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

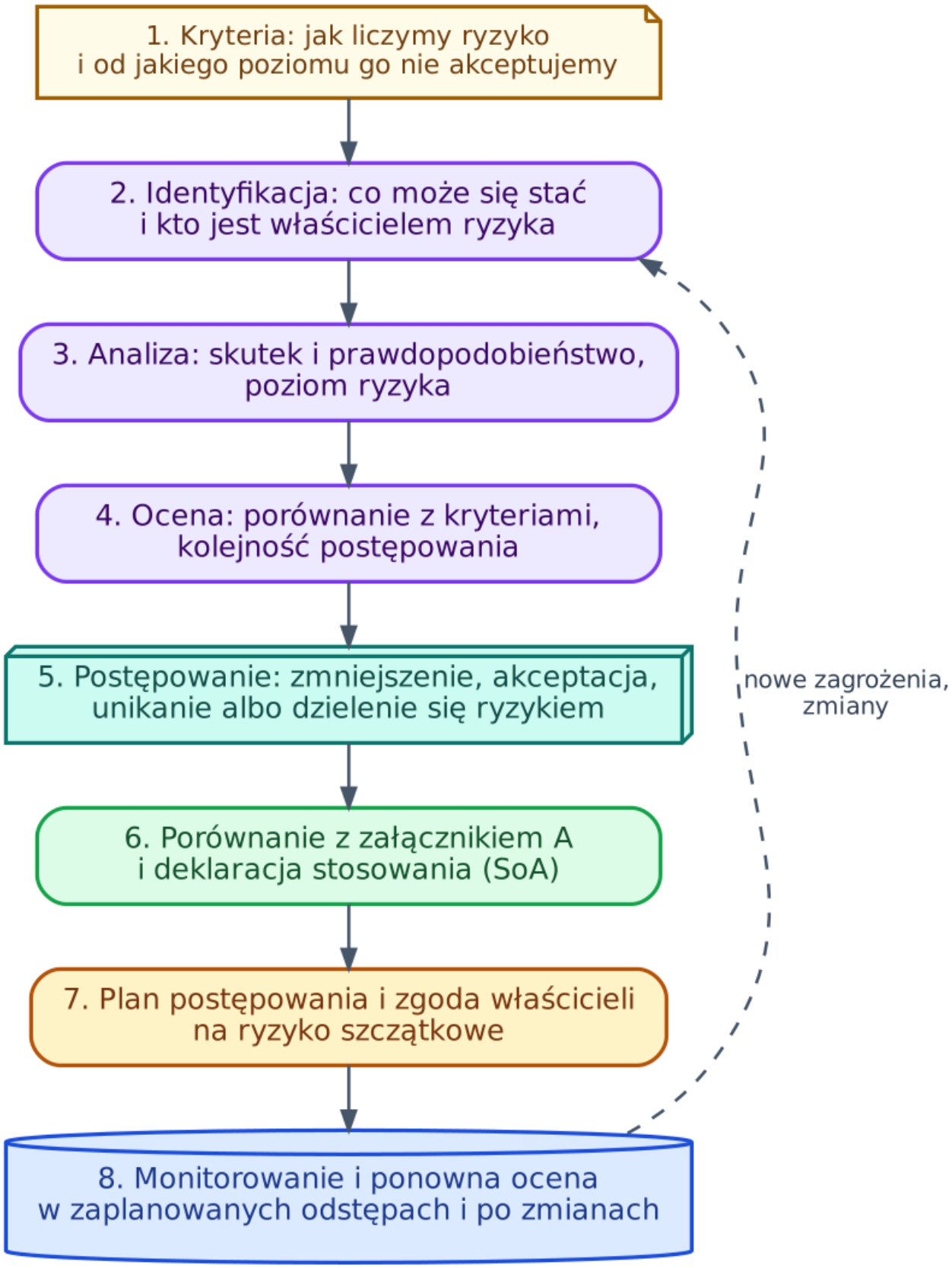
Polityka Zielonej mieści się na jednej stronie: po co chronimy informację, jakie są nasze zobowiązania, kto zatwierdza cele, gdzie są polityki tematyczne. Podpisuje ją pan Zbigniew. Role zapisujemy w macierzy RACI.

> **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.

Revision #3
Created 2026-10-23 17:13:59 UTC by Tomasz Konieczny
Updated 2026-10-26 14:28:07 UTC by Tomasz Konieczny