Start

Opowieść, wybór certyfikatu, plan i laboratorium.

- Certyfikat z ISO/IEC 27001: od rejestru audytorów jakości do PECB Lead Implementer
- Plan 28 dni i papierowe laboratorium: Tomek wdraża ISMS w Zielonej

Certyfikat z ISO/IEC 27001: od rejestru audytorów jakości do PECB Lead Implementer

Poziom: podstawy

Dotyczy: certyfikaty osobiste z ISO/IEC 27001:2022, egzamin PECB ISO/IEC 27001 Lead Implementer, stan na 23 października 2026

Czas: ~20 min

Ta strona otwiera kurs do egzaminu osobistego z normy ISO/IEC 27001. Opowiada, skąd wzięli się certyfikowani audytorzy i wdrażający systemy zarządzania, porównuje certyfikaty dostępne w październiku 2026 roku i wyjaśnia, dlaczego celem tej książki jest PECB ISO/IEC 27001 Lead Implementer. Na końcu mapa książki.

Egzamin z ISO/IEC 27001 nie pyta, jak skonfigurować zaporę. Pyta, co zrobi osoba prowadząca wdrożenie, gdy prezes nie chce podpisać polityki, gdy zakres systemu nie obejmuje magazynu, a audytor znajduje rejestr ryzyk sprzed dwóch lat. To egzamin z zarządzania, w którym technika jest tłem.

Skąd wzięła się sama norma, od brytyjskiego kodeksu praktyki do wydania z 2022 roku, opowiada pierwsza strona książki „ISO/IEC 27001: bezpieczeństwo informacji po ludzku” na półce Standardy pracy: ISO/IEC 27001: od podręcznika Shella do certyfikatu Zielonej. Tam też leżą zabezpieczenia omówione po ludzku, przebieg audytu w firmie i przepisy. Tu tej historii nie powtarzamy: ta książka uczy do egzaminu osobistego.

> Zakres: nie cytujemy tekstu norm ISO ani materiałów szkoleniowych PECB. Definicje są naszą parafrazą z przypisem, a pytania próbne piszemy sami, bez oficjalnych arkuszy i bez tak zwanych dumpów. Do egzaminu i tak potrzebujemy własnego, kupionego egzemplarza normy.

Skróty użyte na tej stronie (24)

Skrót	Co znaczy
AMF	Annual Maintenance Fee: opłata PECB za utrzymanie certyfikatu osobistego w trzyletnim cyklu
APMG	APM Group: brytyjska organizacja akredytująca szkolenia i egzaminy, ma między innymi certyfikaty ISO/IEC 27001 Foundation i Practitioner
B2B	business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych
BSI	British Standards Institution: brytyjska organizacja normalizacyjna, która wydała BS 7799, a dziś także certyfikuje firmy i prowadzi szkolenia, również w Polsce
COFRAC	Comité français d'accréditation: francuska krajowa jednostka akredytująca
CPD	Continuing Professional Development: ciągły rozwój zawodowy; godziny albo punkty szkoleń, które zbieramy, żeby utrzymać certyfikat bez ponownego egzaminu (np. w PeopleCert Plus dla ITIL albo w PECB)
CQI	Chartered Quality Institute: brytyjska organizacja zawodowa specjalistów jakości, prowadzi rejestr audytorów IRCA
EXIN	Examination Institute for Information Science: holenderski dostawca egzaminów IT, między innymi Information Security Foundation
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
IAS	International Accreditation Service: amerykańska jednostka akredytująca, akredytuje między innymi PECB jako jednostkę certyfikującą osoby
IQA	Institute of Quality Assurance: brytyjski instytut zapewnienia jakości, przy którym w 1984 roku powstał rejestr audytorów, dziś CQI
IRCA	International Register of Certificated Auditors: rejestr certyfikowanych audytorów systemów zarządzania prowadzony przez brytyjskie CQI, z kursami zatwierdzonymi u partnerów szkoleniowych
ISMS	Information Security Management System: system zarządzania bezpieczeństwem informacji, czyli polityka, role, ocena ryzyka, cele, pomiar, audyt i doskonalenie, które decydują o zabezpieczeniach i sprawdzają, czy działają
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
PARP	Polska Agencja Rozwoju Przedsiębiorczości: prowadzi Bazę Usług Rozwojowych, w której firmy szkoleniowe publikują szkolenia z dofinansowaniem
PCBC	Polskie Centrum Badań i Certyfikacji: polska jednostka certyfikująca wyroby i systemy zarządzania, w tym ISO/IEC 27001
PECB	Professional Evaluation and Certification Board: kanadyjska jednostka certyfikująca osoby według ISO/IEC 17024, wydaje między innymi certyfikaty ISO/IEC 27001 Lead Implementer i Lead Auditor

Skrót	Co znaczy
PKN	Polski Komitet Normalizacyjny: instytucja, która wydaje polskie wersje norm i sprzedaje je w katalogu
PN-EN	Polska Norma będąca wersją normy europejskiej, np. PN-EN 54 dla elementów systemów sygnalizacji pożaru
PR373	numer kursu CQI i IRCA ISO/IEC 27001:2022 Lead Auditor; pięciodniowe szkolenie u partnera z oceną ciągłą i egzaminem online
TÜV	Technischer Überwachungsverein: niemieckie organizacje nadzoru technicznego (na przykład TÜV SÜD, TÜV NORD), które certyfikują firmy i prowadzą szkolenia audytorów
UKAS	United Kingdom Accreditation Service: brytyjska krajowa jednostka akredytująca
USD	dolar amerykański, waluta cenników AWS

Skąd się wzięło

> **Pojęcie: certyfikat osobisty.** Potwierdzenie wydane konkretnej osobie, że zna normę i umie z niej korzystać. Różni się od certyfikatu firmy: Zielona może mieć certyfikat ISO/IEC 27001 na swój system, a Tomek osobny certyfikat na swoją wiedzę. Jedno nie wymaga drugiego.

Zawód audytora systemu zarządzania urodził się przy jakości. Organizacja, z której wyrosło dzisiejsze brytyjskie CQI (Chartered Quality Institute), powstała w 1919 roku, żeby ograniczyć wadliwą amunicję po pierwszej wojnie światowej, a w 1972 roku przyjęła nazwę Institute of Quality Assurance [16]. Gdy w 1979 roku pojawiła się brytyjska norma systemu jakości BS 5750, a w 1987 roku jej międzynarodowa następczyni ISO 9001, firmy zaczęły zamawiać audyty u niezależnych jednostek. Ktoś musiał sprawdzać, czy audytorzy tych jednostek sami są kompetentni.

W 1984 roku przy IQA powstał Register of Lead Assessors, rejestr wiodących oceniających, który w ciągu następnej dekady stał się IRCA (International Register of Certificated Auditors) [16]. Model był prosty i przetrwał do dziś: zatwierdzony kurs, egzamin, udokumentowane audyty i coroczna opłata za wpis do rejestru. Ciekawostka: pierwsi audytorzy nazywali się oceniającymi (assessors), a słowo „lead” od początku oznaczało osobę, która prowadzi zespół audytorów, a nie po prostu starszego audytora.

Bezpieczeństwo informacji przejęło ten model gotowy. Brytyjski kodeks praktyki BS 7799 z 1995 roku dostał część z wymaganiami, którą dało się certyfikować, a w 2005 roku z tej części powstała międzynarodowa norma ISO/IEC 27001. Równolegle świat systemów zarządzania ujednolicił reguły gry: w 2002 roku ISO 19011 dała jedne wytyczne audytowania dla jakości i środowiska, w 2003 roku ISO/IEC 17024 opisała, jak ma działać jednostka certyfikująca osoby, a ISO/IEC 17021 (dziś 17021-1) opisała jednostki certyfikujące systemy.

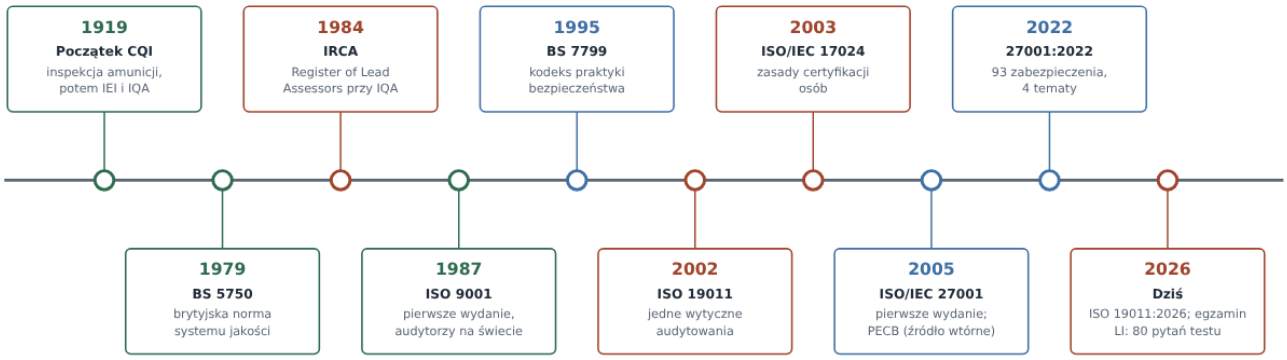
> **Pojęcie: jednostka certyfikująca osoby.** Organizacja, która przeprowadza egzaminy i wydaje certyfikaty osobiste według ISO/IEC 17024, a sama jest sprawdzana przez jednostkę akredytującą. PECB ma taką akredytację między innymi w amerykańskim IAS, brytyjskim UKAS i francuskim COFRAC [21].

W ofercie PECB, kanadyjskiej organizacji z Montrealu założonej według źródła wtórnego w 2005 roku [20], obok ścieżki audytora stoi równoległa ścieżka wdrażającego. Lead Auditor sprawdza, czy system działa, a Lead Implementer go buduje. Obie ścieżki mają te same stopnie zależne od doświadczenia, ten sam rodzaj egzaminu i to samo odnawianie.

Certyfikaty osobiste z norm systemów zarządzania: od rejestru audytorów jakości do ISO/IEC 27001 w 2026

Najpierw audytorzy jakości i ich rejestr, potem wspólne wytyczne audytowania i zasady certyfikacji osób, a na końcu bezpieczeństwo informacji z własnymi ścieżkami dla wdrażających i audytorów.

oś czasu (10 kamieni milowych)



Oś nie jest w skali. Zielony: normy jakości, niebieski: normy bezpieczeństwa informacji, czerwony: audytorzy i certyfikacja osób.

wniosek

Zawód audytora systemu zarządzania urodził się przy jakości, a bezpieczeństwo informacji przejęło od niego gotowy model: norma z wymaganiami, wytyczne audytowania, rejestr osób z egzaminem i doświadczeniem. Dlatego egzamin z ISO/IEC 27001 pyta tyle samo o zarządzanie, co o technikę.

Rysunek 1. Oś czasu: od organizacji kontrolującej amunicję w 1919 roku, przez rejestr audytorów IRCA, ISO 9001, BS 7799 i ISO 19011, po ISO/IEC 27001:2022 i egzamin wielokrotnego wyboru PECB w 2026 roku (kliknięcie otwiera pełny rozmiar)

Stan w 2026 roku

Obowiązuje ISO/IEC 27001:2022 z poprawką Amd 1:2024, która dopisała do rozdziałów o kontekście organizacji pytanie o zmiany klimatu [18]. Okres przejściowy dla certyfikatów według wydania z 2013 roku skończył się 31 października 2025 roku [18], [19]. W maju 2026 roku ukazało się czwarte wydanie ISO 19011, ewolucyjne, z szerszymi wytycznymi o audytach zdalnych [17], a według źródła wtórnego 3 lipca 2026 roku ISO/IEC 27000:2026 z przeglądem rodziny norm i

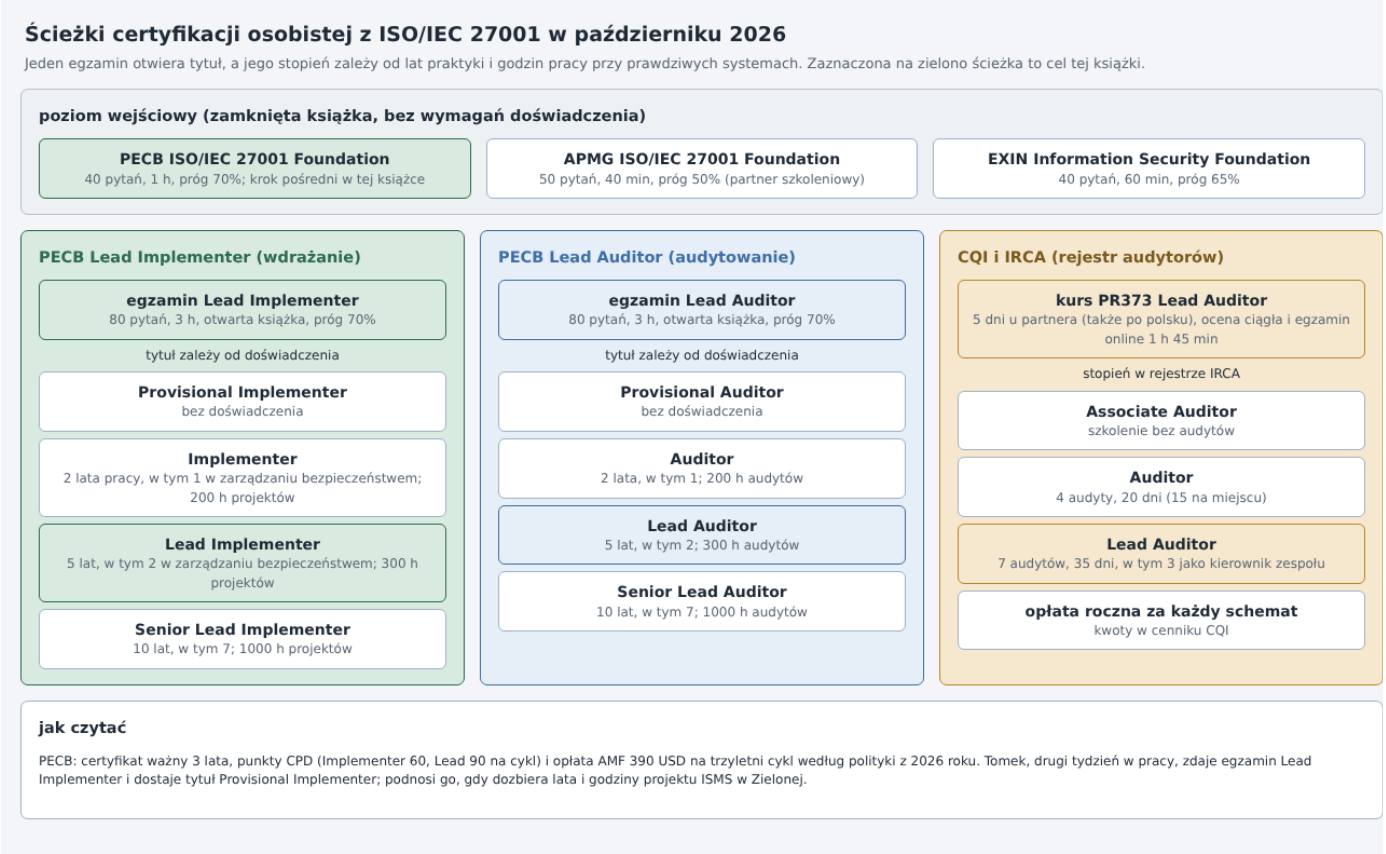
słownikiem [18]. Nowego wydania ISO/IEC 27001 na 23 października 2026 roku nie ma.

PECB zmienił egzamin Lead Implementer z dwunastu pytań opisowych (podręcznik kandydata w wersji 8.0 z 2023 roku) na 80 pytań wielokrotnego wyboru ze scenariuszami (podręcznik w wersji 1.5 z 2026 roku) [2]. Materiały sprzed zmiany wciąż krążą w internecie, więc przy każdym źródle sprawdzamy, który format opisuje.

Jak to działa w jednym obrazku

Rozwiń: jak to działa pod spodem

Egzamin jest jeden dla wszystkich stopni ścieżki. To, czy po zdaniu dostaniemy tytuł Provisional Implementer, Implementer, Lead Implementer czy Senior Lead Implementer, zależy od lat pracy i godzin przy projektach systemów zarządzania, które deklarujemy we wniosku i potwierdzamy referencjami.



Rysunek 2. Ścieżki certyfikacji osobistej z ISO/IEC 27001 w październiku 2026: poziom wejściowy, PECB Lead Implementer, PECB Lead Auditor i rejestr CQI i IRCA (kliknięcie otwiera

pełny rozmiar)

Wybór certyfikatu

Dane z podręczników kandydata, stron dostawców i partnerów szkoleniowych, zebrane 23 października 2026 roku. Opłaty bez podatków.

Certyfikat	Dla kogo	Egzamin	Doświadczenie do pełnego tytułu	Szkolenie	Koszt orientacyjny	Po polsku
PECB ISO/IEC 27001 Foundation	kto zaczyna i chce szybkiego potwierdzenia	40 pytań, 3 odpowiedzi, 1 h, zamknięta książka, próg 70% [3], [5]	brak	podręcznik kandydata wymienia kurs, egzamin można kupić osobno [3], [8] (do potwierdzenia dla Foundation)	egzamin 500 USD i wniosek 200 USD [3]	do potwierdzenia
PECB ISO/IEC 27001 Lead Implementer	wdrażający, administrator w projekcie ISMS	80 pytań, 3 odpowiedzi, scenariusze, 3 h, otwarta książka, próg 70%, online [2], [5]	Lead: 5 lat pracy, w tym 2 w zarządzaniu bezpieczeństwem informacji, i 300 h projektów [2]	nieobowiązkowe: egzamin bez kursu przez myPECB [8]	egzamin 1000 USD, wniosek 500 USD, AMF 390 USD na trzy lata [2], [6]	do potwierdzenia
PECB ISO/IEC 27001 Lead Auditor	audytor wewnętrzny i zewnętrzny	80 pytań, scenariusze, 3 h, otwarta książka, próg 70% [4], [5]	Lead: 5 lat, w tym 2, i 300 h audytów [4]	jak wyżej	jak wyżej	do potwierdzenia
CQI i IRCA, kurs PR373 Lead Auditor	audytor jednostki certyfikującej	ocena ciągła 70% i egzamin online 40 pytań, 1 h 45 min, otwarta książka, minimum w każdej części i 50% razem [11], [12]	Lead Auditor w rejestrze: 7 audytów, 35 dni, w tym 3 jako kierownik [10]	obowiązkowy 5-dniowy kurs u partnera	w Polsce kurs od 3990 zł [13], potem opłata roczna CQI	kurs tak [13], egzamin według przewodnika z 2024 roku po angielsku [11]

Certyfikat	Dla kogo	Egzamin	Doświadczenie do pełnego tytułu	Szkolenie	Koszt orientacyjny	Po polsku
APMG ISO/IEC 27001 Foundation i Practitioner	alternatywa dwustopniowa	Foundation 50 pytań, 40 min, 50%; Practitioner 4 pytania po 20 punktów, 2,5 h, otwarta książka [14]	brak	u partnera	pakiet od 799 EUR [14]	do potwierdzenia
EXIN Information Security Foundation	ogólne podstawy bezpieczeństwa	40 pytań, 60 min, 65%, zamknięta książka [15]	brak	nieobowiązkowe	do potwierdzenia	do potwierdzenia

> Krótkie szkolenia „audytor wewnętrzny ISO/IEC 27001” u polskich jednostek certyfikujących (na przykład dwa dni z testem na koniec [22]) dają zaświadczenie firmy szkoleniowej, a nie certyfikat osobisty akredytowany według ISO/IEC 17024. Do audytów w Zielonej wystarczą, do tytułu z tej książki nie.

Nasz wybór: PECB ISO/IEC 27001 Lead Implementer. Uzasadnienie w czterech punktach:

1. Treść pasuje do pracy administratora: domeny obejmują cały cykl, od kontekstu i ryzyka, przez wdrożenie, po audyt wewnętrzny i przygotowanie do certyfikacji. Wdrażający musi rozumieć audyt, odwrotnie nie zawsze.
2. Egzamin da się zdać bez kursu, online, z wydrukowaną normą na biurku [2], [8]. Szkolenie u partnera jest wygodniejsze (zawiera egzamin, darmową poprawkę, wniosek i pierwszy rok AMF [7]), ale nie jest warunkiem.
3. Tytuł rośnie razem z doświadczeniem: Tomek dostanie Provisional Implementer, a po projekcie w Zielonej może wnioskować o wyższy stopień bez nowego egzaminu.
4. Foundation traktujemy jako krok pośredni, opcjonalny: jego dwie domeny pokrywają się z dwiema pierwszymi domenami egzaminu Lead Implementer, ale kosztuje 700 USD za tytuł, który nic nie dodaje do celu. Lead Auditor (PECB albo IRCA PR373) to alternatywa dla kogoś, kto chce audytować inne firmy: IRCA jest wtedy lepiej rozpoznawalna wśród jednostek certyfikujących, ale wymaga pięciodniowego kursu.

Dlaczego Zielona

Z ŻYCIA WZIĘTE

Wtorek, 10:40. Pan Zbigniew przynosi wydruk ankiety od sieci handlowej, największego odbiorcy sklepu B2B: za półtora roku wszyscy dostawcy z dostępem do ich systemu zamówień mają mieć certyfikat ISO/IEC 27001 albo udowodnić, że do niego idą. Pan Wojtek, który co roku pyta nas o kopie i konta byłych pracowników, mówi, że „to nie jest projekt IT, tylko projekt firmy, ale bez IT się nie uda". Ustalamy, że Tomek w cztery tygodnie zda Lead Implementer, a w trakcie nauki zrobi na papierze całe wdrożenie dla Zielonej: zakres, rejestr ryzyk, deklarację stosowania, politykę i plan audytu.

Zielona ma już kawałki systemu, tylko porozrzucane: kopie zapasowe z testami odtwarzania, zgłoszenia i zmiany w GLPI, kontrolę dostępu do serwerowni, Defendera na stacjach. Brakuje tego, co spina je w system: zakresu, oceny ryzyka, decyzji kierownictwa, celów i dowodu, że ktoś to sprawdza. Każda strona tej książki kończy się artefaktem tego projektu, a po egzaminie teczka z artefaktami będzie punktem wyjścia do prawdziwego wdrożenia.

Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę
Egzamin Lead Implementer to dwanaście pytań opisowych.	Tak było do zmiany formatu. Podręcznik kandydata z 2026 roku opisuje 80 pytań wielokrotnego wyboru z trzema odpowiedziami [2].
Bez pięciodniowego kursu nie można podejść do egzaminu PECB.	Można: egzamin kupujemy w panelu myPECB, bez materiałów kursu [8]. Kurs jest obowiązkowy w ścieżce IRCA.
Otwarta książka znaczy łatwo.	Trzy godziny na 80 pytań to nieco ponad dwie minuty na pytanie. Kto szuka każdej odpowiedzi w normie, nie zdąży.
Po zdaniu jesteśmy Lead Implementerem.	Tytuł zależy od doświadczenia. Bez lat praktyki dostajemy Provisional Implementer [2].
Certyfikat jest na zawsze.	Ważność to trzy lata, z punktami CPD i opłatą AMF [6].
Kto zna zabezpieczenia, zda.	Zabezpieczenia to część jednej domeny. Najwięcej pytań dotyczy planowania, ryzyka i decyzji kierownictwa.

Mapa tej książki

Książka ma osiem stron w czterech rozdziałach.

Strona	Na jakie pytanie odpowiada

Certyfikat z ISO/IEC 27001: od rejestru audytorów jakości do PECB Lead Implementer	Skąd się wzięły certyfikaty osobiste, który wybrać, jak wygląda egzamin w 2026 roku
Plan 28 dni i papierowe laboratorium: Tomek wdraża ISMS w Zielonej	Co robimy którego dnia, jak kupić egzamin i normę, jakie artefakty powstaną
Zasady, pojęcia i wymagania ISMS: domeny 1 i 2 egzaminu	Czym jest system zarządzania, co jest w rozdziałach 4 do 10 i w załączniku A
Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA	Jak zacząć projekt, wyznaczyć zakres, ocenić ryzyko i napisać deklarację stosowania
Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany	Jak z planu zrobić działający system i zostawić dowody
Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania	Skąd wiemy, że system działa, jak prowadzić audyt według ISO 19011
Ciągłe doskonalenie i audyt certyfikacyjny: od niezgodności do certyfikatu	Co z niezgodnościami, jak przebiega certyfikacja według ISO/IEC 17021-1
Próbny egzamin Lead Implementer: 80 własnych pytań i strategia na dzień egzaminu	Czy jesteśmy gotowi i jak przejść trzy godziny z otwartą książką

Nota metodyczna: czego nie wiemy

- Czy egzamin PECB Lead Implementer i Foundation jest dostępny po polsku. Podręczniki odsyłają do listy egzaminów PECB, a polskiej wersji podręcznika nie znaleźliśmy (jest czeska). Język wybieramy przy zapisie w myPECB.
- Czy opłata AMF 390 USD dotyczy całego trzyletniego cyklu, czy jest rozkładana na lata. Polityka PECB z 2026 roku podaje kwotę „na trzy lata” w części zatytułowanej „roczne opłaty” [6], a źródło wtórne podaje 100 USD rocznie [23].
- Czy egzamin CQI i IRCA po kursie po polsku jest prowadzony po polsku. Przewodnik dla kandydatów z 2024 roku mówi o egzaminie po angielsku z dodatkowymi 30 minutami [11].
- Daty powstania PECB: źródło wtórne [20], PECB jej nie podaje.
- Czy polska wersja językowa PN-EN ISO/IEC 27001 już się ukazała: w marcu 2024 roku PCBC pisała, że nie [19]. Sprawdzamy w katalogu PKN.

Powiązane: ITIL Foundation (Version 5): egzamin, zapis i plan na 14 dni · Standard pracy administratora Zielonej: zasady na pierwszy dzień · Bezpieczeństwo fizyczne: skąd się wzięły

zamki, karty i kamery i dlaczego serwerownia nie wystarczy zamknąć na klucz

Źródła

Dostęp 23 października 2026.

[1] PECB, strona szkolenia ISO/IEC 27001 Lead Implementer (agenda pięciu dni, siedem domen, poziomy certyfikatu, 31 punktów CPD za szkolenie). [2] PECB, Candidate Handbook ISO/IEC 27001 Lead Implementer (multiple choice), wersja 1.5, 2026 (80 pytań, trzy odpowiedzi, scenariusze po pięć pytań, próg 70%, otwarta książka, liczba pytań w domenach, wymagania doświadczenia, opłaty); dla porównania wersja 8.0 z 2023 roku (12 pytań opisowych). [3] PECB, Candidate Handbook ISO/IEC 27001:2022 Foundation, wersja 1.5, 2026. [4] PECB, Candidate Handbook ISO/IEC 27001 Lead Auditor (multiple choice), wersja 1.5, 2026. [5] PECB Support, „What is the duration of an exam” (Foundation 1 h, Lead 3 h, dodatkowy czas). [6] PECB, Certification Maintenance Policy 2026 (AMF, CPD 60, 90, 180 godzin na cykl). [7] PECB, Exam Rules and Policies (poprawki, materiały, termin 12 miesięcy). [8] PECB Help, „How do I schedule an exam if I did not attend a PECB training event”. [9] PECB, myPECB Online Examinee Manual. [10] CQI i IRCA, strony stopni Auditor i Lead Auditor. [11] CQI i IRCA, Online Exams Guide for Learners, 2024 (udostępniany przez BSI). [12] TÜV SÜD, strona kursu PR373 ISMS Lead Auditor (punktacja i ocena ciągła; źródło partnera). [13] BSI Polska, „Audytor Wiodący ISO/IEC 27001:2022 (CQI/IRCA)” i „ISO/IEC 27001:2022 Lead Implementer” (ceny, język). [14] Innovative Learning, pakiet APMG ISO/IEC 27001 Foundation i Practitioner (źródło partnera). [15] Skillsoft Global Knowledge, EXIN Information Security Foundation (źródło partnera). [16] CQI, „Our history”. [17] CQI, „ISO 19011:2026 revision: guidance for management system auditing”. [18] Bright Defense, „ISO 27001: What Changed in 2026?” (źródło wtórne). [19] PCBC, komunikat z 5 marca 2024 o przejściu na ISO/IEC 27001:2022. [20] EverybodyWiki, PECB (źródło wtórne). [21] PECB, Accreditations and Affiliations. [22] Baza Usług Rozwojowych PARP, szkolenie TÜV SÜD Polska „Auditor wewnętrzny systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001:2022”, luty 2026. [23] RiskProfs, „PECB ISO 27001 certification cost”, czerwiec 2026 (źródło wtórne).

Plan 28 dni i papierowe laboratorium: Tomek wdraża ISMS w Zielonej

Poziom: podstawy

Dotyczy: egzamin PECB ISO/IEC 27001 Lead Implementer (podręcznik kandydata 1.5, 2026), ISO/IEC 27001:2022 z Amd 1:2024, stan na 23 października 2026

Czas: ~30 min czytania, potem 28 dni po półtorej do dwóch godzin

Egzamin w liczbach, zapis i egzamin online, a potem plan na 28 dni z laboratorium, które nie wymaga ani jednego serwera: Tomek wdraża system zarządzania bezpieczeństwem informacji w Zielonej jako projekt ćwiczeniowy i co kilka dni oddaje jeden artefakt. Wracamy tu codziennie, żeby sprawdzić, co dziś, i dzień przed egzaminem, żeby przejść listę kontrolną.

Na egzaminie Lead Implementer laboratorium nie ma klawiatury: są scenariusze firm i pytania, co zrobi osoba prowadząca wdrożenie. Najlepszym treningiem jest więc zrobić wdrożenie samemu, choćby na papierze. Każdy artefakt z tej strony odpowiada jednemu z wymagań normy, a gotowa teczka posłuży Zielonej jako punkt startowy prawdziwego projektu.

ZAŁOŻENIA SCENARIUSZA

w laboratorium zakres ISMS Zielonej obejmuje usługi IT świadczone przez zespół IT dla całej firmy, w tym serwerownię w Pamiątkowie i magazyn w Swarzędzu; sklep B2B i jego dostawca oprogramowania są stroną zainteresowaną i dostawcą, a nie częścią zakresu. Zakres „cała firma”, który Zielona proponuje naprawdę, opisuje Zakres i ryzyko w Zielonej: rejestr aktywów, macierz ryzyka i plan postępowania; w laboratorium ćwiczymy węższy wariant.

Skróty użyte na tej stronie (12)

Skrót	Co znaczy
AMF	Annual Maintenance Fee: opłata PECB za utrzymanie certyfikatu osobistego w trzyletnim cyklu
B2B	business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych

Skrót	Co znaczy
CPD	Continuing Professional Development: ciągły rozwój zawodowy; godziny albo punkty szkoleń, które zbieramy, żeby utrzymać certyfikat bez ponownego egzaminu (np. w PeopleCert Plus dla ITIL albo w PECB)
ISMS	Information Security Management System: system zarządzania bezpieczeństwem informacji, czyli polityka, role, ocena ryzyka, cele, pomiar, audyt i doskonalenie, które decydują o zabezpieczeniach i sprawdzają, czy działają
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
PECB	Professional Evaluation and Certification Board: kanadyjska jednostka certyfikująca osoby według ISO/IEC 17024, wydaje między innymi certyfikaty ISO/IEC 27001 Lead Implementer i Lead Auditor
PKN	Polski Komitet Normalizacyjny: instytucja, która wydaje polskie wersje norm i sprzedaje je w katalogu
SoA	Statement of Applicability: deklaracja stosowania, dokument wymagany przez ISO/IEC 27001, który dla każdego zabezpieczenia z załącznika A mówi, czy je stosujemy, dlaczego i czy jest wdrożone
USD	dolar amerykański, waluta cenników AWS
UTC	Coordinated Universal Time: uniwersalny czas bez strefy, punkt odniesienia dla wszystkich stref czasowych na świecie
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

Karty artefaktów laboratorium i czynności organizacyjnych. Czytamy nagłówek, zakrywamy resztę i mówimy z pamięci, co ma zawierać artefakt i któremu wymaganiu odpowiada.

□□ TYLKO ODCZYT

Założenie teczki: ISMS-cwiczenie

Katalog `\\fs01\IT\ISMS-cwiczenie` z podkatalogami `artefakty`, `notatki` i `dziennik`. Każdy plik ma w nazwie numer artefaktu i wersję, na przykład `A4-rejestr-ryzyk-v0.3.xlsx`, bo nadzór nad wersjami to też wymaganie normy (rozdział 7.5).

□□ **IT** = Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

TYLKO ODCZYT

Przygotowanie artefaktu A1: karta projektu i analiza luk

Cel projektu, sponsor (pan Zbigniew), kierownik (my), zespół, budżet, ryzyka projektu, harmonogram. Do tego analiza luk: tabela wymagań rozdziałów 4 do 10 ze stanem „jest, częściowo, brak” i dowodem.

TYLKO ODCZYT

Przygotowanie artefaktu A2: kontekst, strony zainteresowane i zakres

Sprawy wewnętrzne i zewnętrzne, w tym klimat (Amd 1:2024), lista stron zainteresowanych z ich wymaganiami, zaznaczenie, które wymagania spełnia system, oraz opis zakresu z granicami, lokalizacjami i stykami z tym, co poza zakresem (rozdziały 4.1 do 4.3).

TYLKO ODCZYT

Przygotowanie artefaktu A3: polityka bezpieczeństwa informacji i role

Jedna do dwóch stron polityki podpisanej przez kierownictwo, z zobowiązaniem do spełniania wymagań i do doskonalenia, oraz macierz ról: kto za co odpowiada, kto zatwierdza, kogo informujemy (rozdziały 5.2 i 5.3).

TYLKO ODCZYT

Przygotowanie artefaktu A4: metodyka i rejestr ryzyk

Kryteria akceptacji ryzyka, skale skutku i prawdopodobieństwa, sposób liczenia poziomu, a potem co najmniej dziesięć ryzyk Zielonej z właścicielami (rozdziały 6.1.2 i 8.2).

TYLKO ODCZYT

Przygotowanie artefaktu A5: plan postępowania z ryzykiem

Dla każdego ryzyka powyżej progu: wybrana opcja, zabezpieczenia, odpowiedzialny, termin, ryzyko szczątkowe i podpis właściciela ryzyka (rozdziały 6.1.3 i 8.3).

TYLKO ODCZYT

Przygotowanie artefaktu A6: deklaracja stosowania i cele

Wycinek deklaracji stosowania (SoA) z dwudziestoma zabezpieczeniami: czy stosujemy, dlaczego, czy wdrożone. Do tego trzy mierzalne cele bezpieczeństwa informacji z terminem i właścicielem (rozdziały 6.1.3 d i 6.2).

SoA = Statement of Applicability: deklaracja stosowania, dokument wymagany przez ISO/IEC 27001, który dla każdego zabezpieczenia z załącznika A mówi, czy je stosujemy, dlaczego i czy jest wdrożone

TYLKO ODCZYT

Przygotowanie artefaktu A7: nadzór nad dokumentami

Krótka procedura: kto tworzy, kto zatwierdza, gdzie leży wersja obowiązująca, jak wycofujemy stare wersje i jak długo trzymamy zapisy (rozdział 7.5).

TYLKO ODCZYT

Przygotowanie artefaktu A8: kompetencje, świadomość i komunikacja

Macierz kompetencji dla ról z A3, plan szkoleń i kampanii świadomości na rok oraz plan komunikacji: co, kiedy, do kogo, kto i jakim kanałem (rozdziały 7.2 do 7.4).

TYLKO ODCZYT

Przygotowanie artefaktu A9: karta wskaźników

Pięć wskaźników powiązanych z celami z A6: wzór, źródło danych, częstotliwość, próg, właściciel, kto ocenia wynik (rozdział 9.1).

TYLKO ODCZYT

Przygotowanie artefaktu A10: program i plan audytu wewnętrznego

Program na trzy lata według ryzyka i plan jednego audytu: cel, zakres, kryteria, audytor niezależny od audytowanego, harmonogram rozmów (rozdział 9.2).

TYLKO ODCZYT

Przygotowanie artefaktu A11: protokół przeglądu zarządzania

Wszystkie wejścia, których wymaga norma, i decyzje kierownictwa na wyjściu: zmiany, zasoby, szanse doskonalenia (rozdział 9.3).

TYLKO ODCZYT

Przygotowanie artefaktów A12 i A13: niezgodności i gotowość do certyfikacji

Rejestr niezgodności z korekcją, przyczyną, działaniem korygującym i oceną skuteczności (rozdział 10.2), oraz lista kontrolna gotowości do audytu etapu 1 i etapu 2.

TYLKO ODCZYT

Zakup egzaminu: panel myPECB

Egzamin Lead Implementer kupujemy bez szkolenia w panelu myPECB: kategoria egzaminu, język, termin, akceptacja zasad, płatność. W pakiecie bez szkolenia jest jedno podejście, a poprawka kosztuje osobno.

TYLKO ODCZYT

Zakup normy: wydrukowany egzemplarz ISO/IEC 27001

Na egzaminie z otwartą książką wolno mieć papierowy egzemplarz normy głównej. Kupujemy własny (ISO, PKN albo sklep myPECB), drukujemy i oklejamy zakładkami rozdziały 4 do 10 i załącznik A. Kopia z internetu łamie licencję.

ISO = International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie · **PKN** = Polski Komitet Normalizacyjny: instytucja, która wydaje polskie wersje norm i sprzedaje je w katalogu

Z życia wzięte

Z ŻYCIA WZIĘTE

Środa, 7:55. Tomek przychodzi z kubkiem kawy i wydrukowaną normą, w której zakładki już się nie mieszczą: ma ich czterdzieści. Pierwszego dnia próbnego egzaminu szuka w normie odpowiedzi na każde pytanie i po półtorej godziny jest przy trzydziestym. Następnego dnia zostawia jedenaście zakładek, po jednej na rozdział i na tematy załącznika A, a na kartce obok spisuje, w którym rozdziale leży każdy z obowiązkowych dokumentów.

Egzamin w liczbach

Co	Wartość	Źródło
Liczba pytań	80 wielokrotnego wyboru, każde z trzema odpowiedziami, jedna poprawna	[1]
Rodzaje pytań	samodzielne i scenariuszowe; po każdym scenariuszu pięć pytań	[1]
Poziomy	43 pytania na rozumienie, zastosowanie i analizę, 37 na ocenę	[1]
Czas	3 godziny	[2]
Dodatkowy czas	przy egzaminie w języku, który nie jest naszym ojczystym: 30 minut według podręcznika [1]; instrukcja online mówi o 20 procentach czasu po zaznaczeniu opcji „Non-Native Speaker” [5]	[1], [5]
Próg	70 procent, czyli 56 poprawnych z 80	[1]
Materiały	otwarta książka: papierowa norma ISO/IEC 27001, materiały szkoleniowe i własne notatki ze szkolenia (w aplikacji albo wydrukowane)	[1], [3]
Forma	online w aplikacji PECB Exams z nadzorem przez kamerę albo na papierze u partnera	[1], [3]
Wynik	przy egzaminie online od razu po wysłaniu odpowiedzi	[3]
Poprawka	bez limitu podejść, co najmniej 15 dni po pierwszym podejściu; darmowa raz w ciągu 12 miesięcy przy szkoleniu, e-learningu albo samodzielnym kursie PECB	[3]
Opłaty bez szkolenia	egzamin 1000 USD, wniosek o certyfikat 500 USD	[1]

Co	Wartość	Źródło
Opłaty ze szkoleniem	w cenie partnera: egzamin, jedna poprawka, wniosek i pierwszy rok AMF	[1], [3]
Utrzymanie	ważność 3 lata; AMF 390 USD na cykl; CPD: Implementer 60 h, Lead Implementer 90 h na cykl; Provisional bez CPD i AMF	[4]

Pojęcie: AMF (Annual Maintenance Fee). Opłata za utrzymanie certyfikatu PECB. Polityka z 2026 roku podaje 390 USD „na trzy lata", więc przed zapisem sprawdzamy w panelu, czy płacimy raz, czy w ratach (do potwierdzenia).

Pojęcie: CPD (Continuing Professional Development). Godziny ciągłego rozwoju: szkolenia, konferencje, praca przy systemach zarządzania, samodzielna nauka. W PECB deklarujemy je w panelu w trakcie trzyletniego cyklu.

Tytuł zależy od doświadczenia

Tytuł	Lata pracy	W tym w zarządzaniu bezpieczeństwem informacji	Godziny projektów systemu zarządzania
Provisional Implementer	brak	brak	brak
Implementer	2	1	200
Lead Implementer	5	2	300
Senior Lead Implementer	10	7	1000

Wszystkie stopnie wymagają tego samego egzaminu i podpisania kodeksu etyki PECB [1]. Tomek, drugi tydzień w pracy, dostanie Provisional Implementer. Projekt ISMS w Zielonej, gdy przejdzie z papieru do prawdziwego wdrożenia, da mu godziny projektu, a lata dołożą się same. Czy praca administratora przy zabezpieczeniach liczy się jako „zarządzanie bezpieczeństwem informacji", ocenia PECB na podstawie opisu i referencji (do potwierdzenia przy wniosku).

Zapis i koszty

1. Zakładamy konto myPECB na imię i nazwisko dokładnie jak w dowodzie.
2. Wybieramy drogę. Bez szkolenia: egzamin 1000 USD plus wniosek 500 USD, bez materiałów kursu [1], [6]. Z partnerem PECB: szkolenie pięciodniowe, e-learning albo

samodzielny kurs z materiałami ponad 450 stron [2], cenę podaje partner.
3. Rezerwujemy termin pierwszego dnia planu. Godziny w panelu są w UTC [5], więc przeliczamy na czas polski.
4. Kupujemy normę ISO/IEC 27001:2022 z poprawką Amd 1:2024. Cenę sprawdzamy u wydawcy (do potwierdzenia); egzemplarz kupiony w sklepie myPECB i przypisany do konta można otworzyć też w aplikacji egzaminacyjnej [5].
5. Po zdanym egzaminie składamy wniosek o certyfikat z opisem doświadczenia i kontaktami do osób, które je potwierdzą. Przy szkoleniu cały cykl trzeba zamknąć w 12 miesięcy od końca kursu, przy e-learningu i samodzielnym kursie od zakupu [3].

> Własne notatki: zasady dopuszczają „notatki ze szkolenia”. Czy kandydat bez szkolenia może mieć wydrukowane własne notatki, pytamy przed egzaminem pod adresem online.exams@pecb.com i zachowujemy odpowiedź (do potwierdzenia). Plan zakłada najgorszy wariant: na biurku tylko norma.

Egzamin online z nadzorem

Według instrukcji dla zdających online [5]:

Co	Wymaganie
System	Windows 10 albo 11 lub macOS, aplikacja PECB Exams, test „Check Compatibility” z samymi zielonymi polami
Łącze	co najmniej 1 Mb/s w obie strony, opóźnienie poniżej 200 ms; porty 80 i 443 oraz porty kamery nadzorującego
Ekran	jeden monitor, stacja dokująca odłączona
Kamera i mikrofon	kamera 720p, mikrofon włączony; komputer stacjonarny wymaga kamery zewnętrznej
Programy	zamknięte narzędzia zdalnego dostępu i komunikatory (TeamViewer, AnyDesk, Teams)
Pokój	sami, porządek, dobre światło, pokazanie pokoju kamerą dookoła
Biurko	bez telefonu, bez długopisu, bez słuchawek; woda tylko w butelce bez etykiety
Dokument	ważny dokument ze zdjęciem; dane, których nie trzeba pokazywać, zasłaniamy
Przerwa	jedna, pięć minut, tylko do toalety; ponad 10 minut poza kamerą kończy egzamin
Start	logowanie 30 minut przed czasem; zegar egzaminu nie zatrzymuje się

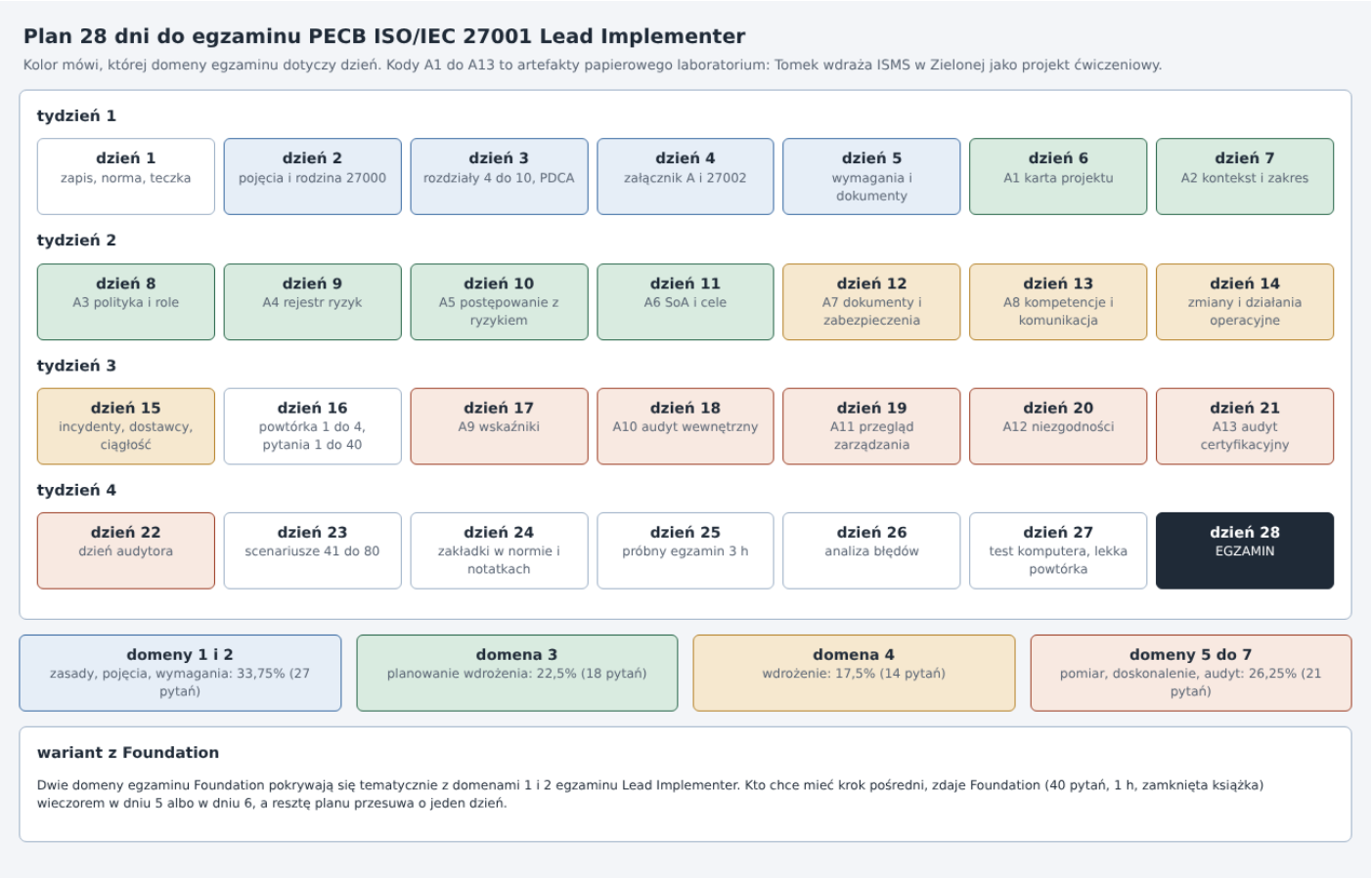
Laptop służbowy z Zielonej zostawiamy w szufladzie: Defender, zasady Intune i VPN mogą blokować porty kamery albo samą aplikację, a instrukcja wprost ostrzega, że urządzenia w domenie mogą wymagać zgody IT. Tomek zdaje na prywatnym komputerze. Długopisu nie ma, więc zakładki w normie są jedynym narzędziem nawigacji.

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: okno „Check Compatibility” aplikacji PECB Exams na komputerze Tomka, wszystkie wskaźniki zielone, widoczna nazwa egzaminu ISO/IEC 27001 Lead Implementer i godzina startu w UTC.

Plan 28 dni

Plan zakłada półtorej do dwóch godzin dziennie przez cztery tygodnie. Kolejność idzie za domenami egzaminu, a najwięcej dni dostaje planowanie (domena 3), które daje najwięcej pytań.



◫ *Rysunek 1. Plan 28 dni: dni 2 do 5 pojęcia i wymagania, dni 6 do 11 planowanie z artefaktami A1 do A6, dni 12 do 15 wdrożenie, dni 17 do 22 pomiar, doskonalenie i audyt, dni 25 do 28 próba, analiza i egzamin (kliknięcie otwiera pełny rozmiar)*

Dzień	Temat	Domena	Strona do przeczytania	Artefakt albo zadanie	Czas
1	Egzamin, zapis, zakup normy, teczka, dziennik pomyłek	wszystkie	ta strona, Certyfikat z ISO/IEC 27001: od rejestru audytorów jakości do PECB Lead Implementer	termin zarezerwowany, teczka założona	1,5 h
2	Informacja, poufność, integralność, dostępność, aktywa, rodzina ISO/IEC 27000	1	Zasady, pojęcia i wymagania ISMS: domeny 1 i 2 egzaminu	słowniczek dwudziestu pojęć	1,5 h
3	System zarządzania, wspólna struktura rozdziałów, PDCA, podejście procesowe	1	ta sama strona	mapa rozdziałów 4 do 10 z pamięci	1,5 h
4	Załącznik A, ISO/IEC 27002, tematy i atrybuty zabezpieczeń	1	ta sama strona	dziesięć zabezpieczeń Zielonej przypisanych do tematów	1,5 h
5	Wymagania rozdział po rozdziale, obowiązkowe informacje udokumentowane	2	ta sama strona	lista obowiązkowych dokumentów z numerami rozdziałów	1,5 h
6	Inicjacja projektu, uzasadnienie, analiza luk	3	Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA	A1	1,5 h
7	Kontekst, strony zainteresowane, zakres	3	ta sama strona	A2	1,5 h
8	Przywództwo, polityka, role	3	ta sama strona	A3	1,5 h

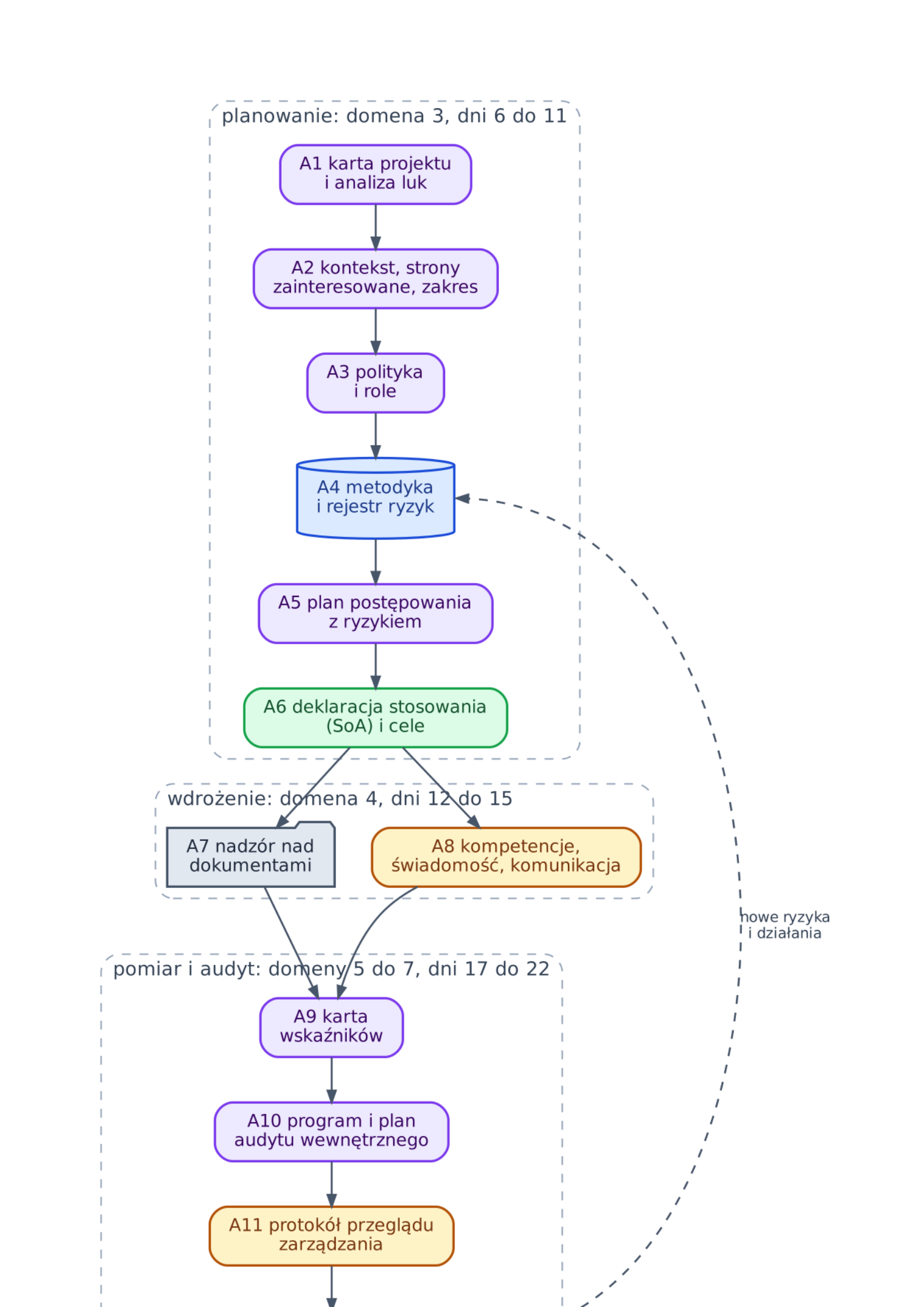
Dzień	Temat	Domena	Strona do przeczytania	Artefakt albo zadanie	Czas
9	Metodyka ryzyka, identyfikacja, analiza, ocena	3	ta sama strona	A4	2 h
10	Postępowanie z ryzykiem, ryzyko szczątkowe	3	ta sama strona	A5	2 h
11	Deklaracja stosowania, cele	3	ta sama strona	A6	1,5 h
12	Plan wdrożenia zabezpieczeń, informacje udokumentowane	4	Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany	A7	1,5 h
13	Kompetencje, świadomość, komunikacja	4	ta sama strona	A8	1,5 h
14	Planowanie zmian, zarządzanie zmianą, działania operacyjne	4	ta sama strona, Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć	trzy zmiany Zielonej opisane jako zmiany w ISMS	1,5 h
15	Incydenty bezpieczeństwa, dostawcy, ciągłość działania	4	ta sama strona, Incydent i incydent poważny: od zgłoszenia do zamknięcia	ścieżka zgłoszenia incydentu bezpieczeństwa w GLPI	1,5 h
16	Powtórka domen 1 do 4	1 do 4	Próbny egzamin Lead Implementer: 80 własnych pytań i strategia na dzień egzaminu	pytania 1 do 40 bez limitu czasu	2 h

Dzień	Temat	Domena	Strona do przeczytania	Artefakt albo zadanie	Czas
17	Monitorowanie, pomiar, analiza i ocena	5	Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania	A9	1,5 h
18	Audyt wewnętrzny według ISO 19011	5	ta sama strona	A10	2 h
19	Przegląd zarządzania	5	ta sama strona	A11	1,5 h
20	Niezgodności, działania korygujące, ciągłe doskonalenie	6	Ciągłe doskonalenie i audyt certyfikacyjny: od niezgodności do certyfikatu	A12	1,5 h
21	Wybór jednostki, etapy audytu certyfikacyjnego	7	ta sama strona	A13	1,5 h
22	Dzień audytora: dowody, ustalenia, raport, odpowiedź na niezgodność	5 do 7	ta sama strona i strona o audycie wewnętrznym	odpowiedź na dwie niezgodności z próbnego raportu	1,5 h
23	Scenariusze	wszystkie	strona egzaminu próbnego	pytania 41 do 80 bez limitu czasu	2 h
24	Nawigacja po normie	wszystkie	wydrukowana norma	jedenaście zakładek, kartka „gdzie co leży”	1 h
25	Próbny egzamin na czas	wszystkie	strona egzaminu próbnego	80 pytań w 3 godziny, sama norma na biurku	3,5 h
26	Analiza błędów	wszystkie	dziennik pomyłek, Fiszki	każda pomyłka opisana i poprawiona	2 h
27	Test komputera, lekka powtórka	wszystkie	lista kontrolna z tej strony	„Check Compatibility” w tym samym pokoju i sieci	1 h
28	Egzamin	wszystkie	lista kontrolna	egzamin	3,5 h z odprawą

> Wariant z Foundation: dwie domeny egzaminu Foundation (zasady i pojęcia, system zarządzania) pokrywają się z dniami 2 do 5. Kto chce krok pośredni, zdaje Foundation (40 pytań, 1 godzina, zamknięta książka, próg 70%) wieczorem w dniu 5 albo w dniu 6, a resztę planu przesuwa o dzień.

Laboratorium papierowe

Laboratorium to teczka dokumentów, które powstałyby w prawdziwym wdrożeniu, w wersji skróconej. Nie ma tu instalacji ani maszyn: jest arkusz kalkulacyjny, edytor tekstu i Zielona, którą znamy z całej bazy. Artefakty powstają w kolejności, w jakiej wymaga ich norma, bo każdy następny korzysta z poprzedniego.


planowanie: domena 3, dni 6 do 11
A1 karta projektu i analiza luk
A2 kontekst, strony zainteresowane, zakres
A3 polityka i role
A4 metodyka i rejestr ryzyk
A5 plan postępowania z ryzykiem
A6 deklaracja stosowania (SoA) i cele
wdrożenie: domena 4, dni 12 do 15
A7 nadzór nad dokumentami
A8 kompetencje, świadomość, komunikacja
pomiar i audyt: domeny 5 do 7, dni 17 do 22
A9 karta wskaźników
A10 program i plan audytu wewnętrznego
A11 protokół przeglądu zarządzania
nowe ryzyka i działania

Rysunek 2. Artefakty laboratorium: planowanie A1 do A6, wdrożenie A7 i A8, pomiar i audyt A9 do A13; niezgodności i decyzje wracają do rejestru ryzyk (kliknięcie otwiera pełny rozmiar)

Artefakt	Wymaganie normy	Dzień	Minimalna treść w ćwiczeniu	Gdzie w egzaminie
A1 karta projektu i analiza luk	ogólnie 4 do 10	6	jedna strona plus tabela luk	domena 3
A2 kontekst, strony, zakres	4.1, 4.2, 4.3	7	dwie strony	domeny 2 i 3
A3 polityka i role	5.1, 5.2, 5.3	8	polityka na stronę, macierz ról	domena 3
A4 metodyka i rejestr ryzyk	6.1.1, 6.1.2, 8.2	9	kryteria i dziesięć ryzyk	domena 3
A5 plan postępowania z ryzykiem	6.1.3, 8.3	10	wiersz na każde ryzyko ponad progiem	domena 3
A6 SoA i cele	6.1.3 d, 6.2	11	dwadzieścia wierszy, trzy cele	domena 3
A7 nadzór nad dokumentami	7.5	12	procedura na stronę	domena 4
A8 kompetencje, świadomość, komunikacja	7.2, 7.3, 7.4	13	trzy tabele	domena 4
A9 karta wskaźników	9.1	17	pięć wskaźników	domena 5
A10 program i plan audytu	9.2	18	program na trzy lata i plan jednego audytu	domena 5
A11 protokół przeglądu zarządzania	9.3	19	wejścia i decyzje	domena 5
A12 rejestr niezgodności	10.1, 10.2	20	trzy niezgodności z próbnego audytu	domena 6
A13 lista gotowości	wymagania jednostki certyfikującej	21	lista na etap 1 i etap 2	domena 7

Numery rozdziałów podajemy według układu ISO/IEC 27001:2022; nazwy wymagań są naszym streszczeniem. Gdy coś w ćwiczeniu jest niepewne, decyzję zapisujemy w karcie projektu jako założenie, tak jak w prawdziwym projekcie.

Jak pracujemy codziennie

Dzień ma trzy części: około 40 minut czytania strony, 40 minut pracy nad artefaktem i 10 minut na dziennik pomyłek oraz Fiszki z pamięci. W dniach bez artefaktu drugą część zajmują pytania z egzaminu próbnego z danej domeny.

Raz w tygodniu, zawsze w piątek, robimy „przegląd teczki” jak przegląd zarządzania w miniaturze: co powstało, co jest niespójne z poprzednimi artefaktami, co zmieniamy. Niespójność rejestru ryzyk z deklaracją stosowania to najczęstsza niezgodność w prawdziwych audytach i najczęstsza pułapka w scenariuszach egzaminu.

Lista kontrolna na dzień przed egzaminem

1. „Check Compatibility” w tym samym pokoju, na tym samym komputerze i w tej samej sieci, bez błędów.
2. Dokument ze zdjęciem, nazwisko zgodne z kontem myPECB.
3. Wydrukowana norma z zakładkami, a jeśli PECB potwierdził na piśmie notatki, to tylko te notatki.
4. Biurko puste: bez telefonu, długopisu, zegarka elektronicznego i drugiego monitora.
5. Godzina startu przeliczona z UTC, domownicy wiedzą, że przez trzy i pół godziny nikt nie wchodzi.

Częste błędy

Objaw	Przyczyna	Co robimy
Na próbie nie wystarcza czasu	szukanie każdej odpowiedzi w normie	zakładki tylko na rozdziały i tematy, odpowiedzi „z głowy”, norma tylko przy pytaniach o konkretne wymaganie
Rejestr ryzyk i SoA sobie przeczą	artefakty robione osobno	SoA zawsze z planu postępowania z ryzykiem, przegląd teczki w piątek
Aplikacja PECB Exams nie łączy kamery	blokada portów przez zaporę albo VPN	prywatny komputer, łącze domowe bez VPN, test 48 godzin wcześniej
Po egzaminie tytuł niższy, niż się spodziewaliśmy	brak lat w zarządzaniu bezpieczeństwem albo godzin projektów	tytuł podnosimy później wnioskiem, bez nowego egzaminu
Voucher ze szkolenia przepadł	minęło 12 miesięcy od końca kursu	termin egzaminu rezerwujemy pierwszego dnia

Objaw	Przyczyna	Co robimy
Odpowiedzi z materiałów o starym egzaminie	dwanaście pytań opisowych, wydanie normy z 2013 roku	sprawdzamy, czy źródło mówi o 80 pytaniach i o wydaniu z 2022 roku

Ćwiczenia

1. Na ile pytań możemy odpowiedzieć źle i nadal zdać?

Odpowiedź

Na dwadzieścia cztery. Próg to 70 procent z 80, czyli 56 poprawnych, więc 24 pytania mogą być złe.

1. Mamy osiem lat pracy jako administrator, w tym trzy lata, w których odpowiadaliśmy za zasady bezpieczeństwa, i około 250 godzin przy wdrożeniu polityk i audytów w poprzedniej firmie. Jaki tytuł możemy dostać po zdaniu egzaminu?

Odpowiedź

Implementer: spełniamy dwa lata pracy, w tym rok w zarządzaniu bezpieczeństwem, i 200 godzin projektów. Do Lead Implementera brakuje 50 godzin projektów (wymagane 300), lata mamy z zapasem. Ostateczną ocenę doświadczenia robi PECB na podstawie wniosku.

1. Dlaczego artefakt A6 (SoA) powstaje dopiero po A5, a nie razem z A2?

Odpowiedź

Bo norma każe wybrać zabezpieczenia na podstawie postępowania z ryzykiem, a dopiero potem porównać je z załącznikiem A i spisać decyzje w deklaracji stosowania. SoA zrobiona przed oceną ryzyka byłaby listą życzeń bez uzasadnień.

1. Ile kosztuje droga bez szkolenia do pierwszego trzyletniego cyklu certyfikatu i co nie jest w niej zawarte?

Odpowiedź

Egzamin 1000 USD, wniosek 500 USD i AMF 390 USD na cykl według polityki z 2026 roku, razem około 1890 USD plus norma. Nie ma w niej materiałów szkoleniowych ani darmowej

poprawki: drugie podejście płacimy osobno.

Powiązane: Certyfikat z ISO/IEC 27001: od rejestru audytorów jakości do PECB Lead Implementer · Plan 30 dni i laboratorium RHEL w Zielonej · GLPI w Zielonej: zgłoszenia, SLA i katalog usług na docker01

Źródła: [1] PECB, Candidate Handbook ISO/IEC 27001 Lead Implementer (multiple choice), wersja 1.5, 2026 (format, poziomy, próg, materiały, wymagania doświadczenia, opłaty, dodatkowy czas); [2] PECB Support, „What is the duration of an exam” i strona szkolenia Lead Implementer (materiały ponad 450 stron, 31 CPD); [3] PECB, Exam Rules and Policies (poprawki po 15 dniach, darmowa poprawka w 12 miesięcy, materiały, termin 12 miesięcy, wynik online); [4] PECB, Certification Maintenance Policy 2026 (AMF, CPD); [5] PECB, myPECB Online Examinee Manual (wymagania techniczne, pokój, przerwa, start, UTC, 20 procent czasu); [6] PECB Help, „How do I schedule an exam if I did not attend a PECB training event”. Dostęp 23 października 2026.