TaylorWessing

hvs consulting

Quo vadis NIS-2?

Rechtliche & praktische Tipps für die Umsetzung

26. Februar 2025 | Mario Melmer & Dr. Axel Freiherr von dem Bussche

Wer sind wir?

Mario Melmer
Head of Information Security HvS

mario.melmer@hvs-consulting.de
www.hvs-consulting.de

Beratungsschwerpunkte

- Etablierung ISMS
- InfoSec-Consulting & -Coaching
- ISMS Audits und -Gap Analysen
- IT-Notfall & Krisenmanagement
- Stv. Prüfstellenleiter für Prüfungen gem. §8 BSIG (KRITIS)
- Lead Auditor für ISO 27001

Dr. Axel Freiherr von dem Bussche
LL.M. (L.S.E.), CIPP/E

a.bussche@taylorwessing.com
www.taylorwessing.com

Beratungsschwerpunkte

- Informationstechnologie
- Telekommunikation
- Datenschutz
- Urheber- & Medienrecht
- Litigation & Dispute Resolution
- Technology, Media & Communications

Chambers RANKED IN Europe 2024 Axel von dem Bussche

The LEGAL 500 DEUTSCHLAND FÜHRENDE NAMEN 2024

Inhalt

1	Warum NIS-2?	4
2	Wer ist betroffen und was sind die Anforderungen?	11
3	Der Weg zur NIS-2 Konformität	31

1 | Warum NIS-2?

TaylorWessing

Was ist NIS-2?

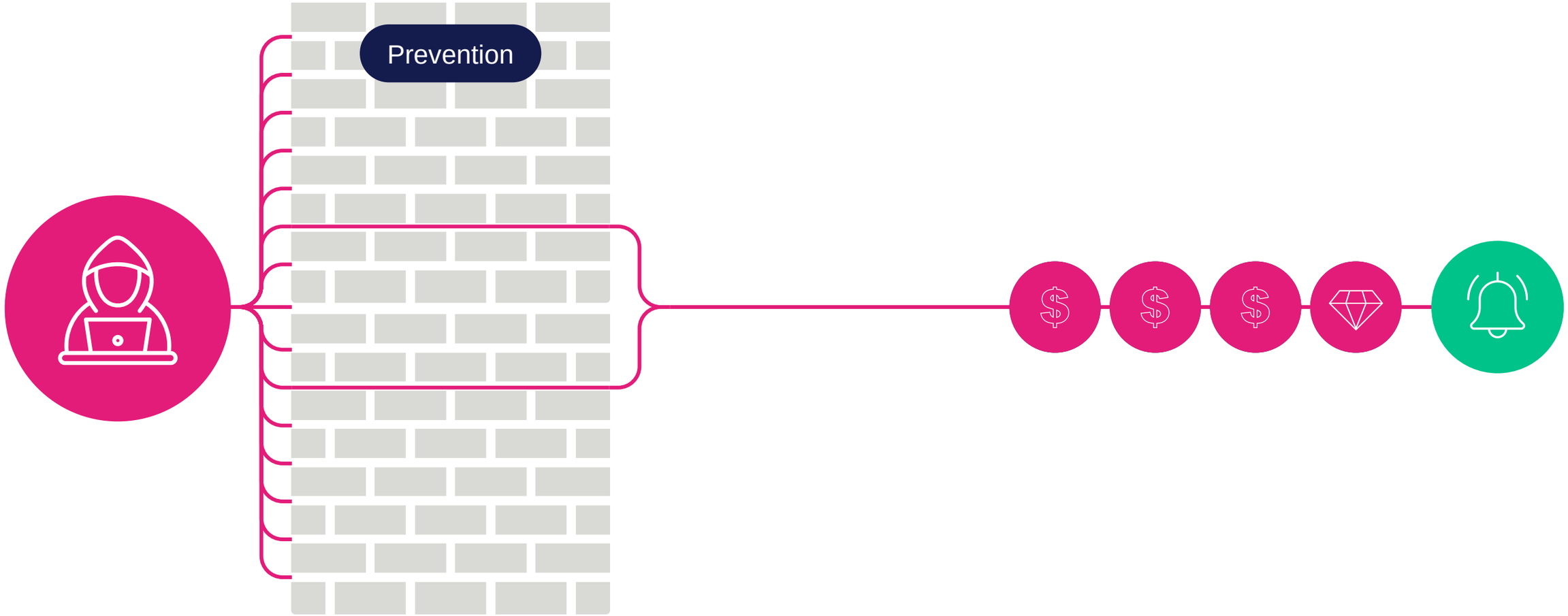
NIS-2-RL

- EU-Richtlinie zur Verbesserung der Cybersicherheit und der Widerstandsfähigkeit von Netzwerken und Informationssystemen in Europa
- **Gilt seit Dezember 2024**
- To Do: die Richtline in nationales Gesetz umzuwandeln

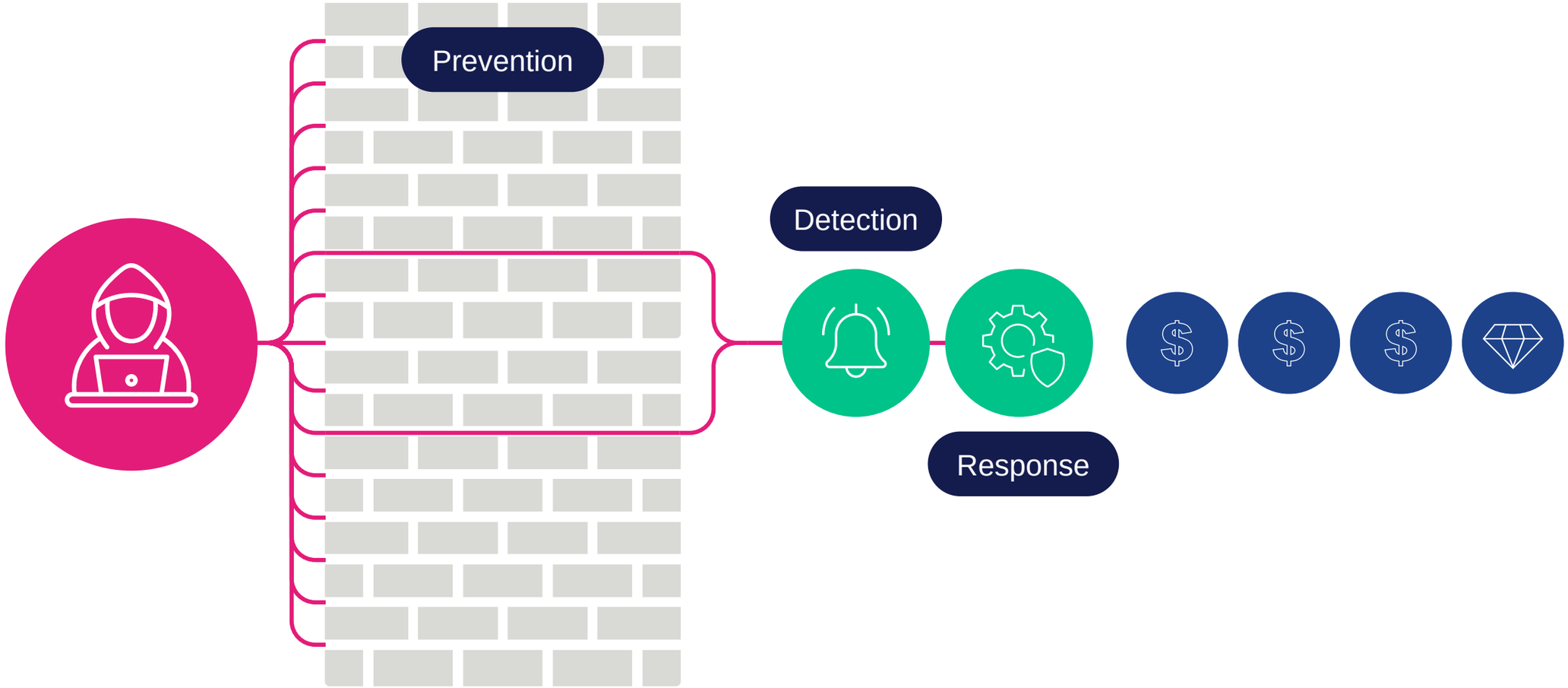
NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

- Deutsches Gesetz zur Umsetzung der NIS-2 Richtlinie
- **Aktuell gibt es einen Entwurf**
- **Soll dann unmittelbar in Kraft treten**

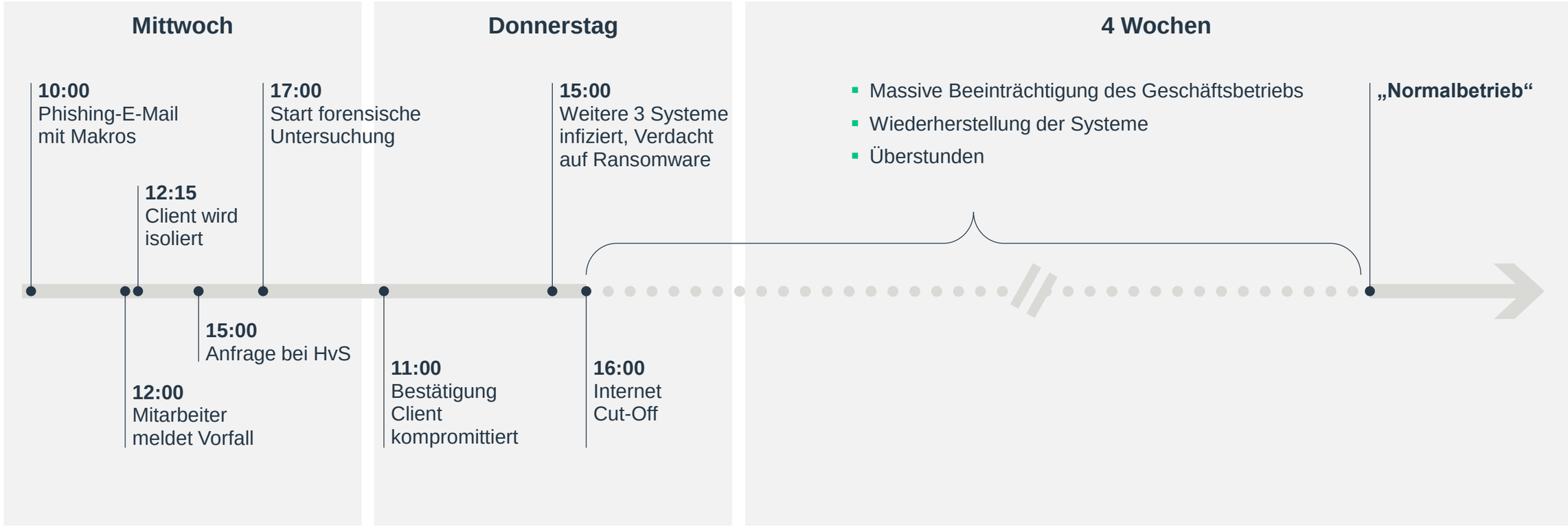
Cyber-Resilience (früher)



Cyber-Resilience (heute)



Ein „positiver“ Incident



Jedes Unternehmen sollte ein ISMS etablieren (unabhängig von gesetzlichen Vorgaben), weil man damit sein Geschäft schützt!

2 Wer ist betroffen und was sind die Anforderungen?

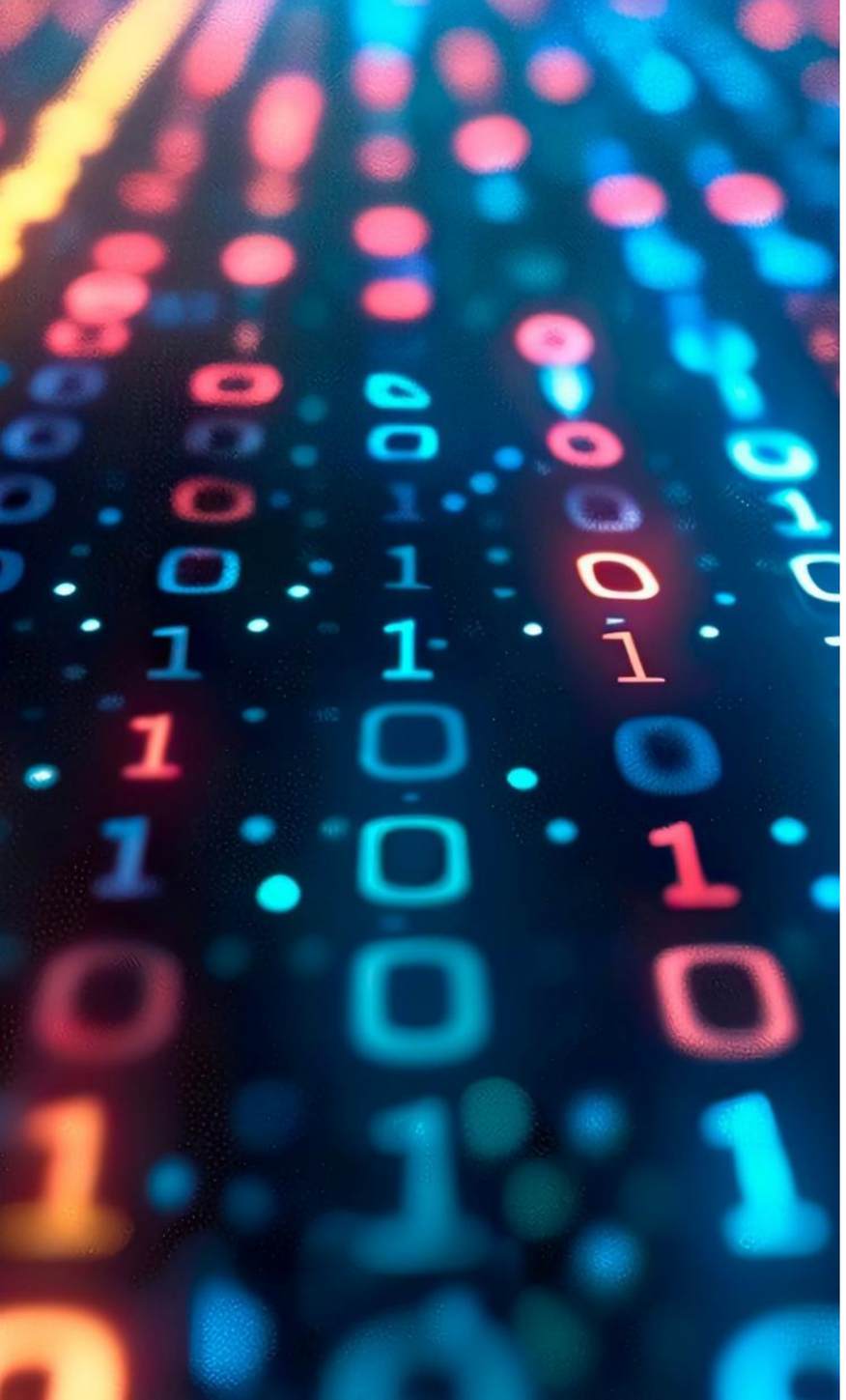
2.1 Allgemeines

2.2 Anwendungsbereich

2.3 Pflichten

2.4 Rechtsfolgen

2.5 To-Dos für Unternehmen



2.1 Allgemeines

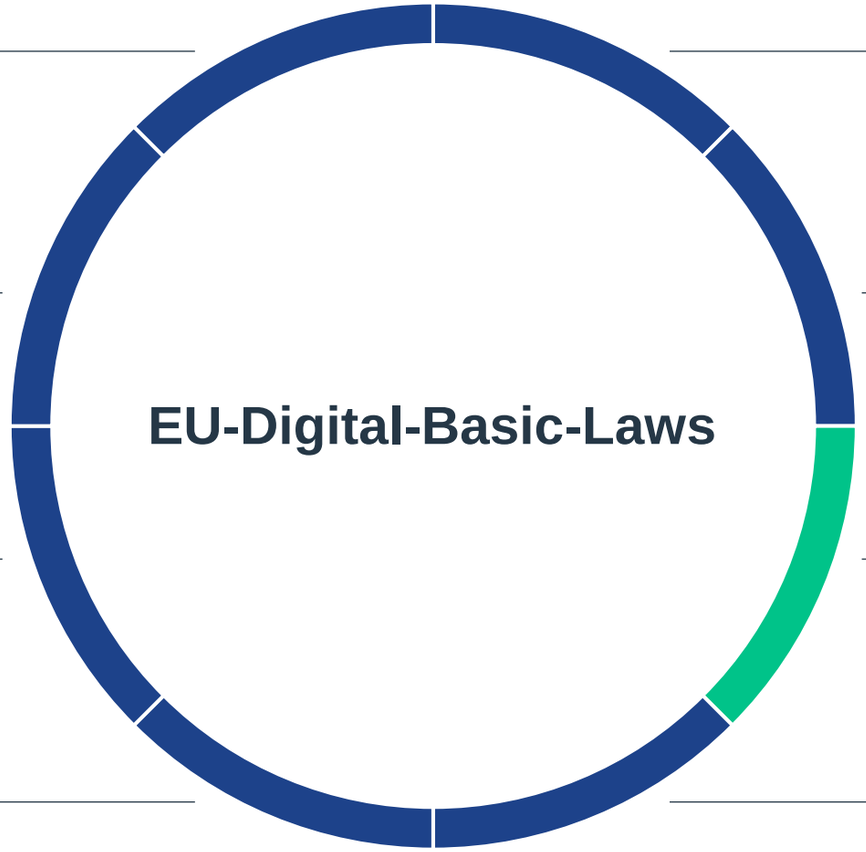
Überblick: „Digital-Basic-Laws”

DSGVO
Datenschutzgrundverordnung

DSA
Digital Services Act

DGA
Data Governance Act

DMA
Digital Markets Act



DA
Data Act

NIS-2-RL
Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union

KI-VO
Verordnung über Künstliche Intelligenz

DORA
Verordnung über die digitale operationale Resilienz im Finanzsektor

Also noch so ein Cybersicherheits-Gesetz?

KRITIS DachG	NIS-2	Cyber Resilience Act (CRA)	IT-SiG / KritisV / BSIG
TDDDG	NIS2UmsuCG	DORA	DSGVO & BDSG

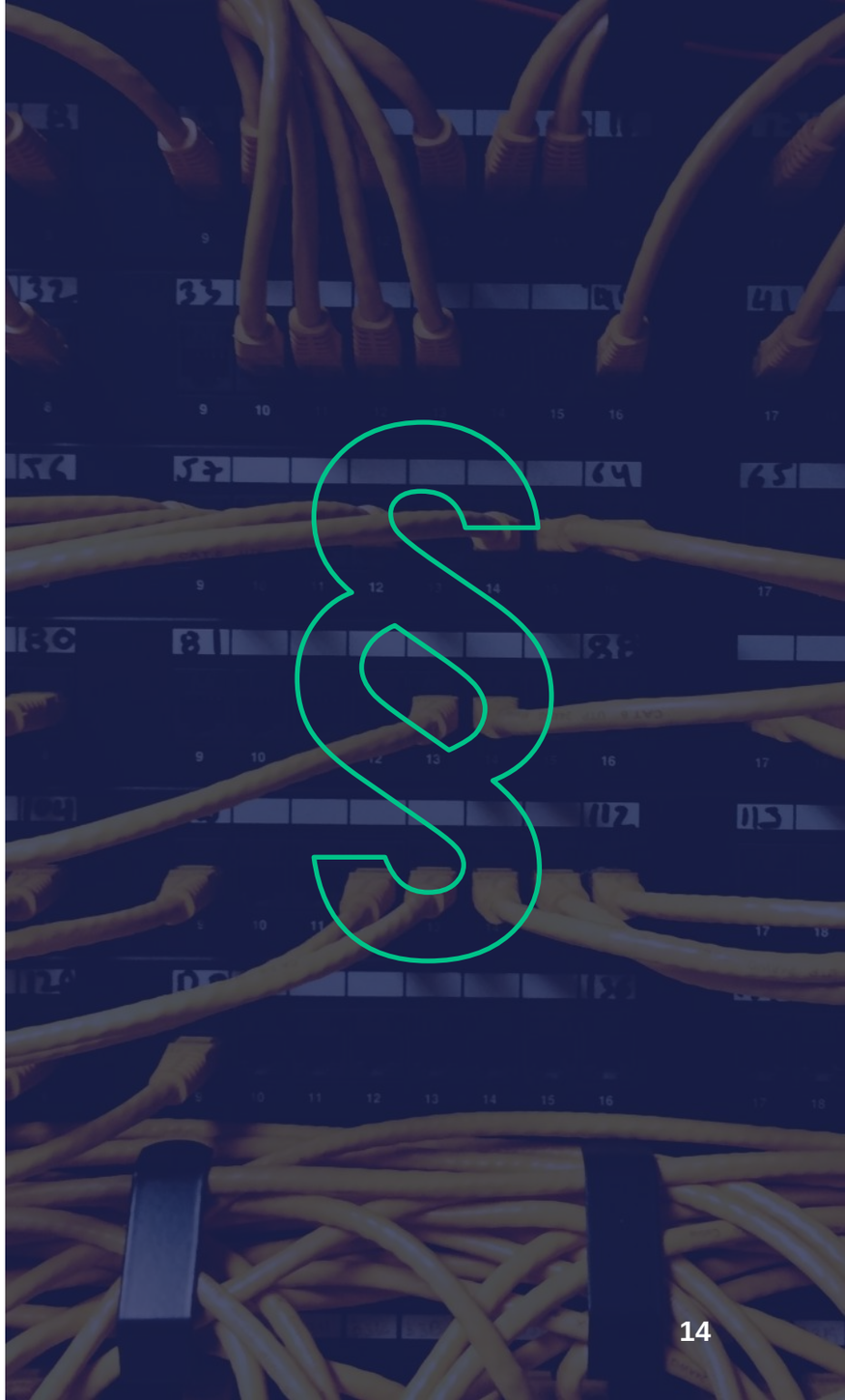
Ziel der NIS-2-Richtlinie

Art. 1 Abs. 1 NIS-2 RL

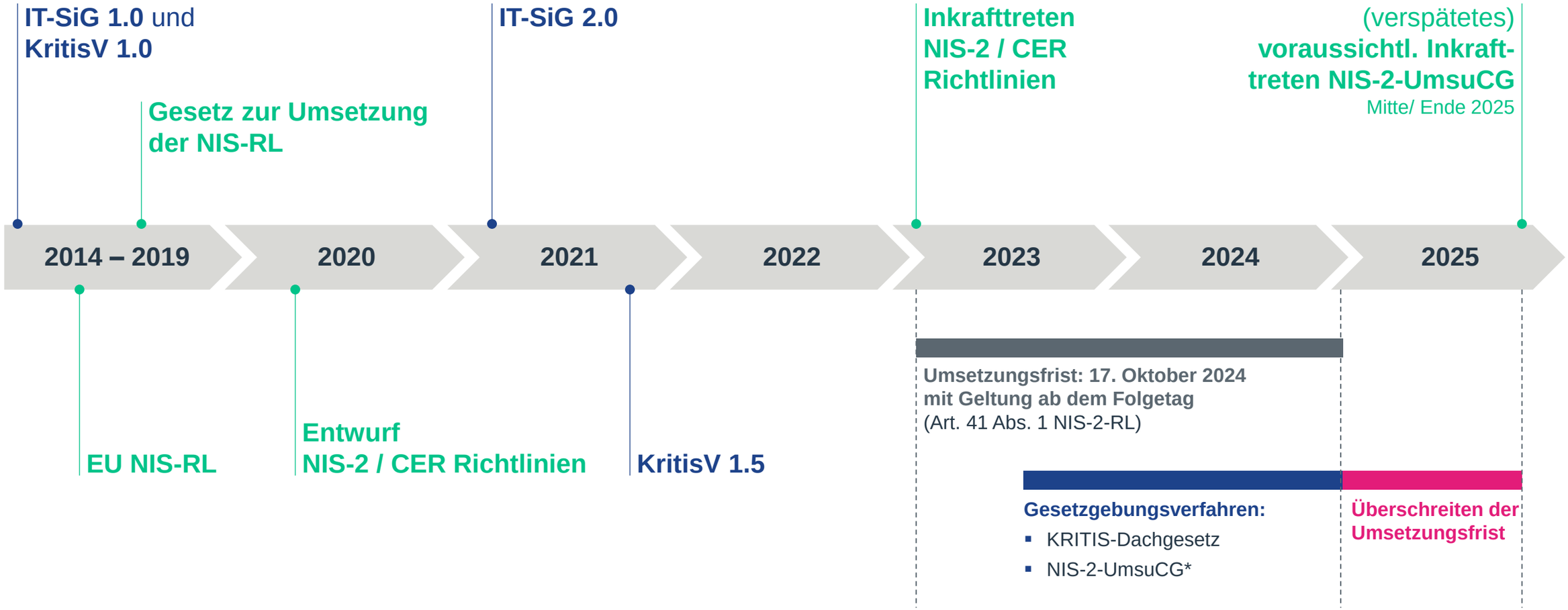
Weiterentwicklung des Cybersicherheitsniveaus der Europäischen Union durch Schaffung eines gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen

Pflichten für Unternehmen

- **Cybersecurity:**
  konkrete Pflichten zum Risikomanagement, Vorfallsmeldungen, technische Maßnahmen und Governance
- **Aufsicht:**
  Registrierungspflicht, Nachweise, Meldepflichten und verbindlicher Informations-austausch



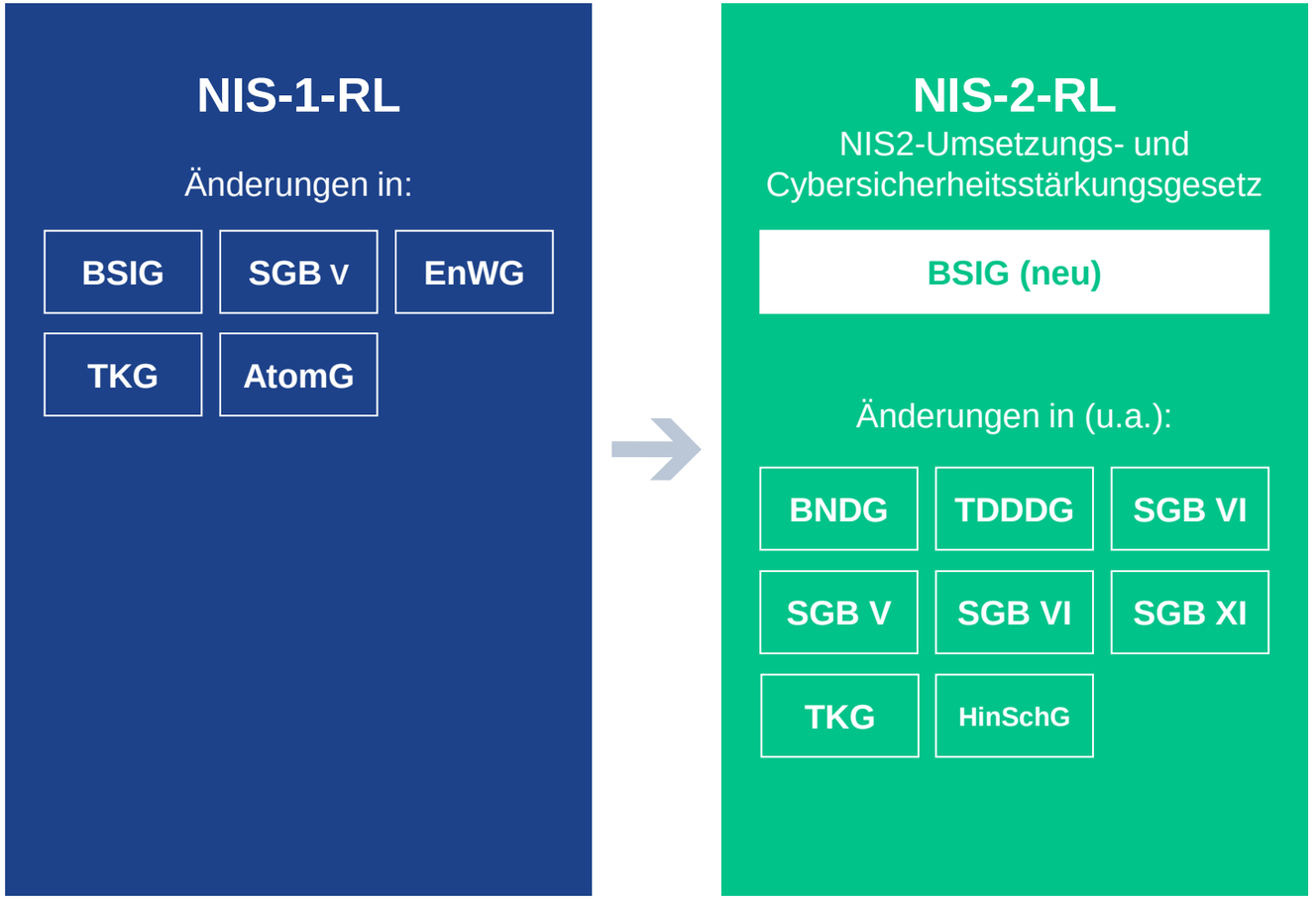
Historie der IT-Sicherheitsregelungen



***NIS-2-UmsuCG:** deutsches NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Wesentliche Änderungen zur bisherigen Rechtslage

1. Weiter **Anwendungsbereich** (*ca. 25.550* neu betroffene Unternehmen)
2. Unterteilung in **wesentliche** und **wichtige Einrichtungen** (Zuordnung wirkt sich auf Pflichtenkatalog der Einrichtung und Durchsetzungsbefugnisse der Behörde aus)
3. Erweiterter **Pflichtenkatalog** für Mitgliedstaaten und wichtige Einrichtungen (v.a. erweiterte Präventionsmaßnahmen, Einbeziehung von Lieferketten)
4. Einstufige **Meldepflicht** → *Dreistufiges* Melderegime
5. Verschärfte **Aufsichts- und Durchsetzungsbefugnisse**



2.2 Anwendungsbereich

TaylorWessing

Anwendungsbereich der NIS-2-Richtlinie

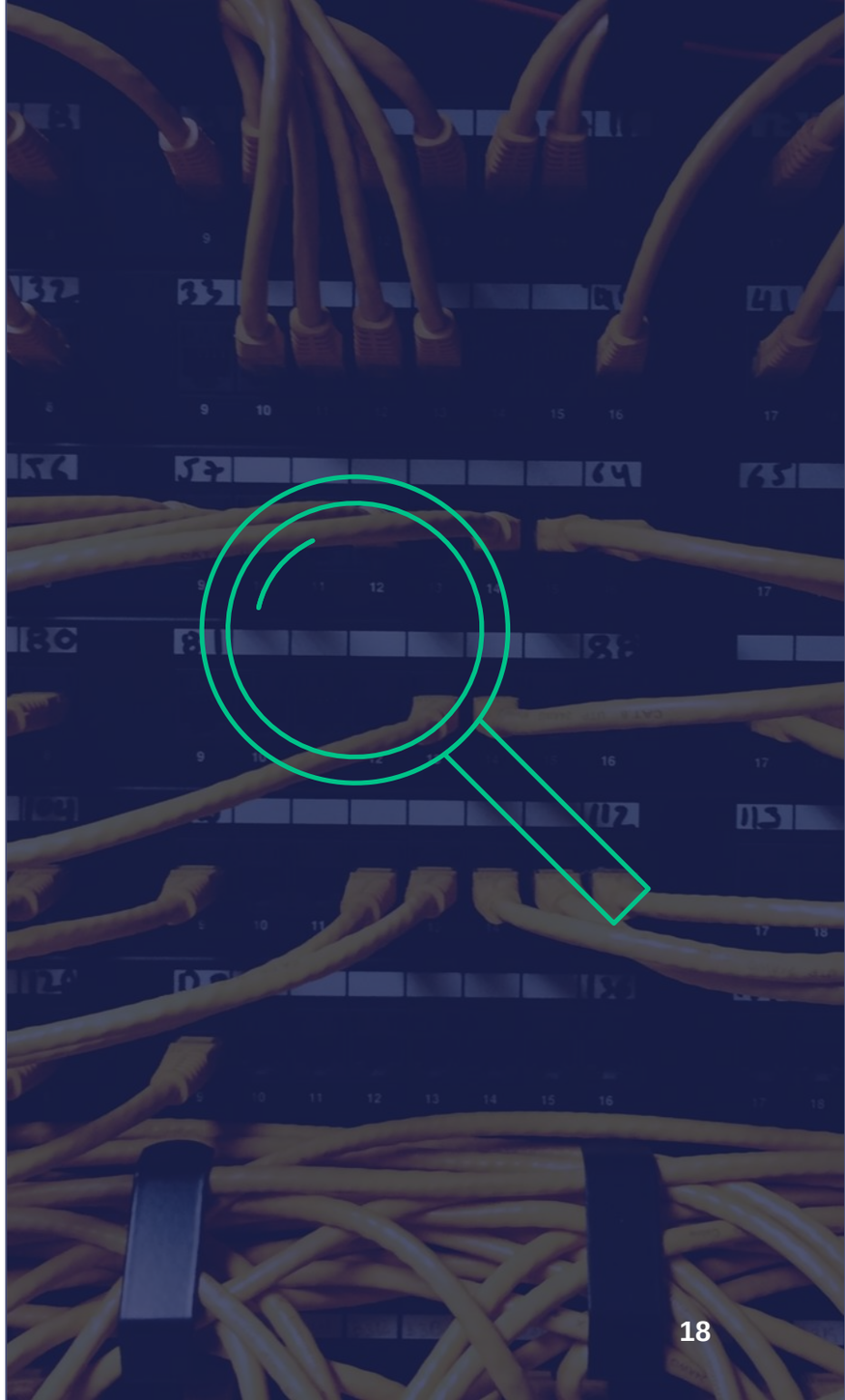
Persönlich: alle Einrichtungen iSd Art. 2 NIS-2-RL // § 28 BSIG-E

- Öffentliche oder private Einrichtungen des Anhang I („hohe Kritikalität“) oder II („sonstige kritische Sektoren“: z.B. Energie, Verkehr, Bankwesen, etc.), wenn Schwellenwerte überschritten werden.
- Klein- und Kleinstunternehmen sind grds. vom Anwendungsbereich der NIS-2-RL ausgenommen. Ausnahmen:
  - *Art. 2 Abs. 2:* unabhängig von der Größe, Dienste z.B. von Vertrauensdienste-anbietern erbracht
  - *Art. 2 Abs. 3, 4:* unabhängig von der Größe auch dann, wenn als kritische Einrichtung eingestuft/ Einrichtung Domänennamenregistrierungsdienste erbringt

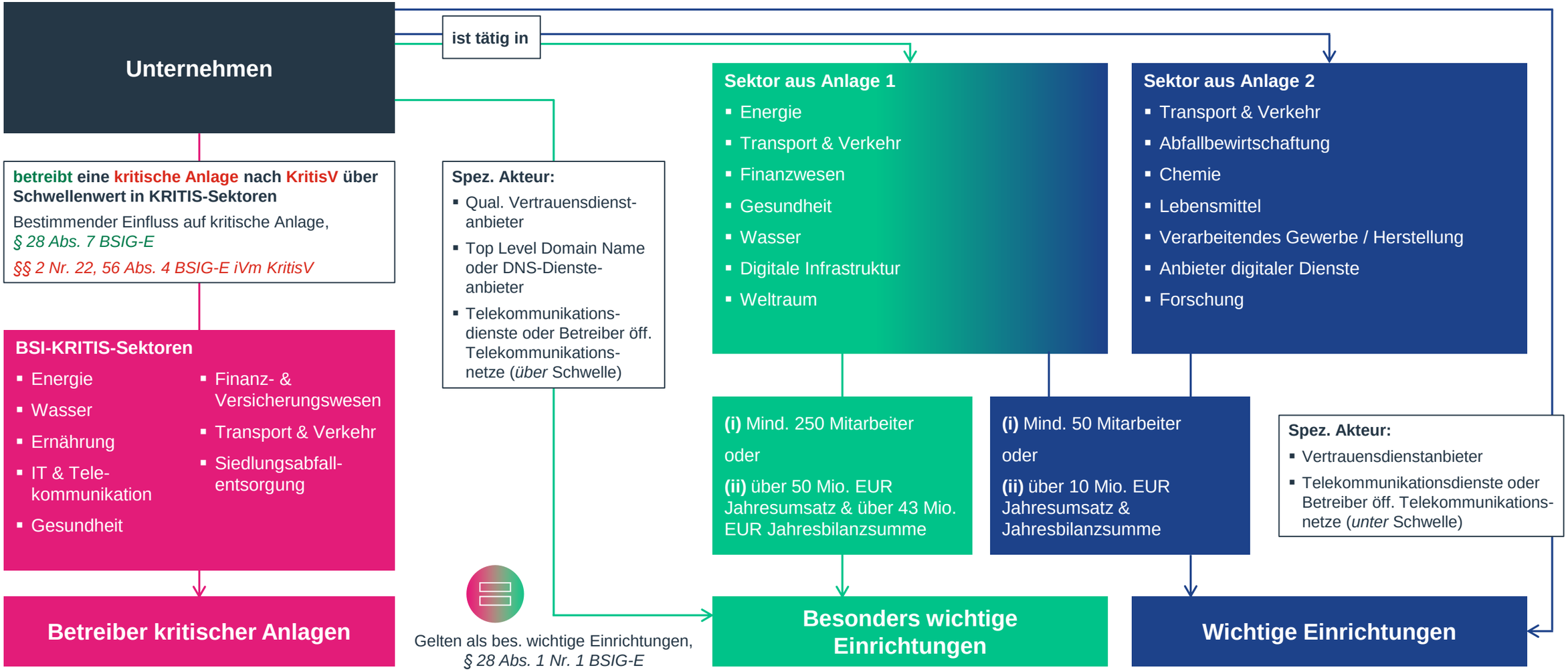
Räumlich:
in den EU-Mitgliedstaaten

Zeitlich:

- **Inkrafttreten:** 16. Januar 2023
- **Umsetzungsfrist:**
  bis zum 18. Oktober 2024
- **In D:** NIS-2-Umsetzungs- und Cyber-sicherheitsstärkungsgesetz



Anwendungsbereich: Umgesetzte NIS-2 Vorgaben
§ 28 BSIG-E



2.3 Pflichten

Pflichten von Betreibern und Einrichtungen

Pflicht	Betreiber kritischer Anlagen	Bes. wichtige Einrichtung	Wichtige Einrichtung
Maßnahmen Risikomanagement, *§ 30*	*	☑	☑
Höhere Maßstäbe für KRITIS, *§ 31 Abs. 1*	☑	⊗	⊗
Besondere Maßnahmen, *§ 31 Abs. 2*	☑	⊗	⊗
Meldepflichten, *§ 32*	*	☑	☑
Registrierung, *§ 33, § 34*	☑	☑	☑
Unterrichtungspflichten (Kunden), *§ 35*	*	☑	☑
Leistungsorgane Umsetzung, *§ 38*	*	☑	☑
Nachweise, *§ 39*	☑	tlw. (§ 61 BSIG-E)	tlw. (§ 62 BSIG-E)

***implizit, da Betreiber kritischer Anlagen auch besonders wichtige Einrichtungen sind,** *§ 28 Abs. 1 Nr. 1 BSIG-E*

Risikomanagementmaßnahmen
§§ 30, 31 BSIG-E

Art. 21 NIS-2-RL

*Einrichtungen müssen geeignete, verhältnismäßige und wirksame **technische und organisatorische Maßnahmen zur Vermeidung von Risiken für die Sicherheit** ihrer Netz- und Informationssysteme treffen.*

§ 30 Abs. 8 und 9 BSIG-E.

*Für besonders wichtige Einrichtungen und Betreiber kritischer Anlagen können **branchenspezifische Sicherheitsstandards** vorgeschlagen und deren Schutzintensität festgestellt werden.*

Mindestanforderungen

- Konzepte in Bezug auf Risikoanalyse und Sicherheit für IT
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs- und Krisenmanagements
- Sicherheit und Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, IT-Komponenten und IT-Prozessen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
- Verfahren zur Cyberhygiene und Schulungen zur Cybersicherheit
- Konzepte und Verfahren zur Kryptografie und Verschlüsselung
- Sicherheit des Personals, Konzepte für Zugriffskontrollen und
- Verwendungen von Multi-Faktor-Authentifizierungen

Angemessenheit der Risikomanagementmaßnahmen
§§ 30, 31 BSIG-E

Wichtige Einrichtungen | **Besonders wichtige Einrichtungen**

§ 30 Abs. 1

Verhältnismäßigkeit der Maßnahmen, Faktoren:

- Ausmaß der Risikoexposition
- Größe der Einrichtung
- Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen
- Schwere der Sicherheitsvorfälle
- Gesellschaftliche und wirtschaftliche Auswirkungen der Sicherheitsvorfälle

Betreiber kritischer Anlagen

§ 31 Abs. 1

*„Für **Betreiber kritischer Anlagen** gelten (…) über das Schutzniveau dieser Einrichtungen [besonders wichtige und wichtige] **hinausgehende Maßnahmen** nach **§ 30 Abs. 1 S. 1** als **verhältnismäßig**, wenn der dafür **erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung** der betroffenen Anlage steht.“*

§ 31 Abs. 2 BSIG-E

Zudem ist als besondere Maßnahme zwingend ein **System zur Erkennung von Angriffen** einzusetzen

Zentrales Element: Meldepflichten
§ 32 BSIG-E

Betreiber kritischer Anlagen*	Besonders wichtige Einrichtungen	Wichtige Einrichtungen

… müssen erhebliche Sicherheitsvorfälle unverzüglich an melden *(Art. 23 NIS-2-RL)*

Innerhalb von 24 Stunden – Frühe Erstmeldung:
Besteht Verdacht auf rechtswidrige oder böswillige Handlungen oder grenzüberschreitende Auswirkungen?

Innerhalb von 72 Stunden – Meldung:
Erste Bewertung, einschließlich Schweregrad, Auswirkungen und Kompromittierungsindikatoren + Aktualisierung der Erstmeldung

Innerhalb eines Monats – Sicherheitsvorfall abgeschlossen: Abschlussmeldung
Ausführliche Beschreibung, ein-schließlich Schweregrad, Auswirkungen, Angaben zur Bedrohung,
bzw. zugrunde liegende Ursachen, getroffene und laufende Abhilfemaßnahmen, ggf. grenz-überschreitende Auswirkungen

Sicherheitsvorfall dauert an: Fortschrittsmeldung

***Für Betreiber kritischer Anlagen weitere Angaben erforderlich (§ 32 Abs. 3 BSIG-E):**
Art der betroffenen Anlage und der kritischen Dienstleistung, Auswirkungen auf diese.

Weitere Pflichten
nach dem NIS-2-UmsuCG

Unterrichtung
§ 35 BSIG-E

Gilt für **Betreiber kritischer Anlagen**, **besonders wichtiger Einrichtungen** und **wichtiger Einrichtungen**

- ***§ 35 Abs. 1 BSIG-E:***
  Anordnungsbefugnis des BSI Kunden über erhebliche Sicherheitsvorfälle zu unterrichten
- ***§ 35 Abs. 2 BSIG-E:***
  Einrichtungen in speziellen Sektoren müssen Kunden und BSI (selbständig) über **Abhilfemaßnahmen** und erhebliche **Cyberbedrohung** unterrichten, *wenn*
  - Interessen des Kunden denjenigen der Einrichtungen überwiegen

Registrierung
§§ 33, 34 BSIG-E

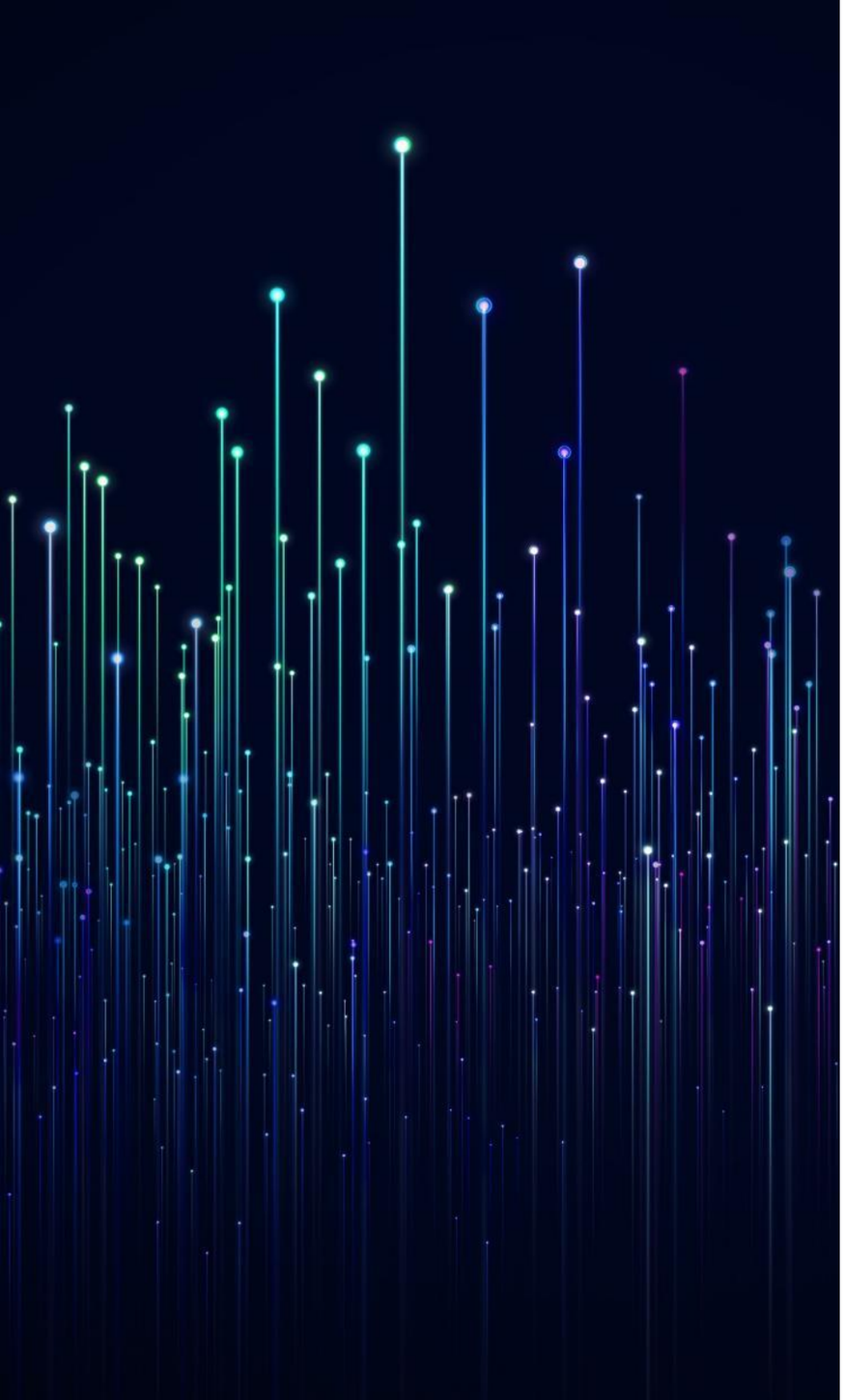
Gilt für **Betreiber kritischer Anlagen**, **besonders wichtiger Einrichtungen**, **wichtiger Einrichtungen** und **Domain-Name-Registry-Diensteanbieter** sowie **speziellen Einrichtungen** nach *§§ 34 Abs. 1, 60 Abs. 1 S. 1 BSIG-E* (z.B. Anbieter von Cloud) deren Hauptniederlassung in Deutschland ist

- **Eigenständige Identifikation und Registrierung**
- **Frist:** 3 Monate
- Weitreichendere Angaben für Betreiber kritischer Anlagen *(§ 33 Abs. 2 BSIG-E)*
- **Missachtung der Registrierung**
  → OWiG + Bußgeld
  *(§§ 65 Abs. 5 Nr. 4, Abs. 2 Nr. 6, Nr. 8 BSIG-E - bis **500 Tsd. EUR**)*
  und **Selbstvornahme der Registrierung BSI**
  (§ 33 Abs. 4 BSIG-E)

Nachweise
§ 39 BSIG-E

Gilt für **Betreiber kritischer Anlagen**

- **Nachweis über (ausreichende) Umsetzung der Risikomanagementmaßnahmen**
  (inkl. System zur Angriffserkennung) – durch:
  - **Sicherheitsaudits**
  - **Prüfungen**
  - **Zertifizierungen**
- Pflicht zur Offenlegung von Sicherheitsmängeln (ggf. Mängelbeseitigungsplan und Beseitigung)
- **Alle drei Jahre**



2.4 | Rechtsfolgen

TaylorWessing

NIS-2-UmsuCG – Aufsicht und Durchsetzung
§§ 61, 62 BSIG-E

Betreiber kritischer Anlagen | **Besonders wichtige Einrichtungen**

§ 61 Abs. 1, Abs. 5 BSIG-E:
Anlasslose Überprüfungsmaßnahmen möglich
→ Stichprobenartig: Audits, Prüfungen oder Zertifizierungen

§ 61 Abs. 3 BSIG-E:
Drei Jahre nach Inkrafttreten können Nachweise über die Erfüllung der Verpflichtungen verlangt werden
→ **Bei Zuwiderhandeln – Maßnahmenkatalog, z.B.:**

- Anweisungen zur Verhütung oder Behebung von Vorfällen
- Anordnung zur Unterrichtung der potenziell Betroffenen eines Cybersicherheitsvorfalls
- Aussetzung der fachrechtsspezifischen Genehmigung
- Vorrübergehende Untersagung der Wahrnehmung der Leitungsaufgaben des Leitungspersonals

Wichtige Einrichtungen

Bei **Anfangsverdacht fehlender Compliance**

§ 62 BSIG-E:
„Rechtfertigen Tatsachen die Annahme, dass (…) Verpflichtungen nicht oder nicht richtig“ umgesetzt sind

§ 61 BSIG-E:
Überprüfung und Maßnahmen möglich,

NIS-2-UmsuCG – Sanktionen
§ 65 BSIG-E

Betreiber kritischer Anlagen

Besonders wichtige Einrichtungen

Bußgeld:

Bis 10 Mio. EUR *(§ 65 Abs. 5 Nr. 1 lit. a)*
wenn Umsatz mehr als 500 Mio. EUR:
bis 2 % des weltw. Jahresumsatzes
(§ 65 Abs. 6)

Bis 1 Mio. EUR *(§ 65 Abs. 5 Nr. 3)*,
Verstoß gegen Nachweispflicht –
nur Betreiber kritischer Anlagen

Wichtige Einrichtungen

Bußgeld:

Bis 7 Mio. EUR *(§ 65 Abs. 5 Nr. 1 lit. b)*
wenn Umsatz mehr als 500 Mio. EUR:
bis 1,4 % des weltw. Jahresumsatzes
(§ 65 Abs. 7)

Allgemeine Bußgeldtatbestände

Bußgeld:

- **Bis 2 Mio. EUR** *(§ 65 Abs. 5 Nr. 2)*
- **Bis 500 Tsd. EUR** *(§ 65 Abs. 5 Nr. 4)*
- **Bis 100 Tsd. EUR** *(§ 65 Abs. 5 Nr. 5)*

2.5 | To-Dos für Unternehmen

TaylorWessing

NIS-2-UmsuCG – To Dos
Übersicht

1. Prüfung: Anwendungsbereich

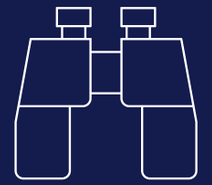
- Betroffenheit des eigenen Unternehmens
- Identifizierung der Rolle:
  - Betreiber kritische Anlage
  - Besonders wichtige Einrichtung
  - Wichtige Einrichtung
- Einschlägige Regulierung? (NIS-2-Pflichten, Dachgesetz-Pflichten)

2. Inaugenscheinnahme von:

- Registrierung
- Umsetzungsplanung der NIS-2-Pflichten → insb. konkrete Risikomanagementmaßnahmen
- Umstrukturierungsmaßnahmen

3. Überwachung & Aktualisierung

- Überwachung der Umsetzung (Letztverantwortung GF)
- Evaluierungsprozesse
- Aktualisierung am Stand der Technik und mit Blick auf neue Gefahrenlagen



3 | Der Weg zur NIS-2 Konformität

TaylorWessing

Was ist zu tun?
§ 30 Risikomanagementmaßnahmen

Umsetzung geeigneter, verhältnismäßiger und wirksamer technischer und organisatorischer Maßnahmen in Bezug auf Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit.

Etablierung eines ISMS

+

- Unterrichtungs-/ & Meldepflichten (bei Vorfällen)
- Nachweispflicht
- Pflichten für Geschäftsführer
- Registrierungspflicht

- InfoSec-**Risikomanagement**-Prozess
- Sicherheit entlang **Lieferkette** (Dienstleistersteuerung)
- Sicherheit entlang des **System-Lifecycles**
- Sicherheit entlang des **Mitarbeiter-Lifecycles**
- Security **Incident Management** Prozess
- Backup & Restore / **Notfall- & Krisenmanagement**
- **Netzwerksicherheit** & Kryptografie
- **Vulnerability Management**
- **Identity- & Access Management** & Multi-Faktor-Authentifizierung
- Prozesse zur **Wirksamkeitsmessung**
- **Security Awareness**

Übliche Vorgehensweise

Gap-Analyse

Framework etablieren

Richtlinien & Prozesse erstellen

InfoSec-Risiko-management

Maßnahmen umsetzen

Internes Audit

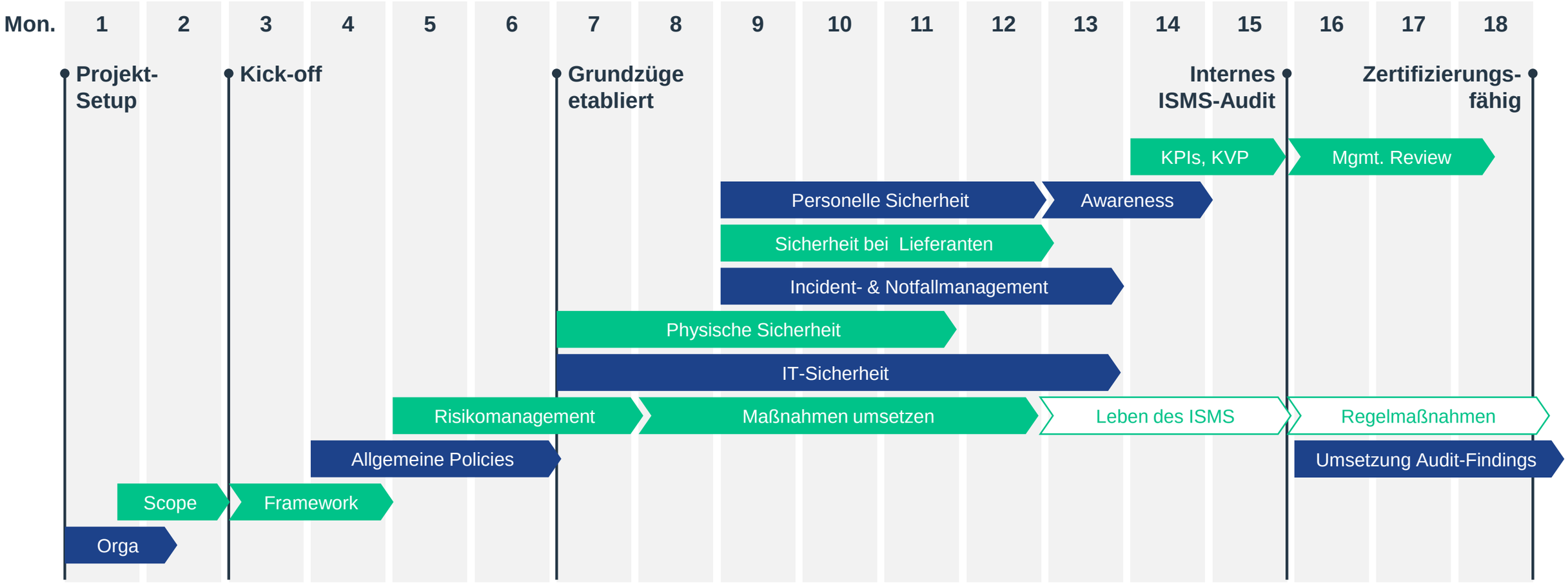
Compliance

NIS-2 Gap-Analyse / Statuserhebung

Zielsetzung	Herausfinden, wo man hinsichtlich der Erfüllung der NIS-2 Anforderungen steht	
Art / Methode	▪ Sichtung von Dokumenten (Konzepte, Richtlinien, Prozesse) ▪ Interview / Befragung der Verantwortlichen	▪ Durchführung von Stichproben und technischen Checks
Referenzstandard	▪ ISO 27001 (zur Orientierung)	▪ Zusätzliche Anforderungen aus NIS-2 und NIS2UmsuCG
Ergebnis	▪ Handlungsbedarf hinsichtlich NIS-2 Compliance ▪ Auditbericht mit Abweichungen um Umsetzungsempfehlungen	▪ Aufwandschätzung zur NIS-2 Compliance ▪ Roadmap mit den wichtigsten Schritten und Meilensteinen
Benötigte Ansprechpartner	▪ IT (Netzwerk, Betrieb, Identity Management, Incident Management, …) ▪ Informationssicherheit ▪ Personalwesen	▪ Unternehmenssicherheit ▪ Einkauf/Beschaffung
		Dauer: ca. 2–4 Tage

Hinweis: wer die ISO 27001 umgesetzt hat, ist bereits gut aufgestellt

typische Roadmap
18 Monate



Wieviel Aufwand bedeutet das?

Kunde A (Produktion / Stahlerzeugung)

- **Zeitraum:** 14 Monate
- **Mitarbeiter:** ca. 1.000 (1 Standort)
- **NIS-2-Relevanz:** wichtige Einrichtung
- **Ziele:**
  - ISO 27001-Niveau (wurde am Projektende zertifiziert)
  - HvS als Know-How Träger / Consultant, ISMS soll nach Projektende selbständig weiterentwickelt werden
- **Kundensituation:**
  - internes Projektteam: 7 Personen (IT, HR, Einkauf)
  - hoher „Pragmatismus“
  - ISMS-Knowhow und -Team vorhanden
  - viele Richtlinien schon vorhanden

- **Auftragsvolumen:** ca. 30 PT
- **Ausmaß:** ca. 0,5 PT / Woche

Kunde B (Produktion / Pharma)

- **Zeitraum:** 12 Monate
- **Mitarbeiter:** ca. 120 (1 Standort)
- **NIS-2-Relevanz:** wichtige Einrichtung
- **Ziele:**
  - ISMS etablieren aber nicht zertifizieren
  - ISB-Rolle im Rahmen des Projekts aufbauen (Know-How Transfer durch HvS)
- **Kundensituation:**
  - internes Projektteam: 2 Personen (IT)
  - Aktuell kein ISMS (Fokus auf IT-Security)
  - Kaum Dokumentation / Richtlinien vorhanden
  - wenig ISMS / ISO 27001-Vorerfahrung
  - QM-System vorhanden (ISO 9001 Zertifizierung)

- **Auftragsvolumen:** ca. 50 PT
- **Ausmaß:** ca. 1 PT / Woche

Schulungspflichten

Alle Mitarbeiter

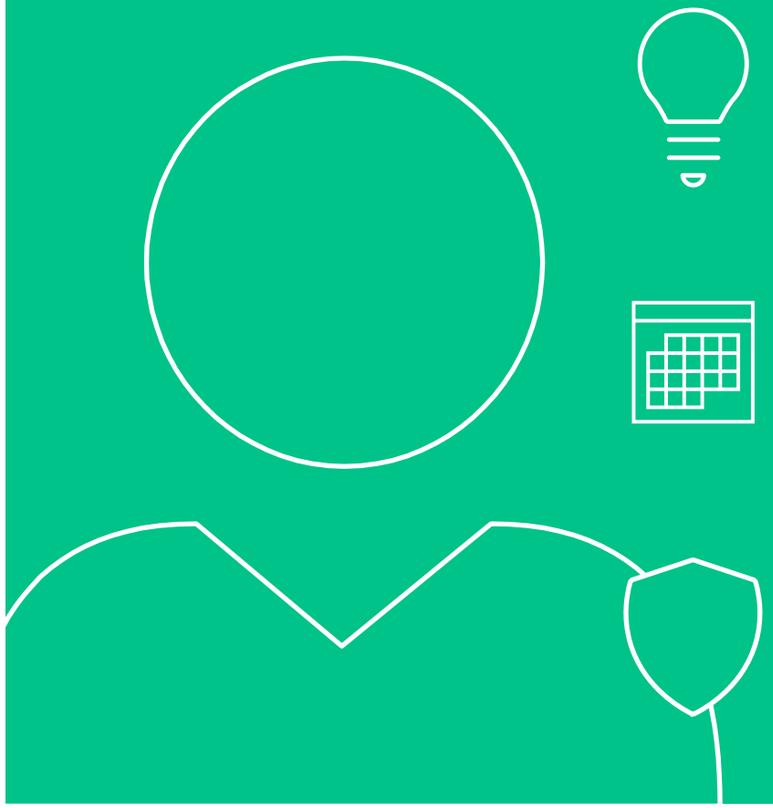
Anwender | Manager

Experten
- Spezielle Themen

Fortgeschritten
- Live Events
- Sonderthemen (ISMS, Priv. Accounts, …)

Grundlagen
- Security E-Learning

Call-to-action



HvS
Dauer: ca. 12 Monate

TaylorWessing
Umsetzung bis: ?

Nicht warten, jetzt starten!

Q&A

TaylorWessing

Wer sind wir?

Mario Melmer
Head of Information Security HvS

mario.melmer@hvs-consulting.de
www.hvs-consulting.de

Beratungsschwerpunkte

- Etablierung ISMS
- InfoSec-Consulting & -Coaching
- ISMS Audits und -Gap Analysen
- IT-Notfall & Krisenmanagement
- Stv. Prüfstellenleiter für Prüfungen gem. §8 BSIG (KRITIS)
- Lead Auditor für ISO 27001

Dr. Axel Freiherr von dem Bussche
LL.M. (L.S.E.), CIPP/E

a.bussche@taylorwessing.com
www.taylorwessing.com

Beratungsschwerpunkte

- Informationstechnologie
- Telekommunikation
- Datenschutz
- Urheber- & Medienrecht
- Litigation & Dispute Resolution
- Technology, Media & Communications

Chambers RANKED IN Europe 2024 Axel von dem Bussche

The LEGAL 500 DEUTSCHLAND FÜHRENDE NAMEN 2024

TaylorWessing

Vielen Dank!

Europa > Mittlerer Osten > Asien

taylorwessing.com