Fundamenty i planowanie ISMS

Zasady, pojęcia i wymagania oraz planowanie wdrożenia.

- Zasady, pojęcia i wymagania ISMS: domeny 1 i 2 egzaminu
- Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA

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

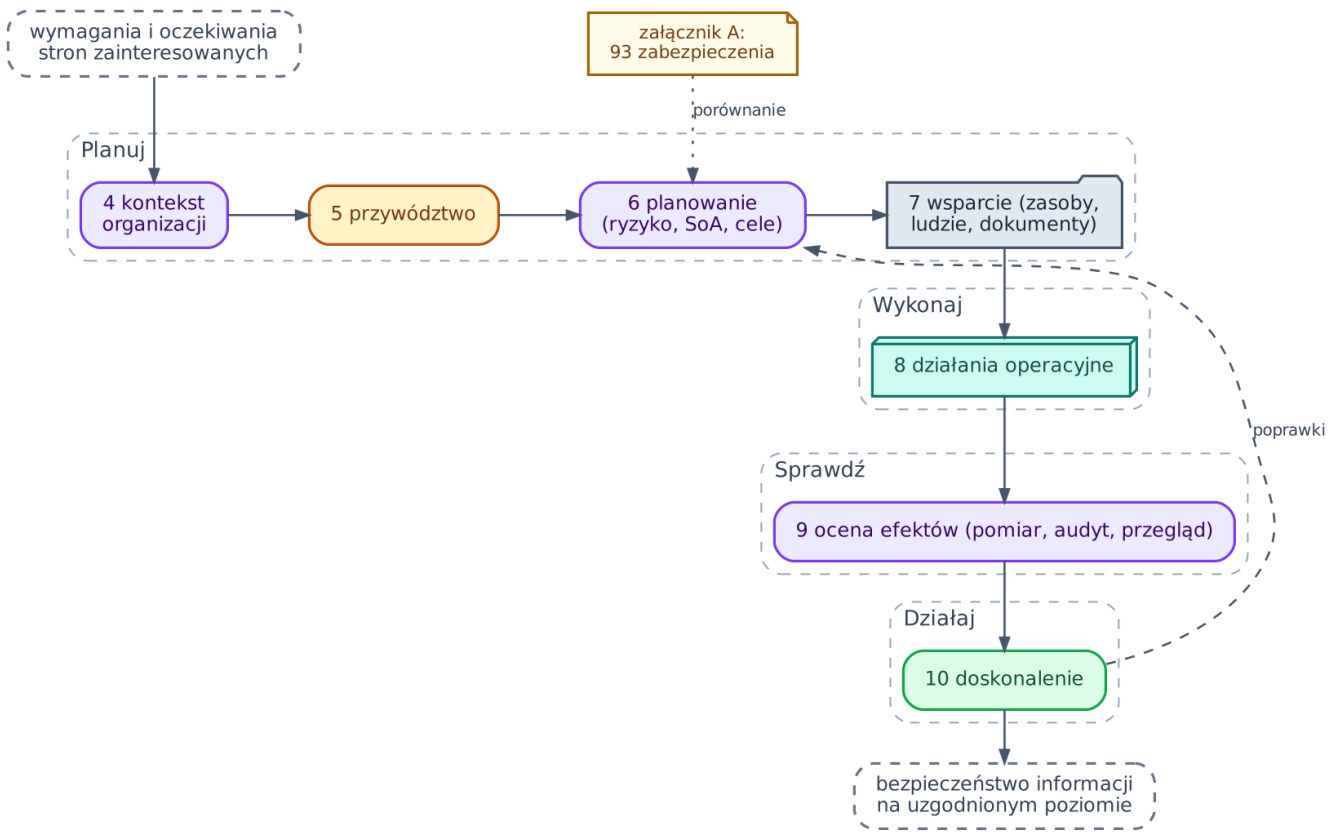
Czwartek, 15:20. Ola przysyła Tomkowi link do „szablonu ISO 27001 do pobrania”: 114 zabezpieczeń, obszary A.5 do A.18 i rozdział „Procedura działań zapobiegawczych”. Tomek prawie wkleja go do teczki, ale zauważa, że w jego wydrukowanej normie załącznik A ma 93 pozycje, a działań zapobiegawczych jako 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.

Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA

Poziom: średnio

Dotyczy: PECB ISO/IEC 27001 Lead Implementer, domena 3 (18 pytań, 22,5%, najwięcej na egzaminie), ISO/IEC 27001:2022 rozdziały 4 do 6, ISO/IEC 27005:2022

Czas: ~90 min czytania, dni 6 do 11 planu, artefakty A1 do A6

Od decyzji prezesa do deklaracji stosowania: jak zacząć projekt, zrozumieć firmę i jej otoczenie, wyznaczyć zakres, zdobyć politykę i role, ocenić ryzyko, wybrać zabezpieczenia i ustalić cele. To najwięcej pytań na egzaminie i najwięcej pracy w prawdziwym wdrożeniu. Wracamy tu przy każdym scenariuszu, w którym ktoś „zaczyna od zabezpieczeń”.

Wszystkie przykłady pochodzą z papierowego laboratorium: Tomek przygotowuje artefakty A1 do A6 dla Zielonej. Liczby w rejestrze ryzyk i skale są naszym ćwiczeniem, a nie wzorem z normy, bo norma nie narzuca metody, tylko wymaga, żeby była opisana i dawała powtarzalne wyniki.

ZAŁOŻENIA SCENARIUSZA

zakres ISMS w ćwiczeniu to usługi IT świadczone przez zespół IT dla całej Zielonej, z serwerownią w Pamiątkowie i usługami dla magazynu w Swarzędzu; księgowość, magazyn i sprzedaż korzystają z tych usług i są właścicielami części ryzyk. Zakres, który Zielona naprawdę proponuje (cała firma), i jej macierz ryzyka 3 na 3 opisuje strona Zakres i ryzyko w Zielonej: rejestr aktywów, macierz ryzyka i plan postępowania; w laboratorium celowo ćwiczymy węższy zakres i skalę 1 do 5, żeby zobaczyć, że jedno i drugie jest wyborem organizacji. Ryzyka laboratorium mają numery L-01 do L-10, żeby nie myliły się z rejestrem R-01 z tamtej strony.

Skróty użyte na tej stronie (12)

Skrót	Co znaczy

B2B	business to business: sprzedaż i systemy skierowane do innych firm, nie do klientów indywidualnych
CISO	Chief Information Security Officer: dyrektor do spraw bezpieczeństwa informacji; ISO/IEC 27001 nie wymaga takiego stanowiska, tylko przypisania odpowiedzialności
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
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
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
PESTLE	Political, Economic, Social, Technological, Legal, Environmental: czynniki zewnętrzne (polityczne, ekonomiczne, społeczne, technologiczne, prawne, środowiskowe), które wpływają na organizację i jej usługi
RACI	Responsible, Accountable, Consulted, Informed: tabela ról, która dla każdego zadania mówi, kto wykonuje, kto odpowiada i zatwierdza, kogo pytamy i kogo informujemy
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
SWOT	Strengths, Weaknesses, Opportunities, Threats: prosta analiza mocnych i słabych stron oraz szans i zagrożeń, używana do opisania kontekstu organizacji

Fiszka

Karty pojęć i pułapek domeny 3. Czytamy nagłówek, zakrywamy resztę, mówimy z pamięci.

□□ TYLKO ODCZYT

Rozpoczęcie projektu: uzasadnienie i zgoda kierownictwa

Projekt zaczyna się od celu biznesowego (wymaganie klienta, przepisy, ryzyko), uzasadnienia, wstępnego zakresu, budżetu i formalnej zgody najwyższego kierownictwa. Bez tej zgody nie ma kogo poprosić o politykę ani o akceptację ryzyka.

Pułapka: w scenariuszu, w którym kierownictwo „jeszcze się zastanawia”, najlepszą odpowiedzią jest prawie zawsze zdobycie zaangażowania kierownictwa, a nie zakup narzędzia.

TYLKO ODCZYT

Analiza luk: stan obecny wobec wymagań

Porównanie tego, co firma już ma, z wymaganiami rozdziałów 4 do 10 i z zabezpieczeniami z załącznika A. Wynik: lista luk, która jest podstawą planu projektu.

Pułapka: analiza luk nie zastępuje oceny ryzyka. Mówi, czego brakuje względem normy, a nie, co grozi firmie.

TYLKO ODCZYT

Ustalenie kontekstu: sprawy wewnętrzne i zewnętrzne

Sprawy, które wpływają na zdolność systemu do osiągania wyników: kultura, struktura, systemy, przepisy, rynek, technologia, dostawcy. Od 2024 roku także odpowiedź na pytanie, czy zmiana klimatu jest istotną sprawą.

Pułapka: kontekst nie jest dokumentem obowiązkowym, ale audytor zapyta, skąd wiemy, co go tworzy. Zwykle wystarcza tabela albo analiza SWOT czy PESTLE.

SWOT = Strengths, Weaknesses, Opportunities, Threats: prosta analiza mocnych i słabych stron oraz szans i zagrożeń, używana do opisania kontekstu organizacji · **PESTLE** = Political, Economic, Social, Technological, Legal, Environmental: czynniki zewnętrzne (polityczne, ekonomiczne, społeczne, technologiczne, prawne, środowiskowe), które wpływają na organizację i jej usługi

TYLKO ODCZYT

Ustalenie stron zainteresowanych: kto i czego wymaga

Lista stron istotnych dla systemu, ich wymagania i decyzja, które z tych wymagań spełniamy przez ISMS. Wymagania mogą obejmować przepisy, umowy i oczekiwania.

Pułapka: wymaganie strony zainteresowanej nie staje się automatycznie wymaganiem systemu. Organizacja decyduje, które przyjmuje (4.2 c).

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

Wyznaczenie zakresu: granice i styki

Zakres opisuje, czego dotyczy system: procesy, lokalizacje, aktywa, ludzie, technologie, oraz styki i zależności z tym, co poza zakresem. Musi uwzględniać kontekst i wymagania stron. Jest obowiązkową informacją udokumentowaną.

Pułapka: zakres wąski jest dozwolony, ale nie może wykluczać tego, bez czego usługa w zakresie nie działa, bez opisania styku. Wykluczenie serwerowni z zakresu usług IT to błąd.

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

TYLKO ODCZYT

Wykazanie przywództwa: najwyższe kierownictwo

Kierownictwo zapewnia politykę i cele zgodne ze strategią, włącza wymagania systemu w procesy firmy, daje zasoby, komunikuje, wspiera ludzi i kierowników oraz promuje doskonalenie.

Pułapka: odpowiedzialność za system można przypisać, ale przywództwa nie da się oddelegować na pełnomocnika ani na dział IT.

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

TYLKO ODCZYT

Ustanowienie polityki: bezpieczeństwo informacji

Polityka pasuje do celu organizacji, daje ramy dla celów, zawiera zobowiązanie do spełniania wymagań i do ciągłego doskonalenia. Jest udokumentowana, zakomunikowana w firmie i dostępna dla stron zainteresowanych, gdy trzeba.

Pułapka: polityka nie musi być długa i nie opisuje konfiguracji. Szczegóły należą do polityk tematycznych i procedur.

TYLKO ODCZYT

Przypisanie ról: odpowiedzialność i uprawnienia

Kierownictwo przypisuje i komunikuje role, w tym odpowiedzialność za zgodność systemu z normą i za raportowanie o jego wynikach do kierownictwa.

Pułapka: norma nie wymaga stanowiska CISO ani pełnomocnika o konkretnej nazwie. Wymaga, żeby te dwie odpowiedzialności były przypisane.

□□ **CISO** = Chief Information Security Officer: dyrektor do spraw bezpieczeństwa informacji; ISO/IEC 27001 nie wymaga takiego stanowiska, tylko przypisania odpowiedzialności

□□ TYLKO ODCZYT

Działania wobec ryzyk i szans: 6.1.1

Planujemy, jak poradzić sobie z ryzykami i szansami dla samego systemu (czy osiągnie wyniki, czy uniknie skutków ubocznych, czy będzie się doskonalił), na podstawie kontekstu i wymagań stron.

Pułapka: 6.1.1 to szersze ryzyka systemu, na przykład „brak budżetu na projekt”. Ryzyka dla informacji ocenia proces z 6.1.2.

□□ TYLKO ODCZYT

Ustalenie kryteriów: akceptacja i ocena ryzyka

Przed oceną ustalamy kryteria akceptacji ryzyka i kryteria przeprowadzania oceny. Powtórzona ocena ma dawać spójne, ważne i porównywalne wyniki.

Pułapka: kryteria ustala się przed identyfikacją ryzyk, nie po. Inaczej każdy poziom „wychodzi” akceptowalny.

□□ TYLKO ODCZYT

Ocena ryzyka: identyfikacja, analiza, ewaluacja

Identyfikacja ryzyk dla poufności, integralności i dostępności informacji w zakresie, ze wskazaniem właścicieli; analiza możliwych skutków i realnego prawdopodobieństwa; ewaluacja, czyli porównanie z kryteriami i ustalenie kolejności postępowania.

Pułapka: norma z 2022 roku nie wymaga podejścia opartego na aktywach. ISO/IEC 27005:2022 opisuje dwa podejścia: od aktywów i od zdarzeń (scenariuszy).

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

TYLKO ODCZYT

Wybór opcji postępowania: cztery drogi

Zmniejszenie ryzyka przez zabezpieczenia (w ISO/IEC 27005 modyfikacja), zachowanie, czyli świadoma akceptacja, unikanie przez rezygnację z działania, oraz dzielenie się ryzykiem, na przykład z ubezpieczycielem albo dostawcą.

Pułapka: przeniesienie ryzyka na dostawcę nie przenosi odpowiedzialności za informację. Ubezpieczenie dzieli skutki finansowe, nie chroni danych.

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

TYLKO ODCZYT

Sporządzenie deklaracji stosowania: SoA

Deklaracja stosowania zawiera potrzebne zabezpieczenia (z załącznika A i spoza niego), uzasadnienie ich włączenia, informację, czy są wdrożone, i uzasadnienie wyłączenia każdego zabezpieczenia z załącznika A, którego nie stosujemy.

Pułapka: SoA powstaje po wyborze zabezpieczeń z postępowania z ryzykiem. Zabezpieczenia wybieramy do ryzyk, a załącznik A służy do sprawdzenia, czy nic nie pominęliśmy.

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

Zatwierdzenie planu: właściciele ryzyk

Plan postępowania z ryzykiem i pozostające ryzyko szczątkowe zatwierdzają właściciele ryzyk.

Pułapka: zatwierdzenie przez wdrażającego albo przez dział IT za właściciela ryzyka to w scenariuszach zawsze zła odpowiedź.

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

TYLKO ODCZYT

Ustalenie celów: mierzalne i z planem

Cele bezpieczeństwa informacji są spójne z polityką, mierzalne, jeśli to wykonalne, uwzględniają wymagania i wyniki oceny ryzyka, są monitorowane, komunikowane i aktualizowane. Do każdego planujemy: co zrobimy, jakie zasoby, kto, do kiedy i jak ocenimy wynik.

Pułapka: „poprawić bezpieczeństwo” nie jest celem. „Do 31 marca 2027 roku 95 procent pracowników po szkoleniu z phishingu” jest.

TYLKO ODCZYT

Planowanie zmian: 6.3

Zmiany w systemie zarządzania (zakres, role, procesy, narzędzia) robimy w sposób zaplanowany. To wymaganie dodane w 2022 roku.

Pułapka: 6.3 dotyczy zmian w ISMS. Zmiany w systemach IT nadzoruje zabezpieczenie o zarządzaniu zmianą (8.32) i działania operacyjne (8.1).

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

Z życia wzięte

Z ŻYCIA WZIĘTE

Poniedziałek, 9:05. Tomek kładzie przed panem Zbigniewem rejestr ryzyk z prośbą o podpis pod ryzykiem szczątkowym „ransomware na sql01”. Prezes pyta, czemu to on, skoro to sprawa informatyków. Tomek tłumaczy, że ryzyko dotyczy zamknięcia miesiąca i faktur, więc jego właścicielem jest pani Halina, a prezes zatwierdza tylko budżet na drugą kopię niezmienną. Pani Halina czyta, że po zmianach odtworzenie zajmie do czterech godzin, i podpisuje, ale dopisuje warunek: test odtwarzania przed każdym zamknięciem roku.

Jak to działa

Rozwiń: jak to działa pod spodem

Planowanie ma dwie części: projektową (zgoda, analiza luk, plan projektu) i systemową (kontekst, zakres, przywództwo, ryzyko, cele). Część projektowa kończy się wraz z wdrożeniem, systemowa zostaje na zawsze i jest powtarzana przy każdym przeglądzie.

A1: karta projektu i analiza luk

Pole karty	Zielona
Cel	certyfikat ISO/IEC 27001 przed terminem z ankiety sieci handlowej, czyli w ciągu 18 miesięcy
Sponsor	pan Zbigniew, prezes
Kierownik projektu	my, administrator; Tomek jako członek zespołu
Zespół	IT (dwie osoby), pani Halina, Marek, Ola, Kasia po kilka godzin w miesiącu
Budżet	do potwierdzenia przez prezesa po analizie luk
Ryzyka projektu	listopadowy zakaz zmian, mała liczba osób w IT, zamknięcie miesiąca

Analiza luk w Zielonej pokazuje typowy obraz firmy, która ma dobre praktyki techniczne bez systemu: zabezpieczenia technologiczne częściowo są (kopie z testami, Defender, MFA w poczcie), organizacyjne częściowo (zmiany w GLPI), a rozdziały 4, 5, 6 i 9 prawie w całości są do zrobienia.

A2: kontekst, strony zainteresowane i zakres

Strona zainteresowana	Wymaganie albo oczekiwanie	Spełniamy przez ISMS?
sieć handlowa, odbiorca B2B	certyfikat ISO/IEC 27001, zgłaszanie incydentów w 24 godziny	tak
klienci sklepu B2B	ochrona danych osobowych i handlowych	tak
pracownicy	jasne zasady, ochrona danych kadrowych	tak
organ ochrony danych osobowych	zgodność z RODO	tak, w części dotyczącej bezpieczeństwa
dostawca WMS	zdalny dostęp do `ora01` do serwisu	tak, przez zasady dostępu dostawców

Strona zainteresowana	Wymaganie albo oczekiwanie	Spełniamy przez ISMS?
właściciel budynku w Swarzędzu	dostęp do pomieszczeń technicznych	nie, poza zakresem; styk opisany

Czy Zielona jako hurtownia spożywcza podlega przepisom o krajowym systemie cyberbezpieczeństwa, omawia książka „ISO/IEC 27001: bezpieczeństwo informacji po ludzku”, która przyjmuje, że Zielona złożyła wniosek o wpis jako podmiot ważny: ISO/IEC 27001: od podręcznika Shella do certyfikatu Zielonej. W laboratorium wpisujemy organ nadzoru do tabeli jako stronę zainteresowaną, a ostateczną kwalifikację zostawiamy prawnikowi.

Przykładowy zakres w naszych słowach: „System zarządzania bezpieczeństwem informacji obejmuje projektowanie, utrzymanie i wsparcie usług IT Zielonej sp. z o.o. (infrastruktura serwerowa, sieć, poczta, księgowość, system magazynowy, sklep B2B, stacje robocze) świadczonych przez dział IT w Pamiątkowie i Swarzędzu, zgodnie z deklaracją stosowania w wersji 1.0”.

A3: polityka i role

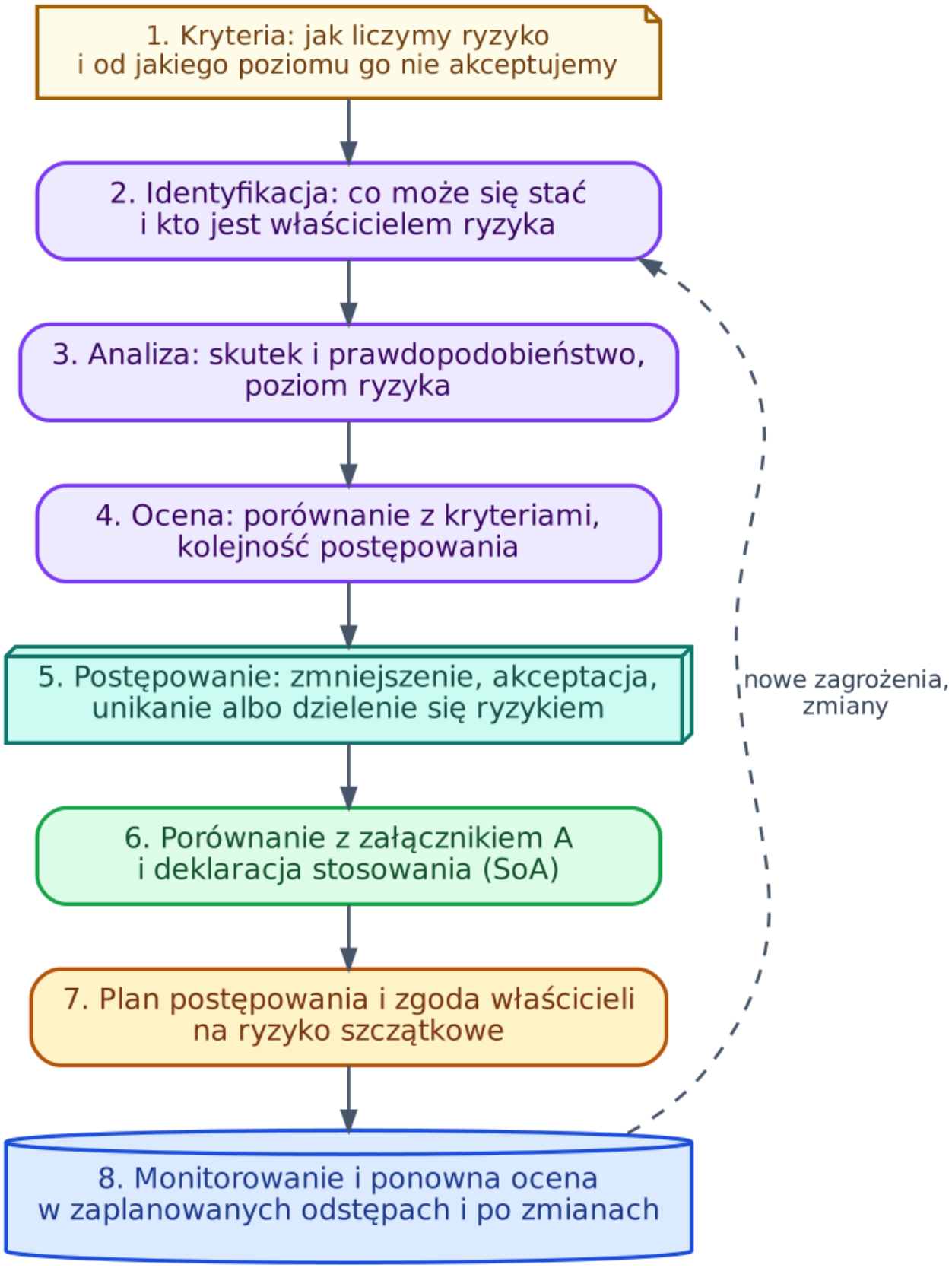
Polityka Zielonej mieści się na jednej stronie: po co chronimy informację, jakie są nasze zobowiązania, kto zatwierdza cele, gdzie są polityki tematyczne. Podpisuje ją pan Zbigniew. Role zapisujemy w macierzy RACI.

> **Pojęcie: macierz RACI.** Tabela, która dla każdego zadania mówi, kto wykonuje (Responsible), kto odpowiada i zatwierdza (Accountable), kogo pytamy o zdanie (Consulted) i kogo informujemy (Informed).

Zadanie	pan Zbigniew	my (IT)	Tomek	właściciel procesu
zatwierdzenie polityki	A	R	C	I
ocena ryzyka	I	A	R	C
akceptacja ryzyka szczątkowego	I	C	I	A
raport o wynikach ISMS dla kierownictwa	I	A	R	I

A4: metodyka i rejestr ryzyk

Proces oceny ryzyka i postępowania z nim pokazuje schemat. Norma wymaga, żeby był opisany i powtarzalny; ISO/IEC 27005:2022 daje do tego wytyczne.


1. Kryteria: jak liczymy ryzyko
i od jakiego poziomu go nie akceptujemy
2. Identyfikacja: co może się stać
i kto jest właścicielem ryzyka
3. Analiza: skutek i prawdopodobieństwo,
poziom ryzyka
4. Ocena: porównanie z kryteriami,
kolejność postępowania
5. Postępowanie: zmniejszenie, akceptacja,
unikanie albo dzielenie się ryzykiem
6. Porównanie z załącznikiem A
i deklaracja stosowania (SoA)
7. Plan postępowania i zgoda właścicieli
na ryzyko szczątkowe
8. Monitorowanie i ponowna ocena
w zaplanowanych odstępach i po zmianach
nowe zagrożenia,
zmiany

Rysunek 1. Proces zarządzania ryzykiem w ISMS: kryteria, identyfikacja, analiza, ocena, postępowanie, porównanie z załącznikiem A i SoA, zgoda właścicieli i monitorowanie (kliknięcie otwiera pełny rozmiar)

Nasza metodyka w ćwiczeniu: skutek i prawdopodobieństwo w skali 1 do 5, poziom to iloczyn. Poziom do 6 akceptujemy, od 8 do 12 obniżamy w ciągu roku, od 15 obniżamy natychmiast. To nasz wybór, nie wymóg normy.

Nr	Ryzyko (scenariusz)	Właściciel	S	P	Poziom	Decyzja
L-01	ransomware szyfruje `sql01` i kopie dostępne z sieci, księgowość stoi w zamknięciu miesiąca	pani Halina	5	3	15	zmniejszenie
L-02	wyciek danych klientów sklepu B2B przez podatność aplikacji	Kasia	4	3	12	zmniejszenie
L-03	konto byłego pracownika aktywne miesiącami	my	3	3	9	zmniejszenie
L-04	zgubiony laptop handlowca z danymi klientów	Kasia	3	3	9	zmniejszenie
L-05	przelew na fałszywe konto po wiadomości podszywające j się pod dostawcę	pani Halina	4	2	8	zmniejszenie
L-06	awaria łącza Swarzędza o 6:00, skanery bez WMS	Marek	3	2	6	akceptacja

Nr	Ryzyko (scenariusz)	Właściciel	S	P	Poziom	Decyzja
L-07	serwis dostawcy WMS przez zdalny dostęp bez MFA	Marek	4	3	12	zmniejszenie
L-08	pożar serwerowni w Pamiątkowie	my	5	1	5	akceptacja z kopią w Swarzędzu
L-09	wyciek danych odbiorców u firmy kurierskiej, której przekazujemy adresy wysyłek	Marek	3	2	6	dzielenie (umowa powierzenia i ubezpieczenie)
L-10	pomysł Oli na test sztucznej inteligencji na danych klientów w publicznej usłudze	Ola	4	3	12	unikanie (zakaz do czasu oceny)

A5: plan postępowania z ryzykiem

Ryzyko	Zabezpieczenia	Odpowiedzialny	Termin	Ryzyko szczątkowe
L-01	kopia niezmienna na `bkp02`, MFA dla kont administratorów, segmentacja sieci kopii, test odtwarzania co kwartał	my	31.03.2027	S 5, P 1, poziom 5, podpis pani Haliny
L-03	odbieranie dostępu w procesie odejścia w GLPI, przegląd kont co miesiąc	my i kadry	31.12.2026	S 3, P 1, poziom 3

Ryzyko	Zabezpieczenia	Odpowiedzialny	Termin	Ryzyko szczątkowe
L-07	dostęp dostawcy tylko przez VPN z MFA i na zgłoszenie, nagrywanie sesji	Marek	31.01.2027	S 4, P 1, poziom 4

A6: deklaracja stosowania i cele

Wycinek deklaracji. Numery zabezpieczeń według ISO/IEC 27001:2022 i 27002:2022, nazwy w naszym streszczeniu.

Nr	Zabezpieczenie (nasza nazwa)	Stosujemy	Uzasadnienie	Wdrożone
5.1	polityki bezpieczeństwa	tak	wymaganie 5.2, wszystkie ryzyka	częściowo
5.15	kontrola dostępu	tak	L-03, L-07	częściowo
5.19	bezpieczeństwo w relacjach z dostawcami	tak	L-07, L-09	nie
5.23	bezpieczeństwo usług chmurowych	tak	L-10, archiwum kopii w chmurze	nie
6.3	świadomość, edukacja, szkolenia	tak	L-05, L-10	nie
6.7	praca zdalna	tak	L-04	częściowo
7.2	fizyczne wejście	tak	L-08, ochrona serwerowni	tak
8.13	kopie zapasowe	tak	L-01, L-08	tak
8.28	bezpieczne programowanie	tak	aplikacje zespołu Oli	częściowo
8.30	prace rozwojowe zlecone na zewnątrz	nie	sklep B2B kupiony jako gotowy produkt, bez zleconych zmian; dostawcę obejmują 5.19 do 5.22	nie dotyczy

Cele na rok: (1) kopie niezmienne dla wszystkich serwerów w zakresie do 31 marca 2027 roku, (2) 95 procent pracowników po szkoleniu z phishingu do 31 marca 2027 roku, (3) konto zablokowane najpóźniej w dniu odejścia w 100 procentach przypadków, mierzone co miesiąc. Do każdego celu wpisujemy właściciela, zasoby i sposób oceny.

Częste błędy

Objaw	Przyczyna	Co robimy
Projekt zaczyna się od zakupu narzędzia do ryzyk	technika przed zarządzaniem	najpierw zgoda kierownictwa, kontekst i zakres
Zakres wycina serwerownię albo dostawcę, od którego zależy usługa	chęć skrócenia audytu	zakres może być wąski, ale styki i zależności opisujemy i kontrolujemy
Ryzyko szczątkowe podpisuje dział IT	mylenie wykonawcy z właścicielem	podpisuje właściciel ryzyka
SoA zrobiona z załącznika A, rejestr ryzyk później	odwrócona kolejność	ryzyko, postępowanie, potem SoA
Cele bez liczb i terminów	cel pomylony z hasłem	cel mierzalny, z właścicielem i planem oceny
Wyłączenie zabezpieczenia „bo jest drogie”	koszt jako uzasadnienie	wyłączenie z braku ryzyka albo braku zastosowania; drogie zabezpieczenie zastępujemy innym

□□ Ćwiczenia

1. Pan Zbigniew chce, żeby zakres objął całą firmę, łącznie z produkcją etykiet w wynajętej hali. Co zmienia to w artefaktach A2, A4 i A6?

Odpowiedź

W A2 dochodzą nowe procesy, lokalizacja i strony zainteresowane (właściciel hali, odbiorcy etykiet). W A4 trzeba zidentyfikować ryzyka dla informacji w nowych procesach, z nowymi właścicielami. W A6 część dotąd niepotrzebnych zabezpieczeń (na przykład fizyczne dla hali) staje się potrzebna. Wszystko trzeba przejść tym samym procesem, a nie dopisać do SoA.

1. Ola mówi, że w zakresie „nie ma sensu” ocena ryzyka dla papierowych dokumentów, bo „to nie IT”. Jak odpowiadamy?

Odpowiedź

Ocena ryzyka dotyczy informacji w zakresie w każdej postaci. Jeśli wydruki list płac są w zakresie, ich poufność jest objęta oceną. Zakres może wyłączyć procesy, ale nie rodzaj nośnika informacji w procesie, który jest w zakresie.

1. Ryzyko L-06 ma poziom 6 i jest akceptowane. Kto i kiedy może zmienić tę decyzję?

Odpowiedź

Właściciel ryzyka, Marek, przy kolejnej zaplanowanej ocenie ryzyka albo po zmianie, na przykład gdy magazyn przejdzie na trzy zmiany w listopadzie i skutek awarii łącza wzrośnie. Ocena ryzyka jest powtarzana w zaplanowanych odstępach i po istotnych zmianach (8.2).

1. Które z tych zdań jest celem bezpieczeństwa informacji w rozumieniu normy: „Chronimy dane klientów”, „Zero udanych ataków”, „Do 30 czerwca 2027 roku wszystkie konta zdalnego dostępu z MFA”?

Odpowiedź

Trzecie: jest spójne z polityką, mierzalne, ma termin i da się je monitorować. Pierwsze to zobowiązanie z polityki, drugie jest mierzalne, ale nierealne i nie wiadomo, kto i jak je realizuje.

Powiązane: Zasady, pojęcia i wymagania ISMS: domeny 1 i 2 egzaminu · Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany · Strategia kopii zapasowych Zielonej: RPO, RTO, reguła 3-2-1-1-0 i dwie lokalizacje

Źródła: [1] ISO/IEC 27001:2022 z Amd 1:2024, rozdziały 4 do 6 i 8.2, 8.3 (nasze streszczenie, bez cytatów); [2] ISO/IEC 27005:2022 (podejście od aktywów i od zdarzeń, opcje postępowania z ryzykiem; nasze streszczenie); [3] ISO/IEC 27002:2022 (numery i tematy zabezpieczeń); [4] PECB, Candidate Handbook ISO/IEC 27001 Lead Implementer, wersja 1.5, 2026 (domena 3, 18 pytań). Metodyka, skale i rejestr ryzyk są naszym ćwiczeniem. Dostęp 23 października 2026.