMEN BEIM ERWERB VON IT-SYSTEMEN	1
3.12. MANAGEMENT UND OFFENLEGUNG VON SCHWACHSTELLEN	1
3.14. SENSIBILISIERUNG UND VERMITTLUNG GRUNDLEGENDER VERFAHREN DER CYBERHYGIENE	1

2 Standard-Vorgehen Gap-Analyse

Kickoff

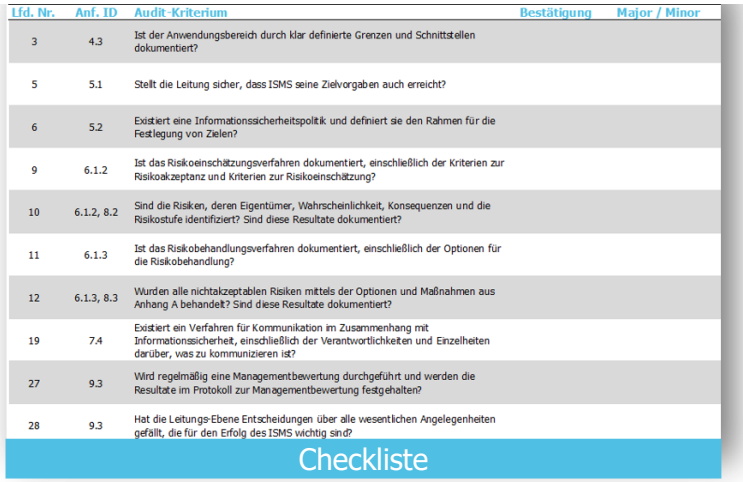
Team-Raum



Zeitplan

Audit

- Dokumente prüfen
- Begehung
- Interviews
- Stichproben / Validierung



Lfd. Nr.	Anf. ID	Audit-Kriterium	Bestätigung	Major / Minor
3	4.3	Ist der Anwendungsbereich durch klar definierte Grenzen und Schnittstellen dokumentiert?		
5	5.1	Stellt die Leitung sicher, dass ISMS seine Zielvorgaben auch erreicht?		
6	5.2	Existiert eine Informationssicherheitspolitik und definiert sie den Rahmen für die Festlegung von Zielen?		
9	6.1.2	Ist das Risikoeinschätzungsverfahren dokumentiert, einschließlich der Kriterien zur Risikoakzeptanz und Kriterien zur Risikoeinschätzung?		
10	6.1.2, 8.2	Sind die Risiken, deren Eigentümer, Wahrscheinlichkeit, Konsequenzen und die Risikostufe identifiziert? Sind diese Resultate dokumentiert?		
11	6.1.3	Ist das Risikobehandlungsverfahren dokumentiert, einschließlich der Optionen für die Risikobehandlung?		
12	6.1.3, 8.3	Wurden alle nichtakzeptablen Risiken mittels der Optionen und Maßnahmen aus Anhang A behandelt? Sind diese Resultate dokumentiert?		
19	7.4	Existiert ein Verfahren für Kommunikation im Zusammenhang mit Informationssicherheit, einschließlich der Verantwortlichkeiten und Einzelheiten darüber, was zu kommunizieren ist?		
27	9.3	Wird regelmäßig eine Managementbewertung durchgeführt und werden die Resultate im Protokoll zur Managementbewertung festgehalten?		
28	9.3	Hat die Leitungs-Ebene Entscheidungen über alle wesentlichen Angelegenheiten gefällt, die für den Erfolg des ISMS wichtig sind?		

Checkliste

Bericht (Empfehlung)

- Erfüllungsgrad (Gaps)
- Handlungsempfehlung (priorisiert)

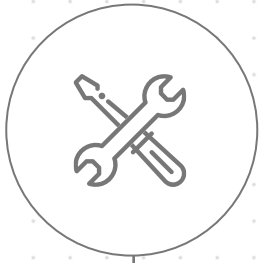
Empfehlung zu 3.1 – Risikoanalyse

Aus Sicht des Audit-Teams deckt die Skala der Eintrittswahrscheinlichkeit mit mindestens einem Ereignis / Jahr als maximale Häufigkeit nicht vollständig den Bereich von häufigen Ereignissen ab. Es gibt Ereignisse, die auch monatlich, wöchentlich oder häufiger eintreten können. Auch der Bereich der Schadenhöhe scheint für minimalen Schaden nicht weit genug formuliert zu sein. Es wird daher empfohlen die beiden Skalen (Eintrittswahrscheinlichkeit und Schadenhöhe) und Stufen noch einmal zu überdenken und anzupassen, so dass die Skalen Bereiche wie 1/Woche, 1/Monat 1/Jahr, 1/10 Jahre abdecken.
Die Beschreibung der Risikobeurteilung sollte auch entsprechend geprüft und angepasst werden, damit diese in der praktischen Umsetzung eigenständig (d.h. ohne ISB) von Risikoeigentümern vorgenommen werden kann.

Masterplan – Schritt 3

NIS-2 Betroffenheit

- Kriterien zur Betroffenheit (Sektor, Größe) prüfen (lassen)
- Einstufung als „wichtiges", „besonders wichtiges" oder Kritis-Unternehmen dokumentieren
- Registrierung bei BSI-Portal durchführen



NIS-2 Gap-Analyse

- Kick-off / Abschluss-Meeting
- Bereitstellung Austauschplattform
- Dokumentationslage prüfen
- Nachweise prüfen / validieren
- Remote / On-Site Workshop
- Bericht erstellen

Abweichungen beheben

- Richtlinien erstellen
- Technische Maßnahmen planen
- Prozesse dokumentieren
- IT-Betrieb (Security) unterstützen

Awareness / Schulung

- NIS-2 und Information Security Schulung erstellen
- Mitarbeiterschulung durchführen
- Management briefen

NIS-2 ready

1 2 3 4 5

3 Fallbeispiel – Follow-up zu Gap-Analyse

Input von Gap-Analyse

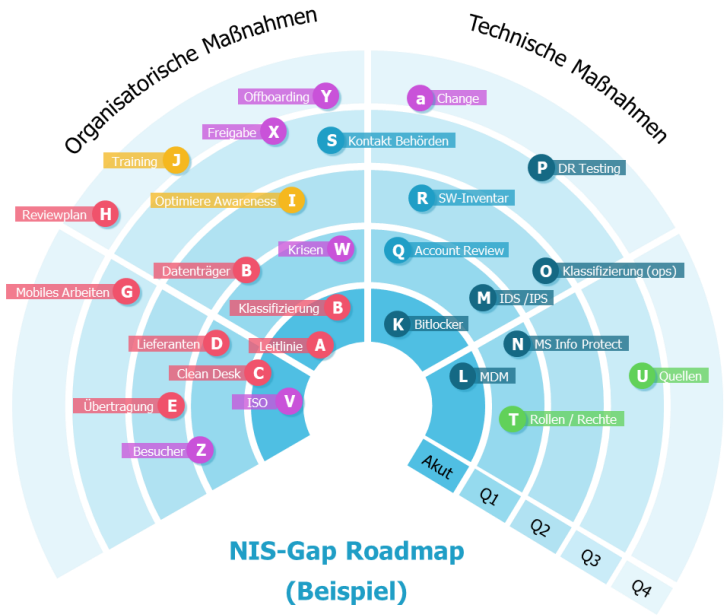
- Gap-Analyse (Report)
- Priorisierung
- Umsetzungstimeline (12 Monate)

	Priorität 1 Findings	Priorität 2 Findings	Priorität 3 Findings
Führung Das Management muss Engagement und Unterstützung für das Informationssicherheitsmanagementsystem (ISMS) zeigen.	11	10	1
Planung Risiken und Chancen im Bereich der Informationssicherheit müssen identifiziert und Maßnahmen zur Behandlung geplant werden.	2	1	1
Unterstützung Notwendige Ressourcen, einschließlich Schulungen und Kommunikation, müssen bereitgestellt werden, um das ISMS zu unterstützen.	2	2	0
Betrieb Die geplanten Maßnahmen und Prozesse zur Informationssicherheit müssen umgesetzt und aufrechterhalten werden.	1	5	2

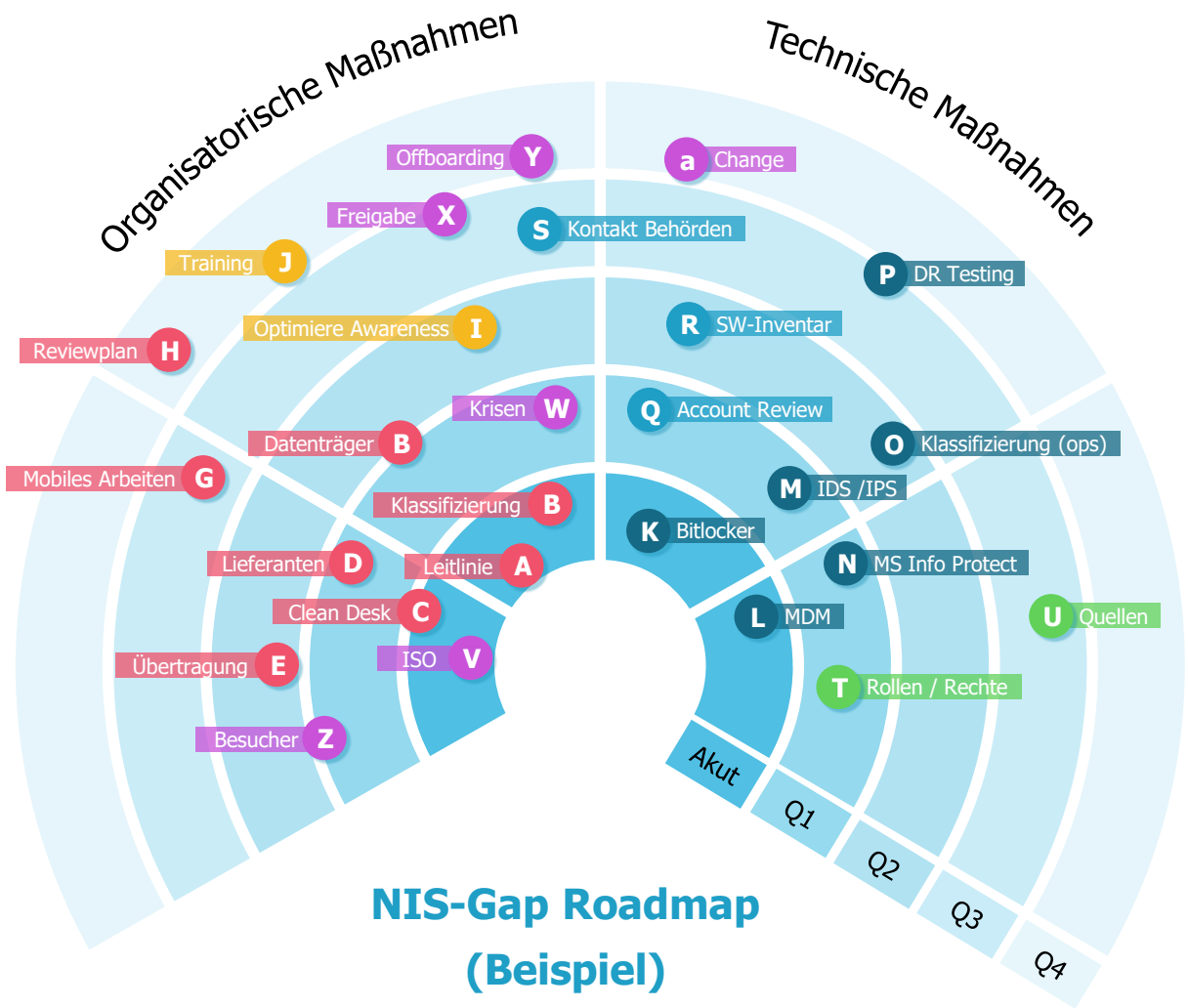
Maßnahmenplan

- A ISMS-Leitlinie erstellen
- B Richtlinie „Klassifizierung Informationen“
- C Richtlinie „Clean Desk“ umsetzen
- D Richtlinie „Lieferantenmanagement“
- E Richtlinie „Sichere Übertragungswege“
- F Richtlinie „Datenträger“ umsetzen
- G Richtlinie „Mobiles Arbeiten“ umsetzen
- H Richtlinien „Reviewplan“ erstellen
- I Awarenesstraining optimieren
- J Awarenesstraining durchführen
- K Bitlocker einführen
- L Mobile Device Management umsetzen
- M IDS / IPS Rollout
- N MS Information Protection konfigurieren
- O Klassifizierung operationalisieren
- P Disaster Recovery Testing
- Q „Account Access Review“ etablieren
- R Software-Inventar dokumentieren
- S Kontakt zu Behörden herstellen
- T Rollen- / Rechtekonzept dokumentieren
- U Dokumentation „Quellen“
- V Bestellung ISO
- W Krisenszenarien dokumentieren
- X „Freigabe“-Prozess dokumentieren
- Y „Offboarding“-Prozess dokumentieren
- Z „Besucher“-Prozess optimieren
- a „Change“-Prozess optimieren

Roadmap



3 Fallbeispiel - Umsetzungsplan

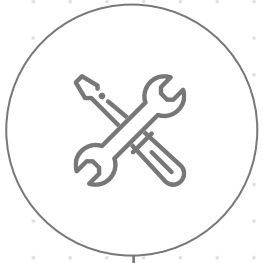


- A ISMS-Leitlinie erstellen
- B Richtlinie „Klassifizierung Informationen“
- C Richtlinie „Clean Desk“ umsetzen
- D Richtlinie „Lieferantenmanagement“
- E Richtlinie „Sichere Übertragungswege“
- F Richtlinie „Datenträger“ umsetzen
- G Richtlinie „Mobiles Arbeiten“ umsetzen
- H Richtlinien „Reviewplan“ erstellen
- I Awarenesstraining optimieren
- J Awarenesstraining durchführen
- K Bitlocker einführen
- L Mobile Device Management umsetzen
- M IDS / IPS Rollout
- N MS Information Protection konfigurieren
- O Klassifizierung operationalisieren
- P Disaster Recovery Testing
- Q „Account Access Review“ etablieren
- R Software-Inventar dokumentieren
- S Kontakt zu Behörden herstellen
- T Rollen- / Rechtekonzept dokumentieren
- U Dokumentation „Quellen“
- V Bestellung ISO
- W Krisenszenarien dokumentieren
- X „Freigabe“-Prozess dokumentieren
- Y „Offboarding“-Prozess dokumentieren
- Z „Besucher“-Prozess optimieren
- a „Change“-Prozess optimieren

Masterplan – Schritt 4

NIS-2 Betroffenheit

- Kriterien zur Betroffenheit (Sektor, Größe) prüfen (lassen)
- Einstufung als „wichtiges", „besonders wichtiges" oder Kritis-Unternehmen dokumentieren
- Registrierung bei BSI-Portal durchführen



NIS-2 Gap-Analyse

- Kick-off / Abschluss-Meeting
- Bereitstellung Austauschplattform
- Dokumentationslage prüfen
- Nachweise prüfen / validieren
- Remote / On-Site Workshop
- Bericht erstellen

Abweichungen beheben

- Richtlinien erstellen
- Technische Maßnahmen planen
- Prozesse dokumentieren
- IT-Betrieb (Security) unterstützen

Awareness / Schulung

- NIS-2 und Information Security Schulung erstellen
- Mitarbeiterschulung durchführen
- Management briefen

NIS-2 ready

1 2 3 4 5

4 Howto: Schulung & Meldung

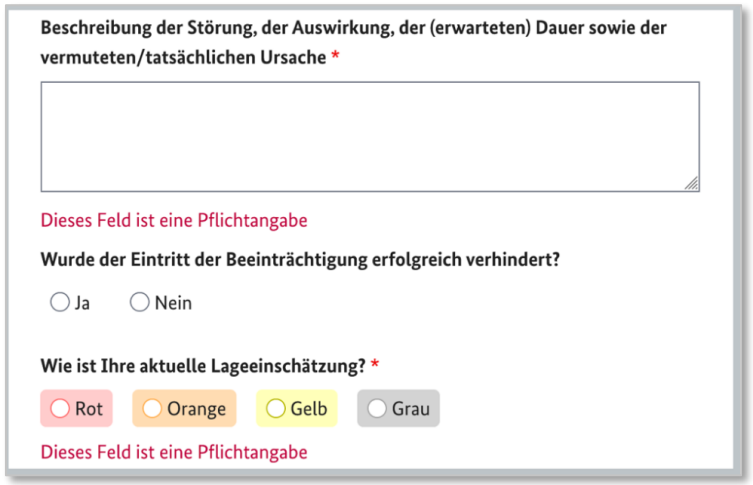
Management Schulung (§38)

- Keine formellen Vorgaben zu Inhalt, Form und Frequenz
- Interpretationsspielraum bei Geschäftsleitung möglich

§ 38 Abs. 3: Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagement-praktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Meldung (§32)

- Allgemeine Meldestelle BSI
- Erheblicher Sicherheitsvorfall Meldung nach maximal 72 h (Erstmeldung 24 h)



Impact auf Incident Prozess

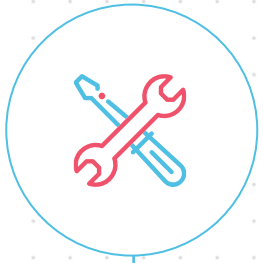
NIS-2 betroffene Unternehmen müssen ihren Incident Prozess anpassen, um Meldefristen und Schnittstellen zum BSI korrekt zu bedienen

Ready !?

NIS-2 Betroffenheit

- Kriterien zur Betroffenheit (Sektor, Größe) prüfen (lassen)
- Einstufung als „wichtiges", „besonders wichtiges" oder Kritis-Unternehmen dokumentieren
- Registrierung bei BSI-Portal durchführen

1



NIS-2 Gap-Analyse

- Kick-off / Abschluss-Meeting
- Bereitstellung Austauschplattform
- Dokumentationslage prüfen
- Nachweise prüfen / validieren
- Remote / On-Site Workshop
- Bericht erstellen

2

Abweichungen beheben

- Richtlinien erstellen
- Technische Maßnahmen planen
- Prozesse dokumentieren
- IT-Betrieb (Security) unterstützen

3

Awareness / Schulung

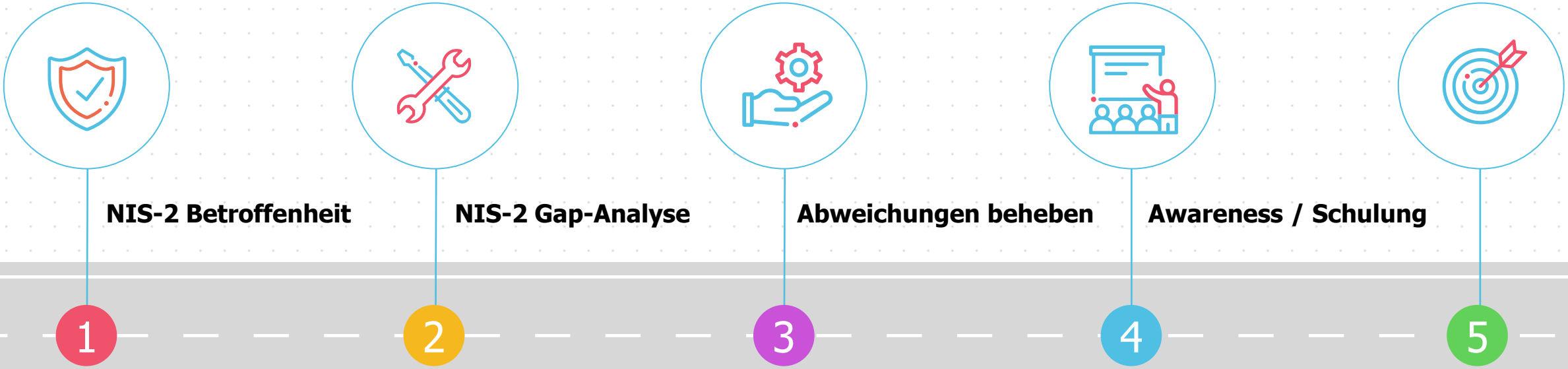
- NIS-2 und Information Security Schulung erstellen
- Mitarbeiterschulung durchführen
- Management briefen

4

NIS-2 ready

5

Wo helfen wir Ihnen - Aufwandsindikation



1 Stunde Betroffenheit prüfen

5 Tage Gap-Analyse durchführen

50 Tage NIS-2 Gaps abarbeiten

10 Tage IT-Notfallhandbuch

2 Tage Management-Schulung

Experience Day 2026 | Masterclass Session 2

Impulse für Ihr Business von morgen.

18.00 Uhr

- Keynote mit Steven Nicolin | Microsoft in der Champions Hall

Wir freuen uns über Feedback