PECB

BEYOND RECOGNITION

NIS 2 DIRECTIVE LEAD IMPLEMENTER

Kandidatenhandbuch

PECB

Inhaltsverzeichnis

ABSCHNITT I: EINFÜHRUNG

Über PECB

PECB ist eine Zertifizierungsstelle, die Ausbildung[1], Zertifizierung und Zertifikatslehrgänge für Personen in einer Vielzahl von Disziplinen anbietet.

Durch unsere Präsenz in mehr als 150 Ländern helfen wir Fachleuten, ihre Kompetenz in verschiedenen Fachgebieten nachzuweisen, indem wir wertvolle Bewertungs-, Zertifizierungs- und Zertifikatsprogramme nach international anerkannten Normen anbieten.

Unsere Hauptziele sind:

1. Festlegung der Mindestanforderungen, die für die Zertifizierung von Fachleuten und die Erteilung von Bezeichnungen erforderlich sind
2. Überprüfung und Verifizierung der Qualifikationen von Personen, um sicherzustellen, dass diese die Anforderungen für eine Zertifizierung erfüllen
3. Aufrechterhaltung und fortlaufende Verbesserung des Bewertungsprozesses für die Zertifizierung von Personen
4. Zertifizierung von qualifizierten Personen, Erteilung von Bezeichnungen und Führung entsprechender Verzeichnisse
5. Festlegung von Anforderungen für die regelmäßige Erneuerung von Zertifizierungen und Sicherstellung, dass die zertifizierten Personen diese Anforderungen erfüllen
6. Sicherstellung, dass die PECB-Fachleute in ihrer beruflichen Praxis ethische Standards einhalten
7. Vertretung unserer Interessengruppen in Angelegenheiten von gemeinsamem Interesse
8. Förderung der Vorteile von Zertifizierungs- und Zertifikatsprogrammen für Fachleute, Unternehmen, staatliche Stellen und die Öffentlichkeit

Unsere Mission

Unseren Kunden umfassende Dienste in den Bereichen Prüfung, Zertifizierung und Zertifikatsprogramme anzubieten, die Vertrauen schaffen und der Gesellschaft als Ganzem zugutekommen.

Unsere Vision

Der globale Maßstab für die Bereitstellung professioneller Zertifizierungsdienste und Zertifikatsprogramme zu werden.

Unsere Werte

Integrität, Professionalität, Fairness

[1] Der Begriff Ausbildung bezieht sich auf die von PECB entwickelten und über unsere Partner weltweit angebotenen Schulungen.

Der Wert der PECB-Zertifizierung

Weltweite Anerkennung
Die PECB-Zertifikate sind international anerkannt und werden von vielen Akkreditierungsstellen unterstützt, so dass Fachleute, die sie erwerben, von unserer Anerkennung auf nationalen und internationalen Märkten profitieren.

Der Wert der PECB-Zertifizierungen wird durch die Akkreditierung des Internationalen Akkreditierungsdienstes (International Accreditation Service, IAS-PCB-111), des britischen Akkreditierungsdienstes (United Kingdom Accreditation Service, UKAS-Nr. 21923) und des koreanischen Akkreditierungsrates (Korean Accreditation Board, KAB-PC-08) gemäß ISO/IEC 17024 - Allgemeine Anforderungen an Stellen, die Personen zertifizieren - bestätigt. Der Wert der PECB-Zertifikatsprogramme wird durch die Akkreditierung durch das ANSI Nationaler Akkreditierungsrat (National Accreditation Board, ANAB-Accreditation ID 1003) unter ANSI/ASTM E2659-18, "Standart Verfahren für Zertifikatsprogramme“ (Standard Practice for Certificate Programs) bestätigt.

Die PECB ist assoziiertes Mitglied der Unabhängigen Vereinigung der akkreditierten Registrierungsstellen (The Independent Association of Accredited Registrars, IAAR), Vollmitglied der Internationalen Vereinigung für Personalzertifizierung (International Personnel Certification Association , IPC), zeichnendes Mitglied von IPC MLA und Mitglied von Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine und ITCC. Darüber hinaus ist die PECB ein von der Akkreditierungsstelle für die Zertifizierung nach dem Cybersecurity Maturity Model (CMMC-AB) zugelassener Lizenzpartner (LPP) für den Cybersecurity Maturity Model-Zertifizierungsstandard (CMMC), ist vom Club EBIOS für die EBIOS-Zertifizierung für Risikomanager-Fähigkeiten zugelassen und von der CNIL (Commission Nationale de l'Informatique et des Libertés) für die DPO-Zertifizierung zugelassen. Für weitere Informationen klicken Sie bitte hier.

Hochwertige Produkte und Dienstleistungen
Wir sind stolz darauf, unseren Kunden hochwertige Produkte und Dienstleistungen anbieten zu können, die deren Erfordernissen und Anforderungen entsprechen. Alle unsere Produkte werden von einem Team von Experten und Fachleuten auf der Grundlage der besten Praktiken und Methoden sorgfältig erstellt.

Einhaltung von Normen
Unsere Zertifizierungen und Zertifikatsprogramme sind ein Beweis für die Einhaltung der Normen ISO/IEC 17024 und ASTM E2659. Sie stellen sicher, dass die Anforderungen der Normen mit angemessener Konsistenz, Professionalität und Unparteilichkeit erfüllt und validiert wurden.

Kundenorientierter Service
Wir sind ein kundenorientiertes Unternehmen und behandeln alle unsere Kunden mit Wertschätzung, Wichtigkeit, Professionalität und Ehrlichkeit. PECB verfügt über ein Team von Fachleuten, das für den Umgang mit Anfragen, Fragen und Bedürfnissen zuständig ist. Wir tun unser Bestes, um eine maximale Reaktionszeit von 24 Stunden einzuhalten, ohne die Qualität der Dienstleistungen zu beeinträchtigen.

Flexibilität und Komfort
Online-Lernangebote machen Ihren beruflichen Werdegang komfortabler, da Sie Ihre Lerneinheiten entsprechend Ihrem Lebensstil planen können. Diese Flexibilität verschafft Ihnen mehr Freizeit, bietet mehr Aufstiegsmöglichkeiten und senkt die Kosten.

PECB-Ethikkodex

Der Ethikkodex repräsentiert die höchsten Werte und die Ethik, zu deren Einhaltung sich die PECB verpflichtet hat, da sie die Bedeutung dieser Werte bei der Erbringung von Dienstleistungen und der Gewinnung von Kunden anerkennt.

Die Compliance-Abteilung stellt sicher, dass die Beschäftigten, Kursleitungen, Prüfer, Aufsichtspersonen, Partner, Vertriebspartner, Mitglieder verschiedener Beiräte und Ausschüsse, zertifizierte Personen und Zertifikatsinhaber (im Folgenden "PECB-Fachleute") diesen Ethik-Kodex einhalten. Darüber hinaus betont die Compliance-Abteilung immer wieder die Notwendigkeit, bei der Erbringung von Dienstleistungen gegenüber internen und externen Interessengruppen wie Antragstellern, Kandidaten, zertifizierten Personen, Zertifikatsinhabern, Akkreditierungsbehörden und Regierungsbehörden professionell und mit voller Verantwortung, Kompetenz und Fairness zu handeln.

PECB ist der Überzeugung, dass sie nur dann erfolgreich sein kann, wenn sie die Erfordernisse und Erwartungen ihrer Kunden und Interessenträger vollständig versteht. Um dies zu erreichen, pflegt die PECB eine Kultur, die auf einem Höchstmaß an Integrität, Professionalität und Fairness basiert, die auch ihre Werte sind. Diese Werte sind integraler Bestandteil der Organisation und haben die globale Präsenz und das Wachstum im Laufe der Jahre geprägt und das Ansehen begründet, das die PECB heute genießt.

Die PECB ist davon überzeugt, dass starke ethische Werte eine wesentliche Voraussetzung für gesunde und starke Beziehungen sind. Daher ist es die Hauptverantwortung der PECB, sicherzustellen, dass das Verhalten der PECB-Fachleute in vollem Einklang mit den Prinzipien und Werten der PECB steht.

PECB-Fachleute sind verantwortlich für Folgendes:

1. Bei der Erbringung von Dienstleistungen ein professionelles Verhalten an den Tag zu legen, das sich durch Ehrlichkeit, Genauigkeit, Fairness und Unabhängigkeit auszeichnet
2. Bei der Erbringung ihrer Dienstleistungen jederzeit ausschließlich im besten Interesse ihres Arbeitgebers, ihrer Kunden, der Öffentlichkeit und des Berufsstandes in Übereinstimmung mit diesem Ethikkodex und anderen beruflichen Standards zu handeln
3. Ihre Kompetenz in ihrem jeweiligen Fachgebiet unter Beweis stellen und weiterentwickeln und danach streben, ihre Fähigkeiten und Kenntnisse kontinuierlich zu verbessern
4. Dienstleistungen nur für solche zu erbringen, für die sie qualifiziert und kompetent sind, und Klienten und Kunden in angemessener Weise über die Art der vorgeschlagenen Dienstleistungen, einschließlich aller relevanten Bedenken oder Risiken, zu informieren
5. Ihren Arbeitgeber oder Kunden über alle geschäftlichen Interessen oder Verbindungen zu informieren, die ihr Urteilsvermögen beeinflussen oder beeinträchtigen könnten
6. Die Vertraulichkeit von Informationen über gegenwärtige oder frühere Arbeitgeber oder Kunden während der Erbringung der Dienstleistung zu wahren
7. Alle geltenden Gesetze und Vorschriften des Landes, in dem die Dienstleistung erbracht wurde, einzuhalten
8. Das geistige Eigentum und die Verdienste anderer zu respektieren
9. Keine Weitergabe von vorsätzlich falschen oder gefälschten Informationen, die die Integrität des Bewertungsprozesses eines Kandidaten für eine PECB-Zertifizierung oder ein PECB-Zertifikatsprogramm beeinträchtigen könnten

10. Sich nicht fälschlicherweise als PECB-Vertreter auszugeben, ohne eine entsprechende Lizenz zu besitzen oder das Logo, Zertifizierungen oder Zertifikate von PECB zu missbrauchen
11. In keiner Weise zu handeln, die den Zertifizierungen, den Zertifikatsprogrammen oder dem Ansehen der PECB schaden könnte
12. Vollständige Kooperation bei der Untersuchung nach einem behaupteten Verstoß gegen diesen Ethikkodex

Die vollständige Fassung des Ethik-Kodex der PECB finden Sie unter Ethik-Kodex | PECB.

Einführung in NIS 2 Directive Lead Implementer

Die NIS 2-Richtlinie legt die Anforderungen für die Verbesserung der Sicherheit von Netz- und Informationssystemen in der Europäischen Union (EU) fest. Ein Cybersicherheitsprogramm im Einklang mit den Anforderungen der NIS-2-Richtlinie ermöglicht es Organisationen, ihre Cybersicherheitsmaßnahmen zu verstärken, kritische Infrastrukturen zu schützen und die rechtlichen Anforderungen in der EU zu erfüllen. Die NIS-2-Richtlinie gilt für ein breites Spektrum von Organisationen, die in der Richtlinie als wesentliche oder wichtige Einrichtungen definiert werden, wobei für jeden Sektor bestimmte Größenschwellen gelten. Sie umfasst sowohl Organisationen, die wesentliche oder wichtige Dienste für die europäische Wirtschaft und Gesellschaft erbringen, als auch Organisationen, die in einem Mitgliedstaat die einzigen Anbieter eines kritischen Dienstes sind.

Die Qualifikation „NIS 2 Directive Lead Implementer“ ist eine professionelle Zertifizierung für Personen, die ihre Kompetenz in Bezug auf die Anforderungen der NIS 2-Richtlinie und die Leitung eines Implementierungsteams nachweisen wollen.

Da es sich bei der Implementierung um einen sehr gefragten Beruf handelt, kann der Erwerb einer international anerkannten Zertifizierung Ihre Karriere erheblich (be)fördern und Sie in die Lage versetzen, Ihre beruflichen Ziele zu erreichen.

Dieses Dokument spezifiziert das Zertifizierungsprogramm zum PECB NIS 2 Directive Lead Implementer in Übereinstimmung mit ISO/IEC 17024:2012. Außerdem werden die Schritte beschrieben, die die Bewerber unternehmen müssen, um ihren Berechtigungsnachweis zu erlangen und aufrechtzuerhalten. Es ist daher sehr wichtig, dass Sie alle in diesem Dokument enthaltenen Informationen sorgfältig lesen, bevor Sie Ihren Antrag ausfüllen und einreichen. Bestehen nach dem Lesen dieses Dokuments noch Fragen weiterer Informationsbedarf, wenden Sie sich bitte an das internationale Büro der PECB unter certification.team@pecb.com.

ABSCHNITT II: PRÜFUNGSVORBEREITUNG, REGELN UND RICHTLINIEN

Vorbereitung auf und Planung der Prüfung

Alle Kandidaten sind für ihr eigenes Lernen und ihre Vorbereitung auf die Zertifizierungsprüfungen verantwortlich. Die Teilnahme an der Schulung ist zwar nicht zwingend erforderlich, um zur Prüfung zugelassen zu werden, kann aber die Chancen auf ein erfolgreiches Bestehen der Prüfung deutlich erhöhen.

Um den Prüfungstermin zu planen, haben die Kandidaten zwei Möglichkeiten:

1. Kontaktaufnahme mit einem unserer autorisierten Partner. Um einen autorisierten Partner in Ihrer Region zu finden, gehen Sie bitte zu Aktive Partner. Der Schulungskalender ist auch online verfügbar und kann unter Schulungsveranstaltungen eingesehen werden.
2. Ablegen einer PECB-Prüfung aus der Ferne über die Anwendung PECB Exams. Um eine Fernprüfung zu planen, gehen Sie bitte auf den folgenden Link: Prüfungsveranstaltungen.

Weitere Informationen über Prüfungen, Kompetenzbereiche und Angaben zu Kenntnissen finden Sie in Abschnitt III dieses Dokuments.

Verschiebung der Prüfung

Bei Änderungen des Prüfungsdatums, der Uhrzeit, des Ortes oder anderer Details wenden Sie sich bitte an online.exams@pecb.com.

Anmeldegebühren für Prüfung und Zertifizierung

Die Kandidaten können die Prüfung ablegen, ohne an der Schulung teilzunehmen. Die entsprechenden Preise sind wie folgt:

- Lead Prüfung: 1000$[2]
- Manager Prüfung: 700$
- Foundation Prüfung: 500$
- Transition Prüfung: 500$

Die Antragsgebühr für die Zertifizierung beträgt 500 Dollar.

Für die Kandidaten, die die Schulung über einen der Partner der PECB absolviert haben, deckt die Anmeldegebühr die Kosten für die Prüfung (erster Versuch und erste Wiederholung), den Antrag auf Zertifizierung und die jährliche Aufrechterhaltungsgebühr (AMF) für das erste Jahr ab.

[2]Alle Preise in diesem Dokument sind in US Dollar angegeben.

Kompetenzbereiche

Mit der Prüfung zum „PECB NIS 2 Directive Lead Implementer“ soll sichergestellt werden, dass der Kandidat die notwendigen Kompetenzen erworben hat, um eine Organisation bei der Einrichtung, Implementierung, Verwaltung und Aufrechterhaltung eines Programms zur Einhaltung der NIS 2-Richtlinie zu unterstützen.

Die Zertifizierung zum NIS 2 Directive Lead Implementer richtet sich an:

- Fachleute für Cybersicherheit, die ein umfassendes Verständnis der Anforderungen der NIS-2-Richtlinie erlangen und praktische Strategien zur Implementierung robuster Cybersicherheitsmaßnahmen erlernen möchten
- IT-Manager und -Fachleute, die Einblicke in die Implementierung sicherer Systeme gewinnen und die Resilienz kritischer Systeme verbessern möchten
- Vertreter staatlicher Stellen oder Behörden, die für die Durchsetzung der NIS-2-Richtlinie zuständig sind

Der Inhalt der Prüfung gliedert sich wie folgt:

- **Bereich 1:** Grundlegende Konzepte und Definitionen der NIS-2-Richtlinie
- **Bereich 2:** Planung der Implementierung der Anforderungen der NIS-2-Richtlinie
- **Bereich 3:** Rollen und Verantwortlichkeiten im Bereich Cybersicherheit und Risikomanagement
- **Bereich 4:** Cybersicherheitsmaßnahmen, Handhabung von Vorfällen und Krisenmanagement
- **Bereich 5:** Kommunikation und Sensibilisierung
- **Bereich 6:** Testen und Überwachung eines Cybersicherheitsprogramms

PECB

Bereich 1: Grundlegende Konzepte und Definitionen der NIS-2-Richtlinie

Hauptziel: Sicherstellen, dass der Kandidat in der Lage ist, die Konzepte und Definitionen der NIS-2-Richtlinie zu interpretieren.

Kompetenzen	Kenntnisse
1. Fähigkeit zur Erläuterung der wichtigsten Konzepte im Zusammenhang mit der NIS-2-Richtlinie 2. Fähigkeit, ein umfassendes Wissen über ISO-Normen im Bereich der Informationssicherheit zu entwickeln 3. Fähigkeit, andere beste Praktiken der Branche im Bereich Cybersicherheit zu erkennen, einschließlich NIST Cybersicherheitsrahmen und CIS-Controls 4. Fähigkeit, ENISA-Veröffentlichungen zur Cybersicherheit zu identifizieren 5. Fähigkeit zum Vergleich der NIS-2-Richtlinie mit ihrem Vorgänger, der NIS-Richtlinie 6. Fähigkeit zur Analyse von Struktur, Zielen und Gegenstand der NIS-2-Richtlinie 7. Fähigkeit zur Bewertung der potenziellen Auswirkungen der NIS-2-Richtlinie auf verschiedene Interessenträger, einschließlich wesentlicher und wichtiger Einrichtungen 8. Fähigkeit, die bei Nichteinhaltung der NIS-2-Richtlinie verhängten Geldbußen zu nennen 9. Fähigkeit, die wichtigen EU-Organisationen zu erkennen und zu beschreiben, die an der Durchsetzung und Regulierung der Cybersicherheit in der Europäischen Union beteiligt sind	1. Kenntnis der wichtigsten Konzepte und der Terminologie der NIS-2-Richtlinie 2. Kenntnis der ISO-Normen im Bereich der Informationssicherheit, einschließlich ISO/IEC 27001 und ISO/IEC 27002 3. Kenntnisse der für die Informations- und Cybersicherheit relevanten rechtlichen Rahmenbedingungen und Regelungen, einschließlich des Gesetzes über digitale Märkte, des Gesetzes über digitale Dienste, des Gesetzes zur digitale operationale Resilienz, des EU-Cybersicherheitsgesetzes, des europäischen Gesetzes über Cyberresilienz, des Datenverwaltungsgesetzes, der DSGVO und der überarbeiteten Zahlungsdiensterichtlinie 4. Kenntnisse über den Anwendungsbereich der NIS-2-Richtlinie und deren Vergleich mit der NIS-Richtlinie 5. Kenntnisse über die Beziehung zwischen der NIS-2-Richtlinie und der Normenreihe ISO/IEC 27000 6. Kenntnisse der Struktur, der Ziele und des Gegenstands der NIS-2-Richtlinie und ihrer Auswirkungen auf Organisationen und kritische Infrastrukturbereiche 7. Kenntnisse über die Auswirkungen der NIS-2-Richtlinie 8. Kenntnisse der Geldbußen bei Nichteinhaltung der NIS-2-Richtlinie und der Kriterien für die Festlegung solcher Geldbußen 9. Kenntnis der wichtigsten EU-Organisationen, die für die Steuerung, Regulierung und Überwachung der Cybersicherheit zuständig sind, und ihrer Rolle bei der Durchsetzung der NIS-2-Richtlinie

Bereich 2: Planung der Implementierung der Anforderungen der NIS-2-Richtlinie

Hauptziel: Sicherstellen, dass der Kandidat in der Lage ist, die wichtigsten Anforderungen der NIS-2-Richtlinie zu erkennen und zu erklären und deren Implementierung zu planen.

Kompetenzen	Kenntnisse
1. Fähigkeit zur Erläuterung der Bestandteile der NIS-2-Richtlinie, einschließlich Governance, Krisenmanagement, Risikomaßnahmen und Berichtspflichten	1. Kenntnis der Bestandteile und Anforderungen der NIS-2-Richtlinie, einschließlich Definitionen, Governance, Krisenmanagement, Risikomanagement und Berichtspflichten
2. Fähigkeit zur Festlegung der Herangehensweise für die Implementierung der Anforderungen der NIS-2-Richtlinie	2. Kenntnis der wichtigsten Ansätze und Methoden zur Implementierung der Anforderungen der NIS-2-Richtlinie
3. Fähigkeit, die für die Planung der Implementierung der Anforderungen der NIS-2-Richtlinie erforderlichen Informationen zu sammeln, zu analysieren und zu interpretieren	3. Kenntnis der einschlägigen Ziele zur Einhaltung der NIS-2-Richtlinie und wie diese erreicht werden können
4. Fähigkeit zur Interpretation und Festlegung von Zielen für die Einhaltung der NIS-2-Richtlinie	4. Kenntnisse darüber, was typischerweise den internen und externen Kontext einer Organisation ausmacht
5. Fähigkeit, den internen und externen Kontext einer Organisation zu analysieren und zu berücksichtigen	5. Kenntnis der Ansätze zum Verstehen des Kontexts einer Organisation
6. Fähigkeit, die Rollen und Verantwortlichkeiten der wichtigsten interessierten Parteien während und nach der Implementierung der Anforderungen der NIS-2-Richtlinie zu identifizieren	6. Kenntnis der Techniken, die zur Sammlung von Informationen über eine Organisation und zur Durchführung einer Gap-Analyse verwendet werden
7. Fähigkeit zur Durchführung einer Gap-Analyse und zur Klärung der Ziele für die Einhaltung der NIS-2-Richtlinie	7. Kenntnisse über einen Projektplan bzw. ein Projektteam zur Implementierung der NIS-2-Richtlinie
8. Fähigkeit, den Anwendungsbereich des Programms zur Implementierung der NIS-2-Richtlinie zu definieren und zu begründen, angepasst an die spezifischen Ziele der Organisation zur Einhaltung der NIS-2-Richtlinie	8. Kenntnis der wichtigsten Organisationsstrukturen, die in einer Organisation für die Steuerung der Implementierung der NIS-2-Richtlinie geeignet sind
9. Fähigkeit zur Erläuterung der Anforderungen der NIS-2-Richtlinie in Bezug auf Governance und Cybersicherheitsstrategie	9. Kenntnis der Merkmale des Anwendungsbereichs der NIS-2-Richtlinie in Bezug auf organisatorische, technologische und physische Grenzen
10. Fähigkeit zur Entwicklung eines Programms zur Einhaltung der Cybersicherheit	10. Kenntnis der Artikel der NIS-2-Richtlinie, die sich mit Governance und nationaler Cybersicherheitsstrategie befassen
11. Fähigkeit, die Arten von Politiken zu erkennen und eine Cybersicherheitspolitik zu entwickeln	11. Kenntnis der notwendigen Tätigkeiten zur Entwicklung eines Programms zur Einhaltung der Cybersicherheit

	12. Kenntnis der besten Praktiken und Techniken für die Erarbeitung und Festlegung von Cybersicherheitspolitiken und -verfahren

Bereich 3: Rollen und Verantwortlichkeiten im Bereich Cybersicherheit und Risikomanagement

Hauptziel: Sicherstellen, dass der Kandidat in der Lage ist, Rollen und Verantwortlichkeiten im Bereich der Cybersicherheit zu definieren und ein Risikomanagement durchzuführen

Kompetenzen	Kenntnisse
1. Fähigkeit zur Analyse der Organisationsstruktur und zur Zuweisung von Schlüsselrollen und Verantwortlichkeiten im Zusammenhang mit der Cybersicherheit 2. Fähigkeit zur Definition von Rollen und Verantwortlichkeiten innerhalb der Organisation 3. Fähigkeit zum Aufbau eines wirksamen Cybersicherheitsteams innerhalb der Organisation 4. Fähigkeit zur wirksamen Verwaltung von Cybersicherheitsressourcen 5. Fähigkeit zur Identifizierung von Cybersicherheitsrisiken durch Beurteilung von Bedrohungen, Schwachstellen und potenziellen Auswirkungen 6. Fähigkeit zur Analyse von Cybersicherheitsrisiken, um deren Wahrscheinlichkeit und mögliche Folgen zu bestimmen 7. Fähigkeit zur Bewertung von Cybersicherheitsrisiken, um sie auf Grundlage ihrer Bedeutung für und ihrer potenziellen Auswirkungen auf das Unternehmen zu priorisieren 8. Fähigkeit zur Implementierung von Risikobehandlungsstrategien zur Minderung der identifizierten Cybersicherheitsrisiken 9. Fähigkeit zur effektiven Kommunikation und Konsultation mit relevanten Interessenträgern in Bezug auf Cybersicherheitsrisiken und Strategien zur Risikominderung 10. Fähigkeit zur Führung von Aufzeichnungen und zur Berichterstattung über Cybersicherheitsrisiken sowie zur kontinuierlichen Überwachung und	1. Kenntnis der Organisationsstruktur 2. Kenntnis der Rollen und Verantwortlichkeiten im Bereich der Cybersicherheit 3. Kenntnis der Anforderungen der NIS-2-Richtlinie in Bezug auf die Verwaltung von Werten 4. Kenntnis der Verwaltung von Werten im Bereich der Cybersicherheit 5. Kenntnis der Anforderungen der NIS-2-Richtlinie in Bezug auf das Risikomanagement 6. Kenntnis der Leitfäden für das Risikomanagement, z. B. ISO 31000, ISO/IEC 27005 und ENISA-Veröffentlichungen 7. Kenntnis der Identifizierung und Analyse von Cybersicherheitsrisiken zur Bestimmung der Wahrscheinlichkeit und der möglichen Folgen 8. Kenntnis der Bewertung von Cybersicherheitsrisiken zur Implementierung wirksamer Risikobehandlungsstrategien 9. Kenntnisse über die Kommunikation und Beratung mit relevanten Interessenträgern in Bezug auf Cybersicherheitsrisiken 10. Kenntnisse über die Führung von Aufzeichnungen und die Berichterstattung über Cybersicherheitsrisiken deren Behandlung und deren Status 11. Kenntnisse über die Überwachung und Überprüfung des Verfahrens zur Bestimmung der Wirksamkeit von Bemühungen im Cybersicherheitsrisikomanagement

Überprüfung der Wirksamkeit des Cybersicherheitsrisikomanagements	

Bereich 4: Cybersicherheitsmaßnahmen, Handhabung von Vorfällen und Krisenmanagement

Hauptziel: Sicherstellen, dass der Kandidat in der Lage ist, die für die Einhaltung der NIS-2-Richtlinie erforderlichen Cybersicherheitsprozesse umzusetzen, einschließlich Cybersicherheitsmaßnahmen, Sicherheit in der Lieferkette, Handhabung von Vorfällen und Krisenmanagement.

Kompetenzen	Kenntnisse
1. Fähigkeit zur Auslegung der Anforderungen der NIS-2-Richtlinie in Bezug auf Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit 2. Fähigkeit zur Erläuterung von Sicherheitsmaßnahmen im Personalbereich auf der Grundlage der besten Praktiken der Branche 3. Fähigkeit, beste Praktiken für eine wirksame Zugangssteuerung zum Schutz von Netz- und Informationssystemen zu erläutern 4. Fähigkeit zur Anwendung von kryptographischen Techniken zur Verbesserung der Datensicherheit 5. Fähigkeit, die notwendigen Maßnahmen zum Schutz von Netzwerkdiensten und -systemen zu identifizieren und umzusetzen 6. Fähigkeit zur Auswahl und Implementierung von Risikomanagementprozessen in der Lieferkette, zur Einrichtung von Prozessen für den Umgang mit Schwachstellen und zur Verbesserung der Informationssicherheit in Lieferantenbeziehungen 7. Fähigkeit, sich auf Cybersicherheitsvorfälle vorzubereiten, sie zu erkennen, zu melden, zu bewerten, darauf zu reagieren und daraus zu lernen 8. Fähigkeit zur Erstellung eines Krisenmanagementplans, von Krisenkommunikationsplänen und Notfallkommunikationssystemen zur Bewältigung schwieriger Situationen 9. Fähigkeit zur Entwicklung umfassender Pläne zur Aufrechterhaltung und Wiederherstellung der Betriebsfähigkeit zur Sicherstellung der Betriebsfähigkeit	1. Kenntnis der Anforderungen der NIS-2-Richtlinie in Bezug auf technische, betriebliche und organisatorische Maßnahmen 2. Kenntnis der für das Risikomanagement erforderlichen Cybersicherheitsmaßnahmen, z. B. Personalsicherheit, Zugangssteuerung, Kryptographie und Netzsicherheit 3. Kenntnis der Anforderungen der NIS-2-Richtlinie in Bezug auf Maßnahmen zur Gewährleistung der Sicherheit in der Lieferkette 4. Kenntnis des Risikomanagements in der Lieferkette, des Umgangs mit Schwachstellen und der Praktiken der Informationssicherheit in Lieferantenbeziehungen 5. Kenntnis der Prozesse zur Vorbereitung und Reaktion auf sowie zur Erkennung, Meldung, Bewertung und Auswertung von Cybersicherheitsvorfällen 6. Kenntnis der Rolle und der Verantwortlichkeiten von CSIRTs bei der Handhabung von Vorfällen gemäß der NIS-2-Richtlinie 7. Kenntnis der durch die NIS-2-Richtlinie vorgeschriebenen Berichtspflichten für die an der Handhabung von Vorfällen beteiligten Parteien 8. Kenntnis der Anforderungen der NIS-2-Richtlinie an die Mitgliedstaaten und die CSIRTs in Bezug auf das Krisenmanagement im Bereich der Cybersicherheit 9. Kenntnisse über Krisenmanagement und die Merkmale und Bedeutung der Krisenkommunikation 10. Kenntnisse im Bereich Business Continuity Management (Aufrechterhaltung der

	Betriebsfähigkeit), einschließlich Strategien und Wiederherstellungsplanung

Bereich 5: Kommunikation und Sensibilisierung

Hauptziel: Sicherstellen, dass der Kandidat in der Lage ist, wirksame Kommunikations-, Kompetenzentwicklungs- und Sensibilisierungsprogramme zu entwickeln und zu implementieren, um die Ziele der Cybersicherheit und der Organisation zu unterstützen sowie die Anforderungen der NIS-2-Richtlinie zu erfüllen.

Kompetenzen	Kenntnisse
1. Fähigkeit zur Planung und Durchführung von Tätigkeiten zur Kompetenzentwicklung, einschließlich Programmen zur Schulung und Sensibilisierung 2. Fähigkeit, die Struktur und Art von Kompetenzentwicklungsprogrammen im Einklang mit den Unternehmenszielen zu definieren 3. Fähigkeit zur wirksamen Durchführung von Programmen zur Schulung und Sensibilisierung, um den ermittelten Bedarf zu decken 4. Fähigkeit, die Ergebnisse und die Wirksamkeit von Programmen zur Schulung und Sensibilisierung zu beurteilen und zu bewerten 5. Fähigkeit zur Planung, Durchführung und Bewertung von Kommunikationstätigkeiten zur Erreichung der Kommunikationsziele 6. Fähigkeit, die Anforderungen der NIS-2-Richtlinie in Bezug auf das Bewusstsein für Cybersicherheit und den Informationsaustausch zu erkennen 7. Fähigkeit zur Anwendung der Prinzipien einer effektiven Kommunikationsstrategie	1. Kenntnis der Anforderungen der NIS-2-Richtlinie an das Bewusstsein für Cybersicherheit in der Europäischen Union 2. Kenntnisse über Tätigkeiten und Programme zur Kompetenzentwicklung 3. Kenntnisse über die Gestaltung von Kompetenzprogrammen zur Erreichung der Unternehmensziele 4. Kenntnis des Prozesses zur Durchführung von wirksamen Programmen zur Schulung und Sensibilisierung 5. Kenntnisse über die Bewertung der Ergebnisse und der Wirksamkeit von Programmen zur Schulung und Sensibilisierung 6. Kenntnis der strategischen Kommunikation und ihrer Grundsätze: Transparenz, Angemessenheit, Glaubwürdigkeit, Reaktionsfähigkeit und Klarheit 7. Kenntnisse über wirksame Kommunikationsstrategien 8. Kenntnis der Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit und der freiwilligen Meldung relevanter Informationen gemäß der NIS-2-Richtlinie

Bereich 6: Testen und Überwachung eines Cybersicherheitsprogramms

Hauptziel: Sicherstellen, dass der Kandidat in der Lage ist, ein Cybersicherheitsprogramm im Einklang mit der NIS-2-Richtlinie wirksam zu auditieren, zu messen, zu überwachen und fortlaufend zu verbessern.

Kompetenzen	Kenntnisse
1. Fähigkeit, Cybersicherheitstests zu verstehen und zu erklären 2. Fähigkeit, die Anforderungen der NIS-2-Richtlinie in Bezug auf Sicherheitsaudits und Selbstbewertungen zu erkennen 3. Fähigkeit zur Durchführung interner Audits, zum Umgang mit Nichtkonformitäten und zum Verständnis der Audit-Grundlagen 4. Fähigkeit zur Durchführung von Selbstbewertungen anhand von Rahmenwerken wie dem ENISA Selbstbewertungsrahmen (Self-Assessment Framework) 5. Fähigkeit, Messziele zu definieren, Leistungsindikatoren festzulegen und Überwachungsmethoden zu bestimmen 6. Fähigkeit, die Rolle der CSIRTs und der zuständigen Behörden bei der Überwachung von Cyber-Bedrohungen im Sinne der NIS-2-Richtlinie zu erkennen 7. Fähigkeit zu bestimmen, was überwacht werden muss, Überwachungsergebnisse effektiv zu melden und geeignete Überwachungsmethoden auszuwählen 8. Fähigkeit, Änderungsfaktoren zu überwachen, Cybersicherheitsmaßnahmen aufrechtzuerhalten und zu verbessern und Verbesserungen zu dokumentieren	1. Kenntnisse über Testtechniken im Bereich der Cybersicherheit 2. Kenntnis der Anforderungen der NIS-2-Richtlinie in Bezug auf Selbstbewertungen und die Rolle einer solchen Bewertung bei der Sicherstellung der Einhaltung der NIS-2-Richtlinie 3. Kenntnis der internen Konformitätsbewertung und der internen Audittätigkeiten 4. Kenntnis des ENISA-Selbstbewertungsrahmens und anderer Instrumente zur Bewertung der Cybersicherheit 5. Kenntnis der Messziele, Leistungsindikatoren und Überwachungsmethoden zur Bewertung der Wirksamkeit von Cybersicherheitsprogrammen 6. Kenntnis der Anforderungen der NIS-2-Richtlinie für CSIRTs zur Überwachung und Analyse von Bedrohungen, Schwachstellen und Vorfällen auf nationaler Ebene 7. Kenntnisse über die Berichterstattung der Überwachungsergebnisse an Interessenträger und die Auswahl geeigneter Überwachungsmethoden 8. Kenntnisse über die Überwachung von Änderungsfaktoren, die Aufrechterhaltung und Verbesserung von Cybersicherheitsmaßnahmen und die Dokumentation von Verbesserungen

Auf Grundlage der oben genannten Bereiche und ihrer Relevanz wurden 80 Multiple-Choice-Fragen in die Prüfung aufgenommen, die in der folgenden Tabelle zusammengefasst sind:

				Erforderliches Verständnisniveau/ Verständnisebene (kognitiv/taxonomisch)	
		Anzahl der Fragen/Punkte pro Kompetenzbereich,	Prozentsatz der Prüfung, der jedem Kompetenzbereich gewidmet ist bzw. für jeden Kompetenzbereich Punkte erhält,	Fragen der Kompetenzebene Verständnis, Anwendung und Analyse	Fragen, die die Bewertung messen
Kompetenzbereiche	Grundlegende Konzepte und Definitionen der NIS-2-Richtlinie	10	12.5	X	
	Planung der Implementierung der Anforderungen der NIS-2-Richtlinie	20	25	X	
	Rollen und Verantwortlichkeiten im Bereich der Cybersicherheit und des Risikomanagements	15	18.75		X
	Cybersicherheitsmaßnahmen, Handhabung von Vorfällen und Krisenmanagement	15	18.75		X
	Kommunikation und Bewusstsein	10	12.5	X	
	Testen und Überwachung eines Cybersicherheitsprogramms	10	12.5		X
	Insgesamt	**80**	**100 %**		
	Anzahl der Fragen pro Verständnisebene			**40**	**40**
	Prozentualer Anteil der Fragen pro Verständnisebene (kognitiv/Taxonomie)			**50 %**	**50 %**

Für das Bestehen müssen **70 %** der Prüfung (hier 56 Fragen) richtig beantwortet werden.

Nach bestandener Prüfung können die Kandidaten mit entsprechendem Erfahrungsstand den Berechtigungsnachweis „ PECB Certified NIS 2 Directive Lead Implementer“ beantragen.

Ablegen der Prüfung

Allgemeine Informationen zur Prüfung
Die Kandidaten müssen mindestens 30 Minuten vor Beginn der Prüfung eintreffen/anwesend sein.

Kandidaten, die zu spät kommen, erhalten keine zusätzliche Zeit, um die Verspätung auszugleichen, und werden möglicherweise nicht zur Prüfung zugelassen.

Die Kandidaten müssen ein gültiges Ausweisdokument (Personalausweis, Führerschein oder Reisepass) mitbringen und ihn der Aufsichtsperson vorlegen.

Am Tag der Prüfung (schriftliche Prüfungen) kann den Kandidaten, die die Prüfung in einer Fremdsprache ablegen, auf Antrag eine zusätzliche Zeit gewährt werden, und zwar wie folgt:
- 10 zusätzliche Minuten für Foundation-Prüfungen
- 20 zusätzliche Minuten für Manager-Prüfungen
- 30 zusätzliche Minuten für Lead-Prüfungen

Format und Art der PECB-Prüfung
1. **Papierbasiert (Schriftlich auf Papier):** Die Prüfungen werden auf Papier durchgeführt, wobei die Kandidaten nichts anderes als das Prüfungspapier und einen Stift benutzen dürfen. Die Verwendung von elektronischen Geräten wie Laptops, Tablets oder Telefonen ist nicht erlaubt. Die Prüfungssitzung wird von einer von der PECB zugelassenen Aufsichtsperson an dem Ort beaufsichtigt, an dem der Partner die Schulung organisiert hat.
2. **Online:** Die Prüfungen werden elektronisch über die Anwendung PECB Exams bereitgestellt. Die Verwendung von elektronischen Geräten wie Tablets und Handys ist nicht erlaubt. Die Prüfungssitzung wird von einem Aufsichtsführenden der PECB über die Anwendung PECB Exams und eine externe/integrierte Kamera fernüberwacht.

Weiterführende Informationen zur Online-Prüfung finden Sie im PECB Online Exam Guide.

Die PECB-Prüfungen werden in zwei Varianten angeboten:
1. Prüfung mit freier Beantwortung / Freitext
2. Prüfung mit Multiple-Choice-Fragen

Diese Prüfung besteht aus Multiple-Choice-Fragen: Mithilfe der Multiple-Choice-Prüfung kann das Verständnis eines Kandidaten über sowohl einfache als auch komplexe Konzepte bewertet werden. Sie umfasst sowohl eigenständige als auch szenariobasierte Fragen. Eigenständige Fragen stehen unabhängig innerhalb der Prüfung und sind nicht kontextabhängig, wohingegen szenariobasierte Aufgaben kontextabhängig sind, d. h. sie werden auf der Grundlage eines Szenarios entwickelt, das der Kandidat lesen soll, und es wird erwartet, dass er Antworten auf fünf Fragen zu diesem Szenario gibt. Bei der Beantwortung von eigenständigen und szenariobasierten Fragen müssen die Kandidaten verschiedene Konzepte und Prinzipien anwenden, die während der Schulung erklärt wurden, Probleme analysieren, Alternativen identifizieren und bewerten, mehrere Konzepte oder Ideen kombinieren usw.

Jede Multiple-Choice-Frage hat drei Antwortmöglichkeiten, von denen nur eine die richtige Antwort ist.

Dies ist eine Prüfung mit offenen Büchern. Der Kandidat darf die folgenden Referenzmaterialien verwenden:

- Eine gedruckte Ausgabe der NIS-2-Richtlinie
- Schulungsmaterialien (Zugriff über die App PECB Exams und/oder gedruckt)
- Persönliche Notizen aus der Schulung (Zugriff über die App PECB-Exams und/oder gedruckt)
- Ein Wörterbuch in Papierform

Ein Beispiel für die Prüfungsfragen finden Sie weiter unten.

Anmerkung: Die PECB wird sukzessive zu Multiple-Choice-Prüfungen übergehen. Sie werden ebenfalls ‚Open Book' sein und szenariobasierte Fragen enthalten, die es der PECB ermöglichen, das Wissen, die Fähigkeiten und die Kompetenzen der Kandidaten zu bewerten, Informationen in neuen Situationen anzuwenden (Anwenden), Verbindungen zwischen Ideen herzustellen (Analysieren) und einen Standpunkt oder eine Entscheidung zu begründen (Bewerten).

Für weitere Informationen über Prüfungsarten, verfügbare Sprachen und andere Details wenden Sie sich bitte an examination.team@pecb.com oder gehen Sie auf die Liste der PECB-Prüfungen..

Beispiele für Prüfungsfragen

TechLink, ein multinationales Unternehmen, ist auf die Bereitstellung einer breiten Palette von Cloud-Computing-Diensten spezialisiert, die auf den Finanz- und Gesundheitssektor zugeschnitten sind. Ihre Dienstleistungen ermöglichen es Organisationen, das volle Potenzial der Cloud-Technologie zu nutzen, die digitale Transformation voranzutreiben und öffentliche Dienste weltweit zu verbessern.

TechLink ist in der Europäischen Union tätig und fällt als wesentliche Einrichtung unter den Regulierungsrahmen der NIS-2-Richtlinie. *TechLink* musste noch die notwendigen Sicherheitsvorkehrungen treffen, um seine Netzwerke und Systeme angemessen zu schützen und die Einhaltung der Richtlinie zu gewährleisten. Also wurde ein umfassendes Cybersicherheitsprogramm eingeleitet. Das Unternehmen verfolgte einen Ansatz, der es ermöglichte, hohe Produktionsstandards festzulegen, ohne bestimmte Methoden vorzuschreiben, und so effiziente und innovative Wege zur Erfüllung dieser Standards zu finden.

In Übereinstimmung mit Artikel 21 der NIS-2-Richtlinie entwickelte das Unternehmen eine Strategie für das Business Continuity Management (BCM, Aufrechterhaltung der Betriebsfähigkeit). Der Ansatz für die Entwicklung der BCM-Strategie umfasste eine vertraglich vereinbarte Wiederherstellung durch eine dritte Partei, um externe Unterstützung für die Wiederherstellung von Schlüsselprozessen zu erhalten, und eine Option zur Änderung von Schlüsselprozessen, um betriebliche Abläufe unter ressourcenbeschränkten Umständen anzupassen. Dieser Ansatz erleichterte eine flexible Reaktion auf Vorfälle, indem er ein Gleichgewicht zwischen externer Unterstützung und internen Anpassungen herstellte, um den Wiederherstellungsprozess zu beschleunigen und gleichzeitig wichtige Bedenken des Managements, wie Planungsaufwand, Implementierungskosten und vertragliche Vereinbarungen mit Drittanbietern, zu berücksichtigen.

Als Teil des Cybersicherheitsprogramms konzentrierte sich *TechLink* auf die Gewährleistung der Sicherheit von Netz- und Informationssystemen durch die Förderung einer Kultur des Risikomanagements, einschließlich Risikobeurteilungen und der Implementierung von Cybersicherheitsmaßnahmen. Gemäß der NIS-2-Richtlinie wurden diese Maßnahmen vom Leitungsorgan des Unternehmens genehmigt. Das Leitungsorgan ist mit allgemeinen Risikomanagementpraktiken gut vertraut, doch das Unternehmen hielt es für nicht erforderlich, zusätzliche Schulungen zum Risikomanagement im Bereich der Cybersicherheit durchzuführen, da eines der Mitglieder über Fachwissen im Bereich der Cybersicherheit verfügt.

TechLink sah sich vor kurzem mit einem schwerwiegenden Vorfall im Bereich der Cybersicherheit konfrontiert, bei dem ein ausgeklügelter Cyberangriff auf die kritischen Systeme des Unternehmens abzielte und eine Sicherheitslücke im Bereich der sensiblen Kundendaten entstand. Dieser Vorfall bot die Gelegenheit, den Willen des Unternehmens zu demonstrieren, die NIS-2-Richtlinie unbedingt einzuhalten. Das Unternehmen isolierte die betroffenen Systeme und dämmte das Eindringen ein, um weiteren Schaden zu verhindern. Anschließend informierte es umgehend die zuständigen Behörden, einschließlich der nationalen staatlichen Stellen, innerhalb von 24 Stunden nach der Entdeckung. Die betroffenen Kunden wurden ebenfalls über den Vorfall und die Maßnahmen zum Schutz der Daten informiert. Das Unternehmen legte einen Abschlussbericht vor, der eine detaillierte Beschreibung, die Art der Bedrohung, die angewandten und laufenden Minderungsmaßnahmen sowie die grenzüberschreitenden Auswirkungen enthielt.

Beantworten Sie auf der Grundlage des obigen Szenarios die folgenden Fragen:

1. **Welche potenziellen Strafen könnten *TechLink* im Falle der Nichteinhaltung der NIS-2-Richtlinie drohen?**
   A. 7 Mio. € oder 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes
   B. **10 Mio. € oder 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes**
   C. 5 Mio. € oder 1 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes

2. **Welche Anforderung der NIS-2-Richtlinie hat *TechLink* vernachlässigt?**
   A. **Schulung der Mitglieder des Leitungsorgans zu Praktiken des Cybersicherheitsrisikomanagements**
   B. Sicherstellen der Genehmigung von Cybersicherheitsmaßnahmen durch die Gruppe für die Resilienz kritischer Einrichtungen
   C. Schaffung eines Leitungsorgans mit fünf Mitgliedern, die über umfassende Erfahrungen im Bereich der Cybersicherheit verfügen

3. **Welchen Regulierungsansatz hat TechLink gewählt, um die NIS-2-Richtlinie einzuhalten?**
   A. Befehl und Kontrolle
   B. **Leistungsbasiert**
   C. Management-basiert

4. **Welcher Aspekt der Meldepflicht gemäß Artikel 23 der NIS-2-Richtlinie wurde angesichts der Maßnahmen, die TechLink als Reaktion auf den Cyberangriff auf seine kritischen Systeme ergriffen hat, von TechLink nicht eingehalten?**
   A. **Übermittlung eines Zwischenberichts zum Status auf Antrag**
   B. Der ENISA einen zusammenfassenden Bericht über einen bedeutenden Vorfall zukommen zu lassen
   C. Übermittlung einer öffentlichen Bekanntgabe des Vorfalls innerhalb von 48 Stunden nach seiner Entdeckung

5. **Welchen Ansatz für die Entwicklung der BCM-Strategie hat *TechLink* verwendet?**
   A. Betrieb an mehreren Standorten
   B. Backup-Vorkehrung
   C. **Kombinierte Vorkehrung**

Sicherheitsrichtlinie für Prüfungen

Die PECB ist bestrebt, die Integrität ihrer Prüfungen und des gesamten Prüfungsprozesses zu schützen, und verlässt sich auf das ethische Verhalten von Bewerbern, potenziellen Bewerbern, Kandidaten und Partnern, um die Vertraulichkeit der PECB-Prüfungen zu wahren. Diese Richtlinie zielt darauf ab, inakzeptables Verhalten zu unterbinden und eine faire Behandlung aller Kandidaten zu gewährleisten.

Jegliche Offenlegung von Informationen über den Inhalt von PECB-Prüfungen stellt einen direkten Verstoß gegen diese Richtlinie und den PECB-Ethikkodex dar. Folglich müssen Kandidaten, die an einer PECB-Prüfung teilnehmen, eine Vertraulichkeits- und Geheimhaltungsvereinbarung unterzeichnen und sich an Folgendes halten:

1. Die Fragen und Antworten des Prüfungsmaterials sind das exklusive und vertrauliche Eigentum der PECB. Sobald die Kandidaten die Prüfung bei der PECB eingereicht haben, haben sie keinen Zugriff mehr auf das Original oder eine Kopie der Prüfung.
2. Den Kandidaten ist es untersagt, Informationen über die Fragen und Antworten der Prüfung preiszugeben oder solche Details mit anderen Kandidaten oder Personen zu besprechen.
3. Den Kandidaten ist es nicht gestattet, prüfungsrelevante Materialien aus dem Prüfungsraum mitzunehmen.
4. Es ist den Kandidaten nicht gestattet, Kopien von Prüfungsmaterialien (schriftlich, fotokopiert oder anderweitig) anzufertigen oder zu versuchen, Kopien anzufertigen, einschließlich, aber nicht beschränkt auf Fragen, Antworten oder Bildschirmdarstellungen.
5. Kandidaten dürfen sich nicht an betrügerischen Prüfungsaktivitäten beteiligen oder diese fördern, wie z. B.:
    - Einsicht in das Prüfungsmaterial oder den Antwortbogen eines anderen Kandidaten
    - Hilfe von der Aufsichtsperson, einem Kandidaten oder einer anderen Person zu erhalten oder zu leisten
    - Verwendung von nicht genehmigten Leitfäden, Handbüchern, Tools usw., einschließlich der Verwendung von "Brain Dump"-Seiten, da diese von der PECB nicht genehmigt sind

Sobald sich ein Kandidat Unregelmäßigkeiten oder Verstößen gegen die oben genannten Punkte bewusst wird oder bereits ist, ist er dafür verantwortlich, diese Punkte zu befolgen. Andernfalls werden Kandidaten, wenn solche Unregelmäßigkeiten auftreten, direkt an die PECB gemeldet oder sollten sie solche Unregelmäßigkeiten sehen, sollten sie diese sofort der PECB melden.

Die Kandidaten sind allein dafür verantwortlich, die PECB-Prüfungsregeln und -richtlinien, die Vertraulichkeits- und Geheimhaltungsvereinbarung und den Ethikkodex zu verstehen und einzuhalten. Daher erhalten die Kandidaten keine Rückerstattung, wenn ein Verstoß gegen eine oder mehrere Regeln festgestellt wird. Darüber hinaus hat die PECB das Recht, je nach Schwere des Falls, den Kandidaten die Zulassung zu einer PECB-Prüfung zu verweigern oder sie zu einer Wiederholung der Prüfung aufzufordern, wenn während oder nach dem Benotungsprozess Unregelmäßigkeiten festgestellt werden.

Jeder Verstoß gegen die oben genannten Punkte fügt der PECB einen nicht wieder gutzumachenden Schaden zu, der nicht durch Geld ausgeglichen werden kann. Daher kann die PECB geeignete Maßnahmen ergreifen, um die unbefugte Weitergabe oder den Missbrauch von Prüfungsmaterialien zu unterbinden oder zu verhindern, einschließlich der Erwirkung einer sofortigen einstweiligen Verfügung.

Die PECB wird Maßnahmen gegen Personen ergreifen, die gegen die Regeln und Richtlinien verstoßen, einschließlich eines dauerhaften Ausschlusses von der Erlangung von PECB-Berechtigungsnachweisen und des Entzugs früherer Berechtigungen. Die PECB wird darüber hinaus rechtliche Schritte gegen Einzelpersonen oder Organisationen einleiten, die ihre Urheberrechte, Eigentumsrechte und ihr geistiges Eigentum verletzen.

Ergebnisse der Prüfung

Die Prüfungsergebnisse werden Ihnen per E-Mail mitgeteilt.

- Die Zeitspanne für die Benachrichtigung beginnt mit dem Prüfungstermin und beträgt drei bis acht Wochen für Prüfungen in freier Beantwortung und zwei bis vier Wochen für Multiple-Choice-Prüfungen auf Papier.
- Bei Online-Multiple-Choice-Prüfungen erhalten die Kandidaten ihre Ergebnisse sofort.

Kandidaten mit bestandener Prüfung können einen der Berechtigungsnachweise des jeweiligen Zertifizierungsprogramms beantragen.

Kandidaten, die die Prüfung nicht bestanden haben, erhalten in der E-Mail eine Liste der Bereiche mit offensichtlichen Wissenslücken, damit sie sich besser auf eine Wiederholung vorbereiten können.

Kandidaten, die mit den Ergebnissen nicht einverstanden sind, können innerhalb von 30 Tagen nach Erhalt der Ergebnisse per E-Mail an examination.team@pecb.com eine erneute Bewertung beantragen. Nach 30 Tagen eingehende Anträge auf eine Neubewertung werden nicht bearbeitet. Wenn Kandidaten mit den Ergebnissen der Neubewertung nicht einverstanden sind, haben sie ab dem Datum, an dem sie die neu bewerteten Prüfungsergebnisse erhalten haben, 30 Tage Zeit, um eine Beschwerde über das PECB-Ticketing-System einzureichen. Beschwerden, die nach Ablauf der 30 Tage eingehen, werden nicht bearbeitet.

Richtlinie für Prüfungswiederholungen

Die Anzahl der Wiederholungen einer Prüfung ist nicht begrenzt. Es gibt jedoch gewisse Einschränkungen hinsichtlich der Zeitspanne zwischen den einzelnen Prüfungswiederholungen.

Wird die Prüfung beim ersten Versuch nicht bestanden, kann die erste Wiederholungsprüfung frühestens 15 Tage nach der Erstprüfung erfolgen.

Anmerkung: Die Kandidaten, die die Schulung bei einem unserer Partner absolviert und die Erstprüfung nicht bestanden haben, sind berechtigt, die Prüfung innerhalb von 12 Monaten nach Erhalt des Gutscheincodes kostenlos zu wiederholen, da die für die Schulung gezahlte Gebühr eine Erst- und eine Wiederholungsprüfung beinhaltet. Andernfalls fallen Gebühren für die Wiederholung an.

Den Kandidaten, die die Wiederholungsprüfung nicht bestehen, empfiehlt die PECB, sich mit einer Schulung besser auf die Prüfung vorzubereiten.

Zur Vereinbarung einer Wiederholungsprüfung müssen Kandidaten mit einer absolvierten Schulung je nach Prüfungsformat:die nachstehenden Schritte befolgen:

1. Online-Prüfung: Lösen Sie bei der Planung der Wiederholungsprüfung den Coupon-Code von der Erstprüfung ein, damit Ihnen die Gebühr erlassen wird
2. Papierprüfung: Kandidaten müssen sich an den PECB-Partner/Vertriebspartner wenden, der die Erstprüfung organisiert hat, um die Wiederholungsprüfung zu vereinbaren (Datum, Uhrzeit, Ort, Kosten).

Kandidaten, die die Online-Prüfung direkt bei der PECB abgelegt haben ohne vorher eine Schulung bei einem Partner absolviert zu haben, fallen nicht unter diese Regelung. Das Verfahren zur Planung der Wiederholung der Prüfung ist dasselbe wie für die erste Prüfung.

PECB

ABSCHNITT III: ZERTIFIZIERUNGSPROZESS UND ANFORDERUNGEN

Berechtigungsnachweis PECB NIS 2 Directive

Alle PECB-Zertifizierungen haben spezifische Anforderungen hinsichtlich Ausbildung und Berufserfahrung. Um herauszufinden, welcher Berechtigungsnachweis für Sie das Richtige ist, sollten Sie Ihre beruflichen Anforderungen berücksichtigen und die Kriterien für die Zertifizierungen analysieren.

Berechtigungsnachweise im Programm PECB NIS 2 Directive haben folgende Anforderungen:

Qualifikation	Aus-/Bildung	Prüfung	Berufliche Erfahrung	MS Projekterfahrung	Andere Anforderungen
PECB Certified NIS 2 Directive Provisional Implementer	Mindestens Sekundarschulbildung	Prüfung PECB Certified NIS 2 Directive Lead Implementer oder gleichwertig	Keine	Keine	Unterzeichnung des PECB-Ethikkodexes
PECB Certified NIS 2 Directive Implementer			Zwei Jahre: Ein Jahr Berufserfahrung im Bereich Cybersicherheitsmanagement	Projekttätigkeiten: Insgesamt 200 Stunden	
PECB Certified NIS 2 Directive Lead Implementer			Fünf Jahre: Zwei Jahre Berufserfahrung im Bereich Cybersicherheitsmanagement	Projekttätigkeiten: Insgesamt 300 Stunden	
PECB Certified NIS 2 Directive Senior Lead Implementer			Zehn Jahre: Sieben Jahre Berufserfahrung im Bereich Cybersicherheitsmanagement	Projekttätigkeiten: Insgesamt 1.000 Stunden	

Anrechenbar sind solche Implementierungstätigkeiten, die den besten Praktiken im Bereich Implementierung und Management entsprechen. Dazu gehören:

1. Durchführung umfassender Risikobeurteilungen speziell für Systeme kritischer Infrastrukturen
2. Steuerung von Reaktionsplänen bei Vorfällen, die auf die Anforderungen der NIS-2-Richtlinie zugeschnitten sind
3. Umsetzung geeigneter Sicherheitsmaßnahmen und -kontrollen
4. Einführen von Metriken und Leistungsindikatoren
5. Handhabung von und Reaktion auf Cybersicherheitsvorfälle
6. Durchführung von Managementbewertungen
7. Leitung eines Cybersicherheitsteams

Beantragung der Zertifizierung

Alle Kandidaten mit bestandener PECB-Prüfung (oder ein von der PECB anerkanntes Äquivalent) sind berechtigt, die PECB-Berechtigungsnachweise zu beantragen, für die sie beurteilt wurden. Um eine PECB-Zertifizierung zu erhalten, müssen bestimmte Bildungs- und Berufsanforderungen erfüllt werden Die Kandidaten müssen das Online-Zertifizierungsantragsformular ausfüllen (das über ihr PECB-Konto aufgerufen werden kann), wozu die Kontaktdaten von Personen gehören, die die Berufserfahrung der Kandidaten bestätigen können. Die Kandidaten können ihren Antrag auf Englisch, Französisch, Deutsch, Spanisch oder Koreanisch einreichen. Sie können wählen, ob sie online oder per Rechnung bezahlen möchten. Für weitere Informationen wenden Sie sich bitte an certification.team@pecb.com.

Der Online-Antrag auf Zertifizierung ist sehr einfach und dauert nur wenige Minuten:

- Registrieren Sie Ihr Konto
- Überprüfen Sie Ihre E-Mail auf den Bestätigungslink
- Melden Sie sich an, um die Zertifizierung zu beantragen

Weitere Informationen zur Beantragung der Zertifizierung finden Sie hier.

Die Zertifizierungsabteilung prüft, ob der Kandidat alle Zertifizierungsanforderungen für den jeweiligen Berechtigungsnachweis erfüllt. Der Kandidat erhält eine E-Mail über den Status seines Antrags, einschließlich der Entscheidung über die Zertifizierung.

Nach der Genehmigung des Antrags durch die Zertifizierungsabteilung kann der Kandidat das Zertifikat herunterladen und das entsprechende digitale Abzeichen beantragen. Weitere Informationen zum Herunterladen des Zertifikats finden Sie hier, und weitere Informationen zur Beantragung des Digitalen Abzeichens finden Sie hier.

Die PECB bietet Unterstützung auf Englisch und Französisch.

Berufliche Erfahrung

Die Bewerber müssen vollständige und korrekte Angaben zu ihrer Berufserfahrung machen, einschließlich Berufsbezeichnung(en), Anfangs- und Enddatum, Tätigkeitsbeschreibung(en) und mehr. Den Bewerbern wird empfohlen, ihre früheren oder derzeitigen Aufgaben zusammenzufassen und dabei so detailliert wie möglich zu beschreiben, welche Aufgaben sie bei den einzelnen Tätigkeiten hatten. Ausführlichere Informationen können in den Lebenslauf eingefügt werden.

Berufliche Referenzen

Für jeden Antrag sind zwei berufliche Referenzen erforderlich. Sie müssen von Personen stammen, die mit dem Kandidaten in einem beruflichen Umfeld zusammengearbeitet haben und seine Erfahrung im Bereich des Cybersicherheitsmanagements sowie seinen derzeitigen und früheren beruflichen Werdegang bestätigen können. Berufliche Referenzen von Personen, die unter der Aufsicht des Bewerbers stehen oder mit ihm verwandt sind, sind nicht gültig.

Erfahrung mit Cybersicherheitsprojekten

Das Projektprotokoll des Kandidaten für den Bereich Cybersicherheit wird überprüft, um sicherzustellen, dass der Kandidat die erforderliche Anzahl von Projekttätigkeitsstunden aufweist.

Bewertung der Zertifizierungsanträge

Die Zertifizierungsabteilung prüft jeden Antrag, um festzustellen, ob der Kandidat alle Voraussetzungen für die Zertifizierung oder das Zertifikatsprogramm erfüllt hat. Ein Kandidat, dessen Antrag geprüft wird, wird schriftlich benachrichtigt und erhält, falls erforderlich, einen angemessenen Zeitrahmen, um zusätzliche Unterlagen vorzulegen. Reagiert ein Kandidat nicht bis zum Ablauf der Frist oder legt er die erforderlichen Unterlagen nicht innerhalb des vorgegebenen Zeitrahmens vor, prüft die Zertifizierungsabteilung den Antrag auf Grundlage der ursprünglich vorgelegten Informationen, was letztendlich zu einer Herabstufung auf eine niedrigere Qualifikationsstufe führen kann.

ABSCHNITT IV: ZERTIFIZIERUNGSRICHTLINIEN

Verweigerung der Zertifizierung

Die PECB kann die Zertifizierung / das Zertifikatsprogramm verweigern, wenn Kandidaten:

- Den Antrag fälschen
- Gegen die Prüfungsordnung verstoßen
- Gegen den PECB-Ethikkodex verstoßen

Kandidaten, deren Zertifizierung/Zertifikatsprogramm verweigert wurde, können eine Beschwerde im Rahmen des Beschwerde- und Berufungsverfahrens einreichen. Ausführlichere Informationen finden Sie im Abschnitt **Beschwerde- und Berufungsrichtlinie** .

Die Anmeldegebühr für die Zertifizierung / das Zertifikatsprogramm ist nicht erstattungsfähig.

Optionen für den Zertifizierungsstatus

Aktiv

Ihre Zertifizierung ist gültig und wird aufrechterhalten, indem Sie die Anforderungen der PECB bezüglich CPD und AMF erfüllen.

Ausgesetzt

Die PECB kann die Zertifizierung von Kandidaten vorübergehend aussetzen, wenn diese die Anforderungen nicht erfüllen. Andere Gründe für die Aussetzung der Zertifizierung sind unter anderem:

- Die PECB erhält zahlreiche oder schwerwiegende Beschwerden von interessierten Parteien (die Aussetzung erfolgt, bis die Untersuchung abgeschlossen ist).
- Die Logos der PECB oder der Akkreditierungsstellen werden vorsätzlich missbraucht.
- Der Kandidat es versäumt, den Missbrauch einer Zertifizierungsmarke innerhalb der von der PECB festgelegten Zeit zu korrigieren.
- Die zertifizierte Person hat von sich aus eine Aussetzung beantragt.
- Die PECB hält andere Bedingungen für die Aussetzung der Zertifizierung für angemessen.

Entzogen

Die PECB kann die Zertifizierung entziehen (d. h. zurückziehen), wenn der Kandidat die Anforderungen der PECB nicht erfüllt. In solchen Fällen dürfen sich die Kandidaten nicht mehr als PECB zertifizierte Fachleute ausgeben. Weitere Gründe für den Entzug der Zertifizierung können sein, wenn die Kandidaten:

- Gegen den PECB-Ethikkodex verstoßen
- Den Umfang der Zertifizierung falsch darstellen und falsche Angaben machen
- Gegen andere PECB-Regeln verstoßen
- Sonstige Gründe, die die PECB für angemessen hält

Kandidaten, denen die Zertifizierung entzogen wurde, können im Rahmen des Beschwerde- und Berufungsverfahrens eine Beschwerde einreichen. Ausführlichere Informationen finden Sie im Abschnitt **Beschwerde- und Berufungsrichtlinie** .

Andere Statusarten
Neben der aktiven, ausgesetzten oder entzogenen Zertifizierung kann eine Zertifizierung auch freiwillig zurückgezogen werden oder den Emeritus-Status bekommen. Weitere Informationen über diese Status und den Status der dauerhaften Beendigung finden Sie unter Optionen für den Zertifizierungsstatus.

Hoch- und Herabstufung von Berechtigungsnachweisen

Hochstufung von Berechtigungsnachweisen
Fachleute können ihre Berechtigungsnachweise hochstufen lassen, sobald sie nachweisen können, dass sie die Anforderungen erfüllen.

Um eine Hochstufung zu beantragen, müssen sich die Kandidaten in ihr PECB-Konto einloggen, die Registerkarte "My Certifications" besuchen und auf "Upgrade" klicken. Die Gebühr für den Antrag auf Hochstufung beträgt $100.

Herabstufung von Berechtigungsnachweisen
Eine PECB-Zertifizierung kann aus den folgenden Gründen auf ein niedrigeres Berechtigungsnachweisniveau herabgestuft werden:

- Die Zahlung der AMF ist nicht erfolgt.
- Die Fortbildungsstunden (CPD) sind nicht eingereicht worden.
- Es wurden nicht genügend Fortbildungsstunden (CPD) eingereicht.
- Der Nachweis über die Fortbildungsstunden wurde auf Anfrage nicht erbracht.

Anmerkung: *Bei PECB-zertifizierten Fachkräften mit einer Lead-Zertifizierung, die die Erfüllung der Anforderungen für die Aufrechterhaltung der Zertifizierung nicht nachweisen können, wird der Berechtigungsnachweis herabgestuft. Inhabern von Master-Zertifizierungen, die es versäumen, CPDs einzureichen und AMFs zu zahlen, wird ihre Zertifizierung entzogen.*

Erneuerung der Zertifizierung

PECB-Zertifizierungen sind drei Jahre gültig. Um sie aufrechtzuerhalten, müssen die von der PECB zertifizierten Fachleute die mit der jeweiligen Berechtigung verbundenen Anforderungen erfüllen, z. B. die erforderliche Anzahl von Stunden für die kontinuierliche berufliche Weiterentwicklung (CPD). Darüber hinaus müssen sie die jährliche Aufrechterhaltungsgebühr (AMF, 120 $) bezahlen. Weitere Informationen finden Sie auf der Seite zur Aufrechterhaltung der Zertifizierung auf der PECB-Website.

Schließung eines Falles

Wenn die Kandidaten innerhalb eines Jahres keinen Antrag auf Zertifizierung stellen, wird ihr Fall geschlossen. Auch nach Ablauf des Zertifizierungszeitraums haben die Kandidaten das Recht, ihren Fall wieder zu öffnen. Allerdings ist die PECB dann nicht mehr für Änderungen bezüglich der Bedingungen, Standards, Richtlinien und des Kandidatenhandbuchs verantwortlich, die vor der Schließung des Falls galten. Kandidaten, die eine Wiederaufnahme ihres Falls beantragen, müssen dies schriftlich unter certification.team@pecb.com tun und die erforderliche Gebühr entrichten

Beschwerde- und Berufungsrichtlinie

Alle Beschwerden müssen innerhalb von 30 Tagen nach Erhalt der Zertifizierungsentscheidung eingereicht werden. Die PECB wird dem Kandidaten innerhalb von 30 Arbeitstagen nach Erhalt der Beschwerde eine schriftliche Antwort zukommen lassen. Ist die Antwort nicht zufriedenstellend, haben die Kandidaten das Recht, Einspruch einzulegen.

Weitere Informationen über die Beschwerde- und Berufungsrichtlinie finden Sie hier.

ABSCHNITT V: ALLGEMEINE RICHTLINIEN

Prüfungen und Zertifizierungen von anderen akkreditierten Zertifizierungsstellen

Die PECB akzeptiert Zertifizierungen und Prüfungen von anderen anerkannten akkreditierten Zertifizierungsorganisationen. PECB prüft die Anträge im Rahmen ihres Äquivalenzverfahrens, um zu entscheiden, ob die jeweilige(n) Zertifizierung(en) oder Prüfung(en) als gleichwertig zur jeweiligen PECB-Zertifizierung (z. B. ISO/IEC 27001 Lead Implementer) anerkannt werden können.

Nichtdiskriminierung und besondere Vorkehrungen

Alle Anträge der Kandidaten werden objektiv bewertet, unabhängig von deren Alter, Geschlecht, Rasse, Religion, Nationalität oder Familienstand.

Um die Chancengleichheit für alle qualifizierten Personen zu gewährleisten, wird die PECB gegebenenfalls angemessene Vorkehrungen[3] für die Kandidaten treffen. Wenn Kandidaten aufgrund einer Behinderung oder einer bestimmten körperlichen Verfassung besondere Vorkehrungen benötigen, sollten sie den Partner/Vertriebspartner darüber informieren, damit dieser entsprechende Vorkehrungen[4] treffen kann. Alle von den Kandidaten gemachten Angaben zu ihren Behinderungen / besonderen Bedürfnissen werden streng vertraulich behandelt. Um das Formular für Kandidaten mit Behinderungen herunterzuladen, klicken Sie hier.

Verhaltensrichtlinie

Die PECB ist bestrebt, qualitativ hochwertige, konsistente und barrierefrei zugängliche Dienstleistungen zum Nutzen ihrer externen Interessengruppen zu erbringen: Vertriebspartner, Partner, Ausbilder, Aufsichtspersonen, Prüfer, Mitglieder verschiedener Ausschüsse und Beiräte und Kunden (Auszubildende, Prüflinge, zertifizierte Personen und Zertifikatsinhaber) sowie ein positives Arbeitsumfeld zu schaffen und aufrechtzuerhalten, das die Sicherheit und das Wohlbefinden ihrer Mitarbeiter gewährleistet und die Würde, den Respekt und die Menschenrechte ihrer Mitarbeiter achtet.

Mit dieser Richtlinie soll sichergestellt werden, dass die PECB mit inakzeptablem Verhalten externer Interessenträger gegenüber PECB-Personal auf unparteiische, vertrauliche, faire und zeitnahe Weise umgeht. Um die Verhaltensrichtlinie zu lesen, klicken Sie hier.

Erstattungsrichtlinie

Die PECB erstattet Ihnen die geleisteten Zahlungen, wenn die Anforderungen der Erstattungsrichtlinie erfüllt sind. Um die Erstattungsrichtlinie zu lesen, klicken Sie hier.

---

[3] Gemäß ADA kann der Begriff „angemessene Vorkehrungen" Folgendes umfassen: (A) die Bereitstellung von Einrichtungen, die von Mitarbeitern genutzt werden, die für Menschen mit Behinderungen leicht zugänglich und nutzbar sind, und (B) die Umstrukturierung von Arbeitsplätzen, Teilzeitarbeit oder geänderte Arbeitszeiten, die Zuweisung einer freien Stelle, der Erwerb oder die Änderung von Ausstattung oder Geräten, die angemessene Anpassung oder Änderung von Prüfungen, Schulungsmaterialien oder -richtlinien, die Bereitstellung von qualifizierten Lesern oder Dolmetschern und andere ähnliche Vorkehrungen für Menschen mit Behinderungen.

[4] ADA Amendments Act von 2008 (P.L. 110- 325) Abs. 12189. Prüfungen und Schulungen. [Abschnitt 309]: Jede Person, die Prüfungen oder Schulungen im Zusammenhang mit Bewerbungen, Lizenzen, Zertifizierungen oder Berechtigungsnachweisen für sekundäre oder tertiäre Bildungs-, Berufs- oder Handelszwecke anbietet, muss diese Prüfungen oder Schulungen an einem Ort und auf eine Weise anbieten, die für Menschen mit Behinderungen zugänglich sind, oder alternative, zugängliche Vorkehrungen für diese Personen anbieten.

Adresse:

Hauptsitz
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
CANADA

Tel./Fax:

T: +1-844-426-7322
F: +1-844-329-7322

E-Mail:

Prüfung:
examination.team@pecb.com

Zertifizierung:
certification.team@pecb.com

Kundenbetreuung:
support@pecb.com

PECB-Hilfe-Center

Besuchen Sie unser Help Center, um häufig gestellte Fragen (FAQ) zu durchsuchen, Anleitungen zur Nutzung der PECB-Website und -Anwendungen einzusehen, Dokumente zu den PECB-Prozessen zu lesen oder uns über das Online-Tracking-System des Support Centers zu kontaktieren.

www.pecb.com