NIS-2: Der neue Taktgeber für Cyber-Resilienz

Organisation, Strategie und Maßnahmen als Dirigent für Ihre Sicherheit und die Umsetzung der NIS2-Anforderungen

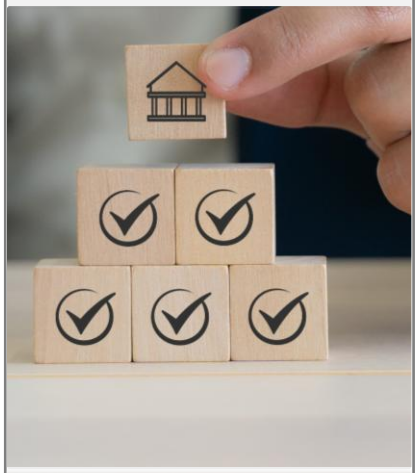
Daniel Kammerbauer, Team Lead GRC, Controlware GmbH

NIS-2

Registrierungspflicht
§33

Meldepflicht
§32

Pflichten für Leitungsorgane
§38



Fachliche Anforderungen
§30ff

NIS-2

heise online

BSI: 11.500 kritische Einrichtungen unter NIS2 registriert

06.03.2026 17:09 Uhr Falk Steiner

(Bild: khunkornStudio / Shutterstock.com)

Zum Registrierungsfristende haben tausende Unternehmen den Prozess abgeschlossen – doch knapp 20.000 fehlen wohl noch.

Bis zum heutigen Stichtag haben sich etwa 11.500 Behörden, Unternehmen und andere kritische Einrichtungen unter dem neuen NIS2-Regime beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registriert. Das teilte ein Sprecher der Bonner Behörde am Nachmittag auf Anfrage von heise online mit.

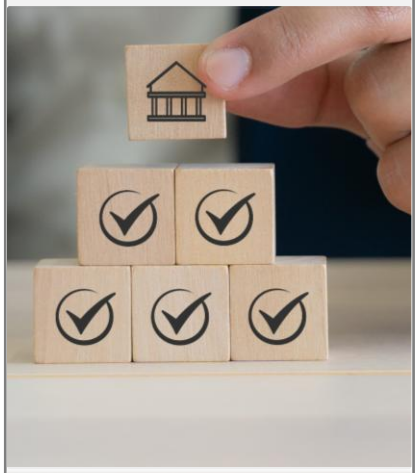
Über 4.000 der nun beim BSI als Betreiber kritischer Anlagen hinterlegten Akteure hätten die Registrierung innerhalb der vergangenen Woche vollzogen. Mitte Februar hatte die Gesamtzahl noch deutlich niedriger

NIS-2

Registrierungspflicht
§33

Meldepflicht
§32

Pflichten für Leitungsorgane
§38



Fachliche Anforderungen
§30ff

NIS-2

Wir unterstützen Sie gerne
sprechen Sie uns an!

Registrierungspflicht

- **Veröffentlichung** des Umsetzungsgesetzes zum **05.12.2025**
- Betroffenheitsanalyse per Legal Entity
- **Rechtsberatung dringend empfohlen**
- **Frist zur Registrierung** bis zum **06.03.2026**
- Registrierung erfolgt zweistufig (MuK, BSI-Portal)

NIS-2

Wir unterstützen Sie gerne
sprechen Sie uns an!

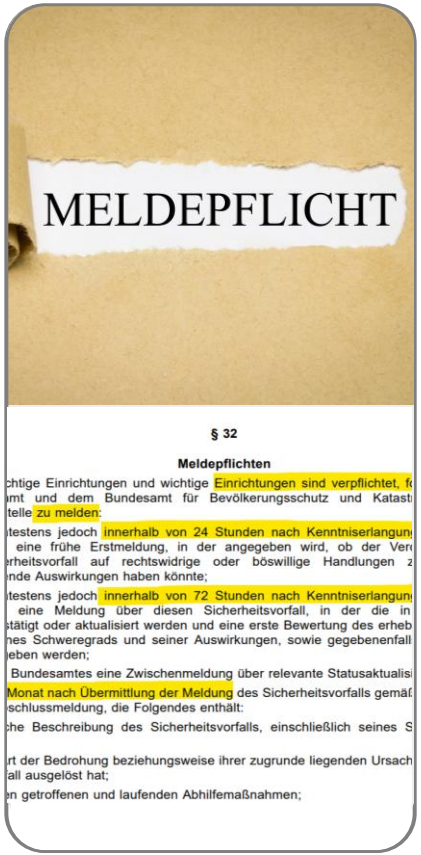
Registrierungspflicht

- **Veröffentlichung** des Umsetzungsgesetzes zum **05.12.2025**
- Betroffenheitsanalyse per Legal Entity
- **Rechtsberatung dringend empfohlen**
- **Frist zur Registrierung** bis zum **06.03.2026**
- Registrierung erfolgt zweistufig (MuK, BSI-Portal)

NIS-2

Meldepflicht

- **„Erhebliche“** Sicherheitsvorfälle
- **Dreistufig – 24h/72h/30d**
- **Inhalt der Meldung ist abhängig der Stufe** und enthält u.a. Schwere, Auswirkung, Ursache, Abhilfemaßnahmen
- **Nähere Definition** in den **Gesetzestexten** oder den **NIS-2-Infopaketen des BSI**

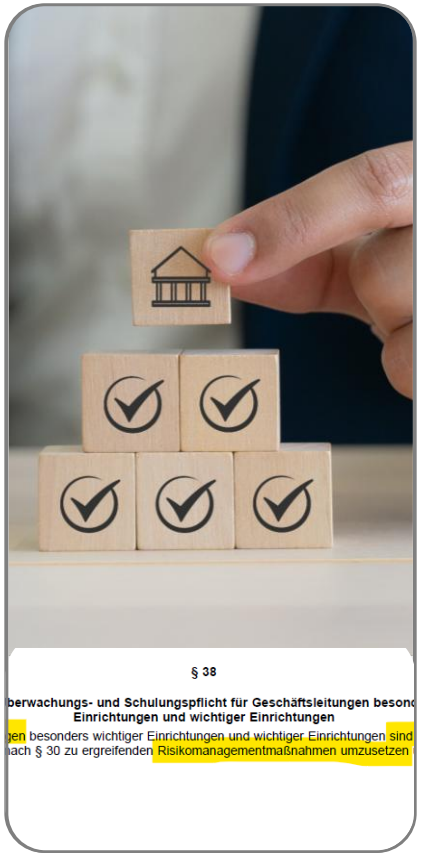


NIS-2

Wir unterstützen Sie gerne sprechen Sie uns an!

Pflichten für Leitungsorgane

- **Delegierbare Umsetzung** der zu ergreifenden Risiko-Management-Maßnahmen**, aber direkte Überwachung!**
- **Schulungspflicht**, **um ihre Rolle im Risiko-Management** und die Überwachungspflicht **ausfüllen zu können – Regelmäßig** oder bei besonderen Ereignissen **durchzuführen**
- **Nähere, inhaltliche Definition der Schulungspflicht** in den Gesetzesbegründungen



NIS-2

Wir unterstützen Sie gerne
sprechen Sie uns an!

Fachliche Anforderungen

- **Abstufung für die unterschiedlichen Einrichtungsarten** (KRITIS > bes. wicht. Einrichtung und wichtige Einrichtungen - u.a. § 31)
- **Verpflichtende Grundsätze:** verhältnismäßig dem jeweiligen Risiko, wirksam, gefahrenübergreifend
- **Verhältnismäßigkeit** ist zu **bewerten** und zu **dokumentieren**
- **Orientierung an** bekannten **Standards & Normen**
- **Säulen der fachlichen Anforderungen (u.a. § 30)**, mit hohem **Gestaltungsspielraum**

Risikoanalyse / -management

technische und organisatorische Maßnahmen

Bewertung der Wirksamkeit

NIS-2

Fachliche Anforderungen

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Quizfrage zum Mitnehmen:

Welche Rollen und davon abgeleitet Personen in Ihrer Organisation können die Rolle eines Risikoeigentümers einnehmen und dürfen aktiv Risiken akzeptieren?

NIS-2

Fachliche Anforderungen, am Beispiel § 30, Abs. 2, Nr. 2

‚Bewältigung von Sicherheitsvorfällen‘

Spezifizierung gemäß EU-Durchführungs-verordnung 2024/2690*	ISO 27001:2022	RUN**	Cyber Risiko Check (CRC)
Konzept für die Bewältigung von Sicherheitsvorfällen	A.5.24	ISMS - Informationssicherheitsstrategie SzA - IS-Vorfallsmanagement	03, 04-1, 04-2 *(Hinweis: allgemeine Punkte, keine spezifische Zuordnung zu den Unterpunkten)*
Überwachung und Protokollierung	A.5.28, A.8.15, A.8.16, A.8.17	SzA - Protokollierung	
Meldung von Ereignissen	A.6.8	SzA - IS-Vorfallsmanagement	
Bewertung und Klassifizierung von Ereignissen	A.5.25	SzA - Angriffserkennung	
Reaktion auf Sicherheitsvorfälle	A.5.26	SzA - IS-Vorfallsmanagement	
Überprüfungen nach Sicherheitsvorfällen	A.5.27	ISMS - Audit und Revision (Compliance) ISMS - Kontinuierliche Verbesserung BCMS - Audit und Revision (Compliance) BCMS - Kontinuierliche Verbesserung	

NIS-2

Wir unterstützen Sie gerne sprechen Sie uns an!

Fachliche Anforderungen, am Beispiel § 30, Abs. 2, Nr. 2

‚Bewältigung von Sicherheitsvorfällen'

Spezifizierung gemäß EU-Durchführungs-verordnung 2024/2690*	ISO 27001:2022	RUN**	Cyber Risiko Check (CRC)
Konzept für die Bewältigung von Sicherheitsvorfällen	A.5.24	ISMS - Informationssicher trategie SzA - IS-Vorfallsmanagem	
Überwachung und Protokollierung	A.5.28, A.8.15, A.8.16, A.8.17	SzA - Protokollier	
Meldung von Ereignissen	A.6.8	SzA - IS-Vorfallsmanagem	
Bewertung und Klassifizierung von Ereignissen	A.5.25	SzA - Angriffserke	
Reaktion auf Sicherheitsvorfälle	A.5.26	SzA - IS-Vorfallsmanagem	
Überprüfungen nach Sicherheitsvorfällen	A.5.27	ISMS - Audit und Revision (Compli ISMS - Kontinuer Verbesserung BCMS - Audit unc Revision (Compliar BCMS - Kontinuierliche Verbesserung	

Spezifizierung gemäß EU-Durchführungsverordnung 2024/2690*	Aktuelle Grundschutz-Praktiken: Sicherheitsvorfallsbearbeitung	Detektion	Monitoring-Evaluation
Konzept für die Bewältigung von Sicherheitsvorfällen	REA.1.1, REA.1.1.1, REA.1.1.2 REA.1.1.3 REA.1.2 REA.1.3	DET.1.1 DET.1.1.1 DET.1.1.2 DET.1.1.3 DET.1.2	
Überwachung und Protokollierung	REA.2.4	DET.3.1 DET.3.1.1 DET.3.1.2 DET.3.1.3 DET.3.1.4 DET.3.1.5 DET.3.1.6 DET.3.1.7 DET.3.1.8 DET.3.1.9 DET.3.1.10 DET.3.1.11	PERF.4.1

NIS-2

Wir unterstützen Sie gerne
sprechen Sie uns an!

Fachliche Anforderungen, am Beispiel § 30, Abs. 2, Nr. 3

‚Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement ‘

Spezifizierung gemäß EU-Durchführungs-verordnung 2024/2690	ISO 27001:2022	TISAX (Trusted Information Security Assessment Exchange)	RUN (Reife- und Umsetzungsgrad-bewertung im Rahmen der Nachweisprüfung)
Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs	A5.29, A. 5.30	1.6.3, 5.2.8, 5.2.9	BCMS - Aufrechterhaltung des Betriebs BCMS - Erproben der Notfallpläne
Backup-Sicherungs- und Redundanzmanagement	A.8.13, A.8.14	1.6.3, 5.2.8, 5.2.9	BCMS Datensicherung & Wiederherstellung
Krisenmanagement	A.5.26, A.5.29, A.5.30	1.6.3, 5.2.8, 5.2.9	BCMS - Geltungsbereich BCMS - Krisenmanagement BCMS - Gesicherte Notfallkommunikationssysteme BCMS - Effektive Behandlung der Kontinuitätsrisiken BCMS - Audit und Revision (Compliance) BCMS - Kontinuierliche Verbesserung
Unterstützende Versorgungsleistungen	A. 7.11	1.6.3, 5.2.8, 5.2.9	PhyM - Wartung PhyM - Versorgungs-einrichtungen

NIS-2

Wir unterstützen Sie gerne
sprechen Sie uns an!

Fachliche Anforderungen, am Beispiel § 30, Abs. 2, Nr. 3

‚Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement ‘

Spezifizierung gemäß EU-Durchführungs-verordnung 2024/2690	ISO 27001:2022	TISAX (Trusted Information Security Assessment Exchange)	RUN (Reife- und Umsetzungsgrad-bewertung im Rahmen der Nachweisprüfung)
Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs	A5.29, A. 5.30	1.6.3, 5.2.8, 5.2.9	BCMS - Aufrechterhaltung des Betriebs BCMS - Erproben der Notfallpläne
Backup-Sicherungs- und Redundanzmanagement	A.8.13, A.8.14		
Krisenmanagement	A.5.26, A.5.29, A.5.		
Unterstützende Versorgungsleistungen	A. 7.11		

Anforderung/Praktik	Notfallplanung	Sicherheitsvorfalls-Behandlung
Notfallplan für die Aufrechterhaltung und Wiederherstellung des Betriebs	NOT.1.1, NOT.1.1.1, NOT.1.1.2, NOT.1.1.3, NOT.1.1.4 NOT.3.1, NOT.3.2, NOT.3.3, NOT.3.4,NOT.3.5, NOT.3.6	REA.2.6.5
Backup-Sicherungs- und Redundanzmanagement	NOT.4.1, NOT.4.2, NOT.4.3, NOT.4.4, NOT.4.5, NOT.4.5.1, NOT.4.5.2, NOT.4.6, NOT.4.7, NOT.4.8, NOT.4.9, NOT.4.10, NOT.4.10, NOT.4.11, NOT.4.12, NOT.4.13, NOT.4.14, NOT.4.15, NOT.4.16, NOT.4.16.1, NOT.4.17	
Krisenmanagement	NOT.2.1, NOT.2.1.1, NOT.2.1.2, NOT.2.1.3, NOT.2.1.4	REA.2.6.5

NIS-2

Wir unterstützen Sie gerne
sprechen Sie uns an!

Organisation

- **Verantwortung und Mandat klären**
- Rollenmodell schärfen
- Gremien- und Entscheidungswege definieren
- Zusammenspiel IT – Fachbereiche – Legal – Informationssicherheit festlegen

Strategie

- Umfeld- und NIS-2-Betroffenheit analysieren (lassen)
- Programm- und Projektmanagement für NIS-2 aufsetzen
- Zielbild festlegen
- Risiko- & Gap-Analyse durchführen
- Roadmap und Prioritäten ableiten
- Anfangen und Spuren hinterlassen

Maßnahmen

- Betroffene Organisation registrieren
- Pflicht gemäß §38 wahrnehmen (Geschäftsführerschulung) und **Leitung mitnehmen**
- Meldeprozess & Incident-Playbooks definieren
- PDCA-Zyklus für Informationssicherheit verankern (ISMS)
- Sicherheitsarchitektur modernisieren

Passt doch eigentlich alles …?

Verantwortung
ISB ist benannt.
AKVs definiert.

Regelwerk
aus Richtlinien und Vorgaben für die Informationssicherheit und den IT-Betrieb existieren

Technische und organisatorische Maßnahmen
präventiv, detektiv, reaktiv

Der Graben zwischen Regelwerk und Wirklichkeit

Passt doch alles …, oder nicht?

Scoping,
Komplexität –
Impact auf Abläufe
und Infrastruktur

Zielbild
funk. & techn.
Anforderungsanalyse
Make / Consult / Buy / Service

Transition-/Migrationsplanung
Betriebsrelevante Aspekte
Abnahme

Go-Live

Idee / Bedarf → **Konzept / Auswahl** → **Umsetzung** → **Go-Live** → **Betrieb**

Technische
Anforderung -
funktionaler Bedarf
wird aufgedeckt

Design
POC
Auswahl

Technische
Umsetzung
Testing

Einführungsphase

Regelbetrieb

Feinkonzeption
Integration
Prozessdesign

Änderungen und
Optimierungen


‚By-Design‘ heißt:
Eingebaut. Nicht angeflanscht.


Wie integriere ich
Governance & Compliance-by-Design
in Prozesse, Projekte und
Infrastrukturen?

‚By-Design‘ heißt: Transparenz

Was sichtbar ist, kann gesteuert werden.
Ohne Transparenz hören Sie immer nur den Knall – nie das, was davor schiefgelaufen ist.

Transparenz

Was sichtbar ist, kann gesteuert werden. Ohne Transparenz hören Sie immer nur den Knall – nie das, was davor schiefgelaufen ist.

Schritte

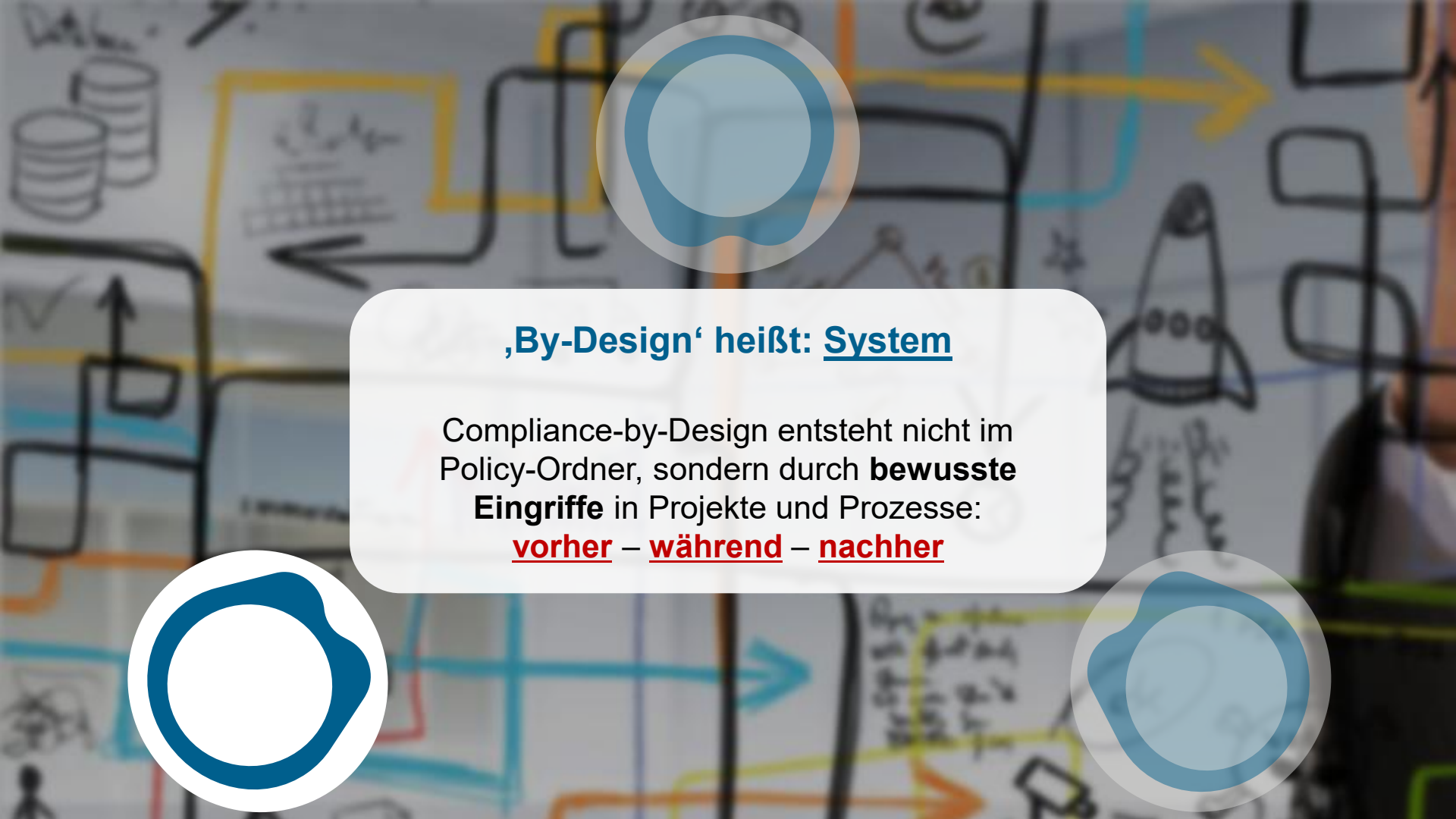
- Kritische Geschäftsprozesse/Services identifizieren und Abhängigkeiten modellieren
- Pro Service: Business Owner, IT-Owner, Schutzbedarf, Regulierungsrelevanz
- Security-/Compliance-Impact-Prüfung in Projekten verankern (“Hand heben”)
- Beispiel:
  - z.B. Gate 0 in Projekten - Security-Impact-Check
  - z.B. Security Impact Analyse in Changes

Was braucht es?

- Minimales Datenmodell
- Verantwortlichkeiten & Awareness
- Vorgefertigte, schlanke Impact Checks

KPIs

- % Anteil der Services mit Schutzbedarf und Owner
- % Anteil der Projekte mit durchgeführter Impact-Prüfung zum vorgegebenen Zeitpunkt



‚By-Design‘ heißt: System

Compliance-by-Design entsteht nicht im Policy-Ordner, sondern durch **bewusste Eingriffe** in Projekte und Prozesse:
vorher – **während** – **nachher**

System und Prozess-Integration

„Security- / Compliance-by-Design entsteht nicht im Policy-Ordner, sondern in drei harten Eingriffen in Projekten und Prozessen:

vorher - während - nachher

Schritte

- Betriebs- und Rollenmodell für Informationssicherheit festlegen
- Gates / Steps in Projektmethodik integrieren
  - Impact + Scope + Anforderungen
  - Controls & Risiken im Design
  - Review vor Go-Live
- Security-Steps als Teil der Definition of Done in den Prozessen und Abläufen
- Kontinuierliche Überprüfung der Wirksamkeit und Verhältnismäßigkeit

Was brauchts?

- Management-Mandat
- Risikobasierter PDCA-Zyklus & RACI-Matrix
- Anpassung von Prozessen und Vorgehensweisen

KPIs

- % Projekte mit nachweislich durchlaufenen Security-Gates
- Anzahl der Security-Showstopper kurz vor Go-Live

‚By-Design‘ heißt: Umsetzung

Technologie alleine macht nicht ‚compliant‘ –
das **„Wie“** entscheidet

Umsetzung

Technologie alleine macht nicht ‚compliant' – das ‚Wie' entscheidet.

Schritte

- Anforderungsanalyse (Regulatorik-Richtlinien-Governance) bestenfalls aus SSOT mit Cross-Walk
- Compliance-by-Design: Policies-/Controls-as-Code, Control-Maßnahmen-Mapping, Integration in Betriebsprozesse
- Evidence-by-Design: definierte, ggf. automatisierte Nachweisführung
- Berücksichtigung von Überprüfungs- und "Rezertifizierungs"-Anforderungen / -prozessen bereits im Konzept und Design

Was brauchts?

- ISMS-/GRC-Plattform als Orchestartor
- Zusammenarbeit
- Übersetzer
- minimale Integrationsarchitektur

KPIs

- • % der Controls mit automatisierter Evidence-Generierung (Ziel > 80 %)
- Durchlaufzeit & Abschlussquote von Überprüfungs- und Rezertifizierungszyklen (> 95 %)

Das Musikstück der Security, Regulatorik und des täglichen Betriebs

Drei Erkenntnisse. Ein Takt. Ihre Entscheidung.

1 Schaffen Sie Transparenz

Was wichtig ist.
Was Aufmerksamkeit benötigt.
Was Security-Impact hat.

2 Entwickeln Sie ein System

Risiko-basierte Maßnahmen.
Integriert in Abläufe und Prozesse.
Eingebaut. Nicht angeflanscht.
Verhältnismäßig.
Verlässlich getan.

3 Gestalten Sie die Umsetzung

Kern der Anforderung treffen.
Innovative Technologie & effiziente Compliance zusammenbringen.
Heute schon an die Nachweise & Audits von Morgen denken.

IT-Security
Roadshow 2026

controlware

Danke für Ihre Aufmerksamkeit.