Egzamin

80 własnych pytań i strategia na dzień egzaminu.

- Próbny egzamin Lead Implementer: 80 własnych pytań i strategia na dzień egzaminu

Próbny egzamin Lead Implementer: 80 własnych pytań i strategia na dzień egzaminu

Poziom: średnio

Dotyczy: PECB ISO/IEC 27001 Lead Implementer, wszystkie siedem domen, format z podręcznika kandydata 1.5 (2026), dni 16, 23, 25 i 26 planu

Czas: 3 godziny na próbę, 2 godziny na analizę

Osiemdziesiąt własnych pytań w formacie egzaminu: trzy odpowiedzi, jedna poprawna, czterdzieści pytań samodzielnych i osiem scenariuszy Zielonej po pięć pytań, w proporcjach domen z podręcznika kandydata PECB. Klucz z wyjaśnieniami jest zwinięty pod każdą częścią. Na końcu strategia na trzy godziny z otwartą książką i zasady egzaminu online.

Pytania napisaliśmy sami na podstawie opisów domen z podręcznika kandydata [1] i przykładów z Zielonej. Nie są kopią oficjalnych pytań PECB, materiałów szkoleniowych ani zbiorów krążących w internecie, i nie sprawdzają znajomości konkretnych sformułowań z egzaminu. Rozkład pytań odpowiada liczbom z podręcznika: domena 1 to 15 pytań, 2 to 12, 3 to 18, 4 to 14, 5 to 10, 6 to 6 i 7 to 5.

Skróty użyte na tej stronie (14)

Skrót	Co znaczy
AI	Artificial Intelligence: sztuczna inteligencja, czyli programy naśladujące ludzkie rozumowanie
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
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)

Skrót	Co znaczy
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
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
PDCA	Plan, Do, Check, Act: cykl doskonalenia planuj, wykonaj, sprawdź, działaj, któremu odpowiada układ rozdziałów norm systemów zarządzania
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
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
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
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Karty pułapek egzaminacyjnych. Czytamy je w dniu 26 i rano w dniu egzaminu.

□□ TYLKO ODCZYT

Rozpoznanie pytania o ocenę: NAJLEPIEJ, NAJPIERW, NAJWIĘKSZY

Prawie połowa pytań (37 z 80 według podręcznika) mierzy ocenę, czyli wybór najlepszego działania. Zwykle dwie odpowiedzi są do obrony, a wygrywa ta, która jest zgodna z normą i z rolą osoby w pytaniu.

□□ TYLKO ODCZYT

Rozwiązywanie pytania „tak, bo” i „nie, bo”

Najpierw decydujemy, czy odpowiedź brzmi tak, czy nie, a dopiero potem czytamy uzasadnienia. Odpowiedź z dobrym „nie” i złym uzasadnieniem jest zła.

□□ TYLKO ODCZYT

Czytanie scenariusza: kto, co, czego brakuje

Scenariusz czytamy raz, uważnie, i zapamiętujemy trzy rzeczy: kto jest kim, co już zrobiono, czego brakuje. Do scenariusza wracamy przy każdym z pięciu pytań, bo odpowiedź musi pasować do tej firmy, a nie do ogólnej zasady.

□□ TYLKO ODCZYT

Korzystanie z normy: tylko do wymagań

Norma na biurku służy do sprawdzenia, czy coś jest wymaganiem i w którym punkcie. Definicji w niej nie ma (są w ISO/IEC 27000), a dobrych praktyk wdrożenia też nie. Pytań o kolejność działań nie rozstrzygamy, kartkując normę.

□□ **ISO** = International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie

□□ TYLKO ODCZYT

Odróżnienie w pytaniu: wymaganie i dobra praktyka

Odpowiedź „musi” albo „zawsze” przy rzeczy, której norma nie wymaga (procedura audytu, konkretne stanowisko, konkretne narzędzie), jest zwykle zła. Odpowiedź „może, jeśli uzasadni” przy zabezpieczeniu z załącznika A jest zwykle dobra.

□□ TYLKO ODCZYT

Odróżnienie w pytaniu: rola wdrażającego i rola kierownictwa

Wdrażający planuje, proponuje, organizuje i dokumentuje. Kierownictwo zatwierdza politykę, daje zasoby i przegląda system. Właściciel ryzyka akceptuje ryzyko. Audytor ustala, a nie naprawia. Odpowiedź, w której ktoś przejmuje cudzą decyzję, jest prawie zawsze zła.

□□ TYLKO ODCZYT

Odrzucenie odpowiedzi technicznej w pytaniu o zarządzanie

Gdy pytanie dotyczy projektu, ludzi albo decyzji, odpowiedź „zainstalować narzędzie” rzadko jest najlepsza. Najpierw zaangażowanie, kryteria, ryzyko, komunikacja.

□□ TYLKO ODCZYT

Zarządzanie czasem: 2 minuty i flaga

180 minut na 80 pytań to 2 minuty i 15 sekund na pytanie. Pierwsze przejście w 120 minut, flaga „Mark for Review” przy każdym wahaniu dłuższym niż dwie minuty. Długopisu nie ma, więc listą wątpliwości jest panel pytań w aplikacji.

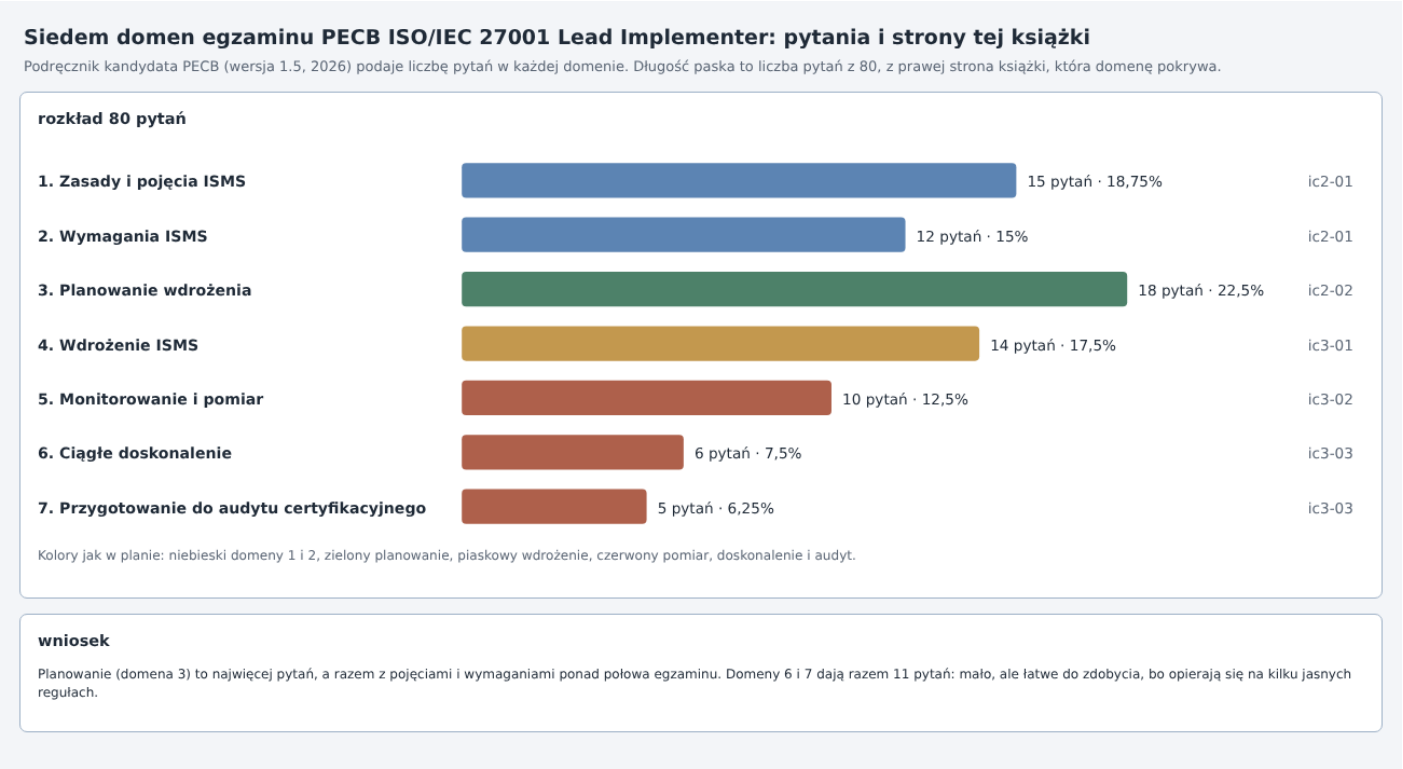
Z życia wzięte

□□ Z ŻYCIA WZIĘTE

Sobota, 9:00. Tomek robi próbę w sali konferencyjnej Zielonej: zegar na trzy godziny, na stole tylko wydrukowana norma z jedenastoma zakładkami. Przy scenariuszu o certyfikacji traci kwadrans na szukanie w normie słowa „niezgodność duża”, którego tam nie ma, bo pochodzi z ISO/IEC 17021-1. Kończy z wynikiem 59 na 80 i z dziesięcioma flagami, z których siedem rozstrzyga dobrze, gdy wraca do treści scenariuszy. W dzienniku zapisuje: do normy zaglądam tylko po numer wymagania.

Jak to działa

Próbny egzamin ma ten sam rozkład pytań co prawdziwy, więc wynik z każdej części pokazuje, gdzie tracimy punkty. Pytania 1 do 40 są samodzielne i obejmują domeny 1 do 4; robimy je w dniu 16 bez limitu czasu. Pytania 41 do 80 to osiem scenariuszy obejmujących domeny 3 do 7; robimy je w dniu 23. W dniu 25 robimy całość na czas.



Rysunek 1. Siedem domen egzaminu PECB ISO/IEC 27001 Lead Implementer z liczbą pytań i stronami tej książki (kliknięcie otwiera pełny rozmiar)

Zasady próby w dniu 25:

1. Zegar na 180 minut. Na biurku tylko wydrukowana norma; notatki tylko wtedy, gdy PECB potwierdził na piśmie, że wolno je mieć.
2. Odpowiedzi zapisujemy w kolumnie na kartce: numer i litera. Na prawdziwym egzaminie długopisu nie będzie, więc flagi zaznaczamy kółkiem przy numerze, a nie notatkami.
3. Klucz otwieramy po upływie czasu.
4. Liczymy punkty osobno dla każdej domeny według kolumny „Domena” w kluczu.

Próg, który traktujemy jako bezpieczny: 62 punkty z 80 (około 78 procent) na naszych pytaniach. Oficjalny próg to 56 punktów (70 procent), ale nasze pytania nie są oficjalnym arkuszem, więc zostawiamy zapas.

Część 1: pytania 1 do 40

Domena 1: zasady i pojęcia (pytania 1 do 15)

1. Ktoś bez uprawnień zmienił ceny w cenniku sklepu B2B. Cennik nie trafił do nikogo spoza firmy, a sklep cały czas działał. Która właściwość informacji została naruszona?

- A. Integralność
- B. Poufność
- C. Dostępność

2. Co NAJLEPIEJ opisuje system zarządzania bezpieczeństwem informacji (ISMS)?

- A. Zestaw narzędzi bezpieczeństwa zainstalowanych w sieci firmy
- B. Dział firmy odpowiedzialny za bezpieczeństwo
- C. Część systemu zarządzania oparta na podejściu do ryzyka, która ustanawia, wdraża, utrzymuje i doskonali bezpieczeństwo informacji

3. Na podstawie której normy organizacja może uzyskać akredytowany certyfikat systemu zarządzania bezpieczeństwem informacji?

- A. ISO/IEC 27001
- B. ISO/IEC 27005
- C. ISO/IEC 27002

4. Ile zabezpieczeń zawiera załącznik A ISO/IEC 27001:2022?

- A. 114
- B. 133
- C. 93

5. Do którego tematu załącznika A należy weryfikacja kandydatów przed zatrudnieniem?

- A. Zabezpieczenia fizyczne
- B. Zabezpieczenia osobowe
- C. Zabezpieczenia organizacyjne

6. Z nieznanego adresu przyszła jedna nieudana próba logowania na konto administratora. Nic więcej się nie stało. Jak to nazywamy?

- A. Niezgodność
- B. Incydent bezpieczeństwa informacji
- C. Zdarzenie bezpieczeństwa informacji

7. Jak nazywa się słabość aktywa albo zabezpieczenia, którą może wykorzystać zagrożenie?

- A. Skutek
- B. Podatność
- C. Ryzyko

8. Jak rodzina ISO/IEC 27000 rozumie ryzyko?

- A. Jako koszt incydentu
- B. Jako wpływ niepewności na cele
- C. Jako prawdopodobieństwo awarii sprzętu

9. Co oznacza słowo „powinien” (should) w ISO/IEC 27002?

- A. Zakaz
- B. Wymaganie, którego niespełnienie jest niezgodnością
- C. Zalecenie

10. Który atrybut ISO/IEC 27002:2022 dzieli zabezpieczenia na zapobiegawcze, wykrywające i korygujące?

- A. Pojęcia cyberbezpieczeństwa
- B. Rodzaj zabezpieczenia
- C. Domeny bezpieczeństwa

11. Któremu etapowi cyklu PDCA odpowiada rozdział 9 ISO/IEC 27001 (ocena efektów)?

- A. Sprawdź
- B. Planuj
- C. Działaj

12. Zielona zleca firmie zewnętrznej administrowanie częścią serwerów. Kto w rozumieniu ISMS odpowiada za bezpieczeństwo informacji w tym procesie?

- A. Zielona, która musi nadzorować proces zlecony na zewnątrz
- B. Jednostka certyfikująca firmy zewnętrznej
- C. Wyłącznie firma zewnętrzna

13. Kopia zapasowa jest zaszyfrowana kluczem, który zaginął. Którą właściwość informacji utraciliśmy?

- A. Poufność
- B. Integralność
- C. Dostępność

14. Która norma daje wytyczne do zarządzania ryzykiem bezpieczeństwa informacji?

- A. ISO/IEC 27006-1
- B. ISO/IEC 27005
- C. ISO/IEC 27004

15. Co opisuje skuteczność (effectiveness) w rozumieniu norm ISO?

- A. Stosunek wyniku do zużytych zasobów
- B. Stopień, w jakim zaplanowane działania zostały zrealizowane i dały zaplanowane wyniki

- C. Zgodność dokumentacji z normą

Domena 2: wymagania (pytania 16 do 27)

16. Którego elementu NIE można wyłączyć, jeśli organizacja deklaruje zgodność z ISO/IEC 27001?

- A. Audytu wewnętrznego
- B. Zabezpieczenia o pracy zdalnej
- C. Zabezpieczenia o bezpiecznym programowaniu

17. Który z tych dokumentów jest obowiązkową informacją udokumentowaną według ISO/IEC 27001:2022?

- A. Regulamin pracy zdalnej
- B. Procedura zarządzania hasłami
- C. Deklaracja stosowania

18. W którym rozdziale ISO/IEC 27001:2022 są wymagania o kompetencjach, świadomości i komunikacji?

- A. 7
- B. 8
- C. 5

19. Który punkt dodano w ISO/IEC 27001:2022 jako nowe wymaganie?

- A. Polityka bezpieczeństwa informacji
- B. Audyt wewnętrzny
- C. Planowanie zmian w systemie zarządzania

20. Co wprowadziła poprawka ISO/IEC 27001:2022/Amd 1:2024?

- A. Uwzględnienie zmiany klimatu w kontekście organizacji i wymaganiach stron zainteresowanych
- B. Nowe zabezpieczenia w załączniku A
- C. Obowiązek certyfikacji dostawców

21. Co organizacja musi zrobić z wynikami monitorowania i pomiaru?

- A. Opublikować je stronom zainteresowanym
- B. Zachować je jako informację udokumentowaną
- C. Omówić je ustnie na przeglądzie zarządzania

22. Według punktu 4.2 wydania 2022 organizacja ustala, które wymagania stron zainteresowanych:

- A. Będą spełniane przez system zarządzania
- B. Zostaną przekazane jednostce certyfikującej
- C. Są wiążące prawnie

23. Zakres ISMS:

- A. Może być ustalony ustnie przez prezesa
- B. Jest obowiązkową informacją udokumentowaną
- C. Wyznacza go jednostka certyfikująca

24. Polityka bezpieczeństwa informacji musi zawierać:

- A. Listę wszystkich zabezpieczeń
- B. Zobowiązanie do ciągłego doskonalenia systemu
- C. Nazwiska administratorów

25. Który punkt wymaga przeprowadzania oceny ryzyka w zaplanowanych odstępach i po istotnych zmianach?

- A. 8.2
- B. 9.3
- C. 6.1.2

26. Kto przeprowadza przegląd zarządzania ISMS?

- A. Kierownik IT
- B. Najwyższe kierownictwo
- C. Audytor wewnętrzny

27. Organizacja usuwa przyczynę niezgodności, żeby nie wróciła. Którego rozdziału normy to dotyczy?

- A. 10
- B. 9
- C. 6

Domena 3: planowanie (pytania 28 do 35)

28. Co jest NAJLEPSZYM pierwszym krokiem projektu wdrożenia ISMS?

- A. Napisanie wszystkich procedur
- B. Uzyskanie zaangażowania i zgody najwyższego kierownictwa
- C. Zakup narzędzia do analizy ryzyka

29. Kto akceptuje ryzyko szczątkowe?

- A. Osoba wdrażająca ISMS
- B. Audytor wewnętrzny
- C. Właściciel ryzyka

30. Kiedy ustalamy kryteria akceptacji ryzyka?

- A. Po audycie certyfikacyjnym
- B. Przed identyfikacją ryzyk
- C. Po ocenie ryzyk

31. Firma kupuje ubezpieczenie od skutków finansowych wycieku danych. Jaka to opcja postępowania z ryzykiem?

- A. Zachowanie ryzyka
- B. Unikanie ryzyka
- C. Dzielenie się ryzykiem

32. Jaki jest główny cel porównania wybranych zabezpieczeń z załącznikiem A?

- A. Wdrożenie wszystkich 93 zabezpieczeń
- B. Upewnienie się, że nie pominięto żadnego potrzebnego zabezpieczenia
- C. Ustalenie budżetu projektu

33. Który cel NAJLEPIEJ spełnia wymagania punktu 6.2?

- A. Poprawić bezpieczeństwo sieci
- B. Do 30 czerwca 2027 roku wszystkie konta zdalnego dostępu z MFA, raport co miesiąc dla kierownictwa
- C. Zero incydentów

34. Co porównuje analiza luk na początku projektu?

- A. Obecny stan organizacji z wymaganiami normy
- B. Ryzyka z kryteriami akceptacji
- C. Zabezpieczenia z budżetem

35. Firma przestaje przechowywać numery kart płatniczych klientów, bo ryzyko jest za duże. Jaka to opcja postępowania z ryzykiem?

- A. Unikanie ryzyka
- B. Zmniejszenie ryzyka
- C. Dzielenie się ryzykiem

Domena 4: wdrożenie (pytania 36 do 40)

36. Który dowód NAJLEPIEJ pokazuje skuteczność szkolenia z rozpoznawania phishingu?

- A. Wynik testu phishingowego przeprowadzonego po szkoleniu
- B. Prezentacja użyta na szkoleniu
- C. Lista obecności ze szkolenia

37. Czego wymaga nadzór nad informacją udokumentowaną?

- A. Kontroli wersji i dostępności dokumentów tam, gdzie są potrzebne
- B. Zatwierdzania każdego dokumentu przez jednostkę certyfikującą
- C. Przechowywania dokumentów wyłącznie na papierze

38. Zmianę awaryjną wdrożono w nocy bez zatwierdzenia. Co NAJLEPIEJ zrobić według dobrej praktyki zarządzania zmianami?

- A. Zarejestrować ją i przejrzeć po fakcie
- B. Nic, bo to wyjątek
- C. Natychmiast ją cofnąć

39. Co według punktu 7.3 powinien wiedzieć każdy, kto pracuje pod nadzorem organizacji?

- A. Znać wyniki audytów jednostki certyfikującej
- B. Znać politykę, swój wkład w skuteczność systemu i skutki niespełniania wymagań
- C. Znać konfigurację zabezpieczeń technicznych

40. Pracownicy nie stosują nowej polityki czystego biurka. Jakie działanie wdrażającego jest NAJLEPSZE?

- A. Wycofać politykę
- B. Wprowadzić kary od następnego dnia
- C. Zaplanować komunikację i szkolenie z wyjaśnieniem powodów, ze wsparciem kierownictwa

Klucz i wyjaśnienia do pytań 1 do 40

Nr	Odp.	Domena	Wyjaśnienie
1	A	1	Zmiana bez uprawnień narusza dokładność i kompletność, czyli integralność. Treść nie wyciekła, a dostęp był zachowany.
2	C	1	ISMS to system zarządzania (polityki, procesy, role, cele), a nie narzędzia ani komórka organizacyjna.

Nr	Odp.	Domena	Wyjaśnienie
3	A	1	Tylko 27001 zawiera wymagania. 27002 i 27005 to wytyczne.
4	C	1	Wydanie 2022 ma 93 zabezpieczenia w czterech tematach. 114 to wydanie 2013.
5	B	1	Weryfikacja przed zatrudnieniem to zabezpieczenie 6.1, temat osobowy.
6	C	1	Zdarzenie wskazuje na możliwe naruszenie. Incydentem byłoby, gdyby z dużym prawdopodobieństwem zaszkodziło.
7	B	1	Zagrożenie wykorzystuje podatność, a ryzyko opisuje skutek i prawdopodobieństwo takiego zdarzenia.
8	B	1	Definicja ogólna z norm ISO: wpływ niepewności na cele, opisywany zwykle skutkiem i prawdopodobieństwem.
9	C	1	W normach ISO „musi” to wymaganie, „powinien” zalecenie, „może” dopuszczenie.
10	B	1	Pojęcia cyberbezpieczeństwa to identyfikacja, ochrona, wykrywanie, reagowanie, odtwarzanie. Rodzaj to zapobiegawcze, wykrywające, korygujące.
11	A	1	Rozdział 9 to monitorowanie, pomiar, audyt i przegląd, czyli Sprawdź. Działaj to rozdział 10.

Nr	Odp.	Domena	Wyjaśnienie
12	A	1	Zlecenie przenosi pracę, nie odpowiedzialność. Procesy zewnętrzne trzeba nadzorować (8.1).
13	C	1	Dane są nadal tajne i niezmienione, ale nie da się z nich skorzystać.
14	B	1	27004 to pomiar, 27006-1 to wymagania dla jednostek certyfikujących.
15	B	1	Stosunek wyniku do zasobów to efektywność. Zgodność to spełnienie wymagań.
16	A	2	Wymagań z rozdziałów 4 do 10 nie wyłączamy. Zabezpieczenia z załącznika A można wyłączyć z uzasadnieniem w SoA.
17	C	2	SoA wymaga 6.1.3 d. Dwa pozostałe mogą być potrzebne, ale norma nie wymienia ich wprost.
18	A	2	Rozdział 7 to wsparcie: zasoby, kompetencje, świadomość, komunikacja, informacje udokumentowane.
19	C	2	Punkt 6.3 jest nowy w wydaniu 2022. Audyt i polityka były wcześniej.
20	A	2	Poprawka dopisała zmianę klimatu do punktów 4.1 i 4.2, nie zmieniła załącznika A.
21	B	2	Dowody wyników monitorowania i pomiaru są obowiązkową informacją udokumentowaną (9.1).
22	A	2	Wydanie 2022 dodało wybór wymagań, które ISMS ma spełniać.

Nr	Odp.	Domena	Wyjaśnienie
23	B	2	Zakres ustala organizacja i dokumentuje go (4.3).
24	B	2	Polityka zawiera między innymi zobowiązanie do spełniania wymagań i do doskonalenia (5.2).
25	A	2	6.1.2 opisuje proces oceny, a 8.2 każe go wykonywać cyklicznie i po zmianach.
26	B	2	Wymaganie 9.3 przypisuje przegląd najwyższemu kierownictwu.
27	A	2	Niezgodności i działania korygujące są w rozdziale 10 (doskonalenie).
28	B	3	Bez kierownictwa nie ma polityki, zasobów ani akceptacji ryzyka.
29	C	3	Plan postępowania i ryzyko szczątkowe zatwierdzają właściciele ryzyk (6.1.3).
30	B	3	Kryteria ustalone po ocenie dopasowuje się do wyników, a wyniki tracą porównywalność.
31	C	3	Ubezpieczenie przenosi część skutków finansowych, nie zmienia zagrożenia.
32	B	3	Załącznik A to lista kontrolna, nie obowiązkowy katalog do wdrożenia.
33	B	3	Cel ma być mierzalny, mieć termin, właściciela i sposób oceny.
34	A	3	Ryzyka z kryteriami porównuje ocena ryzyka, nie analiza luk.

Nr	Odp.	Domena	Wyjaśnienie
35	A	3	Rezygnacja z działania, które tworzy ryzyko, to unikanie.
36	A	4	Norma wymaga oceny skuteczności działań, a nie tylko faktu szkolenia.
37	A	4	Postać jest dowolna, liczy się nadzór nad wersjami, dostępem, ochroną i zatrzymaniem.
38	A	4	Zmiana awaryjna też przechodzi przez proces, tylko szybszą ścieżką z przeglądem po fakcie.
39	B	4	To trzy elementy świadomości. Konfiguracja należy do kompetencji wybranych ról.
40	C	4	Zarządzanie zmianą zaczyna się od wyjaśnienia i wsparcia, a nie od kary.

Część 2: scenariusze, pytania 41 do 80

Scenariusz 1: Zielona rusza z projektem (pytania 41 do 45)

> Duży odbiorca sklepu B2B wymaga od Zielonej certyfikatu ISO/IEC 27001 w ciągu roku. Pan Zbigniew proponuje, żeby zakres objął tylko sklep B2B na serwerach `my01` i `mongo01`, bez serwerowni, sieci i administratorów, „bo tak będzie szybciej”. Tomek przygotował dwunastostronicową politykę, w której są też reguły zapory i długość haseł. Ocenę ryzyka zrobił sam dział IT w jedno popołudnie, bez spisanych kryteriów, a właścicielem wszystkich ryzyk wpisał administratora. Pan Zbigniew chce mianować Tomka pełnomocnikiem i nie

> uczestniczyć w dalszych pracach.

41. Czy proponowany zakres jest właściwy?

- A. Nie, bo zakres nie może pomijać zależności, bez których usługa w zakresie nie działa, bez opisania styków i ich nadzoru
- B. Nie, bo zakres zawsze musi obejmować całą firmę
- C. Tak, zakres może być dowolnie wąski

42. Co NAJLEPIEJ zrobić z polityką Tomka?

- A. Skrócić ją do celu, zobowiązań i ram dla celów, a reguły techniczne przenieść do polityk tematycznych i procedur
- B. Zostawić, bo dłuższa polityka daje więcej ochrony
- C. Wysłać ją do zatwierdzenia jednostce certyfikującej

43. Czy mianowanie Tomka pełnomocnikiem i wycofanie się prezesa spełnia wymagania o przywództwie?

- A. Tak, jeśli pełnomocnik ma certyfikat Lead Implementer
- B. Nie, bo najwyższe kierownictwo musi wykazać przywództwo i zaangażowanie, choć może przypisać role
- C. Tak, bo norma pozwala przekazać wszystko pełnomocnikowi

44. Co jest NAJWIĘKSZYM problemem oceny ryzyka?

- A. Dział IT nie może identyfikować ryzyk
- B. Ocena powinna być w arkuszu, a nie w dokumencie
- C. Brak ustalonych kryteriów, przez co wyniki nie są spójne, ważne i porównywalne

45. Kto powinien być właścicielem ryzyka „sklep B2B niedostępny w szczycie przed świętami”?

- A. Osoba odpowiedzialna za sprzedaż przez sklep, z uprawnieniem do decyzji o tym ryzyku
- B. Dostawca oprogramowania sklepu
- C. Administrator serwera `my01`

Scenariusz 2: postępowanie z ryzykiem i deklaracja stosowania (pytania 46 do 50)

>

> Metodyka Zielonej mówi: poziom ryzyka to iloczyn skutku i prawdopodobieństwa w skali 1 do 5, poziom do 6 można zaakceptować. W rejestrze są między innymi: ransomware na `sql01` (15), zdalny serwis dostawcy WMS bez MFA (12) i awaria łącza w Swarzędzu (6). Tomek skopiował do deklaracji stosowania wszystkie 93 zabezpieczenia z dopiskiem „stosujemy”, bez uzasadnień, a jedno wyłączył z uzasadnieniem „zbyt drogie”. Ola chciała przetestować publiczną usługę sztucznej inteligencji na danych klientów; kierownictwo zakazało tego do czasu oceny.

46. Co zgodnie z metodyką można zrobić z ryzykiem awarii łącza (poziom 6)?

- A. Przenieść je na operatora łącza
- B. Obowiązkowo je zmniejszyć
- C. Zaakceptować je, a decyzję potwierdza właściciel ryzyka

47. Czy deklaracja stosowania Tomka spełnia wymaganie 6.1.3 d?

- A. Nie, bo SoA musi zawierać uzasadnienie włączenia zabezpieczeń i informację, czy są wdrożone
- B. Tak, bo stosowanie wszystkich zabezpieczeń jest bezpieczniejsze
- C. Tak, bo uzasadnienie potrzebne jest tylko przy wyłączeniach

48. Czy „zbyt drogie” jest właściwym uzasadnieniem wyłączenia?

- A. Nie, wyłączenie powinno wynikać z braku ryzyka albo braku zastosowania, a drogie zabezpieczenie można zastąpić innym
- B. Tak, jeśli wyłączenie zatwierdzi prezes
- C. Tak, koszt jest zawsze dobrym uzasadnieniem

49. Jaka opcja postępowania z ryzykiem odpowiada zakazowi testu AI na danych klientów?

- A. Dzielenie się ryzykiem
- B. Zachowanie ryzyka
- C. Unikanie ryzyka

50. Plan postępowania dla ryzyka serwisu WMS jest gotowy. Co powinno nastąpić przed wdrożeniem?

- A. Zgoda jednostki certyfikującej
- B. Zatwierdzenie planu i ryzyka szczątkowego przez właściciela ryzyka
- C. Audyt wewnętrzny planu

Scenariusz 3: dokumenty i ludzie (pytania 51 do 55)

> Procedury Zielonej leżą w trzech miejscach: na udziale `fs01`, w starych e-mailach i w BookStacku, a ich wersje się różnią. Pracownicy magazynu pracują na zmianach przy terminalach i nie czytają poczty. Jedyny dowód szkoleń to listy obecności. Nowi pracownicy podpisują politykę pierwszego dnia, bez wyjaśnienia. Marek sprzeciwia się blokadzie terminali po pięciu minutach bezczynności, bo „o 6:00 skanery muszą działać od razu”.

51. Co NAJLEPIEJ zrobić z procedurami w trzech miejscach?

- A. Wydrukować wszystkie wersje do segregatora
- B. Zakazać zmian w procedurach
- C. Ustalić jedno źródło wersji obowiązujących, oznaczyć je i wycofać wersje nieaktualne

52. Jak komunikować się z pracownikami magazynu, żeby spełnić punkt 7.4?

- A. Komunikować tylko z kierownikami
- B. Komunikować wyłącznie na piśmie
- C. Ustalić, co, kiedy, z kim i jak komunikujemy, i dobrać kanał do odbiorców, na przykład odprawę zmiany

53. Co norma mówi o dowodach kompetencji administratorów?

- A. Przechowuje je jednostka certyfikująca
- B. Nie są wymagane
- C. Organizacja zachowuje je jako informację udokumentowaną

54. Czy podpis pod polityką w pierwszym dniu pracy wystarcza do zapewnienia świadomości?

- A. Tak, bo świadomość dotyczy tylko działu IT
- B. Tak, podpis jest dowodem świadomości
- C. Nie, potrzebne jest szkolenie wprowadzające i sprawdzenie, czy pracownik zna politykę, swój wkład i skutki niespełniania wymagań

55. Jak NAJLEPIEJ odpowiedzieć na sprzeciw Marka?

- A. Zebrać jego uwagi, ocenić wpływ na pracę i ryzyko, ustalić rozwiązanie z właścicielem procesu i je zakomunikować
- B. Wdrożyć blokadę bez rozmowy
- C. Zrezygnować z zabezpieczenia

Scenariusz 4: incydent i dostawca (pytania 56 do 60)

> W piątek o 16:00 Defender zgłasza szyfrowanie plików na `fs01`. Tomek chce natychmiast odtworzyć serwer z kopii. Wstępna analiza wskazuje, że napastnik wszedł przez zdalny dostęp dostawcy WMS, który działał bez MFA. Dostawca chwali się certyfikatem ISO/IEC 27001, ale jego zakres obejmuje tylko biuro badawcze w innym mieście. Po opanowaniu sytuacji nikt nie spisał wniosków.

56. Co powinno nastąpić NAJPIERW po zgłoszeniu incydentu?

- A. Powiadomienie mediów
- B. Natychmiastowe odtworzenie serwera z kopii
- C. Ograniczenie skutków (odłączenie serwera) i zabezpieczenie dowodów, a dopiero potem odtworzenie

57. Co wynika z certyfikatu dostawcy obejmującego tylko jego biuro badawcze?

- A. Zielona musi natychmiast zerwać umowę
- B. Certyfikat wystarcza jako zapewnienie bezpieczeństwa
- C. Certyfikat nie potwierdza bezpieczeństwa usługi zdalnego serwisu dla Zielonej, więc wymagania trzeba zapisać w umowie i monitorować

58. Nowa konfiguracja dostępu dostawcy przez VPN z MFA ma wejść jeszcze w weekend. Jak ją wprowadzić?

- A. Bez procesu, bo to sytuacja awaryjna
- B. Przez proces zarządzania zmianą, z oceną ryzyka i planem wycofania, choćby ścieżką przyspieszoną
- C. Po uzyskaniu zgody dostawcy, bez rejestracji

59. Którego zabezpieczenia dotyczy brak spisanych wniosków po incydencie?

- A. Wyciągania wniosków z incydentów bezpieczeństwa informacji
- B. Bezpieczeństwa fizycznego
- C. Kopii zapasowych

60. Który wskaźnik NAJLEPIEJ pokaże, czy reagowanie na incydenty się poprawia?

- A. Liczba stron procedury obsługi incydentów
- B. Czas od zgłoszenia do ograniczenia skutków incydentu, mierzony co miesiąc
- C. Liczba alertów Defendera

Scenariusz 5: karta wskaźników (pytania 61 do 65)

> W Zielonej wszyscy chwalą dashboard w Zabbiksie, ale nikt nie omawia jego wyników. Wskaźnik W1 (udane testy odtwarzania) za każdym razem liczony jest inną metodą. Wskaźnik W2 (świadomość) mierzy Tomek, który sam prowadzi szkolenia, a nigdzie nie zapisano, kto ocenia wynik. Wskaźnik W3 (konta zablokowane w dniu odejścia) od trzech miesięcy wynosi 80 procent przy progu 100 procent.

61. Czy sam dashboard w Zabbiksie spełnia wymaganie 9.1?

- A. Nie, organizacja musi też ustalić, kiedy i kto analizuje i ocenia wyniki
- B. Tak, jeśli ma do niego dostęp kierownictwo
- C. Tak, bo pokazuje dane na bieżąco

62. Jaki jest skutek liczenia W1 za każdym razem inną metodą?

- A. To problem tylko dla audytora zewnętrznego
- B. Wyniki nie są porównywalne ani powtarzalne
- C. Nie ma żadnego skutku

63. Gdzie NAJLEPIEJ zapisać, kto mierzy, a kto ocenia W2?

- A. W karcie wskaźnika, w ramach ustaleń wymaganych przez 9.1
- B. W dokumentacji dostawcy narzędzia
- C. W umowie z jednostką certyfikującą

64. Co NAJLEPIEJ zrobić z wynikiem W3?

- A. Przeanalizować przyczyny, zarejestrować działanie w rejestrze niezgodności i przekazać wynik na przegląd zarządzania
- B. Przestać mierzyć ten wskaźnik
- C. Obniżyć próg do 80 procent

65. Który wskaźnik NAJLEPIEJ mierzy skuteczność zabezpieczenia „kopie zapasowe”?

- A. Odsetek udanych testów odtwarzania wykonanych w zaplanowanym terminie
- B. Zajęta pojemność dysków na `bkp01`
- C. Liczba zadań kopii w harmonogramie

Scenariusz 6: audyt wewnętrzny i przegląd zarządzania (pytania 66 do 70)

> Tomek zaplanował, że sam przeprowadzi audyt procesu odbierania dostępu, który od miesiąca prowadzi. Program audytów obejmuje wyłącznie zabezpieczenia techniczne. Raport z audytu podaje dla każdej niezgodności gotowe rozwiązanie. Przegląd zarządzania prowadzi dział IT bez prezesa. Na przeglądzie wychodzi, że problem z kontami byłych pracowników wraca od roku.

66. Co wynika z planu, że Tomek sam audytuje proces, który prowadzi?

- A. Narusza to obiektywizm i bezstronność audytu, więc trzeba zmienić audytora
- B. Wymaga to zgody jednostki certyfikującej
- C. To dopuszczalne w małej firmie bez ograniczeń

67. Co jest problemem programu audytów?

- A. Nie ma problemu, technika jest najważniejsza
- B. Program musi w cyklu objąć cały system, w tym wymagania rozdziałów 4 do 10
- C. Program powinien obejmować wyłącznie załącznik A

68. Jak ocenić raport z gotowymi rozwiązaniami dla każdej niezgodności?

- A. Działania korygujące ustala audytowany, a audytor opisuje ustalenia z dowodami
- B. Raport powinien zawierać wyłącznie rozwiązania
- C. To obowiązkowa dobra praktyka

69. Czy przegląd prowadzony przez dział IT bez prezesa spełnia wymaganie 9.3?

- A. Nie, przegląd przeprowadza najwyższe kierownictwo
- B. Tak, jeśli prezes podpisze protokół później
- C. Tak, jeśli są omówione wszystkie wejścia

70. Co jest wymagane wobec problemu z kontami, który wraca od roku?

- A. Powtórzenie korekcji przy każdym wystąpieniu
- B. Zmiana audytora wewnętrznego
- C. Ustalenie przyczyny, wdrożenie działań korygujących i sprawdzenie ich skuteczności

Scenariusz 7: niezgodności i doskonalenie (pytania 71 do 75)

> Audyt wewnętrzny stwierdził, że dwa konta byłych pracowników są aktywne. Tomek je zablokował i zamknął niezgodność tego samego dnia. Po trzech miesiącach problem wrócił. W analizie zapisano przyczynę „błąd pracownicy kadr”. Marek proponuje, żeby terminale w magazynie same się blokowały po zmianie, a Ola chce napisać osobną procedurę działań zapobiegawczych, „bo norma tego wymaga”.

71. Czym było zablokowanie kont przez Tomka?

- A. Działaniem korygującym
- B. Korekcją
- C. Szansą doskonalenia

72. Jak ocenić zamknięcie niezgodności tego samego dnia?

- A. Jako niepełne, bo zabrakło analizy przyczyny, działania korygującego i oceny jego skuteczności
- B. Jako poprawne
- C. Jako poprawne, jeśli zgodził się audytor

73. Co NAJLEPIEJ zrobić z przyczyną „błąd pracownicy kadr”?

- A. Przyjąć ją i ukarać pracownicę
- B. Przenieść odpowiedzialność na dział IT
- C. Kontynuować analizę, aż znajdziemy przyczynę w procesie, na przykład zgłaszanie odejść e-mailem bez potwierdzenia

74. Czym jest pomysł Marka?

- A. Incydentem
- B. Niezgodnością
- C. Szansą doskonalenia

75. Jak odpowiedzieć Oli?

- A. Ma rację, wymaga tego załącznik A
- B. Ma rację, wymaga tego rozdział 10
- C. ISO/IEC 27001:2022 nie ma osobnego wymagania o działaniach zapobiegawczych, zapobieganie realizuje planowanie oparte na ryzyku

Scenariusz 8: audyt certyfikacyjny (pytania 76 do 80)

> Zielona wybiera jednostkę certyfikującą. Jedna z ofert to „pakiet: wdrożenie i certyfikat” od tej samej jednostki, inna jest najtańsza, ale od jednostki bez akredytacji. Po wyborze akredytowanej jednostki odbywa się etap 1, a na etapie 2 audytorka stwierdza niezgodność dużą: przegląd zarządzania nie odbył się ani razu. Tomek nie zgadza się z inną, małą niezgodnością i chce o niej dyskutować aż do skutku na spotkaniu zamykającym.

76. Jak ocenić ofertę „wdrożenie i certyfikat” od tej samej jednostki?

- A. Narusza bezstronność jednostki certyfikującej, więc wybieramy inną jednostkę albo innego doradcę
- B. Jest korzystna, bo jednostka zna system
- C. Jest dopuszczalna, jeśli doradza inny pracownik tej jednostki

77. Co grozi przy wyborze najtańszej jednostki bez akredytacji?

- A. Akredytacja dotyczy tylko audytorów, nie jednostek
- B. Odbiorca może nie uznać certyfikatu, więc sprawdzamy akredytację i jej zakres
- C. Nic, akredytacja nie ma znaczenia

78. Jaki jest główny cel etapu 1?

- A. Ocena dokumentacji systemu i gotowości do etapu 2
- B. Wydanie certyfikatu
- C. Sprawdzenie skuteczności wszystkich zabezpieczeń

79. Co oznacza niezgodność duża stwierdzona na etapie 2?

- A. Audytor wiodący wyda certyfikat warunkowo
- B. Certyfikat zostanie wydany, a działania będą sprawdzone za rok
- C. Certyfikat nie zostanie wydany, dopóki jednostka nie zweryfikuje korekcji i działań korygujących

80. Jak NAJLEPIEJ postąpić w sporze o ustalenie?

- A. Zażądać zmiany audytorki w trakcie spotkania
- B. Przedstawić dowody na spotkaniu, a jeśli spór trwa, skorzystać z procedury odwołań jednostki
- C. Odmówić podpisania raportu i zakończyć audyt

Klucz i wyjaśnienia do pytań 41 do 80

Nr	Odp.	Domena	Wyjaśnienie
41	A	3	Wąski zakres jest dozwolony, ale musi uwzględniać styki i zależności (4.3). Sklep nie działa bez serwerowni i administratorów.
42	A	3	Polityka nadaje kierunek. Szczegóły należą do niższych dokumentów, które łatwiej zmieniać.
43	B	3	Role można przypisać (5.3), przywództwa (5.1) nie można oddelegować.
44	C	3	Kryteria akceptacji i przeprowadzania oceny trzeba ustalić przed oceną (6.1.2).
45	A	3	Właściciel ryzyka ma odpowiedzialność i uprawnienie do zarządzania ryzykiem, zwykle po stronie biznesu.
46	C	3	Poziom mieści się w kryterium akceptacji. Akceptacja to też decyzja właściciela.
47	A	3	SoA ma uzasadnić włączenie, wyłączenie i podać stan wdrożenia.
48	A	3	Zabezpieczenia dobieramy do ryzyka. Gdy ryzyko istnieje, szukamy innego sposobu jego obniżenia.
49	C	3	Rezygnacja z działania, które tworzy ryzyko, to unikanie.
50	B	3	Zatwierdzenie przez właścicieli ryzyk jest częścią 6.1.3.

Nr	Odp.	Domena	Wyjaśnienie
51	C	4	Nadzór nad informacją udokumentowaną obejmuje wersje i dostępność tam, gdzie są potrzebne (7.5.3).
52	C	4	Norma wymaga zaplanowania komunikacji, w tym sposobu dopasowanego do odbiorcy.
53	C	4	Dowody kompetencji są obowiązkowe (7.2).
54	C	4	Świadomość dotyczy wszystkich pod nadzorem organizacji, a podpis nie pokazuje zrozumienia.
55	A	4	Zarządzanie zmianą wymaga zaangażowania właścicieli procesów. Możliwy kompromis to inny czas blokady na terminalach.
56	C	4	Odtworzenie przed zabezpieczeniem dowodów niszczy materiał do analizy i może przywrócić napastnika.
57	C	4	Liczy się zakres certyfikatu. Relacje z dostawcami nadzorujemy zabezpieczeniami 5.19 do 5.22.
58	B	4	Zmiany awaryjne też przechodzą przez proces zmian (8.32).
59	A	4	Wnioski z incydentów to zabezpieczenie 5.27.
60	B	5	Mierzymy wynik procesu. Liczba alertów zależy głównie od napastników i ustawień.
61	A	5	Monitorowanie bez analizy i oceny nie wystarcza.

Nr	Odp.	Domena	Wyjaśnienie
62	B	5	Metody pomiaru powinny dawać porównywalne i powtarzalne wyniki.
63	A	5	Organizacja ustala, kto mierzy i kto analizuje oraz ocenia.
64	A	5	Wynik poniżej celu jest wejściem do działań korygujących i przeglądu.
65	A	5	Skuteczność kopii to możliwość odtworzenia, a nie samo wykonywanie kopii.
66	A	5	Audytor nie audytuje własnej pracy (9.2).
67	B	5	Audyt wewnętrzny sprawdza zgodność z wymaganiami normy i organizacji oraz skuteczność systemu.
68	A	5	Audytor ustala, audytowany decyduje o działaniach. Tak zachowujemy obiektywizm.
69	A	5	Wymaganie przypisuje przegląd najwyższemu kierownictwu.
70	C	6	Powracająca niezgodność pokazuje, że działały tylko korekcje (10.2).
71	B	6	Korekcja usuwa skutek. Działanie korygujące usuwa przyczynę.
72	A	6	Wymaganie 10.2 obejmuje przyczynę, działania i przegląd ich skuteczności.
73	C	6	Błąd ludzki rzadko jest przyczyną źródłową. Pytamy, co w procesie na niego pozwoliło.

Nr	Odp.	Domena	Wyjaśnienie
74	C	6	Nie dotyczy niespełnionego wymagania, tylko możliwości poprawy.
75	C	6	Osobne działania zapobiegawcze były w wydaniu 2005.
76	A	7	Jednostka nie może doradzać przy wdrożeniu systemu, który certyfikuje (ISO/IEC 17021-1).
77	B	7	Zaufanie do certyfikatu opiera się na akredytacji jednostki według ISO/IEC 17021-1 i 27006-1.
78	A	7	Skuteczność w praktyce sprawdza etap 2, a decyzję podejmuje jednostka po audycie.
79	C	7	Przy niezgodności dużej decyzja czeka na weryfikację działań.
80	B	7	Jednostka ma procedurę odwołań i skarg. Spotkanie zamykające służy wyjaśnieniu, nie negocjacjom.

Dzień 26: analiza błędów

Każdy błąd zapisujemy w dzienniku pomyłek z jedną z sześciu przyczyn: nie znałem pojęcia, pomyliłem dwa podobne pojęcia, pomyliłem wymaganie z dobrą praktyką, oddałem decyzję niewłaściwej roli, nie wróciłem do treści scenariusza, zabrakło czasu. Cztery środkowe przyczyny są najtańsze do usunięcia.

Potem liczymy wynik w każdej domenie. Domena z wynikiem poniżej 70 procent wraca do Fiszki ze swojej strony: domeny 1 i 2 do Zasady, pojęcia i wymagania ISMS: domeny 1 i 2 egzaminu, domena 3 do Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA, domena 4 do Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany, domena 5 do Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania, domeny 6 i 7 do Ciągłe doskonalenie i audyt

certyfikacyjny: od niezgodności do certyfikatu.

Na koniec dnia spisujemy na jednej kartce dziesięć par, które nam się mylą (korekcja i działanie korygujące, zdarzenie i incydent, program i plan audytu, etap 1 i etap 2), i odkładamy ją na rano. Na egzamin kartki nie bierzemy.

Dzień 28: strategia na dzień egzaminu

Przed egzaminem:

- Rano tylko kartka z dziesięcioma parami i Fiszka z tej strony. Nowych tematów nie zaczynamy.
- Logowanie w aplikacji PECB Exams 30 minut przed startem; godzina w panelu jest w UTC [3].
- Na biurku: wydrukowana norma, dokument ze zdjęciem, woda w butelce bez etykiety. Bez telefonu, długopisu i słuchawek [3].
- Przy egzaminie po angielsku zaznaczamy opcję „Non-Native Speaker” przed startem, jeśli nam przysługuje [3].

W trakcie egzaminu:

- Pierwsze przejście: 120 minut na 80 pytań. Odpowiedź zaznaczamy zawsze, także przy fladze.
- Scenariusz czytamy raz, w całości, przed pierwszym z jego pięciu pytań. Przy każdym pytaniu wracamy do niego wzrokiem, a nie do normy.
- Normę otwieramy tylko wtedy, gdy pytanie dotyczy tego, czy coś jest wymaganiem, i wiemy, w którym rozdziale szukać.
- Drugie przejście: 45 minut na flagi. Pierwszą odpowiedź zmieniamy tylko z konkretnego powodu.
- Ostatnie 15 minut: rezerwa i sprawdzenie, czy w panelu nie ma pytań bez odpowiedzi. Odpowiedzi zapisują się tylko po przyciskach „Save and Next” i „Save and Previous” [3].
- Przerwa: jedna, pięć minut, tylko do toalety, a zegar w tym czasie biegnie dalej [3].

Po egzaminie:

- Wynik egzaminu online widzimy od razu po wysłaniu odpowiedzi [2].
- Przy wyniku zaliczającym składamy w myPECB wniosek o certyfikat z opisem doświadczenia i kontaktami do osób, które je potwierdzą, i zapisujemy w kalendarzu termin odnowienia za trzy lata oraz terminy CPD i AMF [1], [4].

- Przy wyniku niezaliczającym wracamy do dnia 26. Kolejne podejście jest możliwe najwcześniej po 15 dniach; darmowe tylko przy szkoleniu, e-learningu albo samodzielnym kursie PECB i w ciągu 12 miesięcy [2].

Częste błędy

Objaw	Przyczyna	Co robimy
Brak czasu na drugie przejście	szukanie odpowiedzi w normie	norma tylko po numer wymagania, pierwsze przejście w 120 minut
Dobre odpowiedzi w części 1, słabe w scenariuszach	odpowiedzi według ogólnej zasady, a nie według firmy ze scenariusza	przy każdym pytaniu wracamy do opisu scenariusza
Wybór odpowiedzi „musi” przy dobrej praktyce	mylenie normy z 27002 i z materiałami szkoleniowymi	Fiszka „wymaganie i dobra praktyka”
Wybór odpowiedzi, w której wdrażający akceptuje ryzyko albo audytor naprawia	mylenie ról	Fiszka „rola wdrażającego i rola kierownictwa”
Wysoki wynik na naszych pytaniach, niski na egzaminie	znamy styl naszych pytań, a nasze odpowiedzi poprawne bywają najdłuższe	analizujemy uzasadnienia, a nie wzór odpowiedzi; jeśli kupiliśmy kurs PECB, robimy też ćwiczenia z materiałów kursu
Zmiana dobrej odpowiedzi na złą przy fladze	niepewność bez powodu	zmieniamy tylko z konkretnym argumentem

□□ Ćwiczenia

1. Po próbie mamy 58 punktów: 25 z 27 w domenach 1 i 2, 11 z 18 w domenie 3, 9 z 14 w domenie 4 i 13 z 21 w domenach 5 do 7. Co robimy w dniu 26?

Odpowiedź

Wynik jest tuż nad progiem 56. Najsłabsze są domena 3 (61 procent) i domeny 5 do 7 (62 procent), a domena 3 ma też najwięcej pytań. Dzień 26 dzielimy: najpierw Fiszka i ćwiczenia z planowania, potem Fiszki z pomiaru, doskonalenia i certyfikacji, a na koniec ponownie scenariusze 1, 2 i 5 do 8 bez zaglądania do klucza.

1. Pytanie brzmi: „Czy deklaracja stosowania musi zawierać wszystkie zabezpieczenia z załącznika A?”, a odpowiedzi to „Tak, bo…”, „Nie, bo…” i drugie „Nie, bo…”. Jak je rozwiązujemy?

Odpowiedź

Najpierw decyzja: SoA musi odnieść się do każdego zabezpieczenia z załącznika A (włączenie albo wyłączenie z uzasadnieniem), ale nie musi ich wszystkich stosować. Dalej wybieramy to „Nie, bo”, którego uzasadnienie mówi właśnie o uzasadnionych wyłączeniach, a odrzucamy to, które mówi na przykład „bo SoA jest dokumentem opcjonalnym”.

1. Na egzaminie zostało 20 minut i 15 pytań bez odpowiedzi. Co robimy?

Odpowiedź

Zaznaczamy odpowiedź przy każdym z 15 pytań, choćby po szybkim przeczytaniu, bo podręcznik nie przewiduje punktów ujemnych, a puste pytanie na pewno nie daje punktu (zasadę punktowania warto potwierdzić w podręczniku przed egzaminem). Przy scenariuszach czytamy tylko zdania o osobach i brakach, a dopiero na koniec wracamy do flag.

Powiązane: Plan 28 dni i papierowe laboratorium: Tomek wdraża ISMS w Zielonej · Ciągłe doskonalenie i audyt certyfikacyjny: od niezgodności do certyfikatu · Próbny egzamin: 40 własnych pytań i strategia na dzień egzaminu

Źródła: [1] PECB, Candidate Handbook ISO/IEC 27001 Lead Implementer (multiple choice), wersja 1.5, 2026 (80 pytań, trzy odpowiedzi, scenariusze po pięć pytań, 43 i 37 pytań według poziomu, liczba pytań w domenach, próg 70 procent, otwarta książka, wniosek o certyfikat); [2] PECB, Exam Rules and Policies (wynik online od razu, poprawka po 15 dniach, darmowa poprawka w ciągu 12 miesięcy); [3] PECB, myPECB Online Examinee Manual (logowanie 30 minut wcześniej, UTC, biurko, przerwa pięć minut, zapisywanie odpowiedzi, opcja „Non-Native Speaker”); [4] PECB, Certification Maintenance Policy 2026 (CPD i AMF). Pytania są własne, napisane na podstawie opisów domen, a nie oficjalnych arkuszy ani materiałów szkoleniowych. Dostęp 23 października 2026.