PECB

BEYOND RECOGNITION

# ISO/IEC 27005
# RISK MANAGER

## Příručka kandidáta

PECB

# Obsah

# SEKCE I: ÚVOD

## O PECB

PECB je certifikační orgán, který poskytuje vzdělávací[1], , certifikační a certifikační programy pro jednotlivce v široké škále oborů.

Svým působením ve více než 150 zemích pomáháme odborníkům prokázat jejich kompetence v různých oblastech odbornosti tím, že poskytujeme hodnotné hodnocení, certifikaci a certifikační programy podle mezinárodně uznávaných standardů.

**Naše hlavní cíle jsou:**

1. Stanovení minimálních požadavků nezbytných pro certifikaci odborníků
2. Přezkoumání a ověření kvalifikace žadatelů, aby se zajistilo, že jsou způsobilí žádat o certifikaci
3. Vypracování a udržování spolehlivých hodnocení pro certifikaci
4. Udělování certifikací kvalifikovaným kandidátům, vedení záznamů a zveřejňování adresáře držitelů platné certifikace
5. Stanovení požadavků na pravidelné obnovování certifikace a zajištění dodržování těchto požadavků
6. Zajištění dodržování etických norem v profesní praxi kandidátů
7. Zastupování svých členů v záležitostech společného zájmu, je-li to vhodné
8. Propagování výhod certifikace organizacím, zaměstnavatelům, státním úředníkům, odborníkům z příbuzných oborů a veřejnosti

**Naše poslání**

Poskytovat našim klientům komplexní služby v oblasti zkoušení, certifikace a certifikačních programů, které vzbuzují důvěru a jsou prospěšné pro celou společnost.

**Naše vize**

Stát se celosvětovým etalonem v oblasti poskytování profesních certifikačních služeb a certifikačních programů.

**Naše hodnoty**

Integrita, profesionalita, spravedlnost

[1] Vzdělávání se vztahuje na vzdělávací kurzy vyvinuté PECB a nabízené po celém světě prostřednictvím naší sítě partnerů.

## Hodnota certifikace PECB

**Celosvětové uznání**
Osvědčení PECB jsou mezinárodně uznávaná a schválená mnoha akreditačními orgány, takže odborníci, kteří o ně usilují, budou mít prospěch z našeho uznání na domácím i mezinárodním trhu.

Hodnota certifikací PECB je potvrzena akreditací od International Accreditation Service (IAS-PCB-111), United Kingdom Accreditation Service (UKAS-No. 21923) a Korean Accreditation Board (KAB-PC-08) podle ISO/IEC 17024 - Obecné požadavky na orgány provádějící certifikaci osob. Hodnota certifikačních programů PECB je potvrzena akreditací od ANSI National Accreditation Board (ANAB-Accreditation ID 1003) podle ANSI/ASTM E2659-18, Standard Practice for Certificate Programs.

PECB je přidruženým členem The Independent Association of Accredited Registrars (IAAR), řádným členem International Personnel Certification Association (IPC), signatářem IPC MLA a členem Club EBIOS, CPD Certification Service, CLUSIF, Credential Engine a ITCC. Kromě toho je společnost PECB schváleným vydavatelem licencovaných partnerů (Licensed Partner Publisher – LPP) od akreditačního orgánu pro certifikaci CMMC-AB (Cybersecurity Maturity Model Certification Body) pro certifikační standard CMMC (Cybersecurity Maturity Model Certification), je schválena klubem EBIOS k nabízení certifikace EBIOS Risk Manager Skills a je schválena CNIL (Commission Nationale de l'Informatique et des Libertés) k nabízení certifikace DPO. Podrobnější informace naleznete zde.

**Vysoce kvalitní produkty a služby**
Jsme hrdí na to, že našim klientům poskytujeme vysoce kvalitní produkty a služby, které odpovídají jejich potřebám a požadavkům. Všechny naše produkty jsou pečlivě připravovány týmem odborníků a profesionálů na základě nejlepších postupů a metodik.

**Soulad s normami**
Naše certifikace a certifikační programy jsou dokladem souladu s normami ISO/IEC 17024 a ASTM E2659. Jsou zárukou, že požadavky norem byly splněny a ověřeny s odpovídající důsledností, profesionalitou a nestranností.

**Služby orientované na zákazníka**
Jsme společnost orientovaná na zákazníka a ke každému našemu klientovi přistupujeme hodnotně, důležitě, profesionálně a poctivě. PECB má tým odborníků, kteří jsou zodpovědní za řešení požadavků, dotazů a potřeb. Snažíme se dodržet maximální dobu odezvy 24 hodin, aniž bychom ohrozili kvalitu služeb.

**Flexibilita a pohodlí**
Díky možnostem online vzdělávání je vaše profesní cesta pohodlnější, protože si můžete výuku naplánovat podle svého životního stylu. Tato flexibilita vám poskytne více volného času, nabízí více možností kariérního postupu a snižuje náklady.

## Etický kodex společnosti PECB

Etický kodex představuje nejvyšší hodnoty a etiku, kterými se PECB plně zavazuje řídit, neboť si uvědomuje jejich důležitost při poskytování služeb a získávání klientů.

Oddělení pro dodržování předpisů dbá na to, aby zaměstnanci, školitelé, zkoušející, dohlížitelé, partneři, distributoři, členové různých poradních sborů a výborů, certifikované osoby a držitelé certifikátů (dále jen "odborníci PECB") dodržovali tento etický kodex. Kromě toho divize Compliance důsledně zdůrazňuje nutnost chovat se při poskytování služeb profesionálně a s plnou odpovědností, kompetentně a spravedlivě vůči interním i externím zainteresovaným stranám, jako jsou žadatelé, kandidáti, certifikované osoby, držitelé certifikátů, akreditační orgány a státní orgány.

PECB je přesvědčena, že k dosažení úspěchu organizace musí plně porozumět potřebám a očekáváním klientů a zúčastněných stran. Za tímto účelem PECB podporuje kulturu založenou na nejvyšší úrovni integrity, profesionality a spravedlnosti, které jsou zároveň jejími hodnotami. Tyto hodnoty jsou nedílnou součástí organizace a v průběhu let charakterizovaly celosvětovou přítomnost a růst a založily pověst, které se PECB dnes těší.

PECB věří, že silné etické hodnoty jsou pro zdravé a pevné vztahy zásadní. Proto je prvořadou odpovědností PECB zajistit, aby odborníci PECB projevovali chování, které je plně v souladu se zásadami a hodnotami PECB.

Odborníci PECB jsou povinni:

1. Chovat se při poskytování služeb profesionálně, čestně, přesně, spravedlivě a nezávisle
2. Jednat výhradně v nejlepším zájmu svého zaměstnavatele, klientů, veřejnosti a profese v souladu s tímto etickým kodexem a dalšími profesními normami
3. Prokazovat a rozvíjet své kompetence v příslušných oborech a neustále usilovat o zlepšování svých dovedností a znalostí
4. Poskytovat služby pouze kvalifikovaným a kompetentním osobám a náležitě informovat klienty a zákazníky o povaze navrhovaných služeb, včetně všech relevantních obav nebo rizik
5. Informovat svého zaměstnavatele nebo klienta o jakýchkoli obchodních zájmech nebo vazbách, které by mohly ovlivnit nebo zhoršit jeho úsudek
6. Zachovávat důvěrnost informací o všech současných nebo bývalých zaměstnavatelích nebo klientech během poskytování služeb
7. Dodržovat všechny platné zákony a předpisy jurisdikcí v zemi, kde jsou služby poskytovány
8. Respektovat duševní vlastnictví a příspěvky ostatních
9. Nesdělovat záměrně nepravdivé nebo zfalšované informace, které by mohly ohrozit integritu procesu hodnocení kandidáta certifikace PECB nebo certifikačního program PECB
10. Neprezentovat se falešně nebo neoprávněně jako zástupce PECB bez řádné licence nebo zneužívat logo, certifikace nebo certifikáty PECB
11. Nejednat způsobem, který by mohl poškodit pověst PECB, certifikací nebo certifikačních programů
12. Plně spolupracovat při vyšetřování v návaznosti na údajné porušení tohoto etického kodexu

Chcete-li si přečíst úplné znění Etického kodexu PECB, přejděte na stránku Code of Ethics | PECB.

## Představení to ISO/IEC 27005 Risk Manager

ISO/IEC 27005 je mezinárodní norma, která poskytuje pokyny pro management rizik informační bezpečnosti a podporuje obecné koncepty informační bezpečnosti uvedené v normě ISO/IEC 27001. Procesy managementu rizik informační bezpečnosti umožňují organizacím identifikovat, analyzovat a ošetřit rizika spojená s používáním informačních technologií.

Vzhledem k tomu, že kybernetický prostor je stále nebezpečnější, stává se ochrana před hrozbami informační bezpečnosti pro většinu organizací nezbytnou. Základní složkou informační bezpečnosti je management rizik. Jednou z nejžádanějších dovedností na trhu je proto schopnost zavést a uplatňovat systematický přístup k managementu rizik informační bezpečnosti.

Osvědčení "ISO/IEC 27005 Risk Manager" je profesní certifikace pro odborníky v oblasti informační bezpečnosti, jejímž cílem je prokázat způsobilost účinně řídit rizika informační bezpečnosti. Mezinárodně uznávaná certifikace představuje velkou přidanou hodnotu pro vaši kariéru a pomůže vám dosáhnout vašich profesních cílů.

Certifikace PECB nejsou licencí ani pouhým členstvím. Osvědčují znalosti a dovednosti kandidátů získané v našich vzdělávacích kurzech a jsou vydávány kandidátům, kteří mají požadovanou praxi a úspěšně složili zkoušku.

Tento dokument specifikuje certifikační schéma PECB ISO/IEC 27005 Risk Manager v souladu s normou ISO/IEC 17024:2012. Rovněž popisuje kroky, které by měli kandidáti podniknout k získání a udržení svého osvědčení. Proto je velmi důležité, abyste si před vyplněním a odesláním žádosti pečlivě přečetli všechny informace obsažené v tomto dokumentu. Pokud máte po jeho přečtení dotazy nebo potřebujete další informace, obraťte se na mezinárodní kancelář PECB na adrese certification.team@pecb.com.

PECB

# SEKCE II: PŘÍPRAVA NA ZKOUŠKU, PRAVIDLA A POLITIKY

## Příprava na zkoušku a její plánování

Všichni kandidáti jsou zodpovědní za své vlastní studium a přípravu na certifikační zkoušky. Přestože kandidáti nemusí absolvovat vzdělávací kurz, aby mohli přistoupit ke zkoušce, jeho absolvování může výrazně zvýšit jejich šance na úspěšné složení zkoušky.

Pro naplánování zkoušky mají kandidáti dvě možnosti:

1. Kontaktujte některého z našich autorizovaných partnerů. Chcete-li najít autorizovaného partnera ve svém regionu, přejděte na stránku Active Partners. Rozpis školení je k dispozici také online a najdete jej na stránce Training Events.
2. Zkoušku PECB můžete složit na dálku prostřednictvím aplikace PECB Exams application. Chcete-li si naplánovat zkoušku na dálku, přejděte na následující odkaz: Exam Events.

Další informace o zkouškách, doménách kompetencí a znalostech naleznete v sekci III tohoto dokumentu.

## Změna termínu zkoušky

Jakékoli změny týkající se data, času, místa konání zkoušky nebo jiných podrobností můžete konzultovat na adrese online.exams@pecb.com.

## Poplatky za přihlášku ke zkoušce a certifikaci

Kandidáti mohou složit zkoušku, aniž by se zúčastnili vzdělávacího kurzu. Ceny jsou následující:

- Zkouška Lead: 1000 USD [2]
- Zkouška Manager: 700 USD
- Zkouška Foundation: 500 USD
- Zkouška Transition: 500 USD

Poplatek za žádost o certifikaci je 500 USD.

U kandidátů, kteří absolvovali vzdělávací kurz prostřednictvím některého z partnerů PECB, pokrývá cena náklady na zkoušku (první pokus a první opakování), žádost o certifikaci a roční udržovací poplatek (AMF) za první rok.

[2] Všechny ceny uvedené v tomto dokumentu jsou v amerických dolarech.

## Domény kompetencí

Cílem zkoušky "PECB Certified ISO/IEC 27005 Risk Manager" je ověřit, že kandidát získal potřebné kompetence pro vytvoření, zavedení a řízení programu managementu rizik informační bezpečnosti.

Certifikace ISO/IEC 27005 Risk Manager je určena pro:

- Manažery nebo konzultanty, kteří se podílejí na informační bezpečnosti v organizaci nebo jsou za ni odpovědní
- Osoby odpovědné za řízení rizik informační bezpečnosti
- Členy týmů pro informační bezpečnost, IT odborníky a pracovníky odpovědné za ochranu osobních údajů
- Osoby odpovědné za udržování shody s požadavky na bezpečnost informací podle normy ISO/IEC 27001 v organizaci
- Projektové manažery, konzultanty nebo odborné poradce, kteří se snaží zvládnout management rizik informační bezpečnosti

Obsah zkoušky je rozdělen takto:

- **Doména 1:** Základní principy a koncepty managementu rizik informační bezpečnosti
- **Doména 2:** Implementace programu managementu rizik informační bezpečnosti
- **Doména 3:** Rámec a proces managementu rizik informační bezpečnosti založený na ISO/IEC 27005
- **Doména 4:** Další metody posuzování rizik informační bezpečnosti

## Doména 1: Základní principy a koncepty managementu rizik informační bezpečnosti

**Hlavní cíl:** Ověřit, že kandidát rozumí hlavním principům a pojmům managementu rizik informační bezpečnosti a je schopen je interpretovat.

| Kompetence | Znalosti |
|---|---|
| 1. Schopnost porozumět a vysvětlit strukturu normy ISO/IEC 27005<br>2. Schopnost porozumět vztahu mezi normou ISO/IEC 27005 a dalšími rámci pro management rizik<br>3. Schopnost popsat účel managementu rizik a přínosy normy ISO/IEC 27005<br>4. Schopnost porozumět a vysvětlit koncept informační bezpečnosti<br>5. Schopnost porozumět principům informační bezpečnosti: důvěrnosti, integritě a dostupnosti<br>6. Schopnost porozumět a interpretovat definici rizika<br>7. Schopnost porozumět hlavním pojmům a zásadám managementu rizik<br>8. Schopnost porozumět zranitelnostem a hrozbám informační bezpečnosti<br>9. Schopnost vysvětlit pojmy událost, příležitost, následek a pravděpodobnost výskytu<br>10. Schopnost porozumět klasifikaci bezpečnostních opatření podle typu a funkce<br>11. Schopnost porozumět roli vlastníka rizik | 1. Znalost hlavních pojmů a terminologie normy ISO/IEC 27005<br>2. Znalost hlavních norem řady ISO/IEC 27000<br>3. Znalost mezinárodních a oborových norem a rámců pro bezpečnost informací a management rizik<br>4. Znalost rizik informační bezpečnosti, jak jsou definována v normě ISO/IEC 27005<br>5. Znalost definice zranitelnosti<br>6. Znalost rozdílů mezi pojmy rizika a příležitosti<br>7. Znalost definice hrozby<br>8. Znalost pojmů důvěrnost, integrita a dostupnost informací<br>9. Znalost typu a funkce bezpečnostních opatření<br>10. Znalost principů managementu rizik<br>11. Znalost rolí a odpovědností vlastníka rizik<br>12. Znalost výhod managementu rizik |

## Doména 2: Implementace programu managementu rizik informační bezpečnosti

**Hlavní cíl:** Ověřit, že kandidát rozumí programu managementu rizik založenému na normě ISO/IEC 27005 a že je schopen zahájit jeho implementaci.

| Kompetence | Znalosti |
|---|---|
| 1. Schopnost porozumět začlenění cyklu PDCA do programu managementu rizik informační bezpečnosti<br>2. Schopnost pochopit a vysvětlit hlavní kroky potřebné pro vytvoření a zavedení programu managementu rizik informační bezpečnosti<br>3. Schopnost identifikovat role a odpovědnosti klíčových zúčastněných stran během a po zavedení a fungování programu managementu rizik informační bezpečnosti<br>4. Schopnost porozumět koncepci posuzování rizik<br>5. Schopnost porozumět významu politiky managementu rizik<br>6. Schopnost identifikovat zdroje potřebné pro implementaci programu managementu rizik<br>7. Schopnost analyzovat a porozumět vnitřnímu a vnějšímu kontextu organizace<br>8. Schopnost porozumět klíčovým procesům a činnostem organizace<br>9. Schopnost pochopit a stanovit cíle programu managementu rizik<br>10. Schopnost stanovit a udržovat kritéria rizik informační bezpečnosti, včetně kritérií přijatelnosti rizik a kritérií pro provádění hodnocení rizik informační bezpečnosti<br>11. Schopnost definovat a zdůvodnit rozsah procesu managementu rizik informační bezpečnosti a přizpůsobit jej cílům organizace<br>12. Schopnost definovat vhodnou metodu managementu rizik informační bezpečnosti | 1. Znalost procesu managementu rizik<br>2. Znalost toho, jak může vrcholové vedení prokázat vůdčí roli a závazek v oblasti managementu rizik<br>3. Znalost rolí a odpovědností manažera rizik týkajících se programu managementu rizik<br>4. Znalost rolí a odpovědností klíčových zainteresovaných stran při zavádění programu managementu rizik<br>5. Znalost toho, co obvykle tvoří vnitřní a vnější kontext organizace<br>6. Znalost významu porozumění klíčovým procesům a činnostem organizace v oblasti managementu rizik<br>7. Znalost cílů posuzování rizik a způsobů dosažení konkrétních výsledků<br>8. Znalost toho, jak se stanovují kritéria přijatelnosti rizik a kritéria hodnocení rizik informační bezpečnosti<br>9. Znalost cyklů managementu rizik informační bezpečnosti<br>10. Znalost použitelnosti kvantitativní a kvalitativní analýzy při stanovování kritérií přijatelnosti rizik<br>11. Znalost zdrojů potřebných pro management rizik informační bezpečnosti<br>12. Znalost rozsahu a hranic managementu rizik informační bezpečnosti<br>13. Znalost přístupů a metodik používaných pro posuzování rizik informační bezpečnosti<br>14. Znalost hlavních kroků při plánování činností souvisejících s posuzováním rizik |

## Doména 3: Rámec a proces managementu rizik informační bezpečnosti založený na ISO/IEC 27005

**Hlavní cíl:** Ověřit, že kandidát je schopen identifikovat, analyzovat, vyhodnocovat, ošetřovat, komunikovat, zaznamenávat a průběžně monitorovat rizika informační bezpečnosti podle normy ISO/IEC 27005.

| Kompetence | Znalosti |
|---|---|
| 1. Schopnost porozumět procesům identifikace, analýzy a hodnocení rizik informační bezpečnosti<br>2. Schopnost určit přístup k identifikaci rizik a pochopit a interpretovat techniky shromažďování informací<br>3. Schopnost identifikovat aktiva, hrozby, existující opatření, zranitelnosti, potenciální následky a vlastníky rizik<br>4. Schopnost porozumět metodikám analýzy rizik a interpretovat je<br>5. Schopnost porozumět a provést posouzení následků<br>6. Schopnost určit úrovně rizika na základě kritérií pro hodnocení rizik<br>7. Schopnost porozumět prioritizaci rizik<br>8. Schopnost porozumět procesu ošetření rizik a možnostem ošetření rizik na základě normy ISO/IEC 27005<br>9. Schopnost vybrat vhodná opatření ke snížení, zachování, vyhnutí se nebo sdílení rizik<br>10. Schopnost porozumět a vysvětlit kritéria přijatelnosti rizik informační bezpečnosti<br>11. Schopnost porozumět managementu zbytkových rizik<br>12. Schopnost porozumět a interpretovat koncept komunikace a konzultací o rizicích<br>13. Schopnost porozumět a interpretovat zásady efektivní komunikace<br>14. Schopnost porozumět a navázat interní a externí komunikaci<br>15. Schopnost porozumět komunikačním cílům a činnostem<br>16. Schopnost porozumět komunikačním přístupům a nástrojům<br>17. Schopnost dokumentovat procesy managementu rizik informační bezpečnosti | 1. Znalost procesů posuzování rizik informační bezpečnosti, včetně identifikace, analýzy a hodnocení rizik<br>2. Znalost přístupů k provádění identifikace rizik informační bezpečnosti<br>3. Znalost technik shromažďování informací<br>4. Znalost definice aktiva a identifikace primárních a podpůrných aktiv<br>5. Znalost identifikace a klasifikace zranitelností, hrozeb a stávajících opatření<br>6. Znalost identifikace potenciálních následků, které mohou mít vliv na dostupnost, důvěrnost, integritu<br>7. Znalost technik analýzy rizik<br>8. Znalost toho, jak by měly být posuzovány následky a pravděpodobnost výskytu a jak by měla být stanovena úroveň rizika<br>9. Znalost hodnocení úrovní rizika na základě kritérií pro hodnocení rizik<br>10. Znalost prioritizace rizik<br>11. Znalost procesu a možností ošetření rizik, včetně modifikace rizik, zachování rizik, vyhnutí se rizikům a sdílení rizik<br>12. Znalost formulace a schvalování plánu ošetření rizik<br>13. Znalost způsobu vyhodnocování a přijímání zbytkových rizik<br>14. Znalost procesu komunikace o rizicích informační bezpečnosti<br>15. Znalost zásad účinné komunikační strategie<br>16. Znalost toho, jak by měla být nastavena interní a externí komunikace<br>17. Znalost komunikačních přístupů a nástrojů<br>18. Znalost dokumentovaných<br>19. Znalost dokumentovaných informací a význam zaznamenávání rizik |

| | |
|---|---|
| 18. Schopnost zaznamenávat a vykazovat výsledky posouzení rizik a ošetření rizik<br>19. Schopnost monitorovat a přezkoumávat efektivnost programu managementu rizik informační bezpečnosti<br>20. Schopnost porozumět konceptu neustálého zlepšování a jeho výhodám v souvislosti s managementem rizik<br>21. Schopnost poradit organizaci, jak neustále zlepšovat efektivnost a účinnost programu managementu rizik informační bezpečnosti | 20. Znalost dokumentace výsledků managementu rizik<br>21. Znalost hlavních pojmů souvisejících s neustálým zlepšováním<br>22. Znalost procesů, které je třeba průběžně monitorovat a přezkoumávat |

## Doména 4: Další metody posuzování rizik informační bezpečnosti

**Hlavní cíl:** Ověřit, že kandidát umí používat metodiky a rámce pro posuzování rizik, jako jsou OCTAVE, MEHARI, EBIOS, NIST, TRA a CRAMM.

| Kompetence | Znalosti |
|---|---|
| 1. Schopnost porozumět metodikám OCTAVE a interpretovat je: OCTAVE, OCTAVE-S, OCTAVE-Allegro a OCTAVE FORTE<br>2. Schopnost provádět hodnocení rizik informační bezpečnosti na základě metodiky OCTAVE Allegro<br>3. Schopnost analyzovat a řídit rizika na základě metody MEHARI<br>4. Schopnost porozumět metodě EBIOS pro provádění posuzování rizik a používat ji<br>5. Schopnost identifikovat publikace NIST pro management rizik<br>6. Schopnost porozumět a interpretovat rámec NIST pro management rizik a využívat jej při řízení rizik informační bezpečnosti<br>7. Schopnost porozumět a interpretovat metodiku CRAMM pro management rizik<br>8. Schopnost porozumět a vysvětlit, jak lze využít metodu harmonizovaného hodnocení hrozeb a rizik (TRA – Harmonized Threat and Risk Assessment) k provádění posouzení rizik | 1. Znalost tří fází metody OCTAVE<br>2. Znalost fází metody OCTAVE-S pro provádění posouzení rizik<br>3. Znalost toho, jak lze fáze metody OCTAVE-Allegro využít k provedení posouzení rizik informační bezpečnosti<br>4. Znalost kroků OCTAVE FORTE pro management rizik<br>5. Znalost tří hlavních fází MEHARI pro management rizik<br>6. Znalost způsobu identifikace, odhadu, hodnocení a ošetření rizik informační bezpečnosti pomocí programu MEHARI<br>7. Znalost metodiky posuzování rizik EBIOS a jejích pěti seminářů a modulů<br>8. Znalost publikací NIST pro řízení rizik<br>9. Znalost sedmi kroků rámce managementu rizik NIST<br>10. Znalost metodiky a nástroje pro analýzu a management rizik CRAMM<br>11. Znalost pěti fází metodiky harmonizovaného hodnocení hrozeb a rizik (TRA – Harmonized Threat and Risk Assessment) |

Na základě výše uvedených domén a jejich významu je do zkoušky zahrnuto 60 otázek, které jsou shrnuty v následující tabulce:

| | | | | Požadovaná úroveň porozumění (kognitivní/taxonomická) | |
|---|---|---|---|---|---|
| | | Počet otázek/bodů pro každou oblast kompetencí | % zkoušky věnované jednotlivým doménám kompetencí/bodům za ně | Otázky, které měří porozumění, aplikaci a analýzu. | Otázky, které měří hodnocení |
| Domény kompetencí | Základní principy a koncepty managementu rizik informační bezpečnosti | 13 | 21.67 | X | |
| | Implementace programu managementu rizik informační bezpečnosti | 7 | 11.67 | X | |
| | Rámec a proces managementu rizik informační bezpečnosti založený na ISO/IEC 27005 | 31 | 51.67 | | X |
| | Další metody posuzování rizik informační bezpečnosti | 9 | 15 | X | |
| | Celkem | **60** | **100 %** | | |
| | Počet otázek na úroveň porozumění | | | **29** | **31** |
| | % zkoušky věnované každé úrovni porozumění (kognitivní/taxonomie) | | | **48.3 %** | **51.7 %** |

Podmínkou úspěšného složení zkoušky je dosažení **70 %**.

Po úspěšném složení zkoušky mohou kandidáti požádat o získání osvědčení “PECB Certified ISO/IEC 27005 Risk Manager”.

## Skládání zkoušky

**Obecné informace o zkoušce**
Kandidáti jsou povinni dostavit se na zkoušku nejméně 30 minut před jejím začátkem.

Kandidátům, kteří se dostaví pozdě, nebude poskytnut dodatečný čas jako náhrada za pozdní příchod a nemusí být připuštěni ke zkoušce.

Kandidáti jsou povinni předložit platný průkaz totožnosti (občanský průkaz, řidičský průkaz nebo cestovní pas) a ukázat jej zkušebnímu komisaři.

Pokud o to v den zkoušky požádáte (papírové zkoušky), může být kandidátům skládajícím zkoušku v jiném, než mateřském jazyce poskytnut dodatečný čas, a to následovně:

- 10 minut navíc pro zkoušky Foundation
- 20 minut navíc pro zkoušky Manager
- 30 minut navíc pro zkoušky Lead

**Formát a typ zkoušky PECB**

1. **Listinná:** Zkoušky se skládají na papíře, přičemž kandidát nesmí používat nic jiného než papír a pero. Používání elektronických zařízení, jako jsou notebooky, tablety nebo telefony, není povoleno. Na průběh zkoušky dohlíží zkušební komisař schválený PECB v místě, kde partner pořádá vzdělávací kurz.
2. **Online:** Zkoušky jsou poskytovány elektronicky prostřednictvím aplikace PECB Exams. Používání elektronických zařízení, jako jsou tablety a mobilní telefony, není povoleno. Na průběh zkoušky dohlíží na dálku zkušební komisař PECB prostřednictvím aplikace PECB Exams a externí/integrované kamery.

Podrobnější informace o online formátu najdete v průvodci online zkouškou PECB Online Exam Guide.

Zkoušky PECB jsou k dispozici ve dvou typech:

1. Zkouška s otázkami typu esej
2. Zkouška s otázkami s výběrem odpovědi

**Tato zkouška se skládá z otázek s výběrem odpovědí:** Zkouška s výběrem odpovědí může být použita k vyhodnocení porozumění jednoduchým i složitým pojmům. Obsahuje samostatné otázky i otázky založené na scénáři. Samostatné otázky jsou v rámci zkoušky nezávislé a nejsou závislé na kontextu, zatímco otázky založené na scénáři jsou závislé na kontextu, tj. jsou vypracovány na základě scénáře, který si má kandidát přečíst a má odpovědět na pět otázek souvisejících s tímto scénářem. Při odpovídání na samostatné otázky a otázky založené na scénáři budou kandidáti muset aplikovat různé pojmy a principy vysvětlené během vzdělávacího kurzu, analyzovat problémy, identifikovat a vyhodnotit alternativy, kombinovat několik pojmů nebo myšlenek atd.

Každá otázka s výběrem odpovědi má tři možnosti, z nichž je jedna správná (klíčová odpověď) a dvě nesprávné (distraktory).

Jedná se o zkoušku typu "open-book". Kandidát může použít následující referenční materiály:

- Tištěný výtisk normy ISO/IEC 27005
- Materiály ke vzdělávacímu kurzu (přístupné prostřednictvím aplikace PECB Exams a/nebo vytištěné)
- Veškeré osobní poznámky pořízené během školení (přístupné prostřednictvím aplikace PECB Exams a/nebo vytištěné)
- Slovník v tištěné podobě

Níže je uvedena ukázka zkušebních otázek.

**Poznámka:** PECB postupně přejde na zkoušky s výběrem odpovědí. Budou také typu "open book" a budou obsahovat otázky založené na scénářích, které umožní PECB hodnotit znalosti, schopnosti a dovednosti kandidátů používat informace v nových situacích (aplikovat), vyvozovat souvislosti mezi myšlenkami (analyzovat) a zdůvodňovat postoj nebo rozhodnutí (hodnotit).

Pro konkrétní informace o typech zkoušek, dostupných jazycích a dalších podrobnostech kontaktujte examination.team@pecb.com nebo přejděte na seznam zkoušek List of PECB Exams.

**Vzorové zkušební otázky**

*Techonics* je technologická společnost, která se specializuje na počítačový software a spotřební elektroniku. Pravidelně provádí posouzení rizik, aby zajistila informační bezpečnost. Díky dobře zavedenému procesu managementu rizik informační bezpečnosti je společnost *Techonics* schopna identifikovat potenciální rizika spojená s informačními aktivy a najít jejich řešení. Její rámec managementu rizik je založen na pokynech ISO/IEC 27005.

Poslední proces posuzování rizik informační bezpečnosti ve společnosti *Techonics* proběhl minulý měsíc. Provedla ho Lana, manažerka rizik společnosti *Techonics*, a jeho výsledky poukázaly na některá nová rizika související s politikou hesel. V souladu s rámcem managementu rizik společnosti *Techonics* byl proces posouzení rizik zahájen důkladnou analýzou společnosti a jejích cílů. Poté byla definována základní kritéria týkající se managementu rizik.

Lana, vedla rozhovory s klíčovými pracovníky. Zjistila, že většina zaměstnanců společnosti *Techonics* si byla vědoma toho, že podle zásad pro používání hesel musí jednou za tři měsíce změnit svá hesla. Většina z nich však toto pravidlo nedodržovala, protože jej systém nevynucoval.

Kromě toho zjistila, že zaměstnanci mají tendenci používat slabá hesla, jako je jejich jméno a příjmení. Vzhledem k tomu, že slabá hesla jsou snadno uhodnutelná, mohlo by to představovat vážný problém pro bezpečnost společnosti *Techonics*. Lana identifikovala několik rizikových scénářů týkajících se zjištěné situace, z nichž dva měly "vysokou" úroveň výskytu.

Sam, manažer informační bezpečnosti, navrhl implementaci cloudového multiplatformního správce hesel. Tuto platformu by mohli využívat všichni zaměstnanci k vytváření složitých hesel a jejich ukládání do zabezpečené databáze. Společnost *Techonics* jeho doporučení přijala a začala platformu používat, aby se minimalizovalo riziko spojené se slabými hesly. Kromě toho bylo rozhodnuto, že Sam uspořádá školení o informační bezpečnosti, aby zaměstnance poučil o důležitosti ochrany hesel.

Na základě výše uvedeného scénáře odpovězte na následující otázky:

1. **Společnost *Techonics* použila normu ISO/IEC 27005 jako vodítko pro vytvoření svého rámce managementu rizik informační bezpečnosti. Je to přijatelné?**
   A. Ne, norma ISO/IEC 27005 specifikuje požadavky na dosažení informační bezpečnosti prostřednictvím implementace ISMS
   B. Ano, norma ISO/IEC 27005 se vztahuje na jakýkoli typ rizika bez ohledu na jeho povahu nebo následky
   C. **Ano, norma ISO/IEC 27005 poskytuje návod, který pomáhá organizacím provádět činnosti managementu rizik informační bezpečnosti**

2. **Manažerka rizik Lana zjistila, že zaměstnanci společnosti Techonics si nemění svá hesla, jak to vyžaduje politika hesel. Co Lana identifikovala?**
   A. **Zranitelnost**
   B. Hrozbu
   C. Riziko

**3. Která možnost ošetření rizik byla navržena k ošetření zjištěných rizik týkajících se používání hesel?**

A. Vyhnutí se riziku
B. **Modifikace rizika**
C. Zachování rizika

## Bezpečnostní zásady u zkoušky

PECB se zavazuje chránit integritu svých zkoušek a celého zkušebního procesu a spoléhá na etické chování žadatelů, potenciálních žadatelů, kandidátů a partnerů při zachování důvěrnosti zkoušek PECB. Cílem těchto zásad je řešit nepřijatelné chování a zajistit spravedlivé zacházení se všemi kandidáty.

Jakékoli zveřejnění informací o obsahu zkoušek PECB je přímým porušením této politiky a etického kodexu PECB. Kandidáti, kteří se účastní zkoušky PECB, jsou proto povinni podepsat dohodu o důvěrnosti a mlčenlivosti o zkoušce a musí dodržovat následující ustanovení:

1. Otázky a odpovědi zkušebních materiálů jsou výhradním a důvěrným vlastnictvím PECB. Jakmile kandidáti dokončí odevzdání zkoušky do PECB, nemají již k originálu zkoušky ani k její kopii žádný přístup.
2. Kandidátům je zakázáno sdělovat jakékoli informace týkající se otázek a odpovědí zkoušky nebo diskutovat o těchto podrobnostech s jinými kandidáty nebo osobami.
3. Kandidáti si nesmějí vzít mimo zkušební místnost žádné materiály související se zkouškou.
4. Kandidáti nesmějí kopírovat ani se pokoušet pořizovat kopie (ať už písemné, fotokopírované nebo jiné) jakýchkoli materiálů ke zkoušce, mimo jiné včetně otázek, odpovědí nebo obrázků na obrazovce.
5. Kandidáti se nesmějí účastnit ani podporovat podvodné činnosti při skládání zkoušek, jako např:
    - Nahlížení do zkouškových materiálů nebo odpovědního archu jiného kandidáta
    - Poskytování nebo přijímání jakékoli pomoci od komisaře, kandidáta nebo kohokoli jiného
    - Používání neautorizovaných referenčních příruček, manuálů, nástrojů atd., včetně používání stránek "brain dump", protože nejsou PECB autorizovány.

Jakmile se kandidát dozví nebo si již je vědom nesrovnalostí nebo porušení výše uvedených bodů, je odpovědný za jejich dodržení, jinak, pokud by k takovým nesrovnalostem došlo, budou kandidáti nahlášeni přímo PECB nebo pokud takové nesrovnalosti uvidí, měli by je neprodleně nahlásit PECB.

Kandidáti jsou výhradně odpovědní za pochopení a dodržování pravidel a politik pro zkoušky PECB, dohody o důvěrnosti a mlčenlivosti a etického kodexu. Proto v případě zjištění porušení jednoho nebo více pravidel nebudou kandidátům vráceny žádné peníze. Kromě toho má PECB právo odmítnout právo přihlásit se na zkoušku PECB nebo vyzvat kandidáty k opakování zkoušky, pokud jsou v průběhu a po skončení procesu klasifikace zjištěny nesrovnalosti, a to v závislosti na závažnosti případu.

Jakékoli porušení výše uvedených bodů způsobí společnosti PECB nenapravitelnou škodu, kterou nelze nahradit žádným peněžním prostředkem. Proto může PECB podniknout příslušné kroky k nápravě nebo zabránění neoprávněnému zveřejnění nebo zneužití zkušebních materiálů, včetně získání okamžitého soudního příkazu.

PECB přijme opatření proti osobám, které porušují pravidla a zásady, včetně trvalého zákazu získávat osvědčení PECB a odebrání všech předchozích. PECB bude rovněž podnikat právní kroky proti jednotlivcům nebo organizacím, které porušují její autorská práva, vlastnická práva a duševní vlastnictví.

## Výsledky zkoušky

Výsledky zkoušek vám budou sděleny e-mailem.

- Hodnocení probíhá od data zkoušky a trvá tři až osm týdnů v případě zkoušek typu esej a dva až čtyři týdny v případě papírových zkoušek s výběrem odpovědí.
- U online zkoušek s výběrem odpovědí obdrží kandidáti výsledky okamžitě.

Kandidáti, kteří úspěšně absolvují zkoušku, budou moci požádat o jedno z osvědčení podle příslušného certifikačního systému.

Kandidátům, kteří u zkoušky neuspějí, bude do e-mailu přidán seznam oblastí, v nichž dosáhli špatných výsledků, aby se mohli lépe připravit na opakování zkoušky.

Kandidáti, kteří nesouhlasí s výsledky, mohou do 30 dnů od obdržení výsledků písemně požádat o opětovné hodnocení na adrese examination.team@pecb.com. Žádosti o opětovné hodnocení doručené po 30 dnech nebudou vyřízeny. Pokud kandidáti s výsledky opětovného hodnocení nesouhlasí, mají 30 dní od data, kdy obdrželi výsledky zkoušky, na podání stížnosti prostřednictvím systému PECB Ticketing System. Stížnosti obdržené po uplynutí 30 dnů nebudou zpracovány. PECB Ticketing System.

## Zásady opakování zkoušky

Počet opakování zkoušky není omezen. Existují však určitá omezení, pokud jde o časový interval mezi opakováním zkoušky.

Pokud kandidát neuspěje u zkoušky na první pokus, musí na další pokus (první opakování) počkat 15 dní od původního data zkoušky.

**Poznámka:** Kandidáti, kteří absolvovali vzdělávací kurz u některého z našich partnerů a neuspěli při prvním pokusu o složení zkoušky, mají nárok na bezplatné opakování zkoušky po dobu 12 měsíců od data obdržení kódu kuponu (poplatek zaplacený za vzdělávací kurz zahrnuje první pokus o složení zkoušky a jeden pokus o opakování). Jinak je opakování zkoušky zpoplatněno.

Kandidátům, kteří neuspějí při opakování zkoušky, PECB doporučuje, aby se zúčastnili školení a byli tak na zkoušku lépe připraveni.

Kandidáti, kteří absolvovali vzdělávací kurz, musí pro zajištění opakování zkoušky v závislosti na formátu zkoušky postupovat podle níže uvedených kroků:

1. Online zkouška: při plánování opakování zkoušky použijte původní coupon code, abyste nemuseli hradit poplatek za zkoušku.
2. Papírová zkouška: kandidáti musí kontaktovat partnera/distributora PECB, který původně organizoval zkoušku, aby se domluvili na opakování zkoušky (datum, čas, místo, náklady).

Na kandidáty, kteří neabsolvovali vzdělávací kurz u partnera, ale přihlásili se k online zkoušce přímo u PECB, se tyto zásady nevztahují. Postup pro naplánování opakování zkoušky je stejný jako v případě první zkoušky.

PECB

# SEKCE III: CERTIFIKAČNÍ PROCES A POŽADAVKY

## Osvědčení PECB ISO/IEC 27005

Všechny certifikace PECB mají specifické požadavky na vzdělání a odbornou praxi. Chcete-li určit, které osvědčení je pro vás to pravé, vezměte v úvahu své profesní potřeby a analyzujte kritéria pro jednotlivé certifikace.

Osvědčení ve schématu PECB ISO/IEC 27005 mají následující požadavky:

| Osvědčení | Vzdělání | Zkouška | Pracovní zkušenosti | Zkušenosti s managementem rizik | Další požadavky |
|---|---|---|---|---|---|
| **PECB Certified ISO/IEC 27005 Provisional Risk Manager** | Alespoň středoškolské vzdělání | Zkouška PECB Certified ISO/IEC 27005 Risk Manager nebo rovnocenná | Žádné | Žádné | Podepsání Etického kodexu PECB Code of Ethics |
| **PECB Certified ISO/IEC 27005 Risk Manager** | | | Dva roky: Jeden rok praxe v oblasti managementu rizik informační bezpečnosti | Činnosti v oblasti managementu rizik informační bezpečnosti v celkovém rozsahu 200 hodin | |

Aby mohly být činnosti považovány za platné, měly by se řídit osvědčenými postupy managementu a zahrnovat následující:

1. Definování přístupu k managementu rizik
2. Určení cílů a rozsahu managementu rizik
3. Provedení posouzení rizik
4. Vytvoření programu managementu rizik
5. Definování kritérií pro posuzování a akceptaci rizik
6. Hodnocení možností ošetření rizik
7. Monitorování a přezkoumávání programu managementu rizik

## Podání žádosti o certifikaci

Všichni kandidáti, kteří úspěšně složí zkoušku (nebo ekvivalentní zkoušku akceptovanou PECB), jsou oprávněni požádat o udělení osvědčení PECB, pro které byli hodnoceni. Pro získání osvědčení PECB je třeba splnit specifické požadavky na vzdělání a odbornost. Kandidáti musí vyplnit online formulář žádosti o certifikaci (který je přístupný prostřednictvím účtu PECB), včetně kontaktních údajů osob, které budou kontaktovány za účelem ověření odborné praxe kandidátů. Kandidáti mohou podat žádost v angličtině, francouzštině, němčině, španělštině nebo korejštině. Mohou si zvolit, zda chtějí zaplatit online, nebo zda jim má být vystavena faktura. Další informace získáte na adrese certification.team@pecb.com.

Proces podání online žádosti o certifikaci je velmi jednoduchý a zabere jen několik minut:

- Zaregistrujte svůj účet
- Zkontrolujte si svou e-mailovou schránku kvůli potvrzovacímu odkazu
- Přihlaste se k žádosti o certifikaci

Další informace o tom, jak požádat o certifikaci, naleznete zde.

Certifikační oddělení potvrdí, zda kandidát splňuje všechny certifikační požadavky týkající se příslušného osvědčení. Kandidát dostane e-mail o stavu jeho žádosti, včetně rozhodnutí o certifikaci.

Po schválení žádosti certifikačním oddělením si kandidát bude moci stáhnout certifikát a požádat o příslušný digitální odznak. Více informací o stažení certifikátu naleznete zde a více informací o uplatnění nároku na digitální odznak naleznete zde.

PECB poskytuje podporu v angličtině a francouzštině.

## Pracovní zkušenosti

Kandidáti musí uvést úplné a správné údaje o své odborné praxi, včetně názvu (názvů) pracovní pozice, data zahájení a ukončení, popisu (popisů) pracovní pozice a dalších údajů. Kandidátům se doporučuje, aby shrnuli své předchozí nebo současné úkoly a uvedli dostatečné podrobnosti, které popisují povahu povinností na jednotlivých pracovních místech. Podrobnější informace lze uvést v životopise.

## Pracovní reference

Ke každé žádosti je třeba předložit dvě pracovní reference. Musí se jednat o osoby, které s kandidátem spolupracovaly v pracovním prostředí a mohou potvrdit jeho zkušenosti s managementem rizik informační bezpečnosti, jakož i jeho současnou a předchozí pracovní historii. Odborné reference osob, které spadají pod vedení kandidáta nebo jsou jeho příbuznými, jsou nepřípustné.

## Zkušenosti s managementem rizik

Bude zkontrolován záznam o projektu managementu rizik kandidáta, aby bylo zajištěno, že kandidát splnil požadovaný počet hodin.

## Hodnocení žádostí o certifikaci

Certifikační oddělení posoudí každou žádost, aby ověřilo způsobilost kandidátů pro získání certifikace nebo certifikátu. Kandidát, jehož žádost je posuzována, bude písemně vyrozuměn a v případě potřeby mu bude poskytnuta přiměřená lhůta k předložení dodatečných dokumentů. Pokud kandidát neodpoví ve stanovené lhůtě nebo neposkytne požadovanou dokumentaci v daném časovém rámci, certifikační oddělení potvrdí platnost žádosti na základě původních poskytnutých informací, což může vést ke snížení kvalifikace kandidátů.

PECB

## SEKCE IV: CERTIFIKAČNÍ POLITIKY

### Zamítnutí certifikace

PECB může odmítnout certifikaci/certifikační program, pokud kandidát:

- Zfalšujte žádost
- Poruší zkušební postupy
- Poruší etický kodex PECB

Kandidáti, jejichž certifikační program/certifikát byl zamítnut, mohou podat stížnost prostřednictvím postupu pro podávání stížností a odvolání. Podrobnější informace naleznete v oddíle Politika stížností a odvolání (**Complaint and Appeal Policy**).

Platba za žádost o certifikaci/certifikační program je nevratná.

### Možnosti stavu certifikace

**Aktivní**

Znamená, že vaše certifikace je v pořádku a platná a je udržována plněním požadavků PECB týkajících se CPD a AMF.

**Pozastavena**

Pokud kandidát nesplňuje požadavky, může mu PECB dočasně pozastavit certifikaci. Mezi další důvody pro pozastavení certifikace patří:

- PECB obdrží od zúčastněných stran nadměrné nebo závažné stížnosti (pozastavení bude uplatněno až do ukončení šetření).
- Loga PECB nebo akreditačních orgánů jsou vědomě zneužívána.
- Kandidát nenapraví neoprávněné použití certifikační značky ve lhůtě stanovené PECB.
- Certifikovaná osoba dobrovolně požádala o pozastavení.
- PECB považuje za adekvátní jiné důvody pro pozastavení certifikace.

**Zrušena**

PECB může certifikát zrušit (tj. odebrat), pokud kandidát nesplní stanovené požadavky. V takových případech se kandidáti již nemohou prezentovat jako certifikovaní odborníci PECB. Dalšími důvody pro odebrání certifikace může být, pokud kandidáti:

- Porušení etického kodexu PECB
- Zkreslení a uvedení nepravdivých informací o rozsahu certifikace
- Porušení dalších pravidel PECB
- Jakékoli jiné důvody, které PECB považuje za relevantní

Kandidáti, kterým bylo osvědčení odebráno, mohou podat stížnost v rámci řízení o stížnostech a odvolání. Podrobnější informace naleznete v oddíle Politika stížností a odvolání (**Complaint and Appeal Policy**).

**Další stavy**
Kromě toho, že je certifikace aktivní, pozastavená nebo zrušená, může být dobrovolně odebrána nebo označena jako emeritní. Další informace o těchto stavech a o stavu trvalého ukončení certifikace naleznete v části Možnosti stavu certifikace (Certification Status Options).

## Zvyšování a snižování úrovně osvědčení

**Zvýšení osvědčení**
Odborníci si mohou svá osvědčení zvýšit, jakmile prokáží, že splňují příslušné požadavky.

Chcete-li požádat o zvýšení úrovně, musíte se přihlásit ke svému účtu PECB, přejít na záložku "Moje osvědčení" (My Certifications) a kliknout na "Zvýšit úroveň" (Update). Poplatek za žádost o zvýšení osvědčení je 100 USD.

**Snížení osvědčení**
Certifikát PECB může být snížen na nižší stupeň z následujících důvodů:
- AMF nebyl zaplacen.
- Hodiny CPD nebyly vykázány.
- Nebyl předložen dostatečný počet hodin CPD.
- Na žádost nebyly předloženy důkazy o hodinách CPD.

***Poznámka:*** *Certifikovaným odborníkům PECB, kteří jsou držiteli certifikátů Lead a nepředloží doklad o splnění požadavků na udržování certifikátu, bude osvědčení sníženo. Držitelům certifikátů Master, kteří nepředloží CPD a nezaplatí AMF, budou jejich certifikáty odebrány.*

## Obnovení certifikace
Certifikáty PECB jsou platné tři roky. Pro jejich udržení musí certifikovaní odborníci PECB plnit požadavky související s daným osvědčením, např. musí dodržet požadovaný počet hodin kontinuálního profesního rozvoje (CPD). Kromě toho musí platit roční udržovací poplatek (120 USD). Další informace naleznete na stránce Udržování certifikace (Certification Maintenance) na webových stránkách PECB.

## Uzavření případu
Pokud kandidáti nepožádají o certifikaci ve lhůtě jednoho roku, bude jejich případ uzavřen. I když lhůta pro vydání osvědčení uplyne, mají kandidáti právo svůj případ znovu otevřít. PECB však již neodpovídá za žádné změny týkající se podmínek, standardů, politik a příručky pro kandidáty, které platily před uzavřením případu. Kandidát, který žádá o znovuotevření svého případu, tak musí učinit písemně na adresu certification.team@pecb.com a zaplatit požadovaný poplatek.

## Politika stížností a odvolání
Případné stížnosti musí být podány nejpozději do 30 dnů od obdržení rozhodnutí o certifikaci. PECB poskytne kandidátovi písemnou odpověď do 30 pracovních dnů od obdržení stížnosti. Pokud kandidáti nepovažují odpověď za uspokojivou, mají právo podat odvolání.

Další informace o politice stížností a odvolání naleznete zde.

## SEKCE V: OBECNÉ POLITIKY

### Zkoušky a certifikace od jiných akreditovaných certifikačních orgánů

PECB uznává certifikáty a zkoušky od jiných uznávaných akreditovaných certifikačních orgánů. PECB posoudí žádosti prostřednictvím procesu ekvivalence a rozhodne, zda lze příslušnou(é) certifikaci(y) nebo zkoušku(y) přijmout jako ekvivalentní k příslušné certifikaci PECB (např. certifikace ISO/IEC 27005 Risk Manager).

### Nediskriminace a speciální podmínky

Všechny přihlášky kandidátů budou hodnoceny objektivně bez ohledu na věk, pohlaví, rasu, náboženství, státní příslušnost nebo rodinný stav.

V zájmu zajištění rovných příležitostí pro všechny kvalifikované osoby bude PECB v případě potřeby poskytovat kandidátům přiměřené podmínky. Pokud kandidáti potřebují zvláštní podmínky z důvodu zdravotního postižení nebo specifického fyzického stavu, měli by o tom informovat partnera/distributora, aby mohl učinit příslušná opatření. Veškeré informace, které kandidáti poskytnou ohledně svého postižení/zvláštních potřeb, budou považovány za důvěrné. Chcete-li si stáhnout formulář pro kandidáty se zdravotním postižením, klikněte zde.

### Zásady chování

Cílem PECB je poskytovat vysoce kvalitní, konzistentní a dostupné služby ve prospěch svých externích zainteresovaných stran: distributorů, partnerů, školitelů, inspektorů, zkoušejících, členů různých výborů a poradních sborů a klientů (účastníků vzdělávání, zkoušených, certifikovaných osob a držitelů certifikátů), jakož i vytvářet a udržovat pozitivní pracovní prostředí, které zajišťuje bezpečnost a pohodu zaměstnanců a dbá na důstojnost, respekt a lidská práva svých zaměstnanců.

Účelem této politiky je zajistit, aby PECB nestranně, důvěrně, spravedlivě a včas řešila nepřijatelné chování externích zúčastněných stran vůči zaměstnancům PECB. Chcete-li si přečíst Zásady chování, klikněte zde.

### Zásady vracení platby

PECB vám vrátí platbu, pokud jsou splněny požadavky politiky pro vracení platby. Chcete-li si přečíst politiku pro vracení platby, klikněte zde.

**Address:**

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

**Tel./Fax:**

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

**Emails:**

**Examination:**
examination.team@pecb.com

**Certification:**
certification.team@pecb.com

**Customer Service:**
support@pecb.com

**PECB Help Center**

Visit our Help Center to browse Frequently Asked Questions (FAQ), view manuals for using PECB website and applications, read documents related to PECB processes, or to contact us via Support Center's online tracking system.

www.pecb.com