

NIS-2-Schulung für Geschäftsleitung und Top-Management (Präsenz)

Kontext der NIS-2-Regulierung, Pflichten für die Geschäftsleitung, Risikoanalyse und Risikomanagementmaßnahmen nach § 38 BSIG

Die NIS-2-Richtlinie und das Umsetzungsgesetz zu NIS-2 führen für „wichtige“ und „besonders wichtige“ Einrichtungen verschärfte Pflichten zur Informationssicherheit ein. Wichtiges Element ist die in § 38 BSIG verankerte Schulungspflicht der Geschäftsleitung: Mitglieder der Geschäftsleitung müssen regelmäßig ausreichend Kenntnisse zur Erkennung und Bewertung von Risiken, zu Risikomanagementmaßnahmen sowie zu den Auswirkungen von Risiken und Maßnahmen auf die erbrachten Dienste erwerben. Dieses Seminar ist speziell auf die Perspektive von Geschäftsleitung und Top-Management zugeschnitten. Es vermittelt den Kontext der NIS-2-Regulierung (NIS-2-Richtlinie und deutsches NIS-2-Umsetzungsgesetz, insbesondere BSIG), die übergreifenden Pflichten für die Einrichtung an sich und im Speziellen für die Geschäftsleitung, zeigt Haftungsrisiken und Compliance-Pflichten auf und konzentriert sich zudem auf die vom Gesetz geforderte Risikoanalyse, die normierten Risikomanagementmaßnahmen und die potenziellen Auswirkungen von Risiken und Risikomanagementmaßnahmen auf das eigene Unternehmen. Die Inhalte orientieren sich an der Handreichung des BSI zur Schulungspflicht nach § 38 Abs. 3 BSIG und unterstützen Teilnehmende dabei, ihre Verantwortung im Bereich Informationssicherheit nachweisbar wahrzunehmen.

Inhalte

Rechtlicher Rahmen: NIS-2-Richtlinie und BSIG

- Überblick über NIS-2-Richtlinie und das novellierte BSIG.
- Einordnung der Begriffe in KRITIS, „wichtige“ und „besonders wichtige“ Einrichtungen.
- Rolle der Geschäftsleitung bei Umsetzung, Überwachung und Nachweis der Risikomanagementmaßnahmen.
- Überblick über Haftungsrisiken und Sanktionsrahmen.

Kernbereich 1: Risikoanalyse aus Sicht der Geschäftsleitung

- Was eine Risikoanalyse nach NIS-2/BSIG leisten muss – ohne technische Details.
- Typische Bedrohungen und Schadensszenarien aus Management-Perspektive.
- Lesen und Verstehen von Risiko-Reports: Welche Fragen sollte die Geschäftsleitung stellen?
- Verankerung der Risikoanalyse im Risikomanagement und in der Unternehmensstrategie.

Kernbereich 2: Risikomanagementmaßnahmen und Mindestanforderungen

- Anforderungen an Risikomanagementmaßnahmen nach NIS-2-Richtlinie und § 30 BSIG.
- Überblick über typische technisch-organisatorische Maßnahmen (TOM) und Management-Aufgaben.
- Rolle der Geschäftsleitung: Zielvorgaben, Ressourcen, Priorisierung und Kontrolle.

Kernbereich 3: Auswirkungen von Risiken und Maßnahmen auf die erbrachten Dienste

- Welche Auswirkungen können Sicherheitsvorfälle auf Betrieb, Produktion, Dienstleistungen, Reputation und Finanzen haben?
- Bewertung von Maßnahmen aus Business-Sicht: Wirtschaftlichkeit, Verhältnismäßigkeit, Restrisiko.
- Umgang mit Restrisiken: Dokumentation, Kommunikation und Entscheidungsfindung in der Geschäftsleitung.

Rollen, Verantwortlichkeiten und wirksame Delegation

- Abgrenzung von Aufgaben: Was muss auf Geschäftsleitungsebene bleiben, was kann delegiert werden?
- Zusammenarbeit mit CISO/ISB, IT-Leitung, Datenschutz, Compliance und Risikomanagement.
- Anforderungen an Berichtswege, Kontrollen und Nachweisführung.

Umsetzung in der Praxis: Vom gesetzlichen Rahmen zur eigenen Governance

- Praxisbeispiele zu Sicherheitsvorfällen und Haftung der Geschäftsleitung.
- Ableitung einer eigenen „Roadmap“ für Geschäftsleitungen: Welche Punkte sollten kurzfristig, mittelfristig, langfristig angegangen werden?
- Dokumentation der Schulung und der getroffenen Management-Entscheidungen als Baustein zur Erfüllung der Nachweispflichten.

Hinweis zur Schulungspflicht

Mit diesem Seminar können Mitglieder der Geschäftsleitung ihre Schulungspflicht nach § 38 Abs. 3 BSIG adressieren. Die Inhalte orientieren sich an der Handreichung des BSI zur Schulungspflicht nach § 38 Abs. 3 BSIG und unterstützen Teilnehmende dabei, ihrer Schulungspflicht nachzukommen.

Lernumgebung

In deiner Online-Lernumgebung findest du nach deiner Anmeldung nützliche Informationen, Downloads und Extra-Services zu dieser Qualifizierungsmaßnahme.

Dein Nutzen

Klarheit über Pflichten der Geschäftsleitung:

- Die Anforderungen der NIS-2 und insbesondere § 38 BSIG an Geschäftsleitungen werden verstanden.

Kompetenz in Risikoanalyse und Risikomanagement:

- Die nötigen Kenntnisse werden erworben, um Risikoanalysen zu lesen, zu hinterfragen und die Angemessenheit von Risikomanagementmaßnahmen einzuschätzen – ohne selbst technische:r Expert:in sein zu müssen.

Bewusstsein für Auswirkungen von Risiken:

- Die Auswirkungen von Risiken und getroffenen Maßnahmen auf die von Unternehmen erbrachten Dienste können besser beurteilt werden, um Entscheidungen fundierter treffen zu können.

Haftungsrisiken erkennen und steuern:

- Ein Überblick über persönliche Haftungsrisiken wird gegeben, und es wird gezeigt, wie Governance-Strukturen, Delegation und Nachweise gestaltet werden sollten, um diese Risiken zu reduzieren.

Nachweisbare Weiterbildung der Geschäftsleitung:

- Die Teilnahme belegt, dass der Pflicht zur regelmäßigen Fortbildung im Bereich Informationssicherheit nach § 38 BSIG nachgekommen wurde. Eingeschlossen sind Fragestellungen, die anschließend im Unternehmen beantwortet werden müssen.

Methoden

Vortrag und Präsentation aus Management-Perspektive, konkrete Fallbeispiele und Szenarien, Diskussion von Praxisfragen der Teilnehmenden, Beantwortung individueller Fragen.

Teilnehmer:innenkreis

Das Seminar richtet sich an Mitglieder der Geschäftsleitung, Vorstände, Geschäftsführer:innen und weitere Personen in oberster Leitungsfunktion von Unternehmen und Einrichtungen, die unter die Kategorien „wichtige“ oder „besonders wichtige“ Einrichtungen im Sinne von NIS-2 (und hier v.a. des BSIG) fallen.

Gemäß § 2 Abs. 13 BSIG fällt unter „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist.

Technische Detailkenntnisse werden nicht vorausgesetzt; im Fokus stehen rechtliche, organisatorische und strategische Fragestellungen auf Management-Ebene.

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:

<https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges>



Referent:in



Sabine Sobola

Mein Name ist Sabine Sobola. Ich bin Rechtsanwältin und berate seit über 25 Jahren Unternehmen im IT- und Datenschutzrecht. Ich kenne die Herausforderungen, denen sich Organisationen täglich in Datenschutz- und IT-rechtlicher Hinsicht stellen müssen. Mein Schwerpunkt liegt dabei auf der praktischen Umsetzung von neuen, komplexen gesetzlichen Regelungen, vor allem im IT-Sicherheitsrecht.

Seit Oktober 2021 bin ich Geschäftsführerin der LiIDU GmbH.

Details zur Weiterbildung

Seminar | Präsenz

1 Tag

Termine

19.10.2026

München

Veranstaltungsort

Hyperion Hotel München

Tage & Uhrzeit

Montag, 19.10.2026

09:00 Uhr - 16:00 Uhr

05.02.2027

Berlin

Veranstaltungsort

Mercure Hotel Berlin Tempelhof

Tage & Uhrzeit

Freitag, 05.02.2027

09:00 Uhr - 16:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/41115

Teilnahmegebühr

€ 920,- zzgl. MwSt.

€ 1.094,80 inkl. MwSt.

Die angegebene Teilnahmegebühr beinhaltet

- ein gemeinsames Mittagessen pro vollem Seminartag,
- Pausenverpflegung und
- umfangreiche Arbeitsunterlagen.

Die Übernachtungskosten im Hotel werden von den Teilnehmenden direkt mit dem Hotel abgerechnet. Für die Hotelbuchung findest du in deiner Lernumgebung ein Reservierungsformular.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/41115

E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:

<https://www.haufe-akademie.de/faqs>

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.

Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.

NIS-2-Schulung für Geschäftsleitung und Top-Management (Live-Online)

Kontext der NIS-2-Regulierung, Pflichten für die Geschäftsleitung, Risikoanalyse und Risikomanagementmaßnahmen nach § 38 BSIG

Die NIS-2-Richtlinie und das Umsetzungsgesetz zu NIS-2 führen für „wichtige“ und „besonders wichtige“ Einrichtungen verschärfte Pflichten zur Informationssicherheit ein. Wichtiges Element ist die in § 38 BSIG verankerte Schulungspflicht der Geschäftsleitung: Mitglieder der Geschäftsleitung müssen regelmäßig ausreichend Kenntnisse zur Erkennung und Bewertung von Risiken, zu Risikomanagementmaßnahmen sowie zu den Auswirkungen von Risiken und Maßnahmen auf die erbrachten Dienste erwerben. Dieses Seminar ist speziell auf die Perspektive von Geschäftsleitung und Top-Management zugeschnitten. Es vermittelt den Kontext der NIS-2-Regulierung (NIS-2-Richtlinie und deutsches NIS-2-Umsetzungsgesetz, insbesondere BSIG), die übergreifenden Pflichten für die Einrichtung an sich und im Speziellen für die Geschäftsleitung, zeigt Haftungsrisiken und Compliance-Pflichten auf und konzentriert sich zudem auf die vom Gesetz geforderte Risikoanalyse, die normierten Risikomanagementmaßnahmen und die potenziellen Auswirkungen von Risiken und Risikomanagementmaßnahmen auf das eigene Unternehmen. Die Inhalte orientieren sich an der Handreichung des BSI zur Schulungspflicht nach § 38 Abs. 3 BSIG und unterstützen Teilnehmende dabei, ihre Verantwortung im Bereich Informationssicherheit nachweisbar wahrzunehmen.

Inhalte

Rechtlicher Rahmen: NIS-2-Richtlinie und BSIG

- Überblick über NIS-2-Richtlinie und das novellierte BSIG.
- Einordnung der Begriffe in KRITIS, „wichtige“ und „besonders wichtige“ Einrichtungen.
- Rolle der Geschäftsleitung bei Umsetzung, Überwachung und Nachweis der Risikomanagementmaßnahmen.
- Überblick über Haftungsrisiken und Sanktionsrahmen.

Kernbereich 1: Risikoanalyse aus Sicht der Geschäftsleitung

- Was eine Risikoanalyse nach NIS-2/BSIG leisten muss – ohne technische Details.
- Typische Bedrohungen und Schadensszenarien aus Management-Perspektive.
- Lesen und Verstehen von Risiko-Reports: Welche Fragen sollte die Geschäftsleitung stellen?
- Verankerung der Risikoanalyse im Risikomanagement und in der Unternehmensstrategie.

Kernbereich 2: Risikomanagementmaßnahmen und Mindestanforderungen

- Anforderungen an Risikomanagementmaßnahmen nach NIS-2-Richtlinie und § 30 BSIG.
- Überblick über typische technisch-organisatorische Maßnahmen (TOM) und Management-Aufgaben.
- Rolle der Geschäftsleitung: Zielvorgaben, Ressourcen, Priorisierung und Kontrolle.

Kernbereich 3: Auswirkungen von Risiken und Maßnahmen auf die erbrachten Dienste

- Welche Auswirkungen können Sicherheitsvorfälle auf Betrieb, Produktion, Dienstleistungen, Reputation und Finanzen haben?
- Bewertung von Maßnahmen aus Business-Sicht: Wirtschaftlichkeit, Verhältnismäßigkeit, Restrisiko.
- Umgang mit Restrisiken: Dokumentation, Kommunikation und Entscheidungsfindung in der Geschäftsleitung.

Rollen, Verantwortlichkeiten und wirksame Delegation

- Abgrenzung von Aufgaben: Was muss auf Geschäftsleitungsebene bleiben, was kann delegiert werden?
- Zusammenarbeit mit CISO/ISB, IT-Leitung, Datenschutz, Compliance und Risikomanagement.
- Anforderungen an Berichtswege, Kontrollen und Nachweisführung.

Umsetzung in der Praxis: Vom gesetzlichen Rahmen zur eigenen Governance

- Praxisbeispiele zu Sicherheitsvorfällen und Haftung der Geschäftsleitung.
- Ableitung einer eigenen „Roadmap“ für Geschäftsleitungen: Welche Punkte sollten kurzfristig, mittelfristig, langfristig angegangen werden?
- Dokumentation der Schulung und der getroffenen Management-Entscheidungen als Baustein zur Erfüllung der Nachweispflichten.

Hinweis zur Schulungspflicht

Mit diesem Seminar können Mitglieder der Geschäftsleitung ihre Schulungspflicht nach § 38 Abs. 3 BSIg adressieren. Die Inhalte orientieren sich an der Handreichung des BSI zur Schulungspflicht nach § 38 Abs. 3 BSIg und unterstützen Teilnehmende dabei, ihrer Schulungspflicht nachzukommen.

Lernumgebung

In deiner Online-Lernumgebung findest du nach deiner Anmeldung nützliche Informationen, Downloads und Extra-Services zu dieser Qualifizierungsmaßnahme.

Dein Nutzen

Klarheit über Pflichten der Geschäftsleitung:

- Die Anforderungen der NIS-2 und insbesondere § 38 BSIg an Geschäftsleitungen werden verstanden.

Kompetenz in Risikoanalyse und Risikomanagement:

- Die nötigen Kenntnisse werden erworben, um Risikoanalysen zu lesen, zu hinterfragen und die Angemessenheit von Risikomanagementmaßnahmen einzuschätzen – ohne selbst technische:r Expert:in sein zu müssen.

Bewusstsein für Auswirkungen von Risiken:

- Die Auswirkungen von Risiken und getroffenen Maßnahmen auf die von Unternehmen erbrachten Dienste können besser beurteilt werden, um Entscheidungen fundierter treffen zu können.

Haftungsrisiken erkennen und steuern:

- Ein Überblick über persönliche Haftungsrisiken wird gegeben, und es wird gezeigt, wie Governance-Strukturen, Delegation und Nachweise gestaltet werden sollten, um diese Risiken zu reduzieren.

Nachweisbare Weiterbildung der Geschäftsleitung:

- Die Teilnahme belegt, dass der Pflicht zur regelmäßigen Fortbildung im Bereich Informationssicherheit nach § 38 BSIg nachgekommen wurde. Eingeschlossen sind Fragestellungen, die anschließend im Unternehmen beantwortet werden müssen.

Methoden

Vortrag und Präsentation aus Management-Perspektive, konkrete Fallbeispiele und Szenarien, Diskussion von Praxisfragen der Teilnehmenden, Beantwortung individueller Fragen.

Teilnehmer:innenkreis

Das Seminar richtet sich an Mitglieder der Geschäftsleitung, Vorstände, Geschäftsführer:innen und weitere Personen in oberster Leitungsfunktion von Unternehmen und Einrichtungen, die unter die Kategorien „wichtige“ oder „besonders wichtige“ Einrichtungen im Sinne von NIS-2 (und hier v.a. des BSIg) fallen.

Gemäß § 2 Abs. 13 BSIg fällt unter „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist.

Technische Detailkenntnisse werden nicht vorausgesetzt; im Fokus stehen rechtliche, organisatorische und strategische Fragestellungen auf Management-Ebene.

Open Badges - Zeige auch digital, was du kannst.

Open Badges sind anerkannte, digitale Teilnahmezertifikate. Diese verifizierbaren Nachweise sind der aktuelle Standard für die Einbindung in Karrierenetzwerken wie z.B. LinkedIn.

Damit zeigst du digital, über welche Kompetenzen du verfügst.

Nach erfolgreichem Abschluss erhältst du von uns ein Open Badge.

Mehr erfahren kannst du unter:

<https://www.haufe-akademie.de/seminare-lehrgaenge/trending-topics/open-badges>



Referent:in



Sabine Sobola

Mein Name ist Sabine Sobola. Ich bin Rechtsanwältin und berate seit über 25 Jahren Unternehmen im IT- und Datenschutzrecht. Ich kenne die Herausforderungen, denen sich Organisationen täglich in Datenschutz- und IT-rechtlicher Hinsicht stellen müssen. Mein Schwerpunkt liegt dabei auf der praktischen Umsetzung von neuen, komplexen gesetzlichen Regelungen, vor allem im IT-Sicherheitsrecht.

Seit Oktober 2021 bin ich Geschäftsführerin der LiiDU GmbH.

Details zur Weiterbildung

Seminar | Online

1 Tag

Starttermine

23.11.2026

Live-Online

Durchführung

zoom

Modulzeiten

Montag, 23.11.2026

09:00 Uhr - 16:00 Uhr

Aktuelle Termine und weitere Informationen findest du unter www.haufe-akademie.de/41117

Teilnahmegebühr

€ 920,- zzgl. MwSt.

€ 1.094,80 inkl. MwSt.

Deine Anmeldemöglichkeiten

Online: www.haufe-akademie.de/41115

E-Mail: anmelden@haufe-akademie.de

Buche deine Weiterbildung einfach und schnell online. Gib sonst bitte unbedingt den Namen des Teilnehmenden und die vollständige Rechnungsanschrift mit Telefonnummer sowie E-Mail-Adresse an.

In unserem Bereich Fragen & Antworten (FAQ) findest du alle Antworten auf die häufigsten Fragen rund um unsere Weiterbildungen:

<https://www.haufe-akademie.de/faqs>

Unsere ausführlichen Teilnahmebedingungen findest du auch im Internet unter www.haufe-akademie.de/agb oder im Gesamtprogramm.

Die vollständigen Datenschutzbestimmungen findest du unter www.haufe-akademie.de/datenschutz.

Haufe Akademie GmbH & Co. KG

Munzinger Straße 9, 79111 Freiburg, www.haufe-akademie.de, Beratung: Tel.: +49 761 595339-00, service@haufe-akademie.de