# ISO/IEC 27001:2022 + Amd 1:2024 Systemy zarządzania bezpieczeństwem informacji (SZBI)

Bezpieczeństwo informacji, SZBI, certyfikowalny na całym świecie

181 wymagań. Ta norma może zostać certyfikowana przez akredytowaną jednostkę. Stan na 07/2026.

Norma ISO/IEC 27001 określa wymagania dotyczące systemu zarządzania bezpieczeństwem informacji: opartego na ryzyku, udokumentowanego i o wykazanej skuteczności. Ocena zgodności z nią to akredytowany audyt certyfikacyjny przeprowadzany w dwóch etapach (przegląd dokumentacji, a następnie przegląd skuteczności na miejscu), po którym następują coroczne audyty nadzoru oraz recertyfikacja po trzech latach.

| Firma | Data | Opracował |
|---|---|---|
| | | |

## 4 Kontekst organizacji 8

**4.1-1 Określa się i utrzymuje w aktualności zewnętrzne i wewnętrzne czynniki, które wpływają na zdolność organizacji do osiągnięcia zamierzonych wyników SZBI.**

Jak to wykazać: Wykazywane poprzez analizę kontekstu, prowadzoną jako odrębny dokument lub jako część księgi SZBI: otoczenie rynkowe, sytuacja klientów i umów, ramy prawne (RODO, NIS2), stos technologiczny, liczba zatrudnionych, zależność od dostawców chmurowych. Dla małych organizacji wystarczy jednostronicowa tabela z datą i cyklem przeglądu, o ile przegląd zarządzania pokazuje, że jest ona faktycznie aktualizowana.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**4.1-2 Organizacja określiła, czy zmiana klimatu jest dla niej istotnym zagadnieniem. Ustalenie jest uzasadnione, niezależnie od tego, czy odpowiedź brzmi tak, czy nie.**

Jak to wykazać: Wymaganie to wprowadziła Amd 1:2024 i audytorzy pytają o nie wprost. Prowadź osobny wiersz w analizie kontekstu: okresy upałów wpływające na serwerownie i dostępność, ekstremalne zjawiska pogodowe wpływające na centra danych dostawców chmurowych, stabilność sieci elektroenergetycznej. Uzasadniony wynik nieistotne jest akceptowalny, brak wpisu nie jest.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**4.2-1 Określa się strony zainteresowane istotne dla SZBI.**

Jak to wykazać: Lista interesariuszy obejmująca klientów, personel, podmioty przetwarzające i podprzetwarzające, organy nadzorcze, ubezpieczycieli, jednostkę certyfikującą i udziałowców. W małych organizacjach wystarczy tabela z kolumnami: strona, oczekiwanie i źródło oczekiwania.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**4.2-2 Określa się istotne wymagania tych stron zainteresowanych, w tym wszelkie wymagania związane ze zmianą klimatu.**

Jak to wykazać: Dla każdej strony wskaż konkretne źródło: klauzula umowna, umowa powierzenia przetwarzania danych, ankieta klienta, obowiązek prawny. Amd 1:2024 dodaje uwagę, że strony zainteresowane mogą mieć wymagania związane ze zmianą klimatu. Nie jest to odrębne wymaganie musi, ale audytorzy podnoszą tę kwestię regularnie, na przykład pytania o zrównoważony rozwój w audycie dostawców u dużego klienta. Wystarczy jeden wiersz w tabeli interesariuszy z wynikiem, w tym informacją brak wymagań tego rodzaju.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**4.2-3 Decyduje się i pozostaje możliwe do prześledzenia, które z tych wymagań są realizowane przez SZBI.**

Jak to wykazać: Dodaj do tabeli interesariuszy kolumnę wskazującą regułę, która realizuje dane wymaganie (politykę, zabezpieczenie, załącznik umowny). Pokazuje to, że wymagania nie zostały jedynie zebrane, lecz rzeczywiście przetworzone.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**4.3-1** **Określa się zakres SZBI z uwzględnieniem zagadnień z punktu 4.1, wymagań z punktu 4.2 oraz interfejsów i zależności z działaniami realizowanymi przez strony trzecie.**

Jak to wykazać: Zakres wymienia lokalizacje, jednostki organizacyjne, produkty, systemy i granice sieci. Elementy zlecone na zewnątrz (hosting, dostawcy płatności, wsparcie) opisuje się jako interfejsy z jasno określoną granicą odpowiedzialności. Sztucznie zawężony zakres wycinający procesy kluczowe zostaje odrzucony przez jednostki certyfikujące.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**4.3-2** **Zakres jest dostępny jako informacja udokumentowana i jednoznacznie określa granice SZBI.** Dokument

Jak to wykazać: Zatwierdzony dokument zakresu z wersją, datą i podpisem najwyższego kierownictwa. Jego dokładne brzmienie pojawi się później na certyfikacie, dlatego należy sformułować go precyzyjnie i tak, by dało się go cytować publicznie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**4.4-1** **SZBI, w tym niezbędne procesy i ich wzajemne oddziaływania, jest ustanawiany, wdrażany, utrzymywany i stale doskonalony.**

Jak to wykazać: Mapa procesów lub lista procesów wiążąca zarządzanie ryzykiem, obsługę incydentów, zarządzanie zmianą, audyty i przegląd zarządzania z właścicielami i częstotliwością. Żywy dowód liczy się bardziej niż sam diagram: zgłoszenia, protokoły, wpisy w kalendarzu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

## 5 Przywództwo 8

**5.1-1** **Najwyższe kierownictwo bierze odpowiedzialność za skuteczność SZBI i zapewnia, że polityka oraz cele są ustanowione i spójne z kierunkiem strategicznym.**

Jak to wykazać: Dowody obejmują podpisane zatwierdzenia polityki, zakresu i Deklaracji Stosowania, protokoły przeglądu zarządzania oraz udokumentowane decyzje budżetowe. W bardzo małych organizacjach najwyższe kierownictwo jest często tą samą osobą co właściciel SZBI, co jest akceptowalne, ale musi być jawnie stwierdzone w opisie roli.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.1-2** **Wymagania SZBI są zintegrowane z procesami biznesowymi, a znaczenie skutecznego bezpieczeństwa informacji jest komunikowane.**

Jak to wykazać: Najlepiej widać to tam, gdzie bezpieczeństwo nie jest osobnym segregatorem: kryterium bezpieczeństwa w definicji ukończenia, sprawdzenie bezpieczeństwa w procesie sprzedaży lub zakupów, powtarzający się punkt dotyczący bezpieczeństwa w protokołach spotkań zespołu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.1-3** **Kierownictwo zapewnia niezbędne zasoby, wspiera osoby przyczyniające się do skuteczności SZBI i promuje ciągłe doskonalenie.**

Jak to wykazać: Zatwierdzony budżet na bezpieczeństwo, czas przeznaczony na szkolenia, zaangażowanie zewnętrznych audytorów lub testerów penetracyjnych. Rejestr usprawnień lub działań z wpisami rozłożonymi na kilka kwartałów świadczy o ciągłości, a nie jednorazowym wysiłku.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.2-1** **Ustanawia się politykę bezpieczeństwa informacji odpowiednią do celu organizacji, która stanowi ramy dla celów bezpieczeństwa informacji.** Dokument

Jak to wykazać: Krótki, zatwierdzony dokument polityki, dwie lub trzy strony wystarczą. Wymienia cele ochrony, zakres, odpowiedzialności oraz zasadę podejścia opartego na ryzyku. Ogólnikowy tekst szablonowy bez powiązania z realnym biznesem rzuca się w oczy podczas audytu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.2-2** **Polityka zawiera zobowiązanie do spełniania mających zastosowanie wymagań oraz zobowiązanie do ciągłego doskonalenia SZBI.** Dokument

Jak to wykazać: Oba zobowiązania muszą wystąpić w polityce jako wyraźne zdania i są odczytywane dosłownie podczas audytu etapu 1. Dodatkowo odnieś się do procesów bazowych (rejestr prawny, rejestr usprawnień).

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.2-3** **Polityka jest komunikowana wewnątrz organizacji i udostępniana stronom zainteresowanym w odpowiednim zakresie.** Dokument

Jak to wykazać: Dowód poprzez wpis w intranecie lub na wiki z obowiązkiem zapoznania się, listę kontrolną wdrożenia z potwierdzeniem lub opublikowane streszczenie na stronie internetowej. Lista dystrybucyjna z potwierdzeniami odbioru to najprostszy solidny dowód.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.3-1** **Odpowiedzialności i uprawnienia dla ról istotnych z punktu widzenia bezpieczeństwa są przypisane i komunikowane wewnątrz organizacji.**

Jak to wykazać: Macierz ról (RACI) obejmująca właściciela SZBI, właścicieli ryzyk, właścicieli aktywów, koordynatora incydentów oraz osobę kontaktową ds. ochrony danych. W zespołach jednoosobowych lub bardzo małych przypisz każdą rolę do wskazanej osoby i jawnie udokumentuj wynikającą z tego kumulację ról, zamiast ją ukrywać.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**5.3-2** **Uprawnienie do zapewnienia zgodności SZBI z normą oraz do raportowania wyników SZBI najwyższemu kierownictwu przypisuje się do konkretnej roli.**

Jak to wykazać: Pismo powołujące lub opis roli właściciela SZBI z jawną ścieżką raportowania do kierownictwa. Ścieżka raportowania musi być rzeczywiście udokumentowana w protokołach przeglądu zarządzania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

## 6 Planowanie 21

**6.1.1-1** **Wychodząc od zagadnień z punktu 4.1 i wymagań z punktu 4.2, określa się ryzyka i szanse, którymi trzeba się zająć, tak aby SZBI osiągnął zamierzone wyniki i zapobiegł niepożądanym skutkom.**

Jak to wykazać: Rejestr wiążący zagadnienia kontekstu z ryzykami i szansami, prowadzony osobno lub w ramach rejestru ryzyka. Liczy się identyfikowalność: każde zagadnienie z analizy kontekstu w widoczny sposób prowadzi do oceny albo do uzasadnionej decyzji o jego nieuwzględnianiu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.1.1-2** **Planuje się działania odnoszące się do tych ryzyk i szans, integruje się je z procesami SZBI oraz ocenia ich skuteczność.**

Jak to wykazać: Plan działań z właścicielem, terminem i kryterium skuteczności. Prowadź ocenę skuteczności jako osobną kolumnę, w przeciwnym razie audytowi zabraknie dowodu, że działanie nie tylko wdrożono, lecz także zweryfikowano.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.1.2-1** **Definiuje się i stosuje proces oceny ryzyka bezpieczeństwa informacji; obejmuje on kryteria akceptacji ryzyka i kryteria przeprowadzania ocen ryzyka.** Dokument

Jak to wykazać: Polityka zarządzania ryzykiem ze skalami prawdopodobieństwa i skutku, zdefiniowana macierz ryzyka oraz jasny próg akceptacji. Próg musi być liczbą lub strefą, a nie sformułowaniem w rodzaju według naszego uznania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.1.2-2** **Proces zapewnia, że powtarzane oceny ryzyka dają spójne, ważne i porównywalne wyniki.**

Jak to wykazać: Wykazywane poprzez stałą metodykę z określonymi skalami oraz porównanie dwóch wersji oceny: te same ryzyka, ta sama logika oceny, wyjaśnialne różnice. Datowana wersja zeszłorocznego rejestru ryzyka jest tu najmocniejszym dowodem.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.2-3** **Identyfikuje się ryzyka bezpieczeństwa informacji w celu wykrycia utraty poufności, integralności i dostępności w ramach zakresu, a do każdego ryzyka przypisuje się właściciela ryzyka.**

Jak to wykazać: Rejestr ryzyka odwołujący się do aktywów lub procesów, trzech celów ochrony oraz wskazanego właściciela ryzyka. Właściciel ryzyka musi mieć uprawnienia do jego akceptacji; w małych organizacjach jest to zwykle osoba zarządzająca.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.2-4** **Zidentyfikowane ryzyka są analizowane: określa się potencjalne skutki, realistyczne prawdopodobieństwo oraz wynikający z nich poziom ryzyka.**

Jak to wykazać: Kolumny na skutek, prawdopodobieństwo i wynikowy poziom ryzyka, każda z krótkim uzasadnieniem. Jedno zdanie uzasadnienia na ryzyko zapobiega najczęstszemu ustaleniu audytowemu, czyli liczbom bez wyprowadzenia.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.2-5** **Ryzyka porównuje się z kryteriami akceptacji i priorytetyzuje do postępowania z nimi.**

Jak to wykazać: Rejestr ryzyka musi pokazywać, które ryzyka przekraczają próg akceptacji i w jakiej kolejności będą traktowane. Wystarczy posortowany widok lub kolumna priorytetu.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.2-6** **Proces oceny ryzyka jest dostępny jako informacja udokumentowana.** Dokument

Jak to wykazać: Sama metodyka jest dokumentem obowiązkowym, nie tylko jej wynik. Zatwierdzona polityka z wersją i datą zatwierdzenia, powiązana z indeksem dokumentów SZBI.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-1** **Dla każdego ryzyka przekraczającego próg akceptacji wybiera się odpowiednią opcję postępowania (ograniczenie, unikanie, przeniesienie lub akceptacja).**

Jak to wykazać: Kolumna opcji postępowania w rejestrze ryzyka. Gdy ryzyko jest akceptowane, zapisz uzasadnienie i formalne zatwierdzenie przez właściciela ryzyka; gdy jest przenoszone, wskaż umowę lub polisę ubezpieczeniową.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-2** **Określa się wszystkie zabezpieczenia niezbędne do wdrożenia wybranych opcji postępowania z ryzykiem.**

Jak to wykazać: Formułuj zabezpieczenia konkretnie i w sposób weryfikowalny, z właścicielem i terminem. Odwołanie się do prac technicznych już trwających (wdrożenie MFA, test kopii zapasowych) jest w porządku, o ile wskazuje na zgłoszenie lub artefakt konfiguracyjny.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-3** **Określone zabezpieczenia porównuje się z zabezpieczeniami z załącznika A, aby zweryfikować, że żadne niezbędne zabezpieczenie nie zostało pominięte.**

Jak to wykazać: Porównanie jest odrębnym, identyfikowalnym krokiem, a nie produktem ubocznym. Dowodzi tego kolumna mapowania w rejestrze ryzyka odwołująca się do numerów załącznika A wraz z datowanym protokołem porównania.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-4** **Istnieje Deklaracja Stosowania (SoA). Ocenia ona indywidualnie wszystkie 93 zabezpieczenia załącznika A, wskazuje stosowalność wraz z uzasadnieniem dla każdego zabezpieczenia, stan wdrożenia oraz uzasadnienie każdego wyłączenia.** Dokument

Jak to wykazać: Deklaracja Stosowania jest centralnym dokumentem obowiązkowym i mapą całego audytu. Musi być kompletna: zabezpieczenia niestosowane również figurują wraz z uzasadnieniem, nigdy jako puste wiersze. Zalecane kolumny: numer zabezpieczenia, tytuł, stosowalne tak lub nie, uzasadnienie, stan wdrożenia, odniesienie do polityki lub dowodu, powiązanie z ryzykiem. Wersja i zatwierdzenie kierownictwa są obowiązkowe, ponieważ Deklaracja Stosowania jest konfrontowana z rzeczywistością przy każdym audycie nadzoru.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-5** **Sporządza się plan postępowania z ryzykiem, który łączy zabezpieczenia, odpowiedzialności, terminy i wymagane zasoby.** Dokument

Jak to wykazać: Może to być zakładka w arkuszu ryzyka lub tablica projektowa. Liczy się to, aby terminy były realistyczne i aby niedotrzymane terminy były widocznie przeplanowane, bo dokładnie to sprawdza audytor.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-6** **Plan postępowania z ryzykiem jest zatwierdzany przez właścicieli ryzyk, a pozostałe ryzyka szczątkowe są przez nich formalnie akceptowane.** Dokument

Jak to wykazać: Podpis, zatwierdzenie elektroniczne lub datowana decyzja w protokole. Wystarczy jedna linia w protokole przeglądu zarządzania odwołująca się do wersji rejestru, o ile wersja jest jednoznaczna.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.1.3-7** **Proces postępowania z ryzykiem jest dostępny jako informacja udokumentowana.** Dokument

Jak to wykazać: Zwykle ujęty w tym samym dokumencie polityki co ocena ryzyka. Trzeba opisać przepływ od oceny, przez wybór opcji, po akceptację ryzyka szczątkowego.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.2-1** **Ustanawia się cele bezpieczeństwa informacji dla odpowiednich funkcji i poziomów, spójne z polityką i mierzalne, o ile jest to możliwe.**

Jak to wykazać: Arkusz celów z trzema do sześciu celami, każdy z miernikiem, wartością bazową, wartością docelową i terminem. Przykład: udział systemów z MFA podniesiony z 80 do 100 procent do końca kwartału. Cele bez liczby nie liczą się jako mierzalne.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.2-2** **Cele uwzględniają mające zastosowanie wymagania bezpieczeństwa informacji, a także wyniki oceny i postępowania z ryzykiem.**

Jak to wykazać: Dodaj do arkusza celów kolumnę pochodzenia: z jakiego ryzyka, jakiego wymagania klienta lub jakiego obowiązku prawnego wynika cel. Zapobiega to celom, które wyglądają na dowolne.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.2-3** **Cele są monitorowane, komunikowane i aktualizowane w razie potrzeby.**

Jak to wykazać: Kwartalne śledzenie postępów w arkuszu celów wraz z komunikacją do zespołu, na przykład krótka notatka na wiki lub punkt porządku obrad na spotkaniu zespołu. Historyczne wersje pokazują, że aktualizacje faktycznie się odbywają.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**6.2-4** **Cele bezpieczeństwa informacji są dostępne jako informacja udokumentowana.** Dokument

Jak to wykazać: Wystarczy zatwierdzony dokument celów z datą. Może być częścią przeglądu zarządzania, ale musi tam istnieć jako własna, dająca się odnaleźć sekcja.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.2-5** **Dla każdego celu planuje się, co zostanie zrobione, jakie zasoby są potrzebne, kto jest odpowiedzialny, kiedy zostanie ukończony i jak zostaną ocenione wyniki.**

Jak to wykazać: Te pięć elementów jest weryfikowalnych indywidualnie i pytanych o nie indywidualnie podczas audytu. Ustaw je jako pięć kolumn w arkuszu celów, wtedy zgodność widać na pierwszy rzut oka.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**6.3-1** **Jeśli organizacja stwierdzi, że zmiany w SZBI są potrzebne, przeprowadza się je w sposób zaplanowany.**

Jak to wykazać: Dowodzą tego wnioski o zmianę, protokoły lub zgłoszenia pokazujące przyczynę, ocenę wpływu, zatwierdzenie i wdrożenie. Typowe przyczyny w małych organizacjach: zmiana dostawcy chmury, nowe lokalizacje, pierwsze zatrudnienie.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

## 7 Wsparcie 15

**7.1-1** **Określa się i zapewnia zasoby niezbędne do ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia SZBI.**

Jak to wykazać: Pozycja budżetowa na bezpieczeństwo, licencje narzędzi (menedżer haseł, MDM, platforma logów), zaplanowane dniówki na utrzymanie SZBI oraz usługi audytu zewnętrznego. Faktura lub zatwierdzenie budżetu dowodzi tego szybciej niż jakikolwiek tekst.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.2-1** **Określa się niezbędne kompetencje osób, których praca wpływa na wyniki bezpieczeństwa informacji.**

Jak to wykazać: Macierz kompetencji lub profile ról wymieniające wiedzę wymaganą dla danej roli, na przykład bezpieczne wytwarzanie oprogramowania dla programistów, obsługa incydentów dla koordynatora. W bardzo małych zespołach wystarczy jeden wiersz na osobę.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.2-2** **Kompetencje zapewnia się na podstawie odpowiedniego wykształcenia, szkolenia lub doświadczenia.**

Jak to wykazać: Certyfikaty, potwierdzenia ukończenia kursów, życiorysy lub udokumentowane doświadczenie praktyczne. Samokształcenie jest akceptowalne, jeśli jest udokumentowane, na przykład zaświadczeniami o ukończeniu kursów online lub zaliczonymi wewnętrznymi testami wiedzy.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.2-3** **Tam, gdzie występują braki kompetencyjne, podjęto działania w celu ich usunięcia, a skuteczność tych działań została oceniona.**

Jak to wykazać: Plan szkoleń z porównaniem planu i wykonania oraz sprawdzeniem skuteczności, na przykład wynik testu, wskaźnik klikalności w symulacji phishingowej lub obserwacja w miejscu pracy. Sprawdzenie skuteczności jest często pomijane i stanowi klasyczne drobne ustalenie.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.2-4** **Dostępna jest odpowiednia informacja udokumentowana jako dowód kompetencji.** Dokument

Jak to wykazać: Teczka kompetencji lub szkoleń dla każdej osoby z dowodami i datami. W małych organizacjach wystarczy katalog przechowywanych plików PDF wraz z tabelą zbiorczą.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.3-1** **Osoby pracujące w ramach zakresu są świadome polityki bezpieczeństwa informacji.**

Jak to wykazać: Potwierdzenie przy wdrożeniu i po każdej zmianie polityki, z datą i wersją. Wystarczy funkcja potwierdzenia odczytu na wiki lub podpisana lista.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.3-2** **Osoby znają swój własny wkład w skuteczność SZBI oraz korzyści z poprawy wyników bezpieczeństwa informacji.**

Jak to wykazać: Materiały szkoleniowe i listy obecności, w których widoczny jest związek z własną pracą danej osoby. Audytorzy przeprowadzają wywiady bezpośrednio z personelem, dlatego warto szkolić na konkretnych, codziennych przykładach, a nie na abstrakcyjnych cytatach z normy.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.3-3** **Osoby znają konsekwencje niezgodności z wymaganiami SZBI.**

Jak to wykazać: Podaj konsekwencje w slajdach szkoleniowych i instrukcjach pracy oraz powiąż je z procesem z punktu A.6.4. Nawet organizacje bez pracowników muszą to uwzględnić dla współpracowników i freelancerów poprzez ich umowy.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.4-1** **Określa się komunikację wewnętrzną i zewnętrzną istotną dla SZBI: co jest komunikowane, kiedy, z kim i za pomocą jakich środków.**

Jak to wykazać: Macierz komunikacji z wierszami takimi jak incydent bezpieczeństwa do klientów, powiadomienie organu nadzorczego w ciągu 72 godzin, comiesięczny raport statusu dla kierownictwa. Jest podstawą komunikacji kryzysowej i jest przeglądana po każdym incydencie.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.5.1-1** **SZBI obejmuje informację udokumentowaną wymaganą przez normę, a także informację udokumentowaną, którą organizacja uznała za niezbędną dla skuteczności SZBI.** Dokument

Jak to wykazać: Indeks dokumentów wymieniający każdy dokument SZBI z celem, właścicielem, wersją i miejscem przechowywania. Pokazuje, że dokumenty obowiązkowe są kompletne, i jest najszybszym punktem wejścia dla audytora.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.5.2-1** **Przy tworzeniu i aktualizacji dokumentów zapewnia się odpowiednią identyfikację, format i nośnik, a dokumenty są przeglądane i zatwierdzane pod kątem przydatności.**

Jak to wykazać: Jednolity nagłówek dokumentu z tytułem, wersją, datą, autorem i osobą zatwierdzającą. W środowiskach opartych na Git przeglądy pull requestów z zatwierdzeniem spełniają wymóg przeglądu i zatwierdzenia, pod warunkiem że historia jest niezmienna.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.5.3-1** **Informacja udokumentowana jest dostępna i nadaje się do użycia tam i wtedy, gdy jest potrzebna.**

Jak to wykazać: Centralne miejsce przechowywania dostępne dla wszystkich uprawnionych osób, z funkcją wyszukiwania. Można to sprawdzić metodą próbkowania: każda dana instrukcja pracy musi być możliwa do odnalezienia w mniej niż minutę.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**7.5.3-2** **Informacja udokumentowana jest odpowiednio chroniona, w szczególności przed utratą poufności, niewłaściwym użyciem i utratą integralności.**

Jak to wykazać: Prawa dostępu do dokumentów SZBI oparte na rolach, wersjonowanie z historią, ochrona przed zapisem dla zatwierdzonych wersji oraz kopia zapasowa repozytorium dokumentów. Dowód kopii zapasowej to element najczęściej pomijany.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**7.5.3-3** **Reguluje się dystrybucję, dostęp, wyszukiwanie, przechowywanie, kontrolę zmian oraz retencję i likwidację informacji udokumentowanej.**

Jak to wykazać: Krótka zasada kontroli dokumentów z okresami retencji i regułami usuwania. Musi być uzgodniona z obowiązkami prawnymi (prawo handlowe, prawo podatkowe, RODO) i stanowi podstawę dla punktów A.5.33 i A.8.10.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**7.5.3-4** **Identyfikuje się i kontroluje informację udokumentowaną pochodzenia zewnętrznego niezbędną do planowania i eksploatacji SZBI.**

Jak to wykazać: Lista dokumentów zewnętrznych z wersją i źródłem: normy, akty prawne, przewodniki hartowania dostawców, dokumentacja bezpieczeństwa chmury, umowy powierzenia przetwarzania danych. Bez odniesienia do wersji nie można wykazać kontroli.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

## 8 Działania operacyjne 8

**8.1-1** **Planuje się, wdraża i kontroluje procesy niezbędne do spełnienia wymagań bezpieczeństwa informacji oraz do wdrożenia działań z punktu 6, a dla tych procesów ustanawia się kryteria.**

Jak to wykazać: Podręcznik operacyjny lub runbooki z jasnymi kryteriami, na przykład maksymalny czas wdrożenia krytycznych poprawek, kryteria wydania dla wdrożeń, progi alertów. Kryteria bez liczb są bezwartościowe podczas audytu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**8.1-2** **Dostępna jest informacja udokumentowana w zakresie niezbędnym, aby mieć pewność, że procesy zostały przeprowadzone zgodnie z planem.** Dokument

Jak to wykazać: Zapisy operacyjne jako dowód: historia zgłoszeń, przebiegi pipeline'u CI, raporty z poprawek, logi kopii zapasowych, przeglądy dostępu. Te zapisy są rzeczywistym dowodem skuteczności podczas audytu etapu 2.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**8.1-3** **Zaplanowane zmiany są kontrolowane, a skutki niezamierzonych zmian są przeglądane; w razie potrzeby łagodzi się niekorzystne skutki.**

Jak to wykazać: Proces zmian z zatwierdzeniem i ścieżką wycofania, powiązany z punktem A.8.32. Dla zmian niezamierzonych (błędna konfiguracja, przypadkowa eskalacja uprawnień) udokumentuj incydent i wykaż korektę.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**8.1-4** **Określa się i kontroluje procesy, produkty i usługi dostarczane z zewnątrz, które są istotne dla SZBI.**

Jak to wykazać: Lista dostawców z krytycznością, odniesieniem do umowy i stanem dowodów (certyfikat ISO 27001 dostawcy, raport SOC 2, umowa powierzenia przetwarzania danych). Dla małych organizacji jest to największa dźwignia, ponieważ i tak większość IT działa zewnętrznie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**8.2-1** **Oceny ryzyka przeprowadza się w zaplanowanych odstępach czasu oraz zawsze wtedy, gdy wystąpią istotne zmiany lub incydenty, biorąc pod uwagę ustalone kryteria.**

Jak to wykazać: Rytm (zwykle roczny) oraz zdefiniowane wyzwalacze dla ocen nieplanowanych. Dowodzą tego datowane wersje rejestru ryzyka oraz wpisy w kalendarzu lub systemie zgłoszeń.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**8.2-2** **Wyniki ocen ryzyka są przechowywane jako informacja udokumentowana.** Dokument

Jak to wykazać: Historyczne wersje rejestru ryzyka z datami, nie tylko stan bieżący. Nadpisywanie pliku uniemożliwia wykazanie rozwoju sytuacji; rozwiązuje to wersjonowanie w systemie plików lub w Git.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**8.3-1** **Wdraża się plan postępowania z ryzykiem.**

Jak to wykazać: Porównaj plan z rzeczywistością: ukończone działania z datą wdrożenia i konkretnym artefaktem (konfiguracja, polityka, umowa). Otwarte działania wymagają udokumentowanego uzasadnienia i nowego terminu docelowego.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**8.3-2** **Wyniki postępowania z ryzykiem są przechowywane jako informacja udokumentowana.** Dokument

Jak to wykazać: Raporty statusu lub zamknięte pozycje działań z odniesieniem do dowodu. Sam rejestr wystarczy, jeśli każdy wiersz zawiera datę ukończenia i odnośnik do dowodu.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

## 9 Ocena wyników 21

**9.1-1** **Określa się, co należy monitorować i mierzyć, w tym procesy i zabezpieczenia bezpieczeństwa informacji.**

Jak to wykazać: Arkusz wskaźników z możliwą do ogarnięcia liczbą solidnych miar: zaległości w poprawkach, pokrycie MFA, czas rozwiązywania incydentów, wynik ostatniego testu odtworzenia, otwarte ustalenia. Kilka wskaźników, które są faktycznie zbierane, jest lepsze niż długa lista życzeń.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.1-2** **Definiuje się metody monitorowania, pomiaru, analizy i oceny, które dają ważne wyniki.**

Jak to wykazać: Udokumentuj źródło danych i sposób obliczenia dla każdego wskaźnika, na przykład eksport ze skanera podatności lub z raportu dostawcy tożsamości. Identyfikowalność źródła jest sednem ważności.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.1-3** **Określa się, kiedy i przez kogo przeprowadza się monitorowanie i pomiar oraz kiedy wyniki są analizowane i oceniane.**

Jak to wykazać: Dodaj do arkusza wskaźników kolumny częstotliwości i właściciela. Powtarzający się termin w kalendarzu na ocenę dowodzi regularności lepiej niż jakikolwiek opis.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.1-4** **Wyniki monitorowania i pomiaru są przechowywane jako informacja udokumentowana.** Dokument

Jak to wykazać: Zarchiwizowane oceny, wyeksportowane pulpity nawigacyjne lub arkusz wskaźników prowadzony jako szereg czasowy. Widok na żywo bez historii nie spełnia wymagania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.1-5** **Wyniki bezpieczeństwa informacji oraz skuteczność SZBI ocenia się na podstawie wyników pomiarów.**

Jak to wykazać: Pisemna ocena, nie tylko liczby: trend, przyczyny, potrzeba działania. Ten tekst oceny jest jednocześnie wkładem do przeglądu zarządzania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.2.1-1** **Audyty wewnętrzne są przeprowadzane w zaplanowanych odstępach czasu i dostarczają informacji o tym, czy SZBI jest zgodny z własnymi wymaganiami organizacji oraz z wymaganiami normy i jest skutecznie wdrożony.**

Jak to wykazać: Przed audytem certyfikującym musi zostać zakończony co najmniej jeden pełny cykl audytu wewnętrznego obejmujący cały zakres. Bez tego certyfikacja jest nieosiągalna; to jedna z najczęstszych przeszkód przy pierwszych certyfikacjach.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.2.2-1** **Planuje się, ustanawia i utrzymuje program audytów; definiuje on częstotliwość, metody, odpowiedzialności, wymagania dotyczące planowania i raportowania oraz uwzględnia znaczenie poszczególnych procesów i wyniki poprzednich audytów.**

Jak to wykazać: Wieloletni program audytów obejmujący wszystkie punkty i wszystkie mające zastosowanie zabezpieczenia w całym cyklu certyfikacji, z wyższą częstotliwością dla obszarów krytycznych. W pełni wystarczy prosta tabela na trzy lata.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.2.2-2** **Dla każdego audytu definiuje się kryteria audytu i zakres audytu.**

Jak to wykazać: Plan audytu na daną datę z kryteriami (norma, polityki wewnętrzne, umowy) i jasnym zakresem. Jednostronicowy plan audytu na każdy audyt wystarcza i jednocześnie stanowi podstawę raportu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.2.2-3** **Audytorów dobiera się, a audyty przeprowadza się w sposób zapewniający obiektywizm i bezstronność. Nikt nie audytuje własnej pracy.**

Jak to wykazać: Niezależność jest tu najtrudniejszą przeszkodą: kto napisał polityki i skonfigurował systemy, ten nie może ich audytować. W bardzo małych organizacjach oznacza to niemal zawsze zewnętrznego audytora wewnętrznego, na przykład zakontraktowanego konsultanta lub kolegę z firmy partnerskiej; umowa audytowa wraz z deklaracją niezależności audytora stanowi dowód. Dopiero w wystarczająco dużych zespołach rolę można rotacyjnie przekazywać wewnętrznie osobie niemającej odpowiedzialności za audytowany obszar, co następnie trzeba pokazać w macierzy ról.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.2.2-4** **Wyniki audytu są raportowane właściwemu kierownictwu.**

Jak to wykazać: Raport z audytu z ustaleniami, niezgodnościami, zaleceniami i listą dystrybucyjną, wraz z dowodem przekazania kierownictwu, na przykład punktem w protokole lub datowanym przekazaniem mailowym.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**9.2.2-5** **Zachowuje się informację udokumentowaną dotyczącą programu audytów i wyników audytów.** Dokument

Jak to wykazać: Przechowuj w jednym miejscu program audytów, plany audytów, raporty z audytów oraz wynikające z nich działania. Powiązanie ustalenia z działaniem korygującym (punkt 10.2) musi być widoczne od początku do końca.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.1-1** **Najwyższe kierownictwo dokonuje przeglądu SZBI w zaplanowanych odstępach czasu, aby zapewnić jego ciągłą przydatność, adekwatność i skuteczność.**

Jak to wykazać: Co najmniej raz w roku i zaplanowany przed audytem zewnętrznym. Nawet w bardzo małych organizacjach musi istnieć datowany, podpisany protokół, także gdy kierownictwo i właściciel SZBI to ta sama osoba.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-1** **Przegląd zarządzania uwzględnia status działań z poprzednich przeglądów zarządzania.**

Jak to wykazać: Protokół zaczyna się od tabeli kontrolnej decyzji z poprzedniego roku i ich aktualnego statusu. Bez tego odniesienia wstecznego przegląd uznaje się za niekompletny.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-2** **Przegląd zarządzania uwzględnia zmiany w zewnętrznych i wewnętrznych zagadnieniach istotnych dla SZBI, w tym istotne aspekty zmiany klimatu.**

Jak to wykazać: Osobny punkt porządku obrad odnoszący się do zaktualizowanej analizy kontekstu. Zmiana klimatu nie jest wymieniona wprost w treści tego punktu (Amd 1:2024 zmienia jedynie punkty 4.1 i 4.2), ale wchodzi tutaj poprzez zmiany w zagadnieniach z punktu 4.1, a audytorzy tego oczekują. Nawet wynik nieistotne, bez zmian musi znaleźć się w protokole.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-3** **Przegląd zarządzania uwzględnia zmiany w potrzebach i oczekiwaniach stron zainteresowanych istotnych dla SZBI.**

Jak to wykazać: Nowe wymagania klientów wynikające z umów i ankiet bezpieczeństwa, nowe obowiązki prawne, wymagania jednostki certyfikującej. Zapisz je jako listę ze źródłami w protokole.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-4** **Przegląd zarządzania uwzględnia informacje zwrotne dotyczące wyników bezpieczeństwa informacji, w tym niezgodności i działania korygujące, wyniki monitorowania i pomiarów, wyniki audytów oraz stopień realizacji celów bezpieczeństwa informacji.**

Jak to wykazać: Traktuj te cztery bloki jako osobne punkty porządku obrad, w przeciwnym razie jeden z nich zabraknie później w protokole. Dołącz arkusz wskaźników, raport z audytu i arkusz celów jako załączniki.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-5** **Przegląd zarządzania uwzględnia informacje zwrotne od stron zainteresowanych.**

Jak to wykazać: Skargi klientów mające aspekt bezpieczeństwa, wyniki audytów klienckich, zgłoszenia z kanału sygnalizacji nieprawidłowości, informacje zwrotne od usługodawców. Zapisz to w protokole nawet wtedy, gdy ustaleniem jest, że żadnych nie otrzymano.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-6** **Przegląd zarządzania uwzględnia wyniki oceny ryzyka oraz status planu postępowania z ryzykiem.**

Jak to wykazać: Dołącz bieżący rejestr ryzyka oraz stan wdrożenia planu postępowania, wraz z wyraźnym potwierdzeniem akceptacji ryzyka szczątkowego przez właścicieli ryzyk.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.2-7** **Przegląd zarządzania uwzględnia możliwości ciągłego doskonalenia.**

Jak to wykazać: Punkt porządku obrad z konkretnymi pomysłami na usprawnienia i decyzją co do każdego z nich. Przyjęte pomysły trafiają do rejestru usprawnień jako wpisy z terminami.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.3-1** **Wyniki przeglądu zarządzania obejmują decyzje dotyczące możliwości ciągłego doskonalenia oraz wszelkiej potrzeby zmian w SZBI.**

Jak to wykazać: Protokół kończy się sekcją decyzji: decyzja, właściciel, termin. Protokół bez decyzji stanowi ustalenie podczas audytu, ponieważ brakuje wtedy efektu przywództwa.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**9.3.3-2** **Zachowuje się informację udokumentowaną jako dowód wyników przeglądu zarządzania.** Dokument

Jak to wykazać: Podpisany protokół z datą, uczestnikami, danymi wejściowymi, oceną i decyzjami. Jest to jeden z pierwszych dokumentów, o które jednostka certyfikująca prosi na etapie 1.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

## 10 Doskonalenie 7

**10.1-1** **Przydatność, adekwatność i skuteczność SZBI są stale doskonalone.**

Jak to wykazać: Rejestr usprawnień zasilany z kilku źródeł (audyty, incydenty, pomysły, odchylenia wskaźników) z widocznym postępem w czasie. Ciągłość na przestrzeni kilku miesięcy jest dowodem, a nie liczba wpisów.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**10.2-1** **Gdy wystąpi niezgodność, organizacja na nią reaguje: kontroluje ją i koryguje oraz zajmuje się jej skutkami.**

Jak to wykazać: Raport niezgodności z natychmiastowym działaniem i datą. Źródłami są audyty wewnętrzne, audyty zewnętrzne, incydenty i obserwacje z codziennej działalności; wszystkie zasilają ten sam rejestr.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**10.2-2** **Ocenia się, czy potrzebne jest działanie usuwające przyczyny, tak aby niezgodność nie powtórzyła się ani nie wystąpiła gdzie indziej; obejmuje to sprawdzenie, czy istnieją lub mogą wystąpić podobne niezgodności.**

Jak to wykazać: Udokumentuj analizę przyczyny źródłowej, na przykład metodą 5 razy dlaczego lub diagramem Ishikawy, wraz z wyraźnym stwierdzeniem dotyczącym możliwości przeniesienia na inne systemy lub procesy. Krok dotyczący możliwości przeniesienia jest najczęściej pomijany.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**10.2-3** **Wdraża się niezbędne działania korygujące, a ich skuteczność jest przeglądana.**

Jak to wykazać: Dla każdego działania zapisz datę wdrożenia, artefakt dowodowy oraz późniejszy przegląd skuteczności z własną datą. Dwa pola daty na wiersz to najprostszy sposób, by nie zgubić przeglądu skuteczności.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**10.2-4** **W razie potrzeby wprowadza się zmiany w SZBI w wyniku niezgodności.**

Jak to wykazać: Jeśli niezgodność wynika z luki w polityce, rejestrze ryzyka lub Deklaracji Stosowania, zmiana musi stać się tam widoczna. Odnośnik od niezgodności do zaktualizowanej wersji dokumentu zamyka łańcuch.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**10.2-5** **Działania korygujące są odpowiednie do skutków napotkanych niezgodności.**

Jak to wykazać: Ocena wagi w rejestrze, z której wynika proporcjonalność działania. Ani drobnostki traktowane jak projekt, ani poważne odchylenia załatwiane zwykłym mailem przypominającym.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**10.2-6** **Zachowuje się informację udokumentowaną dotyczącą charakteru niezgodności, podjętych w odpowiedzi działań oraz wyników działań korygujących.** Dokument

Jak to wykazać: Rejestr niezgodności i działań korygujących z kolumnami: charakter, przyczyna, działanie, właściciel, termin oraz wynik przeglądu skuteczności. Jest to dowód obowiązkowy, ściągany podczas każdego audytu nadzoru.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

## A.5 Załącznik A: Zabezpieczenia organizacyjne 37

**A.5.1** **Polityki bezpieczeństwa informacji: Definiuje się nadrzędną politykę bezpieczeństwa informacji oraz polityki tematyczne, zatwierdzone przez kierownictwo, komunikowane i przeglądane w zaplanowanych odstępach czasu oraz zawsze wtedy, gdy wystąpią istotne zmiany.** Dokument

Jak to wykazać: Zestaw polityk z wersją, datą zatwierdzenia i datą kolejnego przeglądu, wraz z dowodem potwierdzenia odbioru. Dla małych organizacji wystarczy polityka ramowa oraz garść polityk tematycznych (dostęp, kryptografia, praca zdalna, incydenty).

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.2** **Role i odpowiedzialności w zakresie bezpieczeństwa informacji: Role i odpowiedzialności w zakresie bezpieczeństwa informacji są definiowane i przydzielane stosownie do potrzeb organizacji.**

Jak to wykazać: Macierz ról z nazwiskami, zastępcami i zadaniami. W bardzo małych organizacjach wskaż jawnie, gdzie kilka ról kumuluje się w jednej osobie, i powiąż to z zabezpieczeniami kompensującymi z punktu A.5.3.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.3** **Rozdzielenie obowiązków: Obowiązki i obszary odpowiedzialności, które mają się wzajemnie kontrolować, nie są powierzane jednej osobie. Celem jest, aby nikt nie mógł samodzielnie zainicjować, zatwierdzić i ukryć zmiany.**

Jak to wykazać: W małych organizacjach pełne rozdzielenie jest strukturalnie niemożliwe; ogólnikowe stwierdzenie zgodne załamuje się natychmiast podczas rozmowy audytowej. To, co się broni, to szczera analiza: które kombinacje obowiązków są krytyczne (wytwarzanie i wdrażanie, nadawanie uprawnień i ich używanie, inicjowanie i zatwierdzanie płatności), które z nich spoczywają na jednej osobie i jakie zabezpieczenia kompensujące mają zastosowanie. Sprawdzone podejścia to niezmienne dzienniki audytowe dostępne dla strony trzeciej, MFA na kontach uprzywilejowanych, zautomatyzowane bramki CI i ochrona gałęzi zamiast weryfikacji na cztery oczy, okresowy przegląd logów przez osobę zewnętrzną oraz oddzielne zatwierdzanie płatności. Przechowuj analizę i zabezpieczenia kompensujące jako odrębny, datowany dokument i powiąż go z Deklaracją Stosowania.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.4** **Odpowiedzialności kierownictwa: Kierownictwo wymaga od całego personelu stosowania bezpieczeństwa informacji zgodnie z ustanowionymi politykami i procedurami.**

Jak to wykazać: Zobowiązanie w umowach o pracę i umowach z podwykonawcami, potwierdzenie zapoznania się z politykami przy wdrożeniu oraz regularne przypomnienia ze strony kierownictwa. Dowody: podpisane deklaracje zobowiązania i protokoły spotkań.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.5** **Kontakt z organami: Utrzymuje się odpowiednie kontakty z właściwymi organami, z możliwością nawiązania kontaktu w razie potrzeby.**

Jak to wykazać: Lista kontaktów z właściwym organem nadzorczym ds. ochrony danych osobowych, policją lub jednostką ds. cyberprzestępczości, krajowym punktem zgłaszania incydentów cyberbezpieczeństwa (CSIRT) oraz, jeśli dotyczy, kanałami zgłoszeniowymi NIS2. Zaznacz terminy (takie jak 72 godziny zgodnie z RODO) bezpośrednio na liście.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.6** **Kontakt z grupami zainteresowań specjalnych: Utrzymuje się kontakty z grupami zainteresowań specjalnych, forami bezpieczeństwa i stowarzyszeniami branżowymi.**

Jak to wykazać: Członkostwa, subskrybowane biuletyny ostrzegawcze (krajowy CERT, biuletyny producentów), udział w grupach zainteresowań specjalnych. Prosty dowód: lista subskrypcji oraz jeden przykład tego, jak biuletyn doprowadził do działania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.7** **Analiza zagrożeń: Zbiera się i analizuje informacje o zagrożeniach bezpieczeństwa informacji, aby wyprowadzić z nich odpowiednie działania.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Wykonalne dla małych organizacji: subskrybuj biuletyny krajowego CERT i biuletyny producentów, a następnie przeprowadzaj krótki comiesięczny przegląd z decyzją o istotności i wynikającymi z niej zgłoszeniami. Dowodem jest analiza, nie subskrypcja.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.8** **Bezpieczeństwo informacji w zarządzaniu projektami: Bezpieczeństwo informacji jest zintegrowane z zarządzaniem projektami, niezależnie od rodzaju projektu.**

Jak to wykazać: Punkty bezpieczeństwa na liście kontrolnej projektu: potrzeby ochrony, przegląd ryzyka, sprawdzenie ochrony danych, zatwierdzenie bezpieczeństwa przed uruchomieniem produkcyjnym. W zespołach zwinnych zakotwicz je jako stałe punkty w definicji gotowości i definicji ukończenia.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.9** **Inwentaryzacja informacji i innych powiązanych aktywów: Tworzy się i utrzymuje inwentaryzację informacji i innych powiązanych aktywów wraz ze wskazanymi właścicielami.**

Jak to wykazać: Ewidencja aktywów obejmująca sprzęt, oprogramowanie, usługi chmurowe, magazyny danych, domeny i konta, każde z właścicielem i potrzebami ochrony. W małych organizacjach można ją zbudować automatycznie z eksportu MDM, listy licencji i konsoli chmurowej; aktualna data jest obowiązkowa.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.10** **Dopuszczalne użycie informacji i innych powiązanych aktywów: Identyfikuje się, dokumentuje i wdraża zasady dopuszczalnego użycia i obchodzenia się z informacją oraz innymi powiązanymi aktywami.** Dokument

Jak to wykazać: Polityka dopuszczalnego użycia dla urządzeń, sieci, kont chmurowych i narzędzi AI, z potwierdzeniem zapoznania się. Urządzenia prywatne i zewnętrzne usługi AI powinny być objęte wprost, ponieważ to tam dochodzi do większości wycieków.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.11** **Zwrot aktywów: Gdy stosunek pracy się kończy lub zmienia, reguluje się i potwierdza pisemnie, że wszystkie wydane urządzenia, klucze, konta i dokumenty zostają zwrócone.**

Jak to wykazać: Lista kontrolna offboardingu z potwierdzeniem zwrotu laptopa, tokenów, kluczy, certyfikatów i nośników danych, wraz z dezaktywacją kont tego samego dnia. Dotyczy to w takim samym stopniu freelancerów i stażystów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.12** **Klasyfikacja informacji: Informacje klasyfikuje się według potrzeb ochrony w zakresie poufności, integralności, dostępności i wymagań prawnych.**

Jak to wykazać: Prosty schemat z trzema lub czterema poziomami (publiczna, wewnętrzna, poufna, ściśle poufna) oraz konkretnymi zasadami postępowania dla każdego poziomu. Zapisz przypisanie w ewidencji aktywów lub w rejestrze czynności przetwarzania.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.13** **Etykietowanie informacji: Poziom klasyfikacji jest rozpoznawalny na samym dokumencie, pliku lub wiadomości, tak aby odbiorcy wiedzieli, jak się z nim obchodzić, bez konieczności pytania.**

Jak to wykazać: Etykietowanie w nagłówku dokumentu, nazwie pliku, temacie wiadomości e-mail lub za pomocą etykiet poufności w pakiecie biurowym w chmurze. Dowód poprzez próbki faktycznie oznakowanych dokumentów, nie tylko poprzez samą zasadę.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.14** **Przekazywanie informacji: Obowiązują zasady, procedury i porozumienia dotyczące przekazywania informacji wewnątrz organizacji oraz stronom zewnętrznym.**

Jak to wykazać: Zasada wskazująca, który kanał jest dozwolony dla którego poziomu klasyfikacji: zaszyfrowana poczta elektroniczna lub pokój danych dla treści poufnych, zakaz wysyłania przez prywatne komunikatory. Zabezpiecz poufne przekazy umowami o zachowaniu poufności.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.15** **Kontrola dostępu: Ustanawia się i wdraża zasady kontroli dostępu fizycznego i logicznego do informacji i innych powiązanych aktywów, oparte na wymaganiach biznesowych i bezpieczeństwa.**

Jak to wykazać: Polityka kontroli dostępu zgodna z zasadą wiedzy koniecznej i najmniejszych uprawnień, z mapowaniem ról na uprawnienia. Dowód poprzez faktyczną konfigurację uprawnień u dostawcy tożsamości, nie tylko poprzez samą politykę.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.16** **Zarządzanie tożsamością: Zarządza się pełnym cyklem życia tożsamości.**

Jak to wykazać: Proces od utworzenia, przez zmianę, po dezaktywację, najlepiej scentralizowany u dostawcy tożsamości z jednokrotnym logowaniem. Bez współdzielonych kont grupowych; tam, gdzie jest to technicznie nieuniknione, nazwij konto, uzasadnij je i rejestruj jego użycie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.17** **Informacje uwierzytelniające: Przydzielanie i zarządzanie informacjami uwierzytelniającymi jest kontrolowane przez proces zarządzania wymagający od osób właściwego obchodzenia się z nimi.**

Jak to wykazać: Menedżer haseł jako obowiązkowe narzędzie, polityka dotycząca jakości haseł i MFA, bezpieczny dostęp początkowy oraz procedura resetu z weryfikacją tożsamości. Dowód poprzez zrzuty ekranu konfiguracji i raport menedżera haseł.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.18** **Prawa dostępu: Prawa dostępu są przydzielane, przeglądane, zmieniane i usuwane zgodnie z polityką kontroli dostępu.**

Jak to wykazać: Okresowy przegląd dostępu, co najmniej raz w roku, z udokumentowanym wynikiem dla każdego konta oraz dowodem usuniętych uprawnień. Usunięcie w dniu odejścia to punkt, który audytorzy chętnie śledzą na konkretnym przypadku.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.19** **Bezpieczeństwo informacji w relacjach z dostawcami: Definiuje się i wdraża procesy i procedury zarządzania ryzykami bezpieczeństwa wynikającymi z korzystania z produktów i usług stron trzecich.**

Jak to wykazać: Lista dostawców z poziomem krytyczności i głębokością oceny. Dla dostawców krytycznych pozyskuj dowody (certyfikat ISO 27001, raport SOC 2), zamiast przeprowadzać własne audyty, co jest jedyną realistyczną drogą dla małych organizacji.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.20** **Uwzględnianie bezpieczeństwa informacji w umowach z dostawcami: Z każdym dostawcą uzgadnia się istotne wymagania bezpieczeństwa i zapisuje je w umowach.**

Jak to wykazać: Załącznik umowny dotyczący bezpieczeństwa informacji z obowiązkami zgłaszania incydentów, zasadami dotyczącymi podprzetwarzających, obowiązkami usuwania danych i prawami audytu. Dla usług standardowych wystarczą warunki dostawcy wraz z umową powierzenia przetwarzania danych, o ile ich treść została sprawdzona i udokumentowana.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.21** **Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT: Definiuje się i wdraża procesy zarządzania ryzykami bezpieczeństwa w łańcuchu dostaw technologii informacyjno-komunikacyjnych.**

Jak to wykazać: Obejmuje to zależności programowe oraz własnych poddostawców dostawców. W praktyce: zestawienie komponentów oprogramowania (SBOM) lub lista zależności, zautomatyzowane sprawdzanie podatnych pakietów w CI oraz pozyskiwanie oprogramowania wyłącznie z podpisanych lub oficjalnych kanałów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.22** **Monitorowanie, przegląd i zarządzanie zmianami usług dostawców: Zmiany w usługach dostawców są regularnie monitorowane, przeglądane i zarządzane.**

Jak to wykazać: Roczny przegląd dostawców obejmujący incydenty, raporty dostępności i ważność certyfikatów, wraz z kanałem dla ogłoszeń zmian dostawcy. Zapisz wynik jako krótką notatkę na temat każdego dostawcy.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.23** **Bezpieczeństwo informacji przy korzystaniu z usług chmurowych: Ustanawia się procesy nabywania, korzystania, zarządzania i rezygnacji z usług chmurowych zgodnie z wymaganiami bezpieczeństwa.**

Jak to wykazać: Nowość w wydaniu z 2022 roku i zabezpieczenie kluczowe dla małych organizacji opartych na chmurze. Dowód poprzez politykę chmurową z procesem zatwierdzania nowych usług, udokumentowanym modelem wspólnej odpowiedzialności dla każdej usługi, ustawieniami hartowania oraz strategią wyjścia obejmującą zwrot danych i potwierdzenie usunięcia.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.24** **Planowanie i przygotowanie zarządzania incydentami bezpieczeństwa informacji: Planuje się i ustanawia procesy, role i odpowiedzialności dotyczące obsługi incydentów.** Dokument

Jak to wykazać: Plan reagowania na incydenty ze ścieżką zgłaszania, rolami, poziomami eskalacji, kontaktami poza godzinami pracy i szablonami komunikacji. Realistyczne dla małych zespołów: jedna strona, ale przećwiczona.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.25** **Ocena i decyzja dotycząca zdarzeń bezpieczeństwa informacji: Zdarzenia bezpieczeństwa są oceniane, a decyzję o tym, czy zaklasyfikować je jako incydenty bezpieczeństwa informacji, podejmuje się na tej podstawie.**

Jak to wykazać: Kryteria triażu wraz z macierzą wagi oraz rejestr zdarzeń, w którym odrzucone zdarzenia również figurują z uzasadnieniem. Rozróżnienie między zdarzeniem a incydentem musi być widoczne w rejestrze.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.26** **Reagowanie na incydenty bezpieczeństwa informacji: Incydenty są obsługiwane zgodnie z udokumentowanymi procedurami.**

Jak to wykazać: Teczki incydentów z osią czasu, podjętymi działaniami, zaangażowanymi osobami i decyzją o zamknięciu. Jeśli nie było jeszcze rzeczywistego incydentu, udokumentowane ćwiczenie symulacyjne jest najlepszym dostępnym dowodem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.27** **Wyciąganie wniosków z incydentów bezpieczeństwa informacji: Wiedzę zdobytą z incydentów wykorzystuje się do wzmocnienia zabezpieczeń.**

Jak to wykazać: Przegląd poincydentalny bez szukania winnych, z analizą przyczyny źródłowej i wynikającymi z niej działaniami, powiązany z rejestrem usprawnień oraz, w razie potrzeby, z rejestrem ryzyka.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.28** **Gromadzenie dowodów: Reguluje się sposób identyfikowania, zabezpieczania i przechowywania śladów związanych ze zdarzeniem bezpieczeństwa, tak aby pozostały użyteczne w przyszłości.**

Jak to wykazać: Krótka procedura zabezpieczania dowodów: nie odbudowuj systemów przedwcześnie, zabezpiecz obrazy i logi, udokumentuj łańcuch dowodowy. Dla małych organizacji wystarczy zdefiniować poziom wagi, od którego wzywa się zewnętrznego dostawcę usług informatyki śledczej, wraz z danymi kontaktowymi.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.29** **Bezpieczeństwo informacji w czasie zakłóceń: Organizacja planuje, w jaki sposób bezpieczeństwo informacji jest utrzymywane na odpowiednim poziomie w trakcie zakłócenia.**

Jak to wykazać: Rozwiązania awaryjne nie mogą wyłączać bezpieczeństwa. Udokumentuj, że MFA, rejestrowanie zdarzeń i ograniczenia dostępu obowiązują również w trybie awaryjnym oraz że konta awaryjne (konta break glass) są zapieczętowane, udokumentowane i przeglądane po ich użyciu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.30** **Gotowość ICT do ciągłości działania: Gotowość ICT jest planowana, wdrażana, utrzymywana i testowana na podstawie celów ciągłości działania i wymagań ciągłości ICT.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Dowód poprzez zdefiniowane docelowe czasy odtworzenia (RTO) i docelowe punkty odtworzenia (RPO) dla każdego systemu krytycznego, procedurę odtworzenia oraz co najmniej jeden udokumentowany test rocznie. Udany test odtworzenia z datą i czasem trwania jest tu najmocniejszym pojedynczym dowodem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.31** **Wymagania prawne, ustawowe, regulacyjne i umowne: Identyfikuje się, dokumentuje i utrzymuje w aktualności istotne wymagania oraz sposób ich spełniania.** Dokument

Jak to wykazać: Rejestr prawny obejmujący RODO, prawo telekomunikacyjne, prawo handlowe i podatkowe oraz, jeśli dotyczy, NIS2 lub przepisy branżowe, każdy z regułą realizującą dane wymaganie i datą przeglądu. Roczny przegląd jest wystarczający, ale musi być datowany.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.5.32** **Prawa własności intelektualnej: Wdraża się odpowiednie procedury ochrony praw własności intelektualnej.**

Jak to wykazać: Inwentaryzacja licencji używanego oprogramowania, sprawdzenie licencji open source w produkcie (skaner licencji w CI) oraz zasada postępowania z kodem stron trzecich i kodem generowanym. Dowód: raport licencyjny pochodzący z procesu budowania.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.33** **Ochrona zapisów: Zapisy biznesowe i dowodowe przechowuje się tak, aby nie mogły zostać utracone, nie mogły zostać niepostrzeżenie zmienione i nie mogły dostać się w niepowołane ręce, i to przez cały okres retencji.**

Jak to wykazać: Harmonogram retencji z ustawowymi okresami, przechowywanie odporne na manipulacje, ograniczony dostęp i kopia zapasowa. Dla zapisów istotnych podatkowo podaj wprost ustawowe okresy retencji, ponieważ audytorzy chętnie sprawdzają to konkretnie.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.34** **Prywatność i ochrona danych osobowych (PII): Identyfikuje się i spełnia wymagania dotyczące prywatności i ochrony danych umożliwiających identyfikację osoby (PII) zgodnie z obowiązującym prawem.**

Jak to wykazać: Rejestr czynności przetwarzania, umowy powierzenia przetwarzania danych, koncepcja usuwania danych, proces obsługi praw osób, których dane dotyczą, oraz, jeśli wymagana, ocena skutków dla ochrony danych. Powiązanie tego z SZBI poprzez wspólną listę aktywów pozwala uniknąć podwójnego utrzymywania wszystkiego.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.35** **Niezależny przegląd bezpieczeństwa informacji: Podejście organizacji do zarządzania bezpieczeństwem informacji jest przeglądane niezależnie w zaplanowanych odstępach czasu oraz zawsze wtedy, gdy wystąpią istotne zmiany.**

Jak to wykazać: Dowodzi tego audyt wewnętrzny przeprowadzony przez niezależnego audytora, zewnętrzne testy penetracyjne lub sam audyt certyfikujący. Niezależny oznacza, że nie przeprowadza go osoba odpowiedzialna za przeglądany obszar.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.36** **Zgodność z politykami, zasadami i normami bezpieczeństwa informacji: Zgodność z własnymi politykami bezpieczeństwa organizacji oraz mającymi zastosowanie zasadami jest regularnie sprawdzana.**

Jak to wykazać: Sprawdzenia zgodności z datą i wynikiem, na przykład sprawdzenie konfiguracji względem własnej linii bazowej hartowania, próbkowanie etykietowania dokumentów, zautomatyzowane sprawdzenia polityk w chmurze. Odchylenia zasilają rejestr działań korygujących.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.5.37** **Udokumentowane procedury operacyjne: Procedury operacyjne dla zasobów przetwarzania informacji są dokumentowane i udostępniane osobom, które ich potrzebują.** Dokument

Jak to wykazać: Runbooki dotyczące kopii zapasowych i odtwarzania, wdrożeń, administracji użytkownikami, wprowadzania poprawek i obsługi incydentów. Krótkie i aktualne jest lepsze niż obszerne i nieaktualne; data ostatniej zmiany na każdy runbook jest obowiązkowa.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

## A.6 Załącznik A: Zabezpieczenia dotyczące ludzi 8

**A.6.1** **Weryfikacja: Kandydatów, którzy mają pracować dla organizacji, weryfikuje się z wyprzedzeniem, w granicach prawa i proporcjonalnie do potrzeb ochrony; dla ról wrażliwych weryfikację powtarza się w trakcie zatrudnienia.**

Jak to wykazać: Przy braku pracowników zabezpieczenie to można uzasadnić jako obecnie niestosowane, ale procedura na wypadek zatrudnienia powinna nadal być zdefiniowana i zapisana w Deklaracji Stosowania jako planowana. Wykonalny zakres: weryfikacja tożsamości, życiorysu i referencji wraz z certyfikatami; sprawdzenie niekaralności tylko wtedy, gdy uzasadniają to potrzeby ochrony i pozwala na to prawo. Wymagaj tego samego standardu od freelancerów i podwykonawców poprzez ich umowy, w przeciwnym razie luka otworzy się dokładnie tam.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.2** **Warunki zatrudnienia: Postanowienia umowne określają odpowiedzialności w zakresie bezpieczeństwa informacji personelu i organizacji.**

Jak to wykazać: Klauzula bezpieczeństwa w umowie o pracę lub umowie usługowej odsyłająca do mających zastosowanie polityk. Dla freelancerów ta sama klauzula w umowie usługowej wraz z umową o zachowaniu poufności.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.3** **Świadomość, edukacja i szkolenia w zakresie bezpieczeństwa informacji: Personel i właściwe strony zewnętrzne otrzymują odpowiednie działania podnoszące świadomość i szkolenia, a także regularne aktualizacje dotyczące polityk organizacji.**

Jak to wykazać: Coroczne szkolenie z dowodem obecności i datą, uzupełnione symulacjami phishingu z ocenionym wskaźnikiem klikalności. Nawet osoby samozatrudnione bez personelu potrzebują dowodu własnego doskonalenia zawodowego, na przykład potwierdzeń ukończenia kursów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.4** **Proces dyscyplinarny: Istnieje formalny i komunikowany proces podejmowania działań wobec osób, które naruszyły polityki bezpieczeństwa.**

Jak to wykazać: Przy braku pracowników można to uzasadnić jako obecnie niestosowane, ale proces musi nadal być zdefiniowany na wypadek zatrudnienia; odpada jedynie jego zastosowanie, nie sama zasada. Wymagana jest stopniowana, komunikowana skala reakcji (rozmowa, upomnienie, formalna nagana, zwolnienie) zgodna z prawem pracy i zasadami reprezentacji pracowniczej. Dla podwykonawców odzwierciedl poziom sankcji w umowie, na przykład karą umowną lub prawem do wypowiedzenia.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.5** **Odpowiedzialności po zakończeniu lub zmianie zatrudnienia: Definiuje się, egzekwuje i komunikuje zainteresowanym osobom odpowiedzialności i obowiązki w zakresie bezpieczeństwa, które pozostają w mocy po zakończeniu lub zmianie roli.**

Jak to wykazać: Lista kontrolna offboardingu z usunięciem uprawnień, zwrotem aktywów, przekazaniem obowiązków oraz wyraźnym przypomnieniem o dalej obowiązujących zobowiązaniach do zachowania poufności. Podpisany zapis rozmowy zakończeniowej jest najprostszym dowodem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.6** **Umowy o zachowaniu poufności lub o nieujawnianiu informacji: Określa się, kto musi podpisać umowę o zachowaniu poufności. Treść odpowiada potrzebom ochrony informacji, umowy są podpisywane, archiwizowane i regularnie przeglądane w celu utrzymania ich aktualności.**

Jak to wykazać: Podpisane umowy o zachowaniu poufności dla pracowników, freelancerów, usługodawców i stażystów, z okresem obowiązywania po zakończeniu współpracy. Tabela zbiorcza ze stroną, datą i ważnością sprawia, że portfel jest audytowalny.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.7** **Praca zdalna: Wdraża się środki bezpieczeństwa tam, gdzie osoby pracują poza siedzibą organizacji i uzyskują wówczas dostęp do informacji organizacji.**

Jak to wykazać: Polityka pracy zdalnej i pracy w domu z wymaganiami dotyczącymi szyfrowania dysku, blokady ekranu, bezpiecznego Wi-Fi, użycia VPN lub dostępu opartego na zasadzie zero trust, filtrów prywatyzujących ekran oraz zakazu używania urządzeń prywatnych bez zgody. Dowód poprzez raport zgodności MDM dla urządzeń końcowych.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.6.8** **Zgłaszanie zdarzeń bezpieczeństwa informacji: Istnieje mechanizm, dzięki któremu osoby mogą terminowo zgłaszać zaobserwowane lub podejrzewane zdarzenia bezpieczeństwa.**

Jak to wykazać: Jasno komunikowany kanał zgłaszania (skrzynka pocztowa, kanał czatu, numer telefonu) wraz z zapewnieniem braku sankcji za zgłoszenia dokonane w dobrej wierze. Dowód: liczba zgłoszeń w rejestrze zdarzeń; trwale pusty rejestr jest sygnałem ostrzegawczym podczas audytu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

## A.7 Załącznik A: Zabezpieczenia fizyczne 14

**A.7.1** **Fizyczne granice bezpieczeństwa: Definiuje się i wykorzystuje granice bezpieczeństwa w celu ochrony obszarów zawierających informacje i zasoby przetwarzania informacji.**

Jak to wykazać: Opis granic wraz ze szkicem lub zdjęciami: budynek, biuro, szafa serwerowa. W biurze domowym granicą jest zamykane na klucz pomieszczenie robocze lub, w braku takiego, zamykana szafa; opisz to, zamiast pomijać.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.2** **Wejście fizyczne: Obszary bezpieczne są chronione za pomocą odpowiednich kontroli wejścia i punktów dostępu.**

Jak to wykazać: Rejestr kluczy lub kart dostępu z wydaniem i zwrotem oraz zasada dotycząca gości z towarzyszeniem i rejestrem. Jeśli korzysta się z przestrzeni coworkingowej lub centrum danych, przyjmij jako dowód kontrole wejścia operatora i zabezpiecz je umownie.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.3** **Zabezpieczanie biur, pomieszczeń i obiektów: Projektuje się i wdraża fizyczne zabezpieczenia biur, pomieszczeń i obiektów.**

Jak to wykazać: Drzwi zamykane na klucz, zabezpieczenie okien na parterze, brak poufnych ekranów widocznych z zewnątrz, brak szyldu firmowego na obszarach wrażliwych. Krótki opis wraz ze zdjęciem wystarczy jako dowód.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.4** **Monitorowanie bezpieczeństwa fizycznego: Obiekty są nieprzerwanie monitorowane pod kątem nieautoryzowanego dostępu fizycznego.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Opcje to system alarmowy, czujniki ruchu, monitoring wizyjny lub rejestry wejść. Monitoring wizyjny musi zostać sprawdzony pod kątem zgodności z ochroną danych; w biurze domowym uzasadnioną alternatywą jest połączenie systemu alarmowego, zamkniętego pomieszczenia oraz stwierdzenia, że nie przechowuje się tam wrażliwych serwerów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.5** **Ochrona przed zagrożeniami fizycznymi i środowiskowymi: Zapewnia się ochronę przed zagrożeniami fizycznymi i środowiskowymi, takimi jak klęski żywiołowe oraz zamierzone lub niezamierzone szkody.**

Jak to wykazać: Przegląd zagrożeń pożarem, wodą, upałem, awarią zasilania i włamaniem, wraz z wdrożonymi środkami (czujniki dymu, gaśnice, brak sprzętu pod rurami wodociągowymi, kopia zapasowa przechowywana w innej lokalizacji). Tutaj łączy się to z ustaleniem dotyczącym zmiany klimatu z punktu 4.1.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.6** **Praca w obszarach bezpiecznych: Projektuje się i wdraża środki dotyczące pracy w obszarach bezpiecznych.**

Jak to wykazać: Zasady dla serwerowni lub obszarów o wysokiej poufności: brak nienadzorowanego dostępu stron trzecich, zakaz nagrywania kamerami lub urządzeniami mobilnymi, rejestrowanie wykonywanych prac. Jeśli nie ma obszarów bezpiecznych, można to uzasadnić odwołując się do działania wyłącznie w chmurze.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.7** **Czyste biurko i czysty ekran: Definiuje się i przestrzega zasad czystego biurka dotyczących papierów i nośników wymiennych oraz blokowania ekranów.**

Jak to wykazać: Dotyczy to w pełni również biura domowego i dlatego nie może zostać uznane za niestosowane. Wykazywane poprzez krótką zasadę (zamykanie dokumentów pod kluczem, blokada ekranu po pięciu minutach, brak karteczek samoprzylepnych z danymi uwierzytelniającymi) oraz technicznie wymuszoną blokadę poprzez politykę urządzeń, której konfigurację można wyeksportować.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.8** **Rozmieszczenie i ochrona sprzętu: Sprzęt jest rozmieszczany i chroniony w sposób bezpieczny.**

Jak to wykazać: Umiejscowienie z dala od ciągów komunikacyjnych i miejsc publicznych, brak widoczności z zewnątrz, ochrona przed upałem i wilgocią, linki zabezpieczające dla urządzeń mobilnych. Krótki opis w ramach polityki biura domowego lub biurowej wystarczy.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.9** **Bezpieczeństwo aktywów poza siedzibą: Chroni się aktywa znajdujące się poza siedzibą.**

Jak to wykazać: W małych organizacjach jest to głównie laptop, smartfon i nośniki zewnętrzne, i nie da się tego pominąć. Dowód: wymuszone szyfrowanie dysku, zdalne kasowanie danych włączone przez MDM, zasada zakazująca pozostawiania urządzeń w pojazdach oraz korzystania z sieci publicznych bez VPN, wraz ze ścieżką zgłaszania utraty. Raport zgodności MDM pokazujący stan szyfrowania dla każdego urządzenia jest tu najmocniejszym pojedynczym dowodem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.10** **Nośniki danych: Nośniki danych są zarządzane przez cały ich cykl życia zgodnie ze schematem klasyfikacji i wymaganiami postępowania, od nabycia, przez użycie i transport, po likwidację.**

Jak to wykazać: Dotyczy to nawet pracy wyłącznie mobilnej, ponieważ istnieją pamięci USB, dyski zewnętrzne i nośniki kopii zapasowych. Dowód: rejestr nośników, nośniki szyfrowane, technicznie wymuszony zakaz niezatwierdzonych nośników wymiennych, bezpieczne przechowywanie w zamykanym miejscu oraz przekazanie do punktu A.7.14 po zakończeniu okresu eksploatacji.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.11** **Instalacje pomocnicze: Zasoby przetwarzania informacji są chronione przed awarią instalacji pomocniczych, w szczególności zasilania elektrycznego.**

Jak to wykazać: Tam, gdzie serwery są eksploatowane we własnym zakresie, zasilacz awaryjny wraz z udokumentowanym testem. W konfiguracji wyłącznie chmurowej dowodem jest odniesienie do zobowiązań dostawcy wraz z zasadą, jak kontynuować pracę podczas lokalnej awarii zasilania lub internetu (współdzielenie łącza mobilnego, lokalizacja zapasowa).

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.7.12** **Bezpieczeństwo okablowania: Okablowanie zasilające, danych i komunikacyjne jest chronione przed przechwyceniem, zakłóceniem i uszkodzeniem.**

Jak to wykazać: Tam, gdzie okablowanie jest własne, ochrona przed uszkodzeniem oraz przed nieautoryzowanym dostępem do paneli krosowych. W małych biurach i biurach domowych uzasadnienie jest skromne, ale musi zostać podane: router i gniazda sieciowe nie są publicznie dostępne, nieużywane porty są wyłączone.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.7.13** **Konserwacja sprzętu: Sprzęt jest właściwie konserwowany, aby zapewnić dostępność, integralność i poufność informacji.**

Jak to wykazać: Plan konserwacji lub status wsparcia producenta dla każdego urządzenia oraz zasada dotycząca napraw wykonywanych przez strony trzecie (najpierw usuń nośnik danych lub wykasuj dane oraz zawrzyj umowę o zachowaniu poufności z dostawcą). Śledź daty końca wsparcia w ewidencji aktywów.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.7.14** **Bezpieczna likwidacja lub ponowne wykorzystanie sprzętu: Zanim urządzenie zawierające nośnik danych zostanie przekazane, sprzedane lub zezłomowane, weryfikuje się i rejestruje, że żadne chronione dane ani licencjonowane oprogramowanie nie mogą zostać z niego odtworzone.**

Jak to wykazać: Dotyczy to również biura domowego oraz wycofanych urządzeń prywatnych, które były używane do pracy. Dowód: rejestr kasowania dla każdego urządzenia z numerem seryjnym, datą i metodą (kasowanie kryptograficzne na zaszyfrowanych dyskach SSD, nadpisywanie, fizyczne zniszczenie) lub certyfikat zniszczenia od dostawcy. Dla urządzeń zaszyfrowanych wystarczy udokumentowane zniszczenie klucza, o ile procedura jest opisana.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

## A.8 Załącznik A: Zabezpieczenia technologiczne 34

**A.8.1** **Urządzenia końcowe użytkownika: Chroni się informacje przechowywane, przetwarzane lub dostępne za pośrednictwem urządzeń końcowych użytkownika.**

Jak to wykazać: Linia bazowa hartowania dla każdego systemu operacyjnego, scentralizowane zarządzanie poprzez MDM, szyfrowanie dysku, automatyczne aktualizacje i blokada ekranu. Raport zgodności MDM ze statusem dla każdego urządzenia dowodzi tego wszystkiego naraz.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.2** **Uprzywilejowane prawa dostępu: Przydzielanie i użycie uprzywilejowanych praw dostępu jest ograniczone i zarządzane.**

Jak to wykazać: Lista wszystkich kont administratora z uzasadnieniem, oddzielne konta administracyjne nieużywane do codziennej pracy, wymuszone MFA, ograniczona czasowo eskalacja tam, gdzie to możliwe, oraz okresowy przegląd. W małych organizacjach jest to najważniejsze zabezpieczenie kompensujące dla punktu A.5.3.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.3** **Ograniczenie dostępu do informacji: Dostęp do informacji i innych powiązanych aktywów jest ograniczony zgodnie z ustanowioną polityką kontroli dostępu.**

Jak to wykazać: Koncepcja autoryzacji oparta na rolach i grupach, a nie na indywidualnych nadaniach, wykazywana poprzez eksport przynależności do grup. Regularnie przeglądaj publiczne linki udostępniania w chmurowym magazynie danych i pozwalaj im wygasać.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.4** **Dostęp do kodu źródłowego: Dostęp do odczytu i zapisu kodu źródłowego, narzędzi programistycznych i bibliotek oprogramowania jest odpowiednio zarządzany.**

Jak to wykazać: Uprawnienia repozytorium według roli, chronione gałęzie główne, wymuszone przeglądy lub wymuszone kontrole statusu, brak bezpośredniego push do gałęzi głównej. Dowód poprzez konfigurację ochrony gałęzi oraz listę członków organizacji.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.5** **Bezpieczne uwierzytelnianie: Wdraża się bezpieczne technologie i procedury uwierzytelniania na podstawie ograniczeń dostępu i polityki tematycznej.**

Jak to wykazać: MFA dla całego dostępu zewnętrznego i wszystkich kont administratora, metody odporne na phishing (klucze dostępu, FIDO2) tam, gdzie to możliwe, oraz blokada po nieudanych próbach. Dowód poprzez raport pokrycia MFA od dostawcy tożsamości.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.6** **Zarządzanie pojemnością: Monitoruje się pamięć masową, moc obliczeniową, przepustowość i licencje, a zapotrzebowanie dostosowuje się wystarczająco wcześnie, aby wąskie gardła nigdy nie zagroziły dostępności.**

Jak to wykazać: Monitorowanie pamięci masowej, obciążenia obliczeniowego, limitów licencji i budżetów chmurowych z alertami progowymi. W małych organizacjach wystarczy alert dotyczący wykorzystania dysku i limitów kosztów wraz z rocznym przeglądem pojemności.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.7** **Ochrona przed złośliwym oprogramowaniem: Techniczne zabezpieczenia przed złośliwym oprogramowaniem są aktywne i aktualne, a osoby korzystające z urządzeń są wystarczająco przeszkolone, aby nie osłabiać tych zabezpieczeń.**

Jak to wykazać: Aktywna ochrona punktów końcowych z centralnym przeglądem statusu, filtr poczty sprawdzający załączniki i linki oraz zasada zakazująca uruchamiania niezatwierdzonego oprogramowania. Datowany raport statusu rozwiązania ochronnego jest bezpośrednim dowodem.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.8** **Zarządzanie podatnościami technicznymi: Organizacja aktywnie pozyskuje informacje o podatnościach w wykorzystywanej technologii, decyduje dla każdego ustalenia, w jakim stopniu jest na nie narażona, i zamyka lukę w zdefiniowanych terminach lub uzasadnia inną reakcję.**

Jak to wykazać: Zarządzanie podatnościami ze źródłem (skaner, sprawdzanie zależności w CI, biuletyny producentów), oceną wagi i zdefiniowanymi terminami dla każdego poziomu, na przykład krytyczne w ciągu 7 dni. Dowód: raporty ze skanowania z kilku momentów w czasie pokazujące spadek liczby otwartych ustaleń.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.9** **Zarządzanie konfiguracją: Konfiguracje sprzętu, oprogramowania, usług i sieci, w tym konfiguracje bezpieczeństwa, są ustanawiane, dokumentowane, wdrażane, monitorowane i przeglądane.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Dowód poprzez udokumentowane konfiguracje bazowe (linie bazowe hartowania) i ich egzekwowanie, najlepiej jako infrastrukturę jako kod w systemie kontroli wersji lub poprzez profile MDM. Wykrywanie dryfu konfiguracji oraz okresowe porównanie konfiguracji dopełniają tego.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.10** **Usuwanie informacji: Informacje przechowywane w systemach informatycznych, na urządzeniach i nośnikach danych są usuwane, gdy przestają być potrzebne.**

Jak to wykazać: Nowość w wydaniu z 2022 roku i ściśle powiązana z RODO. Dowód poprzez koncepcję usuwania z okresami retencji dla poszczególnych kategorii danych, technicznie wdrożone polityki retencji w usługach chmurowych i bazach danych oraz logi usunięć. Kopie zapasowe i archiwa logów również potrzebują okresu retencji.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.11** **Maskowanie danych: Maskowanie danych stosuje się zgodnie z polityką tematyczną dotyczącą kontroli dostępu oraz wymaganiami biznesowymi i prawnymi.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. W praktyce: brak danych produkcyjnych w środowiskach testowych i deweloperskich, zamiast tego dane zanonimizowane lub syntetyczne; pseudonimizacja w analityce; maskowanie numerów kont i danych uwierzytelniających w logach i interfejsach wsparcia. Dowód poprzez skrypt lub procedurę generującą dane testowe.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.12** **Zapobieganie wyciekowi danych: Stosuje się środki zapobiegające wyciekowi danych w systemach, sieciach i urządzeniach przetwarzających, przechowujących lub przesyłających informacje wrażliwe.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Realistyczne w małych organizacjach: kontrola linków udostępniania w chmurowym magazynie danych, blokowanie niezatwierdzonych nośników wymiennych, zasady zakazujące przekazywania na prywatne skrzynki pocztowe, sprawdzanie wprowadzania poufnych danych do zewnętrznych usług AI oraz wykrywanie sekretów w kodzie źródłowym. Dowód poprzez konfigurację oraz przeglądy trafień.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.13** **Kopia zapasowa informacji: Istnieją kopie zapasowe danych, oprogramowania i systemów zgodnie z określoną zasadą (zakres, częstotliwość, retencja, lokalizacja), a odtwarzanie z nich jest rzeczywiście testowane w regularnych odstępach czasu.**

Jak to wykazać: Polityka kopii zapasowych z częstotliwością, retencją i kopią przechowywaną poza siedzibą zgodnie z zasadą 3-2-1, szyfrowanie kopii zapasowych oraz ochrona przed nadpisaniem przez ransomware (niezmienne kopie zapasowe). Rozstrzygający jest udokumentowany test odtworzenia z datą i wynikiem, ponieważ nieprzetestowana kopia zapasowa liczy się podczas audytu jako nieistniejąca.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.14** **Redundancja zasobów przetwarzania informacji: Zasoby przetwarzania informacji wdraża się z wystarczającą redundancją, aby spełnić wymagania dostępności.**

Jak to wykazać: Redundancja musi odpowiadać celom dostępności, a nie maksimum możliwości. Dowód poprzez opis architektury z redundantnymi instancjami lub strefami, sprzętem zapasowym oraz uzasadnioną decyzją co do miejsc, w których redundancja jest celowo pominięta.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.15** **Rejestrowanie zdarzeń: Działania istotne z punktu widzenia bezpieczeństwa pozostawiają ślad. Logi są generowane, przechowywane, chronione przed zmianą i rzeczywiście analizowane, a nie tylko zbierane.**

Jak to wykazać: Rejestruj co najmniej logowania i nieudane próby, zmiany uprawnień, działania administracyjne oraz dostęp do danych poufnych. Logi są chronione przed zmianą i mają zdefiniowany okres retencji; w małych organizacjach niezmienne logi są jednocześnie rekompensatą za brak rozdzielenia obowiązków z punktu A.5.3.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.16** **Działania monitorujące: Sieci, systemy i aplikacje są monitorowane pod kątem anomalii, a w celu oceny potencjalnych incydentów bezpieczeństwa podejmuje się odpowiednie działania.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Wykonalne bez własnego zespołu bezpieczeństwa: alerty dostawcy tożsamości dotyczące niemożliwych podróży i serii nieudanych prób, alerty platformy chmurowej dotyczące nietypowych wydatków lub zmian uprawnień, przekierowywane do monitorowanej skrzynki pocztowej z określonym czasem reakcji. Dowód poprzez reguły alertów oraz przykłady obsłużonych alertów.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.17** **Synchronizacja czasu: Wszystkie systemy generujące logi pobierają czas z określonego, zaufanego źródła, tak aby zdarzenia można było prawidłowo uporządkować w czasie między systemami.**

Jak to wykazać: Konfiguracja NTP na serwerach i urządzeniach końcowych oraz jednolita strefa czasowa w logach (najlepiej UTC). Bez zsynchronizowanego czasu rekonstrukcja incydentu zgodnie z punktem A.5.28 się nie broni; wyciąg z konfiguracji wystarczy jako dowód.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.18** **Użycie uprzywilejowanych programów narzędziowych: Użycie programów narzędziowych, które mogą obchodzić zabezpieczenia systemu, jest ograniczone i ściśle kontrolowane.**

Jak to wykazać: Lista zatwierdzonych narzędzi administracyjnych, ograniczenie lokalnych uprawnień administratora, kontrola aplikacji (listy dozwolonych) tam, gdzie to możliwe, oraz rejestrowanie użycia. Dowód: polityka wraz z konfiguracją zarządzania uprawnieniami.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.19** **Instalacja oprogramowania w systemach operacyjnych: Wdraża się procedury i środki bezpiecznego zarządzania instalacją oprogramowania w systemach operacyjnych.**

Jak to wykazać: Wyłącznie zatwierdzone oprogramowanie z zaufanych źródeł, instalacja poprzez centralną dystrybucję lub menedżera pakietów, ścieżka wycofania oraz zachowanie poprzedniej wersji. Dowód poprzez listę zatwierdzeń i logi wdrożeń.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.20** **Bezpieczeństwo sieci: Sieci i aktywne urządzenia sieciowe mają wskazanego właściciela, konfigurację poddaną hartowaniu oraz identyfikowalny zestaw reguł określający, jaki ruch jest w ogóle dozwolony.**

Jak to wykazać: Zestaw reguł zapory sieciowej zgodny z zasadą domyślnej odmowy, udokumentowane otwarte porty z uzasadnieniem, bezpieczna konfiguracja Wi-Fi oraz zmienione domyślne dane uwierzytelniające na urządzeniach sieciowych. Dowód poprzez eksport zestawu reguł oraz zewnętrzny skan portów.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.21** **Bezpieczeństwo usług sieciowych: Identyfikuje się, wdraża i monitoruje mechanizmy bezpieczeństwa, poziomy usług i wymagania zarządzania dla usług sieciowych.**

Jak to wykazać: Dla każdej używanej usługi sieciowej (VPN, DNS, poczta, CDN) udokumentuj zobowiązania bezpieczeństwa oraz własną konfigurację, w tym szyfrowanie w transmisji i zobowiązania dostawcy dotyczące poziomu usług. Dowód: przegląd konfiguracji wraz z umową lub opisem usługi.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.22** **Segregacja sieci: Sieć jest podzielona na strefy, tak aby usługi, grupy użytkowników i systemy o różnych potrzebach ochrony nie mogły osiągać się nawzajem bez filtrowania.**

Jak to wykazać: Oddzielne segmenty sieci lub VLAN dla gości, administracji i produkcji; w chmurze oddzielne konta lub sieci wirtualne z grupami bezpieczeństwa. W biurze domowym wykonalnym rozwiązaniem jest oddzielna sieć lub VLAN dla urządzeń służbowych, odseparowana od urządzeń prywatnych i technologii smart home.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.23** **Filtrowanie ruchu internetowego: Zarządza się dostępem do zewnętrznych stron internetowych, aby ograniczyć narażenie na złośliwe treści.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Osiągalne niewielkim nakładem poprzez usługę DNS z filtrowaniem lub filtrowanie ruchu internetowego wbudowane w ochronę punktów końcowych, z zablokowanymi kategoriami i rejestrowaniem zablokowanych żądań. Dowód poprzez konfigurację filtra oraz wyciąg z raportów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.24** **Użycie kryptografii: Wiążąco definiuje się, gdzie stosuje się szyfrowanie, z jakimi algorytmami oraz jak klucze są generowane, przechowywane, rotowane i niszczone przez cały ich cykl życia.** Dokument

Jak to wykazać: Polityka kryptografii z zatwierdzonymi algorytmami i minimalnymi długościami kluczy, szyfrowanie w transmisji (TLS) i w spoczynku, wraz z procedurą zarządzania kluczami obejmującą generowanie, przechowywanie, rotację i niszczenie. Dowód poprzez politykę wraz z konfiguracją usługi kluczy lub magazynu sekretów.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.25** **Bezpieczny cykl życia wytwarzania: Ustanawia się i stosuje zasady bezpiecznego wytwarzania oprogramowania i systemów.**

Jak to wykazać: Opis procesu wytwarzania z punktami kontrolnymi bezpieczeństwa dla każdej fazy: wymagania, projektowanie, implementacja, testowanie, wydanie, eksploatacja. Dla małych zespołów wystarczy jedna strona odsyłająca do konkretnych bramek CI i obowiązku przeglądu.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.26** **Wymagania bezpieczeństwa aplikacji: Wymagania bezpieczeństwa dla aplikacji są identyfikowane, specyfikowane i zatwierdzane podczas wytwarzania i nabywania.**

Jak to wykazać: Wymagania bezpieczeństwa jako wyraźne pozycje na liście wymagań lub jako wielokrotnego użytku lista kontrolna, oparta na przykład na powszechnie stosowanych standardach weryfikacji bezpieczeństwa aplikacji. Dowód poprzez zgłoszenia lub dokumenty wymagań z aspektem bezpieczeństwa.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.27** **Zasady bezpiecznej architektury i inżynierii systemów: Ustanawia się, dokumentuje i stosuje zasady bezpiecznej inżynierii systemów w działaniach rozwojowych.**

Jak to wykazać: Udokumentowane zasady, takie jak najmniejsze uprawnienia, obrona w głąb, bezpieczne ustawienia domyślne, minimalizacja danych oraz podejście zero trust, wraz z widocznym ich stosowaniem w szkicach architektury lub rejestrach decyzji.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.28** **Bezpieczne kodowanie: W wytwarzaniu oprogramowania stosuje się zasady bezpiecznego kodowania.**

Jak to wykazać: Nowość w wydaniu z 2022 roku. Dowód poprzez wiążące zasady kodowania, statyczną analizę kodu i wykrywanie sekretów jako obowiązkowe bramki CI, użycie zweryfikowanych bibliotek oraz udokumentowane przeglądy kodu. Tam, gdzie rozdzielenie obowiązków jest niemożliwe, wymuszone zautomatyzowane bramki zastępują weryfikację na cztery oczy; uzasadnij to i udokumentuj konfiguracją pipeline'u.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.29** **Testowanie bezpieczeństwa w wytwarzaniu i odbiorze: Definiuje się i wdraża procesy testowania bezpieczeństwa w ramach cyklu życia wytwarzania.**

Jak to wykazać: Zautomatyzowane testy bezpieczeństwa w pipeline (sprawdzanie zależności, analiza statyczna i dynamiczna) wraz z okresowym testem penetracyjnym tam, gdzie potrzeby ochrony są podwyższone. Dowód poprzez datowane raporty testowe oraz śledzenie ustaleń.

◯ Otwarte ◯ W toku ◯ Spełnione ◯ Nie dotyczy

Dowód / uzasadnienie

**A.8.30** **Wytwarzanie zlecane na zewnątrz: Zlecone na zewnątrz działania rozwojowe są kierowane, monitorowane i przeglądane.**

Jak to wykazać: Tam, gdzie wytwarzanie jest zlecane na zewnątrz, zapisz w umowie wymagania bezpieczeństwa, zabezpiecz własność kodu i prawo przeglądu oraz przeprowadzaj przeglądy kodu i testy bezpieczeństwa przed odbiorem. Bez wytwarzania zlecanego na zewnątrz niestosowanie musi zostać spójnie uzasadnione w Deklaracji Stosowania.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.31** **Rozdzielenie środowisk rozwojowego, testowego i produkcyjnego: Środowiska rozwojowe, testowe i produkcyjne są rozdzielone i chronione.**

Jak to wykazać: Oddzielne konta, projekty lub przestrzenie nazw, oddzielne dane uwierzytelniające i oddzielne zbiory danych. W połączeniu z punktem A.8.11 zapewnij, że żadne dane produkcyjne nie trafią do środowisk nieprodukcyjnych. Dowód poprzez przegląd środowisk oraz przydział uprawnień.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.32** **Zarządzanie zmianą: Zmiany w zasobach przetwarzania informacji i systemach informatycznych podlegają procedurom zarządzania zmianą.**

Jak to wykazać: Proces zmian z wnioskiem, oceną wpływu, testowaniem, zatwierdzeniem, wdrożeniem oraz ścieżką wycofania. W zespołach programistycznych pipeline pull requestów z wymuszonymi kontrolami i rejestrowanymi wdrożeniami spełnia ten punkt, o ile historia jest niezmienna.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.33** **Informacje testowe: Informacje testowe są odpowiednio dobierane, chronione i zarządzane.**

Jak to wykazać: Zasada: żadnych rzeczywistych danych osobowych w systemach testowych. Gdy jest to nieuniknione, udokumentuj zatwierdzenie, maskowanie, ograniczenie dostępu oraz usunięcie po zakończeniu testu. Dowód poprzez koncepcję danych testowych oraz logi usunięć.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie

**A.8.34** **Ochrona systemów informatycznych podczas testów audytowych: Testy audytowe wiążące się z dostępem do systemów operacyjnych są planowane i uzgadniane z kierownictwem, aby uniknąć zakłóceń w działalności.**

Jak to wykazać: Porozumienie audytowe z oknem czasowym, zakresem, dostępem tylko do odczytu tam, gdzie to możliwe, rejestrowaniem dostępu audytowego oraz zatwierdzeniem przez kierownictwo. Dotyczy to również testów penetracyjnych: pisemna autoryzacja testu z oknem czasowym i kontaktem awaryjnym stanowi dowód.

○ Otwarte ○ W toku ○ Spełnione ○ Nie dotyczy

Dowód / uzasadnienie