



# MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

---

Warszawa, dnia 19 lutego 2021 r.

Poz. 200

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

z dnia 8 lutego 2021 r.

**w sprawie włączenia kwalifikacji rynkowej „Zarządzanie cyberbezpieczeństwem – ekspert”  
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 – ekspert” 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).

Załącznik do obwieszczenia Ministra Cyfryzacji  
z dnia 8 lutego 2021 r. (poz. 200)

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

**1. Nazwa kwalifikacji rynkowej**

Zarządzanie cyberbezpieczeństwem – ekspert

**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 podnoszenie kompetencji, np. poprzez udział w warsztatach, konferencjach, szkoleniach 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 – ekspert” posiada wiedzę z obszaru bezpieczeństwa informacji i cyberbezpieczeństwa. Posługuje się regulacjami formalno-prawnymi krajowymi i UE z obszaru cyberbezpieczeństwa. Posiada kompetencje do samodzielnej realizacji zadań w obszarze bezpieczeństwa infrastruktury teleinformatycznej. Rozumie działanie algorytmów kryptograficznych oraz zasady zarządzania kontrolą dostępu do zasobów informacyjnych. Dysponuje wiedzą ekspercką z obszaru bezpieczeństwa sieci, systemów operacyjnych, baz danych, rozwiązań chmurowych i oprogramowania. Zna zagadnienia testowania bezpieczeństwa. Posiada wiedzę z obszarów: bezpieczeństwa, środowiskowego, technicznego i związanego z działalnością człowieka, zarządzania usługami IT, zarządzania incydentami bezpieczeństwa, w tym zasad funkcjonowania zespołów CERT/CSIRT. Posiada również wiedzę z zakresu inżynierii śledczej.

<b>Zestaw 1. Posługiwanie się wiedzą z obszaru cyberbezpieczeństwa</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
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, cyberspiesgostwo, militarne wykorzystanie cyberprzestrzeni);</li> <li>- różniczy 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, ustawę o krajowym systemie cyberbezpieczeństwa, ustawę o działaniach antyterrorystycznych – w obszarze cyberbezpieczeństwa, ustawę o usługach zaufania oraz identyfikacji elektronicznej, ustawę o ochronie danych osobowych, przepisy o własności intelektualnej;</li> <li>- omawia opracowania dotyczące cyberbezpieczeństwa RP, w tym: plany, doktryny, koncepcje, wizje, ramy, strategię, 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, strategię, rozporządzenia, analizy);</li> <li>- omawia kodeksy etyki i postępowania sformułowane przez ACM, IEEE oraz AITP.</li> </ul>

<b>Zestaw 2. Kryptografia</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Omawia algorytmy kryptograficzne	<ul style="list-style-type: none"> <li>- charakteryzuje zasady szyfrów symetrycznych i asymetrycznych;</li> <li>- opisuje pojęcia i terminologię związaną z algorytmami szyfrowania, w tym: szyfry blokowe (DES, 3DES, AES), szyfry strumieniowe i RC4, tryby działania szyfrów blokowych, kryptoanaliza;</li> <li>- opisuje kryptograficzne funkcje skrótu m.in. SHA-1, SHA-2, SHA-3, MD5.</li> </ul>
02. Omawia kryptografię klucza publicznego	<ul style="list-style-type: none"> <li>- porównuje działanie algorytmów RSA, krzywych eliptycznych, protokół Diffiego-Hellmana;</li> <li>- omawia podpisy cyfrowe;</li> </ul>

	<ul style="list-style-type: none"> <li>- omawia Infrastrukturę Klucza Publicznego;</li> <li>- identyfikuje i opisuje zbiory osób, polityk, procedur i systemów komputerowych niezbędnych do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego i prywatnego oraz certyfikatów elektronicznych.</li> </ul>
03. Omawia narzędzia kryptograficzne	<ul style="list-style-type: none"> <li>- omawia narzędzia do szyfrowania przechowywanych danych;</li> <li>- omawia narzędzia do szyfrowania przesyłanych danych.</li> </ul>

<b>Zestaw 3. Zarządzanie uprawnieniami dostępu</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Omawia procesy zarządzania uprawnieniami dostępu	<ul style="list-style-type: none"> <li>- opisuje pojęcia: identyfikacja, uwierzytelnienie, autoryzacja i rozliczalność;</li> <li>- porównuje modele kontroli dostępu do zasobów informacyjnych;</li> <li>- omawia metody uwierzytelniania i autoryzacji użytkowników do zasobów informacyjnych, w tym uwierzytelnianie jedno- i wieloskładnikowe;</li> <li>- omawia metodę jednokrotnego uwierzytelniania do systemów informatycznych.</li> </ul>
02. Omawia narzędzia wspomagające kontrolę dostępu	<ul style="list-style-type: none"> <li>- porównuje narzędzia wspomagające kontrolę dostępu (hasła, techniki biometryczne i behawioralne, tokeny, karty kryptograficzne);</li> <li>- omawia narzędzia monitorujące pracę użytkowników uprzywilejowanych.</li> </ul>

<b>Zestaw 4. Bezpieczeństwo sieci</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
Omawia pojęcia związane z budową i zasadą działania sieci komputerowych	<ul style="list-style-type: none"> <li>- rozróżnia zasady działania sieci LAN, MAN, WAN, WLAN, VPN;</li> <li>- opisuje zasady działania urządzeń sieciowych;</li> <li>- charakteryzuje współczesne rozwiązania bezpieczeństwa sieciowego, w tym: zapory sieciowe (ang. Firewall), zapory aplikacyjne (ang. Web Application Firewall), IDS/IPS, UTM, DLP (Data Leakage Protection), SIEM (Security Information and Event Management), DAM (Database Activity Monitoring), PAM (Identity Access Management), EPP/EDR, IdM, SA (Security Analytics), MDM (Mobile Device Management).</li> </ul>
Omawia protokoły i standardy bezpieczeństwa Internetu	<ul style="list-style-type: none"> <li>- charakteryzuje warstwę modelu ISO OSI RM;</li> <li>- omawia zasady działania i bezpieczeństwo protokołów IPv4, IPv6;</li> <li>- wymienia i opisuje protokoły i standardy dotyczące bezpieczeństwa internetowego, w tym: MIME, S/MIME, DKIM, SSL/TLS, HTTPS, Kerberos, X.509, SNMP, DNSSEC;</li> <li>- opisuje zasady działania i bezpieczeństwa sieci bezprzewodowych.</li> </ul>

<b>Zestaw 5. Bezpieczeństwo systemów operacyjnych, baz danych i rozwiązań chmurowych</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Omawia bezpieczeństwo systemów operacyjnych	<ul style="list-style-type: none"> <li>- opisuje model bezpieczeństwa systemu Linuks/Unix;</li> <li>- opisuje model bezpieczeństwa systemu Windows;</li> <li>- wymienia luki w zabezpieczeniach systemów operacyjnych i aplikacji systemowych;</li> <li>- charakteryzuje pojęcia wirtualizacji i bezpieczeństwa infrastruktury zwirtualizowanej.</li> </ul>
02. Omawia pojęcia związane z bazami danych	<ul style="list-style-type: none"> <li>- omawia systemy zarządzania bazami danych;</li> <li>- różnicuje systemy zarządzania bazami danych;</li> <li>- charakteryzuje składniki baz danych;</li> <li>- opisuje techniki, drogi i typy ataków na bazy danych.</li> </ul>
03. Omawia bezpieczeństwo rozwiązań chmurowych	<ul style="list-style-type: none"> <li>- zestawia i opisuje modele usług chmurowych (IaaS, PaaS, SaaS);</li> <li>- charakteryzuje rolę wirtualizacji w rozwiązaniach chmurowych;</li> <li>- charakteryzuje modele realizacyjne rozwiązań chmurowych;</li> <li>- charakteryzuje koncepcje i podejścia do bezpieczeństwa chmur;</li> <li>- opisuje pojęcie Internetu Rzeczy (ang. Internet of Things, IoT).</li> </ul>
<b>Zestaw 6. Bezpieczeństwo oprogramowania</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
01. Opisuje modele cyklu życia oprogramowania	<ul style="list-style-type: none"> <li>- charakteryzuje czynności związane z tworzeniem oprogramowania, w tym: wymagań i specyfikacji, projektowania, implementacji, testowania i weryfikacji, konserwacji (pielegnacji) i ich elementów składowych;</li> <li>- omawia modele cyklu życia oprogramowania, w tym praktyczne zasady monitorowania podatności oraz typowe błędy oprogramowania.</li> </ul>
02. Opisuje bezpieczeństwo aplikacji dostępnych	<ul style="list-style-type: none"> <li>- omawia zagrożenia dla bezpieczeństwa aplikacji desktopowych, webowych i mobilnych;</li> <li>- charakteryzuje techniki ataków na aplikacje desktopowe, webowe i mobilne;</li> <li>- klasyfikuje techniki ataków;</li> <li>- opisuje sposoby zabezpieczania aplikacji desktopowych, webowych i mobilnych.</li> </ul>
<b>Zestaw 7. Testowanie bezpieczeństwa</b>	
<b>Poszczególne efekty uczenia się</b>	<b>Kryteria weryfikacji ich osiągnięcia</b>
Opisuje zasady przeprowadzania	<ul style="list-style-type: none"> <li>- omawia etapy analizy zabezpieczeń systemu teleinformatycznego oraz testów kontrolnych, podczas których sprawdzana jest poprawność instalacji oraz konfiguracji systemu;</li> </ul>

audytów bezpieczeństwa i monitorowania podatności	<ul style="list-style-type: none"> <li>- opisuje zagrożenia dla systemów teleinformatycznych, w tym: ataki sieciowe, zagrożenia transmisji danych, zagrożenia aplikacyjne, zagrożenia komunikacyjne, awarie techniczne, ludzkie błędy, zagrożenia fizyczne, zagrożenia kryptograficzne, przecieki poufnych informacji, ulot elektromagnetyczny;</li> <li>- charakteryzuje metodyki audytu bezpieczeństwa systemów teleinformatycznych;</li> <li>- omawia narzędzia i metody wykrywania podatności w systemach teleinformatycznych.</li> </ul>
Omawia testy penetracyjne	<ul style="list-style-type: none"> <li>- charakteryzuje rodzaje testów penetracyjnych: test penetracyjny z minimalną wiedzą (black box), test penetracyjny z pełną wiedzą (white box lub crystal box), testy penetracyjne grey box będące kompromisem pomiędzy black box i white box, zawierające elementy obu podejść;</li> <li>- opisuje metodyki testów penetracyjnych, w tym: OSSTMM (Open Source Security Testing Methodology Manual), NIST SP 800-42, NIST SP 800-115, ISAAF, P-PEN;</li> <li>- omawia narzędzia stosowane w realizacji testów penetracyjnych.</li> </ul>
<b>Zestaw 8.</b> Bezpieczeństwo środowiskowe, techniczne i związane z działalnością człowieka	
<b>Kryteria weryfikacji ich osiągnięcia</b>	
01. Charakteryzuje zagadnienia dotyczące bezpieczeństwa 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. Charakteryzuje zabezpieczenia dotyczące infrastruktury teleinformatycznej	<ul style="list-style-type: none"> <li>- omawia techniki zapobiegania zagrożeniom środowiskowym, technicznym i związanym z działalnością człowieka;</li> <li>- opisuje metody odtwarzania po naruszeniach bezpieczeństwa środowiskowego, technicznego i związanych z działalnością człowieka;</li> <li>- omawia i wybiera metody pozwalające na uzyskanie wysokiego poziomu niezawodności urządzeń i systemów, w tym: rozwiązania redundancyjne, zasilanie awaryjne.</li> </ul>
<b>Zestaw 9.</b> Elementy zarządzania cyberbezpieczeństwem	
<b>Kryteria weryfikacji ich osiągnięcia</b>	
01. Omawia standardy i organizacje standardyzacyjne w obszarze bezpieczeństwa informacji oraz zarządzania usługami IT	<ul style="list-style-type: none"> <li>- charakteryzuje standardy z obszaru bezpieczeństwa informacji opracowane przez organizacje standardyzacyjne, 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 określonym 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. Zarządzanie ryzykiem	<ul style="list-style-type: none"> <li>- omawia 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> <li>- wymienia etapy procesu zarządzania ryzykiem.</li> </ul>
03 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>- uzasadnia potrzebę ustanawiania strategii zarządzania i polityki ciągłości działania w organizacji.</li> </ul>
04. Zarządzanie incydentami bezpieczeństwa	<ul style="list-style-type: none"> <li>- opisuje standardy oraz regulacje formalno-prawne związane z zarządzaniem incydentami;</li> <li>- wymienia zasady klasyfikacji i kwalifikacji zdarzeń jako incydentów bezpieczeństwa;</li> <li>- omawia zasady nadawania priorytetów obsługi zdarzeń i minimalizacji strat związanych z nieprawidłową obsługą incydentów bezpieczeństwa informacji;</li> <li>- charakteryzuje zasady działania zespołów reagowania na incydenty bezpieczeństwa komputerowego (CERT, CSIRT).</li> </ul>

#### Zestaw 10. Informatyka śledcza

Poszczególne efekty uczenia się	Kryteria weryfikacji ich osiągnięcia
01. Charakteryzuje zagadnienia dotyczące norm, standardów i dobrych praktyk informatyki śledczej	<ul style="list-style-type: none"> <li>- wymienia przykłady 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>- opisuje 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 postępowania przygotowawczego 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 przeprowadzany jest 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-video przebiegu walidacji oraz stanowiska egzaminacyjne umożliwiające samodzielnie 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 prowadzona jest zgodnie z procedurami instytucji certyfikującej we własnym zakresie lub w akredytowanych laboratoriach przez certyfikowanych egzaminatorów;
- każdy asesor walidacyjny oraz obserwator zobowiązany jest 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 jednoznacznie 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 ściągnięte z oskarżenia publicznego lub umyślnie przestępstwo skarbowe.

**8. Termin dokonywania przeglądu kwalifikacji**

Nie rzadziej niż raz na 10 lat