Ramowy program kontroli

w zakresie wykorzystywania systemów teleinformatycznych do realizacji zadań publicznych

wrzesień 2017 r.

## Wstęp

Mając na uwadze wyznaczone przez Szefa Kancelarii Prezesa Rady Ministrów priorytety kontroli na rok 2017, wagę bezpieczeństwa informacji przetwarzanych w systemach teleinformatycznych wykorzystywanych do realizacji zadań publicznych oraz zapewnienie profesjonalnego wsparcia dla kontroli prowadzonych przez jednostki administracji rządowej, Centrum Oceny Administracji Kancelarii Prezesa Rady Ministrów, przy współpracy z Ministerstwem Cyfryzacji, Ministerstwem Spraw Zagranicznych oraz Zachodniopomorskim Urzędem Wojewódzkim, opracowało *Ramowy program kontroli w zakresie wykorzystywania systemów teleinformatycznych do realizacji zadań publicznych*.

*Ramowy program* jest wsparciem dla kontrolerów w przygotowaniu indywidualnych programów kontroli w *zakresie działania systemów teleinformatycznych używanych do realizacji zadań publicznych*, które prowadzi się na podstawie ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*[[1]](#footnote-2) (dalej: *ustawa o informatyzacji*).

*Ramowy program* nie jest obligatoryjny, może on być wykorzystywany w części lub w całości wraz z *Wytycznymi Ministerstwa Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych*[[2]](#footnote-3) (dalej: *Wytyczne*).

## Temat kontroli

Działanie i bezpieczeństwo systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych.

[*Temat kontroli można uzupełnić o okres objęty kontrolą, np. Działanie i bezpieczeństwo systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych w latach 2015-2016.]*

## Podmiot kontrolowany

*[Pełna nazwa i adres]*

Kontroli podlegają podmioty prowadzące rejestry publiczne i realizujące zadania publiczne z wykorzystaniem systemów teleinformatycznych, w szczególności mogą to być:

* podmioty realizujące sektorowe i ponadsektorowe projekty informatyczne,
* podmioty publicznie podległe lub nadzorowane przez organy administracji rządowej,
* jednostki samorządu terytorialnego i ich związki oraz tworzone lub prowadzone przez te jednostki samorządowe osoby prawne i inne samorządowe jednostki organizacyjne, w zakresie systemów oraz rejestrów używanych do realizacji zadań zleconych z zakresu administracji rządowej.

## Okres objęty kontrolą

*[Daty dzienne, miesięczne lub wskazanie lat objętych kontrolą, ew. „do dnia rozpoczęcia czynności kontrolnych” / „do dnia zakończenia czynności kontrolnych” / „z możliwością zasięgania informacji z okresów wcześniejszych”.]*

Np. Od dnia 1 stycznia 2016 r. do dnia rozpoczęcia kontroli z możliwością zasięgania informacji z okresów wcześniejszych, jeżeli miały wpływ na kontrolowane zagadnienie.

## Cel kontroli

Celem kontroli jest racjonalne zapewnienie, że systemy teleinformatyczne wykorzystywane do realizacji zadań publicznych, w tym rejestry publiczne, spełniają minimalne wymagania w zakresie elektronicznej wymiany informacji (interoperacyjności), są bezpieczne i dostępne dla wszystkich obywateli[[3]](#footnote-4).

W szczególności zadaniem kontroli jest ocena zapewnienia:

* spójności rejestrów publicznych oraz współdziałania różnych systemów teleinformatycznych poprzez właściwą organizację wymiany informacji w postaci elektronicznej, współpracę z innymi systemami/rejestrami informatycznymi oraz procesy wspomagania świadczenia usług drogą elektroniczną,
* skutecznego zarządzania bezpieczeństwem informacji dla badanych systemów teleinformatycznych, w tym zapewnienia dostępności, autentyczności, poufności, niezawodności i integralności danych przetwarzanych przez system,
* dostępności treści zawartych na stronach internetowych dla osób z niepełnosprawnościami.

Kryterium kontroli: legalność, celowość, rzetelność.

*[W przypadku kontroli realizowanej w jednostkach samorządu terytorialnego, ich związkach oraz samorządowych jednostkach organizacyjnych, cel i przedmiot kontroli powinien ograniczać się do systemów teleinformatycznych i rejestrów publicznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej. W zakresie pozostałych systemów kontrola może być prowadzona wyłącznie na wniosek[[4]](#footnote-5).*

*Dla kontroli realizowanej w jednostkach samorządu terytorialnego kryteriami kontroli powinny być legalność i rzetelność].*

## Informacje o kontroli

Kontrola prowadzona będzie na podstawie art. 25 ust. 1 pkt 3 lit. … *ustawy o informatyzacji*, w trybie ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[[5]](#footnote-6) (dalej: *ustawa o kontroli*).

*[Podstawa prowadzenia kontroli powinna być uzupełniona w zależności od podmiotu kontrolowanego]*

## Uzasadnienie kontroli

*[W tym miejscu należy wskazać faktyczną przyczynę podjęcia kontroli: realizacja priorytetów kontroli, realizacja planu kontroli, skarga, kontrola sprawdzająca, inicjatywa własna wynikająca z uzyskanych informacji, wynik analizy ryzyka, weryfikacja informacji medialnych o potencjalnych nieprawidłowościach itp.]*

*[Należy wskazać, czy przeprowadzenie kontroli wynika z obowiązków nadzoru.]*

## Wyniki analizy przedkontrolnej

*[W programie kontroli należy zamieścić wyniki analizy przedkontrolnej, tj. wstępne ustalenia i wnioski dokonane na podstawie zgromadzonej przed rozpoczęciem kontroli dokumentacji (np. dokumentacji wskazanej w pkt III.5 Wytycznych MC).*

Przed rozpoczęciem czynności kontrolnych w trybie art. 15 *ustawy o kontroli* można pozyskać i przeanalizować poniższe dokumenty i zestawienia:

* *Informacje zgodne z ankietą dotyczącą działania systemów teleinformatycznych używanych do realizacji zadań publicznych (zał. nr 1 do Wytycznych).*
* *Zestawienie systemów teleinformatycznych używanych do realizacji zadań publicznych (zał. nr 2 do Wytycznych).*
* *Dokumentacja i regulacje wewnętrzne dotyczące Systemu Zarządzania Bezpieczeństwem Informacji (dalej: SZBI), w tym Polityka Bezpieczeństwa Informacji.*
* *Regulamin organizacyjny.*

Na podstawie informacji uzyskanych przed kontrolą zaleca się*:*

* *wstępne rozpoznanie profilu i statutowych zadań jednostki kontrolowanej,*
* *wstępne rozpoznanie systemów i rejestrów publicznych wykorzystywanych do realizacji zadań publicznych,*
* *wstępny wybór do badania szczegółowego systemów, ze szczególnym uwzględnieniem systemów wykorzystywanych do realizacji zadań publicznych,*
* *wstępną ocenę dokumentacji składającej się na SZBI, w szczególności, czy obejmuje wszystkie niezbędne obszary,*
* *wstępnej oceny SZBI, w tym wniosków z przekazanych ankiet,*
* *wstępnej weryfikacji informacji oraz sygnałów zewnętrznych, w tym skarg i przekazów medialnych.].*

**Zidentyfikowane ryzyka związane z kontrolą**

*[Należy zidentyfikować ryzyka związane z kontrolą oraz oszacować prawdopodobieństwo ich materializacji i wpływ na realizację celów kontroli]*

***Przykłady ryzyk:***

* *niewielkie doświadczenie kontrolerów w kontroli tego obszaru,*
* *może wystąpić utrudniony dostęp do dokumentacji niektórych systemów oraz wyjaśnień administratorów, np. w przypadku opieki nad serwerami przez firmy zewnętrzne na podstawie zawartych umów,*
* *duża liczba albo różnorodność systemów IT,*
* *brak albo duża liczba dokumentów do kontroli,*
* *niska świadomość w zakresie wymagań i standardów IT,*
* *wnioskowanie na podstawie niereprezentatywnej próby lub dowodów o małej istotności.*

## Czynniki ryzyka mające wpływ na działalność jednostki kontrolowanej i ich możliwe skutki w postaci potencjalnych nieprawidłowości

*[Należy wskazać czynniki ryzyka mogące mieć negatywny wpływ na działalność systemów teleinformatycznych wykorzystywanych do realizacji zadań jednostki kontrolowanej. Można je ująć w postaci potencjalnych nieprawidłowości. Jeśli jest to możliwe, należy określić również prawdopodobieństwo ich wystąpienia oraz oszacować potencjalny wpływ na realizację najważniejszych zadań jednostki.*

*Przykłady analizy ryzyka: w analizie ryzyka należy uwzględnić mechanizmy kontroli oraz siłę (tj. adekwatność, skuteczność i efektywność) kontroli zarządczej*

|  |  |
| --- | --- |
| **Czynnik ryzyka/ potencjalna nieprawidłowość** | **Pomiar ryzyka\*** |
| **Prawdopodo-bieństwo** | **Wpływ/ Skutek** | **Iloczyn ryzyka** | **Wynik pomiaru**  |
| Niespełnienie wymagań interoperacyjności na poziomie organizacyjnym | 4 | 3 | 12 | duże |
| Niewdrożenie WCAG 2.0 | 4 | 2 | 8 | średnie |
| Brak Systemu Zarządzania Bezpieczeństwem Informacji | 1 | 4 | 4 | małe |
| … | … | … | … | … |
| … | … | … | … | … |

*\*) Skala pomiaru ryzyka: małe (1-4), średnie (5-8), wysokie (9-12), bardzo wysokie (13-16).*

*Przy szacowaniu prawdopodobieństwa i wpływu przyjęto czterostopniową skalę, tj. 1 – małe, 2 – średnie, 3 – wysokie, 4 – bardzo wysokie.*

## Tematyka kontroli

Szczegółowy zakres metodyki kontroli został określony w załączniku nr 1 do niniejszego Programu.

1. **W jaki sposób organizacja wymiany informacji w postaci elektronicznej, w tym zasady współpracy z innymi systemami/rejestrami informatycznymi oraz procesy wspomagania świadczenia usług drogą elektroniczną zapewniają spójność rejestrów publicznych i wspierają współdziałanie systemów teleinformatycznych?**
2. W jaki sposób realizacja usług drogą elektroniczną ułatwia obywatelom i innym urzędom dostęp do świadczonych usług? Jakie działania są podejmowane w celu poszerzenia dostępu do usług drogą elektroniczną?
3. Jak kontrolowany zwiększa zdolności współdziałania systemów teleinformatycznych i rejestrów publicznych? Czy wykorzystuje wzory dokumentów elektronicznych przechowywanych w CRWDE oraz przekazuje własne wzory do tego repozytorium?
4. W jaki sposób zapewnia się przejrzystość zarządzania usługami elektronicznymi? Czy sposób świadczenia usług elektronicznych oparto o model usługowy?
5. Jak zwiększa się zdolność kontrolowanych systemów, w tym rejestrów publicznych do współpracy z innymi systemami lub rejestrami publicznymi? Jakie działania są podejmowane w celu poszerzania zakresu interoperacyjności posiadanych systemów i rejestrów? Czy te działania są skuteczne?
6. W jakim stopniu elektroniczny obieg dokumentów wpływa na uporządkowanie, usprawnianie, zabezpieczenie przepływu dokumentów w jednostce oraz zachowanie wiedzy instytucjonalnej?
7. W jaki sposób zapewniono możliwość wymiany danych pomiędzy systemami informatycznymi. Czy dane są udostępniane w powszechnie dostępnych formatach plików?
8. **W jaki sposób zapewniono skuteczność zarządzania bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych, w tym dostępność, autentyczność, poufność, niezawodność i integralność przetwarzanych danych?**
9. W jaki sposób dokumentacja systemu zarządzania bezpieczeństwem informacji zapewnia o jego działaniu? Czy dokumentacja ta obejmuje najistotniejsze obszary działalności jednostki oraz zapewnia dostępność, autentyczność, poufność, niezawodność i integralność przetwarzanych danych?
10. Jak zarządza się ryzykiem dla bezpieczeństwa informacji? Czy prowadzona jest analiza ryzyka w celu przeciwdziałania utracie integralności, dostępności i poufności informacji? Czy realizowane są działania mające na celu minimalizację materializacji zidentyfikowanych ryzyk?
11. W jaki sposób zarządza się infrastrukturą informatyczną? Czy istnieje bieżąca i aktualna informacja nt. sprzętu i oprogramowania wykorzystywanych do przetwarzania informacji?
12. W jaki sposób zapewnia się poufność danych w systemach informatycznych? Czy proces zarządzania uprawnieniami zapewnia dostęp wyłącznie uprawnionym użytkownikom i tylko w zakresie adekwatnym do realizowanych przez nich obowiązków?
13. W jaki sposób podnosi się kompetencje oraz wiedzę z zakresu bezpieczeństwa wśród osób zaangażowanych w procesy wymiany informacji? Czy wszystkim pracownikom uczestniczącym w przetwarzaniu informacji zapewniono niezbędną wiedzę na temat zasad i systemu bezpieczeństwa informacji?
14. Jakie działania są podejmowane w celu zapewnienia bezpieczeństwa informacji przetwarzanych na odległość, w tym spoza siedziby kontrolowanego? Czy określono reguły i zasady pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość? Jakie inne mechanizmy zapewniają bezpieczeństwo informacji przetwarzanych na odległość? Czy są one wystarczające?
15. W jaki sposób regulacje wewnętrzne, w tym określające zasady współpracy z podmiotami zewnętrznym oraz umowy zawierane przez kontrolowanego gwarantują bezpieczny rozwój oprogramowania i szybkie uruchomienie systemów po awarii oraz zapewniają poufność informacji uzyskanych przez wykonawców umów?
16. Jakie działania są podejmowane w celu identyfikacji incydentów bezpieczeństwa oraz zapobiegania ich występowaniu w przyszłości? Czy są one skuteczne?
17. W jaki sposób wykorzystuje się wyniki audytów w zakresie bezpieczeństwa informacji (wewnętrznych i zewnętrznych)? W jaki sposób przyczyniły się one do wykrywania słabości i doskonalenia systemu zarządzania bezpieczeństwem informacji?
18. Jakie działania podejmuje kontrolowany w celu zapewnienia ciągłości działania systemów teleinformatycznych? Czy tworzy, przechowuje i testuje kopie zapasowe najważniejszych danych?
19. W jaki sposób zapewnia się funkcjonalność, niezawodność, używalność, wydajność, przenaszalność i pielęgnowalność systemów informatycznych na etapach ich projektowania, wdrażania i eksploatacji?
20. W jaki sposób stosowane zabezpieczenia techniczno-organizacyjne zapewniają ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami?
21. W jaki sposób stosowane zabezpieczenia techniczno-organizacyjne redukują ryzyka dla systemów informatycznych wynikające w szczególności z ich podatności na błędy, awarie, wirusy komputerowe, włamania lub obciążenia środowiskowe (np. wilgotność, temperatura, zadymienie)?
22. W jaki sposób zapewnia się rozliczalność działań w systemach informatycznych? Czy kontrolowany gromadzi informacje o tym, kto, kiedy i co wykonał w systemie teleinformatycznym?
23. **W jaki sposób zastosowane rozwiązania techniczne zapewniają dostępność treści zawartych w systemach teleinformatycznych?**
24. Jak uwzględnia się potrzeby osób z niepełnosprawnościami? Czy sposób prezentacji zasobów informacji uwzględnia wymagania Web Content Accessibility Guidelines (WCAG 2.0) na poziomie AA?
25. Jakie działania podjęto na rzecz zapewnienia osobom niepełnosprawnym dostępności treści zawartych na stronach internetowych? Czy były skuteczne? W jakim terminie kontrolowany zapewni dostępność treści zawartych na stronach internetowych?

## Stan prawny przedmiotu kontroli

1. Ustawa z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2017 r. poz. 570 j.t. ze zm.).
2. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. z 2016 r. poz. 113 j.t.).
3. *Standardy kontroli w administracji rządowej* z dnia 31 sierpnia 2017 r.
4. *Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych* zatwierdzone przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

*[Należy również wskazać przepisy regulujące działalność kontrolowanego w tym np. statut oraz zarządzenia wprowadzające Politykę Bezpieczeństwa Informacji]*

## Termin, organizacja i harmonogram realizacji

Zakładana pracochłonność czynności kontrolnych: *[np. 50 kontrolerodni, tj. 25 dni roboczych dwóch kontrolerów].*

|  |
| --- |
| **Plan dla kontroli jednostkowej** (tryb zwykły) |
| Zakładana pracochłonność | **…** | kontrolerodni |
| Zespół kontrolny | **…** | osoby |
| **Istotne przewidywane *kamienie milowe* w kontroli:** | **Data/Okres** | **dzień tygodnia** |
| Data rozpoczęcia czynności kontrolnych: | **…** | … |
| Planowana data przedstawienia osobie nadzorującej komórkę kontroli wstępnej wersji projektu wystąpienia pokontrolnego | **…** | … |
| Planowana data zakończenia czynności kontrolnych | **…** | … |
| Czas potrzebny na przygotowanie ostatecznej wersji projektu wystąpienia pokontrolnego przez kontrolerów (liczony od zakończenia czynności kontrolnych)\* | **… tygodnie** |

## Zespół kontrolny

*[****Kwalifikacje kontrolerów.***

*Zgodnie z art. 28 ust. 1 ustawy o informatyzacji kontrolerem może być osoba pełnoletnia, która:*

* *posiada wykształcenie wyższe,*
* *posiada obywatelstwo państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej lub państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) - strony umowy o Europejskim Obszarze Gospodarczym, chyba że przepisy odrębne uzależniają zatrudnienie jej w jednostce kontrolowanej od posiadania obywatelstwa polskiego,*
* *ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,*
* *nie była karana za umyślne przestępstwo lub umyślne przestępstwo skarbowe,*
* *posiada certyfikat, o którym mowa w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych*[[6]](#footnote-7)*.*

*Certyfikaty uprawniające do przeprowadzania kontroli w rozumieniu art. 25 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, to:*

* *Audytor systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC*

*27001 lub jej odpowiednika międzynarodowego.*

* *Audytor systemu zarządzania usługami informatycznymi według normy PN ISO/IEC 20000 lub jej odpowiednika międzynarodowego.*
* *Audytor systemu zarządzania jakością według normy PN ISO/IEC 9001 lub jej odpowiednika międzynarodowego.*
* *Certified Information System Auditor (CISA).*
* *Certified in the Governance of Enterprise IT (CGEIT).*
* *Certified Internal Auditor (CIA).*
* *Certified Information Systems Security Professional (CISSP).*
* *Europejski Certyfikat Umiejętności Zawodowych Informatyka - EUCIP Professional*
* *specjalizacja Audytor Systemów Informacyjnych.*
* *Systems Security Certified Practitioner (SSCP).]*

*[****Tajemnica kontroli.*** *Zgodnie z art. 28 ust. 2 ustawy o informatyzacji Kontroler jest obowiązany zachować w tajemnicy informacje, które uzyskał w związku z wykonywaniem czynności kontrolnych. Obowiązek zachowania tajemnicy trwa również po ustaniu pełnienia obowiązków kontrolera w urzędzie obsługującym organ dokonujący kontroli.]*

*[Każdy kontroler powinien podpisać oświadczenie o bezstronności – według wzoru zał.
nr 2 oraz oświadczenie o spełnianiu wymagań dla kontrolera systemów teleinformatycznych i o zachowaniu poufności – według wzoru zał. nr 3]*

Kierownik zespołu kontrolnego: [*podpis]*

Kontroler: … [*podpis]*

Kontroler: … [*podpis]*

*[Informacja kto opracował oraz kto akceptował program]*

**Załączniki:**

1. *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*.
2. *Wzór oświadczenia o bezstronności.*
3. *Wzór oświadczenia o spełnieniu wymagań określonych dla kontrolera oraz o zachowaniu poufności.*
1. Z dnia 17 lutego 2005 r., Dz. U. z 2017 r. poz. 570 j.t. ze zm. [↑](#footnote-ref-2)
2. Zatwierdzone w dniu 15 grudnia 2015 r. przez Ministra Cyfryzacji, panią Annę Streżyńską: http://mc.bip.gov.pl/wytyczne/wytyczne-dla-kontroli-dzialania-systemow-teleinformatycznych-uzywanych-do-realizacji-zadan-publicznych.html [↑](#footnote-ref-3)
3. Zgodnie z art. 25 ust. 1 pkt 3 ustawy *o informatyzacji.* [↑](#footnote-ref-4)
4. Art. 25 ust. 3 ustawy o informatyzacji*.* [↑](#footnote-ref-5)
5. Dz. U. Nr 185, poz. 1092. [↑](#footnote-ref-6)
6. Z dnia 10 września 2010 r., Dz.U. z 2010 Nr 177, poz. 1195. [↑](#footnote-ref-7)