PECB BEYOND RECOGNITION

Kandidaten-handbuch

ISO/IEC 27001 LEAD AUDITOR

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 Fachleuten, ihr Engagement und ihre Kompetenz unter Beweis zu stellen, indem wir ihnen 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 Fachkräften erforderlichen Mindestanforderungen
2. Überprüfung und Verifizierung der Qualifikationen von Bewerbern, um sicherzustellen, dass diese die Voraussetzungen für eine Zertifizierung erfüllen
3. Entwicklung und Pflege von zuverlässigen Zertifizierungsbewertungen
4. Erteilung von Zertifizierungen an qualifizierte 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 Kandidaten in ihrer beruflichen Praxis ethische Standards einhalten
7. 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 werden Fachkräfte, die eine PECB-Zertifizierung anstreben, von der Anerkennung der PECB auf dem nationalen und internationalen Markt profitieren.

Kompetentes Personal
Das Team der PECB besteht aus kompetenten Mitarbeitern, die über einschlägige sektorspezifische Erfahrungen verfügen.
Alle unsere Mitarbeiter 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 sorgen dafür, dass die Anforderungen der Norm mit der entsprechenden 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 tun unser Bestes, um eine maximale Reaktionszeit von 24 Stunden einzuhalten, ohne Abstriche bei der Qualität des Dienstes.

PECB Verhaltenskodex

PECB-Fachkräfte:

1. handeln 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 sich beim Anbieten professioneller Dienstleistungen an die professionellen Normen und anwendbaren Techniken halten
3. erhalten die Kompetenz in ihrem jeweiligen Fachgebiet aufrecht und bemühen sich, 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 vorgeschlagenen Dienstleistungen, 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. alle Gesetze und Vorschriften der Länder einhalten, in denen die berufliche Tätigkeit ausgeübt wird
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 den Ruf der PECB oder ihrer Zertifizierungsprogramme beeinträchtigen könnte
11. kooperieren uneingeschränkt bei der Untersuchung eines angeblichen Verstoßes gegen diesen Verhaltenskodex

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

Einführung in ISO/IEC 27001 Lead Auditor

Die ISO/IEC 27001 legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) fest. Die wichtigsten auf dem Markt geforderten Fertigkeiten sind die Fähigkeit, Audits in Übereinstimmung mit dem Zertifizierungsprozess der ISO/IEC 27001 effektiv zu planen und durchzuführen, Audit-Techniken zu beherrschen und ISMS-Audit-Teams und -Programme zu leiten (oder Teil davon zu sein).

Neben der Umsetzung des ISMS benötigen Organisationen die Gewissheit, dass die von ihnen umgesetzten Maßnahmen oder Prozesse wirksam sind. Audits ermöglichen es Organisationen, die Wirksamkeit des vorhandenen ISMS zu bewerten und es weiter zu verbessern.

Der Berechtigungsnachweis „ISO/IEC 27001 Lead Auditor“ ist eine berufliche Zertifizierung für Personen, die ihre Kompetenz zur Auditierung eines Informationssicherheitsmanagementsystems und zur Leitung eines ISMS-Auditteams nachweisen wollen.

In Anbetracht der Tatsache, dass Auditing einer der gefragtesten Berufe ist, kann eine international anerkannte Zertifizierung Ihnen helfen, Ihr Karrierepotenzial auszuschöpfen und Ihre beruflichen Ziele zu erreichen.

Es ist wichtig zu verstehen, dass PECB-Zertifizierungen keine Lizenz oder einfach eine Mitgliedschaft sind. Sie stellen eine Anerkennung im Fachkollegenkreis dar, dass eine Person ihre Kenntnisse und ihr Verständnis einer Reihe von Kompetenzen unter Beweis gestellt hat. PECB-Zertifizierungen werden an Kandidaten vergeben, die ihre Erfahrung nachweisen können und eine standardisierte Prüfung im Zertifizierungsbereich bestanden haben.

In diesem Dokument wird das Zertifizierungsverfahren für den PECB ISO/IEC 27001 Lead Auditor in Übereinstimmung mit ISO/IEC 17024:2012 festgelegt. Dieses Kandidatenhandbuch 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 Ihre Bewerbung ausfüllen und einreichen. Sollten Sie nach dem Lesen des Handbuchs 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

Alle PECB-Zertifizierungen erfordern eine bestimmte Ausbildung und Berufserfahrung. Um den für Sie richtigen Berechtigungsnachweis zu finden, überprüfen Sie die Zulassungskriterien für die verschiedenen Zertifizierungen und Ihre beruflichen Erfordernisse.

Vorbereiten und Planen der Prüfung

Alle Kandidaten sind für ihr Studium und ihre Vorbereitung auf die Zertifizierungsprüfungen selbst verantwortlich. Im Rahmen des Zertifizierungsprozesses sind keine bestimmten Schulungsreihen oder Studienpläne erforderlich. Allerdings kann die Teilnahme an einer Schulung die Wahrscheinlichkeit deutlich erhöhen, eine PECB-Prüfung erfolgreich zu bestehen.

Um eine Prüfung zu planen, haben die Kandidaten zwei Möglichkeiten:

1. Sie können sich mit einem unserer Partner in Verbindung setzen, der Schulungen und Prüfungstermine anbietet. Einen Anbieter von Schulungen in einer bestimmten Region können die Kandidaten auf der Seite Active Partners finden. Die Termine für PECB-Schulungen finden Sie auch auf der Seite Trainingsveranstaltungen..
2. Wenn Sie eine PECB-Prüfung von zu Hause oder einem anderen Ort aus ablegen möchten, können Sie sich dafür unter Prüfungsveranstaltungen anmelden:

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

Anmeldegebühren für Prüfung und Zertifizierung

Die PECB bietet direkte Prüfungen an, bei denen ein Kandidat ohne vorherige Schulungskurse die Prüfung ablegen kann. Die Preise hierfür sind wie folgt:

- Lead-Prüfung: 1000$
- Manager-Prüfung: 700$
- Foundation und Transition Prüfung (Grundlagen und Übergang): 500$

Die Anmeldegebühr für die Zertifizierung beträgt $500.

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

Kompetenzbereiche

Mit bestandener Prüfung zum „PECB Certified ISO/IEC 27001 Lead Auditor“ wird gewährleistet, dass der Kandidat über die notwendige Kompetenz verfügt, ein Audit eines Informationssicherheitsmanagementsystems (ISMS) gemäß den normativen Anforderungen der ISO/IEC 27001 durchzuführen, ein Auditteam unter Anwendung allgemein anerkannter Auditprinzipien, -verfahren und -techniken zu leiten und schließlich interne und externe Audits gemäß den Leitlinien der ISO 19011 und in Übereinstimmung mit den Zertifizierungsprozessen der ISO/IEC 17021-1 zu planen und durchzuführen.

Die Zertifizierung zum ISO/IEC 27001 Lead Auditor richtet sich an:

- Auditoren, die Audits von Informationssicherheitsmanagementsystemen (ISMS) durchführen und leiten wollen
- Manager oder Berater, die den Auditprozess des Informationssicherheitsmanagementsystems beherrschen wollen
- Personen, die für die Aufrechterhaltung der Konformität mit den ISMS-Anforderungen in einer Organisation verantwortlich sind
- Fachexperten, die sich auf ein Audit des Informationssicherheitsmanagementsystems vorbereiten wollen
- Fachberater für Informationssicherheitsmanagement

Der Inhalt der Prüfung gliedert sich wie folgt:

- **Bereich 1:** Grundlegende Prinzipien und Konzepte eines Informationssicherheitsmanagementsystems (ISMS)
- **Bereich 2:** Informationssicherheitsmanagementsystem (ISMS)
- **Bereich 3:** Grundlegende Prinzipien und Konzepte eines Audits
- **Bereich 4:** Vorbereitung eines Audits nach ISO/IEC 27001
- **Bereich 5:** Durchführung eines Audits nach ISO/IEC 27001
- **Bereich 6:** Abschluss eines Audits nach ISO/IEC 27001
- **Bereich 7:** Steuerung eines Auditprogramms nach ISO/IEC 27001

Bereich 1: Grundlegende Prinzipien und Konzepte eines Informationssicherheitsmanagementsystems (ISMS)

Hauptziel: Der Kandidat versteht die Prinzipien und Konzepte der ISO/IEC 27001 und kann diese interpretieren

Kompetenzen	Kenntnisse
1. Fähigkeit, die wichtigsten Konzepte des Informationssicherheitsmanagementsystems zu verstehen und zu erläutern 2. Fähigkeit, die Abläufe in der Organisation und die Entwicklung von Informationssicherheitsstandards zu verstehen und zu erläutern 3. Fähigkeit, die Anforderungen an die Informationssicherheit in einer Organisation zu identifizieren, zu analysieren und zu bewerten 4. Fähigkeit, die wichtigsten Konzepte der Informationssicherheit und des Informationssicherheitsrisikomanagements zu erläutern und zu veranschaulichen	1. Kenntnis der Gesetze, Vorschriften, internationalen und branchenüblichen Normen, Verträge, Marktpraktiken, internen Richtlinien usw., die ein Unternehmen in Bezug auf die Informationssicherheit einhalten muss 2. Kenntnis der wichtigsten Normen mit Bezug zur Informationssicherheit 3. Kenntnis der wichtigsten Konzepte und der Terminologie der ISO/IEC 27001 4. Kenntnis des Risikokonzepts und seiner Anwendung auf die Informationssicherheit 5. Kenntnis der Beziehung zwischen den Aspekten der Informationssicherheit 6. Kenntnis des Unterschieds und der Merkmale von Sicherheitszielen und -maßnahmen 7. Kenntnis des Unterschieds zwischen präventiven, detektiven und korrektiven Maßnahmen

5. Fähigkeit, den Unterschied zwischen Informationswerten, Daten und Aufzeichnungen zu erkennen und zu erläutern 6. Fähigkeit, die Beziehung zwischen Aspekten der Informationssicherheit wie Maßnahmen, Schwachstellen, Bedrohungen, Risiken und Vermögenswerten zu verstehen, zu interpretieren und zu veranschaulichen 7. Fähigkeit, Big Data, künstliche Intelligenz, maschinelles Lernen, Cloud Computing und Auslagerung von Tätigkeiten zu identifizieren und zu erläutern	8. Kenntnis der wichtigsten Merkmale von Big Data, künstlicher Intelligenz, maschinellem Lernen, Cloud Computing und Auslagerung von Tätigkeiten

Bereich 2: Informationssicherheitsmanagementsystem (ISMS) und Anforderungen der ISO/IEC 27001

Hauptziel: Der Kandidat versteht die Anforderungen an ein Informationssicherheitsmanagementsystem auf Grundlage von ISO/IEC 27001 und kann diese interpretieren und identifizieren

Kompetenzen	Kenntnisse
1. Fähigkeit, den Aufbau der Norm ISO/IEC 27001:2022 zu verstehen 2. Fähigkeit, die Komponenten eines Informationssicherheitsmanagementsystems auf Grundlage von ISO/IEC 27001 und dessen Hauptprozesse zu verstehen 3. Fähigkeit, die Anforderungen der ISO/IEC 27001 zu verstehen, zu interpretieren und zu analysieren 4. Fähigkeit, die wichtigsten Schritte bei Einrichtung, Umsetzung, Betrieb, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung des ISMS einer Organisation zu verstehen, zu erläutern und zu veranschaulichen 5. Fähigkeit, die externen und internen Faktoren mit Bezug zum ISMS aufzustellen und die interessierten Parteien und deren Bedürfnisse zu bestimmen 6. Fähigkeit, den Anwendungsbereich des ISMS zu bestimmen 7. Fähigkeit, die Verpflichtung der Leitung zu gewährleisten, eine Informationssicherheitspolitik aufzustellen sowie ISMS-Rollen und -Verantwortlichkeiten zuzuweisen 8. Fähigkeit, Änderungen und Maßnahmen zur Behebung von Risiken zu planen 9. Fähigkeit, die Prozesse der Risikobeurteilung und Risikobehandlung zu verstehen 10. Fähigkeit, die Auswahl geeigneter Maßnahmen auf Grundlage von Anhang A der ISO/IEC 27001 zu verstehen 11. Fähigkeit, die Bewusstseinsbildung und Kompetenz der Beschäftigten im Hinblick auf	1. Kenntnis der Norm ISO/IEC 27001:2022 und der sie unterstützenden Normen 2. Kenntnis der Konzepte, Prinzipien und Terminologie mit Bezug zu Managementsystemen 3. Kenntnis der grundlegenden Merkmale eines integrierten Managementsystems 4. Kenntnis der in den Abschnitten 4 bis 10 aufgeführten Anforderungen der ISO/IEC 27001 5. Kenntnis der 93 im Anhang A der ISO/IEC 27001 aufgeführten Maßnahmen 6. Kenntnis der internen und externen Faktoren sowie interessierten Parteien des ISMS 7. Kenntnis der wichtigsten Schritte zur Festlegung des Anwendungsbereichs des ISMS und der Informationssicherheitspolitik 8. Kenntnis der Führung und der Verpflichtung der obersten Leitung sowie der organisatorischen Rollen und Verantwortlichkeiten mit Bezug zum ISMS 9. Kenntnis der für das Risikomanagement und die Verbesserung der Informationssicherheit relevanten Sicherheitsziele, -prozesse und -verfahren, um Ergebnisse in Übereinstimmung mit den allgemeinen Richtlinien und Zielen einer Organisation zu erzielen 10. Kenntnis der Herangehensweisen und Methoden der Risikobeurteilung und -behandlung 11. Kenntnis der Auswahl von Maßnahmen in Anhang A und deren Einbeziehung in die Erklärung zur Anwendbarkeit 12. Kenntnis des Leistungsbewertungsprozesses, einschließlich Überwachung, Messung,

die Ausübung ihrer Aufgaben mit Bezug zum ISMS zu gewährleisten 12. Fähigkeit, die Leistung des ISMS zu überwachen und zu bewerten sowie interne Audits und Managementbewertungen durchzuführen 13. Fähigkeit, die fortlaufende Verbesserung zu gewährleisten und geeignete Maßnahmen zur Behandlung von Nichtkonformitäten umzusetzen	Analyse und Bewertung, internes Audit und Managementbewertung 13. Kenntnis des Konzepts der fortlaufenden Verbesserung und seiner Anwendung auf ein ISMS

Bereich 3: Grundlegende Prinzipien und Konzepte eines Audits

Hauptziel: Der Kandidat versteht die wichtigsten Konzepte und Prinzipien in Bezug auf ein ISMS-Audit und kann diese interpretieren und anwenden

Kompetenzen	Kenntnisse
1. Fähigkeit, die Anwendung der Auditprinzipien in einem ISMS-Audit zu verstehen, zu erklären und zu veranschaulichen 2. Fähigkeit, Erst-, Zweit- und Drittparteien-Audits zu unterscheiden 3. Fähigkeit, Situationen zu erkennen und zu beurteilen, die die Professionalität des Auditors in Frage stellen und gegen den PECB-Verhaltenskodex verstoßen würden 4. Fähigkeit, ethische Themen unter Berücksichtigung der Verpflichtungen gegenüber dem Audit-Kunden, der auditierten Organisation, den Strafverfolgungs- und Aufsichtsbehörden zu erkennen und zu beurteilen 5. Fähigkeit, die rechtlichen Auswirkungen von Vorschriftswidrigkeiten, die von der auditierten Organisation begangen wurden, zu verstehen 6. Fähigkeit, den Ansatz der evidenzbasierten Auditierung im Kontext eines ISMS-Audit zu erläutern, zu veranschaulichen und anzuwenden 7. Fähigkeit, die Arten und Merkmale von Beweismaterial zu erläutern und zu vergleichen 8. Fähigkeit, die Art und den Umfang des für ein ISMS-Audit erforderlichen Beweismaterials zu bestimmen und zu begründen 9. Fähigkeit, die Auswirkungen von Trends und Technologien im Auditwesen zu verstehen	1. Kenntnis der wichtigsten Auditkonzepte und -prinzipien, wie sie in ISO 19011 beschrieben sind 2. Kenntnis der Unterschiede zwischen Erst-, Zweit- und Drittparteien-Audits 3. Kenntnis der Prinzipien des Auditing wie Integrität, sachliche Darstellung, angemessene berufliche Sorgfalt, Vertraulichkeit, Unabhängigkeit, evidenzbasierter Ansatz und risikobasierter Ansatz 4. Kenntnis der beruflichen Verantwortung des Auditors und des PECB-Verhaltenskodex 5. Kenntnis des evidenzbasierten Ansatzes bei einem Audit 6. Kenntnis der verschiedenen Arten von Auditnachweisen, wie z. B. physische, mathematische, bestätigende, technische, analytische, dokumentarische und mündliche 7. Kenntnis der für die auditierte Organisation und das Land, in dem sie tätig ist, geltenden Gesetze und Vorschriften 8. Kenntnis der Verwendung von Big Data bei Audits 9. Kenntnis der Auditierung ausgelagerter Tätigkeiten

Bereich 4: Vorbereitung eines Audits nach ISO/IEC 27001

Hauptziel: Der Kandidat kann ein Audit des Informationssicherheitsmanagementsystems vorbereiten

Kompetenzen	Kenntnisse
1. Fähigkeit, die Schritte und Aktivitäten zur Vorbereitung eines ISMS-Audits unter Berücksichtigung des spezifischen Kontexts des Audits zu verstehen und darzustellen 2. Fähigkeit, den Grad der Wesentlichkeit zu bestimmen und zu bewerten und den risikobasierten Ansatz in den verschiedenen Phasen eines ISMS-Audits anzuwenden 3. Fähigkeit, das angemessene Niveau einer hinreichenden Sicherheit zu beurteilen, das für ein ISMS-Audit erforderlich ist 4. Fähigkeit, die Rollen und Verantwortlichkeiten der Leitung und der Mitglieder des Auditteams sowie der Fachexperten zu verstehen und zu erläutern 5. Fähigkeit, die Durchführbarkeit des Audits zu bestimmen 6. Fähigkeit, die Ziele, die Kriterien und den Anwendungsbereich für ein ISMS-Audit zu bestimmen, zu bewerten und zu bestätigen 7. Fähigkeit, die Merkmale der Bedingungen für den Auditauftrag zu erläutern, zu veranschaulichen und zu definieren und die besten Praktiken zur Herstellung des Erstkontakts mit einer auditierten Organisation anzuwenden	1. Kenntnis des Verfahrens zur Erstellung des Auditplans 2. Kenntnis des risikobasierten Auditansatzes und der verschiedenen Arten von Risiken im Zusammenhang mit Audittätigkeiten wie inhärentes Risiko, Kontrollrisiko und Entdeckungsrisiko 3. Kenntnis des Konzepts der Wesentlichkeit und seiner Anwendung auf ein Audit 4. Kenntnis des Konzepts der hinreichenden Sicherheit und seiner Anwendung auf das Audit. 5. Kenntnis der wichtigsten Verantwortlichkeiten der Leitung und der Mitglieder des Auditteams sowie der Fachexperten 6. Kenntnis der Ziele, des Anwendungsbereichs und der Kriterien des Audits 7. Kenntnis des Unterschieds zwischen dem Anwendungsbereich eines ISMS und dem eines Audits 8. Kenntnis der Faktoren, die bei der Durchführbarkeit des Audits zu berücksichtigen sind 9. Kenntnis der kulturellen Aspekte, die bei einem Audit zu berücksichtigen sind 10. Kenntnis der Merkmale der Bedingungen für den Auditauftrag und der besten Praktiken zur Herstellung des Erstkontakts mit einer auditierten Organisation

Bereich 5: Durchführung eines Audits nach ISO/IEC 27001

Hauptziel: Der Kandidat kann ein ISMS-Audit effizient durchführen

Kompetenzen	Kenntnisse
1. Fähigkeit, das Audit Stufe 1 unter Berücksichtigung der Bewertungskriterien der dokumentierten Information durchzuführen 2. Fähigkeit, eine Eröffnungsbesprechung zu organisieren und durchzuführen 3. Fähigkeit, das Audit Stufe 2 durch angemessenes Befolgen der für diese Stufe erforderlichen Verfahren durchzuführen 4. Fähigkeit, die besten Kommunikationspraktiken anzuwenden, um die geeigneten Auditnachweise zu sammeln 5. Fähigkeit, die Rollen und Verantwortlichkeiten aller beteiligten Parteien zu berücksichtigen 6. Fähigkeit, Verfahren und Instrumente zur Beweiserhebung zu erläutern, zu veranschaulichen und anzuwenden 7. Fähigkeit, die wichtigsten Stichprobenverfahren für Audits zu erläutern, zu veranschaulichen und anzuwenden 8. Fähigkeit, während eines Audits geeignetes Beweismaterial aus den verfügbaren Informationen zu sammeln und dieses objektiv zu bewerten 9. Fähigkeit, bei einem ISMS-Audit Arbeitspapiere zu erstellen und geeignete Audit-Testpläne auszuarbeiten 10. Fähigkeit, den Prozess der Beweisbewertung bei der Erstellung von Auditfeststellungen zu erläutern und anzuwenden 11. Fähigkeit, das Konzept des Vertrauensvorschusses zu verstehen, zu erklären und zu veranschaulichen 12. Fähigkeit, über angemessene Audit-Beobachtungen in Übereinstimmung mit den Audit-Regeln und -Prinzipien zu berichten 13. Fähigkeit, Qualitätsprüfungen der Auditdokumentation durchzuführen 14. Fähigkeit, Arbeitsunterlagen für Audits auszufüllen	1. Kenntnis der Ziele und des Inhalts der Eröffnungsbesprechung bei einem Audit 2. Kenntnis des Unterschieds zwischen einem Audit Stufe 1 und einem Audit Stufe 2 3. Kenntnis der Anforderungen, Schritte und Aktivitäten des Audits Stufe 1 4. Kenntnis der Bewertungskriterien für die dokumentierte Information und der Anforderungen der ISO/IEC 27001 5. Kenntnis der Anforderungen, Schritte und Aktivitäten des Audits Stufe 2 6. Kenntnis der besten Kommunikationspraktiken während eines Audits 7. Kenntnis der Rollen und Verantwortlichkeiten von Leitenden und Beobachtenden während eines Audits 8. Kenntnis der verschiedenen Konfliktlösungstechniken 9. Kenntnis der Verfahren und Instrumente zur Beweiserhebung wie Interview, Überprüfung der dokumentierten Information, Beobachtung, Analyse, Stichproben und technische Überprüfung 10. Kenntnis der Techniken der Beweisanalyse zur Bestätigung und Bewertung 11. Kenntnis der wichtigsten Konzepte, Prinzipien und Beweiserhebungsverfahren, die bei einem Audit verwendet werden 12. Kenntnis der Vor- und Nachteile der Verwendung von Audit-Checklisten 13. Kenntnis der wichtigsten Stichprobenverfahren und ihrer Merkmale 14. Kenntnis des Verfahrens zur Erstellung des Auditplans 15. Kenntnis der Erstellung und Entwicklung von Arbeitspapieren 16. Kenntnis der besten Praktiken für die Erstellung von Audit-Testplänen

	17. Kenntnis des Prozesses der Bewertung von Nachweisen für den Entwurf von Auditfeststellungen

Bereich 6: Abschluss eines Audits nach ISO/IEC 27001

Hauptziel: Der Kandidat kann ein ISMS abschließen und Audit-Folgetätigkeiten (Follow-up) durchführen

Kompetenzen	Kenntnisse
1. Fähigkeit, den Prozess der Beweisbewertung bei der Erstellung von Auditschlussfolgerungen zu erläutern und anzuwenden 2. Fähigkeit, die Empfehlung für die Zertifizierung zu begründen 3. Fähigkeit, Auditschlussfolgerungen zu erarbeiten und zu präsentieren 4. Fähigkeit, eine Abschlussbesprechung zu organisieren und durchzuführen 5. Fähigkeit, einen Auditbericht gemäß ISO/IEC 27001 zu verfassen und zu verteilen 6. Fähigkeit, Maßnahmenpläne zu bewerten	1. Kenntnis des Prozesses für die Bewertung von Nachweisen zur Vorbereitung von Auditschlussfolgerungen 2. Kenntnis der Präsentation von Auditschlussfolgerungen 3. Kenntnis der Leitlinien und besten Praktiken für die Präsentation von Auditschlussfolgerungen gegenüber der Leitung einer auditierten Organisation 4. Kenntnis der möglichen Empfehlungen, die ein Auditor während des Zertifizierungsaudits erteilen kann 5. Kenntnis der Tagesordnung der Abschlussbesprechung 6. Kenntnis der Leitlinien und besten Praktiken zur Bewertung von Maßnahmenplänen

Bereich 7: Steuerung eines Auditprogramms nach ISO/IEC 27001

Hauptziel: Der Kandidat versteht, wie man ein ISMS-Auditprogramm einrichtet und verwaltet

Kompetenzen	Kenntnisse
1. Fähigkeit, die Tätigkeiten im Anschluss an ein erstes Audit, einschließlich der Auditfolge- und -überwachungsmaßnahmen, durchzuführen 2. Fähigkeit, die Einrichtung eines Auditprogramms und die Anwendung des PDCA-Zyklus in einem Auditprogramm zu verstehen und zu erläutern 3. Fähigkeit, die Bedeutung des Schutzes der Integrität, der Verfügbarkeit und der Vertraulichkeit von Auditaufzeichnungen und die diesbezüglichen Verantwortlichkeiten der Auditoren zu verstehen und zu erläutern 4. Fähigkeit, die Verantwortlichkeiten für den Schutz der Integrität, der Verfügbarkeit und der Vertraulichkeit von Auditaufzeichnungen zu verstehen und zu erläutern 5. Fähigkeit, die Anforderungen im Zusammenhang mit den Komponenten des Managementsystems eines Auditprogramms, wie Qualitäts-, Aufzeichnungs- und Beschwerdemanagement, zu verstehen 6. Fähigkeit, die Handhabungsweise kombinierter Audits in einem Auditprogramm zu verstehen und zu erklären 7. Fähigkeit, den Managementprozess für die dokumentierte Information zu verstehen 8. Fähigkeit, den Prozess der Bewertung der Effizienz des Auditprogramms durch Überwachung der Leistung der einzelnen Auditoren und Audit-Teammitglieder zu verstehen 9. Fähigkeit, die persönlichen Eigenschaften und Verhaltensweisen einzusetzen, die von professionellen Auditoren erwartet werden	1. Kenntnis der Anforderungen, Schritte und Tätigkeiten von Auditfolgemaßnahmen, Überwachungsaudits und Re-Zertifizierungsaudits 2. Kenntnis der Bedingungen für die Änderung, Verlängerung, Aussetzung oder den Entzug der Zertifizierung einer Organisation 3. Kenntnis der Anwendung des PDCA-Zyklus bei der Verwaltung eines Auditprogramms 4. Kenntnis der Anforderungen, Leitlinien und besten Praktiken in Bezug auf Auditressourcen, -verfahren und -richtlinien 5. Kenntnis der von professionellen Auditoren eingesetzten Art von Instrumenten 6. Kenntnis der Anforderungen, Leitlinien und besten Praktiken für die Verwaltung von Auditaufzeichnungen 7. Kenntnis der Anwendung des Konzepts der fortlaufenden Verbesserung auf die Verwaltung eines Auditprogramms 8. Kenntnis der Besonderheiten bei der Umsetzung und Verwaltung eines Erst-, Zweit- oder Drittparteien-Auditprogramms Kenntnis des Kompetenzkonzepts und seiner Anwendung auf Auditoren 9. Kenntnis des Managements von kombinierten Audits 10. Kenntnis der persönlichen Eigenschaften und Verhaltensweisen eines professionellen Auditors

Auf Grundlage der oben genannten Bereiche und ihrer Relevanz enthält die Prüfung 80 Fragen, die in der nachstehenden Tabelle zusammengefasst sind:

				Erforderliche Verständnisebene (kognitiv/Taxonomie)	
		Anzahl der Fragen/Punkte pro Kompetenzbereich	Prozentualer Anteil der Fragen/Punkte pro Kompetenzbereich	Fragen der Kompetenzebene Verständnis, Anwendung und Analyse	Fragen der Kompetenzebene Synthese und Bewertung
Kompetenzbereiche	Grundlegende Prinzipien und Konzepte eines Informationssicherheitsmanagementsystems (ISMS)	13	16.25	X	
	Informationssicherheitsmanagementsystem (ISMS)	8	10	X	
	Grundlegende Prinzipien und Konzepte eines Audits	14	17.5		X
	Vorbereitung eines Audits nach ISO/IEC 27001	12	15	X	
	Durchführung eines Audits nach ISO/IEC 27001	18	22.5		X
	Abschluss eines Audits nach ISO/IEC 27001	7	8.75	X	
	Steuerung eines Auditprogramms nach ISO/IEC 27001	8	10		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 ISO/IEC 27001 Lead Auditor“ beantragen.

Die Prüfung ablegen

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 in Papierform) kann den Kandidaten, die die Prüfung in einer Fremdsprache ablegen, auf Antrag 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. **Schriftlich auf Papier:** Die Prüfungen werden in Papierform bereitgestellt. Die Kandidaten dürfen nichts anderes als das Prüfungspapier und einen Stift benutzen. 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 zum 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. Die Multiple-Choice-Prüfung kann dazu verwendet werden, das Verständnis eines Kandidaten zu vielen Themen zu bewerten, darunter sowohl einfache als auch komplexe Konzepte. Bei der Beantwortung dieser Fragen müssen die 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 Kandidaten lesen sollen, und es wird von ihnen erwartet, dass sie Antworten auf eine oder mehrere Fragen zu diesem Szenario geben. 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 Kandidaten die folgenden Referenzmaterialien verwenden:

- Ein gedrucktes Exemplar der Norm ISO/IEC 27001
- 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 schummeln, 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: 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). Alle PECB Multiple-Choice-Prüfungen bestehen aus einer Frage mit drei Antworten, von denen nur eine richtig ist..

Genauere Informationen über die Prüfungsarten, die verfügbaren Sprachen und andere Details finden Sie in der Liste der PECB-Prüfungen.

Beispiele für Prüfungsfragen

Unternehmen A ist eine Versicherungsgesellschaft mit Hauptsitz in Chicago. Es bietet eine Reihe von Dienstleistungen und Produkten im Bereich der Kranken- und Kfz-Versicherung an. Das Unternehmen hat sich in letzter Zeit zu einer der erfolgreichsten und größten Versicherungsgesellschaften mit mehr als 70 Niederlassungen im ganzen Land entwickelt.

Die Ziele des Unternehmens sind die ordnungsgemäße Verwaltung seiner Werte/Assets und der Schutz der Vertraulichkeit der Kundeninformationen. Das Unternehmen beschloss, sich nach ISO/IEC 27001 zertifizieren zu lassen, da es damit nicht nur seine organisatorischen Ziele erreichen und die internationalen Gesetze und Vorschriften einhalten, sondern auch seinen Ruf verbessern kann. Das Unternehmen leitete die Umsetzung des ISMS mit der Aufstellung einer entsprechenden Strategie ein, die auf einer detaillierten Analyse seiner bestehenden Prozesse und der ISMS-Anforderungen basierte. Besondere Aufmerksamkeit widmete das Unternehmen der Informationssicherheitsrisikobeurteilung, die für das Verstehen der Bedrohungen und Schwachstellen, denen es ausgesetzt war, von entscheidender Bedeutung war. Es wurden auch Risikokriterien festgelegt, um die identifizierten Risiken bewerten zu können.

Unternehmen A erlebte ein schnelles Wachstum, das zu einer komplexen und intensiven Datenverarbeitung führte. Auf der Grundlage der Ergebnisse der Risikobeurteilung beschloss es, zunächst sein bestehendes Informationsklassifizierungsschema zu aktualisieren und dann die erforderlichen Sicherheitsmaßnahmen auf der Grundlage des für jede Informationsklassifizierung erforderlichen Schutzniveaus umzusetzen.

Die als sensibel eingestuften medizinischen Daten seiner Kunden wurden mit der AES-Verschlüsselung verschlüsselt und dann in die private Cloud verschoben. *Unternehmen A* nutzte den Cloud-Speicher wegen seines einfachen Zugriffs. Aufgrund des häufigen Zugriffs seiner Mitarbeiter auf diesen Dienst beschloss das Unternehmen darüber hinaus, den Protokollierungsprozess zu nutzen. Der Dienst wurde so konfiguriert, dass alle für die Bearbeitung medizinischer Ansprüche zuständigen Beschäftigten automatisch Zugriff auf den Cloud-Speicher erhalten.

Da es bei den Cloud-Speicherdiensten zu Sicherheitsverletzungen kam, die entweder auf menschliches Versagen oder auf absichtliche Angriffe zurückzuführen waren, beschloss die IT-Abteilung des Unternehmens, den Zugriff auf die in der Cloud gespeicherten sensiblen Daten einzuschränken, wenn keine Geschäfts-E-Mails verwendet wurden. Darüber hinaus wurde eine Passwort-Manager-Software eingesetzt, um die Passwörter dieser E-Mail-Adressen zu verwalten und sicherere Passwörter zu generieren.

Beantworten Sie anhand dieses Szenarios die folgenden Fragen:

1. **Die IT-Abteilung hat den Zugriff auf den Cloud-Speicher nicht eingeschränkt. Welche der folgenden Bedrohungen kann eine solche Schwachstelle ausnutzen?**
   A. Manipulationen an der Hardware
   B. **Unbefugte Nutzung sensibler Informationen**
   C. Unzureichende Schulung für Cloud-Speicher

2. ***Unternehmen A* verschlüsselt sensible Daten, bevor es sie in die Cloud verschiebt. Welches Prinzip der Informationssicherheit wird in diesem Fall befolgt?**
   A. **Vertraulichkeit, da die Verschlüsselung sicherstellt, dass nur autorisierte Benutzer auf die verschlüsselten Informationen zugreifen können**
   B. Verfügbarkeit, da durch die Verschlüsselung sichergestellt wird, dass die Informationen entweder im Ruhezustand oder während der Übertragung gesichert und somit bei Bedarf zugänglich sind
   C. Integrität, da die Verschlüsselung sicherstellt, dass nur autorisierte Personen Änderungen an den verschlüsselten Informationen vornehmen können

3. ***Unternehmen A* hat beschlossen, den Zugang zu sensiblen Informationen, die in der Cloud gespeichert sind, einzuschränken, wenn keine geschäftlichen E-Mails verwendet werden. Welche Sicherheitsmaßnahme wurde in diesem Fall umgesetzt?**
   A. Detektive Maßnahme
   B. **Präventive Maßnahme**
   C. Korrektive Maßnahme

4. ***Unternehmen A* hat die Risikokriterien bei der Beurteilung seiner Risiken festgelegt. Ist dies notwendig?**
   A. **Ja, denn das Unternehmen sollte die Risikokriterien bei der Beurteilung der Informationssicherheitsrisiken festlegen und beibehalten.**
   B. Nein, denn die Risikokriterien sollten erst festgelegt werden, wenn die Optionen für die Risikobehandlung definiert sind
   C. Nein, denn die Risikokriterien werden festgelegt, wenn die Restrisiken der Informationssicherheit akzeptiert werden.

Erhalt der Prüfungsergebnisse

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 Online-Multiple-Choice-Prüfungen erhalten die Kandidaten ihre Ergebnisse sofort.

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

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 Kandidaten können eine Prüfung beliebig oft wiederholen. 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 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. Die Planung für die Wiederholungsprüfung verläuft so wie bei der Erstprüfung.

Geheimhaltung der Prüfungsinhalte (Exam Security)

Ein wichtiger Teil eines professionellen Zertifizierungsnachweises ist die Gewährleistung der Sicherheit und Vertraulichkeit der Prüfung. Die PECB vertraut auf das ethische Verhalten der Inhaber und Antragsteller von Zertifizierungen, um die Sicherheit und Vertraulichkeit der PECB-Prüfungen zu erhalten. Jegliche Weitergabe von Informationen über PECB-Prüfungsinhalte stellt einen direkten Verstoß gegen den Verhaltenskodex 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

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

Antrag auf Zertifizierung

Alle 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 Bildungs- und Berufsanforderungen erfüllt werden. Die Kandidaten müssen das Online-Zertifizierungsantragsformular ausfüllen (das über ihr PECB-Online-Profil aufgerufen werden kann), wozu die Kontaktdaten von Referenzpersonen gehören, die die Berufserfahrung des Kandidaten bestätigen können. Die Kandidaten können ihren Antrag in verschiedenen Sprachen einreichen. Die Kandidaten können wählen, ob sie online oder per Rechnung bezahlen möchten. Für weitere Informationen wenden Sie sich bitte an certification.team@pecb.com.

Die Online-Beantragung der Zertifizierung ist sehr einfach und nimmt nur wenige Minuten in Anspruch. Dazu:

- Registrieren
- Prüfen Sie Ihre E-Mail auf den Bestätigungslink
- Anmelden und Zertifizierung beantragen

Für weitere Informationen zum Antragsverfahren folgen Sie den Anweisungen in der Anleitung Antrag auf Zertifizierung.

Der Antrag wird genehmigt, sobald die Zertifizierungsabteilung bestätigt hat, dass der Kandidat alle Zertifizierungsanforderungen für den jeweiligen Berechtigungsnachweis erfüllt. 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 sie aufrechtzuerhalten, müssen die Kandidaten jedes Jahr nachweisen, dass sie immer noch zertifizierungsrelevante Aufgaben ausführen. PECB-zertifizierte Fachkräfte müssen jährlich Credits (Fortbildungspunkte) für die Continuous Professional Development (berufliche Weiterbildung, CPD) erbringen und 100 Dollar als Annual Maintenance Fee (Jahresgebühr, AMF) zahlen, um die Zertifizierung aufrechtzuerhalten. Weitere Informationen finden Sie auf der Seite zur Aufrechterhaltung der Zertifizierung auf der PECB-Website.

Schließen eines Falles

Wenn die Kandidaten innerhalb von drei Jahren keinen Antrag auf Zertifizierung stellen, wird ihr Fall geschlossen. Auch nach Ablauf des Zertifizierungszeitraums haben die Kandidaten das Recht, ihren Fall wieder aufzunehmen. 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. Ein Kandidat muss die Wiederaufnahme seines Falles schriftlich beantragen und die erforderliche Gebühr entrichten.

ABSCHNITT III: ZERTIFIZIERUNGSANFORDERUNGEN

ISO/IEC 27001 Lead Auditor

Die Anforderungen an die Zertifizierung als PECB ISO/IEC 27001 Auditor sind:

Berechtigungsnachweis	Prüfung	Berufliche Erfahrung	MS Audit- bzw. Beurteilungserfahrung	Sonstige Anforderungen
PECB Certified ISO/IEC 27001 Provisional Auditor	PECB Certified ISO/IEC 27001 Lead Auditor, Prüfung oder gleichwertig	Keine	Keine	Unterzeichnung des PECB-Ethikkodexes
PECB Certified ISO/IEC 27001 Auditor	PECB Certified ISO/IEC 27001 Lead Auditor, Prüfung oder gleichwertig	Zwei Jahre: Ein Jahr Berufserfahrung im Bereich Informationssicherheitsmanagement	Auditaktivitäten: insgesamt 200 Stunden	Unterzeichnung des PECB Verhaltenskodex
PECB Certified ISO/IEC 27001 Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor Prüfung oder gleichwertig	Fünf Jahre: Zwei Jahre Berufserfahrung im Bereich Informationssicherheitsmanagement	Auditaktivitäten: insgesamt 300 Stunden	Unterzeichnung des PECB Verhaltenskodex
PECB Certified ISO/IEC 27001 Senior Lead Auditor	PECB Certified ISO/IEC 27001 Lead Auditor Prüfung oder gleichwertig	Zehn Jahre: Sieben Jahre Berufserfahrung im Bereich Informationssicherheitsmanagement	Auditaktivitäten: insgesamt 1000 Stunden	Unterzeichnung des PECB Verhaltenskodex

Gültig sind solche Audittätigkeiten, die bewährten Auditpraktiken folgen und Folgendes beinhalten sollten:
1. Planung eines Audits
2. Verwaltung eines Auditprogramms
3. Erstellung von Auditberichten
4. Erstellung von Berichten über Nichtkonformitäten
5. Erstellung von Arbeitsunterlagen für das Audit
6. Überprüfung der dokumentierten Information
7. Vor-Ort-Audit
8. Folgemaßnahmen zu Nichtkonformitäten
9. Leitung eines Auditteams

ABSCHNITT IV: ZERTIFIZIERUNGSREGELN UND -RICHTLINIEN

Berufliche Referenzen

Für jede Bewerbung 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 Informationssicherheitsmanagements sowie seinen derzeitigen und früheren beruflichen Werdegang bestätigen können. Berufliche Referenzen von Personen, die unter der Aufsicht des Kandidaten stehen oder mit ihm verwandt sind, sind nicht gültig.

Berufserfahrung

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.

ISMS-Auditerfahrung

Das Auditprotokoll des Kandidaten wird daraufhin überprüft, dass er die erforderliche Anzahl von Auditstunden absolviert hat. Die folgenden Arten von Audits gelten als gültige Auditerfahrung: Vor-Audit, interne Audits, Zweitparteien-Audits, Drittparteien-Audits oder Stellungnahme-Audits.

Bewertung von Zertifizierungsanträgen

Die Zertifizierungsabteilung prüft jeden Antrag, um festzustellen, ob der Kandidat alle Voraussetzungen für die Zertifizierung erfüllt hat. Ein Kandidat wird über die Prüfung seines Antrags schriftlich benachrichtigt und erhält, falls erforderlich, eine angemessene Frist, um zusätzliche Unterlagen beizubringen. 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.

Verweigerung der Zertifizierung

Die PECB kann die Zertifizierung verweigern, wenn Kandidaten:

- Den Antrag fälschen
- Gegen die Prüfungsordnung verstoßen
- Verstoß gegen den PECB-Ethikkodex
- 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, wenn der Kandidat die Anforderungen nicht erfüllt. 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 versäumt es, den Missbrauch einer Zertifizierungsmarke innerhalb des von der PECB festgelegten Zeitrahmens zu korrigieren.
- Die zertifizierte Person hat freiwillig 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 der Kandidat die Anforderungen der PECB nicht erfüllt. Der Kandidat darf sich dann nicht mehr als PECB-zertifizierte Fachkraft ausgeben. Weitere Gründe für den Entzug der Zertifizierung können sein, wenn Kandidaten:

- Verstoß gegen den PECB-Ethikkodex
- Den Anwendungsbereich der Zertifizierung falsch darstellen und falsche Angaben machen
- Gegen andere PECB-Regeln verstoßen

Höherstufung von Berechtigungsnachweisen

Fachkräfte können eine Höherstufung des Berechtigungsnachweis beantragen, sobald sie nachweisen können, dass sie die Anforderungen erfüllen.

Für die Beantragung einer Höherstufung müssen sich die Kandidaten an ihrem PECB-Konto anmelden und auf der Registerkarte „My Certifications“ (Meine Zertifizierungen) den Link „Upgrade“ (Höherstufung) klicken. Die Gebühr für den Höherstufungsantrag 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-zertifizierten Fachkräften mit einer Lead-Zertifizierung, die die Erfüllung der Anforderungen für die Aufrechterhaltung der Zertifizierung nicht nachweisen können, wird der Berechtigungsnachweis herabgestuft. Dahingegen wird Inhabern von Master-Zertifizierungen, die es versäumen, CPDs einzureichen und AMFs zu zahlen, ihre Zertifizierung entzogen.*

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 endgültigen Einstellung der Tätigkeit 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-zertifizierte Fachkräfte nicht nur an die Grundsätze dieses Kodex halten, sondern auch andere dazu ermutigen und dabei unterstützen. 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 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 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 treffen kann. Alle von den Kandidaten gemachten Angaben zu ihren Behinderungen/Bedürfnissen werden streng vertraulich behandelt.

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

Beschwerden und Einsprüche

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, hat der Kandidat das Recht, Einspruch einzulegen. Weitere Informationen über das Beschwerde- und Einspruchsverfahren finden Sie hier.

(1) Gemäß ADA kann der Begriff "angemessene Vorkehrungen" Folgendes umfassen: (A) vorhandene Einrichtungen, die von Beschäftigten genutzt werden, für Menschen mit Behinderungen leicht zugänglich und nutzbar machen; und (B) die Umstrukturierung von Arbeitsplätzen, Teilzeitarbeit oder geänderte Arbeitszeiten, die Umsetzung auf einen leidensgerechten Arbeitsplatz, die Anschaffung oder Änderung von Geräten oder Ausrüstungen, 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, 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:
Headquarters
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: customer@pecb.com