Modulbeschreibung „NIS-2-Geschäftsleitungsschulung“

Modultitel	NIS-2-Geschäftsleitungsschulung (Schulung für Geschäftsleitungen gemäß § 38 Abs. 3 BSIG)
Kürzel/Modulnummer	NIS2-GL
Fachbereich	Informationssicherheit & Compliance
Modulverantwortlicher	Herr Prof. Dr. Mehrtens
Dozent	Herr Prof. Dr. Mehrtens, Herr Prof. Dr. Treibert
Modultyp	Pflichtschulung für Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen (§ 38 Abs. 3 BSIG); auch als freiwillige Schulung für Geschäftsleitungen nicht regulierter Unternehmen buchbar
Dauer	1/2 Tag, 4 Stunden (Erstschulung), zzgl. jährliche Auffrischungsschulung von 4 Stunden
Häufigkeit des Angebotes	Ausführliche Erstschulung einmalig, danach regelmäßige Folgeschulungen mind. 1x jährlich; Intervall risikoorientiert anzupassen (z. B. bei Wechsel der Geschäftsleitung, signifikanten Änderungen der Geschäftsprozesse, der Risikoexposition oder der Risikomanagementmaßnahmen)
Zielgruppe(n)	Geschäftsleitungen wichtiger und besonders wichtiger Einrichtungen im Sinne des § 38 Abs. 3 BSIG (natürliche Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung der Einrichtung berufen sind). Geeignet auch für Geschäftsleitungen nicht regulierter Unternehmen sowie für weitere Personen, die der Geschäftsleitung zuarbeiten oder anderweitige Entscheidungsvollmacht innehaben.
Angestrebte Lernergebnisse/ Learning outcomes	Diese Schulung basiert auf der Handreichung „Schulung für Geschäftsleitungen“ des BSI zur Schulungspflicht nach § 38 Abs. 3 BSIG. Die Teilnehmenden erlangen ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik. Die Handreichung des BSI konkretisiert die Kerninhalte gemäß § 38 Abs. 3 BSIG und sichert ein einheitliches Vorgehen sowie eine gleichbleibende Qualität der Schulung. Ziel ist die Befähigung der Geschäftsleitung zu informierten, fundierten Entscheidungen im Kontext des Cyberrisikos – nicht ihre Ausbildung zu Informationssicherheits-Expertinnen und -Experten.
Inhalte	**• Risikoanalyse (Erkennung und Bewertung von Risiken)** 1. Überblick über Sinn, Ziele und zentrale Begriffe des Risikomanagements 2. Identifizierung, Bewertung und Überwachung von Risiken 3. Zentrale Risikoquellen, Schwachstellen und Schutzbedarfe der eigenen Einrichtung 4. Grundbegriffe: Eintrittswahrscheinlichkeit, Schadensart und -ausmaß, Risikoakzeptanz 5. Risikomanagement als kontinuierlicher Prozess mit regelmäßiger Überprüfung 6. Regelmäßige Aktualisierung der Risikoanalyse bei neuen Bedrohungen **• Risikomanagementpraktiken (Risikomanagementmaßnahmen)** 1. Geeignete, verhältnismäßige und wirksame technisch-organisatorische Maßnahmen 2. Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit 3. Absicherung aller IT-Systeme, Komponenten und Prozesse der Leistungserbringung 4. Stand der Technik sowie einschlägige europäische und internationale Normen **• Auswirkungen von Risiken und Risikomanagementmaßnahmen** 1. Betriebliche, wirtschaftliche und regulatorische Auswirkungen einschätzen 2. Cybersicherheitsrisiken als Geschäftsrisiken einordnen und bewerten 3. Zielkonflikte zwischen Sicherheitsmaßnahmen und Dienstleistungserbringung 4. Strategien zur Risikobehandlung: Vermeidung, Minderung, Übertragung, Akzeptanz **• Überblick NIS-2-Regulierung und Pflichten der Geschäftsleitung (BSIG)** Ziele und Geltungsbereich des BSIG; Einordnung als wichtige oder besonders wichtige Einrichtung Melde- und Unterrichtungspflichten bei erheblichen Sicherheitsvorfällen Fristen des Melderegimes: Erstmeldung, Zwischen- und Abschlussmeldung Registrierungspflicht und -fristen gegenüber den Aufsichtsbehörden Pflicht zur Umsetzung und Überwachung von Risikomanagementmaßnahmen Mögliche Haftung der Geschäftsleitung für schuldhaft verursachte Schäden Gesetzliche Schulungspflicht nach § 38 Abs. 3 BSIG **• Die zehn Risikomanagementmaßnahmen gemäß BSIG (Teil 1)** 1. Konzepte zur Risikoanalyse und Sicherheit für Informationssysteme 2. Bewältigung von Sicherheitsvorfällen (Incident-Response) 3. Aufrechterhaltung des Betriebs: Backup, Wiederherstellung, Krisenmanagement 4. Sicherheit der Lieferkette **• Die zehn Risikomanagementmaßnahmen gemäß BSIG (Teil 2)** 1. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen 2. Bewertung der Wirksamkeit von Risikomanagementmaßnahmen

	3. Cyberhygiene und Schulungen der Mitarbeitenden 4. Einsatz von Kryptografie und Verschlüsselung 5. Sicherheit des Personals, Zugriffskontrolle und Asset-Management 6. Multi-Faktor-Authentifizierung und gesicherte Kommunikation **• Schulungsformate und Praxisbezug** 1. Risikomanagement-Quarterly mit der/dem Informationssicherheitsbeauftragten 2. Tabletop Exercise/Planspiel zu typischen Risikomanagement-Szenarien 3. Audit-Simulation (z. B. angelehnt an ISO-27001-Audit oder Audit nach § 61 BSIG) 4. Management Red-/Blue-Teaming mit Fokus auf Management-Entscheidungen 5. Sektor- und einrichtungsspezifische Szenarien und Case-Studies 6. Live-Hacking als anschauliche Ergänzung zu anderen Formaten **• Nachweis der Schulungsteilnahme: Schulungsanbieter, Teilnehmende, Datum/Dauer, Inhalte mit Bezug zu § 38 Abs. 3 BSIG**
Lehrformen	Interaktives Präsenzseminar mit Fallbeispielen, Tabletop Exercise und moderierter Diskussion; alternativ auch als Blended-Learning-Format oder in zeitlich dezentralen Modulen möglich
Unterrichtssprache	Deutsch
Voraussetzungen zur Weiterbildung	Keine speziellen IT-technischen Vorkenntnisse erforderlich. Die Teilnehmenden sollten bereit sein, sich mit ihrer gesetzlichen Rolle und Verantwortung als Geschäftsleitung einer wichtigen oder besonders wichtigen Einrichtung nach § 38 BSIG auseinanderzusetzen.
Prüfungsleistung(en)	Eine Prüfungsleistung ist gesetzlich nicht vorgeschrieben und wird nicht abgenommen. Der Nachweis der Schulung erfolgt durch eine aussagekräftige Dokumentation (Schulungsanbieter, Teilnehmende mit Name/Rolle, Datum/Uhrzeit/Dauer, behandelte Inhalte/Formate mit Bezug zu § 38 Abs. 3 BSIG). Optional kann ergänzend eine unbenotete Lernerfolgskontrolle (z. B. Kurz-Quiz oder Fallstudien-Reflexion) angeboten werden; sie ersetzt nicht die aktive, nachvollziehbare Mitwirkung der Geschäftsleitung an Entscheidungen des Risikomanagements.
Workload / Arbeitsaufwand	mind. 4 h (Erstschulung), zzgl. jährliche Auffrischung
Kontaktzeit	4 h (Erstschulung) / 3 h (Auffrischung)
Selbststudium	optional: Lektüre der BSI-Handreichung „Schulung für Geschäftsleitungen“ (ca. 1 h)
Geplante Gruppengröße	max. 15 Personen
Verwendbarkeit des Moduls	Modul ist auch für freiwillige Schulungen von Geschäftsleitungen nicht regulierter Einrichtungen einsetzbar; Inhalte sind sektorspezifisch anpassbar.
Literatur	Bundesamt für Sicherheit in der Informationstechnik (BSI): „Schulung für Geschäftsleitungen“ – Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen wichtiger Einrichtungen und besonders wichtiger Einrichtungen nach dem BSI-Gesetz sowie für freiwillige Schulungen von Geschäftsleitungen nicht-regulierter Unternehmen, Version 1.0, 17.04.2026; BSI-Gesetz (BSIG), insbesondere §§ 30, 38, 61, 62.