Wdrożenie, pomiar i audyt

Wdrożenie, monitorowanie, audyt wewnętrzny, doskonalenie i audyt certyfikacyjny.

- Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany
- Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania
- Ciągłe doskonalenie i audyt certyfikacyjny: od niezgodności do certyfikatu

Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany

Poziom: średnio

Dotyczy: PECB ISO/IEC 27001 Lead Implementer, domena 4 (14 pytań, 17,5%), ISO/IEC 27001:2022 rozdziały 7 i 8, ISO/IEC 27002:2022

Czas: ~70 min czytania, dni 12 do 15 planu, artefakty A7 i A8

Jak z deklaracji stosowania zrobić działający system: plan wdrożenia zabezpieczeń, dokumenty, które ktoś czyta, kompetencje i świadomość ludzi, komunikacja, zmiany, incydenty i dostawcy. Na egzaminie ta domena pyta zwykle o kolejność i o dowody: co zrobić najpierw i po czym poznać, że działa. Wracamy tu, gdy scenariusz mówi „polityka jest, ale nikt jej nie stosuje”.

Szczegóły poszczególnych zabezpieczeń, od kontroli dostępu po kopie zapasowe, opisuje po ludzku książka „ISO/IEC 27001: bezpieczeństwo informacji po ludzku”, między innymi na stronach Zabezpieczenia dla IT po ludzku: dostęp, tożsamość i konta uprzywilejowane i Zabezpieczenia dla IT po ludzku: systemy, sieć i dane, a w tej bazie leżą strony praktyczne, do których odsyłamy w tabelach. Ta strona patrzy na wdrożenie oczami kierownika projektu.

Skróty użyte na tej stronie (8)

Skrót	Co znaczy
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
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
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu

Skrót	Co znaczy
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
RACI	Responsible, Accountable, Consulted, Informed: tabela ról, która dla każdego zadania mówi, kto wykonuje, kto odpowiada i zatwierdza, kogo pytamy i kogo informujemy
WMS	Warehouse Management System: system zarządzania magazynem

Fiszka

Karty pojęć i pułapek domeny 4. Czytamy nagłówek, zakrywamy resztę, mówimy z pamięci.

□□ TYLKO ODCZYT

Opracowanie planu wdrożenia: zadania z SoA

Każde zabezpieczenie z deklaracji stosowania, które nie jest jeszcze wdrożone, dostaje zadanie, właściciela, termin, zasoby i dowód ukończenia. Kolejność wynika z poziomu ryzyka.

Pułapka: wdrażamy według ryzyka, nie według numeracji załącznika A ani według tego, co najłatwiejsze.

□□ **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

Projektowanie zabezpieczenia: cel, właściciel, dowód

Zanim zabezpieczenie powstanie, ustalamy, jaki ma cel, kto za nie odpowiada, jak działa w praktyce i jaki ślad zostawi. Zabezpieczenie bez śladu jest dla audytora niewidzialne.

Pułapka: „mamy to w głowie” nie jest dowodem. Dowodem jest zapis, log, protokół albo obserwacja.

□□ TYLKO ODCZYT

Tworzenie informacji udokumentowanej: opis, format, zatwierdzenie

Dokument ma identyfikację (tytuł, data, autor, numer), odpowiedni format i nośnik oraz jest przeglądany i zatwierdzany pod kątem przydatności. Zakres dokumentacji zależy od wielkości firmy, złożoności procesów i kompetencji ludzi.

Pułapka: norma nie wymaga papieru ani konkretnego systemu. Strona w BookStacku z historią wersji jest dokumentem.

□□ TYLKO ODCZYT

Nadzór nad informacją udokumentowaną: wersje i dostęp

Dokument jest dostępny tam, gdzie potrzebny, i chroniony przed utratą poufności, niewłaściwym użyciem i zmianą. Nadzorujemy dystrybucję, dostęp, przechowywanie, wersje, okres zatrzymania i usuwanie, także dla dokumentów z zewnątrz.

Pułapka: dokumenty zewnętrzne (umowy, normy, instrukcje dostawców) też podlegają nadzorowi, jeśli są potrzebne systemowi.

□□ TYLKO ODCZYT

Zapewnienie zasobów: ludzie, czas, pieniądze, narzędzia

Organizacja ustala i zapewnia zasoby potrzebne do ustanowienia, wdrożenia, utrzymania i doskonalenia systemu (7.1).

Pułapka: brak zasobów to częsta przyczyna źródłowa niezgodności, ale zasoby daje kierownictwo, nie wdrażający.

□□ TYLKO ODCZYT

Zapewnienie kompetencji: ustalić, zapewnić, ocenić, udokumentować

Ustalamy, jakich kompetencji wymagają role, zapewniamy je przez wykształcenie, szkolenie albo doświadczenie, a gdy trzeba, podejmujemy działania (szkolenie, mentoring, zmiana przydziału, zatrudnienie) i oceniamy ich skuteczność. Dowody kompetencji zachowujemy.

Pułapka: lista obecności ze szkolenia nie dowodzi kompetencji. Potrzebna jest ocena skuteczności, na przykład test albo obserwacja.

□□ TYLKO ODCZYT

Budowanie świadomości: trzy rzeczy, które każdy wie

Każdy, kto pracuje pod nadzorem organizacji, zna politykę bezpieczeństwa informacji, wie, jak przyczynia się do skuteczności systemu, i zna skutki niespełniania wymagań.

Pułapka: świadomość to nie to samo co kompetencja. Pani Halina nie musi umieć skonfigurować MFA, ale musi wiedzieć, dlaczego go używa i gdzie zgłosić podejrzany e-mail.

□□ **MFA** = Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu

□□ TYLKO ODCZYT

Planowanie komunikacji: co, kiedy, z kim, jak

Ustalamy potrzeby komunikacji wewnętrznej i zewnętrznej: o czym komunikujemy, kiedy, z kim i w jaki sposób.

Pułapka: komunikacja z klientami i organami po incydencie też należy do planu komunikacji, nie tylko biuletyn dla pracowników.

□□ TYLKO ODCZYT

Zarządzanie zmianą organizacyjną: ludzie po stronie projektu

Wdrożenie zmienia przyzwyczajenia: hasła, zgłoszenia, czyste biurko. Pomaga widoczny sponsor, wyjaśnienie „po co”, małe kroki, szkolenia przed wymaganiem i zbieranie opinii.

Pułapka: opór ludzi to normalna część wdrożenia. W scenariuszu najlepszą odpowiedzią jest zwykle komunikacja i zaangażowanie, a nie kara.

□□ TYLKO ODCZYT

Nadzór operacyjny: 8.1

Planujemy, wdrażamy i nadzorujemy procesy potrzebne systemowi, ustalamy dla nich kryteria, zachowujemy zapisy, nadzorujemy zmiany planowane i skutki nieplanowanych oraz procesy, produkty i usługi dostarczane z zewnątrz.

Pułapka: procesy zlecone na zewnątrz nadal są w naszym systemie. Outsourcing przenosi pracę, nie odpowiedzialność.

TYLKO ODCZYT

Zarządzanie zmianami: zabezpieczenie 8.32

Zmiany w systemach przetwarzania informacji przechodzą przez proces: wniosek, ocena ryzyka i wpływu, zatwierdzenie, test, wdrożenie, możliwość wycofania, zapis.

Pułapka: zmiana awaryjna też jest zmianą. Można ją zatwierdzić szybciej, ale po fakcie musi trafić do rejestru i przeglądu.

TYLKO ODCZYT

Zarządzanie incydentami: od zgłoszenia do wniosków

Zabezpieczenia 5.24 do 5.28 i 6.8: przygotowanie procesu i ról, zgłaszanie zdarzeń przez pracowników, ocena i decyzja, czy to incydent, reagowanie, wyciąganie wniosków i zabezpieczanie dowodów.

Pułapka: najpierw ograniczenie skutków i zabezpieczenie dowodów, potem naprawa. Reinstalacja zaatakowanego serwera przed zebraniem dowodów niszczy materiał do analizy.

TYLKO ODCZYT

Kontrola dostawców: umowa, wymagania, monitorowanie

Zabezpieczenia 5.19 do 5.22: wymagania bezpieczeństwa w umowach, łańcuch dostaw ICT, monitorowanie i przegląd usług dostawców, zarządzanie zmianami u nich.

Pułapka: certyfikat ISO/IEC 27001 dostawcy pomaga, ale trzeba sprawdzić, czy jego zakres obejmuje usługę, którą od niego kupujemy.

ICT = Information and Communication Technology: technologie informacyjne i komunikacyjne, czyli systemy, sieci i usługi IT razem z łącznością · **ISO** = International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie

TYLKO ODCZYT

Przekazanie do eksploatacji: koniec projektu, początek systemu

Gdy zabezpieczenia działają, a właściciele procesów przejęli odpowiedzialność, projekt się kończy. System działa dalej: pomiar, audyt i przegląd przejmują rolę kierownika projektu.

Pułapka: zamknięcie projektu nie jest zakończeniem wdrożenia ISMS. Certyfikacja wymaga dowodów działania przez pewien czas, zwykle kilku miesięcy (do potwierdzenia u jednostki certyfikującej).

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

Z życia wzięte

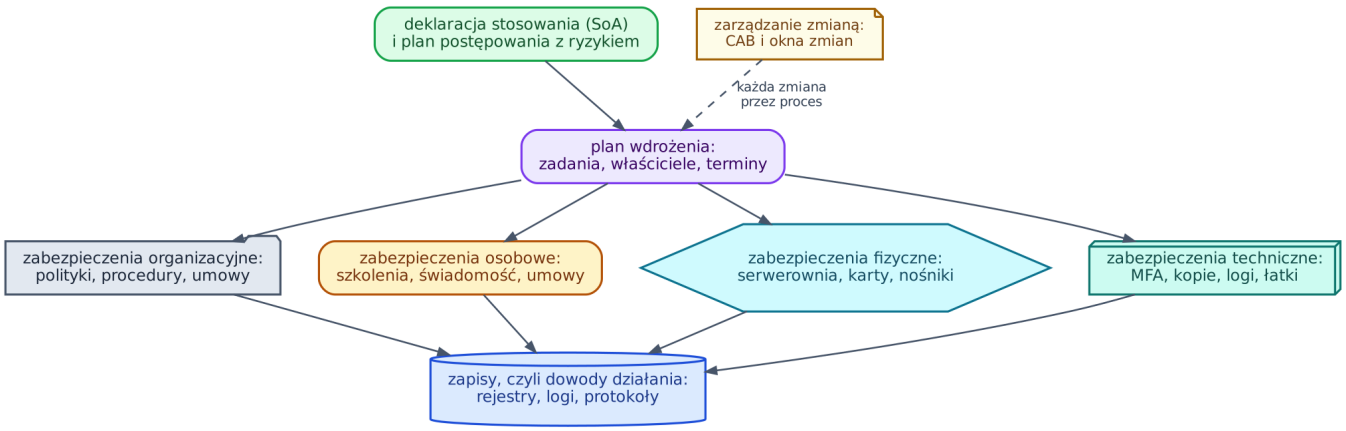
Z ŻYCIA WZIĘTE

Piątek, 16:00. Tomek wysyła wszystkim pracownikom nową politykę haseł jako załącznik do e-maila z prośbą o „zapoznanie się do poniedziałku”. W poniedziałek pani Halina dzwoni, że nie może się zalogować do Optimy, bo „ktoś zmienił hasła”, a Marek pyta, czy skanery w magazynie też muszą mieć dwanaście znaków. Okazuje się, że polityka weszła w życie bez planu wdrożenia, bez szkolenia i bez zmiany w GLPI. Tomek dopisuje do A8: najpierw komunikacja i szkolenie, potem termin, a zmiana ustawień przez proces zmian.

Jak to działa

Rozwiń: jak to działa pod spodem

Wdrożenie przekłada decyzje z planowania na cztery rodzaje zabezpieczeń i zostawia po każdym ślad. Zarządzanie zmianą pilnuje, żeby nic nie weszło na produkcję obok procesu.



Rysunek 1. Od deklaracji stosowania do działania: plan wdrożenia rozdziela zadania na zabezpieczenia organizacyjne, osobowe, fizyczne i techniczne, każde zostawia zapisy jako dowody, a zmiany przechodzą przez proces zmian (kliknięcie otwiera pełny rozmiar)

Plan wdrożenia w Zielonej

Zabezpieczenie	Zadanie	Właściciel	Dowód	Strona w bazie
8.13 kopie zapasowe	kopia niezmienna na `bkp02`, test odtwarzania co kwartał	my	protokół testu	Testy odtwarzania: plik, maszyna, baza i cała lokalizacja
5.15 kontrola dostępu	odbieranie dostępu w dniu odejścia	my i kadry	zgłoszenia w GLPI, raport kont	Wnioski o usługę, katalog usług i onboarding: od nowego konta do odebrania dostępu
8.32 zarządzanie zmianami	każda zmiana przez GLPI i CAB	my	rejestr zmian	Zmiany, organ zatwierdzający i okna zmian: jak zmieniamy, żeby nic nie zepsuć
5.24 do 5.28 incydenty	ścieżka incydentu bezpieczeństwa w GLPI	my	zgłoszenia i raporty po incydencie	Incydent i incydent poważny: od zgłoszenia do zamknięcia

Zabezpieczenie	Zadanie	Właściciel	Dowód	Strona w bazie
8.8 podatności	priorytety łatek z Defendera	my	raport miesięczny	Zarządzanie podatnościami i raporty: co łatać najpierw
7.2 fizyczne wejście	przegląd uprawnień kart co kwartał	my	raport z kontrolera	Kontrola dostępu: karty, PIN, biometria, kontrolery i audyt uprawnień
6.3 świadomość	szkolenie z phishingu i test	Tomek	wyniki testu	brak strony, plan w A8

A7: nadzór nad dokumentami

Procedura Zielonej w pięciu punktach: dokumenty ISMS leżą w jednej książce BookStacka z historią wersji, właściciel dokumentu przegląda go co najmniej raz w roku, zatwierdza go osoba wskazana w macierzy RACI, wersje wycofane są oznaczane i niedostępne z menu, a zapisy (protokoły, raporty) zatrzymujemy przez trzy lata, czyli cały cykl certyfikacji. Okres zatrzymania jest naszą decyzją; przepisy mogą wymagać dłuższego dla części zapisów.

> Zrzut do uzupełnienia: strona polityki bezpieczeństwa informacji w BookStacku Zielonej, otwarta zakładka „Wersje” z trzema wersjami, widoczny autor, data i komentarz „zatwierdzone przez prezesa”.

A8: kompetencje, świadomość i komunikacja

Rola	Kompetencje	Jak zapewniamy	Jak sprawdzamy skuteczność
kierownik ISMS (my)	ISO/IEC 27001, ryzyko, audyt	egzamin Lead Implementer, doświadczenie	certyfikat, wyniki audytu
audytor wewnętrzny	ISO 19011, niezależność	zewnętrzny audytor, pan Wojtek	raport z audytu, ocena jakości audytu

Rola	Kompetencje	Jak zapewniamy	Jak sprawdzamy skuteczność
administratorzy	zabezpieczenia techniczne	szkolenia, ten kurs	przegląd konfiguracji
wszyscy pracownicy	świadomość	szkolenie wprowadzające i coroczne	test phishingowy, quiz

Co komunikujemy	Kiedy	Z kim	Jak
polityka i zmiany zasad	przy zmianie, przed terminem wejścia	wszyscy pracownicy	spotkanie działu, strona w BookStacku
wyniki ISMS	co kwartał i przy przeglądzie	kierownictwo	raport
incydent dotyczący danych klientów	według umowy, na przykład w 24 godziny	sieć handlowa, organ nadzorczy, gdy wymagają przepisy	e-mail i telefon według procedury incydentu
wymagania bezpieczeństwa	przy umowie i zmianie	dostawcy	umowa, aneks

Częste błędy

Objaw	Przyczyna	Co robimy
Polityka obowiązuje, a ludzie jej nie znają	wysyłka e-mailem zamiast komunikacji	plan komunikacji, szkolenie, sprawdzenie świadomości
Szkolenie odbyte, zachowania bez zmian	brak oceny skuteczności	test, obserwacja, powtórka dla osób, które nie zdały
Kilka wersji tej samej procedury w obiegu	brak nadzoru nad dokumentami	jedno miejsce, wersje wycofane oznaczone
Zmiana awaryjna bez śladu	„nie było czasu na zgłoszenie”	rejestracja po fakcie i przegląd na najbliższym CAB
Dostawca ma certyfikat, a mimo to incydent u niego dotyka Zielonej	zakres certyfikatu dostawcy nie obejmował usługi	sprawdzamy zakres certyfikatu i wymagania w umowie
Serwer po ataku przeinstalowany od razu	naprawa przed zabezpieczeniem dowodów	ograniczenie skutków, kopia dowodów, analiza, dopiero potem odtworzenie

□□ Ćwiczenia

1. W Zielonej powstało dwadzieścia procedur, ale nikt ich nie czyta. Co jest najlepszym pierwszym krokiem kierownika ISMS?

Odpowiedź

Sprawdzić, które procedury są potrzebne (wymagane przez normę, ryzyko albo złożoność procesu), uprościć je i połączyć, a potem zaplanować komunikację i szkolenie dla ról, które z nich korzystają. Norma pozwala dopasować ilość dokumentacji do firmy, więc mniej, ale używane, to lepiej niż dużo martwych dokumentów.

1. Dostawca WMS zmienia sposób zdalnego dostępu bez uprzedzenia. Które wymagania i zabezpieczenia to dotyka?

Odpowiedź

Nadzór nad procesami zewnętrznymi i zmianami w 8.1, zabezpieczenia relacji z dostawcami i zarządzania zmianami w ich usługach (5.19 do 5.22), kontrola dostępu (5.15) i zarządzanie zmianami (8.32). Odpowiedzią jest wymaganie powiadamiania o zmianach w umowie i monitorowanie dostępu dostawcy.

1. Tomek pyta, czy lista obecności ze szkolenia z phishingu wystarczy jako dowód kompetencji. Co odpowiadamy?

Odpowiedź

Nie. Lista obecności dowodzi, że szkolenie się odbyło. Kompetencję albo świadomość pokazuje ocena skuteczności, na przykład wynik testu phishingowego po szkoleniu, a norma wymaga oceny skuteczności podjętych działań i zachowania dowodów kompetencji.

1. W piątek o 16:00 Defender zgłasza szyfrowanie plików na `fs01`. Ułóż w kolejności: odtworzenie z kopii, odłączenie serwera od sieci, zgłoszenie incydentu, zabezpieczenie dowodów, wnioski.

Odpowiedź

Zgłoszenie incydentu, odłączenie serwera od sieci (ograniczenie skutków), zabezpieczenie dowodów, odtworzenie z kopii, wnioski. Zgłoszenie i ograniczenie mogą iść równolegle; ważne, żeby dowody zabezpieczyć przed odtworzeniem.

Powiązane: Planowanie wdrożenia ISMS: kontekst, zakres, polityka, ryzyko i SoA · Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania · Alerty, incydenty i EDR: co robimy, gdy Defender coś znajdzie

Źródła: [1] ISO/IEC 27001:2022 z Amd 1:2024, rozdziały 7 i 8 (nasze streszczenie, bez cytatów); [2] ISO/IEC 27002:2022, zabezpieczenia 5.19 do 5.28, 6.3, 6.8, 8.8, 8.13, 8.32 (numery i nasze nazwy); [3] PECB, strona szkolenia ISO/IEC 27001 Lead Implementer (dzień 3: wdrożenie ISMS) i Candidate Handbook, wersja 1.5, 2026 (domena 4, 14 pytań). Dostęp 23 października 2026.

Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania

Poziom: średnio

Dotyczy: PECB ISO/IEC 27001 Lead Implementer, domena 5 (10 pytań, 12,5%), ISO/IEC 27001:2022 rozdział 9, ISO 19011:2026, ISO/IEC 27004

Czas: ~70 min czytania, dni 17 do 19 i 22 planu, artefakty A9 do A11

Skąd wiemy, że system działa: wskaźniki i ich ocena, audyt wewnętrzny prowadzony według ISO 19011 i przegląd, na którym kierownictwo podejmuje decyzje. Strona służy też jako dodatek dla przyszłego audytora: zasady audytu, dowody, ustalenia i zapis niezgodności. Wracamy tu, gdy scenariusz pyta „kto powinien audytować” albo „co musi trafić na przegląd”.

Rozdział 9 normy zamyka pętlę: bez niego system tylko się kręci, a nie poprawia. Na egzaminie Lead Implementer domena 5 ma 10 pytań, ale te same pojęcia wracają w domenach 6 i 7 oraz w scenariuszach, więc w praktyce warte są więcej.

Skróty użyte na tej stronie (9)

Skrót	Co znaczy
CQI	Chartered Quality Institute: brytyjska organizacja zawodowa specjalistów jakości, prowadzi rejestr audytorów IRCA
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
IRCA	International Register of Certificated Auditors: rejestr certyfikowanych audytorów systemów zarządzania prowadzony przez brytyjskie CQI, z kursami zatwierdzonymi u partnerów szkoleniowych
ISMS	Information Security Management System: system zarządzania bezpieczeństwem informacji, czyli polityka, role, ocena ryzyka, cele, pomiar, audyt i doskonalenie, które decydują o zabezpieczeniach i sprawdzają, czy działają
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy

Skrót	Co znaczy
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
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

Fiszka

Karty pojęć i pułapek domeny 5 i audytu. Czytamy nagłówek, zakrywamy resztę, mówimy z pamięci.

□□ TYLKO ODCZYT

Odróżnienie: monitorowanie, pomiar, analiza, ocena

Monitorowanie to ustalanie stanu (czy działa). Pomiar to ustalanie wartości (ile). Analiza to wyciąganie wniosków z danych, a ocena to porównanie wyniku z celem albo kryterium i decyzja, czy jest dobrze.

Pułapka: dashboard w Zabbiksie to monitorowanie. Wymaganie 9.1 jest spełnione dopiero wtedy, gdy ktoś wynik analizuje i ocenia.

□□ TYLKO ODCZYT

Ustalenie pomiaru: sześć pytań z 9.1

Co monitorujemy i mierzymy (procesy i zabezpieczenia), jakimi metodami, kiedy mierzymy, kto mierzy, kiedy analizujemy i oceniamy wyniki oraz kto to robi. Metody powinny dawać porównywalne i powtarzalne wyniki.

Pułapka: pomiar i ocena to dwie role. Osoba zbierająca dane nie musi być tą, która ocenia wynik.

□□ TYLKO ODCZYT

Dobór wskaźnika: skuteczność zabezpieczenia

Dobry wskaźnik ma cel, wzór, źródło danych, częstotliwość, próg i właściciela. ISO/IEC 27004 daje wytyczne i przykłady.

Pułapka: liczba zablokowanych ataków mówi o aktywności napastników, nie o skuteczności zabezpieczenia. Lepszy jest odsetek kont z MFA albo czas do łatki.

ISO = International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie · **MFA** = Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu

TYLKO ODCZYT

Zaplanowanie audytu wewnętrznego: co sprawdza

Audyt wewnętrzny w zaplanowanych odstępach sprawdza, czy system spełnia wymagania samej organizacji i normy oraz czy jest skutecznie wdrożony i utrzymywany.

Pułapka: audyt wewnętrzny musi objąć cały system w cyklu, ale nie musi wszystkiego co roku. Częstotliwość zależy od ważności procesów i wyników wcześniejszych audytów.

TYLKO ODCZYT

Ustanowienie programu audytów: cykl i priorytety

Program audytów określa częstotliwość, metody, odpowiedzialności, planowanie i raportowanie. Uwzględnia ważność procesów i wyniki poprzednich audytów. Dla każdego audytu ustalamy kryteria i zakres.

Pułapka: program to plan na wiele audytów (zwykle cykl certyfikacji), plan audytu to jeden audyt.

TYLKO ODCZYT

Zapewnienie niezależności: obiektywny audytor

Audytorów dobieramy tak, żeby audyt był obiektywny i bezstronny. Audytor nie sprawdza własnej pracy.

Pułapka: w małej firmie audytor wewnętrzny może być pracownikiem, byle nie audytował swojego obszaru. Można też zlecić audyt wewnętrzny osobie z zewnątrz.

TYLKO ODCZYT

Zapamiętanie zasad audytu: ISO 19011

Uczciwość, rzetelna prezentacja wyników, należyta staranność zawodowa, poufność, niezależność, podejście oparte na dowodach i podejście oparte na ryzyku. To siedem zasad z wydania 2018; czy wydanie 2026 zmieniło ich listę albo nazwy, sprawdzamy w normie (do potwierdzenia).

Pułapka: niezależność to zasada audytu, a obiektywizm i bezstronność to jej skutek. Pytania lubią zamieniać te słowa.

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

TYLKO ODCZYT

Odróżnienie: kryteria, dowód, ustalenie, wniosek

Kryteria audytu to wymagania, z którymi porównujemy (norma, polityka, umowa). Dowód z audytu to sprawdzalny zapis, stwierdzenie faktu albo inna informacja. Ustalenie to wynik porównania dowodu z kryteriami. Wniosek z audytu to podsumowanie po rozważeniu wszystkich ustaleń i celów audytu.

Pułapka: „audytor uważa, że” nie jest ustaleniem. Ustalenie zawsze ma dowód i kryterium.

TYLKO ODCZYT

Zbieranie dowodów: rozmowa, obserwacja, dokumenty, próbka

Dowody zbieramy, rozmawiając z ludźmi, obserwując pracę, przeglądając dokumenty i zapisy oraz sprawdzając próbki. Rozmowę potwierdzamy drugim źródłem, gdy to możliwe.

Pułapka: próbka nie daje pewności, tylko rozsądne zaufanie. Audyt zawsze niesie ryzyko, że czegoś nie zobaczymy.

TYLKO ODCZYT

Zapisanie niezgodności: trzy części

Dobrze zapisana niezgodność ma kryterium (które wymaganie), dowód (co widzieliśmy, gdzie, w jakiej próbce) i opis niespełnienia (czego brakuje). Nie zawiera rozwiązania.

Pułapka: audytor nie projektuje działań korygujących. To zadanie audytowanego.

□□ TYLKO ODCZYT

Odróżnienie: audyt pierwszej, drugiej i trzeciej strony

Pierwsza strona: audyt wewnętrzny, robiony przez organizację albo w jej imieniu. Druga: klient audytuje dostawcę, na przykład sieć handlowa Zieloną. Trzecia: niezależna jednostka certyfikująca.

Pułapka: zewnętrzna osoba wynajęta do audytu wewnętrznego nadal robi audyt pierwszej strony.

□□ TYLKO ODCZYT

Przeprowadzenie przeglądu zarządzania: wejścia

Najwyższe kierownictwo w zaplanowanych odstępach przegląda system. Wejścia: stan działań z poprzednich przeglądów, zmiany spraw wewnętrznych i zewnętrznych, zmiany potrzeb stron zainteresowanych, wyniki (niezgodności i działania korygujące, pomiary, audyty, realizacja celów), informacje zwrotne stron, wyniki oceny ryzyka i stan planu postępowania, szanse doskonalenia.

Pułapka: przegląd zarządzania nie jest spotkaniem IT. Bez najwyższego kierownictwa wymaganie nie jest spełnione.

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

□□ TYLKO ODCZYT

Zapisanie wyjść przeglądu: decyzje

Wyjściem są decyzje o szansach doskonalenia i o potrzebie zmian w systemie. Wyniki przeglądu zachowujemy jako dowód.

Pułapka: protokół, w którym są tylko prezentacje, a nie ma decyzji, to słaby dowód. Audytor zapyta, co postanowiono.

Z życia wzięte

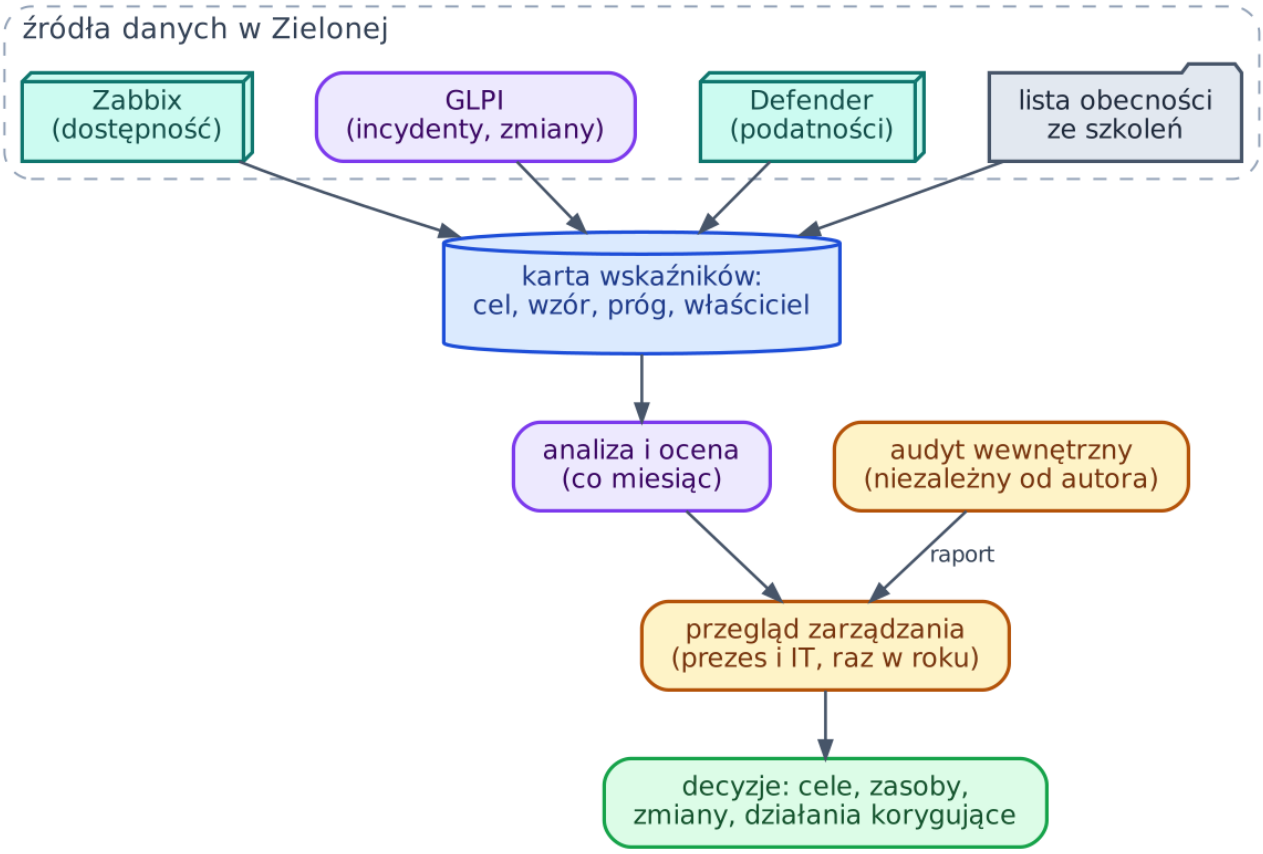
Z ŻYCIA WZIĘTE

Środa, 11:30. Tomek pokazuje panu Wojtkowi plan audytu wewnętrznego: on sam ma sprawdzić proces odbierania dostępu, który przez ostatni miesiąc sam prowadził w GLPI. Pan Wojtek uśmiecha się i pyta, czy Tomek wystawi sobie niezgodność. Zamieniają się: pan Wojtek audytuje odbieranie dostępu, a Tomek, z planem i listą pytań od pana Wojtka, sprawdza nadzór nad dokumentami, którego nie dotykał.

Jak to działa

Rozwiń: jak to działa pod spodem

Pomiar daje liczby, audyt daje niezależne spojrzenie, a przegląd zarządzania zamienia jedno i drugie w decyzje. Bez decyzji kierownictwa pętla doskonalenia się nie zamyka.



Rysunek 1. Monitorowanie i przegląd w Zielonej: Zabbix, GLPI, Defender i listy szkoleń zasilają kartę wskaźników, wyniki i raport z audytu trafiają na przegląd zarządzania, który kończy się decyzjami (kliknięcie otwiera pełny rozmiar)

A9: karta wskaźników

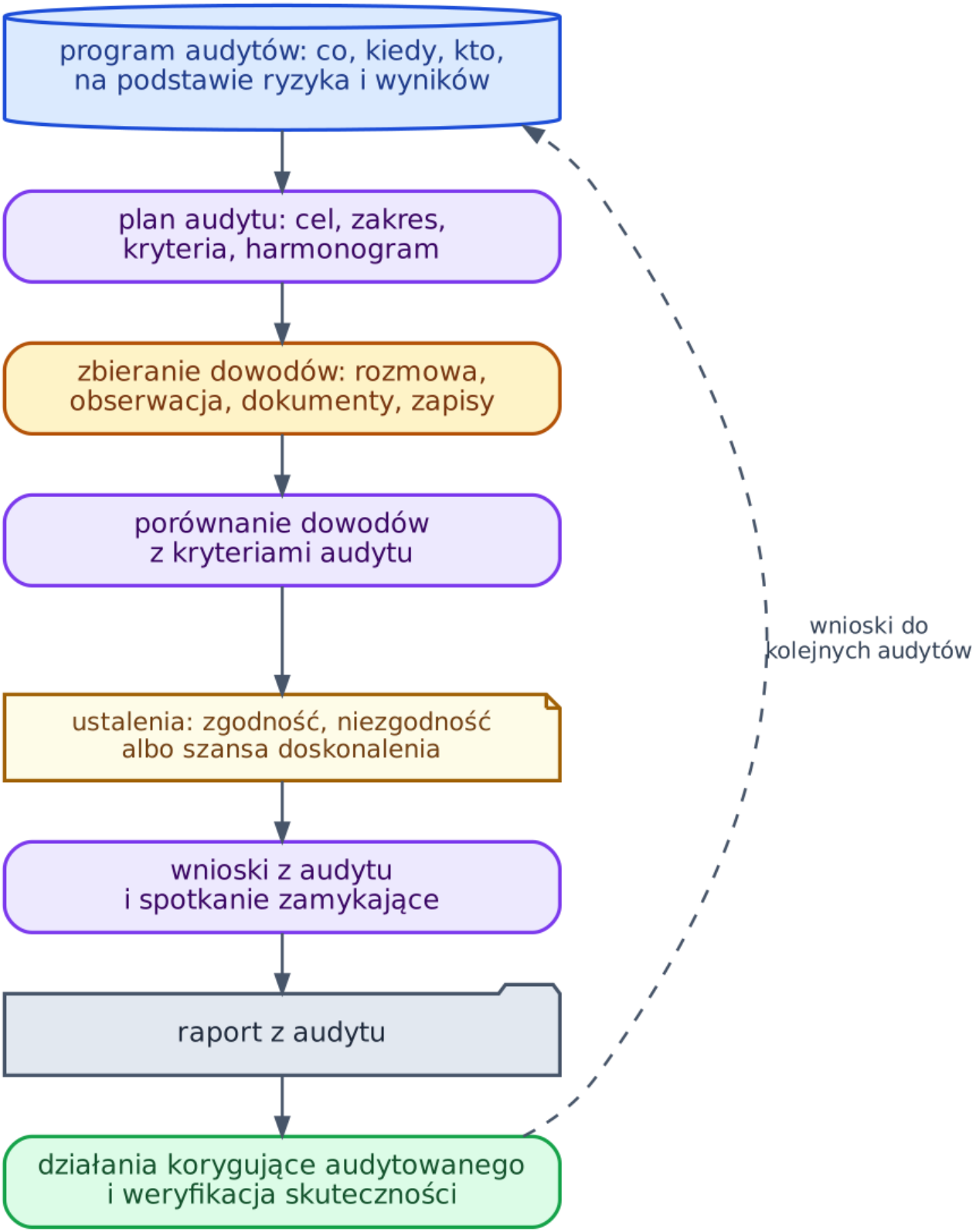
Nr	Wskaźnik	Wzór	Źródło	Częstotliwość	Próg	Właściciel
W1	serwery z kopią niezmienną i udanym testem odtwarzania w kwartale	serwery z testem / serwery w zakresie	protokoły testów	kwartał	100% do 31.03.2027	my
W2	pracownicy po szkoleniu z phishingu z wynikiem testu co najmniej 80%	zdani / zatrudnieni	wyniki testu	kwartał	95% do 31.03.2027	Tomek
W3	konta zablokowane w dniu odejścia	zablokowane w dniu odejścia / odejścia	GLPI i raport kont AD	miesiąc	100%	my
W4	czas od publikacji krytycznej podatności do łatki	mediana dni	Defender	miesiąc	do 14 dni	my
W5	zmiany wdrożone bez zatwierdzenia	liczba	rejestr zmian w GLPI	miesiąc	0	my

Wyniki analizujemy co miesiąc, a oceniamy na przeglądzie zarządzania. Gdy wskaźnik spada poniżej progu dwa razy z rzędu, otwieramy zgłoszenie w rejestrze niezgodności i szans doskonalenia.

Audyt wewnętrzny według ISO 19011

> **Pojęcie: ISO 19011.** Wytyczne audytowania systemów zarządzania: zasady audytu, zarządzanie programem, przeprowadzanie audytu i kompetencje audytorów. Czwarte

wydanie ukazało się w maju 2026 roku jako zmiana ewolucyjna, z szerszymi wytycznymi o audytach zdalnych i narzędziach cyfrowych [2]. Wytyczne dla audytu ISMS uzupełnia ISO/IEC 27007.



Rysunek 2. Audyt według ISO 19011: program, plan, dowody, porównanie z kryteriami, ustalenia, wnioski i spotkanie zamykające, raport, działania korygujące audytowanego i wnioski

do kolejnych audytów (kliknięcie otwiera pełny rozmiar)

A10: program i plan audytu wewnętrznego

Rok	Co audytujemy	Dlaczego
2027, przed certyfikacją	wszystkie rozdziały 4 do 10 i zabezpieczenia z ryzyk powyżej 12	pierwszy pełny audyt jest warunkiem etapu 2
2028	dostawcy, incydenty, praca zdalna, procesy z niezgodnościami z 2027	wyniki poprzedniego audytu i zmiany
2029	pozostałe zabezpieczenia, pełny przegląd rozdziałów 4 do 10 przed recertyfikacją	zamknięcie cyklu

Plan jednego audytu: cel (sprawdzić skuteczność odbierania dostępu i kopii zapasowych), zakres (procesy w Pamiątkowie i Swarzędzu, okres od lipca do września), kryteria (ISO/IEC 27001:2022, SoA w wersji 1.0, procedura odbierania dostępu), audytorzy (pan Wojtek dla dostępu, Tomek dla kopii zapasowych, bo kopiami zajmujemy się my), harmonogram (spotkanie otwierające 9:00, rozmowy do 14:00, spotkanie zamykające 15:00).

Przykład zapisu niezgodności, który Tomek ćwiczy w dniu 22:

Część	Treść
Kryterium	procedura odbierania dostępu (wersja 1.2) i zabezpieczenie 5.18 z deklaracji stosowania: dostęp odbieramy w dniu odejścia
Dowód	próbka dziesięciu odejść z trzeciego kwartału w GLPI i raport kont AD z dnia audytu: konta `piotr.zielinski` i `anna.kowal` aktywne 12 i 30 dni po odejściu
Opis	dostęp nie został odebrany w dniu odejścia w dwóch z dziesięciu sprawdzonych przypadków

A11: przegląd zarządzania

Przegląd Zielonej odbywa się raz w roku i dodatkowo po incydencie poważnym. Uczestnicy: pan Zbigniew (przewodniczy), my, Tomek, pani Halina, Marek. Protokół ma dwie części: tabelę wszystkich wejść z rozdziału 9.3 z krótkim stanem i listę decyzji z właścicielem i terminem.

Decyzja (przykład)	Właściciel	Termin

budżet na drugą kopię niezmienną w Swarzędzu	pan Zbigniew	31.01.2027
zmiana celu W2 z 95 na 90 procent dla magazynu, z dodatkowym szkoleniem na zmianach	Marek	30.06.2027
dopisanie wymagania powiadamiania o zmianach do umowy z dostawcą WMS	Marek	31.03.2027

Częste błędy

Objaw	Przyczyna	Co robimy
Dużo wykresów, żadnych decyzji	monitorowanie bez oceny	do każdego wskaźnika próg, właściciel i ocena na przeglądzie
Audytor sprawdza własny proces	mała firma, wygoda	zamiana obszarów albo audytor z zewnątrz
Audyt wewnętrzny tydzień przed certyfikacją, bez czasu na działania	zła kolejność	audyt i przegląd z wyprzedzeniem, czas na działania korygujące
Przegląd zarządzania bez prezesa	„to sprawa IT”	przegląd prowadzi najwyższe kierownictwo
Niezgodność zapisana jako „brak procedury” bez dowodu	opinia zamiast ustalenia	kryterium, dowód, opis niespełnienia
Raport z audytu podaje gotowe rozwiązania	audytor w roli doradcy	rozwiązania należą do audytowanego

□□ Ćwiczenia

1. Marek proponuje wskaźnik „liczba incydentów bezpieczeństwa w magazynie”. Czy to dobry wskaźnik skuteczności zabezpieczeń? Co proponujemy?

Odpowiedź

Sam w sobie słaby: mała liczba może znaczyć dobre zabezpieczenia albo brak zgłaszania. Lepiej łączyć go z miarami zabezpieczeń, na przykład odsetkiem terminali z aktualnym systemem, odsetkiem pracowników po szkoleniu i czasem od zgłoszenia do reakcji. Liczbę incydentów zostawiamy jako tło do analizy.

1. Czy pan Wojtek, zewnętrzny audytor wynajęty przez Zieloną, prowadzi audyt pierwszej czy trzeciej strony?

Odpowiedź

Pierwszej. Audyt wewnętrzny jest robiony przez organizację albo w jej imieniu, a pan Wojtek działa na zlecenie Zielonej. Audyt trzeciej strony robi jednostka certyfikująca.

1. Na przeglądzie zarządzania pan Zbigniew mówi: „Wszystko zielone, zamykamy”. Czego brakuje w protokole, żeby spełniał wymaganie 9.3?

Odpowiedź

Omówienia wszystkich wejść, w tym zmian w kontekście i potrzebach stron, wyników oceny ryzyka i stanu działań z poprzedniego przeglądu, oraz wyjść: decyzji o szansach doskonalenia i potrzebie zmian. Decyzja „bez zmian” też jest decyzją, ale musi wynikać z omówionych wejść i być zapisana.

1. W próbce pięciu zmian z GLPI audytor znajduje jedną zmianę bez zatwierdzenia. Zapisz niezgodność w trzech częściach.

Odpowiedź

Kryterium: zabezpieczenie 8.32 z deklaracji stosowania i procedura zmian Zielonej (zmiana wymaga zatwierdzenia przed wdrożeniem). Dowód: w próbce pięciu zmian z września zmiana konfiguracji zapory na `fw01` została wdrożona bez wpisu zatwierdzenia. Opis: jedna z pięciu sprawdzonych zmian nie została zatwierdzona przed wdrożeniem.

Powiązane: Wdrożenie ISMS: zabezpieczenia, dokumenty, ludzie, komunikacja i zmiany · Ciągłe doskonalenie i audyt certyfikacyjny: od niezgodności do certyfikatu · Audyt fizyczny serwerowni i biura: lista kontrolna i własny czytnik kart

Źródła: [1] ISO/IEC 27001:2022 z Amd 1:2024, rozdział 9 (nasze streszczenie, bez cytatów); [2] CQI i IRCA, „ISO 19011:2026 revision: guidance for management system auditing” (czwarte wydanie, maj 2026, zmiany ewolucyjne, audyty zdalne); [3] ISO 19011:2018 (siedem zasad audytu, pojęcia kryteriów, dowodów, ustaleń i wniosków; nasza parafraza); [4] ISO/IEC 27004 i ISO/IEC 27007 (wytyczne pomiaru i audytu ISMS; wydania do potwierdzenia); [5] PECB, Candidate Handbook ISO/IEC 27001 Lead Implementer, wersja 1.5, 2026 (domena 5, 10 pytań) i Candidate Handbook ISO/IEC 27001 Lead Auditor, wersja 1.5, 2026 (domeny audytu). Dostęp 23 października 2026.

Ciągłe doskonalenie i audyt certyfikacyjny: od niezgodności do certyfikatu

Poziom: średnio

Dotyczy: PECB ISO/IEC 27001 Lead Implementer, domena 6 (6 pytań, 7,5%) i domena 7 (5 pytań, 6,25%), ISO/IEC 27001:2022 rozdział 10, ISO/IEC 17021-1, ISO/IEC 27006-1:2024

Czas: ~60 min czytania, dni 20 do 22 planu, artefakty A12 i A13

Co robimy z niezgodnością, żeby nie wróciła, jak system ma się poprawiać sam z siebie i jak wygląda droga od wniosku do jednostki certyfikującej do certyfikatu na trzy lata. Druga część strony to dodatek dla audytora: jak pracuje jednostka certyfikująca według ISO/IEC 17021-1. Wracamy tu przed każdym audytem zewnętrznym i przy pytaniach o „dużą" i „małą" niezgodność.

Domeny 6 i 7 dają razem tylko 11 pytań, ale opierają się na kilku jasnych regułach, więc są najtańszymi punktami na egzaminie. W Zielonej to też najbliższa przyszłość: po audycie wewnętrznym i przeglądzie zarządzania z poprzedniej strony przychodzi kolej na jednostkę certyfikującą.

Skróty użyte na tej stronie (8)

Skrót	Co znaczy
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
PCA	Polskie Centrum Akredytacji: krajowa jednostka akredytująca, która sprawdza, czy jednostki certyfikujące w Polsce działają kompetentnie i bezstronnie
PCBC	Polskie Centrum Badań i Certyfikacji: polska jednostka certyfikująca wyroby i systemy zarządzania, w tym ISO/IEC 27001

Skrót	Co znaczy
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

Fiszka

Karty pojęć i pułapek domen 6 i 7. Czytamy nagłówek, zakrywamy resztę, mówimy z pamięci.

TYLKO ODCZYT

Odróżnienie: korekcja i działanie korygujące

Korekcja usuwa skutek wykrytej niezgodności (blokujemy zapomniane konto). Działanie korygujące usuwa przyczynę, żeby niezgodność nie wróciła (kadry zgłaszają odejście automatycznie z systemu kadrowego).

Pułapka: samo „naprawiliśmy” to korekcja. Audytor zapyta o przyczynę i o to, czy podobne niezgodności nie występują gdzie indziej.

TYLKO ODCZYT

Postępowanie z niezgodnością: 10.2 krok po kroku

Reagujemy (nadzorujemy i korygujemy, radzimy sobie ze skutkami), oceniamy potrzebę działania (przegląd, przyczyna, czy podobne występują albo mogą wystąpić), wdrażamy działania, sprawdzamy ich skuteczność, w razie potrzeby zmieniamy system. Zachowujemy zapis niezgodności, działań i wyników.

Pułapka: działania mają być adekwatne do skutków niezgodności. Jedno zapomniane konto nie wymaga nowego systemu kadrowego.

TYLKO ODCZYT

Analiza przyczyn: pięć razy dlaczego

Pytamy „dlaczego” tak długo, aż dojdziemy do przyczyny, na którą możemy wpłynąć, zwykle w procesie, a nie w człowieku. Pomagają też diagram Ishikawy i oś czasu zdarzeń.

Pułapka: „błąd ludzki” rzadko jest przyczyną źródłową. Pytamy dalej: dlaczego człowiek mógł się pomylić.

TYLKO ODCZYT

Zapamiętanie wymagania: ciągłe doskonalenie

Organizacja stale doskonali przydatność, adekwatność i skuteczność systemu (10.1). Źródła: wyniki pomiaru, audyty, przegląd zarządzania, incydenty, pomysły ludzi.

Pułapka: doskonalenie nie musi być skokowe. Małe, stałe poprawki też się liczą.

TYLKO ODCZYT

Odróżnienie: działanie zapobiegawcze i podejście oparte na ryzyku

Wydania normy od 2013 roku nie mają osobnego wymagania o działaniach zapobiegawczych. Zapobieganie realizuje planowanie z 6.1: ocena ryzyka i szans.

Pułapka: odpowiedź „uruchamiamy procedurę działań zapobiegawczych” pochodzi z wydania 2005.

TYLKO ODCZYT

Wybór jednostki certyfikującej: akredytacja i zakres

Wybieramy jednostkę akredytowaną do certyfikacji ISO/IEC 27001 (w Polsce akredytuje PCA), sprawdzamy zakres jej akredytacji, doświadczenie w naszej branży, terminy i koszty. Czas audytu jednostka liczy według ISO/IEC 27006-1, głównie od liczby osób w zakresie.

Pułapka: jednostka certyfikująca nie może nam doradzać przy wdrożeniu systemu, który potem certyfikuje. To zasada bezstronności.

ISO = International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie · **PCA** = Polskie Centrum Akredytacji: krajowa jednostka akredytująca, która sprawdza, czy jednostki certyfikujące w Polsce działają kompetentnie i bezstronnie

TYLKO ODCZYT

Przygotowanie do etapu 1: dokumenty i gotowość

Etap 1 sprawdza dokumenty (zakres, polityka, ocena ryzyka, SoA, cele), zrozumienie wymagań, gotowość do etapu 2, wyniki audytu wewnętrznego i przeglądu zarządzania. Często odbywa się częściowo zdalnie.

Pułapka: brak audytu wewnętrznego albo przeglądu zarządzania przed etapem 1 zwykle oznacza, że system nie jest gotowy do etapu 2.

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

TYLKO ODCZYT

Przygotowanie do etapu 2: skuteczność w praktyce

Etap 2 sprawdza, czy system jest wdrożony i skuteczny: rozmowy z ludźmi, obserwacja pracy, próbki zapisów, sprawdzenie zabezpieczeń z SoA.

Pułapka: na etapie 2 audytor pyta zwykłych pracowników, nie tylko IT. Pani Halina musi wiedzieć, gdzie zgłosić incydent.

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

TYLKO ODCZYT

Odróżnienie: niezgodność duża i mała

Niezgodność duża wpływa na zdolność systemu do osiągania zamierzonych wyników, na przykład brak przeglądu zarządzania albo kilka niezgodności z tym samym wymaganiem pokazujących awarię procesu. Niezgodność mała go nie podważa, na przykład jedno nieaktualne pole w rejestrze.

Pułapka: przy niezgodności dużej certyfikat nie zostanie wydany, dopóki jednostka nie sprawdzi korekcji i działań korygujących.

TYLKO ODCZYT

Zapamiętanie pojęcia: szansa doskonalenia

Ustalenie, które nie jest niezgodnością, ale wskazuje miejsce, gdzie można zrobić lepiej. Organizacja decyduje, czy z niego skorzysta.

Pułapka: szansa doskonalenia nie wymaga działania korygującego. Dobrze jednak odnotować decyzję.

□□ TYLKO ODCZYT

Decyzja o certyfikacji: kto ją podejmuje

Decyzję podejmuje jednostka certyfikująca przez osobę albo komisję, która nie brała udziału w audycie, na podstawie raportu i rekomendacji zespołu audytowego.

Pułapka: audytor wiodący nie wydaje certyfikatu. Rekomenduje.

□□ TYLKO ODCZYT

Utrzymanie certyfikatu: nadzór i recertyfikacja

Certyfikat ważny jest trzy lata. W tym czasie audyty nadzoru odbywają się co najmniej raz w roku, a pierwszy w ciągu 12 miesięcy od decyzji o certyfikacji. W trzecim roku, przed wygaśnięciem, recertyfikacja.

Pułapka: audyt nadzoru nie sprawdza całego systemu, ale co roku obejmuje między innymi audyt wewnętrzny, przegląd zarządzania, działania po niezgodnościach i skargi.

□□ TYLKO ODCZYT

Odpowiedź na niezgodność z audytu: plan w terminie

Po audycie przedstawiamy korekcję, analizę przyczyn i działania korygujące w terminie podanym przez jednostkę. Przy niezgodnościach dużych jednostka weryfikuje wdrożenie, czasem dodatkową wizytą.

Pułapka: spór z audytorem rozwiązujemy przez procedurę odwołań jednostki, a nie przez przekonywanie w czasie audytu.

Z życia wzięte

Z ŻYCIA WZIĘTE

Czwartek, 14:45, spotkanie zamykające etapu 2. Audytorka jednostki certyfikującej odczytuje niezgodność małą: dwa konta byłych pracowników aktywne ponad tydzień. Tomek chce od razu tłumaczyć, że już je zablokował. Pan Zbigniew go powstrzymuje: „Zablokowanie to korekcja, a pani pyta, dlaczego to się w ogóle stało”. Do piątku Tomek ma w rejestrze przyczynę (kadry zgłaszały odejścia e-mailem, który czasem ginął) i działanie korygujące: zgłoszenie odejścia z systemu kadrowego tworzy automatycznie zadanie w GLPI.

Jak to działa

Rozwiń: jak to działa pod spodem

Doskonalenie w ISMS ma dwie drogi: reakcyjną (niezgodność, incydent, skarga) i planową (pomiar, audyt, przegląd, szanse). Obie kończą się zmianą w systemie, a jej skuteczność sprawdzamy w kolejnym cyklu.

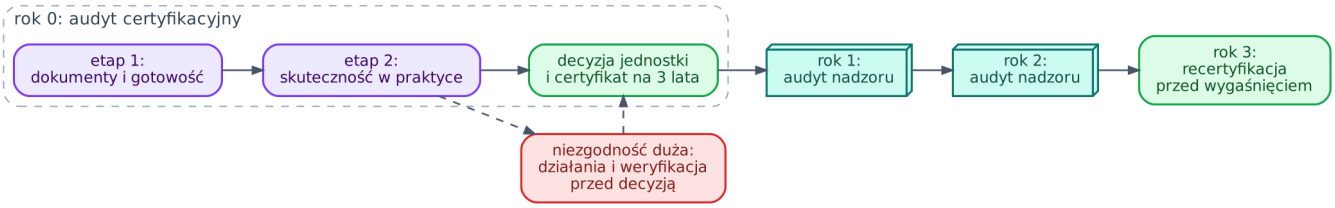
A12: rejestr niezgodności i działań korygujących

Nr	Źródło	Opis	Korekcja	Przyczyna	Działanie korygujące	Właściciel, termin	Skuteczność
N1	audyt wewnętrzny	2 z 10 kont aktywne po odejściu	blokada kont, przegląd wszystkich kont	odejścia zgłaszane e-mailem, bez potwierdzenia	zadanie w GLPI z systemu kadrowego, raport miesięczny	my, 31.01.2027	W3 przez trzy miesiące 100%
N2	audyt wewnętrzny	zmiana na `fw01` bez zatwierdzenia	zatwierdzenie po fakcie, przegląd zmian z kwartału	brak kategorii zmiany awaryjnej, presja czasu	kategoria zmiany awaryjnej z zatwierdzeniem telefonicznym i wpisem w 24 h	my, 15.12.2026	W5 równe 0 przez kwartał

Nr	Źródło	Opis	Korekcja	Przyczyna	Działanie korygujące	Właściciel, termin	Skuteczność
N3	przegląd wskaźników	brak oceny skuteczności szkoleń	test dla osób po szkoleniu	plan szkoleń bez etapu oceny	test po każdym szkoleniu w A8	Tomek, 28.02.2027	wyniki W2 w raporcie kwartalnym

Droga do certyfikatu

> **Pojęcie: akredytacja.** Potwierdzenie przez niezależną jednostkę akredytującą (w Polsce PCA, Polskie Centrum Akredytacji), że jednostka certyfikująca działa kompetentnie i bezstronnie według ISO/IEC 17021-1 i ISO/IEC 27006-1. Certyfikat od jednostki bez akredytacji formalnie istnieje, ale klienci, tacy jak sieć handlowa, zwykle go nie uznają.



Rysunek 1. Cykl certyfikacji: etap 1 i etap 2 w roku zero, decyzja jednostki i certyfikat na trzy lata, niezgodność duża wstrzymuje decyzję do weryfikacji działań, audyty nadzoru w latach pierwszym i drugim, recertyfikacja w trzecim (kliknięcie otwiera pełny rozmiar)

Według ISO/IEC 17021-1, jeśli jednostka nie może zweryfikować korekcji i działań korygujących niezgodności dużych w ciągu sześciu miesięcy od ostatniego dnia etapu 2, przed rekomendacją certyfikacji powtarza etap 2 (do potwierdzenia w aktualnym wydaniu i w regulaminie wybranej jednostki). Dokładne terminy odpowiedzi na niezgodności małe ustala jednostka.

A13: lista gotowości Zielonej

Etap	Sprawdzamy	Stan
przed wnioskiem	zakres i liczba osób w zakresie do wyceny, wybór akredytowanej jednostki	do zrobienia

Etap	Sprawdzamy	Stan
przed etapem 1	zakres, polityka, metodyka i wyniki oceny ryzyka, plan postępowania, SoA, cele, wyniki audytu wewnętrznego i przeglądu zarządzania	w teczce A2 do A11
przed etapem 2	zapisy z co najmniej kilku miesięcy działania, zamknięte albo zaplanowane działania z audytu wewnętrznego, pracownicy po szkoleniu	do zrobienia
logistyka	sala, harmonogram rozmów, przewodnik po serwerowni, dostęp do GLPI i BookStacka w trybie odczytu	do zrobienia
po audycie	odpowiedź na niezgodności w terminie, plan audytów nadzoru	po audycie

Dla audytora: ISO/IEC 17021-1 po ludzku

> **Pojęcie: ISO/IEC 17021-1.** Wymagania dla jednostek, które audytują i certyfikują systemy zarządzania. Obowiązuje wydanie z 2015 roku; jego aktualność sprawdzamy w katalogu ISO (do potwierdzenia). Dla ISMS dochodzą wymagania ISO/IEC 27006-1:2024, a dla samego audytu wytyczne ISO 19011 i ISO/IEC 27007.

Zasady, na których opiera się zaufanie do certyfikatu, w naszym streszczeniu:

Zasada	Co znaczy w praktyce
bezstronność	jednostka nie doradza przy wdrożeniu, audytor nie audytuje firmy, w której niedawno pracował albo doradzał
kompetencja	audytorzy znają normę, branżę i technikę w zakresie
odpowiedzialność	za zgodność systemu odpowiada organizacja, a jednostka za ocenę opartą na wystarczających dowodach
otwartość	informacja o certyfikacie jest dostępna, kto pyta, może sprawdzić jego zakres i ważność
poufność	jednostka chroni informacje, które zobaczyła w czasie audytu

Zasada	Co znaczy w praktyce
reagowanie na skargi	skargi na certyfikowaną firmę i na samą jednostkę mają procedurę
podejście oparte na ryzyku	jednostka uwzględnia ryzyko błędnej oceny przy planowaniu audytu

Raport z audytu certyfikacyjnego zawiera między innymi cel, zakres i kryteria audytu, ustalenia z dowodami, niezgodności, wnioski i rekomendację dla osoby podejmującej decyzję. Audytor wiodący odpowiada za raport, a decyzja należy do jednostki.

Częste błędy

Objaw	Przyczyna	Co robimy
Ta sama niezgodność na każdym audycie	korekcja bez działania korygującego	analiza przyczyn i ocena skuteczności działań
Przyczyna: „błąd pracownika”	analiza zatrzymana za wcześnie	pięć razy dlaczego, szukamy przyczyny w procesie
Jednostka certyfikująca proponuje „pakiet wdrożenie plus certyfikat”	naruszenie bezstronności	wybieramy inną jednostkę albo innego doradcę
Etap 2 kończy się niezgodnością dużą „brak przeglądu zarządzania”	przegląd odłożony na po audycie	przegląd i audyt wewnętrzny przed etapem 1
Kłótnia z audytorem o ustalenie	brak wiedzy o procedurze odwołań	wyjaśniamy dowody na spotkaniu, a spór przez odwołanie
Certyfikat od jednostki bez akredytacji	najtańsza oferta	sprawdzamy akredytację i jej zakres przed podpisaniem umowy

□□ Ćwiczenia

1. Na etapie 2 audytor stwierdza, że Zielona nie przeprowadziła w ogóle audytu wewnętrznego, bo „audyt certyfikacyjny i tak wszystko sprawdzi”. Jaka to niezgodność i co dalej?

Odpowiedź

Niezgodność duża: brak całego procesu z rozdziału 9.2 podważa zdolność systemu do oceny i doskonalenia. Certyfikat nie zostanie wydany, dopóki Zielona nie przeprowadzi audytu

wewnętrznego, nie przeanalizuje przyczyny i nie przedstawi działań, a jednostka ich nie zweryfikuje.

1. Do której drogi doskonalenia należy pomysł Marka, żeby terminale magazynowe blokowały się po pięciu minutach bezczynności, zgłoszony na spotkaniu działu?

Odpowiedź

Do drogi planowej: to szansa doskonalenia, a nie reakcja na niezgodność. Rejestrujemy ją, oceniamy wpływ na ryzyko i pracę zmiany o 6:00 i decydujemy, czy wdrażamy, przez proces zmian.

1. Doradca, który pomagał Zielonej pisać politykę, pracuje od niedawna jako audytor w jednostce certyfikującej i zostaje wyznaczony do audytu Zielonej. Co z tym robimy?

Odpowiedź

Zgłaszamy jednostce konflikt. Według zasady bezstronności z ISO/IEC 17021-1 osoba, która niedawno doradzała organizacji, nie powinna jej audytować; jednostka ma obowiązek zarządzać takim zagrożeniem bezstronności i wyznaczyć innego audytora.

1. Pan Zbigniew pyta, ile audytów zewnętrznych czeka Zieloną w pierwszym cyklu certyfikacji. Co odpowiadamy?

Odpowiedź

Audyt certyfikacyjny w dwóch etapach, dwa audyty nadzoru (w pierwszym i drugim roku, pierwszy w ciągu 12 miesięcy od decyzji) i audyt recertyfikacyjny przed wygaśnięciem certyfikatu w trzecim roku. Liczbę dni każdego audytu jednostka wylicza według ISO/IEC 27006-1.

Powiązane: Monitorowanie, pomiar, audyt wewnętrzny i przegląd zarządzania · Próbny egzamin Lead Implementer: 80 własnych pytań i strategia na dzień egzaminu · Problemy, analiza przyczyn i postmortem: żeby ta sama awaria nie wróciła

Źródła: [1] ISO/IEC 27001:2022 z Amd 1:2024, rozdział 10 (nasze streszczenie, bez cytatów); [2] ISO/IEC 17021-1:2015 (zasady, etapy audytu, niezgodności duże i małe, decyzja o certyfikacji, nadzór i recertyfikacja; nasza parafraza, aktualność wydania do potwierdzenia); [3] ISO/IEC 27006-1:2024 (wymagania dla jednostek certyfikujących ISMS, czas audytu); [4] PECB, strona szkolenia ISO/IEC 27001 Lead Implementer (dzień 4: monitorowanie, doskonalenie i przygotowanie do audytu certyfikacyjnego) i Candidate Handbook, wersja 1.5, 2026 (domeny 6 i 7); [5] PCBC, komunikat z 5

marca 2024 (przejście certyfikatów na wydanie 2022 do 31 października 2025). Dostęp 23 października 2026.