PECB BEYOND RECOGNITION

Handbuch für Kandidatinnen

ISO/IEC 27005 RISK MANAGER

PECB

Inhaltsverzeichnis

ABSCHNITT I: EINFÜHRUNG

Über PECB

Die PECB ist eine Zertifizierungsstelle, die Ausbildung[1] und Zertifizierung nach ISO/IEC 17024 für Personen in einer Vielzahl von Disziplinen anbietet.

Wir helfen dem Fachpersonal, sein Engagement und seine Kompetenz nachzuweisen, indem wir ihm wertvolle Bewertungs- und Zertifizierungsdienste nach international anerkannten Normen anbieten. Unser Ziel ist es, Dienstleistungen zu erbringen, die Vertrauen schaffen und fortlaufende Verbesserung fördern, Anerkennung ausdrücken und der Gesellschaft als Ganzes zugute kommen.

Die wichtigsten Ziele der PECB sind:

1. Festlegung der für die Zertifizierung von Fachpersonal erforderlichen Mindestanforderungen
2. Überprüfung und Verifizierung der Qualifikationen von Antragstellern, um sicherzustellen, dass sie die Anforderungen für die Zulassung zum Zertifizierungsprozess erfüllen
3. Entwicklung und Pflege von zuverlässigen Zertifizierungsbewertungen
4. Erteilung von Zertifizierungen an qualifizierte Kandidatinnen und Kandidaten, Führung von Aufzeichnungen und Veröffentlichung eines Verzeichnisses aller Inhaber einer gültigen Zertifizierung
5. Festlegung von Anforderungen für die regelmäßige Erneuerung der Zertifizierung und Gewährleistung der Einhaltung dieser Anforderungen
6. Sicherstellung, dass die Kandidatinnen und Kandidaten in ihrer beruflichen Praxis ethische Standards einhalten
7. Die Vertretung ihrer Mitglieder in Angelegenheiten von gemeinsamem Interesse, soweit erforderlich
8. Bewerben der Vorteile einer Zertifizierung gegenüber Organisationen, Arbeitgebern, öffentlichen Stellen, Fachleuten aus verwandten Bereichen und der Öffentlichkeit

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

Der Wert einer PECB-Zertifizierung

Was spricht für die PECB als Ihre Zertifizierungsstelle?

Globale Anerkennung

Unsere Zertifizierungen sind international anerkannt und durch den International Accreditation Service (IAS) akkreditiert. Dieser ist Unterzeichner des IAF Multilateral Recognition Arrangement (MLA), das die gegenseitige Anerkennung akkreditierter Zertifizierungen zwischen den Unterzeichnern des MLA und die Anerkennung akkreditierter Zertifizierungen auf vielen Märkten gewährleistet. Daher wird Fachpersonal, das eine PECB-Zertifizierung anstrebt, von der Anerkennung der PECB auf dem nationalen und internationalen Markt profitieren.

Kompetentes Personal

Das Team der PECB besteht aus kompetenten Personen, die über einschlägige branchenspezifische Erfahrungen verfügen.
Alle unsere Beschäftigten verfügen über berufliche Qualifikationen und werden ständig geschult, um unseren Kunden mehr als zufriedenstellende Dienstleistungen zu bieten.

Einhaltung von Normen

Unsere Zertifizierungen sind ein Nachweis für die Einhaltung der ISO/IEC 17024. Sie gewährleisten, dass die normativen Anforderungen mit der angemessenen Konsistenz, Professionalität und Unparteilichkeit erfüllt und validiert wurden.

Kundenbetreuung

Wir sind ein kundenorientiertes Unternehmen und behandeln alle unsere Kunden mit Wertschätzung, Respekt, Professionalität und Ehrlichkeit. Die PECB verfügt über ein Expertenteam, das sich um die Anfragen, Probleme, Sorgen, Bedürfnisse und Meinungen unserer Kunden kümmert. Wir bemühen uns, eine maximale Reaktionszeit von 24 Stunden einzuhalten, ohne Abstriche bei der Qualität des Services.

PECB-Ethikkodex

PECB-Fachkräfte:

1. verhalten sich professionell, mit Ehrlichkeit, Genauigkeit, Fairness, Verantwortung und Unabhängigkeit
2. handeln jederzeit ausschließlich im besten Interesse ihres Arbeitgebers, ihrer Kunden, der Öffentlichkeit und des Berufsstandes, indem sie beim Anbieten professioneller Dienstleistungen die beruflichen Standards und einschlägigen Techniken einhalten
3. erhalten die Kompetenz in ihrem jeweiligen Fachgebiet aufrecht und sind bestrebt, ihre beruflichen Fähigkeiten fortlaufend zu verbessern
4. bieten nur professionelle Dienstleistungen an, für deren Erbringung sie qualifiziert sind, und informieren die Kunden angemessen über die Art der angebotenen Dienstleistung, einschließlich aller relevanten Bedenken oder Risiken
5. informieren jeden Arbeitgeber oder Kunden über alle geschäftlichen Interessen oder Verbindungen, die ihr Urteilsvermögen beeinflussen oder ihre Fairness beeinträchtigen könnten
6. behandeln Informationen vertraulich und privat, die sie im Rahmen des beruflichen und geschäftlichen Umgangs mit derzeitigen oder früheren Arbeitgebern oder Kunden erhalten haben
7. halten stets alle Gesetze und Vorschriften der Länder ein, in denen sie ihre berufliche Tätigkeit ausüben
8. respektieren das geistige Eigentum und die Beiträge anderer
9. geben weder absichtlich noch auf andere Weise falsche oder verfälschte Informationen weiter, die die Integrität des Bewertungsprozesses eines Kandidaten für eine berufliche Bestimmung beeinträchtigen könnten
10. handeln in keiner Weise, die das Ansehen der PECB oder ihrer Zertifizierungsprogramme beeinträchtigen könnte
11. kooperieren uneingeschränkt bei der Untersuchung eines möglichen Verstoßes gegen diesen Ethikkodex

Die vollständige Version des PECB-Ethikkodexes kann hier. heruntergeladen werden.

Überblick ISO/IEC 27005 Risk Manager

Die ISO/IEC 27005 ist eine internationale Norm, die einen Leitfaden zur Handhabung von Informationssicherheitsrisiken bereitstellt und die in ISO/IEC 27001 festgelegten allgemeinen Konzepte der Informationssicherheit unterstützt. Die Prozesse zur Handhabung von Informationssicherheitsrisiken ermöglichen es Organisationen, Risiken im Zusammenhang mit der Nutzung von Informationstechnologie zu identifizieren, zu analysieren und zu behandeln.

Da der Cyberspace zunehmend gefährlicher wird, ist der Schutz vor Bedrohungen im Bereich der Informationssicherheit für die meisten Unternehmen unerlässlich geworden. Ein zentraler Bestandteil der Informationssicherheit ist das Risikomanagement. Eine der meistgefragten Kompetenzen auf dem Markt ist daher die Fähigkeit, einen systematischen Ansatz für die Handhabung von Informationssicherheitsrisiken festzulegen und umzusetzen.

Der Berechtigungsnachweis „ISO/IEC 27005 Risk Manager“ ist eine berufliche Zertifizierung für das Fachpersonal im Bereich der Informationssicherheit, das seine Kompetenz für die wirksame Handhabung von Informationssicherheitsrisiken nachweisen möchte. Eine international anerkannte Zertifizierung ist von großem Wert für Ihre Karriere und wird Ihnen helfen, Ihre beruflichen Ziele zu erreichen.

Es ist wichtig zu verstehen, dass PECB-Zertifizierungen keine Lizenz oder eine Mitgliedschaft sind. Sie stehen für die Anerkennung durch Gleichrangige und weisen nach, dass eine Person eine Reihe von Kompetenzen beherrscht und verstanden hat. PECB-Zertifizierungen werden an Kandidatinnen und Kandidaten vergeben, die ihre Erfahrung nachweisen können und eine standardisierte Prüfung im Zertifizierungsbereich bestanden haben.

Dieses Dokument legt das Zertifizierungsprogramm PECB ISO/IEC 27005 Risk Manager in Übereinstimmung mit ISO/IEC 17024:2012 fest. Dieses Handbuch für Kandidatinnen und Kandidaten enthält ebenfalls Informationen über den Prozess für den Erwerb und die Aufrechterhaltung der Berechtigungsnachweise. Es ist sehr wichtig, dass Sie alle in diesem Kandidatenhandbuch enthaltenen Informationen lesen, bevor Sie Ihren Antrag ausfüllen und einreichen. Sollten Sie nach dem Lesen noch Fragen haben, wenden Sie sich bitte an das internationale Büro der PECB unter certification.team@pecb.com.

ABSCHNITT II: PECB-ZERTIFIZIERUNGSPROZESS UND PRÜFUNGSVORBEREITUNG, REGELN UND RICHTLINIEN

Welche Zertifizierung ist die richtige für Sie

Jede PECB-Zertifizierung weist bestimmte Anforderungen an die Ausbildung und berufliche Erfahrung auf. Um die für Sie geeignete Qualifikation zu finden, gleichen Sie am besten die Zulassungskriterien für die verschiedenen Zertifizierungen mit Ihren beruflichen Erfordernissen ab.

Vorbereiten und Planen der Prüfung

Alle Kandidatinnen und Kandidaten sind für ihren Lernfortschritt und ihre Vorbereitung auf die Zertifizierungsprüfungen selbst verantwortlich. Im Rahmen des Zertifizierungsprozesses sind keine bestimmten Schulungsreihen oder Studienpläne erforderlich. Nichtsdestotrotz kann die Teilnahme an einer Schulung die Chancen der Kandidatinnen und Kandidaten deutlich erhöhen, eine PECB-Prüfung zu bestehen.

Für die Planung einer Prüfung gibt es zwei Möglichkeiten:

1. Sie setzen sich mit einem unserer Partner in Verbindung, der Schulungen und Prüfungstermine anbietet. Einen Anbieter von Schulungen in einer bestimmten Region können die Kandidatinnen und Kandidaten oft unter Active Partners finden. Der Zeitplan für die PECB-Schulungen ist ebenfalls unter Training Events verfügbar.
2. Sie legen die PECB-Prüfung mit der Prüfungs-App PECB Exam zu Hause oder an sonst einem Ort ab. Die Prüfungsveranstaltungen finden Sie hier: Exam Events.

Weitere Informationen über Prüfungen, Kompetenzbereiche und geforderte Kenntnisse finden Sie in *Abschnitt III* dieses Dokuments.

Anmeldegebühren für Prüfung und Zertifizierung

Die PECB bietet Direktprüfungen an, bei denen Kandidatinnen und Kandidaten die Prüfung ohne vorherige Schulung ablegen können. Die Preise hierfür sind wie folgt:

- Lead-Prüfung: 1000$
- Manager-Prüfung: 700$
- Foundation- und Transition Prüfung: 500$

Die Antragsgebühr für die Zertifizierung beträgt $500.

Für alle Kandidatinnen oder Kandidaten, die bei einem der PECB-Partner die Schulung absolviert und die Prüfung abgelegt haben, beinhaltet die Antragsgebühr die Kosten für die Prüfung, den Antrag auf Zertifizierung und die jährliche Aufrechterhaltungsgebühr (AMF) für das erste Jahr.

Kompetenzbereiche

Mit der Prüfung **„PECB Certified ISO/IEC 27005 Risk Manager“** soll sichergestellt werden, dass die erforderlichen Kompetenzen für die Einrichtung, Umsetzung und Steuerung eines Programm zur Handhabung von Informationssicherheitsrisiken vorhanden sind.

Die Zertifizierung zum ISO/IEC 27005 Risk Manager ist für folgenden Personenkreis gedacht:

- Führungskräfte oder Berater/innen, die für Informationssicherheit in einer Organisation verantwortlich oder daran beteiligt sind
- Personen, die für die Handhabung von Informationssicherheitsrisiken verantwortlich sind
- Mitglieder von Informationssicherheitsteams, IT-Fachpersonal und Datenschutzbeauftragte
- Personen, die für die fortlaufende Konformität mit den Anforderungen der ISO/IEC 27001 an die Informationssicherheit in einer Organisation verantwortlich sind
- Projektleiter/innen, Berater/innen oder Fachberater/innen, die die Handhabung von Informationssicherheitsrisiken beherrschen wollen

Die Prüfung deckt die folgenden Kompetenzbereiche ab:

- **Bereich 1:** Grundlegende Prinzipien und Konzepte der Handhabung von Informationssicherheitsrisiken
- **Bereich 2**: Umsetzung eines Programms zur Handhabung von Informationssicherheitsrisiken
- **Bereich 3:** Rahmenwerk und Prozesse für das Informationssicherheitsrisikomanagement auf der Grundlage von ISO/IEC 27005
- **Bereich 4:** Andere Methoden zur Beurteilung von Informationssicherheitsrisiken

PECB

Bereich 1: Grundlegende Prinzipien und Konzepte der Handhabung von Informationssicherheitsrisiken

Hauptziel: Die Kandidatinnen und Kandidaten verstehen die wichtigsten Grundsätze und Konzepte des Informationssicherheitsrisikomanagements können diese interpretieren.

Kompetenzen	Geforderte Kenntnisse
1. Kann den Aufbau der ISO/IEC 27005 verstehen und erklären	1. Kenntnisse über die wichtigsten Konzepte und die Terminologie von ISO/IEC 27005
2. Kann die Beziehung zwischen ISO/IEC 27005 und anderen Rahmenwerken für das Risikomanagement verstehen	2. Kenntnisse über die wichtigsten Normen der ISO/IEC 27000-Familie
3. Kann den Zweck des Risikomanagements und die Vorteile von ISO/IEC 27005 beschreiben	3. Kenntnisse über internationale und branchenspezifische Normen und Rahmenwerke für Informationssicherheit und Risikomanagement
4. Kann das Konzept der Informationssicherheit verstehen und erläutern	4. Kenntnisse über die Informationssicherheitsrisiken, wie sie in ISO/IEC 27005 definiert sind
5. Kann die Grundsätze der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – verstehen	5. Kenntnisse über die Definition von Schwachstellen
6. Kann die Definition von Risiko verstehen und interpretieren	6. Kenntnisse über die Unterschiede zwischen den Konzepten von Risiken und Chancen
7. Kann die wichtigsten Konzepte und Grundsätze des Risikomanagements verstehen	7. Kenntnisse über die Definition von Bedrohungen
8. Kann Schwachstellen und Bedrohungen im Bereich der Informationssicherheit verstehen	8. Kenntnisse über die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
9. Kann die Konzepte von Ereignis, Chance, Folge und Wahrscheinlichkeit erläutern	9. Kenntnisse über die Art und Funktion von Sicherheitsmaßnahmen
10. Kann die Klassifizierung von Sicherheitsmaßnahmen nach Art und Funktion verstehen	10. Kenntnisse über die Grundsätze des Risikomanagements
11. Kann die Rolle des Risikoeigentümers verstehen	11. Kenntnisse über die Rollen und Verantwortlichkeiten des Risikoeigentümers
	12. Kenntnisse über die Vorteile des Risikomanagements

PECB

Bereich 2: Umsetzung eines Programms zur Handhabung von Informationssicherheitsrisiken

Hauptziel: Die Kandidatinnen und Kandidaten verstehen die Umsetzung eines Risikomanagementprogramms auf der Grundlage der ISO/IEC 27005 und können dies initiieren.

Kompetenzen	Geforderte Kenntnisse
1. Kann die Integration des PDCA-Zyklus in das Programm zur Handhabung von Informationssicherheitsrisiken verstehen 2. Kann die wichtigsten Schritte verstehen und erläutern, die für die Einführung und Umsetzung eines Programms zur Handhabung von Informationssicherheitsrisiken erforderlich sind 3. Kann die Rollen und Verantwortlichkeiten der wichtigsten Interessenträger während und nach der Umsetzung und dem Betrieb eines Programms zur Handhabung von Informationssicherheitsrisiken identifizieren 4. Kann das Konzept der Risikobeurteilung verstehen 5. Kann die Bedeutung einer Risikomanagementpolitik verstehen 6. Kann die für die Implementierung eines Risikomanagementprogramms erforderlichen Ressourcen identifizieren 7. Kann den internen und externen Kontext einer Organisation analysieren und verstehen 8. Kann die wichtigsten Prozesse und Aktivitäten einer Organisation verstehen 9. Kann Ziele für das Risikomanagementprogramm verstehen und festlegen 10. Kann Kriterien für Informationssicherheitsrisiken, einschließlich Risikoakzeptanzkriterien und Kriterien für die Durchführung von Risikobeurteilungen der Informationssicherheit, festlegen und pflegen 11. Kann den Anwendungsbereich des Prozesses zur Handhabung von Informationssicherheitsrisiken definieren und begründen und diesen an die Ziele der Organisation anpassen	1. Kenntnisse über den Risikomanagementprozess 2. Kenntnisse darüber, wie die oberste Leitung Führung und Verpflichtung in Bezug auf das Risikomanagement nachweisen kann 3. Kenntnisse über die Rollen und Verantwortlichkeiten eines Risikomanagers im Rahmen des Risikomanagementprogramms 4. Kenntnisse über die Rollen und Verantwortlichkeiten der wichtigsten Interessenträger bei der Umsetzung eines Risikomanagementprogramms 5. Kenntnisse darüber, was typischerweise den internen und externen Kontext einer Organisation ausmacht 6. Kenntnisse über die Bedeutung des Verstehens von Schlüsselprozessen und -aktivitäten einer Organisation im Risikomanagement 7. Kenntnisse über die Ziele der Risikobeurteilung und die Erzielung spezifischer Ergebnisse 8. Kenntnisse darüber, wie Kriterien zur Akzeptanz und Beurteilung von Informationssicherheitsrisiken festgelegt werden 9. Kenntnisse über die Zyklen des Informationssicherheitsrisikomanagements 10. Kenntnisse über die Anwendbarkeit quantitativer und qualitativer Analysen bei der Festlegung von Risikoakzeptanzkriterien 11. Kenntnisse über die für das Informationssicherheitsrisikomanagement erforderlichen Ressourcen 12. Kenntnisse über den Anwendungsbereich und die Grenzen des Informationssicherheitsrisikomanagements

12. Kann eine geeignete Methode für das Management von Informationssicherheitsrisiken definieren	13. Kenntnisse über die für die Informationssicherheitsrisikobeurteilung verwendeten Ansätze und Methodiken 14. Kenntnisse über die wichtigsten Schritte zur Planung von Aktivitäten zur Risikobeurteilung

Bereich 3: Rahmenwerk und Prozesse für das Informationssicherheitsrisikomanagement auf der Grundlage von ISO/IEC 27005

Hauptziel: Die Kandidatinnen und Kandidaten können Informationssicherheitsrisiken auf der Grundlage von ISO/IEC 27005 identifizieren, analysieren, bewerten, behandeln, kommunizieren, aufzeichnen und fortlaufend überwachen.

Kompetenzen	Geforderte Kenntnisse
1. Kann die Prozesse der Identifizierung, Analyse und Bewertung von Informationssicherheitsrisiken verstehen 2. Kann den Ansatz zur Risikoidentifizierung bestimmen und Techniken zur Informationsgewinnung verstehen und interpretieren 3. Kann Werte, Bedrohungen, bestehende Maßnahmen, Schwachstellen, mögliche Folgen und Risikoeigentümer identifizieren 4. Kann Methodiken der Risikoanalyse verstehen und interpretieren 5. Kann die Abschätzung von Folgen verstehen und durchführen 6. Kann das Risikoniveau anhand von Risikobewertungskriterien bestimmen 7. Kann die Risikopriorisierung verstehen 8. Kann, den Prozess und die Optionen der Risikobehandlung auf der Grundlage von ISO/IEC 27005 verstehen 9. Kann geeignete Maßnahmen zur Minderung, Beibehaltung, Vermeidung oder Teilung von Risiken auswählen 10. Kann Kriterien zur Risikoakzeptanz im Bereich der Informationssicherheit verstehen und erläutern 11. Kann den Umgang mit Restrisiken verstehen 12. Kann das Konzept der Risikokommunikation und -absprache verstehen und interpretieren 13. Kann die Grundsätze einer wirksamen Kommunikation verstehen und interpretieren 14. Kann interne und externe Kommunikation verstehen und festlegen 15. Kann Ziele und Aktivitäten der Kommunikation verstehen 16. Kann Ansätze und Instrumente der Kommunikation verstehen	1. Kenntnisse über die Prozesse der Risikobeurteilung der Informationssicherheit, einschließlich Risikoidentifizierung, -analyse und -bewertung 2. Kenntnisse über die Ansätze zur Durchführung einer Risikoidentifizierung im Bereich der Informationssicherheit 3. Kenntnisse über die Techniken der Informationsgewinnung 4. Kenntnisse über die Definition eines Vermögenswerts und die Identifizierung von primären und unterstützenden Vermögenswerten 5. Kenntnisse über die Identifizierung und Klassifizierung von Schwachstellen, Bedrohungen und bestehenden Maßnahmen 6. Kenntnisse über die Identifizierung potenzieller Folgen, die sich auf die Verfügbarkeit, Vertraulichkeit und Integrität auswirken könnten 7. Kenntnisse über die Techniken der Risikoanalyse 8. Kenntnisse darüber, wie Folgen und Wahrscheinlichkeit beurteilt und das Risikoniveau bestimmt werden sollte 9. Kenntnisse über die Bewertung der Risikoniveaus anhand von Risikobewertungskriterien 10. Kenntnisse über die Priorisierung von Risiken 11. Kenntnisse über den Prozess und die Optionen der Risikobehandlung, einschließlich Risikoänderung, Risikobeibehaltung, Risikovermeidung und Risikoteilung 12. Kenntnisse über die Ausarbeitung und Genehmigung eines Plans für die Risikobehandlung

17. Kann Prozesse zur Handhabung von Informationssicherheitsrisiken dokumentieren 18. Kann die Ergebnisse der Risikobeurteilung und Risikobehandlung aufzeichnen und berichten 19. Kann die Wirksamkeit eines Programms zur Handhabung von Informationssicherheitsrisiken überwachen und überprüfen 20. Kann das Konzept der fortlaufenden Verbesserung und dessen Vorteile für das Risikomanagement verstehen 21. Kann eine Organisation beraten, wie sie die Wirksamkeit und Effizienz eines Programms zur Handhabung von Informationssicherheitsrisiken fortlaufend verbessern kann	13. Kenntnisse darüber, wie Restrisiken bewertet und akzeptiert werden 14. Kenntnisse über den Prozess der Kommunikation von Informationssicherheitsrisiken 15. Kenntnisse über die Grundsätze einer effizienten Kommunikationsstrategie 16. Kenntnisse darüber, wie die interne und externe Kommunikation gestaltet werden sollte 17. Kenntnisse über Ansätze und Instrumente der Kommunikation 18. Kenntnisse über dokumentierte Information und die Bedeutung der Aufzeichnung von Risiken 19. Kenntnisse über die Dokumentation der Ergebnisse des Risikomanagements 20. Kenntnisse über die wichtigsten Konzepte im Zusammenhang mit der fortlaufenden Verbesserung 21. Kenntnisse über die Prozesse, die fortlaufend überwacht und überprüft werden müssen

PECB

Bereich 4: Andere Methoden zur Beurteilung von Informationssicherheitsrisiken **Hauptziel:** Die Kandidatinnen und Kandidaten können Methodiken und Rahmenwerke zur Risikobeurteilung wie OCTAVE, MEHARI, EBIOS, NIST, Harmonized TRA und CRAMM anwenden.	
Kompetenzen	**Geforderte Kenntnisse**
1. Kann OCTAVE-Methodiken verstehen und interpretieren: OCTAVE method, OCTAVE-S, OCTAVE Allegro und OCTAVE FORTE 2. Kann eine Informationssicherheitsrisikobeurteilung auf Grundlage der Methode OCTAVE Allegro durchführen 3. Kann Risiken auf Grundlage der Methode MEHARI analysieren und handhaben 4. Kann die Methode EBIOS zur Durchführung von Risikobeurteilungen verstehen und anwenden 5. Kann NIST-Veröffentlichungen für das Risikomanagement identifizieren 6. Kann das NIST Risk Management Framework verstehen, interpretieren und für die Handhabung von Informationssicherheitsrisiken einsetzen 7. Kann die CRAMM-Methodik für das Risikomanagement verstehen und interpretieren 8. Kann die Verwendung der Methode Harmonized Threat and Risk Assessment (TRA) für die Durchführung von Risikobeurteilungen verstehen und erläutern	1. Kenntnisse über die drei Phasen von OCTAVE method 2. Kenntnisse über die Phasen von OCTAVE-S zur Durchführung der Risikobeurteilung 3. Kenntnisse darüber, wie die Phasen von OCTAVE Allegro für die Durchführung einer Informationssicherheitsrisikobeurteilung genutzt werden können 4. Kenntnisse über die Schritte von OCTAVE-FORTE für das Risikomanagement 5. Kenntnisse über die drei Hauptphasen von MEHARI für das Risikomanagement 6. Kenntnisse darüber, wie Informationssicherheitsrisiken mit MEHARI identifiziert, abgeschätzt, bewertet und behandelt werden können 7. Kenntnisse über die Methodik von EBIOS zur Risikobeurteilung und der fünf Workshops und Module 8. Kenntnisse über die NIST-Veröffentlichungen zum Risikomanagement 9. Kenntnisse über die sieben Schritte des NIST Risk Management Framework 10. Kenntnisse über die Methodik und Instrumente von CRAMM für die Analyse und Handhabung von Risiken 11. Kenntnisse über die fünf Phasen der Methodik Harmonized Threat and Risk Assessment (TRA)

Die Prüfung besteht aus 60 Fragen, die aus den oben aufgeführten Bereichen anhand ihrer Relevanz ausgewählt wurden. Die Zusammensetzung ist in der folgenden Tabelle dargestellt:

				Erforderliches Verständnisniveau (kognitiv/taxonomisch)	
		Anzahl der Fragen/Punkte pro Kompetenzbereich	Prozentualer Anteil der Fragen/Punkte pro Kompetenzbereich	Fragen, die Verstehen, Anwendung und Analyse messen	Fragen, die Synthese und Bewertung messen
Kompetenzbereiche	Grundlegende Prinzipien und Konzepte der Handhabung von Informationssicherheitsrisiken	13	21,67	X	
	Umsetzung eines Programms zur Handhabung von Informationssicherheitsrisiken	7	11,67	X	
	Rahmenwerk und Prozesse für das Informationssicherheitsrisikomanagement auf der Grundlage von ISO/IEC 27005	31	51,67		X
	Andere Methoden zur Beurteilung von Informationssicherheitsrisiken	9	15	X	
	Insgesamt	**60**	**100%**		
	Anzahl der Fragen pro Verständnisebene			**29**	**31**
	Prozentualer Anteil der Fragen pro Verständnisebene (kognitiv/Taxonomie)			**48,3 %**	**51,7 %**

Für das Bestehen müssen **70 %** der Prüfungsfragen richtig beantwortet werden.

Nach bestandener Prüfung können die Kandidatinnen und Kandidaten einen Antrag auf Ausstellung des Berechtigungsnachweises „PECB Certified ISO/IEC 27005 Risk Manager“ stellen. Hier sind die jeweiligen Erfahrungsniveaus zu berücksichtigen.

Die Prüfung ablegen

Allgemeine Informationen zur Prüfung

Die Kandidatinnen und Kandidaten müssen mindestens 30 Minuten vor Beginn der Prüfung eintreffen/anwesend sein. Kandidatinnen und Kandidaten, die zu spät ankommen, erhalten keine zusätzliche Zeit, um die Verspätung auszugleichen, und könnten nicht zur Prüfung zugelassen werden.

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

Falls am Tag der Prüfung (in Papierform) beantragt, kann Kandidatinnen und Kandidaten, die die Prüfung in einer Fremdsprache ablegen, eine zusätzliche Zeit gewährt werden:

- 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. **Auf Papier:** Die Prüfungen werden in Papierform bereitgestellt. Die Kandidatinnen und Kandidaten dürfen nichts anderes als das Prüfungspapier und einen Stift benutzen. Die Verwendung von elektronischen Geräten wie Laptops, Tablets oder Telefonen ist nicht zulässig. 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 zulässig. Die Prüfungssitzung wird von einem Aufsichtsführenden der PECB über die Anwendung PECB Exams und eine externe/integrierte Kamera fernüberwacht.

Ausführlichere Informationen über das Online-Format 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 enthält Multiple-Choice-Fragen: Dieses Format wurde ausgewählt, weil es sich als effektiv und effizient für die Messung und Bewertung von Lernergebnissen im Zusammenhang mit den festgelegten Kompetenzbereichen erwiesen hat. Mithilfe der Multiple-Choice-Prüfung kann das Verständnis der Kandidatinnen und Kandidaten über sowohl einfache als auch komplexe Konzepte bewertet werden. Bei der Beantwortung dieser Fragen müssen die Kandidatinnen und Kandidaten verschiedene Prinzipien anwenden, Probleme analysieren, Alternativen bewerten, mehrere Konzepte oder Ideen kombinieren usw. Die Multiple-Choice-Fragen sind szenariobasiert, d. h. sie wurden auf Grundlage eines Szenarios entwickelt, das die Kandidatinnen und Kandidaten zuerst lesen und danach Antworten auf eine oder mehrere Fragen zu diesem Szenario geben sollen. Bei dieser Multiple-Choice-Prüfung dürfen aufgrund der kontextabhängigen Charakteristik der Fragen weitere Unterlagen (Open Book) genutzt werden. Im Folgenden finden Sie Beispiele für Prüfungsfragen.

Da es sich hier um eine Open-Book-Prüfung handelt, dürfen die Kandidatinnen und Kandidaten die folgenden Referenzmaterialien verwenden:

- Ein gedrucktes Exemplar der ISO/IEC 27005
- 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

Jeder Versuch, während der Prüfung abzuschreiben, zusammenzuarbeiten oder anderweitig zu betrügen, führt automatisch zum Nichtbestehen der Prüfung.

Die PECB-Prüfungen sind in Englisch und anderen Sprachen verfügbar. Um zu erfahren, ob die Prüfung in einer bestimmten Sprache verfügbar ist, wenden Sie sich bitte an examination.team@pecb.com.

Anmerkung: PECB wird schrittweise zu Multiple-Choice-Prüfungen übergehen. Sie werden ebenfalls ‚Open Book' sein und aus szenariobasierten Fragen bestehen, anhand derer die PECB das Wissen, die Fähigkeiten und die Kompetenzen der Kandidatinnen und Kandidaten im Hinblick darauf bewerten kann, wie Informationen in neuen Situationen angewendet (Anwenden), Verbindungen zwischen Konzepten hergestellt (Analysieren) und ein Standpunkt oder eine Entscheidung begründet (Bewerten) wird. Alle Multiple-Choice-Prüfungen der PECB bestehen aus einer Frage mit drei Antworten, von denen nur eine richtig ist..

Spezifische Informationen über Prüfungsarten, verfügbare Sprachen und weitere Details finden Sie in der Liste der PECB Prüfungen.

PECB

Prüfungsbeispiel für szenariobasierte Fragen

Techonics ist ein Technologieunternehmen, das sich auf Computersoftware und Unterhaltungselektronik spezialisiert hat. Das Unternehmen führt regelmäßig Risikobeurteilungen durch, um die Informationssicherheit zu gewährleisten. Durch den gut funktionierenden Prozess zur Handhabung von Informationssicherheitsrisiken ist *Techonics* in der Lage, potenzielle Risiken im Zusammenhang mit Informationswerten zu identifizieren und Lösungen zu finden. Das Rahmenwerk für das Risikomanagement basiert auf dem Leitfaden der ISO/IEC 27005.

Der letzte Prozess der Risikobeurteilung der Informationssicherheit bei *Techonics* fand im letzten Monat statt. Die Risikobeurteilung wurde von Lana, der Risikomanagerin von *Techonics*, durchgeführt, und die Ergebnisse zeigten einige neue Risiken im Zusammenhang mit der Passwortpolitik auf. Gemäß dem Rahmenwerk für das Risikomanagement von *Techonics* wurde der Prozess der Risikobeurteilung durch eine sorgfältige Analyse des Unternehmens und seiner Ziele eingeleitet. Dann wurden die grundlegenden Kriterien für das Risikomanagement festgelegt.

Lana befragte das Schlüsselpersonal. Sie fand heraus, dass die meisten Beschäftigten von *Techonics* sich bewusst waren, dass sie ihre Passwörter gemäß der Passwortpolitik alle drei Monate ändern müssen. Die meisten von ihnen hielten sich jedoch nicht daran, da das System dies nicht erzwingen konnte.

Darüber hinaus fand sie heraus, dass die Beschäftigten dazu neigen, schwache Passwörter wie ihren Vor- und Nachnamen zu verwenden. Da solche schwachen Passwörter leicht zu erraten sind, könnte dies zu einem ernsthaften Problem für die Sicherheit von *Techonics* werden. Im Hinblick auf diese Situation identifizierte Lana mehrere Risikoszenarien, von denen zwei eine Eintrittswahrscheinlichkeit von „Hoch“ aufwiesen.

Sam schlug als Informationssicherheitsmanager die Implementierung eines cloudbasierten und plattformübergreifenden Passwortmanagers vor. Die Plattform könnte von allen Mitarbeitern genutzt werden, um komplexe Passwörter zu generieren und diese in einer sicheren Datenbank zu speichern. *Techonics* nahm seine Empfehlung an und begann mit der Nutzung der Plattform, um das Risiko im Zusammenhang mit schwachen Passwörtern zu minimieren. Darüber hinaus wurde beschlossen, dass Sam Schulungen zur Informationssicherheit organisieren würde, um das Personal über die Bedeutung des Passwortschutzes aufzuklären.

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

1. ***Techonics* hat die ISO/IEC 27005 als Leitfaden für die Einrichtung seines Rahmenwerks für das Informationssicherheitsrisikomanagement verwendet. Ist dies akzeptabel?**
   A. Nein, ISO/IEC 27005 spezifiziert die Anforderungen zur Erreichung von Informationssicherheit durch die Implementierung eines ISMS
   B. Ja, ISO/IEC 27005 ist auf jede Art von Risiko anwendbar, unabhängig von dessen Beschaffenheit oder Folgen
   C. **Ja, ISO/IEC 27005 bietet eine Anleitung zur Unterstützung von Organisationen bei der Durchführung von Maßnahmen zur Handhabung von Informationssicherheitsrisiken**

2. **Lana, die Risikomanagerin, hat herausgefunden, dass die Beschäftigten von *Techonics* ihre Passwörter nicht geändert haben, wie es die Passwortpolitik vorschreibt. Was hat Lana identifiziert?**
   A. **Eine Schwachstelle**
   B. Eine Bedrohung
   C. Ein Risiko

3. **Welche Option für die Risikobehandlung wurde vorgeschlagen, um die identifizierten Risiken bei der Verwendung von Passwörtern zu behandeln?**
   A. Risikovermeidung
   B. **Risikoänderung**
   C. Risikobeibehaltung

Die Prüfungsergebnisse erhalten

Die Prüfungsergebnisse werden Ihnen per E-Mail mitgeteilt.

- Bei Multiple-Choice-Prüfungen in Papierform kann die Bearbeitung und die Benachrichtigung zwei bis vier Wochen in Anspruch nehmen.

- Bei Multiple-Choice-Prüfungen im Online-Format erhalten die Kandidatinnen und Kandidaten ihre Ergebnisse sofort.

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

Kandidatinnen und Kandidaten, die die Prüfung nicht bestanden haben, erhalten in der E-Mail eine Liste der Bereiche, in denen sie schlecht abgeschnitten haben, damit sie sich besser auf eine Wiederholung vorbereiten können.

Richtlinie für Prüfungswiederholungen

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

- Wird die Prüfung beim ersten Versuch nicht bestanden, kann die erste Wiederholungsprüfung frühestens 15 Tage nach der Erstprüfung erfolgen.
  Anmerkung: Die Kandidatinnen und 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.

Wird auch die Wiederholungsprüfung nicht bestanden, empfiehlt die PECB, sich mit einer Schulung besser auf die Prüfung vorzubereiten.

Zur Vereinbarung einer Wiederholungsprüfung müssen Kandidatinnen und 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 der Erstprüfung ein, damit Ihnen die Gebühr erlassen wird
2. Papierprüfung: Sie müssen sich an denjenigen PECB-Partner/Vertriebspartner wenden, der die Erstprüfung organisiert hat, um die Wiederholungsprüfung zu vereinbaren (Datum, Uhrzeit, Ort, Kosten).

Kandidatinnen und 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. Die Planung für die Wiederholungsprüfung verläuft so wie bei der Erstprüfung.

Geheimhaltung der Prüfungsinhalte (Exam Security)

Ein wichtiger Teil eines beruflichen Zertifizierungsnachweises ist die Gewährleistung der Geheimhaltung und Vertraulichkeit in Bezug auf die Prüfungsinhalte. Die PECB vertraut auf das ethische Verhalten der Inhaber und Antragsteller von Zertifizierungen, um die Geheimhaltung und Vertraulichkeit der PECB-Prüfungen zu bewahren. Jegliche Weitergabe von Informationen über PECB-Prüfungsinhalte stellt einen direkten Verstoß gegen den Ethikkodex der PECB dar. Gegen Personen, die gegen diese Regeln und Richtlinien verstoßen, wird

die PECB Maßnahmen ergreifen, zu denen der dauerhafte Ausschluss von der Erlangung von Berechtigungsnachweisen der PECB und der Entzug aller bisherigen Berechtigungsnachweise gehören. Die PECB wird darüber hinaus rechtliche Schritte gegen Personen oder Organisationen einleiten, die die Urheberrechte, Eigentumsrechte und das geistige Eigentum der PECB verletzen.

Verlegen der Prüfung

Für Änderungen in Bezug auf das Prüfungsdatum, die Uhrzeit, den Prüfungsort oder andere Details wenden Sie sich bitte an examination.team@pecb.com.

Antrag auf Zertifizierung

Alle Kandidatinnen und Kandidaten mit bestandener PECB-Prüfung (oder ein von der PECB anerkanntes Äquivalent) sind berechtigt, die PECB-Berechtigungsnachweise zu beantragen, für die sie geprüft wurden. Um eine PECB-Zertifizierung zu erhalten, müssen bestimmte Ausbildungs- und Berufsanforderungen erfüllt werden. Die Kandidatinnen und Kandidaten müssen das Online-Antragsformular für die Zertifizierung ausfüllen (das über ihr PECB-Online-Profil aufgerufen werden kann), wozu die Kontaktdaten von Referenzpersonen gehören, die die Berufserfahrung der Kandidatinnen und Kandidaten bestätigen können. Der Antrag kann in verschiedenen Sprachen eingereicht werden. Die anfallenden Gebühren können wahlweise online oder per Rechnung bezahlen werden. Für weitere Informationen wenden Sie sich an certification.team@pecb.com.

Der Online-Antragsprozess für die Zertifizierung ist sehr einfach und nimmt nur wenige Minuten in Anspruch. Dazu:

- Registrieren Sie Ihr Konto
- Prüfen Sie Ihre E-Mail auf den Bestätigungslink
- Loggen Sie sich ein, um die Zertifizierung zu beantragen

Weitere Informationen zum Antragsverfahren finden Sie der englischsprachigen Anleitung Apply for Certification.

Der Antrag wird genehmigt, sobald die Zertifizierungsabteilung bestätigt hat, dass alle Zertifizierungsanforderungen für den jeweiligen Berechtigungsnachweis erfüllt sind. Der jeweilige Status des Antrags wird per E-Mail an die bei der Beantragung angegebene E-Mail mitgeteilt. Wenn der Antrag genehmigt wurde, können die Kandidaten die Zertifizierung von ihrem PECB-Konto herunterladen.

Die PECB bietet Support sowohl auf Englisch als auch auf Französisch.

Erneuern Sie Ihre Zertifizierung

Die Gültigkeitsdauer von PECB-Zertifizierungen beträgt drei Jahre. Um diese aufrechtzuerhalten, müssen die Kandidatinnen und Kandidaten jedes Jahr nachweisen, dass sie immer noch zertifizierungsrelevante Aufgaben ausführen. PECB-zertifiziertes Fachpersonal muss jährlich Credits (Fortbildungspunkte) für die kontinuierliche berufliche Weiterbildung (Continual Professional Development,CPD) erbringen und 100 Dollar als Jahresgebühr (Annual Maintenance Fee, AMF) zahlen, um die Zertifizierung aufrechtzuerhalten. Weitere Informationen finden Sie in der Richtlinie zur Aufrechterhaltung der Zertifizierung der PECB-Website.

Schließen eines Falles

Stellen die Kandidatinnen und Kandidaten innerhalb von drei Jahren keinen Antrag auf Zertifizierung, wird ihr Fall geschlossen. Auch nach Ablauf des Zertifizierungszeitraums haben die Kandidatinnen und Kandidaten das Recht, ihren Fall wieder aufzunehmen. Allerdings ist die PECB nicht länger für Änderungen bezüglich der Bedingungen, Standards, Richtlinien und des Handbuchs für Kandidatinnen und Kandidaten verantwortlich, die vor der Schließung des Falls galten. Für eine Wiederaufnahme eines Falles muss dies schriftlich beantragt und die erforderliche Gebühr entrichtet werden.

ABSCHNITT III: ZERTIFIZIERUNGSANFORDERUNGEN

ISO/IEC 27005 Risk Manager

Die Anforderungen für PECB ISO/IEC 27005 Manager-Zertifizierungen sind:

Berechtigungsnachweis	Prüfung	Berufliche Erfahrung	Erfahrung im Risikomanagement	Sonstige Anforderungen
PECB Certified ISO/IEC 27005 Provisional Risk Manager	PECB Certified ISO/IEC 27005 Risk Manager Prüfung oder gleichwertig	Keine	Keine	Unterzeichnung des PECB-Ethikkodex
PECB Certified ISO/IEC 27005 Risk Manager	PECB Certified ISO/IEC 27005 Risk Manager Prüfung oder gleichwertig	Zwei Jahre: Ein Jahr Berufserfahrung in der Handhabung von Informationssicherheitsrisiken	Tätigkeiten im Bereich Informationssicherheitsrisikomanagement: insgesamt 200 Stunden	Unterzeichnung des PECB-Ethikkodex

Berücksichtigungsfähig sind solche Tätigkeiten, die bewährten Verfahren bzw. Best Practices für die Umsetzung und Steuerung des Risikomanagements entsprechen. Dazu gehört Folgendes:

1. Definieren eines Risikomanagementansatzes
2. Bestimmen der Ziele und des Anwendungsbereichs des Risikomanagements
3. Durchführen einer Risikobeurteilung
4. Entwickeln eines Risikomanagementprogramms
5. Definieren von Kriterien für die Risikobewertung und -akzeptanz
6. Bewerten von Optionen für die Risikobehandlung
7. Überwachen und überprüfen des Risikomanagementprogramms

ABSCHNITT IV: REGELN UND RICHTLINIEN FÜR DIE ZERTIFIZIERUNG

Berufliche Referenzen

Für jeden Antrag sind zwei berufliche Referenzen erforderlich. Sie müssen von Personen stammen, die mit den Kandidatinnen oder Kandidaten in einem professionellen Umfeld zusammengearbeitet haben und deren Erfahrung im Bereich des Informationssicherheitsrisikomanagement sowie deren derzeitigen und früheren beruflichen Werdegang bestätigen können. Berufliche Referenzen von Personen, die unter der Aufsicht der Kandidatin oder des Kandidaten stehen oder mit ihr oder ihm verwandt sind, sind nicht gültig.

Berufserfahrung

Die Kandidatinnen und Kandidaten müssen vollständige und korrekte Angaben zu ihrer Berufserfahrung machen, einschließlich Berufsbezeichnung(en), Anfangs- und Enddatum, Tätigkeitsbeschreibung(en) und mehr. Es wird empfohlen, frühere oder derzeitige Aufgaben zusammenzufassen und dabei so detailliert wie möglich zu beschreiben, welche Aufgaben bei den einzelnen Tätigkeiten wahrgenommen wurden. Ausführlichere Informationen können in den Lebenslauf eingefügt werden.

Erfahrung im Risikomanagement

Anhand des Protokolls für Risikomanagementprojekte der Kandidatinnen und Kandidaten wird überprüft, ob die erforderliche Anzahl von Risikomanagementstunden erreicht wurde.

Begutachtung von Zertifizierungsanträgen

Die Zertifizierungsabteilung begutachtet jeden Antrag, um festzustellen, ob alle Voraussetzungen für die Zertifizierung erfüllt sind. Kandidatinnen und Kandidaten, deren Anträge begutachtet werden, werden schriftlich benachrichtigt, falls zusätzliche Unterlagen beizubringen sind. Bei Bedarf wird ein angemessener Zeitrahmen zuerkannt. Wird auf die Benachrichtigung bis zum Ablauf der Frist nicht reagiert oder die erforderlichen Unterlagen werden nicht innerhalb des vorgegebenen Zeitrahmens vorgelegt, begutachtet die Zertifizierungsabteilung den Antrag auf Grundlage der ursprünglich vorgelegten Informationen, was letztendlich zu einer Herabstufung auf eine niedrigere Qualifikationsstufe führen kann.

Verweigerung der Zertifizierung

Die PECB kann die Zertifizierung verweigern, falls Kandidatinnen oder Kandidaten:

- Den Antrag fälschen
- Gegen die Prüfungsverfahren verstoßen
- Gegen den PECB-Ethikkodex verstoßen
- Die Prüfung nicht bestehen

Ausführlichere Informationen finden Sie im Abschnitt „Beschwerde und Einspruch“.

Die Antragsgebühr für die Zertifizierung ist nicht erstattungsfähig.

Aussetzung der Zertifizierung

Die PECB kann die Zertifizierung vorübergehend aussetzen, falls die Kandidatin oder der Kandidat die Anforderungen nicht erfüllt. Sonstige Gründe für die Aussetzung der Zertifizierung sind unter anderem:

- Die PECB erhält zahlreiche oder schwerwiegende Beschwerden von interessierten Parteien (Aussetzung bis zum Abschluss der Untersuchung).
- Die Logos der PECB oder der Akkreditierungsstellen werden vorsätzlich missbraucht.
- Die Kandidatin oder der Kandidat versäumt es, den Missbrauch einer Zertifizierungsmarke innerhalb des von der PECB festgelegten Zeitrahmens zu korrigieren.
- Die zertifizierte Person hat aus eigenen Stücken eine Aussetzung beantragt.
- Die PECB hält sonstige Gründe für die Aussetzung der Zertifizierung für angemessen.

Widerruf der Zertifizierung

Die PECB kann die Zertifizierung entziehen, wenn die Anforderungen der PECB nicht erfüllt sind. Die Kandidatinnen und Kandidaten dürfen sich dann nicht länger als PECB-zertifiziertes Fachpersonal ausgeben. Weitere Gründe für den Widerruf der Zertifizierung können sein, falls Kandidatinnen und Kandidaten:

- Gegen den PECB-Ethikkodex verstoßen
- Den Geltungsbereich der Zertifizierung falsch darstellen und falsche Angaben dazu machen
- Gegen andere PECB-Regeln verstoßen

Höherstufung von Berechtigungsnachweisen

Fachpersonal kann eine Höherstufung des Berechtigungsnachweis beantragen, sobald nachgewiesen ist, dass alle Anforderungen erfüllt sind.

Für die Beantragung einer Höherstufung müssen sich die Kandidatinnen und Kandidaten an ihrem PECB-Konto anmelden und auf der Registerkarte „My Certifications“ (Meine Zertifizierungen) den Link „Upgrade“ (Höherstufung) klicken. Die Antragsgebühr für eine Höherstufung 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 CPD-Stunden eingereicht.
- Der Nachweis über die CPD-Stunden wurde auf Anfrage nicht erbracht.

Anmerkung: *Bei PECB-zertifiziertem Fachpersonal mit einer Lead-Zertifizierung, das die Erfüllung der Anforderungen für die Aufrechterhaltung der Zertifizierung nicht nachweisen kann, wird der Berechtigungsnachweis herabgestuft. Dahingegen wird die Zertifizierung von Inhaberinnen und Inhabern von Master-Zertifizierungen widerrufen, die es versäumen, CPDs einzureichen und AMFs zu zahlen.*

Sonstige Status

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

ABSCHNITT V: ALLGEMEINE RICHTLINIEN DER PECB

PECB-Ethikkodex

Die Einhaltung des PECB-Ethikkodexes ist eine freiwillige Verpflichtung. Es ist wichtig, dass sich PECB-zertifiziertes Fachpersonal nicht nur an die Grundsätze dieses Kodex hält, sondern auch andere dazu ermutigt und dabei unterstützt. Weitere Informationen finden Sie hier.

Andere Prüfungen und Zertifizierungen

PECB akzeptiert Zertifizierungen und Prüfungen von anderen anerkannten und akkreditierten Zertifizierungsstellen. 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 Auditor) anerkannt werden können.

Nichtdiskriminierung und besondere Vorkehrungen

Alle Anträge von Kandidatinnen und Kandidaten werden objektiv begutachtet, unabhängig von deren Alter, Geschlecht, ethnischer Herkunft, Religion, Nationalität oder Familienstand.
Um die Chancengleichheit für alle qualifizierten Personen zu gewährleisten, wird die PECB gegebenenfalls angemessene Vorkehrungen für die Kandidatinnen und Kandidaten treffen. Sollten Kandidatinnen oder Kandidaten aufgrund einer Behinderung oder einer bestimmten körperlichen Verfassung besondere Vorkehrungen benötigen, sollten sie den Partner/Vertriebspartner darüber informieren, damit dieser entsprechende Vorkehrungen treffen kann. Alle von den Kandidatinnen und Kandidaten gemachten Angaben zu ihren Behinderungen/Bedürfnissen werden streng vertraulich behandelt.

Klicken Sie hier , um das Formular für Kandidatinnen und Kandidaten mit Behinderungen herunterzuladen.

Beschwerden und Einsprüche

Beschwerden müssen innerhalb von 30 Tagen nach Erhalt der Zertifizierungsentscheidung eingereicht werden. Die PECB lässt der Kandidatin bzw. dem Kandidaten innerhalb von 30 Arbeitstagen nach Erhalt der Beschwerde eine schriftliche Antwort zukommen. Ist die Antwort nicht zufriedenstellend, hat die Kandidatin bzw. der Kandidat das Recht, einen Einspruch einzulegen. Weitere Informationen zu den Beschwerde- und Einspruchsverfahren finden Sie hier.

(1) Gemäß ADA kann der Begriff "angemessene Vorkehrungen" Folgendes umfassen: (A) die Bereitstellung von Einrichtungen, die von Beschäftigten 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 Vorlesern oder Dolmetschern und andere ähnliche Vorkehrungen für Menschen mit Behinderungen.

(2) 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, Lizenzierung, Zertifizierung oder Erteilung von Berechtigungsnachweisen für sekundäre oder postsekundäre 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, barrierefreie Vorrichtungen 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

PECB Help 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.

E-Mail-Adressen:
Prüfung: examination.team@pecb.com
Zertifizierung: certification.team@pecb.com
Kundenbetreuung: support@pecb.com