Zasady, pojęcia i wymagania ISMS: domeny 1 i 2 egzaminu

Poziom: podstawy

Dotyczy: PECB ISO/IEC 27001 Lead Implementer, domena 1 (15 pytań, 18,75%) i domena 2 (12 pytań, 15%), ISO/IEC 27001:2022 z Amd 1:2024 i ISO/IEC 27002:2022

Czas: ~60 min, dni 2 do 5 planu

Słownik i szkielet normy: czym jest informacja i jej bezpieczeństwo, czym system zarządzania różni się od zbioru zabezpieczeń, co stoi w rozdziałach 4 do 10 i w załączniku A, które dokumenty są obowiązkowe. Te dwie domeny to razem 27 pytań, a dwie domeny egzaminu Foundation pokrywają się z nimi tematycznie. Wracamy tu przy każdym pytaniu, w którym dwie odpowiedzi różnią się jednym słowem.

Definicje na tej stronie są naszą parafrazą na podstawie ISO/IEC 27000 i ISO/IEC 27001:2022 [1], [2]; nie cytujemy tekstu norm. Polskie nazwy pojęć bierzemy z polskich wydań norm z rodziny 27000 tam, gdzie je znamy, a nazwy angielskie podajemy w nawiasie, bo na egzaminie w języku angielskim zobaczymy właśnie je. Normę i zabezpieczenia omówione po ludzku opisuje książka „ISO/IEC 27001: bezpieczeństwo informacji po ludzku”, zaczynając od strony ISO/IEC 27001 po ludzku: system zarządzania, rozdziały 4 do 10, Załącznik A i deklaracja stosowania; tu interesuje nas tylko to, czego wymaga egzamin.

Skróty użyte na tej stronie (7)

Skrót	Co znaczy
HLS	High Level Structure: dawna nazwa wspólnej struktury norm systemów zarządzania, czyli tych samych rozdziałów 4 do 10 w ISO 9001, 14001, 27001 i innych
ICT	Information and Communication Technology: technologie informacyjne i komunikacyjne, czyli systemy, sieci i usługi IT razem z łącznością
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

Skrót	Co znaczy
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
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

Fiszka

Karty pojęć i pułapek. Czytamy nagłówek, zakrywamy resztę i mówimy definicję własnymi słowami, potem sprawdzamy.

□□ TYLKO ODCZYT

Zapamiętanie definicji: informacja i aktywo

Informacja to dane, które mają dla organizacji znaczenie i wartość, w dowolnej postaci: w bazie, na papierze, w głowie pracownika. Aktywo (asset) to wszystko, co ma wartość dla organizacji, także sprzęt, oprogramowanie, usługi i ludzie z ich wiedzą.

Pułapka: odpowiedź „informacja to tylko dane w systemach IT” jest za wąska. Umowa w szafie księgowości też jest w zakresie.

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

□□ TYLKO ODCZYT

Rozróżnienie: poufność, integralność, dostępność

Poufność (confidentiality): informacja nie trafia do osób ani procesów, które nie mają do niej prawa. Integralność (integrity): informacja jest dokładna i kompletna. Dostępność (availability): uprawniona osoba może z niej skorzystać wtedy, gdy potrzebuje.

Pułapka: zaszyfrowana kopia, której nie da się odtworzyć, bo zgubiono klucz, chroni poufność i niszczy dostępność.

□□ TYLKO ODCZYT

Zapamiętanie definicji: bezpieczeństwo informacji

Zachowanie poufności, integralności i dostępności informacji. Mogą dochodzić inne właściwości: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Pułapka: bezpieczeństwo informacji to nie to samo co cyberbezpieczeństwo. Obejmuje też papier, rozmowy i budynki.

□□ TYLKO ODCZYT

Zapamiętanie definicji: system zarządzania i ISMS

System zarządzania to powiązane elementy organizacji (polityki, cele, procesy, role), które służą ustaleniu celów i ich osiąganiu. ISMS (system zarządzania bezpieczeństwem informacji) to taki system nastawiony na bezpieczeństwo informacji i oparty na zarządzaniu ryzykiem.

Pułapka: ISMS to nie zbiór zabezpieczeń ani program komputerowy. Zabezpieczenia są wynikiem działania systemu, a nie systemem.

□□ **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

□□ TYLKO ODCZYT

Odróżnienie: norma z wymaganiami i norma z wytycznymi

ISO/IEC 27001 zawiera wymagania i tylko na jej podstawie certyfikuje się organizację. ISO/IEC 27002 (zabezpieczenia), 27003 (wdrożenie), 27004 (pomiar) i 27005 (ryzyko) dają wytyczne. ISO/IEC 27006-1 i 27007 dotyczą jednostek certyfikujących i audytu.

Pułapka: „certyfikat ISO/IEC 27002” nie istnieje dla organizacji. Certyfikat dotyczy zawsze 27001.

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

□□ TYLKO ODCZYT

Rozpoznanie słów: musi, powinien, może

W normach ISO słowo odpowiadające „musi” (shall) oznacza wymaganie, „powinien” (should) zalecenie, „może” (may) dozwoloną możliwość, a „potrafi” (can) możliwość albo zdolność.

Pułapka: zalecenie z ISO/IEC 27002 nie jest wymaganiem. Audytor nie wystawi niezgodności za to, że nie robimy czegoś dokładnie tak, jak radzi 27002, jeśli nasze zabezpieczenie spełnia cel.

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

□□ TYLKO ODCZYT

Zapamiętanie układu: rozdziały 4 do 10

4 kontekst organizacji, 5 przywództwo, 6 planowanie, 7 wsparcie, 8 działania operacyjne, 9 ocena efektów, 10 doskonalenie. Rozdziały 1 do 3 to zakres normy, odwołania i terminy, bez wymagań.

Pułapka: ten sam układ mają ISO 9001, 14001 i inne normy systemów zarządzania (wspólna struktura, dawniej Annex SL i HLS). Dzięki temu łatwo zbudować system zintegrowany.

□□ **ISO** = International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie · **HLS** = High Level Structure: dawna nazwa wspólnej struktury norm systemów zarządzania, czyli tych samych rozdziałów 4 do 10 w ISO 9001, 14001, 27001 i innych

□□ TYLKO ODCZYT

Odróżnienie: wymaganie z rozdziałów 4 do 10 i zabezpieczenie z załącznika A

Żadnego wymagania z rozdziałów 4 do 10 nie można wyłączyć, jeśli chcemy deklarować zgodność. Zabezpieczenie z załącznika A można uznać za niepotrzebne, ale wyłączenie trzeba uzasadnić w deklaracji stosowania.

Pułapka: „nie mamy audytu wewnętrznego, bo jesteśmy małą firmą” to niezgodność. „Nie stosujemy zabezpieczenia o bezpiecznym tworzeniu oprogramowania, bo nie tworzymy oprogramowania” może być uzasadnionym wyłączeniem.

□□ TYLKO ODCZYT

Rozpoznanie tematów: załącznik A

93 zabezpieczenia w czterech tematach: organizacyjne (37, numery 5.x), osobowe (8, numery 6.x), fizyczne (14, numery 7.x) i technologiczne (34, numery 8.x). Numeracja odpowiada rozdziałom ISO/IEC 27002:2022.

Pułapka: odpowiedzi z wydania 2013 (114 zabezpieczeń w 14 obszarach, numery A.5 do A.18) są nieaktualne.

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

TYLKO ODCZYT

Rozpoznanie atrybutów: ISO/IEC 27002

Pięć atrybutów pomaga filtrować zabezpieczenia: rodzaj (zapobiegawcze, wykrywające, korygujące), chronione właściwości (poufność, integralność, dostępność), pojęcia cyberbezpieczeństwa (identyfikacja, ochrona, wykrywanie, reagowanie, odtwarzanie), zdolności operacyjne i domeny bezpieczeństwa.

Pułapka: atrybuty są narzędziem do porządkowania, a nie wymaganiem. Nie trzeba ich stosować.

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

TYLKO ODCZYT

Odróżnienie: zagrożenie, podatność, zdarzenie, incydent

Zagrożenie to możliwa przyczyna niepożądanego zdarzenia (pożar, złodziej, błąd). Podatność to słabość aktywa albo zabezpieczenia, którą zagrożenie może wykorzystać. Zdarzenie bezpieczeństwa informacji to sytuacja wskazująca na możliwe naruszenie. Incydent to zdarzenie albo seria zdarzeń, które z dużym prawdopodobieństwem szkodzą działalności albo bezpieczeństwu informacji.

Pułapka: nieudana próba logowania to zdarzenie. Udane logowanie złodzieja na konto Kasi to incydent.

TYLKO ODCZYT

Zapamiętanie definicji: ryzyko, właściciel ryzyka, ryzyko szczątkowe

Ryzyko to wpływ niepewności na cele, opisywany zwykle skutkiem i prawdopodobieństwem. Właściciel ryzyka to osoba albo rola z odpowiedzialnością i uprawnieniem do zarządzania ryzykiem. Ryzyko szczątkowe to ryzyko, które zostaje po postępowaniu z nim.

Pułapka: właściciel ryzyka nie musi być właścicielem aktywa ani działu IT. Ryzyko szczątkowe akceptuje właściciel ryzyka, a nie wdrażający.

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

TYLKO ODCZYT

Odróżnienie: zabezpieczenie i cel zabezpieczenia

Zabezpieczenie (control) to środek, który utrzymuje albo zmienia ryzyko: polityka, procedura, urządzenie, praktyka. Cel zabezpieczenia mówi, co chcemy osiągnąć.

Pułapka: zabezpieczenie, które nie działa, nadal jest zabezpieczeniem, tylko nieskutecznym. Dlatego mierzymy skuteczność.

TYLKO ODCZYT

Odróżnienie: skuteczność i zgodność

Skuteczność (effectiveness) to stopień, w jakim zaplanowane działania zostały zrealizowane i dały zaplanowane wyniki. Zgodność (conformity) to spełnienie wymagania, niezgodność to jego niespełnienie.

Pułapka: system może być zgodny na papierze i nieskuteczny w praktyce. Etap 2 audytu certyfikacyjnego sprawdza właśnie skuteczność.

TYLKO ODCZYT

Odróżnienie: utrzymywanie i zachowywanie informacji udokumentowanej

Informację utrzymujemy (maintain), gdy ma być aktualna: polityka, procedura, zakres. Informację zachowujemy (retain), gdy jest dowodem: zapis, protokół, wynik. Razem nazywamy je informacjami udokumentowanymi.

Pułapka: norma z 2022 roku nie używa podziału na „dokumenty” i „zapisy”, ale w pytaniach nadal się pojawia. Polityka to dokument utrzymywany, raport z audytu to zapis zachowywany.

TYLKO ODCZYT

Zapamiętanie listy: obowiązkowe informacje udokumentowane

Zakres (4.3), polityka (5.2), proces oceny ryzyka (6.1.2), proces postępowania z ryzykiem (6.1.3), deklaracja stosowania (6.1.3 d), cele (6.2), dowody kompetencji (7.2), informacje potrzebne do zaufania, że procesy działają zgodnie z planem (8.1), wyniki oceny ryzyka (8.2) i postępowania z ryzykiem (8.3), wyniki monitorowania i pomiaru (9.1), program i wyniki audytów (9.2), wyniki przeglądu zarządzania (9.3), niezgodności i działania korygujące (10.2).

Pułapka: „procedura audytu wewnętrznego” nie jest wprost obowiązkowa. Obowiązkowe są dowody programu i wyników.

TYLKO ODCZYT

Zapamiętanie zmian: wydanie 2022 i poprawka 2024

Nowy punkt 6.3 o planowaniu zmian w ISMS, wyraźne wymaganie procesów i ich powiązań w 4.4, wybór wymagań stron zainteresowanych, które system ma spełniać (4.2), zmiany potrzeb stron jako wejście przeglądu zarządzania (9.3), 93 zabezpieczenia zamiast 114, w tym 11 nowych. Poprawka Amd 1:2024 każe ocenić, czy zmiana klimatu jest istotną sprawą i wymaganiem stron.

Pułapka: poprawka z 2024 roku nie tworzy nowego wydania. Mówimy „ISO/IEC 27001:2022 z Amd 1:2024”.

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

Z życia wzięte

Z ŻYCIA WZIĘTE

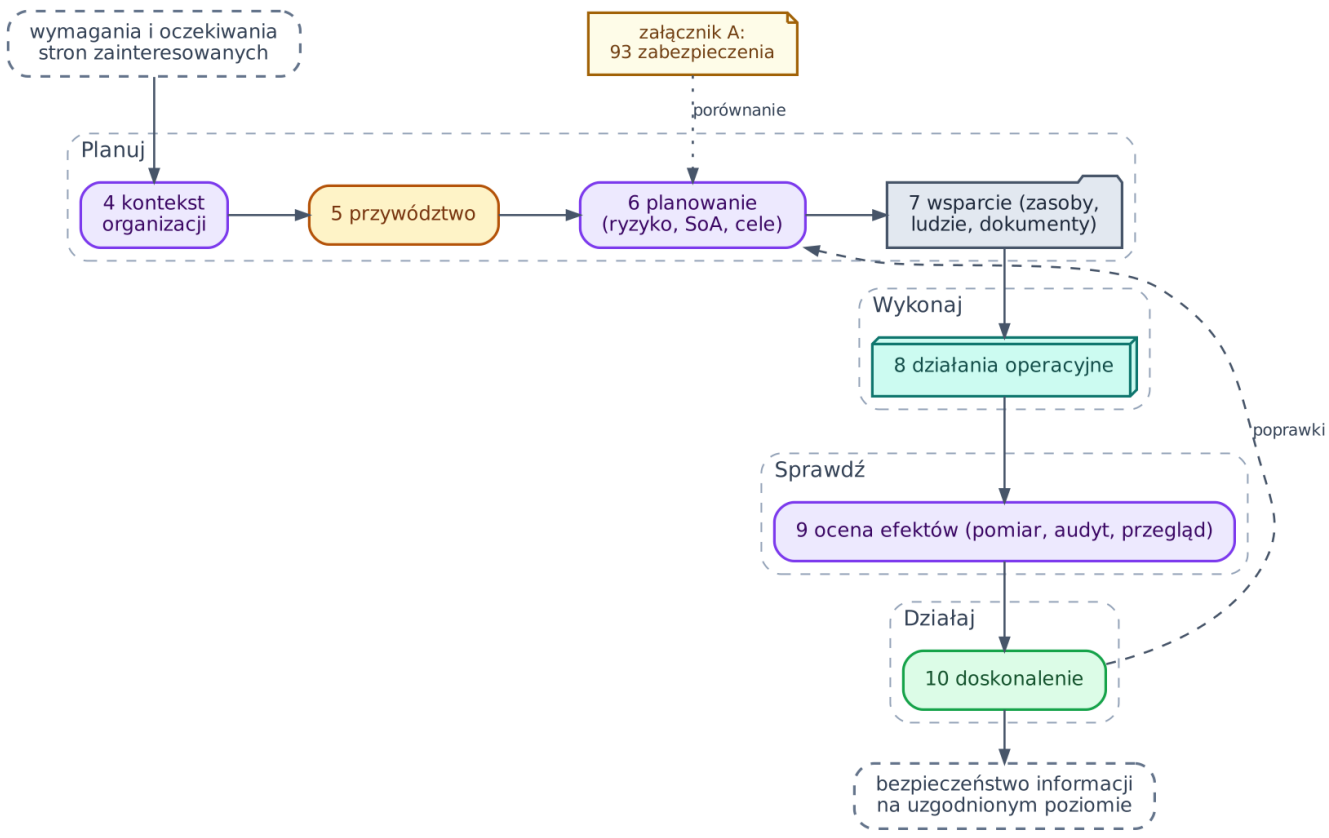
Czwartek, 15:20. Ola przysyła Tomkowi link do „szablonu ISO 27001 do pobrania”: 114 zabezpieczeń, obszary A.5 do A.18 i rozdział „Procedura działań zapobiegawczych”. Tomek prawie wkleja go do teczki, ale zauważa, że w jego wydrukowanej normie załącznik A ma 93 pozycje, a działań zapobiegawczych jako osobnego wymagania nie ma od lat. Szablon trafia do kosza, a do dziennika pomyłek wpis: każde źródło sprawdzamy, z którego wydania pochodzi.

Jak to działa

Rozwiń: jak to działa pod spodem

> **Pojęcie: wspólna struktura norm systemów zarządzania.** Jednakowy układ rozdziałów, wspólne terminy i część wspólnych zdań w normach ISO o systemach zarządzania. ISO/IEC 27001:2022 korzysta z niej w wersji z 2021 roku; w materiałach spotkamy dawne nazwy Annex SL i HLS (High Level Structure).

Norma ma dwie warstwy. Rozdziały 4 do 10 opisują system zarządzania: co trzeba ustalić, zaplanować, zrobić, sprawdzić i poprawić. Załącznik A to katalog zabezpieczeń, z którym porównujemy zabezpieczenia wybrane na podstawie ryzyka, żeby nic ważnego nie umknęło.



Rysunek 1. Rozdziały 4 do 10 ISO/IEC 27001:2022 w cyklu Planuj, Wykonaj, Sprawdź, Działaj; załącznik A porównujemy z wynikiem planowania (kliknięcie otwiera pełny rozmiar)

Pojęcie: PDCA (Plan, Do, Check, Act). Cykl doskonalenia: planujemy, wykonujemy, sprawdzamy wynik i działamy, żeby poprawić. Norma z 2022 roku nie wymienia go z nazwy, ale układ rozdziałów mu odpowiada, a materiały szkoleniowe i pytania często z niego korzystają.

Pojęcie: podejście procesowe. Zarządzanie pracą jako zbiorem powiązanych procesów, z wejściami, wyjściami i właścicielami. Wymaganie 4.4 każe ustalić procesy potrzebne systemowi i ich wzajemne oddziaływanie.

Rodzina ISO/IEC 27000 na egzaminie

Norma	Rodzaj	Do czego przyda się na egzaminie
ISO/IEC 27000	przegląd i słownik, wydanie 2026 według źródła wtórnego [5]	definicje pojęć
ISO/IEC 27001:2022 z Amd 1:2024	wymagania, podstawa certyfikacji	wszystkie domeny, jedyna norma na biurku
ISO/IEC 27002:2022	wytyczne do 93 zabezpieczeń, atrybuty	domeny 1 i 4
ISO/IEC 27003	wytyczne wdrażania wymagań	domeny 3 i 4
ISO/IEC 27004	wytyczne monitorowania i pomiaru	domena 5
ISO/IEC 27005:2022	wytyczne zarządzania ryzykiem	domena 3
ISO/IEC 27006-1:2024	wymagania dla jednostek certyfikujących ISMS	domena 7
ISO/IEC 27007	wytyczne audytu ISMS	domeny 5 i 7
ISO 19011:2026	wytyczne audytowania systemów zarządzania	domena 5
ISO/IEC 17021-1	wymagania dla jednostek certyfikujących systemy	domena 7

Aktualne numery wydań 27003, 27004 i 27007 sprawdzamy w katalogu ISO przed egzaminem (do potwierdzenia); na egzaminie liczy się, do czego służy norma, a nie rok wydania.

Cztery tematy załącznika A na przykładach Zielonej

Temat	Ile	Przykład z Zielonej	Gdzie w bazie
organizacyjne	37	polityki, klasyfikacja informacji, dostawcy, chmura, kopie zapasowe jako ciągłość, zarządzanie incydentami	Standard pracy administratora Zielonej: zasady na pierwszy dzień
osobowe	8	weryfikacja przed zatrudnieniem, szkolenia, zasady pracy zdalnej Kasi, zgłaszanie zdarzeń	Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu
fizyczne	14	strefy i karty do serwerowni, monitoring, niszczenie nośników	Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień
technologiczne	34	MFA, Defender, kopie na `bkp01` i `bkp02`, logi w Graylogu, podatności	Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje

Jedenaście zabezpieczeń dodanych w 2022 roku to według ISO/IEC 27002:2022 między innymi analiza zagrożeń, bezpieczeństwo usług chmurowych, gotowość ICT do ciągłości działania, monitorowanie bezpieczeństwa fizycznego, zarządzanie konfiguracją, usuwanie informacji, maskowanie danych, zapobieganie wyciekom danych, monitorowanie działań, filtrowanie stron i bezpieczne programowanie. Nazwy są naszym streszczeniem.

Wymagania rozdział po rozdziale

Rozdział	O co chodzi w jednym zdaniu (nasze streszczenie)	Obowiązkowa informacja udokumentowana
4 kontekst	rozumiemy firmę, strony zainteresowane i ich wymagania, ustalamy zakres i procesy	zakres
5 przywództwo	kierownictwo bierze odpowiedzialność, ustala politykę, przydziela role	polityka

Rozdział	O co chodzi w jednym zdaniu (nasze streszczenie)	Obowiązkowa informacja udokumentowana
6 planowanie	zajmujemy się ryzykami i szansami, oceniamy ryzyko i postępujemy z nim, ustalamy cele, planujemy zmiany	procesy ryzyka, SoA, wyniki, cele
7 wsparcie	zasoby, kompetencje, świadomość, komunikacja, nadzór nad dokumentami	dowody kompetencji, dokumenty uznane za potrzebne
8 działania operacyjne	robimy to, co zaplanowaliśmy, nadzorujemy zmiany i dostawców, oceniamy ryzyko cyklicznie	zapisy działań, wyniki oceny i postępowania z ryzykiem
9 ocena efektów	monitorujemy, mierzymy, audytujemy i przeglądamy system	wyniki pomiaru, program i wyniki audytów, wyniki przeglądu
10 doskonalenie	stale poprawiamy, reagujemy na niezgodności i usuwamy ich przyczyny	niezgodności i działania korygujące

Częste błędy

Objaw	Przyczyna	Co robimy
Wybieramy odpowiedź z liczbą 114 albo z numerem A.12	materiały do wydania 2013	numeracja 5.x do 8.x i 93 zabezpieczenia
Myślimy, że zalecenie z 27002 jest obowiązkowe	mylimy „powinien” z „musi”	wymagania są tylko w 27001, wytyczne zostawiają wybór sposobu
Uznajemy, że małej firmie wolno pominąć rozdział 9	mylimy wyłączenie zabezpieczenia z wyłączeniem wymagania	wymagań z rozdziałów 4 do 10 nie wyłączamy nigdy
Mylimy zdarzenie z incydentem	oba słowa w pytaniu, różnica w skutku	incydent szkodzi albo z dużym prawdopodobieństwem zaszkodzi
Szukamy w normie definicji	definicje są w ISO/IEC 27000, nie w 27001	definicje uczymy się z pamięci, norma na biurku służy do wymagań
Mylimy właściciela ryzyka z właścicielem aktywa	podobne nazwy	ryzyko akceptuje osoba z uprawnieniem do decyzji o nim

□□ Ćwiczenia

1. Pani Halina drukuje listę płac i zostawia ją w drukarce na korytarzu. Której właściwości informacji grozi ta sytuacja i do którego tematu załącznika A należą zabezpieczenia, które

jej zapobiegają?

Odpowiedź

Poufności. Zabezpieczenia są w kilku tematach: zasada czystego biurka i ekranu to temat fizyczny, druk z odbiorem po zalogowaniu karty to rozwiązanie techniczne, a szkolenie pani Haliny to temat osobowy. Na egzaminie wybieramy odpowiedź, która pasuje do opisu w pytaniu, a nie jedyną słuszną.

1. Zielona nie tworzy oprogramowania, ale zespół Oli pisze aplikacje wewnętrzne na PostgreSQL. Czy w deklaracji stosowania można wyłączyć zabezpieczenie o bezpiecznym programowaniu?

Odpowiedź

Nie, bo założenie jest fałszywe: Zielona tworzy oprogramowanie, choć tylko na własny użytek. Wyłączenie byłoby uzasadnione dopiero wtedy, gdyby nikt w zakresie systemu nie pisał ani nie zamawiał kodu. Uzasadnienie wyłączenia musi wynikać z ryzyka i z rzeczywistości.

1. Które z tych dokumentów są obowiązkowe według ISO/IEC 27001:2022: polityka haseł, deklaracja stosowania, procedura audytu wewnętrznego, wyniki przeglądu zarządzania?

Odpowiedź

Deklaracja stosowania (6.1.3 d) i wyniki przeglądu zarządzania (9.3). Polityka haseł i procedura audytu mogą być potrzebne, jeśli tak zdecydujemy w 7.5.1 albo wynikają z wybranych zabezpieczeń, ale sama norma nie wymienia ich wprost jako obowiązkowych.

1. Tomek pisze w słowniczku: „ISMS to Defender, MFA i kopie zapasowe”. Co poprawiamy?

Odpowiedź

To lista zabezpieczeń, a nie system zarządzania. ISMS to polityka, role, ocena ryzyka, cele, procesy, pomiar, audyt i doskonalenie, które decydują, jakie zabezpieczenia stosujemy i czy działają. Defender, MFA i kopie są wynikiem działania systemu.

Powiązane: Plan 28 dni i papierowe laboratorium: Tomek wdraża ISMS w Zielonej · Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA · Słownik pracy administratora: usługa, incydent, wniosek, problem i zmiana

Źródła: [1] ISO/IEC 27000 (przegląd i słownik; definicje sparafrazowane, nie cytowane); [2] ISO/IEC 27001:2022 i Amd 1:2024 (układ rozdziałów, lista informacji udokumentowanych; nasze streszczenie); [3] ISO/IEC 27002:2022 (tematy, liczby zabezpieczeń, atrybuty; nasze streszczenie); [4] PECB, Candidate Handbook ISO/IEC 27001 Lead Implementer, wersja 1.5, 2026 (domeny 1 i 2, liczba pytań) i Candidate Handbook ISO/IEC 27001:2022 Foundation, wersja 1.5, 2026; [5] Bright Defense, „ISO 27001: What Changed in 2026?” (Amd 1:2024, ISO/IEC 27000:2026; źródło wtórne). Dostęp 23 października 2026.

Revision #3
Created 2026-10-23 17:13:57 UTC by Tomasz Konieczny
Updated 2026-10-26 14:28:05 UTC by Tomasz Konieczny