PECB BEYOND RECOGNITION

# Kandidaten-Handbuch

## ISO/IEC 27001 LEAD IMPLEMENTER

PECB

# Inhaltsverzeichnis

# ABSCHNITT I: Einleitung

## 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. Unsere Aufgabe ist es, Dienstleistungen zu erbringen, die Vertrauen schaffen, zu ständiger Verbesserung führen, Anerkennung bringen und der Gesellschaft als Ganzes zugute kommen.

**Zu den Hauptzielen der PECB gehören:**

1. Festlegung der für die Zertifizierung von Fachleuten erforderlichen Mindestanforderungen
2. Überprüfung und Verifizierung der Qualifikationen von Bewerbern, um sicherzustellen, dass sie für die Zertifizierung in Frage kommen
3. Entwicklung und Aufrechterhaltung zuverlässiger Zertifizierungsbewertungen
4. Erteilung von Zertifizierungen an qualifizierte Kandidaten, Führung von Aufzeichnungen und Veröffentlichung eines Verzeichnisses der Inhaber einer gültigen Zertifizierung
5. Aufstellung von Anforderungen für die regelmäßige Erneuerung der Zertifizierung und Sicherstellung der Einhaltung dieser Anforderungen
6. Sicherstellung, dass die Kandidaten ethische Normen in ihrer beruflichen Praxis einhalten
7. Vertretung der Mitglieder in Fragen von gemeinsamem Interesse, wo dies angebracht ist
8. Förderung der Vorteile der Zertifizierung bei Organisationen, Arbeitgebern, Behörden, Fachleuten in ähnlichen Bereichen und der Öffentlichkeit

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

## Der Wert der PECB-Zertifizierung

**Warum sollten Sie sich für die PECB als Ihre Zertifizierungsstelle entscheiden?**

### 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 Fachleute, 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, Wichtigkeit, Professionalität und Ehrlichkeit. Die PECB verfügt über ein Expertenteam, das sich um Kundenanfragen, Probleme, Sorgen, Bedürfnisse und Meinungen kümmert. Wir tun unser Bestes, um eine maximale Reaktionszeit von 24 Stunden einzuhalten, ohne die Qualität der Dienstleistung zu beeinträchtigen.

## PECB-Ethikkodex

**PECB-Fachkräfte werden:**

1. sich professionell, mit Ehrlichkeit, Genauigkeit, Fairness, Verantwortung und Unabhängigkeit verhalten.
2. Jederzeit ausschließlich im besten Interesse ihres Arbeitgebers, ihrer Kunden, der Öffentlichkeit und des Berufsstandes handeln, indem sie sich bei der Erbringung professioneller Dienstleistungen an die professionellen Normen und anwendbaren Techniken halten
3. Ihre Kompetenz in ihrem jeweiligen Fachgebiet aufrechterhalten und sich bemühen, ihre beruflichen Fähigkeiten ständig zu verbessern
4. Nur professionelle Dienstleistungen anbieten, für deren Erbringung sie qualifiziert sind, und die Kunden angemessen über die Art der vorgeschlagenen Dienstleistungen, einschließlich aller relevanten Bedenken oder Risiken, informieren
5. Jeden Arbeitgeber oder Kunden über alle geschäftlichen Interessen oder Verbindungen zu informieren, die ihr Urteilsvermögen beeinflussen oder ihre Fairness beeinträchtigen könnten
6. Informationen, die sie im Rahmen des beruflichen und geschäftlichen Umgangs mit derzeitigen oder früheren Arbeitgebern oder Kunden erhalten haben, vertraulich und privat zu behandeln
7. alle Gesetze und Vorschriften der Länder einhalten, in denen die berufliche Tätigkeit ausgeübt wird
8. Das intellektuelle Eigentum und die Beiträge anderer zu respektieren
9. weder absichtlich noch anderweitig falsche oder gefälschte Informationen weitergeben, die die Integrität des Beurteilungsprozesses eines Kandidaten für eine Berufsbezeichnung beeinträchtigen könnten
10. Nicht in einer Weise zu handeln, die den Ruf der PECB oder ihrer Zertifizierungsprogramme beeinträchtigen könnte
11. Bei der Untersuchung eines behaupteten Verstoßes gegen diesen Ethikkodex uneingeschränkt zu kooperieren

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

## Einführung in ISO/IEC 27001 Lead Implementer

ISO/IEC 27001 legt die Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) fest. Die wichtigsten auf dem Markt geforderten Fähigkeiten sind die Fähigkeit, das ISMS effektiv zu planen, zu implementieren und zu verwalten, die Informationssicherheitsrisiken zu bewerten und zu behandeln, die Informationssicherheitskontrollen auszuwählen und zu implementieren und die ISMS-Implementierungsteams zu leiten (oder ihnen anzugehören).

Die Zertifizierung „ISO/IEC 27001 Lead Implementer" ist eine professionelle Zertifizierung für Personen, die ihre Kompetenz zur Implementierung eines Informationssicherheitsmanagementsystems und zur Leitung eines ISMS-Implementierungsteams nachweisen wollen.

Da die Implementierung 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 die PECB-Zertifizierungen keine Lizenz oder einfache Mitgliedschaften sind. Sie stellen eine Anerkennung durch Gleichrangige dar, dass eine Person ihre Fähigkeiten und ihr Verständnis für eine Reihe von Kompetenzen nachgewiesen hat. PECB-Zertifizierungen werden an Kandidaten vergeben, die Erfahrung nachweisen können und eine standardisierte Prüfung im Zertifizierungsbereich bestanden haben.

Dieses Dokument spezifiziert das PECB ISO/IEC 27001 Lead Implementer Zertifizierungsprogramm in Übereinstimmung mit ISO/IEC 17024:2012. Dieses Kandidatenhandbuch enthält auch Informationen über das Verfahren, mit dem Kandidaten ihre Berechtigungsnachweise erwerben und aufrechterhalten können. 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 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

## Entscheiden Sie, welche Zertifizierung die richtige für Sie ist

Alle PECB-Zertifizierungen erfordern eine bestimmte Ausbildung und Berufserfahrung. Prüfen Sie die Zulassungskriterien für die verschiedenen Zertifizierungen und Ihre beruflichen Anforderungen, um den für Sie richtigen Nachweis zu finden.

## Vorbereitung und Terminierung der Prüfung

Alle Kandidaten sind für ihr eigenes Lernen und ihre Vorbereitung auf die Zertifizierungsprüfungen verantwortlich. Für den Zertifizierungsprozess ist keine bestimmte Anzahl von Schulungen oder Studienplänen erforderlich. Dennoch kann die Teilnahme an einer Schulung die Aussichten der Kandidaten auf ein erfolgreiches Bestehen der PECB-Prüfung erheblich erhöhen.

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

1. Sie können sich an einen unserer Partner wenden, der Schulungen und Prüfungssitzungen anbietet. Um einen Schulungsanbieter in einer bestimmten Region zu finden, sollten sich die Kandidaten an die Seite Active Partnerswenden. Der Zeitplan für die PECB-Schulungen ist auch unter Schulungsveranstaltungenverfügbar
2. Eine PECB-Prüfung über die PECB-Prüfungsanwendung, auf die Sie hier zugreifen können, von zu Hause aus oder von jedem beliebigen Ort aus ablegen: Prüfung Veranstaltungen..

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 die Prüfung ablegen kann, ohne die Schulung zu besuchen. Die entsprechenden Preise sind wie folgt:

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

Die Antragsgebühr für die Zertifizierung beträgt 500 Dollar.

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

## Kompetenzbereiche

Das Ziel der „PECB ISO/IEC 27001 Lead Implementer"-Prüfung ist es, sicherzustellen, dass der Kandidat die notwendigen Kompetenzen erworben hat, um eine Organisation bei der Einrichtung, Implementierung, Verwaltung und Aufrechterhaltung des Informationssicherheits-Managementsystems (ISMS) auf der Grundlage der ISO/IEC 27001-Anforderungen zu unterstützen.

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

- Manager oder Berater, die an der Implementierung eines Informationssicherheits-Managementsystems in einer Organisation beteiligt und damit befasst sind
- Projektleiter, Berater oder Fachberater, die die Implementierung eines Informationssicherheits-Managementsystems beherrschen wollen
- Personen, die für die Aufrechterhaltung der Konformität mit den Anforderungen der ISO/IEC 27001 in einer Organisation verantwortlich sind
- Mitglieder eines ISMS-Implementierungsteams

Die Prüfung umfasst die folgenden Kompetenzbereiche:

- **Bereich 1:** Grundlegende Konzepte und Prinzipien eines Informationssicherheitsmanagementsystems (ISMS)
- **Bereich 2:** Informationssicherheitsmanagementsystem (ISMS)
- **Bereich 3:** Planung einer ISMS-Implementierung auf der Grundlage von ISO/IEC 27001
- **Bereich 4:** Implementierung eines ISMS auf der Grundlage von ISO/IEC 27001
- **Bereich 5:** Überwachung und Messung eines ISMS auf der Grundlage von ISO/IEC 27001
- **Bereich 6:** Kontinuierliche Verbesserung eines ISMS auf der Grundlage von ISO/IEC 27001
- **Bereich 7:** Vorbereitung auf ein ISMS-Zertifizierungsaudit

PECB

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

**Hauptziel:** Sicherstellen, dass der Kandidat die Konzepte und Prinzipien von ISO/IEC 27001 versteht und interpretieren kann

| Kompetenzen | Wissenserklärungen |
|---|---|
| 1. Fähigkeit, die wichtigsten Konzepte der Informationssicherheit zu verstehen und zu erläutern<br>2. Fähigkeit, den Unterschied und die Beziehung zwischen Informationen und Vermögenswerten zu erklären<br>3. Fähigkeit, den Unterschied zwischen Dokumenten, Spezifikationen und Aufzeichnungen zu verstehen<br>4. Fähigkeit, die Beziehung zwischen den Konzepten von Schwachstelle, Bedrohung und Risiko sowie deren Auswirkungen zu verstehen<br>5. Fähigkeit, die Konzepte der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu verstehen<br>6. Fähigkeit, die Klassifizierung von Sicherheitskontrollen und deren Ziele zu verstehen und zu interpretieren<br>7. Fähigkeit, die Beziehung zwischen den Elementen der Informationssicherheit zu verstehen | 1. Kenntnisse über die Gesetze, Vorschriften, internationalen und branchenüblichen Normen, Verträge, Marktpraktiken, internen Richtlinien, bewährten Verfahren usw., die ein Unternehmen einhalten muss<br>2. Kenntnisse über die wichtigsten Konzepte und die Terminologie von ISO/IEC 27001<br>3. Kenntnisse über Informationssicherheitsrisiken und deren Bedeutung in einem ISMS<br>4. Kenntnisse über die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen<br>5. Kenntnisse über Schwachstellen, Bedrohungen und Risiken der Informationssicherheit<br>6. Kenntnisse über die potenziellen Auswirkungen, die die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen beeinträchtigen können<br>7. Kenntnisse über den Unterschied zwischen verschiedenen Arten von Sicherheitskontrollen wie z. B. technische, rechtliche, administrative und verwaltungstechnische Kontrollen<br>8. Kenntnisse über den Unterschied zwischen Sicherheitskontrollen, die nach ihrer Funktion klassifiziert werden, wie z. B. präventive, korrektive und aufdeckende Kontrollen |

PECB

## Bereich 2: Informationssicherheitsmanagementsystem (ISMS)

**Hauptziel:** Sicherstellen, dass der Kandidat die in Anhang A der ISO/IEC 27001 aufgeführten Sicherheitskontrollen versteht und in der Lage ist, diese umzusetzen

| Kompetenzen | Wissenserklärungen |
|---|---|
| 1. Fähigkeit zur Auswahl, Gestaltung und Beschreibung von Informationssicherheitskontrollen<br>2. Fähigkeit, die Sicherheitsarchitektur der Organisation zu definieren<br>3. Fähigkeit, die mit der Entwicklung und dem Einsatz von Informationssystemen verbundenen Aktivitäten zu identifizieren und zu erläutern<br>4. Fähigkeit, die Implementierung ausgewählter Informationssicherheitskontrollen zu dokumentieren<br>5. Fähigkeit zum Verstehen, Interpretieren und Analysieren der Kontrollen in Anhang A der ISO/IEC 27001<br>6. Fähigkeit zur Implementierung von Anhang-A-Kontrollen auf der Grundlage von ISO/IEC 27001 und bewährten Praktiken | 1. Kenntnisse über gängige Sicherheitsdienste wie z. B. Zugangskontrolldienste, Abgrenzungskontrolldienste, Integritätsdienste, kryptografische Dienste sowie Audit- und Überwachungsdienste<br>2. Kenntnisse über die gängigsten Architekturrahmenwerke<br>3. Kenntnisse der 93 Kontrollen in Anhang A der ISO/IEC 27001<br>4. Kenntnisse über die vier Gruppen von Anhang-A-Kontrollen wie organisatorische Kontrollen, Personenkontrollen, physische Kontrollen, technologische Kontrollen<br>5. Kenntnisse über die Auswahl und Implementierung von Kontrollen nach Anhang A der ISO/IEC 27001<br>6. Kenntnisse über die Dokumentation der ausgewählten Informationssicherheitskontrollen |

PECB

## Bereich 3: Planung einer ISMS-Implementierung auf der Grundlage von ISO/IEC 27001

**Hauptziel:** Sicherstellen, dass der Kandidat in der Lage ist, die Implementierung des ISMS auf der Grundlage von ISO/IEC 27001 zu planen

### Kompetenzen

1. Fähigkeit, die für die Planung einer ISMS-Implementierung erforderlichen Informationen zu sammeln, zu analysieren und zu interpretieren
2. Fähigkeit, Ziele der Informationssicherheit und des ISMS zu verstehen und festzulegen
3. Fähigkeit, ISMS-Risiken und deren Auswirkungen zu erkennen und zu interpretieren
4. Fähigkeit, den internen und externen Kontext einer Organisation zu analysieren und zu berücksichtigen
5. Fähigkeit, die für die Implementierung des ISMS erforderlichen Ressourcen zu identifizieren
6. Fähigkeit, die für die Implementierung des ISMS erforderlichen Ressourcen zu verwalten, abzuschätzen und zu überwachen
7. Fähigkeit, die Rollen und Verantwortlichkeiten der wichtigsten interessierten Parteien während und nach der Implementierung und dem Betrieb eines ISMS zu identifizieren
8. Fähigkeit, einen ISMS-Projektplan zu entwerfen, abzulegen und zu überprüfen
9. Fähigkeit, eine Gap-Analyse durchzuführen und die Ziele des Informationssicherheitsmanagements zu klären
10. Fähigkeit, einen Anwendungsbereich des ISMS zu definieren und zu begründen, der an die spezifischen Informationssicherheitsziele der Organisation angepasst ist
11. Fähigkeit, eine ISMS-Richtlinie zu entwickeln und einzuführen
12. Fähigkeit, die verschiedenen Schritte des Risikobeurteilungsprozesses durchzuführen
13. Fähigkeit, das Dokument zur Erklärung der Anwendbarkeit zu verstehen und zu verfassen

### Wissenserklärungen

1. Kenntnisse über die wichtigsten Projektmanagementkonzepte, Terminologie, Prozesse und bewährte Praktiken
2. Kenntnisse über die wichtigsten Ansätze und Methoden zur Implementierung eines ISMS
3. Kenntnisse typischer Informationssicherheits- und ISMS-Ziele und der Erreichung spezifischer Ergebnisse
4. Kenntnisse darüber, was typischerweise den internen und externen Kontext einer Organisation ausmacht
5. Kenntnisse über die Ansätze zum Verstehen des Kontexts einer Organisation
6. Kenntnisse der Methoden, die zur Sammlung von Informationen über eine Organisation und zur Durchführung einer Gap-Analyse eines Managementsystems verwendet werden
7. Kenntnisse über einen ISMS-Projektplan und ein ISMS-Projektteam
8. Kenntnisse über die für eine ISMS-Implementierung erforderlichen Ressourcen
9. Kenntnisse über die wichtigsten Organisationsstrukturen, die für die Verwaltung eines ISMS in einer Organisation anwendbar sind
10. Kenntnisse über die Merkmale eines ISMS-Anwendungsbereichs in Bezug auf die organisatorischen, technologischen und physischen Grenzen
11. Kenntnisse über die bewährten Praktiken und Techniken zur Ausarbeitung und Einführung von Strategien und Verfahren für die Informationssicherheit
12. Kenntnisse über die verschiedenen Ansätze und Methoden zur Durchführung der Risikobeurteilung
13. Kenntnisse über die Merkmale des Dokuments zur Anwendbarkeitserklärung

PECB

| Bereich 4: Implementierung eines ISMS auf der Grundlage von ISO/IEC 27001<br><br>**Hauptziel:** Sicherstellen, dass der Kandidat in der Lage ist, ein ISMS auf der Grundlage der Anforderungen von ISO/IEC 27001 implementieren zu können | |
|---|---|
| **Kompetenzen** | **Wissenserklärungen** |
| 1. Fähigkeit, Prozesse zum Aufbau von Kapazitäten für die erfolgreiche Implementierung eines ISMS zu managen<br>2. Fähigkeit, die zur Unterstützung der Implementierung und des Betriebs eines ISMS erforderlichen Dokumentations- und Aufzeichnungsprozesse zu definieren<br>3. Fähigkeit, die für den Betrieb eines ISMS erforderlichen Prozesse zu definieren, zu entwerfen und zu implementieren und sie ordnungsgemäß zu dokumentieren<br>4. Fähigkeit, organisatorisches Wissen zu verstehen, zu verwalten und zu bewerten<br>5. Fähigkeit, die aktuellen Trends und Technologien wie Big Data, künstliche Intelligenz, maschinelles Lernen, Cloud Computing und ausgegliederte Tätigkeiten zu verstehen<br>6. Fähigkeit zur Definition und Implementierung geeigneter Schulungs- und Bewusstseinsprogramme für Informationssicherheit sowie von Kommunikationsplänen<br>7. Fähigkeit, einen ISMS-Kommunikationsplan zu erstellen, um das Verständnis der Informationssicherheitsprobleme, -richtlinien und -leistung einer Organisation zu fördern und Beiträge oder Vorschläge zur Verbesserung der Leistung des ISMS zu liefern<br>8. Fähigkeit, eine Strategie für das Management von Vorfällen und ein Team für die Reaktion auf Vorfälle einzurichten<br>9. Fähigkeit, den Unterschied zwischen Geschäftskontinuität und Notfallwiederherstellung (Disaster recovery) zu verstehen | 1. Kenntnisse über die bewährten Praktiken für das Management des Lebenszyklus dokumentierter Informationen<br>2. Kenntnisse über die Merkmale und die Unterschiede zwischen den verschiedenen dokumentierten Informationen im Zusammenhang mit einer ISMS-Richtlinie, einem Verfahren, einer Leitlinie, einer Norm, einem Basisplan, einem Arbeitsblatt usw.<br>3. Kenntnisse über die drei V's von Big Data: Volume (Datenvolumen), Variety (Datenvielfalt) und Velocity (Datengeschwindigkeit).<br>4. Kenntnisse über schwache und starke künstliche Intelligenz, maschinelles Lernen<br>5. Kenntnisse über Cloud-Computing-Dienste: Infrastruktur als Dienst (IaaS), Plattform als Dienst (PaaS) und Software als Dienst (SaaS)<br>6. Kenntnisse über die Auswirkungen neuer Technologien auf die Informationssicherheit<br>7. Kenntnisse über die Merkmale und die bewährten Praktiken bei der Implementierung von Programmen zur Schulung und Bewusstseinsbildung im Bereich der Informationssicherheit sowie von Kommunikationsplänen<br>8. Kenntnisse über die Kommunikationsziele, Aktivitäten und interessierten Parteien, um deren Unterstützung und Vertrauen zu stärken<br>9. Kenntnisse über den Prozess des Vorfallsmanagements auf der Grundlage bewährter Praktiken der Informationssicherheit<br>10. Kenntnisse über Geschäftskontinuität und Disaster Recovery |

PECB

| Bereich 5: Überwachung und Messung eines ISMS auf der Grundlage von ISO/IEC 27001<br><br>**Hauptziel:** Sicherstellen, dass der Kandidat in der Lage ist, die Leistung eines ISMS zu analysieren, zu bewerten, zu überwachen und zu messen | |
|---|---|
| **Kompetenzen** | **Wissenserklärungen** |
| 1. Fähigkeit zur Überwachung und Bewertung der Wirksamkeit eines ISMS<br>2. Fähigkeit, festzustellen, in welchem Maße die festgelegten ISMS-Ziele erreicht wurden<br>3. Fähigkeit, ein internes ISMS-Auditprogramm zu definieren und implementieren<br>4. Fähigkeit zur Durchführung regelmäßiger und methodischer Überprüfungen, um die Eignung, Angemessenheit, Wirksamkeit und Effizienz eines ISMS auf der Grundlage der Richtlinien und Ziele der Organisation sicherzustellen<br>5. Fähigkeit, einen Management-Review-Prozess zu definieren und durchzuführen | 1. Kenntnisse über die bewährten Praktiken und Techniken zur Überwachung und Bewertung der Wirksamkeit eines ISMS<br>2. Kenntnisse der Konzepte im Zusammenhang mit der Messung und Bewertung<br>3. Kenntnisse über die wichtigsten Konzepte und Komponenten im Zusammenhang mit der Implementierung und Durchführung eines internen ISMS-Auditprogramms<br>4. Kenntnisse über den Unterschied zwischen einer größeren und einer kleineren Nichtkonformität<br>5. Kenntnisse über die Leitlinien und bewährten Praktiken für die Erstellung eines Nichtkonformitätsberichts<br>6. Kenntnisse über die bewährten Praktiken zur Durchführung von Managementbewertungen |

## Bereich 6: Kontinuierliche Verbesserung eines ISMS auf der Grundlage von ISO/IEC 27001

**Hauptziel:** Sicherstellen, dass der Kandidat in der Lage ist, Anleitungen für die kontinuierliche Verbesserung eines ISMS zu geben

| Kompetenzen | Wissenserklärungen |
|---|---|
| 1. Fähigkeit, Nichtkonformitäten zu verfolgen und entsprechende Maßnahmen zu ergreifen<br>2. Fähigkeit, die Ursachen von Nichtkonformitäten zu ermitteln und zu analysieren und Maßnahmenpläne zu deren Behebung vorzuschlagen<br>3. Fähigkeit, eine Organisation zu beraten, wie die Wirksamkeit und Effizienz eines ISMS kontinuierlich verbessert werden kann<br>4. Fähigkeit zur Implementierung von kontinuierlichen Verbesserungsprozessen in einer Organisation<br>5. Fähigkeit, die geeigneten Instrumente zur Unterstützung der kontinuierlichen Verbesserungsprozesse einer Organisation zu bestimmen | 1. Kenntnisse über die wichtigsten Verfahren, Instrumente und Techniken zur Ermittlung der Ursachen von Nichtkonformitäten<br>2. Kenntnisse über den Prozess der Behandlung von Nichtkonformitäten<br>3. Kenntnisse über die wichtigsten Verfahren, Instrumente und Techniken zur Entwicklung von Plänen für Korrekturmaßnahmen<br>4. Kenntnisse über die wichtigsten Konzepte im Zusammenhang mit der kontinuierlichen Verbesserung<br>5. Kenntnisse über die Verfahren zur kontinuierlichen Überwachung von Veränderungsfaktoren<br>6. Kenntnisse über die Aufrechterhaltung und Verbesserung eines ISMS |

PECB

| Bereich 7: Vorbereitung auf ein ISMS-Zertifizierungsaudit<br><br>**Hauptziel:** Sicherstellen, dass der ISO/IEC 27001 Lead Implementer Kandidat in der Lage ist, eine Organisation auf die Zertifizierung nach ISO/IEC 27001 vorzubereiten | |
|---|---|
| **Kompetenzen** | **Wissenserklärungen** |
| 1. Fähigkeit, die wichtigsten Schritte, Prozesse und Aktivitäten im Zusammenhang mit dem ISO/IEC 27001-Zertifizierungsaudit zu verstehen<br>2. Fähigkeit, den Ansatz der Auditnachweise bei einem ISMS-Audit zu verstehen, zu erklären und zu veranschaulichen<br>3. Fähigkeit, eine Organisation bei der Identifizierung und Auswahl einer Zertifizierungsstelle, die ihren Erwartungen entspricht, zu beraten<br>4. Fähigkeit, festzustellen, ob eine Organisation für das ISO/IEC 27001-Zertifizierungsaudit bereit und vorbereitet ist<br>5. Fähigkeit, das Personal einer Organisation für das ISO/IEC 27001-Zertifizierungsaudit zu schulen und vorzubereiten<br>6. Fähigkeit, die Ergebnisse und Schlussfolgerungen des Audits mit externen Auditoren zu diskutieren und anzufechten | 1. Kenntnisse über den evidenzbasierten Ansatz bei einem Audit<br>2. Kenntnisse über die Arten von Audits und ihre Unterschiede<br>3. Kenntnisse über die Unterschiede zwischen Audits der Stufe 1 und der Stufe 2<br>4. Kenntnisse über die Anforderungen, Schritte und Aktivitäten des Audits der Stufe 1<br>5. Kenntnisse über die Kriterien für die Überprüfung der dokumentierten Informationen<br>6. Kenntnisse über die Anforderungen, Schritte und Aktivitäten des Audits der Stufe 2<br>7. Kenntnisse über die Anforderungen, Schritte und Aktivitäten der Auditnachbereitung.<br>8. Kenntnisse über die Anforderungen, Schritte und Aktivitäten von Überwachungsaudits und Rezertifizierungsaudits<br>9. Kenntnisse über die Anforderungen, Leitlinien und bewährten Praktiken für die Entwicklung von Maßnahmenplänen nach einem ISO/IEC 27001-Zertifizierungsaudit |

Anhand der oben genannten Bereiche und ihrer Relevanz wurden 80 Fragen in die Prüfung aufgenommen, die in der nachstehenden Tabelle zusammengefasst sind:

| | | | | Erforderliches Verständnisniveau/ Verständnisebene (kognitiv/taxonomisch) | |
|---|---|---|---|---|---|
| | | Anzahl der Fragen/Punkte pro Kompetenzbereich, | Prozentsatz der Prüfung, der jedem Kompetenzbereich gewidmet ist bzw. für jeden Kompetenzbereich Punkte erhält, | Fragen, die das Verstehen, die Anwendung und die Analyse messen | Fragen, die Synthese und Bewertung messen |
| Kompetenzbereiche | Grundlegende Konzepte und Prinzipien eines Informationssicherheitsmanagementsystems (ISMS) | 15 | 18,75 | X | |
| | Informationssicherheitsmanagementsystem (ISMS) | 12 | 15 | X | |
| | Planung der ISMS Implementierung auf der Grundlage von ISO/IEC 27001 | 18 | 22,5 | | X |
| | Implementierung eines ISMS auf der Grundlage von ISO/IEC 27001 | 14 | 17,5 | | X |
| | Überwachung und Messung eines ISMS auf der Grundlage von ISO/IEC 27001 | 10 | 12,5 | X | |
| | Kontinuierliche Verbesserung eines ISMS auf der Grundlage von ISO/IEC 27001 | 6 | 7,5 | X | |
| | Vorbereitung auf ein ISMS-Zertifizierungsaudit | 5 | 6,25 | | X |
| | Insgesamt | **80** | **100%** | | |
| | Anzahl der Fragen pro Verständnisebene | | | **43** | **37** |
| | Prozentsatz der Prüfung, der den einzelnen Verständnisebenen (kognitiv/taxonomisch) gewidmet ist | | | **53,75%** | **46,25%** |

Das Bestehen der Prüfung wird mit 70% bewertet.

Nach erfolgreichem Bestehen der Prüfung können sich die Kandidaten je nach ihrem Erfahrungsstand für den Berechtigungsnachweis „PECB Certified ISO/IEC 27001 Lead Implementer" bewerben.

## Teilnahme an der Prüfung

### Allgemeine Informationen zur Prüfung

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

Die Kandidaten müssen einen gültigen Ausweis (Personalausweis, Führerschein oder Reisepass) mitbringen und ihn der Aufsichtsperson vorlegen.

Am Tag der Prüfung (schriftliche Prüfungen) kann den Kandidaten, die die Prüfung in einer Fremdsprache ablegen, auf Antrag eine zusätzliche Zeit gewährt werden, und zwar wie folgt:

- 10 zusätzliche Minuten für Foundation-Prüfungen
- 20 zusätzliche Minuten für Manager-Prüfungen
- 30 zusätzliche Minuten für Lead-Prüfungen

### Prüfungsformat und -form der PECB

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

Ausführlichere Informationen über das Online-Format finden Sie im PECB Leitfaden zur Online-Prüfung..

Die PECB-Prüfungen werden in zwei Varianten angeboten:
1. Prüfung mit Aufsatzfragen
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 Grundsätze anwenden, Probleme analysieren, Alternativen bewerten, mehrere Konzepte oder Ideen kombinieren usw. Die Multiple-Choice-Fragen sind szenariobasiert, d. h. sie wurden auf der 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. Diese Multiple-Choice-Prüfung ist ein "offenes Buch", da die Fragen kontextabhängig sind. Nachfolgend finden Sie ein Muster der Prüfungsfragen.

Da es sich bei der Prüfung um eine offene Prüfung (open book) handelt, sind die Kandidaten berechtigt, die folgenden Referenzmaterialien zu verwenden:

- Eine gedruckte Version der ISO/IEC 27001 -Norm
- Schulungsmaterialien (Zugriff über die PECB-Prüfungs-App und/oder ausgedruckt)
- Alle persönlichen Notizen die während der Schulung entstanden sind
- (Zugriff über die PECB-Prüfungs-App und/oder ausgedruckt)
- Ein Wörterbuch in Papierform

Jeglicher Versuch, während der Prüfung zu schummeln, zu kopieren 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:** Die PECB wird schrittweise zu Multiple-Choice-Prüfungen übergehen. Sie werden ebenfalls offen sein und szenariobasierte Fragen enthalten, die es der PECB ermöglichen, das Wissen, die Fähigkeiten und die Kenntnisse der Kandidaten zu bewerten, Informationen in neuen Situationen anzuwenden (apply), Verbindungen zwischen Ideen herzustellen (analyze) und einen Standpunkt oder eine Entscheidung zu begründen (evaluate). Alle PECB Multiple-Choice-Prüfungen bestehen aus einer Frage und drei Alternativen, von denen nur eine richtig ist.

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

## Beispielhafte Prüfungsfragen

**Szenario 1:**
Unternehmen A ist eine Versicherungsgesellschaft mit Hauptsitz in Chicago. Sie 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 Vermögenswerte und der Schutz der Vertraulichkeit der Informationen seiner Kunden. 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 sein Ansehen steigern konnte. Das Unternehmen begann mit der Implementierung des ISMS, indem es eine Implementierungsstrategie auf der Grundlage einer detaillierten Analyse seiner bestehenden Prozesse und der ISMS-Anforderungen festlegte.
Besonderes Augenmerk legte das Unternehmen auf die Risikobeurteilung der Informationssicherheit, die für das Verständnis der Bedrohungen und Schwachstellen, mit denen es konfrontiert war, entscheidend 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 das Unternehmen, zunächst das bestehende Informationsklassifizierungsschema zu aktualisieren und dann die erforderlichen Sicherheitskontrollen auf der Grundlage des für jede Informationsklassifizierung erforderlichen Schutzniveaus zu implementieren.

Die als sensibel eingestuften medizinischen Daten ihrer Kunden wurden mit der AES-Verschlüsselung verschlüsselt und dann in die private Cloud verschoben. Unternehmen A nutzte den Cloud-Speicher wegen des einfachen Zugriffs. Aufgrund des häufigen Zugriffs seiner Mitarbeiter auf diesen Dienst beschloss das Unternehmen, auch den Protokollierungsprozess zu nutzen. Der Dienst wurde so konfiguriert, dass er allen Mitarbeitern, die für die Bearbeitung medizinischer Ansprüche zuständig sind, automatisch Zugang zum Cloud-Speicher gewährt.

Da es bei den Cloud-Speicherdiensten zu Sicherheitsverletzungen kam, die entweder auf menschliches Versagen oder auf vorsätzliche Angriffe zurückzuführen waren, beschloss die IT-Abteilung des Unternehmens, den Zugang zu den in der Cloud gespeicherten sensiblen Informationen einzuschränken, wenn keine professionellen Geschäfts-E-Mails verwendet wurden. Darüber hinaus wurde eine Passwort-Manager-Software eingesetzt, um die Passwörter dieser E-Mail-Adressen zu verwalten und stärkere 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 sie in die Cloud übertragen werden. 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 Sicherheitskontrolle wurde in diesem Fall eingeführt?**
   A. Aufdeckende Kontrolle
   B. **Vorbeugende Kontrolle**
   C. Korrigierende Kontrolle

4. **Unternehmen A hat die Risikokriterien für die Bewertung seiner Risiken festgelegt. Ist dies notwendig?**
   A. **Ja, denn das Unternehmen sollte die Risikokriterien bei der Bewertung der Informationssicherheitsrisiken festlegen und beibehalten.**
   B. Nein, denn die Risikokriterien sollten erst festgelegt werden, wenn die Risikobehandlungsoptionen 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.

- Die Zeitspanne für die Mitteilung beginnt mit dem Prüfungstermin und dauert zwei bis vier Wochen für Multiple-Choice-Prüfungen auf Papier.

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

Kandidaten, die die Prüfung erfolgreich absolvieren, können sich für eines der Berechtigungsnachweise des jeweiligen Zertifizierungsprogramms bewerben.

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.

## Richtlinien für Prüfungswiederholungen

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

- Wenn ein Kandidat die Prüfung beim ersten Versuch nicht besteht, muss er 15 Tage nach dem ersten Prüfungstermin mit dem nächsten Versuch warten (1. Wiederholung).

***Anmerkung:*** Kandidaten, die die Schulung bei einem unserer Partner absolviert haben und den ersten Prüfungsversuch nicht bestanden haben, sind berechtigt, die Prüfung innerhalb eines Zeitraums von 12 Monaten nach Erhalt des Gutscheincodes kostenlos zu wiederholen, da die für die Schulung gezahlte Gebühr einen ersten Prüfungsversuch und eine Wiederholung beinhaltet). Andernfalls fallen Gebühren für die Wiederholung an.

Kandidaten, die die Wiederholung der Prüfung nicht bestehen, empfiehlt die PECB die Teilnahme an einer Schulung, um besser auf die Prüfung vorbereitet zu sein.

Kandidaten, die eine Schulung absolviert haben, müssen die folgenden Schritte befolgen, um eine Wiederholung der Prüfung zu vereinbaren, je nach Prüfungsformat:

1. Online-Prüfung: Verwenden Sie bei der Planung der Wiederholung der Prüfung den anfänglichen Gutscheincode, um die Gebühr zu erlassen.
2. Papierprüfung: Die Kandidaten müssen sich an den PECB-Partner/Vertriebspartner wenden, der die Schulung ursprünglich organisiert hat, um die Wiederholung der Prüfung zu vereinbaren (Datum, Uhrzeit, Ort, Kosten).

Kandidaten, die keine Schulung bei einem Partner absolviert haben, sondern sich direkt bei der PECB zur Online-Prüfung angemeldet haben, fallen nicht unter diese Regelung. Das Verfahren zur Planung der Wiederholung der Prüfung ist dasselbe wie für die erste Prüfung.

## Prüfungs-Sicherheit

Ein wichtiger Bestandteil eines professionellen Zertifizierungsnachweises ist die Gewährleistung der Sicherheit und Vertraulichkeit der Prüfung. Die PECB verlässt sich auf das ethische Verhalten der Zertifizierungsinhaber und -bewerber, um die Sicherheit und Vertraulichkeit der PECB-Prüfungen zu gewährleisten. Jegliche Offenlegung von Informationen über den Inhalt von PECB-Prüfungen stellt einen

direkten Verstoß gegen den Ethikkodex der PECB dar. Die PECB wird Maßnahmen gegen Personen ergreifen, die gegen diese Regeln und Richtlinien verstoßen, einschließlich des dauerhaften Ausschlusses von der Erlangung von PECB-Berechtigungsnachweisen und des Entzugs früherer Berechtigungen. Die PECB wird auch rechtliche Schritte gegen Personen oder Organisationen einleiten, die ihre Urheberrechte, Eigentumsrechte und ihr intellektuelles Eigentum verletzen.

## Verschieben der Prüfung

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

## Antrag auf Zertifizierung

Alle Kandidaten, die die Prüfung (oder ein von der PECB anerkanntes Äquivalent) erfolgreich bestanden haben, sind berechtigt, sich um den PECB-Berechtigungsnachweis zu bewerben, für den 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 zugänglich ist) und die Kontaktdaten von Referenzen angeben, die kontaktiert werden, um die Berufserfahrung des Kandidaten zu bestätigen. Die Kandidaten können ihre Bewerbung in verschiedenen Sprachen einreichen. Kandidaten können entweder online bezahlen oder eine Rechnung stellen lassen. Für weitere Informationen wenden Sie sich bitte an certification.team@pecb.com.

Der Prozess der Online-Zertifizierungsbeantragung ist sehr einfach und dauert nur wenige Minuten, wie folgt:

- Ihr Konto anmelden
- Überprüfen Sie Ihre E-Mail auf den Bestätigungslink
- Anmelden , um die Zertifizierung zu beantragen

Weitere Informationen zum Antragsverfahren finden Sie in diesem Handbuch Antrag auf Zertifizierung.

Der Antrag wird genehmigt, sobald die Zertifizierungsabteilung bestätigt hat, dass der Kandidat alle Zertifizierungsanforderungen für den jeweiligen Berechtigungsnachweis erfüllt. Eine E-Mail wird an die bei der Bewerbung angegebene E-Mail-Adresse geschickt, um den Status der Bewerbung mitzuteilen. 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 an.

## Erneuern Sie Ihre Zertifizierung

Die PECB-Zertifizierungen sind drei Jahre lang gültig. Um sie aufrechtzuerhalten, müssen die Kandidaten jedes Jahr nachweisen, dass sie immer noch Aufgaben ausführen, die mit der Zertifizierung in Zusammenhang stehen. PECB-zertifizierte Fachleute müssen jährlich Fortbildungspunkte nachweisen und eine jährliche Aufrechterhaltungsgebühr von 100 Dollar entrichten, um die Zertifizierung aufrechtzuerhalten. Weitere Informationen finden Sie auf der Seite zur Aufrechterhaltung der Zertifizierung auf der PECB-Website.

## Einen Fall abschließen

Wenn die Kandidaten innerhalb von drei Jahren keinen Antrag auf Zertifizierung stellen, wird ihr Fall eingestellt. Auch wenn der Zertifizierungszeitraum abläuft, haben die Kandidaten das Recht, ihren Fall wieder zu öffnen. Die PECB ist jedoch nicht mehr für Änderungen der Bedingungen, Normen, Richtlinien und des Kandidatenhandbuchs verantwortlich, die vor dem Abschluss des Falls galten. Ein Kandidat, der die Wiederaufnahme seines Falles beantragt, muss dies schriftlich tun und die erforderliche Gebühr entrichten.

PECB

# ABSCHNITT III: ZERTIFIZIERUNGSANFORDERUNGEN

## ISO IEC 27001 Lead Implementer

Die Anforderungen für die PECB ISO/IEC 27001 Implementer-Zertifizierung sind:

| Qualifikation | Prüfung | Berufserfahrung | MS Projekterfahrung | Andere Anforderungen |
|---|---|---|---|---|
| **PECB Certified ISO/IEC 27001 Provisional Implementer** | PECB-Prüfung zum zertifizierten ISO/IEC 27001Lead Implementer oder gleichwertigt | Keine | Keine | Unterzeichnung des PECB-Ethikkodexes |
| **PECB Certified ISO/IEC 27001 Implementer** | PECB-Prüfung zum zertifizierten ISO/IEC 27001Lead Implementer oder gleichwertigt | Zwei Jahre:<br>Ein Jahr Berufserfahrung im Bereich Informationssicherheitsmanagement | Projektaktivitäten: insgesamt 200 Stunden | Unterzeichnung des PECB-Ethikkodexes |
| **PECB Certified ISO/IEC 27001 Lead Implementer** | PECB-Prüfung zum zertifizierten ISO/IEC 27001Lead Implementer oder gleichwertigt | Fünf Jahre:<br>Zwei Jahre Berufserfahrung im Bereich Informationssicherheitsmanagement | Projektaktivitäten: insgesamt 300 Stunden | Unterzeichnung des PECB-Ethikkodexes |
| **PECB Certified ISO/IEC 27001 Senior Lead Implementer** | PECB-Prüfung zum zertifizierten ISO/IEC 27001Lead Implementer oder gleichwertigt | Zehn Jahre:<br>Sieben Jahre Berufserfahrung im Bereich Informationssicherheitsmanagement | Projektaktivitäten: insgesamt 1.000 Stunden | Unterzeichnung des PECB-Ethikkodexes |

Um als gültig angesehen zu werden, sollten die Implementierungsaktivitäten den besten Implementierungs- und Managementpraktiken entsprechen und Folgendes umfassen:

1. Entwurf des ISMS-Plans
2. Initiierung der ISMS-Implementierung
3. Implementierung des ISMS
4. Verwaltung, Überwachung und Aufrechterhaltung des ISMS
5. Identifizierung und Umsetzung von Möglichkeiten zur kontinuierlichen Verbesserung

# 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 mit Informationssicherheitsprojekten sowie seinen aktuellen und früheren beruflichen Werdegang bestätigen können. Berufliche Referenzen von Personen, die unter der Aufsicht des Bewerbers stehen oder mit ihm verwandt sind, sind nicht gültig.

## 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 Projekterfahrung

Das ISMS-Projektprotokoll des Kandidaten wird überprüft, um sicherzustellen, dass der Kandidat die erforderliche Anzahl von Implementierungsstunden erreicht hat.

## Bewertung der Zertifizierungsanträge

Die Zertifizierungsabteilung prüft jeden Antrag, um festzustellen, ob der Kandidat für eine Zertifizierung in Frage kommt. Ein Kandidat, dessen Antrag geprüft wird, wird schriftlich benachrichtigt und erhält, falls erforderlich, einen angemessenen Zeitrahmen, um zusätzliche Unterlagen vorzulegen. Wenn ein Kandidat innerhalb der Frist nicht antwortet oder die geforderten Unterlagen nicht innerhalb des vorgegebenen Zeitrahmens vorlegt, wird die Zertifizierungsabteilung den Antrag auf der Grundlage der ursprünglichen Informationen validieren, was letztendlich zu einer Herabstufung auf eine niedrigere Qualifikation 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
- Nichtbestehen der Prüfung

Ausführlichere Informationen finden Sie im Abschnitt „Beschwerde und Berufung".

Die Anmeldegebühr für die Zertifizierung ist nicht erstattungsfähig.

## Aussetzung/Suspendierung der Zertifizierung

Die PECB kann die Zertifizierung vorübergehend einstellen (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 andere Bedingungen 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-zertifizierter Fachmann ausgeben. Weitere Gründe für den Widerruf der Zertifizierung sind, wenn Kandidaten:

- Den PECB-Ethikkodex verletzen
- Den Umfang der Zertifizierung falsch darstellen und falsche Angaben machen
- Gegen andere PECB-Regeln verstoßen

## Upgrade/Höherstufung von Berechtigungsnachweisen

Fachleute können ein Upgrade auf einen höheren Berechtigungsnachweis beantragen, sobald sie nachweisen können, dass sie die Anforderungen erfüllen.

Um ein Upgrade zu beantragen, müssen sich die Kandidaten in ihr PECB-Konto einloggen, die Rubrik "Meine Zertifizierungen" besuchen und auf den Link "Upgrade" klicken. Die Gebühr für den Upgrade-Antrag beträgt $100.

## Herabstufung von Berechtigungsnachweisen

Eine PECB-Zertifizierung kann aus den folgenden Gründen auf eine niedrigere Stufe herabgestuft werden:

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

***Anmerkung:*** *PECB-zertifizierten Fachleuten, die über eine Lead-Zertifizierung verfügen und die Anforderungen für die Aufrechterhaltung der Zertifizierung nicht nachweisen können, wird ihre Qualifikation herabgestuft. Andererseits wird Inhabern von Master-Zertifizierungen, die keine Fortbildungen vorlegen und keine AMFs zahlen, die Zertifizierung entzogen.*

## Andere Status

Neben der aktiven, ausgesetzten oder widerrufenen Zertifizierung kann eine Zertifizierung auch freiwillig zurückgezogen oder als emeritiert bezeichnet werden. Mehr Informationen über den Status und die dauerhafte Beendigung der Tätigkeit sowie über die Beantragung finden Sie unter Optionen für den Zertifizierungsstatus.

# ABSCHNITT V: ALLGEMEINE POLITIK DER PECB

## PECB-Ethikkodex

Die Einhaltung des PECB-Ethikkodexes ist eine freiwillige Verpflichtung. Es ist wichtig, dass sich PECB-zertifizierte Fachleute nicht nur an die Grundsätze dieses Kodex halten, sondern auch andere dazu ermutigen und unterstützen. Weitere Informationen finden Sie hier.

## Andere Prüfungen und Zertifizierungen

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

## Nicht-Diskriminierung und besondere Vorkehrungen

Alle Bewerbungen werden objektiv bewertet, unabhängig von Alter, Geschlecht, Rasse, Religion, Nationalität oder Familienstand des Bewerbers.
Um allen qualifizierten Personen gleiche Möglichkeiten zu bieten, wird die PECB gegebenenfalls angemessene Vorkehrungen für die Bewerber treffen. Wenn Bewerber aufgrund einer Behinderung oder eines bestimmten körperlichen Zustands besondere Vorkehrungen benötigen, sollten sie den Wiederverkäufer/Vertriebspartner darüber informieren, damit dieser entsprechende Vorkehrungen treffen kann. Sämtliche von den Bewerbern zur Verfügung gestellten Informationen über ihre Behinderung/Bedürfnisse werden streng vertraulich behandelt.

Klicken Sie hier um das Formular für Bewerber mit Behinderungen herunterzuladen.

## Beschwerden und Berufungen

Alle Beschwerden müssen innerhalb von 30 Tagen nach Erhalt der Zertifizierungsentscheidung eingereicht werden. Die PECB wird dem Kandidaten innerhalb von 30 Arbeitstagen nach Erhalt der Beschwerde eine schriftliche Antwort zukommen lassen. Ist die Antwort nicht zufriedenstellend, hat der Kandidat das Recht, Berufung einzulegen. Weitere Informationen zu den Beschwerde- und Berufungsverfahren finden Sie hier.

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

(2) ADA Änderungsgesetz von 2008 (P.L. 110-325) Sec. 12189. Prüfungen und Schulungen. [Abschnitt 309]: Jede Person, die Prüfungen oder Schulungen im Zusammenhang mit Bewerbungen, Lizenzen, Zertifizierungen oder 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, zugängliche Vorkehrungen für diese Personenanbieten.

**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-Hilfe-Center**
Besuchen Sie unser Hilfe-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. Hier geht es zum Hilfe-Center: www.pecb.com/help

**E-Mails**
Prüfung: examination.team@pecb.com
Zertifizierung: certification.team@pecb.com
Kundenbetreuung: support@pecb.com