the blu Experience
...feel the difference

NIS2 – Der direkte Weg zur Umsetzung. Ein Praxisbericht.

Torsten Enk, blu Guard GmbH
(ein Unternehmen der blu Gruppe)

Agenda

01 Ansprechpartner und Vorstellung der **blu** Gruppe

02 NIS2 – Überblick

03 NIS2 – Wer ist betroffen?

04 Bis wann müssen Unternehmen diese umsetzen?

05 Welche Aufgaben hat das Management?

06 Welche Konsequenzen kann die Nichteinhaltung haben?

07 Ist ein ISMS Voraussetzung bzw. Ziel der Umsetzung von NIS2?

08 Wie kann ein Unternehmen NIS2 zielgerichtet umsetzen?

09 Auf welche Stolpersteine sollte das Unternehmen bei der Umsetzung achten?

IHR ANSPRECHPARTNER: TORSTEN ENK

HEAD OF INFORMATION SECURITY

the blu Experience
...feel the difference

Berufliche Expertise

Werdegang:
- seit 1999 in der Revision und IT-Beratung tätig
- 2018-2022 Partner bei Rödl & Partner, Führungsteam Digital GRC, Mitarbeit im Führungsteam Wirtschaftsprüfung; Financial Services
- Seit 2022 blu Guard: Beratung und Prüfung in den Bereichen IT-Revision, Informations- und Cyber-Sicherheit, Notfallmanagement

Expertise:
- IT-Prüfung bei international tätigen Unternehmen
- Interne Revision / IT-Revision – Co-Sourcing mit Fokus auf Finanzdienstleister
- Prüfungsnahe Beratung und Prüfung von Migrationen, Archivierung, Systemeinführung, IT-Prozessen, ISMS-Umsetzung, IKS-Optimierung
- SAP-Prüfung und Datenanalysen

Fach- und Gremienarbeit

- Referent der Frankfurt School of Finance zum „IT-Compliance Manager“
- Institut der Wirtschaftsprüfer: Mitglied der IDW Mittelstandsinitiative
- Dozent an Hochschulen zu IT-Anforderungen, IT-Revision, Prozessmanagement
- Leitung der Fachgruppe IT-Revision der ISACA – Internationaler Berufsverband der IT-Auditoren
- Veröffentlichungen im Rahmen der Fachgruppenarbeit z.B. „Grundlagen der IT-Revision für den Einstieg in die Praxis“
- Referent der IDW Akademie für die Ausbildung zum „IT-Auditor IDW“ und diverse IT-Compliance und SAP Seminare

Aus- und Weiterbildung

- Diplom-Betriebswirt (BA)
- Certified Information Systems Auditor (CISA)
- Certified Data Privacy Solutions Engineer (CDPSE)
- PRINCE2 Zertifizierung (IT-Projektmanagement)
- Solution Consultant: mySAP Financials (FI/CO)
- Zertifizierter ISO27001 Auditor nach BSI IT-Grundschutz (TÜV)

BLU UNTERNEHMENSGRUPPE

- **Die blu** Unternehmensgruppe erbringt seit 2007 mit derzeit ca. 300 Mitarbeitern themenübergreifende IT & Management Leistungen.
- Unabhängiger Anbieter von Informationssicherheit Technologielösungen und Services
- Spezialisiert auf Digital Governance, Risk & Compliance (GRC)
- Zu unseren Kernkompetenzen zählen IT, IoT & OT Asset LifeCycle Management, Security LifeCycle Management und Digitalforensik
- MEHR ERFAHREN https://thebluexperience.de/

GOVERNANCE RISK COMPLIANCE

NIS2 – Überblick

Veröffentlichung der NIS2 Richtlinie

EU-Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau

Im Amtsblatt der EU L333/80 am 27.12.2022 veröffentlicht.

Als Richtlinie in Kraft getreten am 16. Januar 2023

Von den Mitgliedsstaaten bis zum 17. Oktober 2024 umzusetzen - offen!

Ausweitung des NIS2 Anwendungsbereichs

Höheres Maß an IT-Sicherheitsanforderungen

Betroffen sind öffentliche und privatrechtliche Organisationen und Gesellschaften

Aufsichtspflichten für Führungskräfte & IT-Verantwortliche

Nachweis der Umsetzung, Einhaltung & Wirksamkeit der Cybersicherheitsmaßnehmen

Struktur der NIS2 Richtlinie

Erwägungsgründe (144)

- Sollen das Verständnis der Anforderungen erleichtern. Liefern den Kontext, Zielsetzung und Auslegungshinweise.

Artikel (46)

- Definieren die Anforderungen, die die Betroffenen zu erfüllen haben.

...ABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

(1) In dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

(2) Zu diesem Zweck wird in dieser Richtlinie Folgendes festgelegt:

a) die Pflicht für alle Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit (zentrale Anlaufstellen) und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten;

b) Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten für Einrichtungen der in den Anhang I oder II aufgeführten Arten sowie für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden;

c) Vorschriften und Pflichten zum Austausch von Cybersicherheitsinformationen;

d) Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten.

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche oder private Einrichtungen der in den Anhang I oder II genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben.

Artikel 3 Absatz 4 des Anhangs dieser Empfehlung gilt nicht für die Zwecke dieser Richtlinie.

(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen der in den Anhang I oder II genannten Art, wenn

a) [illegible] Die [illegible] bra[illegible]ht werden von:

i) [illegible] von öffe[illegible] elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Ko[illegible]mu[illegible]ka[illegible]

ii) Vertrauensdiensteanbietern;

iii) [illegible]menregistern der [illegible]omäne ob[illegible]rster[illegible]ufe und Domänennamensystem-Diensteanbietern;

b) [illegible] be[illegible] Einrichtung in einem Mi[illegible]glied[illegible]staa[illegible]um [illegible] [illegible] [illegible] A[illegible]bieter eines Dienstes handelt, der für die Aufr[illegible]hter[illegible]alt[illegible]ng kritis[illegible]er ge[illegible]llsc[illegible]aftlich[illegible]er o[illegible]ler [illegible]irtsch[illegible]ftli[illegible]er [illegible]ätigkeiten unerlässlich ist;

c) sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

d) eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

- Kap. I Allgemeine Bestimmungen (Art. 1-6)
- Kap. II Koordinierte Rahmen für die Cybersicherheit (Art. 7-13)
- Kap. III Zusammenarbeit auf Unions- und internationaler Ebene (Art. 14-19)
- Kap. IV Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit (Art. 20-25)
- Kap. V Zuständigkeit und Registrierung (Art. 26-28)
- Kap. VI Informationsaustausch (Art. 29-30)
- Kap. VII Aufsicht und Durchsetzung (Art. 31-37)
- Kap. VIII Delegierte Rechtsakte und Durchführungsrechtsakte (Art. 38-39)
- Kap. IX Schlussbestimmungen (Art. 40-46)

NIS2 – Wer ist betroffen?

Anwendungsbereich

Erweitert den derzeit bestehenden NIS-Geltungsbereich

Umfasst neue Sektoren und Kriterien

Einstufung in „**Wesentlich**“ oder „**Wichtig**“ Einrichtungen

Unterteilung in „**Sektoren mit hoher Kritikalität**“ und „**Weitere kritische Sektoren**“

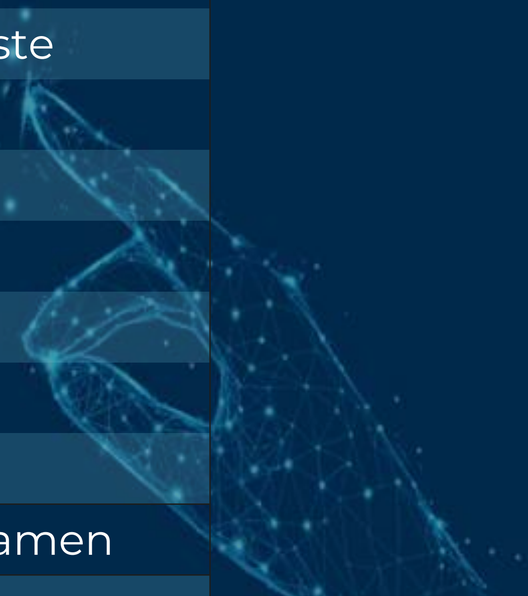
Betroffen sind:

GROSSE Unternehmen (>= 250 Beschäftigte oder mehr als 50 Millionen Umsatz, Bilanzsumme mehr als 43 MEUR)	MITTLERE Unternehmen (50-249 Beschäftigte oder mehr als 10-50 Millionen Umsatz, Bilanzsumme 10-42 MEUR)	KLEINE Unternehmen (11-49 Beschäftigte oder mehr als 2-10 Millionen Umsatz, Bilanzsumme 10-42 MEUR)	KLEINST Unternehmen (< 10 Beschäftigte oder mehr als < 2 Millionen Umsatz, Bilanzsumme < 2 MEUR)

Sektoren

Sektoren mit hoher Kritikalität
Energie
Verkehr
Banken
Finanzmarkt Infrastruktur
Gesundheitswesen
Trinkwasser
Abwasser
Digitale Infrastruktur
ICT-Dienstleistungsmanagement (B2B)
Öffentliche Verwaltungseinrichtungen
Raumfahrt

Weitere kritische Sektoren
Post- und Kurierdienste
Abfallwirtschaft
Chemikalien
Nahrungsmittel
Fertigung
Digitale Anbieter
Forschung
Anbieter von Domänenamen



Die Mitgliedstaaten müssen bis spätestens 17. April 2025 ein Verzeichnis dieser Einrichtungen erstellen und pflegen, das alle zwei Jahre aktualisiert werden muss.
Für dieses Register sind die Einrichtungen verpflichtet, den zuständigen Behörden die folgenden Angaben zu übermitteln:
- Name
- Anschrift und Kontaktangaben
- Relevanter (Teil-)Sektor aus Anhang I und II
- Liste der entsprechenden Mitgliedstaaten, in denen sie tätig sind

Jede Änderung in der Liste muss von den Einrichtungen unverzüglich gemeldet werden.

Vorfallbenachrichtigung

Stufenweise Meldepflichten für Vorfälle, die „**Erhebliche Auswirkungen**“ haben

FRÜHWARNUNG	Innerhalb 24 Stunden
OFFIZIELLE BENACHRICHTIGUNG ÜBER DEN VORFALL	Innerhalb 72 Stunden
ZWISCHENSTANDSBERICHT	Anlassbezogen und auf Anforderung
ABSCHLUSSBERICHT	1 Monat nach Beendigung

BSI NIS2 Betroffenheitsanalyse

NIS-2-Betroffenheitsprüfung

Sind Sie unsicher, ob Ihr Unternehmen vom Gesetzentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) betroffen ist?
Die › **NIS-2-Betroffenheitsprüfung** des BSI bietet Ihnen in wenigen Schritten dafür eine erste Orientierung.

Die NIS-2-Betroffenheitsprüfung stellt Ihnen konkrete, am Gesetzentwurf orientierte Fragen, um Ihr Unternehmen einzuordnen. Die Fragen sind kurz und präzise gehalten und werden bei Bedarf im Kleingeschriebenen tiefer gehend erläutert.

Nachdem Sie den Fragenkatalog durchlaufen haben, erhalten Sie ein auf Ihren Angaben basierendes Ergebnis. Dieses gibt eine automatisierte Ersteinschätzung, ob Ihr Unternehmen vom NIS2UmsuCG betroffen ist - und erläutert Ihnen, was dieser Status bedeutet und welche Pflichten durch den Gesetzgeber vorgezeichnet sind.

Die Nutzung der NIS-2-Betroffenheitsprüfung erfolgt anonym. Das BSI stellt diese im Rahmen seiner Kooperationsaufgabe zur Verfügung. Sie erfasst keine Daten, die personenbezogen sind oder Rückschlüsse zur Identifizierung Ihres Unternehmens geben. Bitte beachten Sie, dass die Hilfe zur Betroffenheitsprüfung von NIS-2 lediglich als Orientierungshilfe dient und Ihr Ergebnis rechtlich nicht bindend ist, da Ihre Antworten automatisiert erstellt und nicht vom BSI oder anderen unabhängigen Stellen geprüft werden. Es besteht kein Anspruch auf Vollständigkeit und Richtigkeit der Inhalte.

Zurzeit basieren die Abfragen der NIS-2-Betroffenheitsprüfung auf dem Gesetzentwurf des NIS2UmsuCG. Sobald das finale Umsetzungsgesetz beschlossen und verabschiedet wurde, wird das BSI die NIS-2-Betroffenheitsprüfung anhand dieses Gesetzes anpassen und aktualisieren.

Haben Sie zu oder nach der Nutzung noch Fragen? Das BSI steht gerne zur Verfügung.

> Die NIS-2-Betroffenheitsprüfung dient als automatische Orientierungshilfe auf Grundlage von Eigenangaben, deren Ergebnis nicht rechtlich bindend ist. Die NIS-2-Betroffenheitsprüfung ersetzt die Prüfung zur Selbst-Identifizierung nicht und hat für eventuelle Verfahren keine Indizwirkung.

Einrichtungen der Bundes-, Landes- und Kommunalverwaltung werden in der NIS-2-Betroffenheitsprüfung nicht betrachtet.

NIS-2-Betroffenheitsprüfung starten ›

DISCLAIMER des BSI:

- Zurzeit basieren die Abfragen der NIS-2-Betroffenheitsprüfung auf dem Gesetzentwurf des NIS2UmsuCG. Sobald das finale Umsetzungsgesetz beschlossen und verabschiedet wurde, wird das BSI die NIS-2-Betroffenheitsprüfung anhand dieses Gesetzes anpassen und aktualisieren.
- Die NIS-2-Betroffenheitsprüfung dient als automatische Orientierungshilfe auf Grundlage von Eigenangaben, deren Ergebnis nicht rechtlich bindend ist.
- Die NIS-2-Betroffenheitsprüfung ersetzt die Prüfung zur Selbst-Identifizierung nicht und hat für eventuelle Verfahren keine Indizwirkung.

Bis wann müssen Unternehmen diese umsetzen?

Umsetzungsfristen

NIS2 Richtlinie, Artikel 41:

Bis zum **17. Oktober 2024** erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis. Ab dem 18. Oktober 2024 wird von den Mitgliedstaaten erwartet, dass sie die Vorschriften, die sie zur Einhaltung der Richtlinie erlassen haben, durchsetzen und implementieren. Bei Erlass der erforderlichen Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Alternativ dazu sollte den Vorschriften bei ihrer amtlichen Veröffentlichung ein separates Dokument oder ein Verweis auf die Richtlinie beigefügt werden.

Cyber-Security Risiko Management

Wesentlich und **Wichtig** eingestufte Unternehmen müssen geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen ergreifen.

Risikoanalyse und Sicherheit von Informationssystemen
Umgang mit Vorfällen
Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs
Sicherheit der Lieferkette
Sicherheit bei der Beschaffung, Entwicklung und Wartung von Systemen
Strategien und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen zum Management von Cybersicherheitsrisiken
Grundlegende Computerhygiene und Schulungen
Richtlinien für den angemessenen Einsatz von Kryptographie
Personalsicherheit & Richtlinien für Zugangskontrollen und Asset Management
Einsatz einer Multi-Faktor gesicherten Sprach-/Video-/Textkommunikation

Welche Aufgaben hat das Management?

Management Verantwortung

Die oberste Führungsebene trägt die Verantwortung für das Cybersicherheits-Risikomanagement in als Wesentlich und Wichtig eingestufte Unternehmen

Verstöße der NIS2-Anforderungen durch das Management können schwerwiegende Folgen haben, einschließlich persönlicher Haftung, vorübergehende Sanktionen und Verwaltungsstrafen

Die Leitungsorgane übernehmen dabei folgende Verpflichtungen:

Genehmigung der Angemessenheit der vom Unternehmen getroffenen Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit
Überwachung der Umsetzung der Risikomanagementmaßnahmen
Teilnahme an Schulungen, um ausreichende Kenntnisse und Fähigkeiten zur Risikoerkennung und Praktiken des Cybersicherheits-Risikomanagements sowie deren Auswirkungen auf die vom Unternehmen erbrachten Dienstleistungen zu erwerben und zu bewerten
Mitarbeitern regelmäßig entsprechende Schulungen anzubieten
Rechenschaft für die Nichteinhaltung der Vorschriften zu tragen

Welche Konsequenzen kann die Nichteinhaltung haben?

Aufsichtspflicht & Durchsetzung der Behörden

Mit Audits und Anfragen von Behörden zu den getroffenen IT-Sicherheitsmaßnahmen ist zu rechnen.

Bei Verstößen ermöglicht NIS2 den nationalen Behörden eine Reihe von Durchsetzungs-befugnissen.

- Erteilung von Verwarnungen bei Nichteinhaltung
- Erteilung verbindlicher Anweisungen
- Anweisung zur Unterlassung eines nicht konformen Verhaltens
- Erfüllung von Anweisungen, Risikomanagementmaßnahmen oder Meldepflichten
- Anweisung zur Information, natürlicher oder juristischer Personen die potenziell von einer erheblichen Cyber-Bedrohung betroffen sind
- Umsetzung von Anweisungen innerhalb einer angemessenen Frist als Ergebnis eines Sicherheitsaudits
- Ernennung eines Überwachungsbeauftragten, um die Einhaltung der Vorschriften zu überwachen
- Anweisung zur Veröffentlichung von Aspekten der Nichteinhaltung
- Verhängung von Bußgeldern
- Zertifizierung, Genehmigung oder Aussetzung in Bezug auf Dienste, wenn die Frist für das Einleiten von Maßnahmen nicht eingehalten wird
- Vorübergehende Absetzung von Hauptgeschäftsführern oder gesetzlichen Vertretern die Führungsaufgaben ausüben

Verwaltungsstrafen / Bußgelder

Bis zu 10.000.000 EUR oder 2 %

des gesamten weltweiten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr, zu dem das **Wesentliche Unternehmen** gehört, je nachdem welcher Betrag höher ist

Bis zu 7.000.000 EUR oder 1,4 %

des gesamten weltweiten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr, zu dem das **Wichtige Unternehmen** gehört, je nachdem welcher Betrag höher ist.

Der Referentenentwurf des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (Stand: Mai 2023) sieht eine überschießende Umsetzung vor und erhöht den Bußgeldrahmen sogar auf bis zu **max. 20 Mio. EUR**.

Ist ein ISMS Voraussetzung bzw. Ziel der Umsetzung von NIS2?

Relevante Rahmenwerke und Standards

Bekannte Standards und Frameworks zur Umsetzung von NIS2:

ISO/IEC 27000	Überblick über Informationssicherheits-Managementsysteme
ISO/IEC 27001	Definition der Anforderungen für die Einrichtung, Umsetzung und Betrieb eines ISMS
ISO/IEC 27002	Liste der Controls und Leitfaden zur Umsetzung
ISO/IEC 27003	Leitlinie für die Implementierung eines ISMS nach ISO/IEC 27001
ISO/IEC 27004	Leitfaden zur Überwachung und Messung der Leistung und Wirksamkeit des ISMS
ISO/IEC 27005	Leitlinien für das Risikomanagement zur ISO/IEC 27001
ISO/IEC 27032	Leitlinie für Internet-Sicherheitspraktiken
ISO/IEC TR 27103	Leitfaden zur Einbindung bestehender Normen und Standards in ein Rahmenwerk für Cybersicherheit

Relevante Rahmenwerke und Standards

Weniger bekannt, aber hilfreich sind in diesem Umfeld folgende Frameworks:

NIST Rahmenwerk für Cybersicherheit	Standards und Praktiken zur Bewältigung von Cybersicherheitsrisiken und Kommunikation zwischen internen und externen Parteien
	Dient als ergänzendes Instrument für bestehende Programme und Prozesse im Unternehmen.
CIS Controls	Maßnahmen und Handlungsempfehlungen des Center for Internet Security (CIS) zur Verbesserung der Cybersecurity-Resilienz von Unternehmen.

NIS 2 Anforderungen und ISO 27k

Zu NIS2 sind laut Artikel 21 folgende u.g. Punkte umzusetzen.

Alle Punkte sind auch Gegenstand der ISO27k mit Fokus von NIS2 auf die rot markierten Themen.

Policies: Richtlinien für Risiken und Informationssicherheit	Risikomanagement zur Bewertung von Cybersicherheits-Risiken	Incident Management: Prävention, Detektion und Bewältigung von Cyber Incidents	Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs: Notfall- und Krisenmanagement	Sicherheit in der Lieferkette	Sicherheit bei der Beschaffung, Entwicklung und Wartung von Systemen
Effektivität: Vorgaben zur Messung von Risiko-Maßnahmen	Grundlegende Computerhygiene und Schulungen	Richtlinien für den angemessenen Einsatz von Kryptographie	Personal: Human Resources Security	Richtlinien für Zugangskontrollen	Information und IT-Asset-Management
	Authentication: Einsatz von Multi-Factor-Authentisierung und SSO	Kommunikation: Einsatz sicherer Sprach-, Video- und Text-Kommunikation	Notfall-Kommunikation: Einsatz gesicherter Notfall-Kommunikations-Systeme	Verfahren und **Fristen** für das Melden von Sicherheitsvorfällen an Aufsichtsorgane	

NIS 2 Anforderungen und ISO 27k

Nr.	NIS2UmsuCG	Anforderung	KRITIS	ISO 27001 2022	NIS2 IT Act
30.1.1	§30 (1) Satz 1	Maßnahmen basierend auf Risiko-Exposition und gesellschaftlichen und wirtschaftlichen Auswirkungen	BSI-3 BSI-15	4.3 6.1 8.2 8.3 A.5.4 A.5.29 A.5.30	
30.1.2	§30 (1) Satz 3	Dokumentation der NIS2 Risiko-Management Maßnahmen	BSI-16	6.1.3 8.3 A.5.31	
30.2.0	§30 (2) Satz 1	Allgefahrenansatz und Stand der Technik	BSI-13 BSI-15	6.1 8.2 8.3 A.5.29 A.5.30	2.1.2
30.2.1a	§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	BSI-13 BSI-14 BSI-16 BSI-85 BSI-86 BSI-87 BSI-88 BSI-89	6.1 8.2 8.3 10.1 A.5.31 A.5.36 A.8.34	2.1.1 2.1.2 2.1.3 2.2.1 2.2.2 2.2.3 2.3.1 2.3.2 2.3.3 2.3.4
30.2.1b	§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	BSI-1 BSI-2 BSI-3	4.1-10.2 A.5.1 A.5.2	1.1.1 1.1.2 1.2.1

Quelle: NIS2-Mapping auf KRITIS und ISO 27001 Cybersecurity – OpenKRITIS

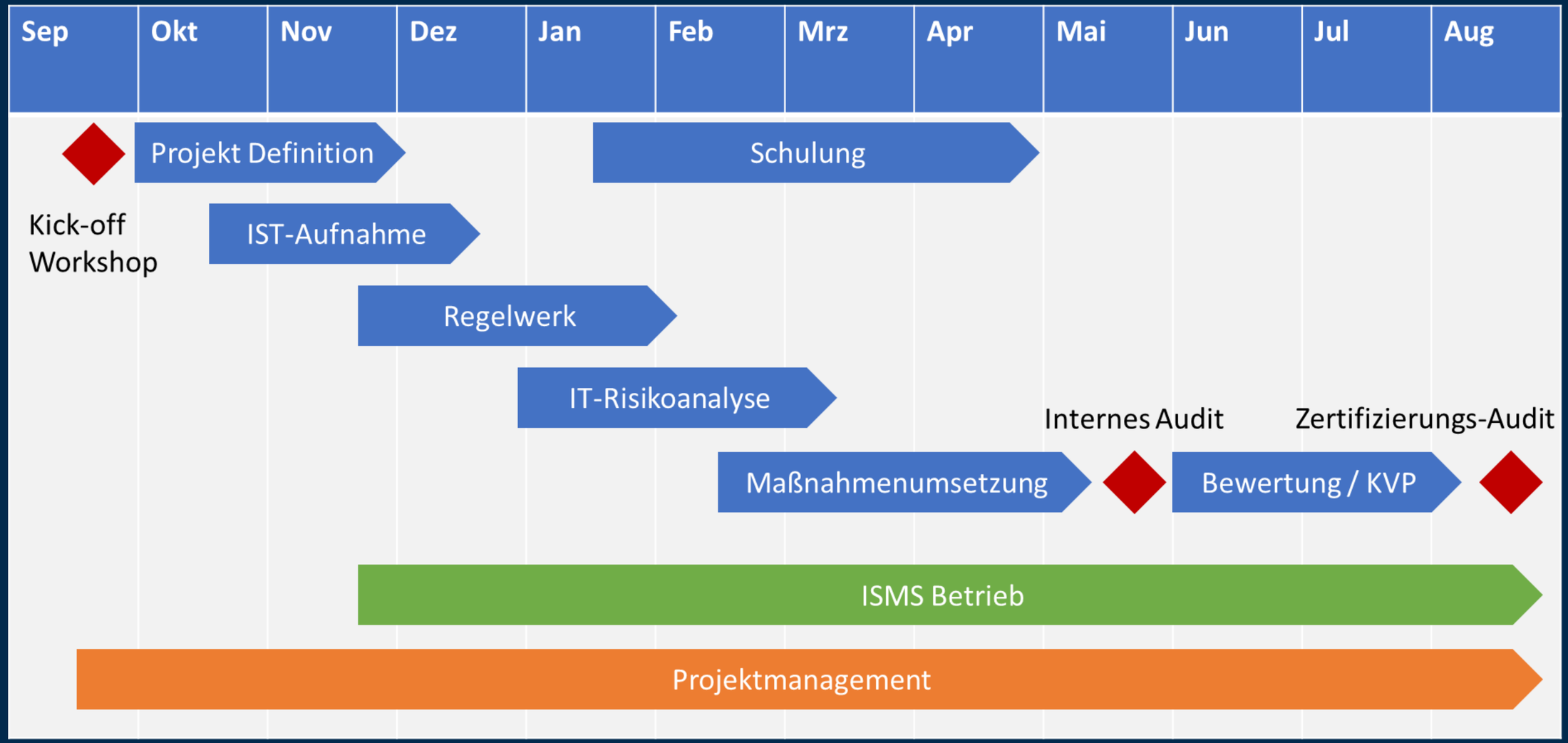
Das NIS2-Umsetzungsgesetz (!nicht verabschiedet) und die EU NIS2-Direktive definieren Anforderungen an das Risiko-Management und Sicherheitsmaßnahmen.

Der ISO/IEC 27001 ff. Standard liefert ein Managementsystem und umfangreiche „Controls“ (93) und Umsetzungshinweise.

openkritis.de ist ein unabhängiges Nachschlagewerk

Wie kann ein Unternehmen NIS2 zielgerichtet umsetzen?

Vorgehen zur ISMS Einführung



Vorgehen mit Fokus auf NIS2 nach dem PDCA Ansatz

Planen (Plan)

Implementieren der NIS 2 – Richtlinie

- Geltungs- und Anwendungsbereich
- Controls (ISO/IEC 27002)

Kontext der Organisation

- Interessengruppen
- Prozesse
- Aufbauorganisation
- Dienstleister

Governance der Cybersicherheit

- Awareness
- Risikomanagement
- Präventive Maßnahmen

Rollen- und Verantwortlichkeiten festlegen

Asset Management

Risikomanagement

Durchführen (Do)

Cybersicherheitsmaßnahmen umsetzen

Sicherheit in der Lieferkette umsetzen

Verfahren für Sicherheitsvorfälle einrichten inkl. Meldung an Aufsichtsbehörden

Krisenmanagement festlegen

Maßnahmen zur Aufrechterhaltung der Betriebsfähigkeit

Sensibilisierungsmaßnahmen

Kommunikation festlegen (intern und extern)

Prüfen (Check)

Cybersicherheitstests durchführen

Interne Audit durchführen

Einrichten und Überwachung von KPIs

Handeln (Act)

Fortlaufende Verbesserung einrichten

Risiken und Maßnahmen regelmäßig überprüfen

Auf Abweichungen / neue Szenarien reagieren

Kick-off Workshop

Vorgehen zur ISMS Einführung / NIS2 Check

Inhalte eines Kick-off Workshops

- Überblick zur Methodik zur Umsetzung der NIS2 Anforderungen
- Ist-Situation des ISMS (Vorstellung durch den Kunden)
- Definition des Ziel-Zustands und der Lücken auf Basis der NIS2 Anforderungen und Reifegrad des ISMS
- Unterstützende Tools zum Umsetzung / Dokumentation des NIS2 konformen ISMS (sofern Bedarf besteht)

Ergebnisse

- Workshop Präsentation inkl. Zielzustand des ISMS zur Umsetzung von NIS2
- Übersicht der notwendigen Dokumentation mit dem aktuellen Stand und bekannten Lücken
- Dokumentation des Anwendungsbereich für das ISMS
- Liste der relevanten Kontrollen und deren aktueller Umsetzungsstand (Statement of Applicability - SOA) mit Bezug zu NIS2
- Projekt- und Meilensteinplan für die weitere Planung und Aufwandschätzung

Beispiel:

Festlegung des ISMS-Anwendungsbereichs

Die Organisation muss den Anwendungsbereich des ISMS definieren.

Unter Berücksichtigung der rechtlichen, vertraglichen und anderen Anforderungen wird der ISMS-Anwendungsbereich gemäß nachfolgender Punkte festgelegt.

Prozess und Services

[Genaue Benennung der Services und/oder Geschäftsprozesse, die im Anwendungsbereich enthalten sind]

Organisationseinheiten

[Genaue Benennung der Organisationseinheiten, die im Anwendungsbereich enthalten sind, und auf welche Weise diese von jenen Organisationseinheiten getrennt gehalten werden, die in den Anwendungsbereich nicht mit einbezogen sind.]

Standorte

[Genaue Benennung der Standorte, die im Anwendungsbereich enthalten sind und auf welche Weise diese von jenen Organisationseinheiten getrennt gehalten werden, die in den Anwendungsbereich nicht mit einbezogen sind.]

Netzwerke und IT-Infrastruktur

[Genaue Benennung der Netzwerke und verwandter IT-Infrastrukturen, die im Anwendungsbereich enthalten sind. Abgrenzung von jenen Netzwerkbereichen, die in den Anwendungsbereich nicht mit einbezogen sind. Beschreibung der Schnittstellen, die den Übergang zwischen beiden Bereichen definieren.]

Ausschlüsse vom Anwendungsbereich

Folgendes ist nicht im Anwendungsbereich enthalten: [genaue Benennung einzelner Elemente der Organisation/einzelner Ressourcen, die explizit vom Anwendungsbereich ausgeschlossen werden sollen].

Dokumenten-Management

Der Eigentümer des Dokuments ist [Stellenbezeichnung]. Dieser prüft das Dokument mindestens halbjährlich hinsichtlich Aktualität und Anwendungsbereich. Technische Neuerungen und Änderungen der Geschäftsprozesse sind zu berücksichtigen.

Vorgehen zur ISMS Einführung / NIS2 Check

Nr.	NIS2UmsuCG	Anforderung	KRITIS	ISO 27001 2022	NIS2 IT Act
30.1.1	§30 (1) Satz 1	Maßnahmen basierend auf Risiko-Exposition und gesellschaftlichen und wirtschaftlichen Auswirkungen	BSI-3 BSI-15	4.3 6.1 8.2 8.3 A.5.4 A.5.29 A.5.30	
30.1.2	§30 (1) Satz 3	Dokumentation der NIS2 Risiko-Management Maßnahmen	BSI-16	6.1.3 8.3 A.5.31	
30.2.0	§30 (2) Satz 1	Allgefahrenansatz und Stand der Technik	BSI-13 BSI-15	6.1 8.2 8.3 A.5.29 A.5.30	2.1.2
30.2.1a	§30 (2) Nr. 1	Konzepte zur Risiko-Analyse (IT-RM)	BSI-13 BSI-14 BSI-16 BSI-85 BSI-86 BSI-87 BSI-88 BSI-89	6.1 8.2 8.3 10.1 A.5.31 A.5.36 A.8.34	2.1.1 2.1.2 2.1.3 2.2.1 2.2.2 2.2.3 2.3.1 2.3.2 2.3.3 2.3.4
30.2.1b	§30 (2) Nr. 1	Konzepte für IT-Sicherheit (ISMS)	BSI-1 BSI-2 BSI-3	4.1-10.2 A.5.1 A.5.2	1.1.1 1.1.2 1.2.1

Quelle: NIS2-Mapping auf KRITIS und ISO 27001 Cybersecurity – OpenKRITIS

Das NIS2-Umsetzungsgesetz (!nicht verabschiedet) und die EU NIS2-Direktive definieren Anforderungen an das Risiko-Management und Sicherheitsmaßnahmen.

Der ISO/IEC 27001 ff. Standard liefert ein Managementsystem und umfangreiche „Controls“ (93) und Umsetzungshinweise.

openkritis.de ist ein unabhängiges Nachschlagewerk

Auf welche Stolpersteine sollte das Unternehmen bei der Umsetzung achten?

Stolpersteine aus der Projekterfahrung

Richtlinien definieren ist schnell gemacht. Der Aufwand der Einrichtung der Verfahren und Kontrollen wird oft unterschätzt.

Unterstützung durch das Management ist unabdingbar, da sich Änderungen auf die gesamte Organisation auswirken

Meist fehlen schon Grundlagen wie eine Prozesslandkarte, ein Compliance-Register, definierte Service Level oder eine vollständige Asset Übersicht.

Unternehmen tun sich oft schwer bei der Benennung ihrer Information Assets.

In größeren Unternehmens-Gruppen sind meist Zuständigkeiten, insbesondere die Richtlinien-Hoheit nicht abschließend geklärt.

Die Dokumentation in Excel, Word oder Confluence ist aufwendig. Zusammenhänge können aber schwer abgebildet werden. Es empfiehlt sich ein GRC-Tool.

VIELEN DANK!

Torsten Enk

Head of Information Security & Audit
Managing Director

+ 49 (151) 1944 3137

Torsten.Enk@blu-gurad.de

www.thebluexperience.de

https://www.linkedin.com/in/torsten-enk-b4540522/

the blu Experience

...feel the difference

Dieses Dokument wird ausschließlich zu Informationszwecken veröffentlicht.
Alle in diesem Dokument angebotenen Bedingungen und Konditionen sind nur Indikativ und vertragsabhängig.
Nichts in diesem Dokument ist Bestandteil einer gesetzlichen Vereinbarung oder eines Angebots von Produkten und Dienstleistungen.