Deloitte.

Together makes progress

Regulierung trifft Finanzierung
NIS2-Compliance im Krankenhaus durch strategische Fördermittelplanung

Regulierung wirkt nur dann, wenn sie operativ und finanziell umsetzbar ist.

Die neue NIS2[1]- und KRITIS-Gesetzgebung fordert das deutsche Gesundheitswesen heraus wie kaum eine andere Regulierung zuvor. Krankenhäuser müssen sich binnen drei Monaten registrieren, Meldeprozesse einführen und ihre Leitungsorgane unmittelbar in die Verantwortung nehmen – ohne Übergangsfristen und mit deutlich verschärfter Haftung. Gleichzeitig stehen Kliniken vor massiven wirtschaftlichen Herausforderungen, verfügen jedoch nur über begrenzte Mittel für Digitalisierung, Resilienz und Cybersicherheit. Das Ergebnis: ein struktureller Zielkonflikt zwischen gesetzlichen Anforderungen, technischer Realität und finanzieller Machbarkeit. Zugleich eröffnet der Krankenhaustransformationsfonds (KHTF[2]) eine seltene Chance, diesen Zielkonflikt aufzulösen, indem er regulatorische Anforderungen mit planbaren Finanzierungsstrukturen verbindet und damit die dringend notwendige Cyber- und Resilienztransformation ermöglicht.

[1] Network and Information Security.
[2] Krankenhaustransformationsfonds.

Warum jetzt? Cyberangriffe auf dem Vormarsch

Die Bedrohungslage verschärft sich, die gesetzliche Regulatorik wird an bestehende Bedarfe angepasst sowie spezifiziert und die Finanzierungsmöglichkeiten verändern sich – und das alles gleichzeitig. Kliniken müssen daher Cybersicherheit, Resilienz digitale Transformation und regulatorische Compliance nicht nur parallel, sondern integriert denken. Und genau hier entsteht der größte Handlungsdruck.

Die aktuellen Kennzahlen zeigen eine deutliche Verschärfung der Lage:

- Rund 74 Prozent mehr Cyberangriffe auf Krankenhäuser[3]
- 30 Prozent aller Kliniken waren bereits von mindestens einem Sicherheitsvorfall betroffen.
- 309 gemeldete Cybervorfälle im Gesundheitsbereich, 54 Prozent davon waren Ransomware-Angriffe[4]

Diese Zahlen verdeutlichen, dass Cyberrisiken längst nicht mehr abstrakte, theoretische Ereignisse sind, sondern immer mehr zu einer realen und stark ansteigenden Bedrohung für den Krankenhausbetrieb werden.

Technologische Realität: der Klinikbetrieb am digitalen Limit

Die wachsende Zahl von Cyberangriffen trifft in den meisten Krankenhausinfrastrukturen auf ein technisches Fundament, das vielerorts bereits täglich am Limit arbeitet. Der Klinikbetrieb bewegt sich heute an der Grenze seiner digitalen Resilienz. Versorgung, Medizintechnik, OT-Infrastrukturen und KI-gestützte Verfahren sind mittlerweile hochgradig vernetzt, wodurch funktionale Abhängigkeiten, mögliche Sicherheitsrisiken und systemtechnische Komplexität steigen. Da moderne Klinikprozesse nur noch mit stabilen digitalen Systemen funktionieren, führen Systemausfälle unmittelbar zu einer massiven Gefährdung für die Patientenversorgung.

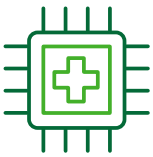
Kliniken müssen daher nicht nur ihre technische Resilienz stärken, sondern auch Governance, Prozesse und Meldefähigkeiten ausbauen, um neben den bereits seit Längerem bestehenden datenschutzrechtlichen Anforderungen auch den Vorgaben aus NIS2, KRITIS und B3S gerecht zu werden.

Abb. 1 – Zentrale Treiber für Cyber Security im Gesundheitswesen

IT, OT und Medizintechnik als Rückgrat der Versorgung
Die Versorgung hängt zunehmend von stabilen IT-, OT- und Medizintechnik-Systemen ab. Vernetzte Geräte, digitale Patientenpfade und KI machen Cyber Security zu einer zentralen Voraussetzung für Betriebsfähigkeit und Versorgungssicherheit.

Medical Device Regulation
Zertifizierte Medizingeräte lassen Updates oft nur eingeschränkt zu. Sicherheitsmaßnahmen müssen daher mit langen Update-Zyklen und regulatorischen Grenzen umgehen.

Datenaustausch
Universitätskliniken vereinen Forschung und Versorgung: Offene Datenräume treffen auf abgeschottete Kliniknetze. Datenschutz, Ethikvorgaben und Innovationsdruck führen schnell zu Schatten-IT (z.B. unkontrollierte Cloud-Nutzung).



KI im Klinikalltag
Der Einsatz von KI steigt schnell. Kliniken benötigen klare KI-Policies zu Use Cases, Governance, Haftung, Beschaffung und Risikoprüfung – sonst entstehen sofort NIS2-, Haftungs- und Reputationsrisiken.

[3] Hasso-Plattner-Institut (HPI): Dörr, C. (2025): Cyberangriffe auf Krankenhäuser nehmen rasant zu – Ergebnisse aus Studien und Interviews zur IT-Sicherheitslage im deutschen Gesundheitswesen. In: G+G Wissenschaft | AOK-Bundesverband, Interview vom 01.09.2025.

[4] European Commission (2026): Cybersecurity in Healthcare – Key figures and EU Action Plan. Directorate-General for Communications Networks, Content and Technology (DG CONNECT). Veröffentlicht am 12.03.2026. Quelle: https://commission.europa.eu/topics/digital-economy-and-society/cybersecurity-healthcare_en, abgerufen am 15. April 2026

Regulatorischer Wandel: neue Verantwortung für Krankenhäuser

Zu der komplexen technischen Ausgangslage kommt eine Regulatorik, die Krankenhäuser und deren Verantwortliche stärker denn je in die Pflicht nimmt, da staatliche Behörden weltweit die zunehmende Bedeutung von Cybersicherheit im Gesundheitssektor erkannt und auch in Europa mit einer Reihe gezielter regulatorischer Maßnahmen reagiert haben.

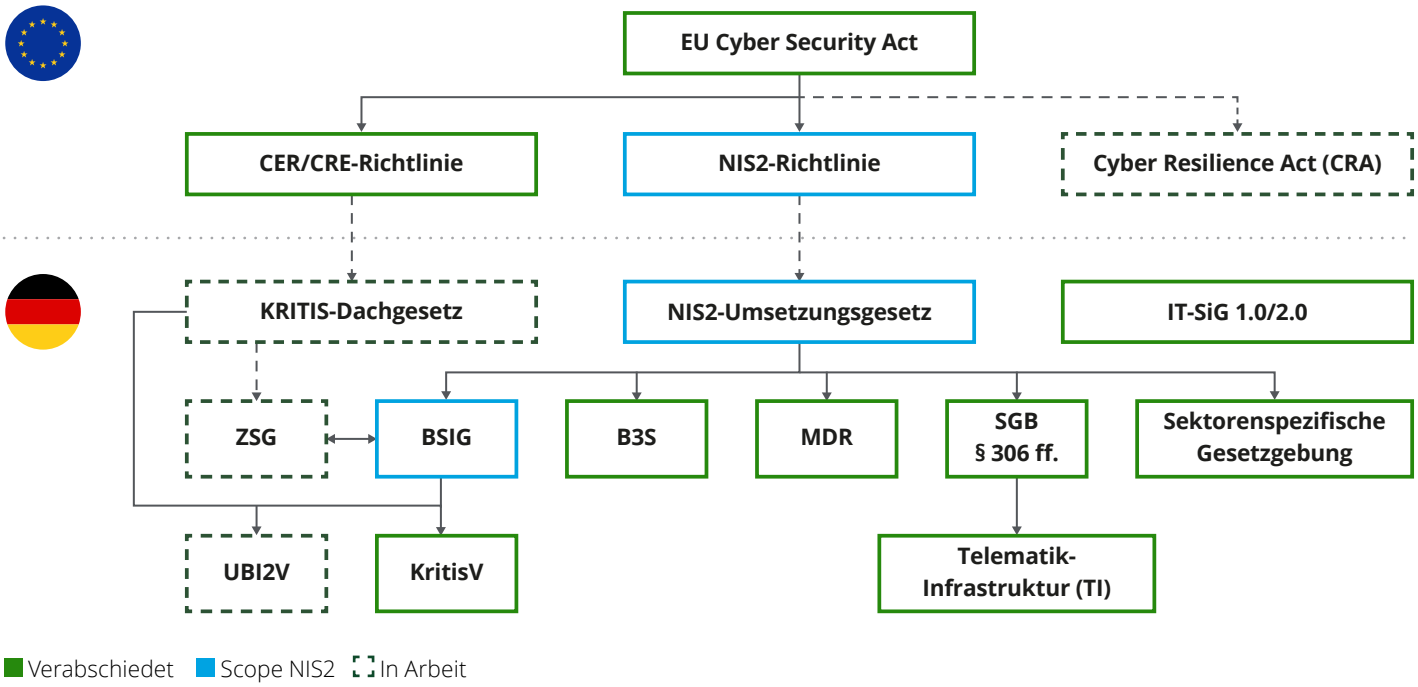
EU-Ebene

- **EU Cyber Security Act (CSA):** Zertifizierungsrahmen für IKT-Produkte seit 2019
- **EU Cyber Resilience Act (CRA):** gesetzlicher Rahmen zur Herstellung von organisatorischen und IT-basierten Vorkehrungen gegen Cyberangriffe (u.a. in Verbindung mit der Medical Device Regulation (MDR)
- **NIS2-Richtlinie:** Deren Umsetzung erfordert Neuerungen wie ein verpflichtendes Risikomanagement, technische Schutzmaßnahmen sowie umfassende Meldepflichten bei Sicherheitsvorfällen.
- **Critical Entities Resilience Directive, EU 2022/2557 (CER-Richtlinie):** physische Sicherheit kritischer Infrastrukturen
- **AI Act:** Rahmenwerk zur Einstufung von Risiken durch AI-Modelle und deren Anwendung
- **Data Governance Act (DGA):** Sicherheitsstandards für die Weiterverarbeitung von Gesundheitsdaten und Förderung der Interoperabilität
- **Datenschutzgrundverordnung (DSGVO):** Europaweit geltender rechtlicher Rahmen für die Anforderungen an Datenschutz und Datensicherheit, welcher durch nationale und sektorspezifische Vorgaben konkretisiert wird

Deutschland-Fokus

- **NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG):** nationale Implementierung der EU-Vorgabe
- **KRITIS-Dachgesetz (kritische Infrastrukturen):** Umsetzung der CER/CRE-Richtlinie
- **Der Branchenspezifische Sicherheitsstandard (B3S):** von der Deutschen Krankenhausgesellschaft (DKG) erarbeiteter Leitfaden zur IT-Sicherheit

Abb. 2 – Cybersicherheitsregulatorik



Für Krankenhäuser ergibt sich daraus ein komplexes Spannungsfeld:

- Sie müssen gleichzeitig technologische Modernisierung vorantreiben,
- hohe Datenschutz- und Sicherheitsstandards erfüllen
- und den wachsenden regulatorischen Anforderungen gerecht werden.

Die zentrale Herausforderung besteht darin, diese drei Schwerpunkte – Verfügbarkeit, Sicherheit und Compliance – in Einklang zu bringen, ohne den operativen Betrieb und die Systemstabilität zu gefährden. Die Umsetzung der NIS2- und KRITIS-Vorgaben erfordert substanzielle Investitionen in Technologie, Qualifizierung und strukturierte Prozessanpassungen. Diese initialen Aufwände sind unvermeidbar, um die regulatorischen Anforderungen wirksam zu erfüllen und eine nachhaltige Sicherheits- und Resilienzbasis für die Zukunft zu schaffen.

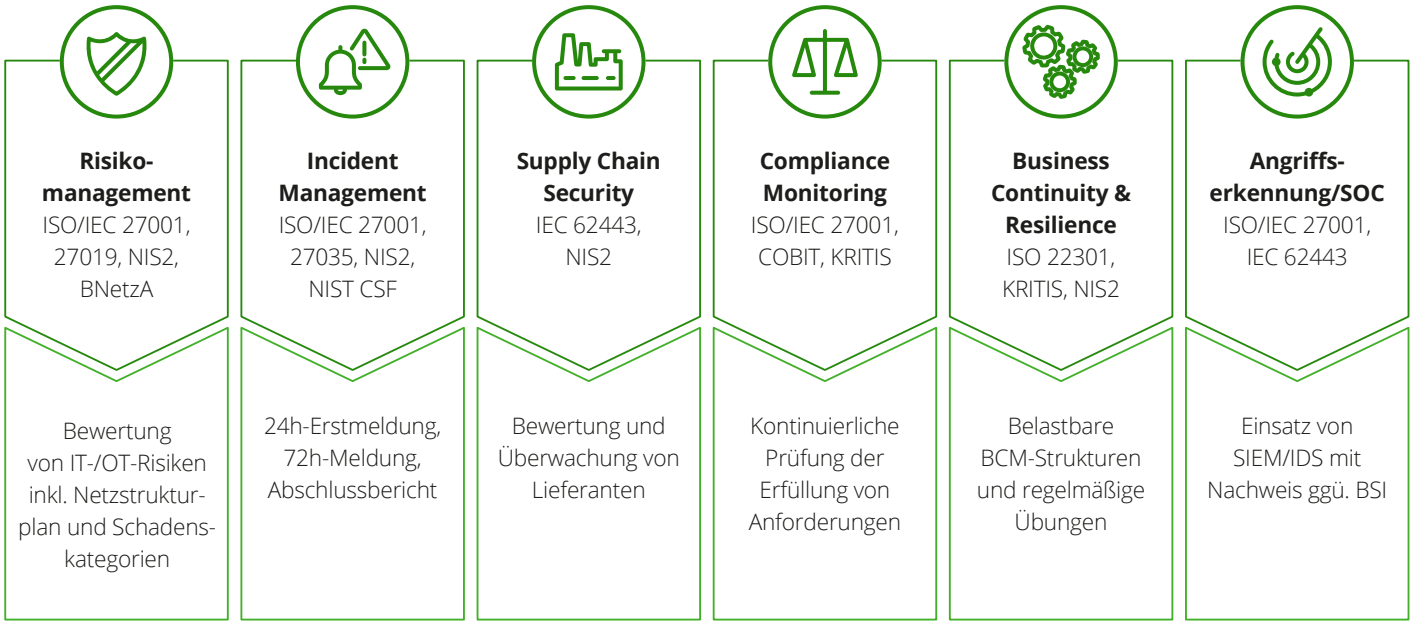
Die eigentliche Herausforderung liegt nicht in der Vielzahl regulatorischer Einzelanforderungen, sondern in ihrer integrierten Umsetzung unter realen Betriebsbedingungen. Priorisierung, Struktur und Finanzierbarkeit werden damit zu entscheidenden Erfolgsfaktoren.

Strategischer Lösungsraum NIS2

Die Erfüllung der oben genannten Vorgaben ist ohne strukturelle und stabile Finanzierung kaum realisierbar, klassische IT-Budgets reichen jedoch in der Regel für die operative Umsetzung der NIS2-Pflichten nicht aus. Abhilfe schafft hier zukünftig der Krankenhaustransformationsfond, mit dem erstmals ein strukturierter Finanzierungsrahmen geschaffen wurde, um sicherheitsrelevante Maßnahmen nachhaltig umzusetzen: Zwischen 2026 und 2035 stehen bis zu 50 Milliarden Euro für die Transformation der Krankenhauslandschaft zur Verfügung.

Über einen ganzheitlich entwickelten, integrierten und umsetzbaren Konzeptansatz ermöglicht Deloitte seinen Kunden, durch Zusammenführung von NIS2-Pflichten mit technischen Sicherheitsmaßnahmen, ausgerichtet auf die Beantragungslogik der KHTF-Antragsprozesse, diese Lücke zu schließen. Sicherheitslösungen werden in mehrjährigen Transformationsvorhaben verankert, förderlogisch strukturiert und über die Länder beantragt. Dadurch werden regulatorisch notwendige Maßnahmen erstmals strategisch finanzierbar.

Abb. 3 – Unmittelbare Handlungsfelder bezüglich Cyber Security



Unser umfassender Ansatz kombiniert regulatorische Anforderungen, technische und organisatorische Maßnahmen und finanzielle Förderlogik in einem konsistenten Transformationsmodell. Er deckt alle Schritte ab: Einstufung, Registrierung, Gap-Analyse, Maßnahmenplanung, KHTF-Roadmap, Umsetzung und Betrieb.

Der Effekt:

- NIS2 sowie KRITIS werden operativ umsetzbar.
- Technische Resilienz wird planbar und investierbar.
- Cyber Security wird ein fester Bestandteil der Krankenhaustransformation.

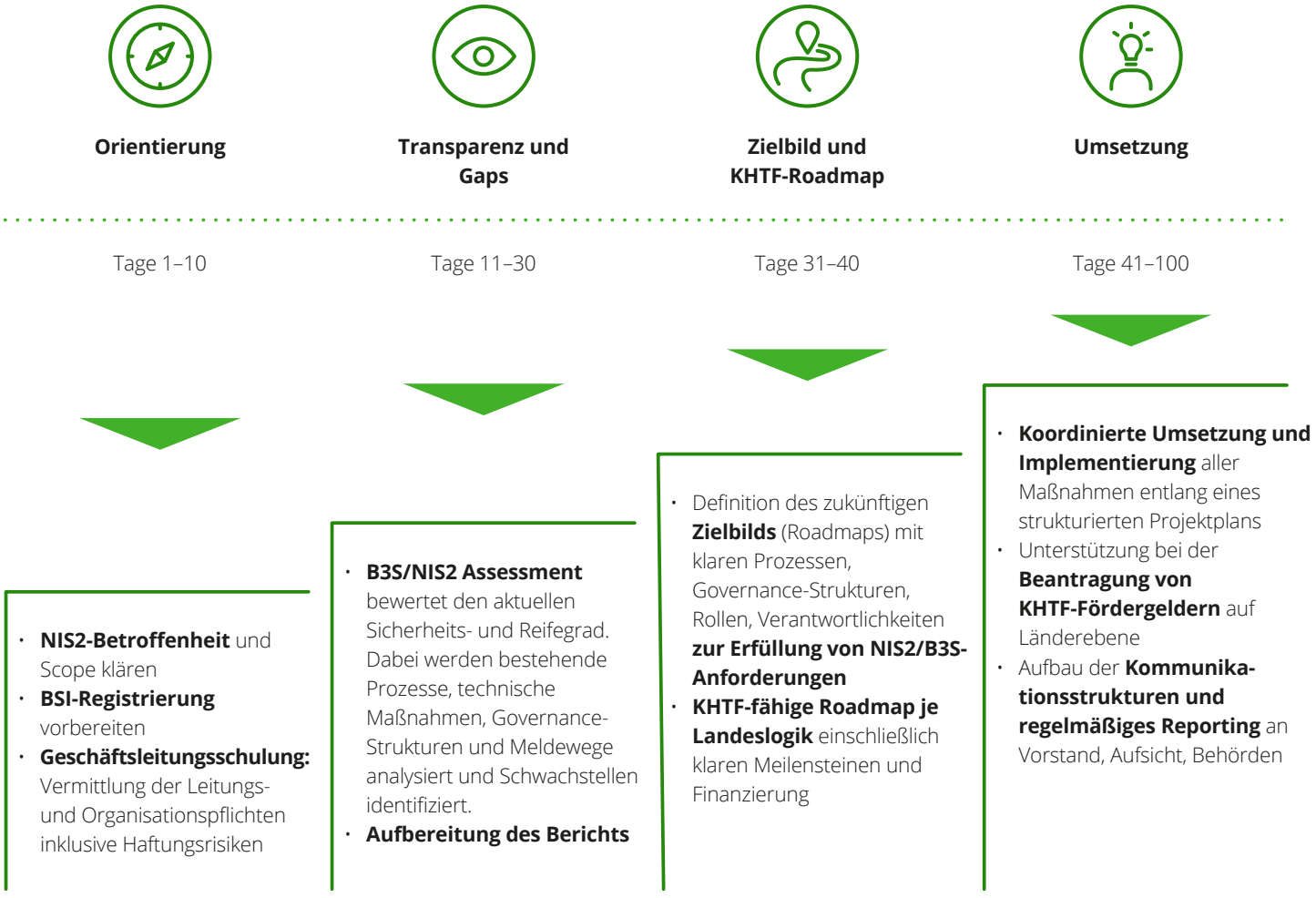
So können Krankenhäuser regulatorische Anforderungen erfüllen, ihre technische Resilienz erhöhen und notwendige Investitionen durch Fördermittel nachhaltig absichern.

Deloittes 100-Tage-Plan

Wie dieser Ansatz operativ konkret umgesetzt wird, zeigt Deloitte in einem klar strukturierten 100-Tage-Plan:

- Zunächst werden die NIS2-Einstufung und die BSI-Registrierung vorgenommen.
- Anschließend werden der laufende Betrieb anhand des B3S bewertet und die NIS2-Gaps transparent gemacht.
- Auf dieser Basis, in Abstimmung mit dem Kunden, entsteht eine KHTF-fähige Roadmap, die technische, organisatorische und betriebliche Maßnahmen priorisiert und finanzierbar macht.
- Parallel dazu beginnen die Umsetzung erster Maßnahmen sowie der Aufbau belastbarer Kommunikations- und Reporting-Strukturen.

Abb. 4 – Deloittes 100-Tage-Plan: die End-to-End Journey für Ihre Organisation



Erfolgsfaktoren

- Frühzeitige Planung: rechtzeitige Vorbereitung auf regulatorische Deadlines
- Integrierte Ansätze: koordinierte Umsetzung verschiedener Compliance-Anforderungen
- Risikoorientierung: systematischer Fokus auf kritische Assets sowie deren Bedrohungen und Schwachstellen in einem integrierten System, das IT-, OT- und regulatorische Managementbereiche verbindet
- KHTF-Förderfähigkeit und Antragstellung: Frühzeitige Identifikation förderfähiger Maßnahmen, strukturierte Erstellung der förderlogischen Narrative sowie Unterstützung bei der Beantragung der KHTF-Mittel auf Länderebene

Effizienzfaktoren

Die Komplexität der regulatorischen Landschaft und die kritische Bedeutung der Krankenhausinfrastruktur erfordern spezialisierte Erfahrungen.

- Regulatorische Expertise: fundiertes Verständnis relevanter gesetzlicher, normativer und branchenspezifischer Anforderungen
- Technische Kompetenz: praktische Erfahrung in der Umsetzung von Sicherheitsmaßnahmen in IT- und OT-Umgebungen
- Branchen-Know-how: spezifisches Verständnis der Herausforderungen im Gesundheitssektor

Warum Deloitte Cyber?
Deloitte Cyber ist der strategische Partner für die sichere Transformation von Krankenhäusern mit tiefem Verständnis für klinische Abläufe, regulatorische Vorgaben und technische Resilienz. Unser integrierter Ansatz reduziert Risiken, erfüllt gesetzliche Anforderungen und ermöglicht die nachhaltige Finanzierung über den KHTF.

Ansprechpartner

Ralph Noll
Partner | Cyber Risk
Tel: +49 211 87722 285
rnoll@deloitte.de

Ibo Teuber
Sector Lead Health Care
Tel: +49 89 29036 7839
iteuber@deloitte.de

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845

Stand 04/2026