Laboratorium Zdalne – Audyt bezpieczeństwa

Przykładowe zagadnienia w audycie systemu IT:

	Zagadnienie	Tak	Nie	Uwagi
1	**Bezpieczeństwo osobowe, uprawnienia do dostępu do IN przetwarzanych w systemie**.			
1.	Czy w jednostce organizacyjnej wyznaczone zostały osoby formalnie odpowiedzialne za zapewnienie funkcjonowania i bezpieczeństwa systemu TI?			
2.	Czy osoby odpowiedzialne w jednostce organizacyjnej za ochronę IN przetwarzanych w systemie TI mają określone zakresy zadań i odpowiedzialności?			
3.	Czy użytkownicy systemu TI posiadają aktualne poświadczenia bezpieczeństwa lub inne formalne uprawnienia dostępu do IN przetwarzanych w systemie?			
4.	Czy wszyscy użytkownicy systemu Ti posiadają ważne zaświadczenia o odbyciu szkolenia w zakresie ochrony IN zgodnie z art. 19 UOIN?			
5.	Czy administrator systemu i inspektor BTI odbyli specjalistyczne szkolenia w zakresie bezpieczeństwa teleinformatycznego, zgodnie z art. 52 ust. 4 UOIN?			
6.	Czy przed dopuszczeniem do pracy w systemie Ti użytkownicy odbyli szkolenie w zakresie zasad bezpiecznego funkcjonowania systemu oraz praktycznego stosowania procedur bezpiecznej eksploatacji?			
7.	Czy w jednostce organizacyjnej prowadzone są okresowe (dodatkowe) szkolenia związane z podnoszeniem świadomości użytkowników systemu TI w zakresie zagrożeń BTI oraz szkolenia związane z obsługą wykorzystywanych w systemie aplikacji, stosowanych środków ochrony fizycznej (kontrola dostępu, SSWiN, telewizja dozorowa), procedur zapewnienia ciągłości działania, itp.?			
8.	Czy użytkownicy systemu Ti potwierdzili fakt zapoznania się i zrozumienia procedur bezpiecznej eksploatacji systemu (PBE)?			
9.	Czy w przypadku zwolnienia z pracy/służby użytkownika systemu TI blokowana jest skutecznie możliwość dostępu do systemu Ti?			
10.	Czy w przypadku zwolnienia z pracy/służby stosowana jest zasada całkowitego rozliczenia użytkownika systemu Ti z posiadanych zasobów? *Uwaga: wymaganie dotyczy przykładowo rozliczenia z posiadanych sprzętów tokenów uwierzytelniających, kluczy, kart identyfikacyjnych, przepustek, itp.?*			
11.	Czy w przypadku zwolnienia z pracy/służby stosowana jest zasada całkowitego rozliczenia użytkownika systemu Ti z posiadanych zasobów?			
12.	Czy w przypadku przeniesienia na inne stanowisko lub zmiany zakresu zadań realizowanych przez użytkownika systemu Ti przeglądane i weryfikowane są uprawnienia dostępu fizycznego i logicznego do informacji/usług/zasobów systemowych?			
13.	Czy określone zostały zasady podejmowania decyzji w sprawie dalszego wykorzystywania zasobów informacyjnych będących w posiadaniu zwalnianych lub przenoszonych na inne stanowiska pracowników lub i ich usunięcia z systemu TI?			

14.	Czy przestrzegane są zasady prowadzenia i aktualizowania listy uprawnionych użytkowników systemu TI?			
15.	Czy przestrzegane są wymogi w zakresie bezpieczeństwa osobowego związane z dostępem do systemu Ti osób niebędących użytkownikami systemu? *Uwaga: dotyczy serwisu biurowego, pracowników, dostawców lub firm odpowiedzialnych za utrzymywanie lub rozwój systemu, dostawców oprogramowania i systemów aplikacyjnych, itp.*			
2	**Bezpieczeństwo fizyczne systemu**			
1.	Czy prawidłowo dobrano rodzaj strefy ochronnych i ich lokalizacje dla poszczególnych elementów systemu?			
2.	Czy formalnie wyznaczone strefy ochronne są zgodne z oposem w SWB?			
3.	Czy strefy ochronne(z uwzględnieniem drzwi, okien, otworów wentylacyjnych, włazów, świetlików itp.) zabezpieczone są pod względem budowalnym i mechanicznym zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa?			
4.	Czy okna w strefach ochronnych zabezpieczone są przed podglądem z zewnątrz w warunkach dziennych i nocnych?			
5.	Czy wszystkie wejścia do strefy ochronnej zabezpieczone są przez systemy kontroli dostępu?			
6.	Czy prawidłowo eksploatowany jest system SWiN zabezpieczający strefy ochronne?			
7.	Czy prawidłowo działa system dozoru CCTV, czy rejestry są właściwie zabezpieczone i przechowywane przez okres umożlwiający odtworzenie zdarzeń w przypadku wykrycia incydentu bezpieczeństwa?			
8.	Czy strefy ochronne zabezpieczone są przy pomocy sytemu alarmu pożarowego, zgodnie z obowiązującymi przepisami ppoż. oraz zapisami zawartymi w SWB?			
9.	Czy do strefy ochronnych wprowadzona została kontrola wnoszonego i wynoszonego sprzętu?			
10.	Czy okablowanie (informacyjne i zasilające) systemu Ti jest zabezpieczone zgodnie z zapisami zawartymi w SWB?			
11.	Czy elementy systemów wspomagających pracę systemu Ti (zasilanie, klimatyzacja, monitoring, temperatury, wilgotność, zalania itp.) gwarantują ciągłą pracę systemu zgodnie z zapisami zawartymi w SWB?			
12.	Czy zasady zarządzania dostępem fizycznym(nadawanie / blokowanie upoważnień do wejścia) do stref ochronnych są zgodne z zapisami zawartymi w SWB?			
13.	Czy listy dostępu do stref ochronnych są przeglądane i aktualizowane zgodnie z zasadami zwartymi w SWB?			
14.	Czy prowadzona jest weryfikacja osób wchodzących do strefy ochronnych?			
15.	Czy prowadzona jest rejestracja osób wchodzących do stref ochronnych?			
16.	Czy przyznawanie /odbieranie środków kontroli dostępu fizycznego(klucze, karty, kody, hasła itp.) do stref ochronnych prowadzone jest zgodnie z zapisami zawartymi w SWB?			
17.	Czy ustawienia środków kontroli dostępu do stref ochronnych (kody, hasła, PIN-y) są zmieniane zgodnie z zapisami zawartymi w SWB?			
3	**Ochrona elektromagnetyczna**			
1.	Czy zaszły jakieś zmiany w otoczeniu systemu Ti, które mogą mieć wpływ na wyznaczoną sprzętową strefę ochrony elektromagnetycznej (SSOE)?			
2.	Czy urządzenia systemu Ti posiadają aktualne certyfikaty ochrony elektromagnetycznej?			
3.	Czy wdrożone środki ochrony elektromagnetycznej eksploatowane są zgodnie z dokumentacją bezpieczeństwa			

	systemu Ti i wymaganiami wynikającymi z posiadanych certyfikatów?			
4	**Urządzenia i narzędzia kryptograficzne** *Uwaga: dotyczy tylko systemów teleinformatyczny, w których transmisja informacji niejawnych odbywa się pomiędzy strefami ochronnymi.*			
1.	Czy system Ti chroni poufność przesyłanych informacji przy pomocy certyfikowanych urządzeń lub narzędzi kryptograficznych?			
2.	Czy ustawienia konfiguracyjne i ukompletowanie urządzeń kryptograficznych jest zgodne z SWB?			
3.	Czy ważne są certyfikaty ochrony kryptograficznej urządzeń i narzędzi kryptograficznych wykorzystywanego w systemie TI?			
4.	Czy w systemie używa się mechanizmów kryptograficznych do wykrywania zmian w przesyłanych informacjach dokonanych podczas transmisji poza strefy ochronne? *Uwaga: dotyczy tylko sieci, kiedy z analizy ryzyka wynika, iż aspekt integralności ma krytyczne znaczenie oraz tylko takich sieci, które wymieniają informację miedzy elementami systemu przy pomocy łączy publicznych(zabezpieczonych kryptograficznie)*			
5.	Czy wykorzystywane są mechanizmy kryptograficzne do zapobiegania nieautoryzowanemu ujawnieniu i modyfikacji przechowywanych na nośnikach informacji niejawnych, o ile nie są one chronione przez zabezpieczenia fizyczne?			
6.	Czy generacja i dystrybucja kluczy kryptograficznych używanych w systemie TI odbywa się zgodnie z SWB? *Uwaga: generacja i zarządzanie kluczami kryptograficznymi może być wykonywane „ręcznie”(bezpieczne dystrybucja kluczy na specjalnych nośnikach) lub przy użyciu zautomatyzowanych mechanizmów wspartych stosowanymi procedurami.*			
7.	Czy urządzenia kryptograficzne są w odpowiedni sposób oznakowane i zabezpieczone plombami?			
8.	Czy ewidencja materiałów kryptograficznych prowadzona jest zgodnie z dokumentacją bezpieczeństwa systemu Ti?			
9.	Czy materiały kryptograficzne (karty, moduły uwierzytelniające, hasła, PIN-kody, itp.) są odpowiednio zabezpieczone i zdeponowane w bezpiecznym miejscu?			
10.	Czy zapewniona jest dostępność informacji w przypadku utraty kluczy kryptograficznych przez użytkowników?			
11.	Czy niszczenie, wycofywanie z użycia materiałów kryptograficznych odbywa się zgodnie z dokumentacją bezpieczeństwa systemu Ti?			
5	**Ciągłości działania, kopie zapasowa, alternatywne łącza, urządzenia, zasilanie awaryjne**			
1.	Czy aktualny jest wykaz osób odpowiedzialnych w jednostce za ciągłość działania systemu Ti i czy aktualne są ich dane kontaktowe?			
2.	Czy osoby odpowiedzialne za realizację planu ciągłości działania zostały przeszkolone w zakresie ich zadań zgodnie z zaplanowaną częstotliwością			
3.	Czy plan ciągłości działania systemu jest testowany i aktualizowany zgodnie z wymogami opisanymi w SWB?			
4.	Czy kopie zapasowe danych systemu Ti są tworzone i przechowywane zgodnie za zasadami opisanymi w SWB?			
5.	Czy tworzone i właściwie przechowywane są kopie zapasowe systemów operacyjnych, oprogramowania krytycznego dla systemu, łącznie z kopiami spisu elementów systemu oraz kopiami dokumentacji i bezpieczeństwa systemu?			
6.	Czy wprowadzone i testowane są mechanizmy umożliwiające odzyskanie danych i rekonstrukcje systemu do pierwotnego			

	stanu po zakłóceniu, awarii lub innym incydencie bezpieczeństwa TI?			
7.	Czy testowane są kpie zapasowa (ze zdefiniowaną przez jednostkę częstotliwością)?			
8.	Czy zabezpieczono rządzenia (system) zasalania awaryjnego?			
9.	Czy zabezpieczono alternatywne łącza telekomunikacyjne?			
6	**Ustawienia konfiguracyjne systemu i urządzeń, zarządzanie konfiguracją**			
1.	Czy konfiguracja systemu Ti jest zgodna z opisem w SWB?			
2.	Czy osoby odpowiedzialne za zarządzanie konfiguracją systemu znają i wypełniają prawidłowo swoje obowiązki?			
3.	Czy zasady i procedury aktualizowania bezpiecznej konfiguracji systemu Ti są przestrzegane?			
4.	Czy przechowywane są starsze wersje bezpiecznej konfiguracji systemu TI?			
5.	Czy w systemie TI określona została lista oprogramowania (operacyjnego, aplikacyjnego i narzędziowego) dopuszczonego do wykorzystywania?			
6.	Czy określone zostały rodzaje zmian konfiguracji, które muszą zostać odnotowane w dokumentacji bezpieczeństwa systemu TI?			
7.	Czy są testowane i oceniane pod kątem wpływu na funkcjonowanie i bezpieczeństwo systemu TI planowane do wprowadzenia zmian?			
8.	Czy jednostka organizacyjna analizuje nowe oprogramowanie w wydzielonym środowisku testowy przed uruchomienie w środowisku operacyjnym TI?			
9.	Czy w systemie TI wdrożono zakaz wykorzystywania przez użytkowników wszelakich nieautoryzowanych (w tym także prywatnych) urządzeń elektronicznych, nośników i oprogramowania oraz czy jest on respektowany?			
10.	Czy konfiguracja systemu Ti zapobiega możliwości wprowadzania przez użytkowników nieautoryzowanych zmian (np. instalacji prywatnego oprogramowania)?			
11.	Czy w systemie TI wprowadzone i udokumentowane zostały obowiązkowe ustawienia konfiguracyjne elementów TI (np. ustawienie zabezpieczeń systemu operacyjnego)?			
12.	Czy w systemie TI stosowana jest zasada minimalizacji funkcjonalności polegająca na instalowaniu, uaktywnianiu i wykorzystywaniu wyłącznie funkcji, protokołów komunikacyjnych i usług niezbędnych do prawidłowej realizacji zadań, do których system Ti został przeznaczony?			
13.	Czy prowadzone są przeglądy systemu TI w celu identyfikacji i usunięcia zbędnych funkcji portów, protokołów, i/lub usług z częstotliwością określoną w SWB?			
14.	Czy użytkownicy systemu TI poinformowani zostali o swojej odpowiedzialności za powieszone do wykorzystania lub nadzoru urządzenia i oprogramowanie?			
15.	Czy istnieje i jest stale aktualizowana lista urządzeń i oprogramowania powierzonych do wykorzystywania lub nadzoru przez użytkowników systemu TI?			
16.	Czy w jednostce organizacyjnej przeprowadzana jest inwentaryzacja wszystkich elementów systemu TI i okablowania w celu zapewnienia rozliczności w zakresie powierzonego użytkownikom sprzętu i oprogramowania?			
7	**Utrzymanie systemu, przeglądy diagnostyczne, naprawy**			
1.	Czy prowadzona jest dokumentacja dotycząca napraw i przeglądów diagnostyczny systemu Ti zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa systemu?			
2.	Czy w systemie Ti kontrolowane jest wykorzystanie urządzeń i			

	narzędzi diagnostycznych?			
3.	Czy przyznawanie uprawnień dostępu do systemu dla pracowników serwisu jest zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa systemu TI?			
4.	Czy dokonywanie napraw elementów systemu Ti poza lokalizacjami organizacji jest przeprowadzane i dokumentowane zgodnie z dokumentacją bezpieczeństwa systemu TI?			
5.	Czy prace naprawcze i przeglądy prowadzone przez serwis zewnętrzny są nadzorowane i dokumentowane przez administratora systemu lub uprawnionych pracowników?			
6.	Czy warunki realizacji umów serwisowych przez dostawców zewnętrznych są zgodne z zapisami zawartymi w SWB?			
7.	Czy wyznaczono osoby odpowiedzialne w jednostce za nadzór nad pracami naprawczymi i przeglądami prowadzonymi przez serwis zewnętrzne?			
8	**Zapobieganie i reagowanie na incydenty bezpieczeństwa TI, ochrona przed oprogramowaniem złośliwym**			
1.	Czy w systemie Ti wykonywane są okresowe testy bezpieczeństwa w celu weryfikacji poprawności działania poszczególnych zabezpieczeń ?			
2.	Czy wprowadzone zostały zasady i procedury wykonywania bieżącej analizy i oceny bezpieczeństwa systemu TI?			
3.	Czy stosowane są testy penetracyjne lub narzędzia do przeprowadzenia automatycznej analizy i oceny skuteczności zabezpieczeń zastosowanych w systemie TI zgodnie z SWB?			
4.	Czy wprowadzone zostały zasady i procedury związane z przygotowaniem planu działań naprawczych lub korekcyjnych w celu usunięcia nieprawidłowości stwierdzonych w czasie weryfikacji poprawności działania zabezpieczeń(np. okresowe testy bezpieczeństwa), a także w sytuacji związanej z koniecznością lub potrzebą wprowadzenia zmian w systemie Ti (np. w wyniku wystąpienia incydentu bezpieczeństwa TI lub na podstawie wyników okresowo przeprowadzonego procesu szacowania ryzyka)?			
5.	Czy zidentyfikowano wszystkie połączenia międzysystemowe pomiędzy akredytowanym systemem TI a innymi systemami (przetwarzającymi IN lub jawne)?			
6.	Czy dla każdego zidentyfikowanego połączenia międzysystemowego udokumentowana została charakterystyka interfejsu, wymagania dotyczące bezpieczeństwa oraz rodzaj przekazywanych informacji?			
7.	Czy monitorowane są połączenia międzysystemowe oraz dokonywane okresowo analizy i oceny wymagań bezpieczeństwa oraz zastosowanych zapieczeń?			
8.	Czy prowadzone są okresowe szkolenia w zakresie problematyki reagowania na incydenty bezpieczeństwa?			
9.	Czy w jednostce organizacyjnej wykonywane są okresowe ćwiczenia w zakresie reagowania użytkowników systemu TI oraz osób odpowiedzialnych za funkcjonalnie i bezpieczeństwo systemu Ti na incydent bezpieczeństwa?			
10.	Czy w systemie TI zastosowano mechanizmy lub procedury zapobiegające incydentom bezpieczeństwa TI , w tym zabezpieczające przed działaniem oprogramowania złośliwego, a także umożliwiające jak najszybsze wykrywanie incydentów bezpieczeństwa TI oraz zapewniające niezwłoczne informowanie odpowiednich osób o wykrytym incydencie?			
11.	Czy dla systemu Ti przeprowadzany jest ponowny proces szacowania ryzyka w przypadku zaistnienia istotnego incydentu bezpieczeństwa TI?			
12.	Czy w systemie Ti wdrożone zostały metody postępowania z			

	incydentami bezpieczeństwa?			
13.	Czy w systemie TI dokumentuje się przypadki wystąpienia incydentów bezpieczeństwa oraz sposób wyjaśnienia przyczyn powstania incydentów i ich skutków?			
14.	Czy system Ti chroniony jest przez złośliwym oprogramowaniem?			
15.	Czy jednostak ogranizacyjan akutalizuje machanizmy ochrony przed kodem złośliwym (łącznie z bazą sygantu) zgodnie z polityką i procedurami zarządzania zamianami konfiguracji?			
16.	Czy mechanizmy ochrony przed kodem złośliwym są skonfigurowane tak, aby uruchomiać oprogramowanie wykrywające kod złośliwy po uruchomieniu systemu na stacjach roboczych, i w takiej konfiguracji, aby wykrywać i usuwać kod złośliwy przynajmniej: (i) przesłana za pośrednictwem poczty elektronicznej, w tym jako załącznik do poczty elektronicznej, (ii) wprowadzany w wyniku dostępu do stron WWW oraz (iii) wprowadzany za pośrednictwem nośników przenośnych?			
17.	Czy monitorowane są zdarzenia mające wpływ na bezpieczeństwo IN przetwarzanych w systemie TI?			
9	**Zasady wprowadzania poprawek, aktualizacja oprogramowania**			
1.	Czy poprawki/uaktualnienia do oprogramowania i systemu operacyjnego wprowadzane są na bieżąco, odpowiednio testowane i dokumentowane?			
2.	Czy określone zostały przypadki, w których dla wprowadzanych poprawek/uaktualnień oprogramowania konieczne jest testowanie bezpieczeństwa systemu sprawdzające wpływ poprawek na efektywność działania kluczowych elementów systemu i potencjalny „efekt uboczny”?			
3.	Czy system Ti wykrywa nieautoryzowane zmiany w oprogramowaniu i konfiguracji?			
10	**Ochrona informatycznych nośników danych**			
1.	Czy istnieje wykaz rodzajów informatycznych nośników danych dopuszczonych do wykorzystania w systemie TI?			
2.	Czy oznaczenie nośników wykorzystywanych do przetwarzania IN są zgodne z przepisami w tym zakresie?			
3.	Czy nosiki zawierające IN są właściwe ewidencjonowane i przechowywane?			
4.	Czy właściwie realizowane są zasady przedzielania uprawnień użytkownikom do korzystania z nośnika i rozliczania użytkowników z posiadanych nośników?			
5.	Czy wdrożono odpowiednie środki służące zabezpieczeniu nośników oznaczonych klauzulami przekazywanych pomiędzy strefami ochronnymi?			
6.	Czy obniżane są klauzule tajności nośników i czy przestrzegane są zasady ich obniżania?			
7.	Czy wdrożono środki umożliwiające realizację procedur niszczenia klasyfikowanych nośników danych?			
11	**Identyfikacja i uwierzytelnianie użytkowników i urządzeń**			
1.	Czy wprowadzono mechanizmy uwierzytelniania użytkowników podczas dostępu do urządzeń i usług systemu zgodne z opisanymi w SWB?			
2.	Czy prawidłowo dystrybuowane i ewidencjonowane są narzędzia wykorzystywane w procesie identyfikacji i uwierzytelnienia (karty chipowe, tokeny)?			
3.	Czy hasła użytkowników systemu mają odpowiednią długość i stopień złożoności i czy są zmieniane zgodnie z SWB?			
4.	Czy hasła administratora systemu, inspektora BTI, hasła dostępu do BIOS-u zostały odpowiednio zabezpieczone i			

	zdeponowane w bezpiecznym miejscu?			
5.	Czy zabezpieczono i zdeponowano w bezpiecznym miejscu wszystkie niezbędne do prawidłowego zarządzania hasła administracyjne(w tym do np. urządzeń sieciowych)?			
6.	Czy wdrożone zostały mechanizmy uwierzytelniania urządzeń w systemie, w tym urządzeń peryferyjnych przy próbie podłączenia do systemu TI?			
12	**Kontrola dostępu do systemu**			
1.	Czy wprowadzony jest rejestr użytkowników uprawnionych do pracy w systemie z wyszczególnieniem informacji o posiadanych przez nich uprawnieniach?			
2.	Czy rejestr użytkowników jest uaktualniany na bieżąco?			
3.	Czy zarządzanie kontami użytkowników systemu TI (zakładanie, przyznawanie uprawnień, modyfikowanie uprawnień, blokowanie, usunięcie itp.) jest zgodne z zapisami zawartymi w dokumentacji bezpieczeństwa?			
4.	Czy przegląd działań użytkowników dokonywana jest zgodnie z opisanym w SB okresem czasowym i zakresem objętym przeglądem?			
5.	Czy między węzłami sieci systemów TI, znajdującymi się w różnych lokalizacjach stosowane są mechanizmy kontroli dostępu przepływu danych zgodnie z zapisami zawartymi w SWB?			
6.	Czy w systemie TI zastosowano separacje oraz zróżnicowany zakres uprawnień wynikającą z podziału na role w systemie TI, zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa			
7.	Czy w systemie stosuje się zasadę przyznawania „minimum uprawnień" wymaganych do pracy w systemie?			
8.	Czy w systemie TI zastosowano automatyczną blokadę dostępu do zasobów, po wyczerpaniu nieudanych prób logowań, których liczba jest określona w dokumentacji bezpieczeństwa systemu?			
9.	Czy w systemie zastosowano ostrzeżenie o logowaniu do systemu TI zawierającego informacje niejawne?			
10.	Czy system Ti blokuje dostęp użytkownika po braku jego aktywności w czasie zdefiniowanym w SWB?			
11.	Czy w systemie Ti wykorzystuje się zdalny dostęp przewodowy do zasobów zgodnie z zapisami SWB?			
12.	Czy w systemie Ti wykorzystuje się zdalny dostęp bezprzewodowy do zasobów zgodnie z zapisami SWB			
13.	Czy w systemie TI wykorzystuje się urządzenia przenośne komunikujące się z zasobami systemu?			
14.	Czy system łączy się w sposób zgodny z zapisami SWB z innymi systemami przetwarzającymi informacje niejawne?			
15.	Czy system TI połączony jest w sposób zgodny z zapisami SWB z otwartymi systemami i sieciami?			
16.	Czy w systemie TI zainstalowano mechanizmy współdzielenia zasobów działające zgodnie z zapisami zwartymi w SWB?			
17.	Czy zarządzanie informacjami ogólnie dostępnymi dla użytkowników systemu Ti odbywa się zgodnie z zapisami zawartymi w dokumentacji bezpieczeństwa systemu?			
13	**Audyt wewnętrzny, testy bezpieczeństwa systemu**			
1.	Czy wyznaczone zostały obszary wysokiego ryzyka, które wymagają częstych audytów wewnętrznych, weryfikujących zgodność stanu zabezpieczeń systemu TI z opisem w SWB zastosowanych środków ochrony systemu?			
2.	Czy audyty wewnętrzne przeprowadzane są zgodnie z zaplanowaną w PBE częstotliwością?			
3.	Czy ustalono osoby odpowiedzialne za przeprowadzanie okresowych audytów wewnętrznych i czy zostały im przydzielone zadania w tym zakresie?			

4.	Czy były przeprowadzane dodatkowe, nieplanowane audyty wewnętrzne spowodowane wystąpieniem incydentu bezpieczeństwa?			
5.	Czy audyty wewnętrzne są odpowiednio dokumentowane?			
6.	Czy zalecenia poaudytowe zostały zrealizowane?			
7.	Czy w systemie Ti określone zostały zdarzenia, które podlegają procedurom audytu bezpieczeństwa systemu Ti z powodu ich istotności dla bezpieczeństwa system ?			
8.	Czy w systemie TI występują elementy które generują zapis audytowe (np.. mechanizmy systemowe- zasady inspekcji)?			
9.	Czy lista audytowanych w systemie Ti zdarzeń jest okresowo przeglądana i aktualizowana?			
10.	Czy system TI tworzy zapis audytowe dotyczące rodzaju zdarzenia, daty, miejsc i czasu zdarzenia, źródła zdarzenia, skutku zdarzenia (sukces/porażka), tożsamości użytkownika związanego ze zdarzeniami?			
11.	Czy w systemie TI wprowadzono taką pojemność baz danych zawierających informacje o audytowanych zdarzeniach, aby zapobiec możliwości utraty informacji w skutek przepełnienia w założonym czasie (np. wielkość plików zawierających dziennik zdarzeń)?			
12.	Czy w systemie Ti są okresowo przeglądane i analizowane zapisy audytowe?			
13.	Czy w systemie TI analizowane są zapisy audytowe znajdujące się w różnych repozytoriach w celu uzyskania kompleksowego obrazu stanu bezpieczeństwa systemu?			
14.	Czy w systemie Ti wykorzystywany jest wewnętrzny zegar do znakowania czasem zapisów audytowych?			
15.	Czy w systemie Ti synchronizowane są zegary wewnętrznych komponentów systemu?			
16.	Czy system Ti zapewnia ochronę informacji i narzędzi audytowanych przed nieautoryzowanym dostępem, modyfikacją oraz usunięciem?			
17.	Czy system Ti ogranicza dostęp do zapisów audytowch oraz zarządzania ustawieniami zapisów audytowych wyłącznie do personelu zajmującego się funkcjonowaniem i bezpieczeństwem systemu TI (administratorów i inspektorów BTI)?			
14	**Zarządzanie ryzykiem**			
1.	Czy formalnie została powołana struktura organizacyjna odpowiedzialna za zarządzanie ryzykiem w systemie TI?			
2.	Czy dokonywane są, zgodnie z zaplanowaną częstotliwością okresowe przeglądy ryzyka?			
3.	Czy zostały zrealizowane zalecenia wynikające z przeprowadzonego przeglądu ryzyka?			
4.	Czy opracowano listę zmian, które wymagają dodatkowego szacowania ryzyka?			
5.	Czy przeprowadzane były dodatkowe szacowania ryzyka wnikające z zaistnienie istotnego incydentu bezpieczeństwa teleinformatycznego?			
6.	Czy przeprowadzane były szacowania ryzyka po wykryciu nowych zagrożeń lub zidentyfikowaniu nowych podatności, które nie były rozpatrywane podczas wcześniejszego szacowania ryzyka dla bezpieczeństwa IN?			
7.	Czy przeprowadzane były szacowania ryzyka, jeżeli zmianie lub rozszerzeniu uległo przeznaczenie, zdania lub funkcjonalność systemu TI?			
8.	Czy monitorowane są czynniki ryzyka bezpieczeństwa systemu oraz, czy odpowiednio raportowane są wszelkie naruszenia bezpieczeństwa?			
9.	Czy okresowo przeglądane są rejestry zdarzeń systemów ochrony fizycznej, czy są właściwie przechowywane?			

10.	Czy są aktualne wyznaczone ryzyka szczątkowe i czy zostały zaakceptowane przez KJO?			
11.	Czy audyt wewnętrzny systemu przeprowadzany jest zgodnie z zaplanowaną częstotliwością i w wyznaczonym zakresie?			
12.	Czy w czasie audytu wewnętrznego stwierdzono inne, nieuwzględnione w procesie zarządzania ryzykiem zagrożenia?			
13.	Czy realizowano zalecenia po audytowe?			
14.	Czy eksploatacja systemu TI odbywa się zgodnie z warunkami udzielonej akredytacji bezpieczeństwa TI?			
15.	Czy przeprowadzane są szkolenia dla użytkowników systemu uświadamiające zagrożenia oraz dotyczące bezpiecznej eksploatacji systemu?			
16.	Czy określone zostały zasady i odpowiedzialności za organizowanie, prowadzenie i dokumentowanie szkoleń użytkowników systemu TI?			
15	**Wprowadzenie zmian w systemie i w dokumentacji bezpieczeństwa systemu TI, warunki ponownej akredytacji, wycofanie z eksploatacji**			
1.	Czy określone zostały zasady i procedury wprowadzania zmian do systemu TI oraz uaktualniania dokumentacji bezpieczeństwa systemu TI?			
2.	Czy określone zostały sytuacje, po wystąpieniu których wymagane jest przeprowadzenie ponownej akredytacji bezpieczeństwa systemu TI?			
3.	Czy dla systemu TI określone zostały zasady i procedury postepowania w przypadku zakończenia eksploatacji systemu TI?			