

Das NIS2 4 CEO Programm entsteht in Zusammenarbeit mit:



mybreev



100 % Online & On-Demand abrufbar

2,5 statt 4 Stunden

Smartes NIS2-Schulungsprogramm für Ihr Managementteam

Ziel dieses Qualifizierungs- bzw. Befähigungsprogramms ist der systematische Erwerb, die vertiefte Auseinandersetzung sowie die formalisierte Nachweisführung von Kompetenzen im Bereich der Cybersicherheit, wie sie in unmittelbarem Bezug zu den Anforderungen des **§ 38 Abs. 1 und Abs. 3 des Gesetzes zur Umsetzung der NIS2-Richtlinie (NIS2UmsuCG)** stehen.

Im Fokus steht die Befähigung von Führungspersonen und Aufsichtsorganen, ihre gesetzlich normierten Verantwortlichkeiten im Kontext der Informationssicherheit und Cybersicherheit nicht lediglich deklaratorisch, sondern inhaltlich fundiert, risikoorientiert und wirksam wahrnehmen zu können. Dies schließt sowohl das Verständnis der regulatorischen Rahmenbedingungen als auch die Anwendung praxisrelevanter Instrumente zur Bewertung, Steuerung und Kontrolle cyberbezogener Gefährdungslagen mit ein.

Im Sinne der **organisationalen Resilienz** und der normativen Erwartung an ein angemessenes Risikomanagement umfasst das angestrebte Kompetenzprofil insbesondere:

- die strukturierte Erfassung und Interpretation relevanter gesetzlicher und technischer Anforderungen,
- die Fähigkeit zur Analyse komplexer Bedrohungsszenarien und zur Ableitung geeigneter, verhältnismäßiger Schutzmaßnahmen,
- sowie die rechtssichere Dokumentation und Nachweisführung der ergriffenen Maßnahmen gegenüber internen und externen Prüf- und Aufsichtsinstanzen.

Durch die erfolgreiche Umsetzung dieser Zielsetzung wird ein bedeutsamer Beitrag zur rechtskonformen und verantwortungsbewussten **Steuerung von Informationssicherheit auf Leitungsebene** geleistet – im Einklang mit den Maßgaben des Standes der Technik sowie den spezifischen Anforderungen des sektorübergreifenden regulatorischen Umfelds.

Die inhaltliche Tiefe entspricht einem **klassischen Schulungsumfang** von ca. vier Stunden, wie er auch in einschlägigen Orientierungshilfen, unter anderem der **BSI-Handreichung** zur Sensibilisierung von Führungskräften im Kontext NIS2, als angemessen beschrieben wird.

Durch den Einsatz innovativer, didaktisch verdichteter Lernmethoden (u. a. Micro-Learning, praxisnahe Szenarien und fokussierte Wissensanker) wird dieser Content in einer effektiven Lernzeit von rund **2,5 Stunden vermittelt** – ohne Abstriche bei Vollständigkeit, Nachvollziehbarkeit oder Compliance-Relevanz.

Zielgruppe

Primäre Zielgruppe des Programms sind Mitglieder der Geschäftsleitung, insbesondere:

- Geschäftsführende Vorstände,
- Vorstände und Aufsichtsräte (bei AGs),
- Geschäftsführer*innen (bei GmbHs),
- Verwaltungsräte (bei Genossenschaften),
- Sowie sonstige Organ- oder Leitungsmitglieder mit strategischer Gesamtverantwortung.

Programmüberblick

Modul 1: Einführung in die NIS2 (für alle Mitarbeitenden)

Modul 2: Grundlagen der Cybersicherheit für Führungskräfte

Modul 3: Risikomanagement in der Welt der Sicherheitstechnik

Modul 4: Grundverständnis von Cyberbedrohungen, -
Kriminalität und deren Dynamik

Modul 5: Branchenspezifische Szenario-Trainings

Dazu gehören Szenarien aus: Gesundheitswesen, Energie,
Wasserwirtschaft, Rechenzentrum-Betrieb, Finanzwesen, Produzierende
Gewerbe, Chemie, Lebensmittelindustrie, Raumfahrt

inklusive Kompetenzerwerbzertifikat

*Details siehe weiter unten „Unser Curricular“

Modul-Release und Schulungsablauf

Q1 2026	Q2 2026	Q3 2026	Q4 2026	Q&A Webinar
Modul 1 + 2	Modul 3	Modul 4	Modul 5	
Q&A Webinar	Q&A Webinar	Q&A Webinar		

Das NIS2 4 CEO Programm entsteht in Zusammenarbeit mit:



mybreev

NIS4
CEO

Branchenspezifische Szenario-Trainings

Unser Schulungsprogramm beinhaltet **branchenspezifische Trainingsmodule**, die gezielt auf die Anforderungen und Risiken einzelner Sektoren abgestimmt sind.

Diese Module greifen reale Szenarien und Bedrohungslagen aus Bereichen wie dem Gesundheitswesen, der Energieversorgung, der Kommunalverwaltung, dem Finanzsektor oder der kritischen Produktion auf.

Ziel dieser Trainings ist es, das **erlernte Wissen praktisch anzuwenden**.

Mithilfe von szenariobasierten Übungen und Fallbeispielen werden unterschiedliche Gefährdungen und Schwachstellen adressiert, die von den Teilnehmenden analysiert, bewertet, behandelt und nachverfolgt werden. Dadurch wird praxisnah trainiert, wie **Risikobewertung, Risikobehandlung** und **Risikokommunikation** in realen Entscheidungssituationen effektiv umgesetzt werden können.

Entwickelt von:



Dr. - Ing. Erfan Koza

*Universitärer Forscher
und Kursautor*

Erfahrung aus 50+
Sicherheitsprojekten für
Industrie & Bundesbehörden



Peter Vahrenhorst

Kriminalhauptkommissar a. D.

25 Jahre Erfahrung im Bereich
Cyber-Kriminalität & und
Cyber Crime Prevention



mybreev GmbH

*Digitaler Content Publisher
und Schulungsanbieter*

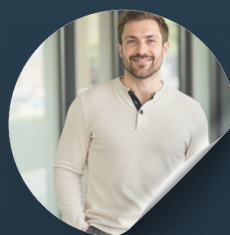
Über 500 Schulungsprojekte und
über 4 Millionen geschulte
Mitarbeitende weltweit.



Asiye Öztürk

*Lead-Auditorin und
BSI-Kritisprüferin*

Über 10 jährige Erfahrung im
Bereich Implementierung und
auditing von ISMS, B3S für
kritische Infrastrukturen



Marvin Michael Gatermann

*CEO bei DAFI Deutsche Akademie für
Informationssicherheit*

Mehrjährige Erfahrung in
CISO-Trainings & Leadership-
Weiterbildung

Unser Curricular

Grundsatz zur Entwicklung: Kenntnisse und Fähigkeiten gemäß § 38 Abs. 1 NIS2 UmsuCG

Aus dem Gesetzestext ergeben sich zwei zentrale Bereiche, in denen die Unternehmensleitung über Kenntnisse und Fähigkeiten verfügen muss:

1. Risikokompetenz in Bezug auf Cybersicherheit

Gesetzestext: „... um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen...“

Daraus lassen sich folgende Kenntnisse und Fähigkeiten ableiten:

- Grundverständnis von Cyberbedrohungen und deren Dynamik
- Fähigkeit zur Bewertung von Cybersicherheitsrisiken
- Verständnis von Auswirkungen von Cybervorfällen auf Geschäftsprozesse und kritische Dienste
- Kompetenz zur Einordnung von Bedrohungslagen in den organisatorischen Kontext
- Kenntnis relevanter Angriffsvektoren (z.B. Ransomware, Social Engineering, Supply Chain Attacks)
- Verständnis von Schwachstellenmanagement, Angriffsflächenreduktion und Sicherheitsniveaus
- Vertrautheit mit Risikobewertungsmodellen und -metriken (z.B. qualitative oder quantitative Risikobewertung).

2. Steuerungs- und Entscheidungskompetenz für Cybersicherheitsmaßnahmen

Zitat: „...sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.“

Daraus lassen sich folgende Kenntnisse und Fähigkeiten ableiten:

- Kenntnis gesetzlicher Anforderungen nach NIS2UmsuCG und relevanter Normen (z.B. ISO/IEC 27001, BSI IT-Grundschutz, IEC 62443)
- Verständnis der organisatorischen Pflichten: z.B. Meldung von Sicherheitsvorfällen, Risikoanalysen, Nachweispflichten
- Fähigkeit, geeignete Sicherheitsstrategien und -maßnahmen zu definieren und zu priorisieren
- Verantwortungsbewusstsein für Sicherheitsgovernance, inklusive Budgets, Ressourcen, Rollen
- Verständnis für Zusammenspiel zwischen Unternehmensleitung, IT- und Informationssicherheitsbeauftragten, Datenschutz, Compliance
- Fähigkeit zur Integration von Cybersicherheit in die Unternehmensstrategie und Entscheidungsprozesse
- Grundkenntnisse über Reaktion auf Sicherheitsvorfälle, Business Continuity, Incident Response und Krisenkommunikation

Das NIS2 4 CEO Programm entsteht in Zusammenarbeit mit:



mybreev

NIS4CEO

Regulatory Mapping

Basierend auf der vorläufigen **BSI-Handreichung** für die Empfehlung zur Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen nach dem **NIS-2-Umsetzungsgesetzentwurf**.

Kap.	Modalverb	Anforderung	Modul-Einbindung
2.1.1	SOLLEN	Geschäftsleitungen SOLLEN die übergreifenden Inhalte und Ziele der NIS-2-Richtlinie bzw. deren nationaler Umsetzung kennen.	M1 + M2
2.1.1	SOLLEN	Geschäftsleitungen SOLL der Geltungsbereich der NIS-2-Richtlinie bzw. deren nationaler Umsetzung vermittelt werden.	M1 + M2
2.1.1	KANN	Geschäftsleitungen KANN die Historie der Cybersicherheitsgesetzgebung vermittelt werden.	M1 + M2
2.1.1	KANN	Geschäftsleitungen KANN die Interaktion der NIS-2-Richtlinie mit weiteren nationalen oder europäischen Cybersicherheitsregulierungen vermittelt werden.	M1 + M2

Kap.	Modalverb	Anforderung	Modul-Einbindung
2.1.2	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über die Pflichten aus § 30 BSIG-E erhalten.	M1 + M2
2.1.2	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen und dokumentieren müssen.	M1 + M2
2.1.2	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass die Risikomanagementmaßnahmen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst geringhalten sollen	M3
2.1.2	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass das Risikomanagement alle informationstechnischen Systeme, Komponenten und Prozesse, die Unternehmen für die Erbringung ihrer Dienste nutzen, adressieren muss.	M3
2.1.2	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass die Maßnahmen den jeweils aktuellen Stand der Technik einhalten sollen, einschlägige europäische und internationale Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen müssen.	M3
2.1.2	SOLLEN	Geschäftsleitungen SOLL die Bewertung der Verhältnismäßigkeit von Maßnahmen vermittelt werden.	M3
2.1.2	SOLLEN	Geschäftsleitungen SOLLEN die Mindestanforderungen aus § 30 Abs. 2 BSIG-E vermittelt werden	M3

2.1.3	SOLLEN	Geschäftsleitungen SOLLEN die Meldepflicht für erhebliche Sicherheitsvorfälle kennen	M1 + M2
2.1.3	SOLLEN	Geschäftsleitungen SOLL das dreistufige Melderegime mit früher Erstmeldung, Meldung und Abschlussmeldungen und deren Fristen vermittelt werden.	M1 + M2
2.1.3	SOLLEN	Geschäftsleitungen SOLL die Möglichkeit von Zwischen- und Fortschrittmeldungen im Meldeprozess vermittelt werden.	M1 + M2
2.1.3	SOLLEN	Geschäftsleitungen SOLLEN die Meldeinhalte im Melderegime kennen	M1 + M2
2.1.3	SOLLEN	Geschäftsleitungen SOLLEN die Unterrichtungspflichten des BSI kennen.	M1 + M2
2.1.3	SOLLEN	Geschäftsleitungen SOLLEN über Rückmeldungen des BSI bei Meldungen informiert werden.	M1 + M2

Kap.	Modalverb	Anforderung	Modul-Einbindung
2.1.4	SOLLEN	Geschäftsleitungen SOLLEN die Registrierungspflicht und -frist für wichtige und besonders wichtige Einrichtungen kennen.	M1 + M2
2.1.4	KANN	Geschäftsleitungen KÖNNEN die verpflichtenden Angaben bei der Registrierung vermittelt werden.	M1 + M2
2.1.4	SOLLEN	Geschäftsleitungen SOLLEN die Möglichkeit für Registrierungen durch das BSI kennen.	M1 + M2
2.1.4	SOLLEN	Geschäftsleitungen SOLLEN über Änderung der Registrierungsangaben und deren Fristen informiert werden.	M1 + M2
2.1.4	SOLLEN	Geschäftsleitungen SOLLEN ggf. über besondere Registrierungspflichten für Betreiber kritischer Anlagen informiert werden.	M1 + M2
2.1.4	SOLLEN	Geschäftsleitungen SOLLEN ggf. über besondere Registrierungspflichten für Einrichtungen der Sektoren digitale Dienste und digitale Infrastrukturen informiert werden	M1 + M2

Das NIS2 4 CEO Programm entsteht in Zusammenarbeit mit:



Kap.	Modalverb	Anforderung	Modul-Einbindung
2.1.5	SOLLEN	Geschäftsleitungen SOLLEN ihre Pflicht zur Umsetzung und Überwachung von Risikomanagementmaßnahmen kennen.	M1 + M2
2.1.5	SOLLEN	Geschäftsleitungen SOLLEN die mögliche Haftung der Geschäftsleitungen für schuldhaft verursachte Schäden kennen.	M1 + M2
2.1.5	SOLLEN	Geschäftsleitungen SOLLEN die Schulungspflicht kennen.	M1 + M2
2.1.5	SOLLEN	Geschäftsleitungen SOLLEN mögliche Sanktionierungen bei Verstößen gegen Verpflichtungen für Einrichtungen oder Geschäftsleitungen kennen	M1 + M2

Kap.	Modalverb	Anforderung	Modul-Einbindung
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über Sinn, Ziele und zentrale Begriffe des Risikomanagements als systematischer Prozess zur Identifizierung, Bewertung und Steuerung von Risiken erhalten.	M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN verstehen, welche Rolle das Risikomanagement im Gesamtkontext der NIS-2-Richtlinie spielt.	M2 + M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN verstehen, dass Risikomanagement aus Risikoidentifikation, Risikoanalyse, Risikobehandlung und Risiküberwachung besteht.	M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass es für das Risikomanagement etablierte nationale und internationale Standards gibt, an denen man sich orientieren kann.	M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über Methoden und Ziele der Risikoanalyse erhalten.	M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN wissen, wie Risiken für die eigene Einrichtung identifiziert werden.	M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN wissen, was physische, digitale, menschliche, prozessuale und immaterielle Assets sind und wie diese in der eigenen Einrichtung identifiziert werden können.	M 3
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über mögliche technische und physische Gefährdungen erhalten.	M 3 + M4
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über mögliche technische und physische Schwachstellen erhalten.	M 3 + M4
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN mit den Grundbegriffen der Risikobewertung vertraut gemacht werden (z. B. Eintrittswahrscheinlichkeit, Schadensausmaß, Risikoakzeptanz).	M 3 + M4
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass auch nicht-technische Risiken (z. B. menschliches Fehlverhalten, Lieferkettenprobleme, organisatorische Schwächen) Teil der Risikobetrachtung sind.	M 3 + M4
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN die möglichen Schadensarten (finanziell, reputativ, betrieblich, rechtlich, technisch, personenbezogen etc.) kennen.	M 3 + M4
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN verstehen, dass die Risikobewertung nicht nur technische Aspekte betrifft, sondern auch wirtschaftliche, rechtliche und reputative Folgen berücksichtigen muss.	M 3 + M4
2.2.1	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass Risikomanagement ein kontinuierlicher Prozess ist, der regelmäßige Überprüfung und Anpassung erfordert.	M2 + M 3 + M4

Kap.	Modalverb	Anforderung	Modul-Einbindung
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN die in § 30 Abs. 2 BSIG-E genannten Mindestmaßnahmen kennen und deren Bedeutung für ihre Einrichtung nachvollziehen können.	M 2
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über Risikomanagementmaßnahmen bekommen, der sich auf ihre Rolle als Management-Ebene und nicht auf tiefe technische Aspekte fokussiert.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN einen Überblick über Strategien zur Risikobehandlung (z. B. Vermeidung, Minderung, Übertragung, Akzeptanz) erhalten.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN verstehen, dass die Risikobehandlungsstrategien Übertragung und Akzeptanz für wichtige und besonders wichtige Einrichtungen eher nicht akzeptabel sind.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN grundlegende Prinzipien und Ziele von Maßnahmen zur Risikominderung kennen.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN über alle weiteren Risikomanagementmaßnahmen informiert sein, die in der Einrichtung bereits implementiert wurden oder deren Einführung geplant ist.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN auch Alternativen zu bestehenden oder geplanten Maßnahmen kennen, um die Angemessenheit der getroffenen Entscheidungen besser einschätzen zu können.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN verstehen, dass technische und organisatorische Maßnahmen aufeinander abgestimmt und regelmäßig überprüft werden müssen.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass Maßnahmen den Stand der Technik einhalten und verhältnismäßig sein müssen.	M 3
2.2.2	SOLLEN	SOLLEN einschätzen können, wie sich technische und organisatorische Maßnahmen auf Geschäftsprozesse, Ressourcenbedarf und Resilienz der Einrichtung auswirken.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN mit typischen Zielkonflikten im Risikomanagement (z. B. Sicherheit vs. Wirtschaftlichkeit) vertraut gemacht werden, um fundierte Entscheidungen mittragen zu können.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN wissen, dass Maßnahmen dokumentiert, nachvollziehbar begründet und kontinuierlich weiterentwickelt werden müssen.	M 3

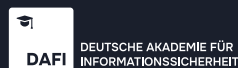
Das NIS2 4 CEO Programm entsteht in Zusammenarbeit mit:



Kap.	Modalverb	Anforderung	Modul-Einbindung
2.2.3	SOLLEN	Geschäftsleitungen SOLLEN die Fähigkeit entwickeln, Risiken und geeignete Maßnahmen gemeinsam zu	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN beurteilen können, welche Auswirkungen bestimmte Risiken auf die Verfügbarkeit, Integrität und Vertraulichkeit der erbrachten Dienste haben können.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN verstehen, wie sich Sicherheitsvorfälle konkret auf die Leistungserbringung, Kundenbeziehungen und gesetzliche Verpflichtungen der Einrichtung auswirken können.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN die potenziellen wirtschaftlichen, rechtlichen und reputativen Folgen unzureichender Risikobehandlung einschätzen können.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN erkennen, wie sich präventive und reaktive Maßnahmen zur Risikobehandlung auf Betriebsabläufe und Dienstkontinuität auswirken	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN verstehen, welche Abhängigkeiten zwischen IT-Systemen, Prozessen und Dienstleistungen bestehen und wie sich Störungen in einem Bereich auf andere auswirken können (Dominoeffekte).	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN in die Lage versetzt werden, Cybersicherheitsrisiken als Geschäftsrisiken einzuordnen und entsprechende Managemententscheidungen zu treffen oder zu unterstützen.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN bewerten können, wie sich Investitionen in Cybersicherheit auf die langfristige Stabilität und Resilienz der Einrichtung auswirken.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN bewerten können, wie sich Investitionen in Cybersicherheit auf die langfristige Stabilität und Resilienz der Einrichtung auswirken.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN verstehen, dass eine unzureichende Umsetzung von Risikomanagementmaßnahmen zu aufsichtsrechtlichen Maßnahmen oder Haftungsrisiken führen kann.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN die Auswirkungen unterschiedlicher Risikobehandlungsstrategien (z. B. Risikotransfer vs. Risikominderung) auf die Dienstqualität und -verfügbarkeit beurteilen können.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN in die Lage versetzt werden, Zielkonflikte zwischen Sicherheitsmaßnahmen und Dienstleistungserbringung zu erkennen und ausgewogen zu bewerten.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN verstehen, dass die Bewertung von Risiken und Maßnahmen in den Kontext der strategischen Gesamtverantwortung fällt und Grundlage für haftungs- und aufsichtsrelevante Entscheidungen ist.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN Risikomanagementmaßnahmen in das ganzheitliche Risikomanagement der Einrichtung einbinden.	M 3
2.2.2	SOLLEN	Geschäftsleitungen SOLLEN vermittelt werden, dass ausreichend Ressourcen (Budget, Personal) für die Umsetzung des Risikomanagements bereitgestellt werden müssen.	M 3

Kap.	Schwerpunkt	Anforderung	Modul-Einbindung
2.3.1	Sektor- und einrichtungsspezifische Inhalte	Ergänzend zu den allgemeinen Kerninhalten ist es sinnvoll, sektor- und einrichtungsspezifische Inhalte zu berücksichtigen. Nur wenn Geschäftsleitungen die Anforderungen, typischen Risiken und regulatorischen Rahmenbedingungen ihres jeweiligen Sektors kennen, können sie Risiken realistisch einschätzen und geeignete Maßnahmen mittragen. Dies umfasst insbesondere die besonderen Pflichten sowie relevante branchenspezifische Vorgaben, wie z. B. B3S, ISO-Normen oder sektorspezifische Sicherheitskataloge. Ebenso relevant sind die typischen Bedrohungsszenarien des jeweiligen Sektors sowie die zentralen IT-gestützten Geschäftsprozesse der eigenen Einrichtung. Die Vermittlung dieser Inhalte unterstützt eine wirksame, kontextbezogene Risikobewertung und fördert die Entscheidungsfähigkeit der Geschäftsleitung im spezifischen Organisationskontext.	M 5
2.3.2	Szenarien, Übungen und Fallstudien	Risikomanagement und die Rolle der Geschäftsleitungen können sehr abstrakt und wenig greifbar sein. Schulungen können die vermittelten Inhalte mit Hilfe von Beispielszenarien, interaktiven Übungen oder Fallstudien handhabbarer machen. Diese Formate ermöglichen es den Geschäftsleitungen, das erworbene Wissen auf konkrete Situationen zu übertragen und die eigene Entscheidungs- und Beurteilungskompetenz realitätsnah zu erproben. Besonders wirksam sind Beispiele, die typische Bedrohungslagen, Schwachstellen oder Entscheidungssituationen im eigenen Sektor oder der konkreten Einrichtung abbilden. Ziel ist es, die Wechselwirkungen zwischen Risiken, Maßnahmen und Auswirkungen nachvollziehbar zu machen und die Fähigkeit zu fördern, Risiken unternehmerisch einzuordnen und tragfähige Entscheidungen auf Basis begrenzter Informationen zu treffen.	M 5

Das NIS2 4 CEO Programm entsteht in Zusammenarbeit mit:



mybreev

NIS4CEO