RAPORT Z AUDYTU ZGODNOŚCI Z ISO/IEC 27001

dla

xxx

Przygotował:

Audytel S.A.

Wersja 1.0 z dnia X

SPIS TREŚCI

1. Wstęp

Niniejszy raport przedstawia wyniki prac audytorskich realizowanych przez audytorów w ramach umowy z dnia ……. pomiędzy Audytel S.A. a xxxxxx. 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 XXX pod kątem badania zgodności funkcjonowania Podmiotu z wymaganiami zawartymi w normie ISO/IEC 27001.

Zastrzeżenie: Wyniki audytu przedstawione w raporcie podawane są na podstawie analizy pozyskanego w czasie czynności audytowych materiału dowodowego. Audyt prowadzony jest na określonej przez audytora próbie audytowej i uzyskane dowody audytowe na dzień przeprowadzenia audytu są podstawą do określenia poziomu zgodności realizacji wymagań prawnych i obowiązujących standardów stosowanych przez organizację.

Ocena audytowa stanowi obiektywne, zgodne z materiałem dowodowym oraz stanowiskiem zespołu audytowego wynikającym z jego doświadczenia, wiedzy i uprawnień, określenie poziomu spełnienia wymagań i kryteriów opisanych celem audytowym. Ocena audytowa stanowi jedynie wskazanie potencjalnej drogi rozwoju i doskonalenia organizacji na podstawie ostatecznej decyzji Najwyższego Kierownictwa.

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.

Skalę priorytetu wdrażania zaleceń (zgodnie z punktem 4) zdefiniowano poniżej:

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.

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").

4. Podsumowanie dla Kierownictwa

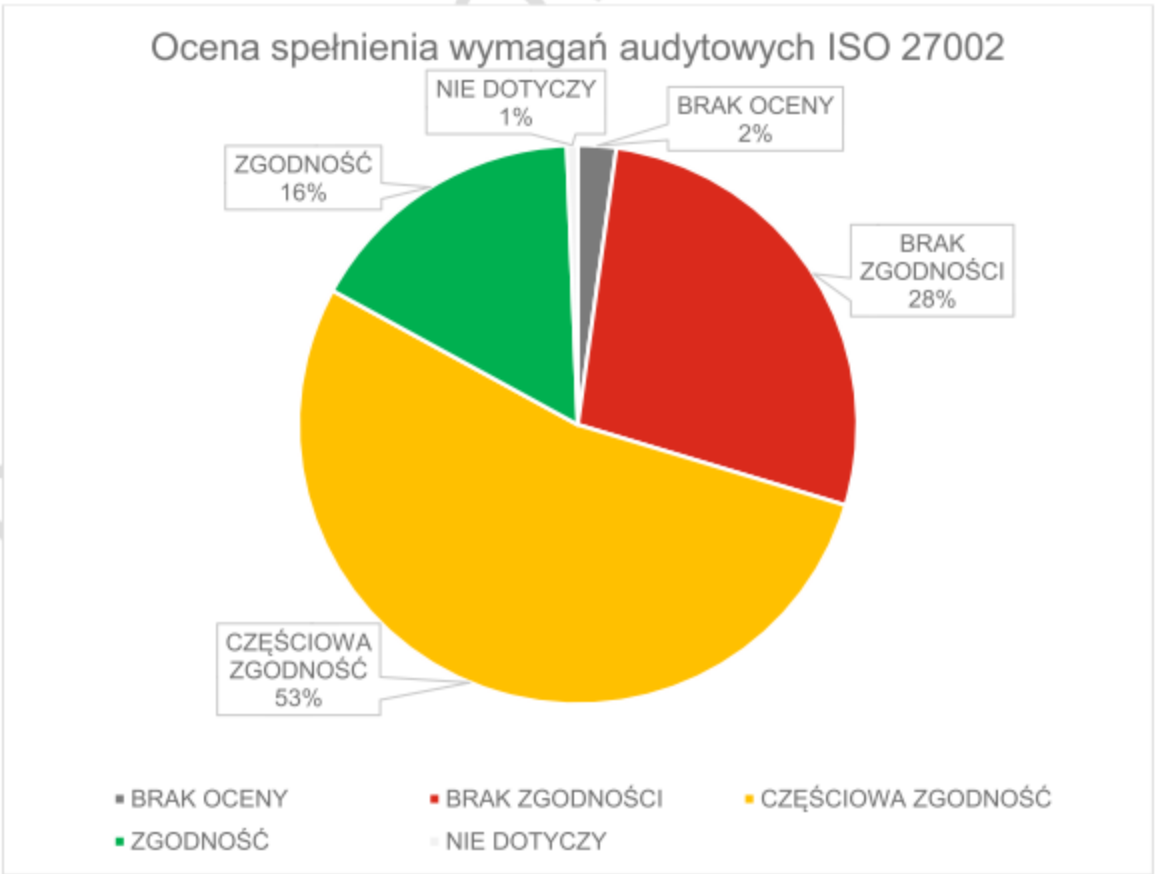
W wyniku przeprowadzonych prac zidentyfikowany został szereg niezgodności lub braków, do których Kierownictwo Podmiotu powinno się odnieść, podejmując decyzje w zakresie dalszego postępowania w obszarze organizacji działalności, dokumentacji, procedur i procesów zapewniających bezpieczeństwo.

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.



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.	Znaczące braki w dokumentacji zarządzania ciągłością działania – w zakresie Polityki Ciągłości Działania, analizy BIA, planów BCP/DRP (ISO 5.29, 5.30)	Ryzyko braku gotowości organizacji do reagowania na zakłócenia; brak wiedzy o krytycznych procesach i zasobach; nieskuteczna reakcja na incydenty i brak możliwości odtworzenia działalności w akceptowalnym czasie.	**Bardzo wysoki**
2.	Brak centralnego rejestru zasobów ICT (ISO 27002 5.9, 5.12, 5.14)	Niemożność skutecznego zarządzania zasobami i ryzykami; utrudnione wykrywanie nieautoryzowanych zmian; brak podstawy do skutecznej klasyfikacji zasobów i przypisania odpowiedzialności.	**Bardzo wysoki**
3.	Niezaktualizowany, podatny na zagrożenia serwer (ISO 27002 5.30)	Wysokie ryzyko podatności na znane ataki; możliwość eskalacji incydentów; potencjalne naruszenie poufności, integralności i dostępności danych.	**Bardzo wysoki**
4.	Brak przypisanych ról i obowiązków dotyczących utrzymania systemu SZBI (ISO 27002 5.1, 5.2)	Brak odpowiedzialności za kluczowe elementy SZBI; niespójność w zarządzaniu ryzykiem, incydentami i zmianami; utrata ciągłości działań i nadzoru nad systemem.	**Bardzo wysoki**
5.	Nieaktualna dokumentacja i brak cyklicznych przeglądów dokumentacji SZBI (ISO 27002 5.1)	Brak zgodności z wymaganiami normy, trudność w wykazaniu spełnienia wymagań regulatorów lub audytorów; ryzyko stosowania nieaktualnych procedur i błędnego postępowania w sytuacjach incydentów.	**Wysoki**
6.	Niepełna dokumentacja w obszarze bezpieczeństwa informacji, szczególnie na poziomie proceduralnym (ISO 27002 5.2, 5.12, 5.14, 5.15, 5.17, 5.22, 5.24, 5.25, 5.26, 5.27, 5.28, 5.31, 5.32, 5.33, 5.34, 5.36, 6.1, 6.4, 6.5, 6.6, 6.7, 6.8, 7.10, 7.12, 8.1, 8.2, 8.3, 8.4, 8.7, 8.9, 8.10, 8.11, 8.12, 8.13, 8.14, 8.15, 8.16, 8.17, 8.18,	Niska spójność działań operacyjnych; niejednolite podejście do zabezpieczeń; trudność w szkoleniu pracowników i egzekwowaniu wymagań; ryzyko nieświadomych naruszeń.	**Wysoki**

L.P.	Obszar braku	Związane ryzyka	Priorytet wdrożenia
	8.19, 8.20, 8.21, 8.24, 8.25, 8.26, 8.27, 8.28, 8.29, 8.30, 8.31, 8.32, 8.33, 8.34)		
7.	Brak wdrożonych zabezpieczeń przed wyciekami danych: brak DLP, nadzorowania nośników wymiennych (ISO 27002 5.11, 8.12)	Ryzyko nieautoryzowanego wycieku danych; brak kontroli nad przenoszeniem informacji poufnych; zwiększone ryzyko incydentów wewnętrznych.	Wysoki
8.	Brak centralnego rejestru uprawnień (ISO 27002 5.10)	Ryzyko nadania nadmiernych lub nieaktualnych uprawnień; brak możliwości szybkiego cofnięcia dostępu; trudność w przeprowadzeniu przeglądów dostępów.	Wysoki
9.	Brak kopii danych z serwera poza lokalizacją firmy (ISO 27002 8.13)	Ryzyko całkowitej utraty danych w przypadku awarii lub katastrofy lokalnej; brak możliwości odtworzenia danych w innym środowisku; ryzyko niespełnienia wymagań RTO i RPO.	Wysoki
10.	Umowa z AAA niezgodna z politykami bezpieczeństwa – brak SLA, prawa do audytu, zobowiązania dostawcy do stosowania się do polityk firmy (ISO 27002 5.20, 5.22)	Ryzyko braku możliwości egzekwowania wymagań bezpieczeństwa; niska przejrzystość współpracy; brak kontroli nad poziomem usług i reakcją na incydenty po stronie dostawcy.	Wysoki
11.	Brak redundantnej architektury w kluczowych obszarach infrastruktury IT (serwery, systemy, aplikacje) (ISO 27002 8.14)	Wysokie ryzyko niedostępności usług; możliwość zakłócenia ciągłości działania; potencjalne naruszenie dostępności i niezawodności kluczowych systemów.	Wysoki
12.	Brak skutecznych zabezpieczeń przed zagrożeniami z nośników zewnętrznych i sieci publicznych (ISO 27002 7.10, 8.7)	Wysokie ryzyko infekcji złośliwym oprogramowaniem; możliwość obejścia zabezpieczeń podczas prac serwisowych; potencjalne osłabienie poziomu ochrony i zwiększenie powierzchni ataku.	Wysoki
13.	Brak centralnego rejestru incydentów (ISO 27002 5.24, 5.26)	Niska skuteczność analizy przyczyn i trendów; ryzyko pominięcia incydentów; utrudniona koordynacja reakcji; brak dokumentacji dla celów dowodowych i zgodności regulacyjnej.	Wysoki
14.	Brak monitorowania stacji roboczych (ISO 27002 5.7, 8.16)	Brak bieżącej analizy aktywności użytkowników i wykrywania anomalii; ograniczona zdolność do identyfikacji nadużyć, naruszeń bezpieczeństwa i nieautoryzowanych działań; opóźnienia w reagowaniu na incydenty; trudności w zapewnieniu zgodności z polityką bezpieczeństwa.	Wysoki

Zaleca się, aby XXX:

- 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:
    - opracować procedury bezpieczeństwa podczas konserwacji i działań awaryjnych,
    - rozszerzyć zapisy polityki zarządzania zasobami,
    - rozszerzyć zapisy polityki zarządzania ryzykiem (co najmniej o aspekt ryzyka rezydualnego),
    - opisać proces wydawania i odbierania urządzeń i kart dostępu oraz środki bezpieczeństwa stosowane w tym procesie,
    - uwzględnić wymagania dotyczące poufności, integralności i dostępności w dokumencie klasyfikacji informacji,
    - rozszerzyć dokumentację dotyczącą kopii zapasowych co najmniej o harmonogram kopii zapasowych,
    - opisać stosowane środki bezpieczeństwa w zakresie zapewniania niezawodności i dostępności,
    - rozszerzyć zapisy dotyczące bezpieczeństwa poczty elektronicznej,
    - rozszerzyć dokumentację w obszarze kontroli dostępu, szczególnie w obszarze ról i segregacji obowiązków w procesie oraz zapisy dotyczące weryfikacji użytkownika przed nadaniem mu nowych/zmodyfikowanych dostępów,
    - opisać proces wyboru dostawców, w tym dostawców chmurowych,
    - dostosować i wdrożyć procedurę obsługi incydentów,
    - uzupełnić politykę bezpieczeństwa informacji o szczegółowe zapisy dotyczące zarządzania wymiennymi nośnikami danych, w tym o zasady rejestracji i zatwierdzania nośników, bezpiecznego przechowywania nośników, szyfrowania nośników i transportu fizycznego nośników,
    - określić wymagania bezpieczeństwa dotyczące oprogramowania i jego aktualizacji,
    - rozszerzyć politykę dotyczącą pracy na urządzeniach prywatnych (BYOD) o zasady bezpieczeństwa,
    - opisać zasady bezpiecznej konfiguracji w zakresie sieci i urządzeń,
    - dodać zapisy dotyczące bezpieczeństwa logów,
    - dodać zapisy dotyczące synchronizacji czasu.
- 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,
- 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.

5. Strony uczestniczące w audycie

Przedstawiciele Podmiotu audytowanego

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

Audytorzy

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

6. Wykaz otrzymanych dokumentów do analizy audytowej

1) Polityka Bezpieczeństwa Informacji
2) Procedura zarządzania incydentami bezpieczeństwa
3) Rejestr zasobów ICT
4) Rejestr uprawnień użytkowników
5) Analiza ryzyka bezpieczeństwa informacji
6) Rejestr incydentów bezpieczeństwa
7) Procedura tworzenia i odtwarzania kopii zapasowych
8) Procedura zarządzania dostępem
9) Procedura klasyfikacji informacji i zasobów
10) Plan ciągłości działania (BCP)
11) Raport z testów podatności i analiz technicznych
12) Procedura przeglądu dokumentacji SZBI
13) Rejestr szkoleń z zakresu bezpieczeństwa informacji
14) Umowy z dostawcami zawierające postanowienia bezpieczeństwa
15) Procedura onboardingu i offboardingu pracowników
16) Regulamin pracy zdalnej i BYOD
17) Instrukcja bezpiecznej konfiguracji urządzeń końcowych
18) Instrukcja zarządzania nośnikami wymiennymi
19) Harmonogram przeglądów SZBI
20) Deklaracja zgodności z wymaganiami ISO/IEC 27001

7. Załączniki

1) Załącznik nr 1 - Formularz audytowy ISO 27001 XXX 202X zawierający szczegółowe ustalenia
2) Załącznik nr 2 – Harmonogram działań po audytowych

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

Nr kontroli	Nazwa zabezpieczenia	Sposób weryfikacji	Obserwacje	Ocena spełnienia	Priorytet	Zalecenia
A.5.1	**Główna polityka bezpieczeństwa**	Wywiad/ Dokumentacja	[redacted]	CZĘŚCIOWA ZGODNOŚĆ	Wysoki	[redacted]
A.5.1	**Treść polityki głównej**	Dokumentacja		CZĘŚCIOWA ZGODNOŚĆ	Wysoki	
A.5.1	**Polityki szczegółowe**	Dokumentacja		CZĘŚCIOWA ZGODNOŚĆ	Wysoki	

A.5.1	**Przypisanie odpowiedzialności**	Wywiad		CZĘŚCIOWA ZGODNOŚĆ	Wysoki
A.5.1	**Okresowy przegląd polityki**	Wywiad/ Dokumentacja		BRAK ZGODNOŚCI	Wysoki
A.5.1	**Spójność i aktualizacja**	Wywiad		BRAK ZGODNOŚCI	Wysoki
A.5.1	**Komunikacja zasad**	Wywiad		CZĘŚCIOWA ZGODNOŚĆ	**Średni**
..	.....	.....		.....	.....

A.7.11	**Zabezpieczenia awaryjne i dane kontaktowe**	Wywiad	[redacted]	ZGODNOŚĆ	Nie dotyczy	[redacted]
A.7.12	**Bezpieczeństwo okablowania**	Wywiad	[redacted]	CZĘŚCIOWA ZGODNOŚĆ	Średni	[redacted]
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	[redacted]
A.7.14	**Bezpieczne niszczenie nośników zawierających dane poufne**	Wywiad/Dokumentacja	[redacted]	ZGODNOŚĆ	Nie dotyczy	[redacted]

A.7.14	**Usuwanie etykiet i oznaczeń przed przekazaniem sprzętu**	Wywiad/Dokumentacja	[illegible]	**BRAK ZGODNOŚCI**	**Niski**
A.8.1	**Zasady zarządzania urządzeniami końcowymi użytkowników**	Dokumentacja	[illegible]	**CZĘŚCIOWA ZGODNOŚĆ**	**Wysoki**
A.8.1	**Ograniczoi. dostęp do informacji na urządzeniach końcowych**	Wywiad	[illegible]	**CZĘŚCIOWA ZGODNOŚĆ**	**Średni**

Załącznik nr 2 – Harmonogram działań poaudytowych (propozycja)

L.P.	Obszar braku	Działania na podstawie rekomendacji
1.	Znaczące braki w dokumentacji zarządzania ciągłością działania – w zakresie Polityki Ciągłości Działania, analizy BIA, planów BCP/DRP (ISO 27002 5.29, 5.30)	Wdrożenie działań zgodnie z zaleceniami audytu zgodności z normą ISO 22301
2.	Brak centralnego rejestru zasobów ICT (ISO 27002 5.9, 5.12, 5.14)	[redacted]
3.	Niezaktualizowany, podatny na zagrożenia serwer (ISO 27002 5.30)	
4.	Brak przypisanych ról i obowiązków dotyczących utrzymania systemu SZBI (ISO 27002 5.1, 5.2)	
5.	Nieaktualna dokumentacja i brak cyklicznych przeglądów dokumentacji SZBI (ISO 27002 5.1)	
6.	Niepełna dokumentacja w obszarze bezpieczeństwa informacji, szczególnie na poziomie proceduralnym (ISO 27002 5.2, 5.12, 5.14, 5.15, 5.17, 5.22, 5.24, 5.25, 5.26, 5.27, 5.28, 5.31, 5.32, 5.33, 5.34, 5.36, 6.1, 6.4, 6.5, 6.6, 6.7, 6.8, 7.10, 7.12, 8.1, 8.2, 8.3, 8.4, 8.7, 8.9, 8.10, 8.11, 8.12, 8.13, 8.14, 8.15, 8.16, 8.17, 8.18, 8.19, 8.20, 8.21, 8.24, 8.25, 8.26, 8.27, 8.28, 8.29, 8.30, 8.31, 8.32, 8.33, 8.34)	

L.P.	Obszar braku	Działania na podstawie rekomendacji
7.	Brak wdrożonych zabezpieczeń przed wyciekami danych: brak DLP, nadzorowania nośników wymiennych (ISO 27002 5.11, 8.12)	
8.	Brak centralnego rejestru uprawnień (ISO 27002 5.10)	
9.	Brak kopii danych z serwera poza lokalizacją firmy (ISO 27002 8.13)	
10.	Umowa z AAA niezgodna z politykami bezpieczeństwa – brak SLA, prawa do audytu, zobowiązania dostawcy do stosowania się do polityk firmy (ISO 27002 5.20, 5.22)	
11.	Brak redundantnej architektury w kluczowych obszarach infrastruktury IT (serwery, systemy, aplikacje) (ISO 27002 8.14)	
12.	Brak skutecznych zabezpieczeń przed zagrożeniami z nośników zewnętrznych i sieci publicznych (ISO 27002 7.10, 8.7)	
13.	Brak centralnego rejestru incydentów (ISO 27002 5.24, 5.26)	
14.	Brak monitorowania stacji roboczych (ISO 27002 5.7, 8.16)	

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)

- [illegible]
- [illegible]
- [illegible]

Faza 2 (Wysoki priorytet - 4-14 tydzień)

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Faza 3 (Średni priorytet - 8-20 tydzień)

- [illegible]
- [illegible]

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

- [illegible]