PECB BEYOND RECOGNITION

# Příručka kandidáta

## ISO/IEC 27001 LEAD IMPLEMENTER

PECB

# Obsah

# SEKCE I: ÚVOD

## O PECB

PECB je certifikační orgán, který poskytuje vzdělávání a certifikaci osob v širokém spektru oborů v souladu s normou ISO/IEC 17024.

Pomáháme odborníkům prokázat odhodlání a kompetence tím, že jim poskytujeme cenné služby hodnocení a certifikace podle mezinárodně uznávaných standardů. Naším posláním je poskytovat služby, které podporují důvěru a neustálé zlepšování, prokazují uznání a přinášejí prospěch celé společnosti.

**Hlavní cíl PECB 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

## Hodnota certifikace PECB

**Proč si vybrat PECB jako certifikační orgán?**

### Celosvětové uznání

Naše certifikace jsou mezinárodně uznávané a akreditované International Accreditation Service (IAS); signatářem IAF Multilateral Recognition Arrangement (MLA), který zajišťuje vzájemné uznávání akreditované certifikace mezi signatáři MLA a akceptaci akreditované certifikace na mnoha trzích. Odborníci, kteří získají certifikaci PECB, proto budou mít prospěch z uznání PECB na domácích i mezinárodních trzích.

### Kompetentní pracovníci

Základní tým PECB se skládá z kompetentních osob, které mají příslušné zkušenosti v daném odvětví. Všichni naši zaměstnanci jsou držiteli profesních osvědčení a jsou neustále školeni, aby mohli našim klientům poskytovat více než uspokojivé služby.

### Soulad s normami

Naše certifikace jsou důkazem shody s normou ISO/IEC 17024. Zajišťují, že požadavky normy byly splněny a ověřeny s odpovídající důsledností, profesionalitou a nestranností.

### Služby zákazníkům

Jsme společnost zaměřená na zákazníka a ke všem našim zákazníkům se chováme slušně, zodpovědně, profesionálně a čestně. Společnost PECB má tým odborníků, kteří se věnují podpoře požadavků, problémů, obav, potřeb a názorů zákazníků. Snažíme se udržet maximální dobu odezvy 24 hodin, aniž bychom ohrozili kvalitu služeb.

## Etický kodex společnosti PECB

**PECB profesionálové mají:**

1. Vystupovat profesionálně, čestně, důsledně, spravedlivě, odpovědně a nezávisle
2. Vždy jednat výhradně v nejlepším zájmu svého zaměstnavatele, svých klientů, veřejnosti a profese tím, že budou při poskytování odborných služeb dodržovat profesní standardy a platné techniky
3. Udržovat si kompetence v příslušných oborech a usilovat o neustálé zlepšování svých profesních schopností
4. Nabízet pouze odborné služby, pro jejichž poskytování jsou kvalifikováni, a budou klienty náležitě informovat o povaze navrhovaných služeb, včetně všech relevantních obav nebo rizik
5. Informovat každého zaměstnavatele nebo klienta o jakýchkoli obchodních zájmech nebo vazbách, které by mohly ovlivnit jejich úsudek nebo narušit jejich nestrannost
6. Důvěrně a ohledem na soukromí zacházet s informacemi, které získali během profesního a obchodního jednání s jakýmkoli současným nebo bývalým zaměstnavatelem nebo klientem
7. Dodržovat všechny zákony a předpisy jurisdikcí, v nichž vykonávají odbornou činnost
8. Respektovat duševní vlastnictví a příspěvky ostatních
9. Ne úmyslně ani jinak sdělovat nepravdivé nebo zfalšované informace, které by mohly ohrozit integritu procesu hodnocení kandidáta na profesní označení
10. Nejednat způsobem, který by mohl ohrozit pověst PECB nebo jejích certifikačních programů
11. Plně spolupracovat při vyšetřování v návaznosti na údajné porušení tohoto etického kodexu

Úplné znění etického kodexu společnosti PECB si můžete stáhnout zde.

## Úvod do ISO/IEC 27001 Lead Implementer

Norma ISO/IEC 27001 specifikuje požadavky na vytvoření, zavedení, udržování a neustálé zlepšování systému managementu bezpečnosti informací (ISMS). Nejdůležitějšími dovednostmi, které jsou na trhu požadovány, jsou schopnost efektivně plánovat, zavádět a řídit systém ISMS, posuzovat a ošetřovat rizika bezpečnosti informací, vybírat a zavádět opatření bezpečnosti informací a řídit týmy pro zavádění ISMS (nebo být jejich součástí).

Certifikát "ISO/IEC 27001 Lead Implementer" je profesní osvědčení pro osoby, které chtějí prokázat způsobilost k implementaci systému managementu bezpečnosti informací a vedení týmu pro zavedení ISMS.

Vzhledem k tomu, že profese implementátora je jednou z nejžádanějších, může vám mezinárodně uznávaná certifikace pomoci využít váš kariérní potenciál a dosáhnout vašich profesních cílů.

Je důležité si uvědomit, že certifikace PECB nejsou licencí ani pouhým členstvím. Představují vzájemné uznání, že osoba prokázala znalost a porozumění souboru kompetencí. Certifikace PECB jsou udělovány kandidátům, kteří mohou prokázat zkušenosti a složili standardizovanou zkoušku v dané oblasti certifikace.

Tento dokument specifikuje certifikační schéma PECB ISO/IEC 27001 Lead Implementer v souladu s normou ISO/IEC 17024:2012. Tato příručka pro kandidáty obsahuje také informace o procesu, kterým mohou kandidáti získat a udržovat svá osvědčení. Je velmi důležité, abyste si před vyplněním a podáním žádosti přečetli všechny informace obsažené v této příručce pro kandidáty. Pokud budete mít po jejím přečtení dotazy, obraťte se na mezinárodní kancelář PECB na adrese certification.team@pecb.com.

# SEKCE II: PROCES CERTIFIKACE PECB A PŘÍPRAVA, PRAVIDLA A POLITIKY PRO ZKOUŠKY PECB

## Rozhodněte se, která certifikace je pro vás vhodná

Všechny certifikace PECB mají specifické požadavky na vzdělání a odbornou praxi. Chcete-li určit, která certifikace je pro vás vhodná, ověřte si kritéria způsobilosti pro různé certifikace a své profesní potřeby.

## Příprava a plánování zkoušky

Všichni kandidáti jsou zodpovědní za své studium a přípravu na certifikační zkoušku. V rámci certifikačního procesu není vyžadován žádný konkrétní soubor vzdělávacích kurzů nebo studijní plán. Nicméně absolvování vzdělávacího kurzu může výrazně zvýšit šance kandidátů na úspěšné složení zkoušky PECB.

Kandidáti mají dvě možnosti, jak si naplánovat zkoušku:

1. Kontaktovat některého z našich prodejců, kteří poskytují vzdělávací kurzy a zkoušky. Chcete-li najít poskytovatele školicích kurzů v určitém regionu, měli by kandidáti přejít na stránku Active Partners. Rozpis školicích kurzů PECB je k dispozici také na stránce Training Events.
2. Absolvovat zkoušku PECB na dálku z domova nebo z libovolného místa prostřednictvím aplikace PECB Exam, kterou naleznete zde: Exam Events.

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

### Poplatky za přihlášku ke zkoušce a certifikaci

PECB nabízí přímé zkoušky, kdy se kandidát může přihlásit ke zkoušce, aniž by se zúčastnil vzdělávacího kurzu. Platné jsou následující ceny:

- Zkouška Lead: $1000
- Zkouška Manager: $700
- Zkouška Foundation a Transition: $500

Poplatek za žádost o certifikaci činí $500.

Pro všechny kandidáty, kteří absolvovali vzdělávací kurz a složili zkoušku u některého z partnerů PECB, zahrnuje poplatek za přihlášku pouze náklady spojené se zkouškou, žádostí o certifikaci a prvním rokem ročního udržovacího poplatku (AMF).

## Domény kompetencí

Cílem zkoušky "PECB ISO/IEC 27001 Lead Implementer" je zajistit, aby kandidát získal potřebné kompetence pro podporu organizace při vytváření, zavádění, řízení a udržování systému managementu bezpečnosti informací (ISMS) na bázi požadavků ISO/IEC 27001.

Certifikace ISO/IEC 27001 Lead Implementer je určena pro:

- Manažery nebo konzultanty, kteří se podílejí na zavádění systému managementu bezpečnosti informací v organizaci a zabývají se touto problematikou
- Projektové manažery, konzultanty nebo odborné poradce, kteří chtějí zvládnout zavádění systému managementu bezpečnosti informací
- Osoby odpovědné za udržování souladu s požadavky normy ISO/IEC 27001 v organizaci
- Členům implementačního týmu ISMS

Zkouška pokrývá následující oblasti kompetencí:

- **Doména 1:** Základní principy a pojmy systému managementu bezpečnosti informací (ISMS)
- **Doména 2:** Systém managementu bezpečnosti informací (ISMS)
- **Doména 3:** Plánování zavedení ISMS na bázi normy ISO/IEC 27001
- **Doména 4:** Zavedení ISMS na základě normy ISO/IEC 27001
- **Doména 5:** Monitorování a měření ISMS na bázi normy ISO/IEC 27001
- **Doména 6:** Neustálé zlepšování ISMS na bázi normy ISO/IEC 27001
- **Doména 7:** Příprava na certifikační audit ISMS

PECB

## Doména 1: Základní principy a pojmy systému managementu bezpečnosti informací (ISMS)

**Hlavní cíl:** Zjistit, zda kandidát rozumí zásadám a pojmům ISO/IEC 27001 a zda je schopen je interpretovat

### Kompetence

1. Schopnost porozumět a vysvětlit hlavní pojmy bezpečnosti informací
2. Schopnost vysvětlit rozdíl a vztah mezi informacemi a aktivy
3. Schopnost pochopit rozdíl mezi dokumenty, specifikacemi a záznamy
4. Schopnost porozumět vztahu mezi pojmy zranitelnost, hrozba, riziko a jejich dopadem
5. Schopnost porozumět pojmům důvěrnost, integrita a dostupnost informací
6. Schopnost porozumět a interpretovat klasifikaci bezpečnostních opatření a jejich cílů.
7. Schopnost porozumět vztahům mezi prvky bezpečnosti informací

### Znalosti

1. Znalost zákonů, předpisů, mezinárodních a oborových norem, smluv, postupů na trhu, interních politik, osvědčených postupů atd., které musí organizace dodržovat
2. Znalost hlavních pojmů a terminologie normy ISO/IEC 27001
3. Znalost rizik bezpečnosti informací a jejich významu v ISMS
4. Znalost důvěrnosti, integrity a dostupnosti informací
5. Znalost zranitelností, hrozeb a rizik bezpečnosti informací
6. Znalost potenciálních dopadů, které mohou ovlivnit důvěrnost, integritu nebo dostupnost informací
7. Znalost rozdílů mezi typy bezpečnostních opatření, jako jsou technická, právní, administrativní a manažerská opatření
8. Znalost rozdílu mezi bezpečnostními opatřeními klasifikovanými podle jejich funkce, jako jsou preventivní, nápravné a detekční opatření

PECB

| **Doména 2: Systém managementu bezpečnosti informací (ISMS)**<br><br>**Hlavní cíl:** Zjistit, zda kandidát rozumí bezpečnostním opatřením uvedeným v příloze A normy ISO/IEC 27001 a zda je schopen je zavést | |
|---|---|
| **Kompetence** | **Znalosti** |
| 1. Schopnost vybrat, navrhnout a popsat opatření bezpečnosti informací<br>2. Schopnost definovat bezpečnostní architekturu organizace<br>3. Schopnost identifikovat a znázornit činnosti spojené s vývojem a nasazením informačních systémů<br>4. Schopnost dokumentovat implementaci vybraných opatření bezpečnosti informací<br>5. Schopnost porozumět, interpretovat a analyzovat opatření podle přílohy A ISO/IEC 27001<br>6. Schopnost zavést opatření podle přílohy A ISO/IEC 27001 a osvědčených postupů | 1. Znalost běžných bezpečnostních služeb, jako jsou služby řízení přístupu, služby ochrany na hranicích, služby integrity, kryptografické služby a služby auditu a monitorování<br>2. Znalost nejběžnějších architektonických rámců<br>3. Znalost 93 opatření přílohy A ISO/IEC 27001<br>4. Znalost čtyř skupin opatření přílohy A, jako jsou organizační, osobní, fyzická a technologická opatření<br>5. Znalost výběru a implementace opatření podle přílohy A ISO/IEC 27001<br>6. Znalost dokumentace vybraných opatření bezpečnosti informací |

PECB

## Doména 3: Plánování zavedení ISMS na bázi normy ISO/IEC 27001

**Hlavní cíl:** Zjistit, zda je kandidát schopen naplánovat zavedení ISMS na bázi ISO/IEC 27001

### Kompetence

1. Schopnost shromažďovat, analyzovat a interpretovat informace potřebné k plánování zavedení ISMS
2. Schopnost porozumět a stanovit cíle bezpečnosti informací a ISMS
3. Schopnost identifikovat a interpretovat rizika ISMS a jejich dopady
4. Schopnost analyzovat a zohlednit vnitřní a vnější kontext organizace
5. Schopnost identifikovat zdroje potřebné pro zavedení ISMS
6. Schopnost řídit, odhadovat a monitorovat zdroje potřebné pro zavedení ISMS
7. Schopnost identifikovat role a odpovědnosti klíčových zainteresovaných stran během a po zavedení a při provozování ISMS
8. Schopnost vypracovat, podat a přezkoumat plán projektu ISMS
9. Schopnost provést analýzu mezer a objasnit cíle managementu bezpečnosti informací
10. Schopnost definovat a zdůvodnit rozsah ISMS přizpůsobený konkrétním cílům organizace v oblasti bezpečnosti informací
11. Schopnost vypracovat a stanovit politiku ISMS
12. Schopnost provádět jednotlivé kroky procesu posouzení rizik
13. Schopnost porozumět a vypracovat dokument prohlášení o aplikovatelnosti

### Znalosti

1. Znalost hlavních pojmů, terminologie, procesů a osvědčených postupů projektového managementu
2. Znalost hlavních přístupů a metodik používaných při zavádění ISMS
3. Znalost typických cílů bezpečnosti informací a ISMS a způsobů dosažení konkrétních výsledků
4. Znalost toho, co typicky tvoří vnitřní a vnější kontext organizace
5. Znalost přístupů používaných k pochopení kontextu organizace
6. Znalost technik používaných ke sběru informací o organizaci a k provedení analýzy mezer v systému managementu
7. Znalost plánu projektu ISMS a projektového týmu ISMS
8. Znalost zdrojů potřebných pro zavedení ISMS
9. Znalost hlavních organizačních struktur použitelných v organizaci pro řízení ISMS
10. Znalost charakteristik rozsahu ISMS z hlediska organizačních, technologických a fyzických hranic
11. Znalost osvědčených postupů a technik používaných pro vypracování a stanovení politik a postupů bezpečnosti informací
12. Znalost různých přístupů a metodik používaných k provádění procesu hodnocení rizik
13. Znalost charakteristik dokumentu prohlášení o aplikovatelnosti

## Doména 4: Zavedení ISMS na základě normy ISO/IEC 27001

**Hlavní cíl:** Zjistit, zda je kandidát schopen zavést systém ISMS na základě požadavků ISO/IEC 27001

### Kompetence

1. Schopnost řídit procesy budování kapacit pro úspěšné zavedení ISMS
2. Schopnost definovat procesy správy dokumentace a záznamů potřebných pro podporu zavádění a provozování ISMS
3. Schopnost definovat, navrhnout a zavést procesy potřebné pro provoz ISMS a řádně je dokumentovat
4. Schopnost porozumět znalostem organizace, řídit je a vyhodnocovat
5. Schopnost porozumět současným světovým trendům a technologiím, jako jsou big data, umělá inteligence, strojové učení, cloud computing a outsourcovaný provoz
6. Schopnost definovat a realizovat vhodné programy školení a osvěty v oblasti bezpečnosti informací a plány komunikace
7. Schopnost vytvořit komunikační plán ISMS, který napomáhá pochopení problematiky bezpečnosti informací organizace, jejích politik, výkonnosti a poskytování podnětů nebo návrhů na zlepšení výkonnosti ISMS
8. Schopnost vytvořit politiku správy incidentů a tým pro reakci na incidenty
9. Schopnost porozumět rozdílu mezi kontinuitou činnosti organizace a obnovou po havárii

### Znalosti

1. Znalost osvědčených postupů v oblasti správy dokumentovaného životního cyklu informací
2. Znalost charakteristik a rozdílů mezi různými dokumentovanými informacemi souvisejícími s politikou, postupem, pokynem, normou, základním dokumentem, pracovním listem atd. v rámci ISMS
3. Znalost tří "V" velkých dat: objem, rozmanitost a rychlost
4. Znalost slabé a silné umělé inteligence, strojového učení
5. Znalost služeb cloud computingu: infrastruktura jako služba (IaaS), platforma jako služba (PaaS), software jako služba (SaaS)
6. Znalost dopadu nových technologií na bezpečnost informací
7. Znalost charakteristik a osvědčených postupů při zavádění programů školení a osvěty o bezpečnosti informací a plánů komunikace
8. Znalost komunikačních cílů, činností a zainteresovaných stran pro zvýšení jejich podpory a důvěry
9. Znalost procesu správy incidentů na základě osvědčených postupů bezpečnosti informací
10. Znalost kontinuity činnosti organizace a zotavení po havárii

PECB

| Doména 5: Monitorování a měření ISMS na bázi normy ISO/IEC 27001<br><br>**Hlavní cíl:** Zjistit, zda je kandidát schopen analyzovat, vyhodnocovat, monitorovat a měřit výkonnost ISMS | |
|---|---|
| **Kompetence** | **Znalosti** |
| 1. Schopnost monitorovat a hodnotit efektivnost ISMS<br>2. Schopnost ověřit, do jaké míry byly splněny stanovené cíle ISMS<br>3. Schopnost definovat a zavést program interního auditu ISMS<br>4. Schopnost provádět pravidelná a metodická přezkoumání s cílem zajistit vhodnost, přiměřenost, účinnost a efektivnost ISMS na základě politik a cílů organizace<br>5. Schopnost definovat a provádět proces přezkoumání vedením | 1. Znalost osvědčených postupů a technik používaných k monitorování a hodnocení efektivnosti ISMS<br>2. Znalost pojmů souvisejících s měřením a hodnocením<br>3. Znalost hlavních pojmů a složek souvisejících se zaváděním a provozem programu interního auditu ISMS<br>4. Znalost rozdílu mezi závažnou a méně závažnou neshodou<br>5. Znalost pokynů a osvědčených postupů pro vypracování zprávy o neshodě<br>6. Znalost osvědčených postupů používaných při provádění přezkoumání vedením |

PECB

## Doména 6: Neustálé zlepšování ISMS na bázi normy ISO/IEC 27001

**Hlavní cíl:** Zjistit, zda je kandidát schopen poskytovat pokyny k neustálému zlepšování ISMS

| Kompetence | Znalosti |
|---|---|
| 1. Schopnost sledovat neshody a přijímat příslušná opatření<br>2. Schopnost identifikovat a analyzovat základní příčiny neshod a navrhovat akční plány k jejich odstranění<br>3. Schopnost poradit organizaci, jak neustále zlepšovat efektivnost a účinnost ISMS<br>4. Schopnost zavádět v organizaci procesy neustálého zlepšování<br>5. Schopnost určit vhodné nástroje na podporu procesů neustálého zlepšování v organizaci | 1. Znalost hlavních postupů, nástrojů a technik používaných k identifikaci hlavních příčin neshod<br>2. Znalost procesu řešení neshod<br>3. Znalost hlavních procesů, nástrojů a technik používaných k vypracování plánů nápravných opatření<br>4. Znalost hlavních pojmů souvisejících s neustálým zlepšováním<br>5. Znalost procesů souvisejících s průběžným monitorováním faktorů změn<br>6. Znalost udržování a zlepšování ISMS |

## Doména 7: Příprava na certifikační audit ISMS

**Hlavní cíl:** Zjistit, zda je kandidát na pozici vedoucího implementátora ISO/IEC 27001 schopen připravit organizaci na certifikaci podle ISO/IEC 27001

| Kompetence | Znalosti |
|---|---|
| 1. Schopnost porozumět hlavním krokům, procesům a činnostem souvisejícím s certifikačním auditem ISO/IEC 27001<br>2. Schopnost porozumět, vysvětlit a ilustrovat přístup k důkazům auditu v rámci auditu ISMS<br>3. Schopnost poradit organizaci při identifikaci a výběru certifikačního orgánu, který splní její očekávání<br>4. Schopnost určit, zda je organizace připravena na certifikační audit ISO/IEC 27001<br>5. Schopnost vyškolit a připravit personál organizace na certifikační audit ISO/IEC 27001<br>6. Schopnost argumentovat a zpochybňovat zjištění a závěry auditu vůči externím auditorům | 1. Znalost přístupu k auditu založeného na důkazech<br>2. Znalost typů auditu a jejich rozdílů<br>3. Znalost rozdílů mezi audity 1. a 2. stupně<br>4. Znalost požadavků, kroků a činností v rámci 1. stupně auditu<br>5. Znalost kritérií přezkoumání dokumentovaných informací<br>6. Znalost požadavků, kroků a činností v rámci 2. stupně auditu<br>7. Znalost požadavků, kroků a činností souvisejících s následným auditem<br>8. Znalost požadavků, kroků a činností dozorových auditů a recertifikačních auditů<br>9. Znalost požadavků, pokynů a osvědčených postupů pro vypracování akčních plánů po certifikačním auditu ISO/IEC 27001 |

Vzhledem k výše uvedeným oblastem a jejich významu je do zkoušky zařazeno 80 otázek, které jsou shrnuty v následující tabulce:

| | | | | Požadovaná úroveň porozumění (kognitivní/taxonomická) | |
|---|---|---|---|---|---|
| | | Počet otázek/bodů pro každou doménu kompetencí | % otázek/bodů pro každou doménu kompetencí | Otázky, které měří porozumění, aplikaci a analýzu | Otázky, které měří syntézu a hodnocení |
| Domény kompetencí | Základní principy a pojmy systému managementu bezpečnosti informací (ISMS) | 15 | 18.75 | X | |
| | Systém managementu bezpečnosti informací (ISMS) | 12 | 15 | X | |
| | Plánování zavedení ISMS na bázi ISO/IEC 27001 | 18 | 22.5 | | X |
| | Zavádění ISMS na bázi ISO/IEC 27001 | 14 | 17.5 | | X |
| | Monitorování a měření ISMS na bázi ISO/IEC 27001 | 10 | 12.5 | X | |
| | Neustálé zlepšování ISMS na bázi ISO/IEC 27001 | 6 | 7.5 | X | |
| | Příprava na certifikační audit ISMS | 5 | 6.25 | | X |
| | Celkem | **80** | **100 %** | | |
| | Počet otázek na úroveň porozumění | | | **43** | **37** |
| | % zkoušky věnované jednotlivým úrovním porozumění (kognitivní/taxonomie) | | | **53.75 %** | **46.2 5%** |

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

Po úspěšném složení zkoušky budou moci kandidáti v závislosti na své úrovni zkušeností požádat o získání osvědčení "PECB Certified ISO/IEC 27001 Lead Implementer“.

## 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. **V listinné podobě:** 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 obsahuje otázky s výběrem odpovědi:** Tento formát byl zvolen proto, že se osvědčil jako efektivní a účinný pro měření a hodnocení výsledků učení souvisejících s definovanými oblastmi kompetencí. Zkouška s výběrem odpovědi může být použita k hodnocení kandidátova porozumění mnoha tématům, včetně jednoduchých i složitých pojmů. Při zodpovídání těchto otázek budou kandidáti muset aplikovat různé principy, analyzovat problémy, vyhodnocovat alternativy, kombinovat několik konceptů nebo myšlenek atd. Otázky s výběrem odpovědí jsou založeny na scénáři, což znamená, že jsou vypracovány na základě scénáře, který si mají kandidáti přečíst a očekává se od nich odpověď na jednu nebo více otázek souvisejících s tímto scénářem. Tato zkouška s výběrem odpovědí je "open book" vzhledem k tomu, že otázky jsou závislé na kontextu. Níže naleznete ukázku zkušebních otázek.

Vzhledem k tomu, že zkouška je "open book", mohou uchazeči používat následující referenční materiály:
- Tištěnou verzi normy ISO/IEC 27001
- Školicí materiály (přístupné prostřednictvím aplikace PECB Exams a/nebo vytištěné)
- Veškeré osobní poznámky z průběhu školení (přístupné prostřednictvím aplikace PECB Exams a/nebo vytištěné)

- Slovník v tištěné podobě

Jakýkoli pokus o kopírování, tajnou dohodu nebo jiné podvádění během zkoušky bude automaticky znamenat neúspěšný výsledek.

Zkoušky PECB jsou k dispozici v angličtině a dalších jazycích. Chcete-li zjistit, zda je zkouška dostupná v konkrétním jazyce, kontaktujte prosím examination.team@pecb.com.

**Poznámka:** PECB bude postupně přecházet na zkoušky s výběrem odpovědi. Ty budou rovněž "open book" a budou obsahovat otázky založené na scénáři, 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). Všechny zkoušky PECB s výběrem odpovědi mají jednu otázku a tři alternativní odpovědi, z nichž pouze jedna je správná.

F Konkrétní informace o typech zkoušek, dostupných jazycích a další podrobnosti naleznete na stránce List of PECB Exams.

## Příklady otázek ke zkoušce

**Scénář:**
Společnost A je pojišťovna se sídlem v Chicagu. Nabízí různé služby a produkty zahrnující zdravotní pojištění a pojištění vozidel. Společnost se v poslední době stala jednou z nejúspěšnějších a největších pojišťovacích společností s více než 70 pobočkami po celé zemi.

Cílem společnosti je řádná údržba aktiv a ochrana důvěrnosti informací o klientech. Společnost se rozhodla získat certifikaci podle normy ISO/IEC 27001, protože by jí to pomohlo nejen dosáhnout organizačních cílů a dodržovat mezinárodní zákony a předpisy, ale také zlepšit svou pověst. Společnost zahájila implementaci ISMS definováním implementační strategie na základě podrobné analýzy svých stávajících procesů a požadavků ISMS.

Zvláštní pozornost věnovala společnost posouzení rizik bezpečnosti informací, které bylo klíčové pro pochopení hrozeb a zranitelností, jimž čelila. Definovali také kritéria rizik s cílem vyhodnotit identifikovaná rizika.

Společnost A zaznamenala rychlý růst, který vedl ke složitému a intenzivnímu zpracování dat, a na základě výsledků posouzení rizik se rozhodla nejprve aktualizovat stávající schéma klasifikace informací a poté zavést potřebná bezpečnostní opatření podle úrovně ochrany, kterou jednotlivé klasifikace informací vyžadují.

Lékařské žádosti svých klientů, klasifikované jako citlivé informace, byly zašifrovány s využitím AES šifrování a poté přesunuty do privátního cloudu. Společnost A využívala cloudové úložiště pro jeho snadný přístup. Vzhledem k častému přístupu svých zaměstnanců k této službě se společnost rozhodla využít také proces protokolování. Služba byla nakonfigurována tak, aby automaticky udělovala přístup ke cloudovému úložišti všem zaměstnancům odpovědným za vyřizování lékařských žádostí.

Vzhledem k tomu, že u služeb cloudových úložišť docházelo k narušení bezpečnosti buď v důsledku lidské chyby, nebo úmyslných útoků, rozhodlo se IT oddělení společnosti omezit přístup k citlivým informacím uloženým v cloudu, pokud nebyly používány profesionální pracovní e-maily. Kromě toho použilo software pro správu hesel těchto e-mailových adres a generování silnějších hesel.

Na základě tohoto scénáře odpovězte na následující otázky:

1. **IT oddělení neomezilo přístup ke cloudovému úložišti. Která z níže uvedených hrozeb může tuto zranitelnost zneužít?**
   A. Manipulace s hardwarem
   B. **Neoprávněné použití citlivých informací**
   C. Nedostatečné školení v oblasti cloudových úložišť

2. **Společnost A šifruje citlivé informace před jejich přenesením do cloudu. Který proncip bezpečnosti informací je v tomto případě dodržena?**
   A. **Důvěrnost, protože šifrování zajišťuje, že k šifrovaným informacím mají přístup pouze oprávnění uživatelé**
   B. Dostupnost, protože šifrování zajišťuje, že informace jsou zabezpečeny buď v klidu, nebo při přenosu, a jsou tedy v případě potřeby dostupné
   C. Integrita, protože šifrování zajišťuje, že zašifrované informace jsou upravovány pouze autorizovanými uživateli

3. **Společnost A se rozhodla omezit přístup k citlivým informacím uloženým v cloudu, pokud nebudou použity profesionální pracovní e-maily. Jaké bezpečnostní opatření bylo v tomto případě zavedeno?**
   A. Detekční opatření
   B. **Preventivní opatření**
   C. Nápravné opatření

4. **Společnost A definovala kritéria rizik při posouzení svých rizik. Je to nutné?**
   A. **Ano, protože společnost má při posuzování rizik bezpečnosti informací stanovit a dodržovat kritéria rizik**
   B. Ne, protože kritéria rizik mají být stanovena až při stanovení možností ošetření rizik
   C. Ne, protože kritéria rizik se stanoví, když jsou přijímána zbytková rizika bezpečnosti informací

## Získání výsledků zkoušky

Výsledky zkoušek budou sděleny e-mailem.

- Časové rozmezí pro komunikaci začíná od data zkoušky a trvá dva až čtyři týdny u listinných zkoušek s výběrem odpovědí.

- U online zkoušek s výběrem odpovědí obdrží kandidáti výsledky okamžitě.

Kandidáti, kteří úspěšně absolvují zkoušku, budou moci požádat o jednu z referencí příslušného certifikačního schématu.

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

## Zásady opakování zkoušky

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

- Pokud kandidát neuspěje u zkoušky na první pokus, musí počkat 15 dní od prvního data zkoušky na další pokus (1. opakování).
  ***Poznámka:*** Kandidáti, kteří absolvovali vzdělávací kurz u některého z našich partnerů a neuspěli při prvním pokusu složit zkoušku, mají nárok na bezplatné opakování zkoušky během 12 měsíců od data obdržení kódu kupónu, protože poplatek zaplacený za vzdělávací kurz zahrnuje první pokus o složení zkoušky a jeden pokus o opakování zkoušky. 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 následujícím způsobem:

1. Online zkouška: při plánování opakování zkoušky použijte původní kupón kód pro osvobození od poplatku
2. Zkouška v listinné podobě: kandidáti se musí obrátit na 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 tato pravidla nevztahují. Postup pro naplánování opakování zkoušky je stejný jako v případě původní zkoušky.

## Zabezpečení zkoušky

Důležitou součástí profesního certifikátu je zachování bezpečnosti a důvěrnosti zkoušky. PECB spoléhá na etické chování držitelů certifikací a žadatelů o certifikaci, aby byla zachována bezpečnost a důvěrnost zkoušek PECB. Jakékoli zveřejnění informací o obsahu zkoušek PECB je přímým porušením etického kodexu PECB. PECB podnikne kroky proti všem osobám, které tato pravidla a zásady poruší, včetně trvalého zákazu usilovat o získání osvědčení PECB a odebrání všech předchozích osvědčení. PECB bude rovněž podnikat právní kroky proti jednotlivcům nebo organizacím, které porušují její autorská práva, vlastnická práva a duševní vlastnictví.

## Změna termínu zkoušky

V případě jakýchkoli změn týkajících se data, času, místa konání zkoušky nebo jiných podrobností se obraťte na adresu examination.team@pecb.com.

## Podání žádosti o certifikaci

Všichni kandidáti, kteří úspěšně složí zkoušku (nebo ekvivalentní zkoušku akceptovanou PECB), jsou oprávněni požádat o osvědčení PECB, pro které byli vyzkoušeni. Pro získání osvědčení PECB je třeba splnit zvláštní požadavky na vzdělání a odbornost. Kandidáti jsou povinni vyplnit online formulář žádosti o certifikaci (který je přístupný prostřednictvím jejich online profilu PECB), včetně kontaktních údajů k referencím, které budou kontaktovány za účelem ověření odborné praxe kandidáta. Kandidáti mohou svou žádost podat v různých jazycích. Kandidáti si mohou zvolit, zda chtějí zaplatit online, nebo si nechat vystavit platební doklad. Další informace získáte na adrese certification.team@pecb.com.

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

- Vytvořte si účet
- Zkontrolujte svůj e-mail pro potvrzení spojení
- Přihlaste se a požádejte o certifikaci

Více informací o procesu podávání žádostí naleznete v příručce Apply for Certification.

Žádost bude schválena, jakmile certifikační útvar potvrdí, že kandidát splňuje všechny požadavky certifikace týkající se příslušného osvědčení. Na e-mailovou adresu zadanou během procesu podávání žádosti bude zaslán e-mail, který informuje o stavu podané žádosti. V případě schválení si pak kandidáti budou moci stáhnout certifikát ze svého účtu PECB.

PECB poskytuje podporu v angličtině a francouzštině.

## Obnovení certifikace

Certifikáty PECB jsou platné tři roky. Aby si je kandidáti udrželi, musí každý rok prokázat, že stále vykonávají úkoly, které souvisejí s certifikací. Odborníci s certifikátem PECB musí každoročně dokládat kredity kontinuálního profesního rozvoje (CPD) a platit roční udržovací poplatek (AMF) ve výši 120 USD, aby si certifikát udrželi. Další informace naleznete na stránce Certification Maintenance na webových stránkách PECB.

## Uzavření případu

Pokud kandidáti nepožádají o certifikaci do tří let, bude jejich případ uzavřen. Přestože lhůta pro vydání osvědčení uplyne, kandidáti mají právo svůj případ znovu otevřít. PECB však již nebude odpovídat za jakékoli 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 a zaplatit požadovaný poplatek.

PECB

## SEKCE III: POŽADAVKY NA CERTIFIKACI

### ISO/IEC 27001 Lead Implementer

Požadavky na certifikaci PECB ISO/IEC 27001 Implementer jsou následující:

| Osvědčení | Zkouška | Pracovní zkušenosti | Zkušenosti s projekty MS | Další požadavky |
|---|---|---|---|---|
| **PECB Certified ISO/IEC 27001 Provisional Implementer** | Zkouška PECB Certified ISO/IEC 27001 Lead Implementer nebo ekvivalentní | Žádné | Žádné | Podepsání Etického kodexu PECB |
| **PECB Certified ISO/IEC 27001 Implementer** | Zkouška PECB Certified ISO/IEC 27001 Lead Implementer nebo ekvivalentní | Dva roky: Jeden rok praxe v managementu bezpečnosti informací | Projektové činnosti: celkem 200 hodin | Podepsání Etického kodexu PECB |
| **PECB Certified ISO/IEC 27001 Lead Implementer** | Zkouška PECB Certified ISO/IEC 27001 Lead Implementer nebo ekvivalentní | Pět let: Dva roky praxe v managementu bezpečnosti informací | Projektové činnosti: celkem 300 hodin | Podepsání Etického kodexu PECB |
| **PECB Certified ISO/IEC 27001 Senior Lead Implementer** | Zkouška PECB Certified ISO/IEC 27001 Lead Implementer nebo ekvivalentní | Deset let: Sedm let praxe v managementu bezpečnosti informací | Projektové činnosti: celkem 1.000 hodin | Podepsání Etického kodexu PECB |

Aby byly činnosti při implementaci považovány za platné, měly by se řídit osvědčenými postupy implementace a managementu a zahrnovat následující:

1. Návrh plánu ISMS
2. Zahájení implementace ISMS
3. Implementace ISMS
4. Řízení, monitorování a udržování ISMS
5. Identifikace příležitostí k neustálému zlepšování a jednání na základě těchto příležitostí

PECB

# SEKCE IV: PRAVIDLA A ZÁSADY CERTIFIKACE

## Profesní reference

Ke každé žádosti je třeba předložit dvě profesní reference. Musí se jednat o osoby, které s kandidátem spolupracovaly v pracovním prostředí a mohou potvrdit jeho zkušenosti v oblasti managementu rizik, jakož i jeho současnou a předchozí pracovní historii. Profesní reference osob, které spadají pod vedení kandidáta nebo jsou jeho příbuznými, nejsou platné.

## Profesní zkušenosti

Kandidáti musí uvést úplné a správné údaje o své pracovní praxi, včetně názvu (názvů) pracovní pozice, data zahájení a ukončení, popisu (popisů) pracovní pozice a další údaje. Kandidátům se doporučuje, aby shrnuli své předchozí nebo současné pracovní náplně a uvedli dostatečné podrobnosti k popisu povahy odpovědnosti za každou pracovní pozici. Podrobnější informace mohou být uvedeny v životopise.

## Zkušenosti s managementem rizik

Bude zkontrolován záznam o managementu rizik kandidáta, aby bylo ověřeno, že kandidát má požadovaný počet hodin v oblasti managementu rizik.

## Hodnocení žádostí o certifikaci

Certifikační útvar posoudí každou žádost, aby ověřil, zda je kandidát způsobilý pro certifikaci. 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 útvar potvrdí platnost žádosti na základě původních poskytnutých informací, což může případně vést k jejímu snížení na nižší stupeň certifikace.

## Zamítnutí vydání certifikátu

PECB může odmítnout certifikaci, pokud kandidáti:

- Zfalšují žádost
- Poruší postupy zkoušky
- Poruší etický kodex PECB
- Neuspějí u zkoušky

Podrobnější informace naleznete v sekci “Complaint and Appeal”.

Platba za žádost o certifikaci je nevratná.

## Pozastavení certifikace

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

- PECB obdrží velké množství nebo závažné stížnosti od zúčastněných stran (pozastavení bude uplatněno až do ukončení šetření).
- Loga PECB nebo akreditačních orgánů byla úmyslně zneužita.
- Kandidát neopraví zneužití certifikační značky ve lhůtě stanovené PECB.

- Certifikovaná osoba dobrovolně požádala o pozastavení.
- PECB uzná vhodnými jiné podmínky pro pozastavení certifikace.

## Zrušení certifikace

Pokud kandidát nesplní požadavky PECB, může mu PECB certifikaci odebrat. Kandidáti se pak již nesmějí prezentovat jako odborníci certifikovaní PECB. Dalšími důvody pro odebrání certifikace může být, pokud kandidáti:

- Poruší etický kodex PECB
- Zkreslují a poskytují nepravdivé informace o rozsahu certifikace
- Poruší jiná pravidla PECB

## Aktualizace osvědčení

Specialisté mohou požádat o zvýšení kvalifikace na vyšší stupeň, jakmile prokáží, že splňují požadavky.

Aby mohli kandidáti požádat o aktualizaci, musí se přihlásit ke svému účtu PECB, navštívit záložku "My Certifications" a kliknout na odkaz "Upgrade". Poplatek za žádost o aktualizaci činí 100 USD.

## Snížení úrovně osvědčení

Certifikát PECB může být snížen na nižší úroveň z následujících důvodů:

- AMF nebyl zaplacen
- Nebyly vykázány hodiny CPD
- Byl vykázán nedostatečný počet hodin CPD
- Na vyžádání nebyly předloženy doklady o vykázaných hodinách CPD

***Poznámka:*** *Certifikovaným odborníkům PECB, kteří jsou držiteli certifikátů Lead a nepředloží důkaz o splnění požadavků na udržování certifikace, bude sníženo jejich osvědčení. V případě držitelů certifikátů Master, kteří nepředloží CPD a nezaplatí AMF, budou jejich certifikáty zrušeny.*

## Ostatní stavy

Kromě toho, že je certifikace aktivní, pozastavená nebo zrušená, může být dobrovolně odvolána nebo označena jako emeritní. Více informací o těchto stavech a stavu trvalého ukončení a o tom, jak o ně požádat, naleznete na stránce Certification Status Options.

# SEKCE V: OBECNÉ ZÁSADY SPOLEČNOSTI PECB

## Etický kodex PECB

Dodržování Etického kodexu PECB je dobrovolné. Je důležité, aby profesionálové s certifikací PECB nejen dodržovali zásady tohoto kodexu, ale také aby k tomu vybízeli ostatní a podporovali je. Více informací naleznete zde.

## Další zkoušky a certifikace

PECB uznává certifikáty a zkoušky od jiných uznávaných akreditovaných certifikačních orgánů. PECB posoudí žádosti prostřednictvím svého procesu ekvivalence a rozhodne, zda je možné příslušnou(é) certifikaci(y) nebo zkoušku(y) přijmout jako ekvivalentní k příslušné certifikaci PECB (např. certifikace ISO/IEC 27001 Lead Auditor).

## Nediskriminace a zvláštní úpravy

Všechny žádosti kandidátů budou posuzovány 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 prodejce/distributora, aby mohl učinit příslušná opatření. Veškeré informace, které kandidáti poskytnou ohledně svého postižení/potřeby, budou považovány za přísně důvěrné.

Kliknutím zde si stáhněte formulář pro kandidáty se zdravotním postižením.

## Stížnosti 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 neshledá odpověď uspokojivou, má kandidát právo podat odvolání. Další informace o postupech podávání stížností a odvolání naleznete zde.

(1) Podle ADA může pojem "přiměřené úpravy" zahrnovat: (A) zpřístupnění stávajících zařízení, která zaměstnanci používají, osobám se zdravotním postižením a umožnění jejich užívání; a (B) restrukturalizaci pracovních míst, částečný nebo upravený pracovní úvazek, přeřazení na volné pracovní místo, pořízení nebo úpravu vybavení nebo zařízení, vhodnou úpravu nebo modifikaci zkoušek, školicích materiálů nebo zásad, zajištění kvalifikovaných čtenářů nebo tlumočníků a další podobné úpravy pro osoby se zdravotním postižením.

(2) Zákon o změnách ADA z roku 2008 (P.L. 110-325), § 12189. Zkoušky a kurzy. [§ 309]: Každá osoba, která nabízí zkoušky nebo kurzy související s přihláškami, udělováním licencí, certifikací nebo pověřením pro účely středoškolského nebo pomaturitního vzdělávání, profesního nebo obchodního vzdělávání, musí tyto zkoušky nebo kurzy nabízet na místě a způsobem přístupným osobám se zdravotním postižením nebo nabídnout alternativní přístupné úpravy pro tyto osoby.

**Adresa:**
Sídlo
6683 Jean Talon E,
Suite 336 Montreal,
H1S 0A5, QC,
KANADA

**Tel./Fax**
T: +1-844-426-7322
F: +1-844-329-7322

**Centrum podpory PECB**
Navštivte naše Help Center a projděte si často kladené otázky (FAQ), prohlédněte si příručky pro používání webových stránek a aplikací PECB, přečtěte si dokumenty týkající se procesů PECB nebo nás kontaktujte prostřednictvím online systému podpory.

**E-maily:**
Zkoušky: examination.team@pecb.com
Certifikace: certification.team@pecb.com
Zákaznický servis: support@pecb.com



www.pecb.com