Załącznik nr 1 do *Ramowego Programu kontroli w zakresie wykorzystywania systemów teleinformatycznych do realizacji zadań publicznych*

**Metodyka kontroli w zakresie realizacji Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych,  
wymiany informacji oraz dla systemów teleinformatycznych – przykłady zagadnień, pytań badawczych i metod kontroli.**

Uwaga: niniejszy materiał przedstawia najważniejsze, jednak **nie wszystkie zagadnienia, których może dotyczyć kontrola systemów teleinformatycznych**. Prezentowane zagadnienia / pytania kontrolne / wymagania / dokumenty i dowody / metody badania / wyznaczniki i źródła odniesienia **nie są obowiązkowe** i należy je różnicować zgodnie i w zależności od statutowych zadań kontrolowanej jednostki, złożoności badanych systemów teleinformatycznych oraz stopnia ich wykorzystania w realizacji zadań publicznych oraz w kontaktach z obywatelami.

| **L.p.** | **Obszary kontroli:** | **Zagadnienia objęte kontrolą:** | **Pytania kontrolne / doprecyzowanie wymagań:** | **Badanie podstawowe:** | **Badanie zaawansowane:** | **Wyznaczniki /kontroli i źródła odniesienia:** |
| --- | --- | --- | --- | --- | --- | --- |
| Kontrola w zakresie *realizacji Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji oraz dla systemów teleinformatycznych* obejmuje następujące główne obszary tematyczne:   1. **Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną (interoperacyjność)** 2. **System Zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych (bezpieczeństwo informacji)** 3. **Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych (dostosowanie dla osób niepełnosprawnych).** | | | | | | |
| Kryteriami oceny kontrolowanej działalności są **celowość** (w szczególności zastosowanie optymalnych metod i środków), **legalność** (tj. zgodność z prawem i regulacjami wewnętrznymi oraz **rzetelność** (tj. staranność, sumienność, działanie we właściwym czasie i odpowiednia dokumentacja istotnych czynności).  Ocenie podlegają niezależnie 3 główne obszary kontroli.  **Ostateczna ocena kontroli oraz poszczególnych obszarów, w tym zdiagnozowanych nieprawidłowości i uchybień powinna uwzględniać zakres i charakter realizowanych zadań. W szczególności, większy wpływ na oceny ogólne powinny wywierać ustalenia odnoszące się do tych systemów (oraz ich funkcji), które mają większy związek z realizacją zadań statutowych. Np. mniejszy wpływ na ocenę negatywną powinno mieć ustalenie odnoszące się do niekorzystania ze skrzynki podawczej w jednostkach, które w bardzo ograniczonym zakresie współpracują z podmiotami zewnętrznymi oraz które korzystają z innych równoważnych form komunikacji elektronicznej. Rekomenduje się dokonanie ocen opisowych ze wskazaniem skutków uchybień i nieprawidłowości na realizację zadań publicznych w formie elektronicznej (np. utrudnienie w załatwianiu sprawy, trudności z pozyskaniem danych, ryzyko utraty kluczowych zasobów informacyjnych, możliwość nieautoryzowanych ingerencji, wykluczenie osób z niepełnosprawnościami).** | | | | | | |
| **Oceny powinny być formułowane wyłącznie w odniesieniu do systemów wykorzystywanych do realizacji zadań publicznych, a w przypadku jednostek samorządu terytorialnego oraz tworzonych lub prowadzonych przez te jednostki osób prawnych i innych samorządowych jednostek organizacyjnych, wyłącznie w odniesieniu do systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej. W  zakresie pozostałych systemów, kontrola może być przeprowadzana na wniosek.** | | | | | | |
| **1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.** | | | | | | |
| **1.1** | **Usługi elektroniczne** | * Wykorzystanie narzędzi elektronicznych do świadczenia usług publicznych. * Wykorzystanie elektronicznych form przekazu dokumentów, w tym Elektronicznej Skrzynki Podawczej udostępnionej na platformie ePUAP. * Promocja usług w formie elektronicznej, w tym zamieszczenie na głównej stronie internetowej podmiotu publicznego (i/lub na stronie BIP), odesłania do opisów usług. * Aktualizacja usług w katalogu usług CRWD. | * Jakie są najistotniejsze usługi publiczne realizowane przez kontrolowanego? Czy są realizowane w formie elektronicznej? Jeżeli nie, dlaczego są realizowane w formie papierowej? Czy są realizowane zarówno w formie elektronicznej, jak i papierowej? Jeżeli tak, dlaczego? * Czy w badanym okresie podmioty zewnętrze korzystały z usług świadczonych drogą elektroniczną? Jeżeli nie, to dlaczego? * Czy w przypadku każdej usługi upowszechniono zrozumiałą informację o możliwości jej realizacji w formie elektronicznej? Jeżeli tak, czy sporządzono opis tej usługi? * Czy realizacja usług drogą elektroniczną jest szybsza, sprawniejsza i bardziej przyjazna niż realizacja tej samej usługi w formie papierowej? * Jakie zabezpieczenia stosowane są celem zapewnienia integralności danych przetwarzanych w ramach usług elektronicznych? | * Wykaz usług świadczonych w formie elektronicznej. * Opisy usług świadczonych w formie elektronicznej * Dokumentacja (wydruki) instrukcji i stron internetowych. * Liczniki odwiedzin, zestawienia lub statystyka spraw załatwionych w formie elektronicznej w okresie kontroli. * Skargi i wnioski i opinie podmiotów zewnętrznych odnoszące się do funkcjonowania usług w formie elektronicznej. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Oględziny procedowania dokumentu przekazanego za pomocą ESP. * Test wysyłki pisma na ESP podmiotu publicznego. * Ankieta ewaluacyjna dla podmiotów zewnętrznych załatwiających sprawy w formie usługi elektronicznej lub papierowej. | * Art. 16 ustawy o informatyzacji * Art. 19d ustawy o informatyzacji * § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI * Opisy usług powinny być publikowane w BIP i zawierać wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw.   Rozporządzanie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych. |
| **1.2** | **Centralne Repozytorium Wzorów Dokumentów Elektronicznych (dalej: CRWDE)** | * Wykorzystanie przez kontrolowany podmiot publiczny wzorów dokumentów elektronicznych przechowywanych w CRWDE, jakie zostały już wcześniej opracowane i są używane przez inny podmiot publiczny. * Przekazanie do CRWDE oraz udostępnienie w BIP wzorów dokumentów elektronicznych podmiotu publicznego. | * Czy kontrolowany jest podmiotem zobowiązanym do określenia wzoru dokumentu i przekazania go do CRWDE? Jeżeli tak, czy wszystkie wzory zostały określone i przekazane do CRWDE? * Czy we właściwości kontrolowanego pozostają sprawy, dla których nie określił wzoru dokumentu i nie przekazał do CRWDE? Jeżeli tak, dlaczego zrezygnowano z określenia tego wzoru i przekazania go do CRWDE? * Czy podmiot publiczny poprzez opracowanie nowych wzorów i przekazanie ich do CRWD nie powiela danych jakie zostały wcześniej opracowane i są używane przez inne podmioty publiczne? | * Opracowane wzory dokumentów elektronicznych. * Dokumentacja związana z wykorzystaniem wzorów dokumentów elektronicznych przechowywanych w CRWDE. * Wnioski przekazania wzorów dokumentów elektronicznych do CRWDE. * Centralne Repozytoriom Wzorów Dokumentów Elektronicznych. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Weryfikacja na próbie prowadzonych spraw, czy kontrolowany podmiot publiczny wykorzystuje wzory dokumentów elektronicznych przechowywanych w CRWDE. | * Art. 16a i 16 b *ustawy o informatyzacji* * Art. 19b ust. od 3 do 5 *ustawy o informatyzacji*   Opracowania[[1]](#footnote-2):   * Ogólne zasady tworzenia i publikacji w centralnym repozytorium wzorów dokumentów elektronicznych zwanym dalej centralnym repozytorium. * Opis sposobu oznaczania w pismach w postaci elektronicznej niezbędnych elementów struktury. |
| **1.3** | **Model usługowy** | * Poziom wspierania modelu usługowego w procesie świadczenia usług elektronicznych przez systemy teleinformatyczne podmiotu publicznego. * Weryfikacja sposobu zarządzania usługami w oparciu o ustalone procedury. | * Czy systemy teleinformatyczne wykorzystywane przez kontrolowanego zostały oparte na architekturze modelu usługowego (ang. SOA – Service Oriented Architecture)? * Czy każda usługa elektroniczna została udokumentowana w formie przystępnej dla obsługującego i użytkownika? Czy opis usługi został przekazany do CRWDE? * Czy procedury zarządzania usługami zapewniają identyfikację właściciela merytorycznego usług (właściwa komórka organizacyjna podmiotu publicznego)? * Czy możliwe jest ustalenie podmiotu (komórki merytorycznej) odpowiedzialnego za utrzymanie usług od strony technicznej? Jeżeli tak, jaki to jest podmiot (komórka merytoryczna)? Czy określono/zadeklarowano poziom świadczenia usług? * Czy poziom świadczenia usług jest monitorowany? Jeżeli tak, w jaki sposób? Czy usługa jest realizowana na zadeklarowanym poziomie? * Czy ustalono skuteczne kanały komunikacji pomiędzy obsługującymi usługi (załatwiającymi sprawy drogą elektroniczną), a osobami/komórkami odpowiedzialnymi za utrzymanie usługi (merytorycznie i technicznie)? W jaki sposób komunikuje się błędy w działaniu usługi? | * Wykaz usług elektronicznych. * Dokumentacja systemów teleinformatycznych. * Regulaminy wewnętrzne i zakresy odpowiedzialności. * Procedury obsługi i monitoringu usług. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Weryfikacja na próbie z dokumentacji wykonywania procedur obsługi i monitoringu usług. | * §2 pkt 8 rozporządzenia KRI * § 8 rozporządzenia KRI * § 15 rozporządzenia KRI   *Wymagania w tym obszarze uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie przeglądanie, utrzymanie i udoskonalanie zarzadzania usługą podmiotu realizującego zadania publiczne odbywają się z uwzględnieniem Polskich Norm PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.* |
| **1.4** | **Współpraca systemów teleinformatycznych z innymi systemami** | * Poziom współpracy systemów teleinformatycznych, a w szczególności rejestrów publicznych z innymi systemami podmiotu publicznego lub systemami informatycznymi innych podmiotów publicznych w tym rejestrami referencyjnymi. * Sposób komunikacji z innymi systemami w tym wyposażenie w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami telekomunikacyjnymi za pomocą protokołów komunikacyjnych i szyfrujących zapewniających BI. | * Czy kontrolowany prowadzi rejestry publiczne przy użyciu systemów teleinformatycznych? Jeżeli tak, jakie są to rejestry? Czy systemy te umożliwiają dostarczenie informacji z rejestru drogą elektroniczną? * Czy kontrolowany wykorzystuje systemy teleinformatyczne lub prowadzi rejestry publiczne pozwalające na współpracę z innymi systemami, w tym wykorzystując ich dane jako dane referencyjne? Jeśli nie, dlaczego? * Czy kontrolowany korzysta z narzędzi umożliwiających dostęp do systemów teleinformatycznych, w tym rejestrów publicznych w formie elektronicznej? * Czy dane z systemów teleinformatycznych są udostępnianie/pobierane tylko w zakresie niezbędnym do realizacji zadań? * Czy zapewniono rozliczalność operacji wydania informacji z rejestru publicznego prowadzonego przez podmiot kontrolny? Jeżeli tak, w jaki sposób? * Czy dane z systemów teleinformatycznych są udostępnianie/pobierane bezpłatnie? * Czy zapewniono integralność przetwarzanych danych? | * Umowy (porozumienia) z podmiotami prowadzącymi rejestry referencyjne dotyczące dostępu do danych referencyjnych uzyskiwanych w drodze wymiany. * Opis interfejsów systemu teleinformatycznego, dokumentacja systemu teleinformatycznego. * Schematy przepływu danych podmiotu publicznego. * Rozliczenie wydania informacji z rejestru (tj. logi systemowe potwierdzające pobranie/odebranie określonych danych). * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Oględziny systemów teleinformatycznych podmiotu publicznego. * Badanie zgodności protokołów komunikacyjnych i szyfrujących z obowiązującymi przepisami, normami standardami lub rekomendacjami ustanowionymi przez krajową jednostkę normalizacyjną. | * Art. 14 ustawy o informatyzacji * Art. 15 ustawy o informatyzacji * § 5 ust. 3 pkt 3 rozporządzenia KRI * § 11 rozporządzenia KRI * § 13 rozporządzenia KRI * § 16 rozporządzenia KRI   Informacja o dostępności opisów standardów w zakresie protokołów komunikacyjnych i szyfrujących, zamieszczana przez Ministra Cyfryzacji w BIP zgodnie z § 16 ust. 3 rozporządzenia KRI. |
| **1.5** | **Obieg dokumentów w podmiocie publicznym** | * Regulacje wewnętrzne opisujące sposób zarządzania dokumentacją w kontrolowanym podmiocie. * Zakres stosowania elektronicznego obiegu dokumentów. | * Czy obieg dokumentów w formie elektronicznej porządkuje, ułatwia dostęp i zabezpiecza informacje przed nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem? * Czy doszło do wyeliminowania z obiegu wewnętrznego dokumentów papierowych? Jeżeli nie, to czy podwójny (elektroniczny i papierowy) obieg dokumentów jest uzasadniony? * Czy koszty wdrożenia i użytkowania elektronicznego obiegu dokumentów są zoptymalizowane? * Czy funkcjonujący obieg dokumentów w formie elektronicznej pozwala na zachowanie wiedzy instytucjonalnej? | * Dokumentacja systemu zarządzania dokumentacją, w tym procedury i zasady postępowania z dokumentami zawarte w instrukcjach kancelaryjnych oraz dokumentacja stosowania ww. procedur. * Zakres stosowania elektronicznego obiegu dokumentów. * Opinie obsługujących system w zakresie usprawnienia pracy. * Częstotliwość wysyłki i odbioru dokumentacji w formie papierowej. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Oględziny elektronicznego systemu zarządzania dokumentacją podmiotu publicznego, w tym zabezpieczeń chroniących przed ujawnieniem, modyfikacją, usunięciem lub zniszczeniem informacji. | * Dobre praktyki w zakresie współpracy wewnętrznych systemów obiegów dokumentacji z systemami pozyskującymi dokumentacje z zewnątrz (ESP, ePUAP, formularze, inne systemy kancelaryjne). |
| **1.6** | **Formaty danych udostępniane przez systemy teleinformatyczne** | * Sposób kodowania znaków w dokumentach wysyłanych i odbieranych z systemów teleinformatycznych podmiotu publicznego. * Sposób udostępniania zasobów informatycznych z systemów teleinformatycznych podmiotu publicznego. * Sposób przyjmowania dokumentów elektronicznych przez systemy teleinformatyczne podmiotu publicznego. * Struktura danych i cech informacyjnych dla różnych typów obiektów w rejestrach publicznych udostępnianych przez kontrolowanego. | * Czy dokumenty odbierane/wysyłane w formie elektronicznej są kodowane według standardu Unicode UTF-8 lub w uzasadnionych przypadkach Unicode UTF-16? * Czy zasoby informacyjne są udostępniane w dostępnych formatach danych określonych w zał. nr 2 do rozporządzenia KRI? * Czy w rejestrze publicznym udostępnionym przez kontrolowanego dla każdego typu obiektu zastosowano prawidłową strukturę identyfikatorów? | * Opis formatów danych w systemach podmiotu publicznego. * Dokumentacja systemu teleinformatycznego. * Wybrane, istotne dla realizacji zadań zasoby informacyjne kontrolowanego. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Weryfikacja kodowania znaków na próbie dokumentów przesyłanych w formie elektronicznej. * Weryfikacja prawidłowości struktury identyfikatorów i cech informacyjnych zastosowanych dla różnych typów obiektów zamieszczonych w rejestrach publicznych udostępnianych przez kontrolowanego. | * § 10 oraz zał. nr 1 do rozporządzenia KRI * § 17 ust. 1 rozporządzenia KRI * § 18 ust. 1 rozporządzenia KRI * § 18 ust. 2 zał. nr 2 i 3 rozporządzenia KRI |
| **Ocena obszaru powinna odnosić się do celów realizacji Krajowych Ram Interoperacyjności na tle zadań realizowanych przez kontrolowaną jednostkę. W szczególności ocena może się odnieść do:** (§ 3 rozporządzenia KRI)   * zapewnienia obywatelom oraz przedsiębiorcom dostępności usług świadczonych przez podmioty realizujące zadania publiczne w postaci elektronicznej, * zwiększenia efektywności usług świadczonych przez administrację publiczną, * zapewnienia obywatelom i przedsiębiorcom zmniejszenia obciążeń związanych z realizacją uprawnień i obowiązków przewidzianych w przepisach odrębnych, * zapewnienia podmiotom publicznym redukcji kosztów funkcjonowania, * zapewnienia racjonalnego gospodarowania funduszami publicznymi, * zapewnienia swobody gospodarczej i równego dostępu do rynku informatycznego w zakresie usług i dostaw podczas udzielania zamówień publicznych dla wszystkich jego uczestników, * efektywną realizację drogą elektroniczną ponadgranicznych usług administracji publicznej.   **Ocena negatywna w obszarze nr 1 (interoperacyjność) może zostać przyznana w szczególności, gdy:**   * nie zarządza się usługami realizowanymi przez systemy teleinformatyczne w oparciu o udokumentowane procedury (§ 8 rozporządzenia); * rejestry publiczne prowadzone przez kontrolowanego nie udostępniają danych niezbędnych do realizacji zadań przez inne podmioty publiczne (art. 15 ustawy o informatyzacji); * najistotniejsze zasoby informacyjne są udostępnianie w formatach niestandardowych (18 ust. 2 rozporządzenia KRI). | | | | | | |
| **2. System Zarządzania Bezpieczeństwem Informacji w systemach teleinformatycznych** | | | | | | |
| **2.1** | **Dokumenty z zakresu bezpieczeństwa informacji** | * Dokumentacja SZBI, w tym Polityka BI oraz inne dokumenty stanowiące SZBI. * Dokumentacja przeglądów SZBI, szacowania ryzyka, audytów, incydentów naruszenia BI. * Działania związane z aktualizacją regulacji wewnętrznych w zakresie zmieniającego się otoczenia będące konsekwencją wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń poaudytowych, wniosków z analizy incydentów naruszenia BI. * Stopień zaangażowania kierownictwa podmiotu publicznego w proces ustanawiania i funkcjonowania SZBI oraz zarządzania BI (przeglądy SZBI, szacowanie i obsługa ryzyka BI, egzekwowanie działań związanych z BI). | * Czy dokumentacja SZBI została opracowana, zatwierdzona przez kierownictwo, opublikowana. Jeżeli tak, kiedy (wskazać odpowiednie daty)? Czy poinformowano o tym pracowników? Jeżeli tak, w jakiej formie? * Czy zatwierdzona polityka bezpieczeństwa informacji zawiera/określa: definicję bezpieczeństwa informacji, oświadczenie o intencjach kierownictwa, obowiązek przeprowadzania corocznych audytów wewnętrznych w zakresie bezpieczeństwa informacji, krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji, definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji, odsyłacze do dokumentacji uzupełniającej politykę? * Czy określone zostały zakresy odpowiedzialności związane z bezpieczeństwem informacji i czy przypisano je właściwym osobom? * Czy rozdzielono zakresy i obowiązki, które pozostają w konflikcie ze sobą, w celu zabezpieczenia przed nieuprawnionym lub niezamierzonym modyfikowaniem lub nadużyciem aktywów organizacji? * Czy została opracowana procedura przeglądów polityki bezpieczeństwa? * Czy są przeprowadzane oraz dokumentowane cykliczne przeglądy polityki bezpieczeństwa informacji? Jeżeli tak, kto jest odpowiedzialny za przeprowadzanie ww. przeglądów? * Czy są zbierane dane do przeglądu obejmujące: wyniki wcześniejszych przeglądów, informacje o zmianach, które mogą wpłynąć na podejście jednostki do zarządzania bezpieczeństwem informacji, łącznie ze zmianami środowiska organizacyjnego, celów jednostki, dostępności zasobów, zobowiązań umownych, regulacji wewnętrznych i warunków prawnych lub środowiska technicznego, informacje dotyczące tendencji związanych z zagrożeniami i podatnościami, informacje dotyczące zgłoszonych incydentów związanych z bezpieczeństwem informacji, rekomendacje wydane przez właściwe podmioty, organy? | * Dokumentacja SZBI w tym polityka BI oraz inne dokumenty stanowiące SZBI. * Dokumentacja z przeglądów SZBI. * Raporty z audytów / kontroli zew. / innych badań oceniających Dokumentacja zmian wynikających z wyników szacowania ryzyka, wniosków z przeglądów SZBI, zaleceń/rekomendacji poaudytowych, wniosków z analizy incydentów naruszenia BI. | *N/d* | * § 20 ust. 1 rozporządzenia KRI * § 20 ust. 2 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt 5. Polityki bezpieczeństwa informacji)  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA)  Rozdział 7 Bezpieczeństwo informacji.  Załącznik VII matryce kontroli bezpieczeństwa informacji – polityka bezpieczeństwa informacji. |
| **2.2** | **Analiza zagrożeń związanych z przetwarzaniem informacji** | * Regulacje wewnętrzne opisujące sposób zarządzania ryzykiem BI w urzędzie. * Dokumentacja z przeprowadzania okresowej analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem. * Działania minimalizujące ryzyko zgodnie z planem postępowania z ryzykiem stosownie do szacowania ryzyka. | * Czy zostały opracowane oraz zatwierdzone regulacje wewnętrzne opisujące sposób zarządzania ryzykiem bezpieczeństwa informacji? * Czy podmiot publiczny przedstawił dokumentację z  przeprowadzania analizy ryzyka utraty integralności, poufności lub dostępności informacji, w tym rejestr ryzyk, zawierający informacje o zidentyfikowanych ryzykach, ich poziomie, plan postępowania z ryzykiem? * Czy analiza ryzyka jest procesem ciągłym? * Czy jednostka opracowała i wdrożyła plan postępowania z ryzykiem? * Czy procedura szacowania ryzyka była przeprowadzana w przypadku pojawienia się nowych zagrożeń lub zmiany istotności pierwotnie zidentyfikowanych zagrożeń? | * Dokumentacja zarządzania ryzykiem w tym: procedura przeprowadzania analizy ryzyka, rejestr ryzyk, plan postępowania z ryzykiem. * Dowody utrzymywania i doskonalenia systemu zarządzania ryzykiem. * Dokumentacja zmian w zabezpieczeniach związanych z bieżącą analizą ryzyka. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Przeprowadzenie podczas kontroli własnej analizy ryzyka w zakresie bezpieczeństwa informacji, w celu oceny, czy przedstawione wyniki analizy ryzyka, są rzetelne, dokładne i obejmują wszystkie możliwe ryzyka w tym obszarze. | * § 20 ust. 2 pkt 3 rozporządzenia KRI.   PN-ISO/IEC 27005:2014-01 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA).  Załącznik VII matryca kontroli bezpieczeństwa informacji – matryca ocena ryzyka. |
| **2.3** | **Inwentaryzacja sprzętu i oprogramowania informatycznego** | * Regulacje wewnętrzne opisujące sposób zarządzania sprzętem informatycznym i oprogramowaniem (w tym licencjami na oprogramowanie) oraz funkcjonowania rejestru zasobów teleinformatycznych (bazą konfiguracji CMDB ang. Configuration Management Data Base). * Rejestr zasobów teleinformatycznych (baza konfiguracji CMDB) zawierający informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym: szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. * Sposób aktualizacji rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB). | * Czy zakres rejestru dotyczącego sprzętu pozwala na jednoznaczną identyfikację sprzętu, użytkowników i sposobu jego wykorzystania? W szczególności czy obejmuje elementy takie jak: rodzaj urządzenia, numer inwentarzowy urządzenia, nazwę urządzenia w sieci, adres (lub adresy) IP oraz adres (lub adresy) MAC, komórkę organizacyjną użytkującą urządzenie oraz ew. użytkownika korzystającego z urządzenia, cel w jakim urządzenie jest eksploatowane, parametry konfiguracyjne, wskazanie zainstalowanego oprogramowania, poprzez powiązane z listą inwentarzową, * oprogramowania, fizyczną lokalizację urządzenia, datę zakupu urządzenia, informacje o wsparciu serwisowym, informacje o klasyfikacji urządzenia w związku z informacjami przetwarzanymi przy jego użyciu? * Czy zakres rejestru dotyczącego oprogramowania obejmuje elementy takie jak: nazwa oprogramowania, miejsce instalacji, użytkownik oprogramowania,, ew. wsparcie dostawy, warunki licencjonowania, dowody licencyjne (np. kopie faktur zakupu ze wskazaniem miejsca przechowywania oryginałów)? * Czy procedury określają sposób aktualizacji rejestru zasobów teleinformatycznych (bazy konfiguracji CMDB)? * Czy rejestr zasobów teleinformatycznych (baza konfiguracji CMDB) podlega aktualizacji? Data ostatniej aktualizacji rejestru. * Kto jest odpowiedzialny za przeprowadzanie inwentaryzacji sprzętu i oprogramowania informatycznego? W jakiej formie rejestr jest prowadzony? | * Dokumentacja zarządzania sprzętem i oprogramowaniem, w tym: rejestr zasobów informatycznych. * Procedury prowadzenia rejestru zasobów informatycznych. * Procedury przydzielania, zwrotu sprzętu i oprogramowania. * Procedury korzystania z zasobów informatycznych przez użytkowników. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Szczegółowa weryfikacja aktualności rejestrów (wszystkich lub na wybranych próbach), * Szczegółowa weryfikacja na próbie. * aktywów(zidentyfikowanych podczas oględzin), czy zostały ujęte w rejestrze. | * § 20 ust. 2 pkt 2 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 8. Zarządzanie aktywami). |
| **2.4** | **Zarządzanie uprawnieniami do pracy w systemach informatycznych** | * Regulacje wewnętrzne opisujące zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym do przetwarzania danych osobowych. * Adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień do przetwarzania danych osobowych (rejestr wydanych upoważnień). * Działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp. * Sposób i szybkość odbierania uprawnień byłym pracownikom w systemach informatycznych. | * Czy regulacje wewnętrzne obejmują cały cykl zarządzania dostępem użytkowników od momentu zarejestrowania w systemie do wyrejestrowania z systemu? * Czy dostęp do systemu z wykorzystaniem praw uprzywilejowanego dostępu (konta administracyjne) jest ograniczany i nadzorowany? * Czy sposób i szybkość odbierania uprawnień byłym pracownikom / pracownikom, którzy zmienili zakres zadań lub stanowisko w systemach informatycznych jest zgodny z § 20 ust. 2 pkt 5 rozporządzenia KRI? * Czy przydzielanie poufnych informacji uwierzytelniających (loginów, haseł, kodów pin) zostało sformalizowane i ujęte w ww. regulacjach wewnętrznych? * Czy zostały przewidziane działania w zakresie monitoringu i kontroli dostępu do zasobów teleinformatycznych, w tym przeglądy w celu wykrywania nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów czy nadzorowania samego siebie itp.? * Czy każdy użytkownik posiada unikalny identyfikator dostępności do systemu? * Czy określone dla użytkowników poziomy uprawnień do pracy w systemach teleinformatycznych są adekwatne do ich zakresów czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień o przetwarzania danych osobowych (rejestr wydanych upoważnień), zgodnie z § 20 ust. 2 pkt 4 rozporządzenia KRI? * Jak często i przez kogo dokonywane są przeglądy uprawnień do pracy w systemach informatycznych? * W jaki sposób są dokumentowane wyniki ww. przeglądów i monitorowane wprowadzane czynności korekcyjnych? | * Dokumentacja zarządzania uprawnieniami użytkowników do pracy w systemach teleinformatycznych, w tym procedury nadawania, zmiany i odbierania uprawnień do pracy w systemach teleinformatycznych. * Dokumentacja wykonywania ww. procedur. * Zestawienie użytkowników systemów teleinformatycznych. * Raporty z audytów / kontroli zew. / innych badań oceniających. * Ewidencja upoważnień do przetwarzania danych osobowych. | * Szczegółowa weryfikacja na próbie użytkowników systemów teleinformatycznych w zakresie przestrzegania obowiązku bezzwłocznej zmiany uprawnień jak również w obszarze nieuprawnionego dostępu, nadmiernych uprawnień, konfliktu interesów i nadzorowania samego siebie. | * § 20 ust. 2 pkt 4 rozporządzenia KRI * § 20 ust. 2 pkt 5 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 9. Kontrola dostępu.) |
| **2.5** | **Szkolenia pracowników zaangażowanych w proces przetwarzania informacji** | * Regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesie przetwarzania informacji w systemach teleinformatycznych. * Dokumentacja z przeprowadzonych szkoleń pod kątem zakresu tematycznego, w tym: aktualności informacji o zagrożeniach, skutkach i zabezpieczeniach, wskaźnik liczby osób przeszkolonych w stosunku do wszystkich osób uczestniczących w procesie przetwarzania informacji, a także cykliczności szkoleń. | * Czy regulacje przewidują cykliczną realizację szkoleń? Szkolenia powinny obejmować nie tylko nowych użytkowników, lecz także użytkowników, którzy zmieniają zakres zadań lub stanowisko. Kiedy były realizowane ww. szkolenia? * Czy szkolenia obejmują poza pracownikami, zatrudnionymi na podstawie umowy o pracę, również wszystkie inne osoby współpracujące z instytucją i mające dostęp do jej systemów informatycznych? * Czy szkolenia osób zaangażowanych w proces przetwarzania informacji przewidują m.in. zagadnienia: zagrożenia bezpieczeństwa informacji; skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna; stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich; zgodnie z § 20 ust. 2 pkt 6 rozporządzenia KRI? * Czy osoby przeszkolone zobligowane są do podpisania oświadczenia potwierdzającego, że rozumieją obowiązujące w instytucji regulacje i zobowiązują się do ich przestrzegania, a także znają konsekwencje ich nieprzestrzegania, obejmujące sankcje dyscyplinarne i karne, adekwatne do przepisów obowiązującego prawa? Czy ww. oświadczenia są przechowywane? * Kto jest odpowiedzialny za przygotowanie i prowadzenie szkoleń pracowników zaangażowanych w proces przetwarzania informacji? * Czy, a jeśli tak, w jaki inny sposób kontrolowany podnosi świadomość pracowników w zakresie BI? | * Dokumentacja szkolenia pracowników zaangażowanych w proces przetwarzania informacji, w tym: programy szkoleń i listy uczestników. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Szczegółowa weryfikacja programów szkoleń. * Ocena znajomości przez pracowników podstawowych pojęć z zakresu bezpieczeństwa np. incydent bezpieczeństwa, znajomość wewnętrznych zasad zgłaszania incydentów itp. (na podstawie wyjaśnień lub ankiet). | * § 20 ust. 2 pkt 6 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 7.2.2. Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji.).  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA).  Załącznik VII matryca kontroli bezpieczeństwa informacji – matryca bezpieczeństwo zasobów ludzkich. |
| **2.6** | **Praca na odległość i mobilne przetwarzanie danych** | * Regulacje wewnętrzne zawierające zasady bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość. * Działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość. | * Czy regulacje określają szczegółowe zasady pracy na odległość? * Czy regulacje określają zasady użytkowania urządzeń mobilnych? * Czy sposób wykorzystywania urządzeń mobilnych jest monitorowany? * Czy jednostka podejmuje działania w zakresie stosowania zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość, w tym stosowania zabezpieczeń i procedur bezpieczeństwa przez użytkowników urządzeń przenośnych i pracy na odległość? * Czy uświadomiono użytkownikom zagrożenia wynikające z pracy na odległość i przeszkolono z obowiązujących zasad w ww. zakresie? * Jakie narzędzia są wykorzystywane do zdalnej pracy? | * Dokumentacja dotycząca zarządzania urządzeniami przenośnymi i pracą na odległość, w tym: procedury bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Szczegółowa weryfikacja na próbie dokumentacji związanej z pracą na odległość (zasadność udzielonej zgody, zakres zdalnego dostępu do systemów teleinformatycznych jednostki). * Weryfikacja funkcjonalności mechanizmów szyfrujących. | * § 20 ust. 2 pkt 8 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 6.2 Urządzenia mobilne i telepraca). |
| **2.7** | **Serwis sprzętu informatycznego i oprogramowania** | * Regulacje wewnętrzne, w których określono zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym wymagane klauzule prawne dotyczące BI. * Umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych w zakresie zapisów gwarantujących odpowiedni poziom BI. | * Czy przedstawione umowy serwisowe oraz umowy dotyczące rozwoju systemów teleinformatycznych posiadają zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI? * Czy w przedstawionych umowach serwisowych określony został maksymalny czas skutecznej naprawy sprzętu/oprogramowania (jest to ważniejsze niż określenie czasu reakcji)? * Czy w przedstawionych umowach serwisowych oraz umowach dotyczących rozwoju systemów teleinformatycznych zagwarantowane zostało prawo do kontroli w zakresie oceny bezpieczeństwa przetwarzania danych? * Czy wymagane jest specjalne upoważnienie na dostęp osób trzecich do pomieszczeń i urządzeń gdzie przetwarzane są lub magazynowane informacje szczególnie wrażliwe dla jednostki? * Czy w procedurach bezpieczeństwa wpisany jest obowiązek uczestniczenia i obecności wyznaczonych pracowników przy pracach osób trzecich w miejscach szczególnie wrażliwych dla jednostki? | * Zapisy umów serwisowych. * Zapisy umów dotyczących rozwoju systemów teleinformatycznych. * Dokumentacja wykonania ww. umów. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Szczegółowa weryfikacja na próbie umów oraz dokumentacji z ich wykonania w przypadku, gdy nie jest możliwe sprawdzenie kompletu dokumentacji. | * § 20 ust. 2 pkt 10 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 11.2.4 Konserwacja sprzętu). |
| **2.8** | **Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji** | * Regulacje wewnętrzne, w których określono zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji. * Sposób zgłaszania i postępowania z incydentami (działania korygujące), rejestr incydentów naruszenia BI, wpływ analizy incydentów na SZBI, ewentualna współpraca z CERT.GOV.PL. | * Czy regulacje wewnętrzne lub umowy podpisywane z osobami trzecimi zobowiązują pracowników lub odpowiednio kontrahentów do zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach? * Czy szkolenia z zakresu bezpieczeństwa informacji obejmują zagadnienia dotyczące zasad zgłaszania i  postępowania z incydentami naruszenia bezpieczeństwa informacji? * Czy procedury przewidują mechanizmy umożliwiające liczenie i monitorowanie rozmiarów i kosztów incydentów związanych z bezpieczeństwem informacji? * Czy informacje zebrane podczas oceny incydentów związanych z bezpieczeństwem informacji wykorzystywane są do identyfikowania incydentów powtarzających się lub o znacznych konsekwencjach? * Czy informacje zebrane podczas oceny incydentów związanych z bezpieczeństwem informacji wykorzystywane są w odpowiedni sposób (analiza ryzyka, przeglądy polityki bezpieczeństwa, audyty wewnętrzne)? * Jak zapewniane jest ograniczanie rozprzestrzeniania się incydentów oraz ich likwidacja? Czy prowadzone są czynności mające na celu zwiększenie świadomości pracowników w zakresie zmniejszenia prawdopodobieństwa wystąpienia incydentu? | * Dokumentacja postępowania z incydentami naruszenia BI w tym rejestr incydentów naruszenia BI. * Procedury zgłaszania i postępowania z incydentami, dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | Szczegółowa weryfikacja na próbie incydentów oraz dokumentacji z nimi związanej, w przypadku, gdy nie jest możliwe sprawdzenie wszystkich incydentów. | * § 20 ust. 2 pkt 13 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji).  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA).  Załącznik IV sugerowana matryca kontroli eksploatacji systemów informatycznych – matryca zarządzanie problemami i incydentami. |
| **2.9** | **Audyt wewnętrzny z zakresu bezpieczeństwa informacji** | * Regulacje wewnętrzne, w których określono zasady przeprowadzania audytów wewnętrznych w zakresie BI. * Sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji. * Działania podjęte w wyniku zaleceń poaudytowych. | * Czy jednostka przedstawiła sprawozdania z audytu wewnętrznego w zakresie bezpieczeństwa informacji? * Czy w jednostce podejmowane są działania wynikające z zaleceń poaudytowych? * Czy wyniki audytów w zakresie bezpieczeństwa informacji wykorzystywane są w odpowiedni sposób (analiza ryzyka, przeglądy polityki bezpieczeństwa, zapobieganie incydentom)? * Czy, a jeśli tak, to w jaki inny sposób kontrolowany uzyskuje aktualne i kompleksowe informacje o stanie bezpieczeństwa informacji w jednostce? | * Dokumentacja audytów z zakresu BI. * Dokumentacja realizacji zaleceń poaudytowych. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Ocena zakresu jakości prowadzonych audytów. | * § 20 ust. 2 pkt 14 rozporządzenia KRI.   PN-ISO/IEC 27002:2014-12 (punkt: 12.7 Rozważania dotyczące audytu systemów informacyjnych). |
| **2.10** | **Kopie zapasowe** | * Regulacje wewnętrzne, w których określono zasady tworzenia, przechowywania oraz testowania kopii zapasowych danych i systemów podmiotu publicznego. * Działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja tych działań. | * Czy zostały określone w jednostce wymagania w zakresie zapasowych kopii informacji, oprogramowania oraz systemów zgodnie z analizą ryzyka (częstotliwość wykonania, okres przechowywania)? * Czy w jednostce podejmowane są działania związane z wykonywaniem, przechowywaniem i testowaniem kopii zapasowych danych i systemów oraz dokumentacja tych działań, zgodnie z ustalonymi procedurami wewnętrznymi? * Czy nośniki kopii zapasowych są przechowywane w innej lokalizacji niż ośrodek podstawowy? | * Dokumentacja wykonywania kopii zapasowych w tym: procedury wykonywania, przechowywania i testowania kopii zapasowych. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Oględziny systemu teleinformatycznego wykorzystywanego do wykonywania kopii zapasowych, sprawdzenie istnienia kopii zapasowych. * Przeprowadzenie w obecności kontrolerów przez pracowników podmiotu publicznego dla wybranej próby kopii zapasowych odtworzenia danych z kopii zapasowej w środowisku testowym. | * § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 12.3 Kopie zapasowe) |
| **2.11** | **Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych**   * *Zapewnienie warunków dla uzyskania odpowiedniej funkcjonalności, niezawodności, używalności, wydajności, przenaszalności i pielęgnowalności systemów informatycznych w fazie ich projektowania, wdrażania i eksploatacji, zgodnie z § 15 ust. 1 rozporządzenia KRI;* | * Regulacje wewnętrzne opisujące wymagania w zakresie projektowania systemów teleinformatycznych w urzędzie dotyczące architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągnięcia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu. * Regulacje wewnętrzne opisujące wymagania w zakresie wdrażania systemów teleinformatycznych w urzędzie dotyczące: sposobu dostarczenia i instalacji systemu teleinformatycznego, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji a także warunków i kryteriów odbioru. * Regulacje wewnętrzne opisujące sposób przeprowadzania zmian w systemach teleinformatycznych (w trakcie ich eksploatacji) w tym opis: sposobu zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany. * Regulacje wewnętrzne opisujące proces monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanych wobec wzrostu ilości systemów teleinformatycznych, ilości przetwarzanych danych, ilości użytkowników poprzez podejmowanie działań zapobiegawczych. * Działania związane z wdrażaniem nowych systemów teleinformatycznych oraz wprowadzaniem zmian w systemach eksploatowanych. * Działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności. * Działania zapobiegawcze będące wynikiem dostrzeżonych problemów podczas monitorowania ich pracy. | * Czy jednostka realizuje działania związane z wdrażaniem nowych systemów teleinformatycznych oraz wprowadzaniem zmian w systemach eksploatowanych, zgodnie z odpowiednimi regulacjami wewnętrznymi? * Czy jednostka realizuje działania związane z monitorowaniem systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności, zgodnie z odpowiednimi regulacjami wewnętrznymi? * Czy jednostka realizuje działania zapobiegawcze i naprawcze będące wynikiem dostrzeżonych problemów podczas monitorowania ich pracy, zgodnie z odpowiednimi regulacjami wewnętrznymi? * Czy na etapie projektowanych systemach podejmowane są działania w celu oprogramowania odpowiednich dla osiągnięcia założonych celów rozwiązań funkcjonalnych, sposobu i poziomu zabezpieczeń, prezentacji treści dla osób niepełnosprawnych, wydajności? * Czy w jednostce został ustanowiony proces wdrażania systemów informatycznych określający sposób dostarczenia i instalacji systemu teleinformatycznego, określania wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji technicznej i użytkowej, a także warunków i kryteriów odbioru? * Czy w jednostce został ustanowiony proces zarządzania zmianą w systemach informatycznych zawierający opis: sposobu zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyka, a także określenia sposobu wykonania i odbioru zmiany? | * Regulacje wewnętrzne w przedmiotowym zakresie. * Dokumentacja wdrożeń nowych systemów teleinformatycznych. * Dokumentacja wprowadzanych zmian w systemach eksploatowanych. * Dokumentacja monitorowania systemów teleinformatycznych oraz działań zapobiegawczych będących wynikiem dostrzeżonych problemów podczas monitorowania. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Badanie wdrożenia systemu teleinformatycznego, w tym: postanowień umownych, przygotowania do zamówienia, gospodarności umowy, zapewnienia w umowie poufności i bezpieczeństwa informacji, rzetelności odbiorów, prawidłowości rozliczenia umowy. | * § 15 ust. 1 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (punkt: 14 Pozyskiwanie, rozwój i utrzymanie systemów)  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA). Załącznik III matryce kontroli i rozwijania i nabywania. |
| **2.12** | **Zabezpieczenia techniczno-organizacyjne dostępu do informacji** | * Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych, w tym plan postępowania z ryzykiem. * Regulacje wewnętrzne dotyczące zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie. * Działania związane z monitorowaniem dostępu do informacji np. w systemie informatycznym odnotowującym w bazie danych wszystkie działania użytkowników i administratorów dotyczące systemów teleinformatycznych podmiotu publicznego. Działania związanych z monitorowaniem ruchu osobowego w urzędzie. * Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia BI. * Działania związane z zapewnieniem środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie zabezpieczeń kryptograficznych, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. * Działania związane z ochroną fizyczną informacji zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych, zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. * Działania związane z utylizacją sprzętu informatycznego i nośników danych, a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie BI. | * Czy regulacje wewnętrzne opisują zasady ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami adekwatne do wyników analizy ryzyka i planu postępowania z ryzykiem? Czy regulacje te obejmują zasady ochrony fizycznej nośników informacji i systemów IT? * Czy zastosowane zabezpieczenia techniczno-organizacyjne dostępu do informacji wynikają z planu postępowania z ryzykiem? * Czy zastosowane elementy ochrony fizycznej biur, pomieszczeń i urządzeń zapewniają bezpieczeństwo przetwarzanych informacji, w szczególności danych krytycznych i wrażliwych? * Czy wyznaczono racjonalne granice obszarów bezpiecznych? * Czy określono zasady i wdrożono mechanizmy autoryzacji dostępu do systemów operacyjnych, usług sieciowych i aplikacji, jak również dostępu do pomieszczeń serwerowni? Czy w jednostce są podejmowane działania związane z monitorowaniem ruchu osobowego w urzędzie? Czy określono zasady i wdrożono mechanizmy stosowania zabezpieczeń kryptograficznych? * Czy określono zasady stosowania systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall? * Czy w systemach informatycznych wbudowane są mechanizmy monitorujące dostęp do informacji np. odnotowujące w logach lub w bazie danych wszystkie działania użytkowników, administratorów lub obiektów systemowych. Jakie są zasady zabezpieczenia logów systemowych przed nieautoryzowaną zmianą? Jaki jest okres przechowywania logów? Czy jednostka określiła zasady i podejmuje działania związane z bezpieczną utylizacją sprzętu informatycznego i nośników danych, a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie bezpieczeństwa informacji? | * Dokumenty wprowadzające stosowanie zabezpieczeń. * Dokumentacja zabezpieczeń, w tym: procedury stosowania zabezpieczeń. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | *N/d* | * § 20 ust. 2   PN-ISO/IEC 27002:2014-12 (pkt 11 Bezpieczeństwo fizyczne i środowiskowe)  (pkt 12.5 Nadzór nad oprogramowaniem produkcyjnym)  (pkt 17.1 Ciągłość bezpieczeństwa informacji) |
| **2.13** | **Zabezpieczenia techniczno-organizacyjne systemów informatycznych** | * Regulacje wewnętrzne, w których ustalono zasady w celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez opisy stosowania zabezpieczeń, w tym plan postępowania z ryzykiem. * Działania związane z aktualizacją oprogramowania oraz redukcją ryzyk wynikających z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. * Działania związane z minimalizowaniem ryzyka utraty informacji w wyniku awarii oraz ochroną przed błędami, utratą i nieuprawnioną modyfikacją a także zapewnienie bezpieczeństwa plików systemowych poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych, w tym np.: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia (ang. load balancing), monitorowania parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. * Działania związane z zastosowaniem mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa poprzez stosowanie zabezpieczeń kryptograficznych np.: dla transmisji do urządzeń mobilnych, poczty elektronicznej, a także podpisów kwalifikowanych do autoryzacji dokumentów zgodnie z wynikami analizy ryzyka i planem postępowania z ryzykiem. * Działania podejmowane w związku z dostrzeżeniem nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa. * Działania związane z kontrolą zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa. | * Czy zastosowane zabezpieczenia techniczno-organizacyjne systemów informatycznych wynikają z planu postępowania z ryzykiem? * Czy zastosowane zabezpieczenia techniczno-organizacyjne systemów informatycznych ograniczają ryzyko nieautoryzowanego dostępu? * Czy jednostka określiła zasady i podejmuje działania związane z aktualizacją oprogramowania poprzez: wdrażanie nowych wersji oprogramowania systemowego i użytkowego, instalacją poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy? * Czy jednostka określiła zasady i podejmuje działania związane z minimalizowaniem ryzyka utraty informacji poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych, w tym np.: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia (ang. load balancing), monitorowania parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowania systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych? * Czy jednostka określiła zasady i podejmuje działania związane z zastosowaniem mechanizmów kryptograficznych dla transmisji danych do urządzeń mobilnych i dla poczty elektronicznej, a także z zastosowaniem podpisów kwalifikowanych do autoryzacji dokumentów? * Czy jednostka określiła zasady i podejmuje działania w związku z dostrzeżeniem nieujawnionych podatności systemów teleinformatycznych? * Czy jednostka określiła zasady i podejmuje działania związane z kontrolą zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa? | * Plan postępowania z ryzykiem. * Dokumentacja techniczna zabezpieczeń oraz procedury stosowania zabezpieczeń. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających | *N/d* | * § 20 ust. 2 pkt 12 oraz ust. 4 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12 (12.5 Nadzór nad oprogramowaniem produkcyjnym)  (17.1 Ciągłość bezpieczeństwa informacji)  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli[[2]](#footnote-3) opracowany przez INTOSAI Working Group on IT Audit (WGITA) Załącznik VII matryca kontroli bezpieczeństwa informacji – matryca kontrola dostępu |
| **2.14** | **Rozliczalność działań w systemach informatycznych** | * Regulacje wewnętrzne zawierające zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. * Działania związane z zapewnieniem rozliczalności użytkowników, szczególnie posiadających uprawnienia: administrowania systemami użytkowymi, zmiany konfiguracji systemów operacyjnych i ich zabezpieczeń, przetwarzania danych podlegających prawnej ochronie. * Działania związane z zapewnieniem rozliczalności działań użytkowników lub obiektów systemowych a także rejestracji innych zdarzeń systemowych w zakresie wynikającym z analizy ryzyka. * Działania związane z regularnym przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych. * Okres i sposób przechowywania dzienników systemowych. | * Czy, a jeżeli tak, to jakie regulacje wewnętrzne zawierają zasady dot. rozliczalności działań w systemach informatycznych? * W jaki sposób prowadzone są działania związane z zapewnieniem rozliczalności użytkowników lub obiektów, a także rejestracji innych zdarzeń systemowych w zakresie wynikającym z analizy ryzyka? * Czy, a jeżeli tak, w jaki sposób prowadzone są działania związane z regularnym przeglądaniem logów i ich analizą w celu identyfikacji działań niepożądanych? * Jaki jest okres i sposób przechowywania dzienników systemowych? * Czy wszyscy użytkownicy i administratorzy systemów informatycznych posiadają indywidualne konta? * Czy w zasadach PBI wprowadzono zakaz współdzielenia kont, zakaz przekazywania hasła do własnego konta innym pracownikom? * Czy predefiniowane konta administratorów systemów informatycznych i operacyjnych, baz danych etc. są zablokowane, a ich hasła zabezpieczone przed nieautoryzowanym użyciem? * Czy jednostka określiła zasady i wykorzystuje dzienniki systemowe (logi), w których odnotowuje się działania użytkowników, administratorów lub obiektów systemowych do zapewnieniem rozliczalności użytkowników, tj. do analizy, czy wykonywane przez nich operacje w systemie informatycznym są zgodne z ich kompetencjami? * Czy jednostka określiła odrębne zasady i podejmuje działania związane z zapewnieniem rozliczalności użytkowników posiadających szczególne uprawnienia np. do administrowania systemami, do zmiany konfiguracji systemów informatycznych i operacyjnych i ich zabezpieczeń, do przetwarzania danych podlegających prawnej ochronie? * Czy jednostka określiła zasady i podejmuje działania związane z regularnym przeglądaniem logów i ich analizą w celu identyfikacji innych działań niepożądanych? * Jakie są zasady zabezpieczenia logów systemowych przed nieautoryzowaną zmianą? | * Dokumenty zawierające analizę ryzyka. * Dokumentacja dzienników systemowych, w tym: procedury prowadzenia i dostępu do dzienników systemowych. * Dokumentacja wykonywania ww. procedur. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Przeprowadzenie przeglądu, przez pracowników podmiotu publicznego w obecności kontrolerów, próby logów z wybranego okresu czasu. | * § 21 rozporządzenia KRI   PN-ISO/IEC 27002:2014-12  (9.4 Kontrola dostępu do systemów i aplikacji)  (9.3 Odpowiedzialność użytkowników)  (12.4 Rejestrowanie zdarzeń i monitorowanie)  Podręcznik kontroli systemów informatycznych dla najwyższych organów kontroli opracowany przez INTOSAI Working Group on IT Audit (WGITA). Załącznik VII matryca kontroli bezpieczeństwa informacji – matryca kontrola dostępu |
| **Ocena obszaru powinna odnosić się do celów funkcjonowania systemu zarządzania bezpieczeństwem informacji na tle zadań realizowanych przez kontrolowaną jednostkę.**  **W szczególności ocena może się odnieść do zapewnienia:** (§ 20 rozporządzenia KRI)   * poufności przetwarzanych informacji, co należy rozumieć jako skuteczne ograniczenie dostępu osobom nieuprawnionym, * dostępności przetwarzanych informacji, co jest rozumiane jako możliwość wykorzystania danych na żądanie i w wymaganym czasie, * integralności przetwarzanych informacji, na którą składa się zapewnienie danym:   + autentyczności, tj. zgodności informacji ze stanem rzeczywistym;   + rozliczalności, tj. zapisu przy każdej edycji stosownej informacji o osobie lub podmiocie dokonującym zmiany, o czasie tej zmiany i jej zakresie;   + niezaprzeczalności, tj. identyfikacji wszystkich podmiotów biorących udział w wymianie i przetwarzaniu danych;   + niezawodności, tj. zdolności do przetwarzania w określonych warunkach, przez określony czas lub dla określonej liczby operacji.   **Ocena negatywna w obszarze nr 2 (bezpieczeństwo informacji) może zostać przyznana w szczególności, gdy:**   * nie opracowano, nie ustanowiono i nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) (§ 20 ust. 1 rozporządzenia); * nie została opracowana i wdrożona Polityka Bezpieczeństwa Informacji (Polityka BI) (§ 20 ust. 1 , ust. 2 pkt 12h rozporządzenia); * nie jest przeprowadzana okresowa analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz nie są podejmowane działania minimalizujące to ryzyko, stosownie do wyników przeprowadzonej analizy (§ 20 ust. 2 pkt 3 rozporządzenia); * nie jest przeprowadzany audyt wewnętrzny w zakresie BI co najmniej raz w roku (§ 20 ust. 2 pkt 14 rozporządzenia); * nie zarządza się dostępem do systemów teleinformatycznych w sposób zapewniający, że osoby zaangażowane w proces przetwarzania informacji uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji (§ 20 ust. 2 pkt 4 rozporządzenia); * nie zapewniono szkolenia osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem określonych w zarządzeniu zagadnień (§ 20 ust. 2 pkt 6 rozporządzenia); * nie zapewniono, aby incydenty naruszenia bezpieczeństwa informacji były bezzwłocznie zgłaszane w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących (§ 20 ust. 2 pkt 13 rozporządzenia); * nie zabezpieczono informacji w sposób uniemożliwiający nieuprawnionemu ich ujawnienie, modyfikacje, usunięcie lub zniszczenie (§ 20 ust. 2 pkt 9 rozporządzenia; pkt 2.12 tematyki kontroli); * nie zapewniono, aby w dziennikach systemów zostały odnotowane obligatoryjnie działania użytkowników lub obiektów systemowych (§ 21 rozporządzenia). | | | | | | |
| **3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych** | | | | | | |
| **3.1** | Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych | * Spełnianie przez systemy teleinformatyczne urzędów służące prezentacji zasobów wymagań określonych w § 19 rozporządzenia KRI. * Działania na rzecz zapewnienia osobom niepełnosprawnym dostępności treści zawartych na stronach internetowych | * Które z udostępnianych treści są najistotniejsze dla użytkowników w kontekście zadań kontrolowanej jednostki? * Czy istotne treści są postrzegalne? Tj. czy informacje oraz komponenty interfejsu zostały przedstawione w sposób dostępny dla osób z niepełnosprawnościami? * Czy istotne treści są funkcjonalne? Tj. czy interfejs oraz nawigacja są możliwe do użycia dla osób z niepełnosprawnościami? * Czy istotne treści są zrozumiałe? Tj. czy język treści jest zrozumiały i możliwy do odczytania maszynowego? Czy informacja udostępniona jest w logiczny i przewidywalny sposób? Czy wprowadzono mechanizmy wspierające i korygujące błędy użytkownika? * Czy istotne treści są kompatybilne? Tj. czy udostępniana treść może być poprawnie interpretowana przez różnych klientów użytkownika, w tym technologie wspierające dostęp do treści? * Jakie działania są podejmowane przez kontrolowanego w celu spełnienia wymagać WCAG 2.0? | * Opis zastosowanych rozwiązań technicznych umożliwiających osobom niedosłyszącym lub niedowidzącym zapoznanie się z treścią informacji na stronach internetowych systemów teleinformatycznych podmiotu publicznego. * Dokumentacja systemu teleinformatycznego. * Raporty z audytów / kontroli zew. / innych badań oceniających. | * Weryfikacja wybranych podstron, mediów lub udostępnionych materiałów (próby losowe albo celowe np. podstrony z największą liczbą odsłon, media najczęściej wykorzystywane przez użytkowników, najczęściej ściągane materiały). * Przeprowadzenie pełnego audytu sposobu prezentacji informacji na stronach internetowych systemów telekomunikacyjnych podmiotu publicznego z wykorzystaniem eksperta lub specjalistycznego oprogramowania walidacyjnego. | § 19 rozporządzenia KRI  35 wymagań, które należy spełnić wymienionych zostało w zał. nr 4 do KRI.  Web Content Accessibility Guidelines WCAG 2.0. Polska wersja z dnia 9 lipca 2013 r. opublikowana przez Forum Dostępnej Cyberprzestrzeni pod adresem <http://www.fdc.org.pl/wcag2/> |
| **Pełna dostępność informacji zawartych na stronach internetowych urzędów, zgodnie z § 19 rozporządzenia jest zapewniona tylko wtedy, gdy spełnionych jest wszystkich 35 wymagań wymienionych w załączniku nr 4 do KRI. Systemy teleinformatyczne służące do prezentacji danych stworzone po 31 maja 2012 r. powinny uwzględniać § 19 KRI w momencie ich budowania. Systemy, które już istniały w dniu 31 maja 2012 r. powinny zostać dostosowane do wymogów § 19 KRI do dnia 31 maja 2015 r.**  **Ocena negatywna w obszarze nr 3 (dostosowanie dla osób niepełnosprawnych) powinna zostać przyznana gdy nie zapewniono spełnienia wymagań Web Content Accessibility Guidelines (WCAG 2.0).** | | | | | | |

1. <http://mc.bip.gov.pl/centralne-repozytorium-wzorow-dokumentow-elektronicznych/43003_centralne-repozytorium-wzorow-dokumentow-elektronicznych.html> [↑](#footnote-ref-2)
2. <https://www.nik.gov.pl/plik/id,12303.pdf> [↑](#footnote-ref-3)