Warszawa, dnia 5 marca 2026 r.

Poz. 263

OBWIESZCZENIE MINISTRA CYFRYZACJI[1)]

z dnia 21 lutego 2026 r.

w sprawie włączenia kwalifikacji wolnorynkowej „Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji” do Zintegrowanego Systemu Kwalifikacji

Na podstawie art. 25 ust. 1 i 2 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2024 r. poz. 1606) ogłasza się w załączniku do niniejszego obwieszczenia informacje o włączeniu kwalifikacji wolnorynkowej „Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji” do Zintegrowanego Systemu Kwalifikacji.

Minister Cyfryzacji: wz. *D. Standerski*

1) Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 2720).

Załącznik do obwieszczenia Ministra Cyfryzacji
z dnia 21 lutego 2026 r. (M.P. poz. 263)

INFORMACJE O WŁĄCZENIU KWALIFIKACJI WOLNORYNKOWEJ „ZAPEWNIANIE CYBERBEZPIECZEŃSTWA ROZWIĄZAŃ CHMUROWYCH W ORGANIZACJI” DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

1. Nazwa kwalifikacji wolnorynkowej

Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji

2. Poziom Polskiej Ramy Kwalifikacji przypisany do kwalifikacji wolnorynkowej

5 poziom Polskiej Ramy Kwalifikacji

3. Efekty uczenia się wymagane dla kwalifikacji wolnorynkowej

Syntetyczna charakterystyka efektów uczenia się
Osoba posiadająca kwalifikację wolnorynkową „Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji” zapewnia cyberbezpieczeństwo rozwiązań chmurowych w organizacji, uwzględniając zmienne, nie w pełni przewidywalne warunki, w tym te związane z intencjonalnymi atakami cybernetycznymi (np. phishing, ransomware, ataki typu DDoS – *Distributed Denial of Service*) oraz z pogorszeniem parametrów niezawodności i jakości usług chmurowych. Identyfikuje uwarunkowania związane z zapewnianiem cyberbezpieczeństwa rozwiązań chmurowych w organizacji, w tym uwarunkowania wynikające z obowiązujących aktów prawnych, oczekiwań właścicieli procesów biznesowych oraz dostępnej infrastruktury. Analizuje obowiązujące akty prawne dotyczące cyberbezpieczeństwa rozwiązań chmurowych w organizacji oraz dokumentację techniczną wykorzystywanych rozwiązań chmurowych w organizacji. Na podstawie dokumentacji dostawcy rozwiązań chmurowych w organizacji określa poziom cyberbezpieczeństwa tych rozwiązań chmurowych oraz analizuje możliwości zastosowania różnych mechanizmów zapewniających ich cyberbezpieczeństwo. Identyfikuje ryzyko związane z korzystaniem z poszczególnych rozwiązań chmurowych w organizacji oraz wskazuje potencjalne skutki wystąpienia incydentów naruszających cyberbezpieczeństwo tych rozwiązań. Proponuje koncepcję zabezpieczenia rozwiązania chmurowego w organizacji z wykorzystaniem różnorodnych metod i rozwiązań. Uzasadnia przedstawione propozycje, wskazując wady i zalety poszczególnych rozwiązań oraz związane z nimi koszty i ograniczenia. Analizuje koszty związane z zapewnianiem cyberbezpieczeństwa rozwiązań chmurowych w organizacji oraz analizuje efektywność działań zapewniających cyberbezpieczeństwo tych rozwiązań.

Zestaw 1. Analiza cyberbezpieczeństwa rozwiązań chmurowych w organizacji	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Identyfikuje wymagania prawne dotyczące zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji	– wskazuje typy działalności i dane objęte obowiązującymi aktami prawnymi w kontekście cyberbezpieczeństwa rozwiązań chmurowych w organizacji, – wskazuje obowiązujące akty prawne mogące mieć wpływ na zakres i sposób zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji, – omawia wymagania dotyczące zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji – na podstawie obowiązujących aktów prawnych.

Identyfikuje oczekiwania dotyczące zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji	– formułuje pytania mające zidentyfikować oczekiwania właścicieli procesów biznesowych w zakresie zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji, – identyfikuje uwarunkowania biznesowe i organizacyjne wpływające na wymagania dotyczące zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji, – identyfikuje, w jaki sposób są udostępniane rozwiązania chmurowe w organizacji.
Analizuje możliwości wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji	– formułuje pytania mające zidentyfikować możliwości organizacyjne, techniczne, czasowe i finansowe wdrożenia i stosowania w organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych, – opisuje możliwości oraz ograniczenia związane z wdrożeniem i stosowaniem w organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji – na podstawie dokumentacji technicznej wykorzystywanych systemów teleinformatycznych, – wskazuje bariery w zastosowaniu w danej organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych – wynikające z uwarunkowań biznesowych, organizacyjnych i prawnych.

Zestaw 2. Analiza ryzyka w zakresie cyberbezpieczeństwa rozwiązań chmurowych w organizacji	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Analizuje poziom cyberbezpieczeństwa rozwiązań chmurowych w organizacji	– opisuje rodzaje rozwiązań chmurowych w organizacji, ich właściwości oraz słabe i mocne strony w zakresie zapewniania cyberbezpieczeństwa, – opisuje możliwe zagrożenia dla poufności, integralności oraz dostępności danych i systemów teleinformatycznych związane z wykorzystywaniem danego rozwiązania chmurowego w organizacji, – określa poziom cyberbezpieczeństwa rozwiązania chmurowego w organizacji oraz możliwości stosowania rozwiązań zapewniających cyberbezpieczeństwo – na podstawie dokumentacji dostawcy, – porównuje rozwiązania chmurowe w organizacji pod względem deklarowanego przez dostawcę poziomu cyberbezpieczeństwa oraz możliwości zastosowania rozwiązań zapewniających cyberbezpieczeństwo.
Analizuje rozwiązanie chmurowe w organizacji pod względem zagrożeń dla cyberbezpieczeństwa tego rozwiązania	– wyjaśnia pojęcia poufności, integralności oraz dostępności danych i systemów teleinformatycznych związane z wykorzystywaniem danego rozwiązania chmurowego w organizacji, – wskazuje zagrożenia dla cyberbezpieczeństwa rozwiązania chmurowego w organizacji oraz poufności, integralności i dostępności przetwarzanych w nim danych – na podstawie opisu architektury lub diagramu przepływu danych, – identyfikuje miejsca wystąpienia zagrożenia dla cyberbezpieczeństwa w rozwiązaniu chmurowym w organizacji – na podstawie opisu architektury tego rozwiązania lub diagramu przepływu danych, – identyfikuje rozwiązania chmurowe w organizacji, których cyberbezpieczeństwo jest kluczowe z punktu widzenia działalności organizacji i obowiązujących ją wymagań zewnętrznych, – opisuje skutki dla organizacji wynikające z naruszenia cyberbezpieczeństwa rozwiązania chmurowego.

Ocenia ryzyko wystąpienia zagrożenia dla cyberbezpieczeństwa rozwiązań chmurowych w organizacji	– szacuje prawdopodobieństwo wystąpienia zagrożenia dla cyberbezpieczeństwa rozwiązania chmurowego w organizacji, a także poufności, integralności oraz dostępności przetwarzanych w nim danych, – opisuje skutki wystąpienia incydentu naruszającego cyberbezpieczeństwo rozwiązania chmurowego w organizacji, – ustala poziom i istotność ryzyka dla poszczególnych zagrożeń dotyczących cyberbezpieczeństwa rozwiązania chmurowego w organizacji.

Zestaw 3. Opracowanie koncepcji zapewniania cyberbezpieczeństwa rozwiązań chmurowych w organizacji	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
Analizuje mechanizmy zapewniające cyberbezpieczeństwo rozwiązań chmurowych w organizacji	– omawia typy, wady i zalety mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji (np. szyfrowanie danych, system zapobiegający wyciekowi danych), – porównuje skuteczność różnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji, – omawia warunki wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji, – opisuje zasady doboru mechanizmów zapewniających cyberbezpieczeństwo do typu rozwiązań chmurowych w organizacji, zidentyfikowanych zagrożeń i oczekiwanego poziomu cyberbezpieczeństwa, – wyjaśnia ograniczenia wynikające z zastosowania różnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji.
Analizuje koszty wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji	– opisuje rodzaje kosztów związanych z wdrożeniem i stosowaniem poszczególnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji, – szacuje koszty wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji, – ocenia efektywność zastosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji w odniesieniu do kosztów ich wdrożenia i stosowania, skuteczności działania i zapewniania poziomu cyberbezpieczeństwa, – ocenia zasadność wprowadzenia poszczególnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych w organizacji w odniesieniu do poziomu i istotności ryzyka dla danego zagrożenia.
Proponuje działania zapewniające cyberbezpieczeństwo rozwiązania chmurowego w organizacji	– przygotowuje warianty zapewniania cyberbezpieczeństwa rozwiązania chmurowego w organizacji, – porównuje wady i zalety oraz warunki wdrożenia i stosowania przedstawionych wariantów zapewniania cyberbezpieczeństwa rozwiązania chmurowego w organizacji, – wyjaśnia ograniczenia przedstawionych wariantów zapewniania cyberbezpieczeństwa rozwiązania chmurowego w organizacji, – wskazuje działania i mechanizmy niezbędne do zrealizowania przedstawionego wariantu zapewniania cyberbezpieczeństwa rozwiązania chmurowego w organizacji.

4. Ramowe wymagania dotyczące metod przeprowadzania walidacji, osób przeprowadzających walidację oraz warunków organizacyjnych i materialnych niezbędnych do prawidłowego i bezpiecznego przeprowadzania walidacji

1. Etap weryfikacji

1.1. Metody przeprowadzania walidacji

Możliwe do stosowania metody walidacji to:

– test wiedzy,

– analiza dowodów i deklaracji, która może być uzupełniona wywiadem swobodnym (rozmową z komisją walidacyjną).

1.2. Osoby przeprowadzające walidację

Komisja walidacyjna składa się z minimum dwóch członków spełniających następujące warunki:

– w przypadku przewodniczącego komisji walidacyjnej – posiadanie kwalifikacji pełnej z 7 poziomem Polskiej Ramy Kwalifikacji (dyplom ukończenia studiów drugiego stopnia lub jednolitych studiów magisterskich) oraz co najmniej rocznego doświadczenia w przeprowadzaniu egzaminów w obszarze cyberbezpieczeństwa lub pokrewnych technologii cyfrowych, zdobytego w ciągu ostatnich 6 lat, oraz

– w przypadku asesora – posiadanie kwalifikacji pełnej z 6 poziomem Polskiej Ramy Kwalifikacji (dyplom ukończenia studiów pierwszego stopnia) oraz co najmniej rocznego doświadczenia w przeprowadzaniu egzaminów w obszarze cyberbezpieczeństwa lub pokrewnych technologii cyfrowych, zdobytego w ciągu ostatnich 3 lat.

Ponadto każdy z członków komisji walidacyjnej posiada udokumentowane co najmniej 3-letnie doświadczenie w obszarze projektowania, wdrażania rozwiązań chmurowych w organizacji lub zarządzania nimi lub w obszarze cyberbezpieczeństwa.

1.3. Warunki organizacyjne i materialne niezbędne do prawidłowego i bezpiecznego przeprowadzania walidacji

Walidacja odbywa się w trybie stacjonarnym, zdalnym albo hybrydowym.

Jeżeli walidacja jest organizowana w trybie stacjonarnym, instytucja prowadząca walidację zapewnia pracownię wyposażoną w stanowisko komputerowe dla każdej osoby przystępującej do walidacji.

Jeżeli walidacja jest organizowana w trybie zdalnym albo hybrydowym, instytucja prowadząca walidację zapewnia każdej osobie przystępującej do walidacji indywidualny dostęp do systemu obsługi testów i egzaminów. System ten ma umożliwiać komisji walidacyjnej stałą obserwację osoby przystępującej do walidacji, w szczególności: potwierdzenie jej tożsamości, kontrolę samodzielności pracy oraz zabezpieczenie przebiegu walidacji przed ingerencją osób trzecich. Dzięki temu możliwe będzie wiarygodne sprawdzenie, czy osoba ubiegająca się o nadanie kwalifikacji wolnorynkowej osiągnęła wyodrębnioną część albo całość efektów uczenia się wymaganych dla tej kwalifikacji.

2. Etap identyfikowania i dokumentowania efektów uczenia się

Instytucja prowadząca walidację może zapewniać wsparcie dla osób przystępujących do walidacji w zakresie identyfikowania oraz dokumentowania posiadanych efektów uczenia się. Korzystanie z tego wsparcia nie jest obowiązkowe.

Etapy identyfikowania i dokumentowania mogą być realizowane dowolnymi metodami.

5. Warunki, jakie musi spełnić osoba przystępująca do walidacji, jeżeli zostały określone, albo informacja o braku takich warunków

Brak warunków

6. Inne, poza pozytywnym wynikiem walidacji, warunki uzyskania kwalifikacji wolnorynkowej, jeżeli zostały określone, albo informacja o braku takich warunków

Brak innych, poza pozytywnym wynikiem walidacji, warunków uzyskania kwalifikacji wolnorynkowej

7. Okres ważności certyfikatu kwalifikacji wolnorynkowej – bezterminowy lub określony – oraz warunki przedłużenia ważności, jeżeli okres ważności certyfikatu został określony

Certyfikat jest ważny 3 lata. Przedłużenie ważności certyfikatu następuje na podstawie analizy dowodów i deklaracji potwierdzających wykonywanie w okresie ważności certyfikatu zadań związanych z zapewnianiem cyberbezpieczeństwa rozwiązań chmurowych w organizacji przez okres co najmniej 12 miesięcy.

8. Termin dokonywania przeglądu kwalifikacji wolnorynkowej

Nierzadziej niż raz na 10 lat