RAPORT Z AUDYTU ZGODNOŚCI Z ISO/IEC 27001

dla

[redacted]

PRZYKŁADOWY RAPORT

Przygotował:

Audytel S.A.

Wersja 1.0 z dnia X

© AUDYTEL 2025

SPIS TREŚCI

PRZYKŁADOWY RAPORT

1. Wstęp

Niniejszy raport przedstawia wyniki prac audytorskich realizowanych przez audytorów w ramach umowy z dnia ……. pomiędzy Audytel S.A. oraz [redacted]. Audyt miał na celu ocenę skuteczności wdrożonych mechanizmów bezpieczeństwa informacji oraz ich zgodności z przyjętymi politykami, procedurami i wymaganiami normatywnymi. Zakres audytu obejmował zarówno ocenę zgodności formalnej z wymaganiami normy ISO/IEC 27001, jak i weryfikację praktycznego funkcjonowania wybranych procesów i środków kontrolnych. Badanie przeprowadzono w oparciu o podejście oparte na ryzyku, z uwzględnieniem aktualnych zagrożeń i podatności, mogących wpływać na poufność, integralność i dostępność informacji przetwarzanych przez organizację.

Raport przedstawia podsumowanie prac wykonanych w dniach X - X 202X r., polegających na analizie otrzymanej dokumentacji związanej z działalnością i infrastrukturą teleinformatyczną Podmiotu oraz wywiadach z pracownikami [redacted] pod kątem badania zgodności funkcjonowania Podmiotu z wymaganiami zawartymi w normie ISO/IEC 27001.

PRZYKŁADOWY RAPORT

2. Metodyka oceny

Ocena zgodności z normą ISO 27001 została dokonana w następujących krokach:

1) weryfikacja charakteru działalności Podmiotu w odniesieniu do kontekstu organizacji,
2) identyfikacja wymagań norm mających zastosowanie do Podmiotu w świetle jego struktury, zakresu działalności i otoczenia rynkowego,
3) ocena stopnia spełnienia tych wymagań na podstawie analizy dokumentacji, wywiadów oraz obserwacji,
4) przypisanie priorytetu wdrożeniowego dla zaleceń audytowych w celu określenia kolejności i pilności działań naprawczych.

Ocena spełnienia wymagań (zgodnie z punktem 3) została dokonana w skali zdefiniowanej poniżej:

STATUS	OPIS
BRAK ZGODNOŚCI	Stwierdzono brak dokumentów lub zapisów w otrzymanych dokumentach spełniających dane wymaganie. Wywiady audytowe potwierdziły brak realizacji wymagania.
CZĘŚCIOWA ZGODNOŚĆ	Stwierdzono istnienie dokumentów lub zapisów w otrzymanych dokumentach częściowo spełniających dane wymaganie. Wywiady audytowe potwierdziły częściową realizację wymagania.
ZGODNOŚĆ	Stwierdzono istnienie dokumentów lub zapisów w otrzymanych dokumentach spełniających dane wymaganie. Wywiady audytowe potwierdziły realizację wymagania.
BRAK OCENY	Nie dokonano oceny spełnienia wymagania z uwagi na brak wystarczających informacji lub danych.
NIE DOTYCZY	Wymaganie nie ma zastosowania do działalności Podmiotu ze względu na jego charakter, strukturę organizacyjną lub zakres prowadzonej działalności. Nie stwierdzono przesłanek do jego oceny w ramach audytu.

PRZYKŁADOWY RAPORT

PRIOTYTET	OPIS
BARDZO WYSOKI	Stwierdzone niezgodności lub braki mają krytyczny wpływ na zdolność organizacji do zapewnienia bezpieczeństwa informacji, ciągłości działania lub zgodności z wymaganiami regulacyjnymi. Mogą prowadzić do poważnych incydentów lub naruszeń przepisów. Zaleca się rozpoczęcie działań naprawczych w ciągu 2 tygodni od otrzymania zaleceń.
WYSOKI	Stwierdzone niezgodności mają istotny wpływ na zdolność organizacji do zapewnienia bezpieczeństwa informacji, ciągłości działania lub zgodności z wymaganiami regulacyjnymi i mogą zwiększać ryzyko operacyjne lub regulacyjne. Zaleca się rozpoczęcie działań naprawczych w ciągu 1 miesiąca od otrzymania zaleceń.
ŚREDNI	Stwierdzone niezgodności mogą w dłuższej perspektywie wpływać na skuteczność organizacji w zakresie zapewnienia bezpieczeństwa informacji. Zaleca się rozpoczęcie działań naprawczych w ciągu 3 miesięcy od otrzymania zaleceń.
NISKI	Ustalenia o charakterze doskonalącym, nie mające istotnego wpływu na ryzyko, ale mogące przyczynić się do poprawy efektywności, zgodności lub przejrzystości systemu zarządzania. Zaleca się uwzględnienie zaleceń w planach rozwojowych.
NIE DOTYCZY	Nie wskazano zaleceń.

PRZYKŁADOWY RAPORT

3. Zakres wykonanych prac

W dniach X – X przeprowadzono wywiady audytowe mające na celu potwierdzenie prawidłowości zrozumienia przez Audytora działalności Podmiotu, pozyskanie brakujących dokumentów (na bazie analizy wstępnej) i uzyskanie wyjaśnień dotyczących różnych kwestii w zakresie audytowanej materii. Lista osób uczestniczących w audycie znajduje się w rozdziale 5.

Przeprowadzono analizę otrzymanej dokumentacji związanej z organizacją Podmiotu, bezpieczeństwem informacji i środowiskiem teleinformatycznym oraz dodatkowych dokumentów dostarczonych na prośbę Audytora. Łącznie przeanalizowano 77 dokumentów - wykaz znajduje się w rozdziale 6.

Na tej podstawie stworzono niniejszy raport (dalej „Raport").

W Załączniku nr 1 - Formularz audytowy ISO 27002 XXX 202X szczegółowo zaprezentowano wymagania wraz z obserwacjami i zaleceniami Audytora.

Dla wymagań ISO 27001 dokonano opisu obserwacji Audytora („Obserwacje"), przedstawiono stanowisko dotyczące stopnia zgodności („Ocena") zgodnie z metodyką przyjętą w rozdziale 2 oraz zaprezentowano zalecenia dotyczące ewentualnych działań korygujących („Zalecenia").

PRZYKŁADOWY RAPORT

4. Podsumowanie dla Kierownictwa

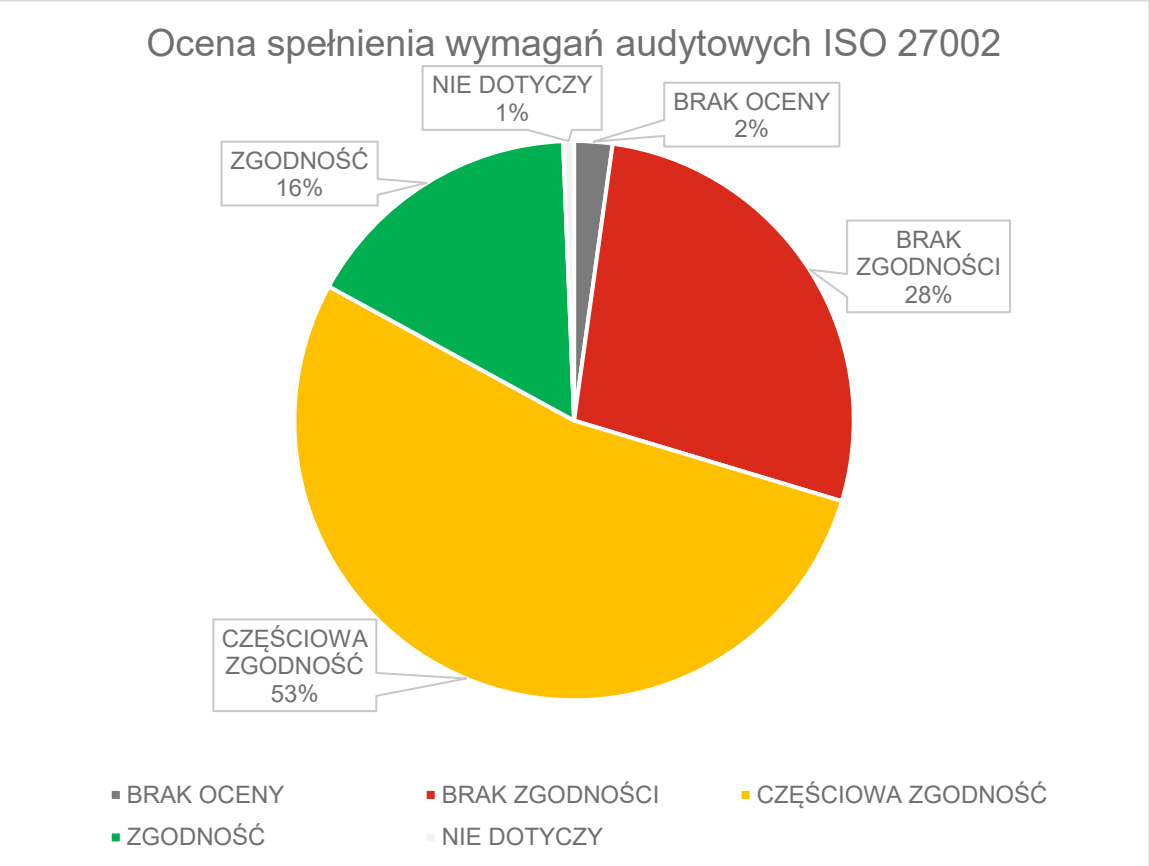
W wyniku przeprowadzonych prac zidentyfikowany został szereg niezgodności lub braków, do których Kierownictwo Podmiotu powinno się odnieść, podejmując decyzje w zakresie dalszego postępowania w obszarze organizacji działalności, dokumentacji, procedur i procesów zapewniających bezpieczeństwo.

W oparciu o przeprowadzone prace zaobserwowano:

- zgodność w **52** pozycjach audytowych,
- częściowa zgodność w **169** pozycjach audytowych,
- całkowity brak zgodności w **87** pozycjach audytowych
- brak możliwości oceny poziomu spełnienia wymagania w **7** pozycjach audytowych,
- **2** pozycje audytowe nie dotyczą Podmiotu.

Pozycja audytowa oznacza pojedynczy wymóg lub logicznie odseparowany fragment wymogu wynikający z normy ISO 27001/27002, który został poddany ocenie w ramach audytu. Odnosi się do jednego punktu normy lub wyodrębnionego fragmentu większego wymagania, o ile możliwe jest jego samodzielne i jednoznaczne ocenienie pod względem zgodności.

Łącznie oceniono **317 pozycji audytowych**, które odpowiadają szczegółowej analizie wszystkich wymagań norm ISO 27002.



PRZYKŁADOWY RAPORT

AUDYTEL

Szczegółowy opis wyników przeprowadzonej analizy przedstawiono w Załączniku nr 1 do niniejszego Raportu.

W toku analizy potwierdzono istnienie podstawowych praktyk związanych z zarządzaniem bezpieczeństwem informacji. Większość wymagań norm została jednak zrealizowana w ograniczonym zakresie lub nie została wdrożona w ogóle. Poniższa tabela przedstawia kluczowe braki, związane z nimi ryzyka oraz ocenę pilności wdrożenia działań korygujących.

L.P.	Obszar braku	Związane ryzyka	Priorytet wdrożenia
1.	[redacted]	[redacted]	Bardzo wysoki
2.	[redacted]	[redacted]	Bardzo wysoki
3.	[redacted]	[redacted]	Bardzo wysoki
4.	[redacted]	[redacted]	Bardzo wysoki
5.	[redacted]	[redacted]	Wysoki
6.	[redacted]	[redacted]	Wysoki
7.	[redacted]	[redacted]	Wysoki

PRZYKŁADOWY RAPORT

L.P.	Obszar braku	Związane ryzyka	Priorytet wdrożenia
8.	[redacted]	[redacted]	Wysoki
9.	[redacted]	[redacted]	Wysoki
10.	[redacted]	[redacted]	Wysoki
11.	[redacted]	[redacted]	Wysoki
12.	[redacted]	[redacted]	Wysoki
13.	[redacted]	[redacted]	Wysoki
14.	[redacted]	[redacted]	Wysoki

PRZYKŁADOWY RAPORT

Zaleca się, aby [redacted]:

- zweryfikował strukturę organizacyjną i ponownie przypisało odpowiedzialności za poszczególne obszary w organizacji, w tym za obszar IT, zarządzanie jakością, utrzymanie SZBI, nadzór nad dokumentacją, zarządzanie uprawnieniami, rejestrowanie zasobów i przeglądy technicznymi, pamiętając o zapewnieniu odpowiedniej separacji ról i obowiązków,
- uzupełnił dokumentację Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z wymaganiami normy ISO/IEC 27002, w tym przede wszystkim należy:
  - [redacted]
- uzupełnił dokumentację Systemu Zarządzania Ciągłością Działania (BCMS) zgodnie z wymaganiami normy ISO/IEC 22301 (zgodnie z zaleceniami ujętymi w Raporcie z audytu BCMS),
- zapewnił regularną aktualizację dokumentacji SZBI oraz wprowadzenie cyklicznych przeglądów polityk i procedur,
- wdrożył techniczne i organizacyjne środki ochrony informacji, w szczególności w zakresie: kontroli kopiowania danych (np. DLP), aktualizacji podatnego serwera, tworzenia kopii zapasowych oraz nadzoru nad dostępem,
- rozważył aktualizację lub zakup serwera,
- rozważył zapewnienie redundancji serwera i kluczowych systemów przetwarzania danych,

PRZYKŁADOWY RAPORT

- przeanalizował i uzupełnił umowy z kluczowymi dostawcami, w tym o zapisy dotyczące poziomów usług (SLA), prawa do audytu oraz obowiązku stosowania polityk bezpieczeństwa obowiązujących w Podmiocie,
- wdrożył i utrzymywał centralny rejestr wszystkich zasobów ICT w Podmiocie,
- wdrożył i utrzymywał centralny rejestr uprawnień w Podmiocie,
- wdrożył i utrzymywał centralny rejestr incydentów w Podmiocie,
- rozważył przechowywanie kopii danych z serwera poza terenem biura,
- rozważył wdrożenie rozwiązania antywirusowego z centralną konsolą zarządzania, umożliwiającego nadzór nad stacjami roboczymi.

Szczegóły dotyczące wdrożenia zaleceń znajdują się w załączniku 1 do niniejszego Raportu.

Wdrożenie wymienionych powyżej działań nie będzie wystarczające do spełnienia wszystkich wymagań ISO 27001/27002 – po wykonaniu najpilniejszych prac należy sukcesywnie wdrażać pozostałe zalecenia zawarte w załączniku 1 do niniejszego Raportu.

Podmiot nie jest zobligowany przepisami prawa do certyfikacji zgodności z normą ISO/IEC 27001/27002, jednak biorąc pod uwagę skalę przetwarzania informacji, zależność od zasobów informacyjnych oraz rosnące wymagania klientów i interesariuszy w zakresie bezpieczeństwa informacji, konieczne jest rozwijanie SZBI jako filaru odporności operacyjnej i zaufania rynkowego.

PRZYKŁADOWY RAPORT

5. Strony uczestniczące w audycie

Przedstawiciele Podmiotu audytowanego

L.P.	IMIĘ I NAZWISKO	OBSZAR
1.	[redacted]	Wsparcie IT
2.	[redacted]	Zarząd [redacted]
3.	[redacted]	Chief Information Security Officer,
4.	[redacted]	Administracja, HR
5.	[redacted]	Zabezpieczenia fizyczne
6.	[redacted]	Audyt wewnętrzny

Audytorzy

L.P.	FUNKCJA AUDYTOWA	IMIĘ I NAZWISKO	POTWIERDZENIE KWALIFIKACJI
1.	Audytor Wiodący		
2.	Audytor Pomocniczy		
3.	Audytor Pomocniczy		

PRZYKŁADOWY RAPORT

6. Wykaz otrzymanych dokumentów do analizy audytowej

7. Załączniki

1) Załącznik nr 1 - Formularz audytowy ISO 27001 [redacted] 202X zawierający szczegółowe ustalenia
2) Załącznik nr 2 – Harmonogram działań poaudytowych

PRZYKŁADOWY RAPORT

Załącznik nr 1 - Formularz audytowy ISO 27001 XXX 202X zawierający szczegółowe ustalenia audytowe (FRAGMENTY)

Nr kontroli	Nazwa zabezpieczenia	Sposób weryfikacji	Obserwacje	Ocena spełnieni	Priorytet	Zalecenia
A.5.1	**Główna polityka bezpieczeństwa**	Wywiad/ Dokumentacja	[redacted]	CZĘŚCIOWA ZGODNOŚĆ	Wysoki	[redacted]
A.5.1	**Treść polityki głównej**	Dokumentacja	[redacted]	CZĘŚCIOWA ZGODNOŚĆ	Wysoki	[redacted]
A.5.1	**P lityki szcz ółowe**	Dokumentacja	[redacted]	CZĘŚCIOWA ZGODNOŚĆ	Wysoki	[redacted]
A.5.1	**Przypisanie odpowiedzialności**	Wywiad	[redacted]	CZĘŚCIOWA ZGODNOŚĆ	Wysoki	[redacted]

PRZYKŁADOWY RAPORT

A.5.1	**Okresowy przegląd polityki**	Wywiad/ Dokumentacja	[redacted]	**BRAK ZGODNOŚCI**	**Wysoki**	[redacted]
A.5.1	**Spójność i aktualizacja**	Wywiad	[redacted]	**BRAK ZGODNOŚCI**	**Wysoki**	[redacted]
A.5.1	**Komunikacja zasad**	Wywiad	[redacted]	**CZĘŚCIOWA ZGODNOŚĆ**	**Średni**	[redacted]
..	**……**	……	……..	**……**	**……..**	……..
A.7.11	**Zabezpieczenia awaryjne i dane kontaktowe**	Wywiad	[redacted]	**ZGODNOŚĆ**	**Nie dotyczy**	Brak.
A.7.12	**Bezpieczeństwo okablowania**	Wywiad	[redacted]	**CZĘŚCIOWA ZGODNOŚĆ**	**Średni**	[redacted]

PRZYKŁADOWY RAPORT

A.7.13	**Konserwacja sprzętu**	Wywiad/Dokumentacja	[redacted]	**CZĘŚCIOWA ZGODNOŚĆ**	**Niski**	[redacted]
A.7.14	**Weryfikacja nośników przed usunięciem lub ponownym użyciem**	Wywiad/Dokumentacja	[redacted]	**ZGODNOŚĆ**	**Nie dotyczy**	Brak.
A.7.14	**Bezpieczne niszczenie nośników zawierających dane poufne**	Wywiad/Dokumentacja	[redacted]	**ZGODNOŚĆ**	**Nie dotyczy**	Brak.
A.7.14	**Usuwanie etykiet i oznaczeń przed przekazaniem sprzętu**	Wywiad/Dokumentacja	[redacted]	**BRAK ZGODNOŚCI**	**Niski**	[redacted]

PRZYKŁAD

A.8.1	**Zasady zarządzania urządzeniami końcowymi użytkowników**	Dokumentacja	[redacted]	**CZĘŚCIOWA ZGODNOŚĆ**	**Wysoki**	
A.8.1	**Ograniczony dostęp do informacji na urządzeniach końcowych**	Wywiad	[redacted]	**CZĘŚCIOWA ZGODNOŚĆ**	**Średni**	[redacted]

PRZY

Załącznik nr 2 – Harmonogram działań poaudytowych (propozycja)

L.P.	Obszar braku	Działania na podstawie rekomendacji
1.	[redacted]	[redacted]
2.	[redacted]	[redacted]
3.	[redacted]	[redacted]
4.	[redacted]	[redacted]
5.	[redacted]	[redacted]
6.	[redacted]	[redacted]
7.	[redacted]	[redacted]
8.	[redacted]	[redacted]

PRZYKŁADOWY RAPORT

L.P.	Obszar braku	Działania na podstawie rekomendacji
9.	[redacted]	[redacted]
10.	[redacted]	[redacted]
11.	[redacted]	[redacted]
12.	[redacted]	[redacted]
13.	[redacted]	[redacted]
14.	[redacted]	[redacted]

PRZYKŁADOWY RAPORT

PRIORYTETYZACJA KLUCZOWYCH DZIAŁAŃ:

Z uwagi na możliwości organizacji zaleca się model sekwencyjny – tj. wdrażanie zaleceń fazami. Jeżeli faza 1 zostanie ukończona wcześniej, należy niezwłocznie podjąć następne działania zgodnie z kolejnymi fazami.

Faza 1 (Pilne - 0-4 tydzień)

- [redacted]
- [redacted]
- [redacted]

Faza 2 (Wysoki priorytet - 4-14 tydzień)

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Faza 3 (Średni priorytet - 8-20 tydzień)

- [redacted]
- [redacted]

Długoterminowy projekt – rozpocząć niezwłocznie; pełne wdrożenie potrwa 39 tygodni)

- [redacted]

PRZYKŁADOWY RAPORT