

Warszawa, dnia 17 lutego 2021 r.

Poz. 189

**OBWIESZCZENIE  
MINISTRA CYFRYZACJI<sup>1)</sup>**

z dnia 8 lutego 2021 r.

**w sprawie włączenia kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem – menedżer”  
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 2020 r. poz. 226) ogłasza się w załączniku do niniejszego obwieszczenia informacje o włączeniu kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem – menedżer” do Zintegrowanego Systemu Kwalifikacji.

Minister Cyfryzacji: *wz. M. Zagórski*

---

<sup>1)</sup> Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716).

INFORMACJE O WŁĄCZENIU KWALIFIKACJI RYNKOWEJ „ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM – MENEDŻER”  
DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

**1. Nazwa kwalifikacji rynkowej**

Zarządzanie cyberbezpieczeństwem – menedżer

**2. Nazwa dokumentu potwierdzającego nadanie kwalifikacji rynkowej**

Certyfikat

**3. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji rynkowej**

Certyfikat jest ważny 5 lat. Przedłużenie następuje na podstawie przedłożenia dokumentów potwierdzających:

- zatrudnienie przez minimum 3 lata w okresie ostatnich 5 lat poprzedzających przedłużenie certyfikatu w charakterze osoby odpowiedzialnej za realizację zadań tożsamy z uzyskaną kwalifikacją;
- ustawiczne doskonalenie kompetencji poprzez między innymi udział w konferencjach, szkoleniach, warsztatach o tematyce tożsamej z uzyskaną kwalifikacją w wymiarze minimum 200 godzin w okresie ostatnich 5 lat poprzedzających przedłużenie certyfikatu.

**4. Poziom Polskiej Ramy Kwalifikacji przypisany do kwalifikacji rynkowej (ewentualnie odniesienie do poziomu Sektorowej Ramy Kwalifikacji)**

6 poziom Polskiej Ramy Kwalifikacji

## 5. Efekty uczenia się wymagane dla kwalifikacji rynkowej

### Syntetyczna charakterystyka efektów uczenia się

Osoba z kwalifikacją „Zarządzanie cyberbezpieczeństwem – menedżer” posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi krajowymi i UE z obszaru cyberbezpieczeństwa. Posiada wiedzę dotyczącą opracowywania strategii cyberbezpieczeństwa w organizacji, wdrażania środków, planów i procedur bezpieczeństwa IT, zarządzania ryzykiem, ciągłości działania oraz incydentami cyberbezpieczeństwa i audytu bezpieczeństwa. Posiada wiedzę w zakresie funkcjonowania zespołów reagowania na incydenty bezpieczeństwa komputerowego. Dysponuje również wiedzą w obszarze bezpieczeństwa infrastruktury teleinformatycznej. Posiada również przygotowanie merytoryczne w obszarze zastosowań informatyki śledczej.

### Zestaw 1. Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa

Poszczególne efekty uczenia się	Kryteria weryfikacji ich osiągnięcia
01.Charakteryzuje pojęcia z zakresu cyberbezpieczeństwa	<ul style="list-style-type: none"> <li>– omawia bezpieczeństwo komputerowe;</li> <li>– omawia cele bezpieczeństwa informacji;</li> <li>– charakteryzuje terminologię z obszaru bezpieczeństwa informacji (np. cyberatak, incydent, wirus);</li> <li>– omawia pojęcia: cyberbezpieczeństwo, cyberprzestrzeń i cyberprzestrzeń RP, bezpieczeństwo i ochrona cyberprzestrzeni, bezpieczeństwo sieci i systemów informatycznych;</li> <li>– charakteryzuje zagrożenia teleinformatyczne (np. cyberprzestępczość, haking, haktywizm, haktywizm patriotyczny, cyberterroryzm, cyberszpiegostwo, militarne wykorzystanie cyberprzestrzeni);</li> <li>– rozróżnia zagrożenia, ataki i aktywa;</li> <li>– omawia funkcjonalne wymagania bezpieczeństwa.</li> </ul>
02.Omawia przepisy prawne i opracowania w obszarze cyberbezpieczeństwa	<ul style="list-style-type: none"> <li>– omawia krajowe przepisy prawne dotyczące cyberbezpieczeństwa, w tym: kodeks karny w obszarze cyberprzestępczości, ustawa o krajowym systemie cyberbezpieczeństwa, ustawa o działaniach antyterrorystycznych w obszarze cyberbezpieczeństwa, ustawa o usługach zaufania oraz identyfikacji elektronicznej, ustawa o ochronie danych osobowych, przepisy o własności intelektualnej;</li> <li>– omawia opracowania dotyczące cyberbezpieczeństwa RP, w tym: plany, doktryny, koncepcje, wizje, ramy, strategie, programy, uchwały dotyczące ochrony cyberprzestrzeni;</li> <li>– omawia wyniki kontroli organów państwowych w obszarze zarządzania cyberbezpieczeństwem;</li> <li>– omawia analizy i rekomendacje eksperckie i naukowe dotyczące cyberbezpieczeństwa w Polsce i na świecie;</li> <li>– omawia przepisy prawne oraz opracowania Unii Europejskiej dotyczące cyberbezpieczeństwa (np. obowiązujące konwencje, dyrektywy, strategie, rozporządzenia, analizy);</li> <li>– omawia kodeksy etyki i postępowania sformułowane przez ACM, IEEE oraz AITP.</li> </ul>

<b>Zestaw 2. Zarządzanie cyberbezpieczeństwem</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01.Omawia standardy i organizacje standaryzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT	<ul style="list-style-type: none"> <li>- charakteryzuje standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standaryzacyjne, takie jak NIST, ITU-T, ISO, IEEE, ISACA;</li> <li>- omawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji według rodziny norm ISO/IEC 27000;</li> <li>- identyfikuje i opisuje zbiór najlepszych praktyk zarządzania usługami IT w odniesieniu do cyberbezpieczeństwa zgodnie z kodeksem postępowania dla działów informatyki określanym jako ITIL (ang. Information Technology Infrastructure Library);</li> <li>- omawia standard COBIT (ang. Control Objectives for Information and related Technology) opracowany przez ISACA oraz IT Governance Institute stanowiący zbiór dobrych praktyk z zakresu IT Governance.</li> </ul>
02.Omawia strategię cyberbezpieczeństwa w organizacji	<ul style="list-style-type: none"> <li>- omawia zasady projektowania cyberbezpieczeństwa;</li> <li>- określa role i przypisuje odpowiedzialności poszczególnych osób w procesie zarządzania cyberbezpieczeństwem;</li> <li>- wymienia i wartościuje zagrożenia oraz ataki, jak również techniki wykorzystywania słabości bezpieczeństwa;</li> <li>- omawia architekturę bezpieczeństwa informacji w organizacji;</li> <li>- wymienia przykłady implementacji strategii w odniesieniu do obowiązujących norm i standardów;</li> <li>- różnicuje sposoby diagnozy i walidacji skuteczności procesu zarządzania cyberbezpieczeństwem.</li> </ul>

<b>Zestaw 3. Zarządzanie ryzykiem</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01.Charakteryzuje standardy i metody oceny ryzyka bezpieczeństwa informacji	<ul style="list-style-type: none"> <li>- omawia i analizuje standardy opisujące procesy oceny ryzyka bezpieczeństwa informatycznego, w tym: ISO 13335, ISO 27005, ISO 31000, NIST SP 800-30;</li> <li>- charakteryzuje inne metodyki szacowania ryzyka, w tym: EBIOS, MAGERIT, CRAMM, MEHARI, MIGRA, OCTAVE.</li> </ul>
02.Charakteryzuje ryzyko bezpieczeństwa informacji w organizacji	<ul style="list-style-type: none"> <li>- opisuje proces zarządzania ryzykiem;</li> <li>- identyfikuje i grupuje wartości aktywów w organizacji;</li> <li>- kategoryzuje zagrożenia i podatności (ryzyka) dla tych aktywów;</li> <li>- omawia podejścia do oceny ryzyka bezpieczeństwa (podstawowe, nieformalne, szczegółowe, łączone);</li> <li>- wybiera i uzasadnia optymalne podejście do oceny ryzyka bezpieczeństwa.</li> </ul>

<b>Zestaw 4. Bezpieczeństwo IT i zarządzanie ciągłością działania</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Charakteryzuje środki, plany i procedury bezpieczeństwa IT	<ul style="list-style-type: none"> <li>- porównuje rodzaje środków bezpieczeństwa (organizacyjne, operacyjne, techniczne) w oparciu o standardy, w tym ISO 27002, ISO 13335, FIPS 200, NIST SP 800-53;</li> <li>- omawia budowę oraz etapy tworzenia i wdrażania planu bezpieczeństwa IT w organizacji;</li> <li>- opisuje aspekty monitorowania zagrożeń w procesie zarządzania bezpieczeństwem IT.</li> </ul>
02. Charakteryzuje regulacje formalno-prawne i standardy związane z zarządzaniem ciągłością działania	<ul style="list-style-type: none"> <li>- omawia zawarte w krajowych aktach prawnych zapisy dotyczące wymagań w zakresie zapewnienia ciągłości działania;</li> <li>- charakteryzuje normy ISO 22301 oraz ISO 22313;</li> <li>- opisuje zasady ustanawiania strategii zarządzania i polityki ciągłości działania w organizacji.</li> </ul>

  

<b>Zestaw 5. Zarządzanie incydentami</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Charakteryzuje obszar zarządzania zespołami reagowania na incydenty bezpieczeństwa komputerowego	<ul style="list-style-type: none"> <li>- charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSIRT);</li> <li>- wskazuje korzyści związane z posiadaniem procedur reagowania na incydenty;</li> <li>- omawia zasady działania krajowego systemu cyberbezpieczeństwa.</li> </ul>
02. Omawia regulacje formalno-prawne, standardy, procedury i dobre praktyki związane z zarządzaniem incydentami	<ul style="list-style-type: none"> <li>- opisuje standardy oraz regulacje formalno-prawne związane z zarządzaniem incydentami;</li> <li>- dobiera i uzasadnia metody zapewnienia usystematyzowanego podejścia do zarządzania i obsługi incydentów bezpieczeństwa informacji;</li> <li>- omawia zasady klasyfikacji i kwalifikacji zdarzeń jako incydentów bezpieczeństwa;</li> <li>- analizuje zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji.</li> </ul>

<b>Zestaw 6. Audyt bezpieczeństwa w obszarze cyberbezpieczeństwa</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01.Charakteryzuje obszar audytu bezpieczeństwa	<ul style="list-style-type: none"> <li>- omawia terminy stosowane w obszarze audytu bezpieczeństwa;</li> <li>- opisuje cele i zakres audytu bezpieczeństwa;</li> <li>- omawia zasady opracowywania wymagań dotyczących audytu bezpieczeństwa;</li> <li>- porównuje standardy audytowania bezpieczeństwa;</li> <li>- omawia przebieg procesu audytu bezpieczeństwa;</li> <li>- opisuje narzędzia wykorzystywane w trakcie audytu bezpieczeństwa;</li> <li>- charakteryzuje zasady raportowania wyników bezpieczeństwa.</li> </ul>

<b>Zestaw 7. Bezpieczeństwo fizyczne i bezpieczeństwo zasobów ludzkich w obszarze cyberbezpieczeństwa</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01.Charakteryzuje zagadnienia dotyczące bezpieczeństwa fizycznego infrastruktury teleinformatycznej	<ul style="list-style-type: none"> <li>- charakteryzuje zagrożenia środowiskowe;</li> <li>- charakteryzuje zagrożenia techniczne;</li> <li>- charakteryzuje zagrożenia związane z działalnością człowieka.</li> </ul>
02.Omawia dobre praktyki i zasady zatrudniania pracowników w obszarze cyberbezpieczeństwa	<ul style="list-style-type: none"> <li>- wymienia cele bezpieczeństwa procesu rekrutacji;</li> <li>- opisuje wytyczne dotyczące sprawdzania kandydatów na kluczowe stanowiska w organizacji związane z zarządzaniem cyberbezpieczeństwem;</li> <li>- wylicza i wartościuje korzyści związane z motywowaniem pracowników do podnoszenia wiedzy z zakresu cyberbezpieczeństwa i stosowania się do procedur w tym zakresie;</li> <li>- charakteryzuje zagadnienia dotyczące obszaru podnoszenia świadomości bezpieczeństwa, szkoleń i programów edukacyjnych;</li> <li>- omawia zagadnienia etyki zawodowej w obszarze cyberbezpieczeństwa i aspekty własności intelektualnej.</li> </ul>

<b>Zestaw 8. Informatyka śledcza</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Charakteryzuje zagadnienia dotyczące norm, standardów i dobrych praktyk informatyki śledczej	<ul style="list-style-type: none"> <li>– charakteryzuje wytyczne dotyczące aspektów technicznych i najlepszych praktyk informatyki śledczej, w tym SWGDE (ang. The Scientific Working Group on Digital Evidence), SWGIT (ang. The Scientific Working Group on Imaging Technology);</li> <li>– omawia standardy ANSI (ang. American National Standards Institute), NIST (ang. National Institute of Standard and Technology) oraz normy międzynarodowe ISO/IEC z rodziny norm ISO/IEC 27000 w obszarze informatyki śledczej.</li> </ul>
02. Charakteryzuje zasady zabezpieczania i metody analizy dowodów elektronicznych	<ul style="list-style-type: none"> <li>– charakteryzuje sposoby prawidłowego zabezpieczania materiału dowodowego na potrzeby dochodzenia wewnętrznego, jak również na potrzeby procesowe;</li> <li>– omawia zasady postępowania z cyfrowymi śladami dowodowymi;</li> <li>– wymienia metody analizy zawartości komputerów i urządzeń mobilnych za pomocą specjalistycznych narzędzi oraz oprogramowania dedykowanego do prowadzenia analiz;</li> <li>– opisuje prawa i obowiązki podmiotów w zakresie realizacji czynności procesowych prowadzonych w ramach postępowań przygotowawczych przez służby bezpieczeństwa i porządku publicznego.</li> </ul>

## **6. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację**

### **1. Etap weryfikacji.**

#### **1.1. Metody.**

Do weryfikacji efektów uczenia się stosuje się wyłącznie: test teoretyczny (pisemny) lub analizę dowodów i deklaracji opcjonalnie uzupełnioną wywiadem swobodnym.

#### **1.2. Zasoby kadrowe.**

Komisja walidacyjna musi składać się z co najmniej dwóch członków, w tym przewodniczącego. Przewodniczący komisji musi spełniać następujące warunki: – posiada kwalifikację pełną z 7 poziomem PRK (dyplom ukończenia studiów II stopnia); – legitymuje się co najmniej 3-letnim doświadczeniem w przeprowadzaniu egzaminów, osiągniętym w okresie ostatnich 6 lat; – legitymuje się co najmniej jednym ważnym certyfikatem CISA, CISM, CRISC, CGEIT, CISSP, wymienionym między innymi w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999). Drugi członek komisji walidacyjnej musi spełniać następujące warunki: – posiada kwalifikację pełną z 6 PRK (dyplom ukończenia studiów I stopnia); – legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze technologii cyfrowej, osiągniętym w okresie ostatnich 3 lat. Ponadto, co najmniej jeden z członków komisji musi posiadać udokumentowane minimum 5-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa.

### 1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne.

Test teoretyczny jest przeprowadzany w ośrodku egzaminacyjnym za pomocą zautomatyzowanego systemu elektronicznego (system rejestracji kandydatów i obsługi egzaminów). Wykorzystanie innych narzędzi/aplikacji pomocniczych, w tym urządzeń mobilnych oraz dostępu do sieci Internet, jest dopuszczalne wyłącznie w sytuacji, w której jest to wymagane specyfiką zadań testowych. Instytucja certyfikująca musi zapewnić: – salę z wyposażeniem multimedialnym i możliwością rejestracji audio-wideo przebiegu walidacji oraz stanowiska egzaminacyjne umożliwiające samodzielną pracę każdej osobie przystępującej do walidacji, np. boksy biurowe zapewniające przeprowadzenie testów z zachowaniem bezpieczeństwa i poufności procesu walidacyjnego; – centralnie zarządzaną platformę informatyczną do przeprowadzania testów i przechowywania wyników (system rejestracji kandydatów i obsługi egzaminów) spełniającą wymagania określone w przepisach RODO; – sprzęt komputerowy oraz dostęp do systemu obsługi testów i egzaminów indywidualnie dla każdego uczestnika; – nadzór osobowy w charakterze obserwatora/obserwatorów w celu zapewnienia prawidłowego przebiegu egzaminu (w tym przeciwdziałania nieuczciwym praktykom). Warunki dodatkowe: – instytucja certyfikująca nie może kształcić oraz prowadzić szkoleń, kursów itp. z zakresu wiedzy ujętej w przedmiotowej kwalifikacji; – walidacja jest prowadzona zgodnie z procedurami instytucji certyfikującej we własnym zakresie lub w akredytowanych laboratoriach przez certyfikowanych egzaminatorów; – każdy asesora walidacyjny oraz obserwator jest zobowiązany do złożenia oświadczenia o braku okoliczności stanowiących podstawę wyłączenia z czynności egzaminacyjnych (np. konflikt interesów).

### 2. Etapy identyfikowania i dokumentowania.

Instytucja certyfikująca musi zapewnić wsparcie doradcy walidacyjnego. Doradca walidacyjny musi spełnić następujące warunki: – zgodność z profilem kompetencyjnym doradcy walidacyjnego określonym w podręczniku „WALIDACJA – nowe możliwości zdobywania kwalifikacji” opracowanym przez Instytut Badań Edukacyjnych, Warszawa 2016 (link:

[http://www.kwalifikacje.gov.pl/download/Publikacje/Walidacja\\_nowe\\_mozliwosci\\_zdobywania\\_kwalifikacji\\_z\\_wkladka.pdf](http://www.kwalifikacje.gov.pl/download/Publikacje/Walidacja_nowe_mozliwosci_zdobywania_kwalifikacji_z_wkladka.pdf));

– min. 5 lat doświadczenia zawodowego w branży teleinformatycznej.

Dokumentacja dowodowa z przeprowadzonej walidacji przechowywana jest przez minimum 5 lat. Ponadto instytucja certyfikująca jest zobowiązana do bezterminowego prowadzenia rejestru wydanych certyfikatów. Certyfikaty muszą być niepowtarzalne (w rozumieniu druku ścisłego zarachowania), posiadać cechy umożliwiające jednoznaczną identyfikację instytucji certyfikującej oraz jedno z wybranych zabezpieczeń – optyczne (np. hologram, kinegram) lub inne.

### 7. Warunki, jakie musi spełniać osoba przystępująca do walidacji

- kwalifikacja pełna z 6 poziomem PRK;
- udokumentowane 3-letnie doświadczenie zawodowe w obszarze cyberbezpieczeństwa w ciągu ostatnich 6 lat;
- oświadczenie o niekaralności za przestępstwo popełnione umyślnie ścigane z oskarżenia publicznego lub umyślnie przestępstwo skarbowe.

### 8. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat.