Deloitte.

Together makes progress

NIS-2 Schulungspflicht für Geschäftsleitungen

Verantwortung, Umsetzung und Compliance im Lichte des BSIG-E

Das Gesetz zur Umsetzung der NIS-2 Richtlinie wurde am 13. November 2025 vom Deutschen Bundestag verabschiedet.

Die NIS-2 Richtlinie ist ein EU-weites Regelwerk zur Stärkung der Cybersicherheit in Unternehmen. Sie verpflichtet wichtige und besonders wichtige Einrichtungen, Cybersicherheit strategisch zu verankern. Eine der wichtigsten Anforderungen ist die Schulung der Geschäftsleitung: Diese ist kein „Nice-to-have", sondern eine gesetzliche Pflicht (§ 38 BSIG-E), die persönliche Haftungsrisiken minimiert und die Resilienz der Organisation nachhaltig stärkt.

Hintergrund und Zielsetzung

Das BSI unterstützt mit der **NIS-2 Geschäftsleitungsschulung** die Erfüllung der Pflicht zur Planung, Umsetzung und Überwachung von Cybersicherheitsmaßnahmen.

Die Schulung macht Informationssicherheit zur „Chefsache" und ist nicht delegierbar. Die Geschäftsleitung trägt die Verantwortung für die Umsetzung und Überwachung von Risikomanagementmaßnahmen (§ 30 BSIG-E).

Kernelemente der Schulungspflicht

Laut BSI sollte die Schulung drei Kernpunkte umfassen:

- **Risikoerkennung und -bewertung**: Geschäftsleitung muss relevante Bedrohungen, Eintrittswahrscheinlichkeiten, Schadensausmaße und Einflussfaktoren verstehen.
- **Risikomanagementmaßnahmen**: Die Geschäftsleitung muss die gesetzlichen Mindestanforderungen gemäß § 30 BSIG-E kennen und zusätzlich geeignete ergänzende Maßnahmen verstehen, die zur Stärkung der Cybersicherheit der Organisation beitragen.
- **Szenarien, Übungen, Fallstudien**: Die Geschäftsleitung muss bewerten können, wie Risiken und deren Gegenmaßnahmen die Verfügbarkeit, Integrität und Vertraulichkeit von Diensten sowie die wirtschaftlichen und regulatorischen Rahmenbedingungen beeinflussen. Praxisnahe Szenarien und Übungen helfen dabei, die theoretischen Inhalte in konkrete Entscheidungen umzusetzen.

Zentrale Lernziele:

NIS-2 und nationale Umsetzung

Zu Beginn der Schulung erhalten die Teilnehmenden einen Überblick über die NIS-2-Richtlinie und deren nationale Umsetzung. Dabei werden insbesondere die **gesetzlichen Pflichten** für wichtige und besonders wichtige Einrichtungen erläutert.

Ein zentrales Element ist das Verständnis der **persönlichen Verantwortung der Geschäftsleitung** gemäß § 38 BSIG-E, einschließlich der Verpflichtung zur Umsetzung und Überwachung von Risikomanagementmaßnahmen.

Risikomanagementmaßnahmen

Die Schulung vermittelt der Geschäftsleitung ein grundlegendes Verständnis für Cybersicherheitsrisiken. Die Geschäftsleitung soll **Risiken erkennen** sowie **Maßnahmen zur Risikobehandlung verstehen** und deren **Auswirkungen auf die Organisation einschätzen** können.

Szenarien, Übungen, Fallstudien

Ergänzend zu diesen Kerninhalten werden **sektor- und einrichtungsspezifische Anforderungen** berücksichtigt. Dies umfasst **branchenspezifische Bedrohungsszenarien**, regulatorische Rahmenbedingungen und zentrale Geschäftsprozesse.

Durch die Einbindung von Szenarien, Übungen und Fallstudien wird die **Schulung praxisnah gestaltet** und die Anwendung des erworbenen Wissens in konkreten Entscheidungssituationen gefördert.

Empfohlene Schulungsintervalle

Empfohlene Dauer: ca. 4 Stunden (halbtägig)
Intervall: mindestens alle 3 Jahre
Abweichungen: erforderlich bei Wechsel in der Geschäftsleitung, signifikanten Änderungen in Geschäftsprozessen oder erhöhter Risikoexposition.

Deloitte-Ansatz für NIS-2 Geschäftsführungsschulung

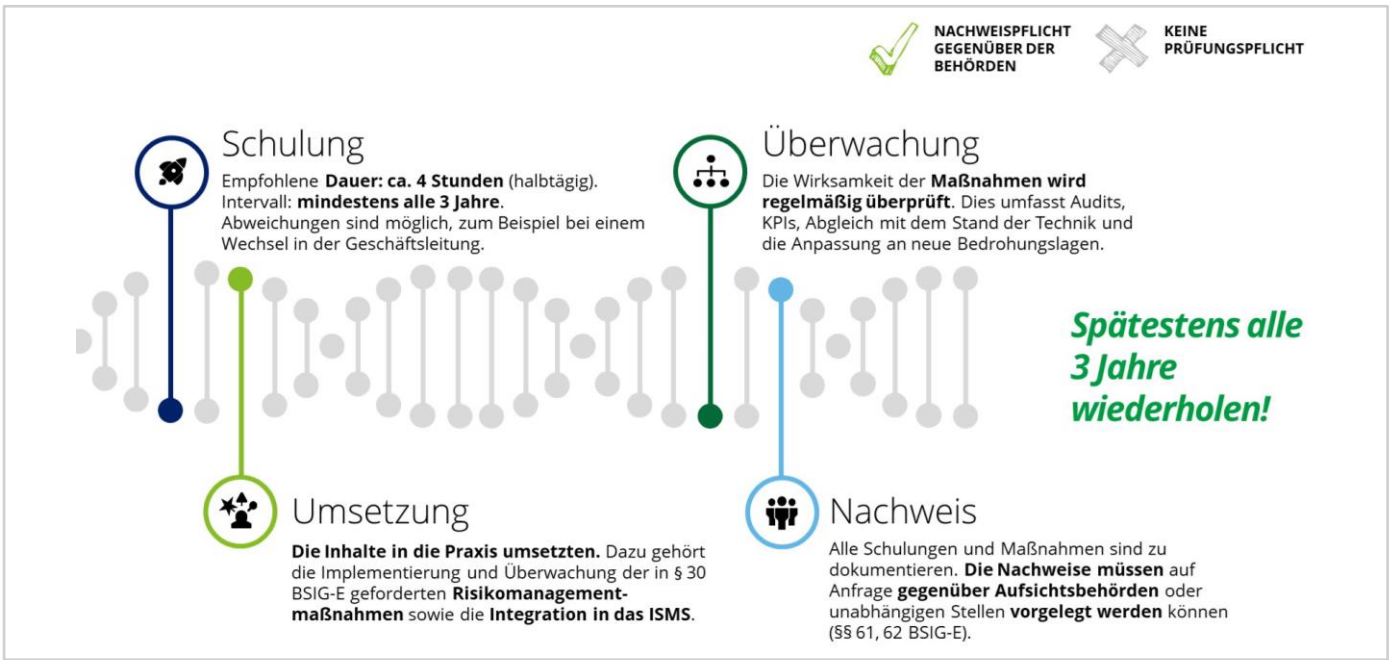
Auf Basis der Regulatorik und den vom BSI bereitgestellten Materialien hat Deloitte ein vierstufiges Schulungskonzept entwickelt, das über die reine Pflicht hinausgeht und echten Mehrwert schafft. Dieser Ansatz folgt einem kontinuierlichen Verbesserungsprozess und umfasst **vier Schritte**: Schulung, Umsetzung, Überwachung und Nachweis:

- In der ersten Phase werden **Kenntnisse vermittelt**, die für die strategische Steuerung der Cybersicherheit erforderlich sind.
- Darauf folgt die **Umsetzung der erlernten Inhalte** in konkrete Maßnahmen, wie die Integration in das Informationssicherheits-managementsystem (ISMS) und die Anpassung von Prozessen.
- **Die Überwachung** stellt sicher, dass die Maßnahmen wirksam sind und dem Stand der Technik entsprechen.
- **Der Nachweis** erfolgt durch eine revisionssichere Dokumentation, die gegenüber Aufsichtsbehörden vorgelegt werden kann.

Der Schulungsprozess wird spätestens alle drei Jahre oder bei besonderen Ereignissen wie z.B. einem Führungswechsel wiederholt. Diese Herangehensweise stellt sicher, dass die Organisation kontinuierlich lernt und sich an neue Bedrohungslagen anpasst.

Deloitte unterstützt Unternehmen dabei, die gesetzlichen Anforderungen nicht nur zu erfüllen, sondern Cybersicherheit als strategischen Erfolgsfaktor zu etablieren.

Wir entwickeln praxisorientierte und maßgeschneiderte Schulungsmaterialien, die individuell auf Ihre Branche und organisatorischen Anforderungen zugeschnitten sind. **Durch regelmäßige Trainings und Überprüfungen bleibt Ihre Cybersicherheitsstrategie dynamisch und kann flexibel auf neue Bedrohungen reagieren**.



Fazit

Die Schulungspflicht nach NIS-2 ist weit mehr als eine regulatorische Vorgabe. Sie ist ein strategisches Instrument, um die Handlungsfähigkeit der Geschäftsleitung im Bereich Cybersicherheit zu stärken. Indem Führungskräfte befähigt werden, Risiken zu erkennen, Maßnahmen zu bewerten und deren Auswirkungen zu verstehen, wird die Grundlage für eine resiliente Organisation geschaffen.

Unternehmen, die diese Pflicht ernst nehmen, reduzieren nicht nur Haftungsrisiken, sondern gewinnen auch Vertrauen bei Kunden, Partnern und Aufsichtsbehörden. Die Investition in Schulungen zahlt sich langfristig aus - durch höhere Sicherheit, geringere Ausfallzeiten und eine bessere Positionierung im Markt.

Wer jetzt handelt, stellt sicher, dass Cybersicherheit nicht als Belastung, sondern als Wettbewerbsvorteil verstanden wird.

Ergänzende Ressourcen:

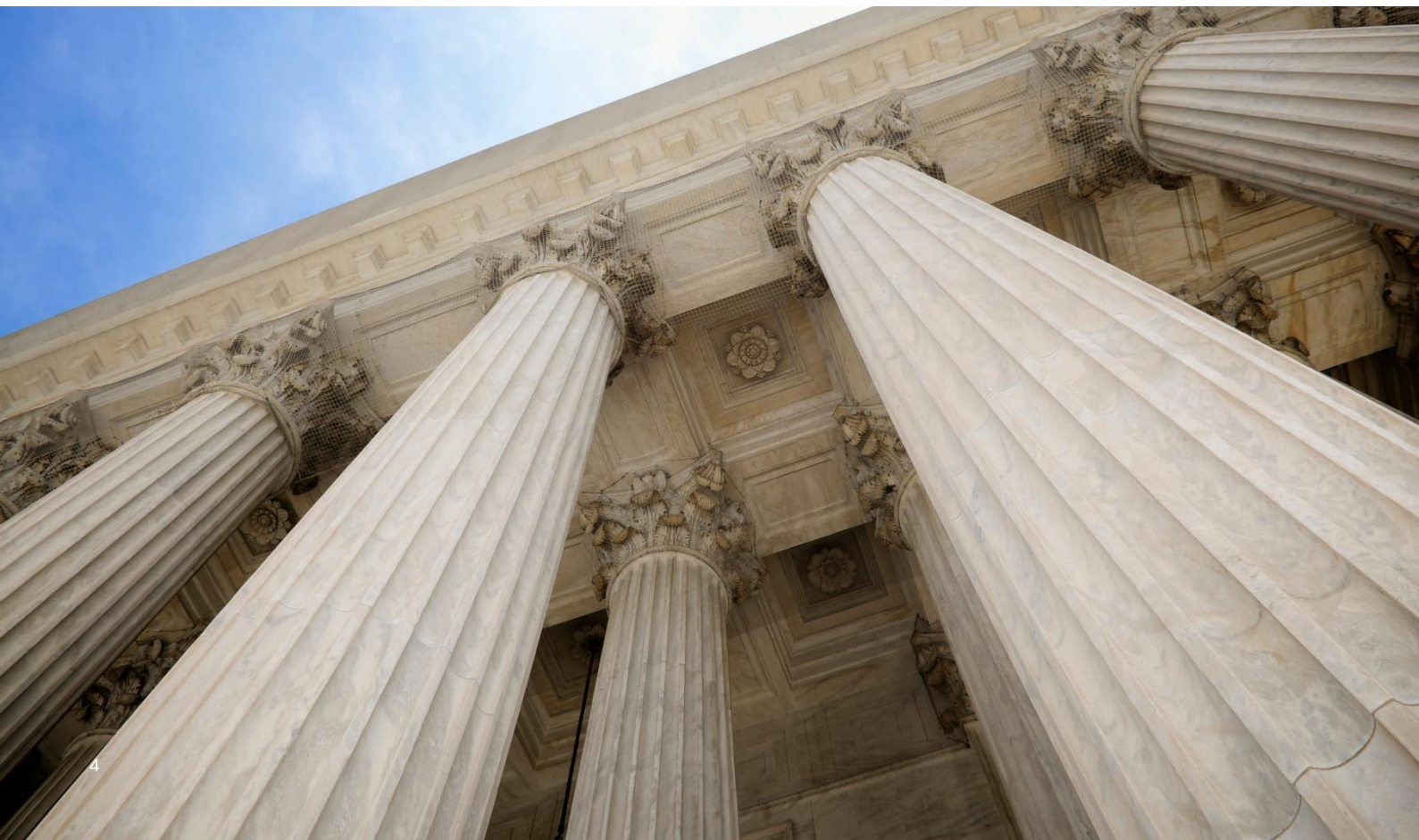
Für vertiefende Einblicke in die Umsetzung der NIS-2 Richtlinie und Best Practices empfehlen wir folgende Deloitte-Publikationen:

- Umsetzung der EU-Direktive NIS-2 in Deutschland (NIS2UmsuCG)
- Navigating NIS-2 Compliance

Über Deloitte Cyber

Deloitte Cyber ist führender Anbieter von Cybersecurityberatung. Unsere Spezialisten unterstützen Unternehmen dabei, ihre digitale Transformation sicher zu gestalten. Unser Fokus auf kritische Infrastrukturen und unsere langjährige Erfahrung in Informationssicherheits-regulatorik machen uns zum vertrauenswürdigen Partner für NIS-2.

Interessiert an einer maßgeschneiderten Schulung für Ihre Geschäftsleitung? Kontaktieren Sie uns - wir entwickeln ein Konzept, das perfekt zu Ihrem Unternehmen passt.



Kontakte

Fabian Mihailowitsch
Partner
Cyber Technology & Transformation
Tel: +49 89 29036 6998
fmihailowitsch@deloitte.de

Tamara Okropiridze
Senior Manager
Cyber Technology & Transformation
Tel: +49 69 75695 7215
tokropiridze@deloitte.de

Oliver Ständert
Director
IoT Strategy & Architecture IT/OT Advisory
Tel: +49 151 58071396
ostaendert@deloitte.de

Deloitte.

Stand 12/2025