

# Zintegrowany Rejestr Kwalifikacji

## Formularz dla kwalifikacji - podgląd

Typ wniosku

Wniosek o włączenie kwalifikacji do ZSK

Nazwa kwalifikacji\*

Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych

Skrót nazwy

Rodzaj kwalifikacji\*

kwalifikacja cząstkowa

Proponowany poziom Polskiej Ramy Kwalifikacji\*

5

Krótką charakterystyką kwalifikacji, obejmującą informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikację oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji\*

Osoba posiadająca kwalifikację „Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych” jest przygotowana do wykonywania zadań związanych z zabezpieczaniem rozwiązań chmurowych. Identyfikuje, wynikające z regulacji prawnych, specyfiki działalności oraz wymagań właścicieli procesów biznesowych, wymagania w zakresie bezpieczeństwa, jakim muszą odpowiadać wykorzystywane rozwiązania chmurowe. Analizuje możliwości techniczne, organizacyjne czasowe i finansowe wdrożenia i stosowania określonych rozwiązań zapewniających bezpieczeństwo rozwiązań chmurowych. Analizuje dostępne na rynku oraz wykorzystywane w organizacji usługi chmurowe pod kątem poziomu ich bezpieczeństwa. Ocenia ryzyko związane z wykorzystywaniem rozwiązań chmurowych, w tym identyfikuje słabe oraz mocne strony rozwiązań chmurowych w zakresie bezpieczeństwa, identyfikuje usługi, których bezpieczeństwo jest kluczowe oraz analizuje skutki wystąpienia incydentów naruszających bezpieczeństwo rozwiązań chmurowych. Na podstawie zidentyfikowanych zagrożeń oraz potencjalnych miejsc ich wystąpienia w rozwiązaniu chmurowym opracowuje koncepcję zapewnienia bezpieczeństwa rozwiązania chmurowego, w szczególności analizuje i dobiera mechanizmy zapewniające bezpieczeństwo rozwiązań chmurowych. Ponadto posiadacz kwalifikacji szacuje koszty wdrożenia i stosowania poszczególnych rozwiązań zapewniających bezpieczeństwo oraz ocenia zasadność ich zastosowania z uwzględnieniem ich kosztów, skuteczności działania oraz zapewnianego poziomu bezpieczeństwa. Orientacyjna wysokość opłaty za przeprowadzenie walidacji i wystawienie dokumentu potwierdzającego otrzymanie danej kwalifikacji: 3.000,00 zł (trzy tysiące złotych).

Orientacyjny nakład pracy potrzebny do uzyskania kwalifikacji [godz.]\*

## Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji\*

Kwalifikacja kierowana jest do osób pracujących lub planujących pracę w zakresie projektowania i wdrażania usług chmurowych w różnego typu organizacjach. Zainteresowane kwalifikacją mogą być również osoby zarządzające usługami chmurowymi w organizacjach, administratorzy sieci, osoby odpowiedzialne za systemy informatyczne w organizacjach, osoby odpowiedzialne za bezpieczeństwo informacji oraz specjaliści ds. cyberbezpieczeństwa chcący się specjalizować w rozwiązaniach chmurowych.

Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)



Możliwe jest przygotowanie do uzyskania kwalifikacji w ramach obowiązkowych zajęć edukacyjnych z zakresu kształcenia zawodowego (branżowa szkoła I stopnia, technikum, szkoła policealna) [Rozporządzenie MEN z dnia 16 maja 2019 r.](#)

## Wymagane kwalifikacje poprzedzające

Opis

Nie dotyczy

Lista

## W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji\*

Nie dotyczy

## Zapotrzebowanie na kwalifikację\*

„Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych” to kwalifikacja, która odpowiada na rosnące zapotrzebowanie przedsiębiorstw wszystkich sektorów gospodarki podejmujących się lub planujących podjąć się przeprowadzenia implementacji rozwiązań chmurowych. Są one istotną częścią procesów określanych jako transformacja cyfrowa, która od początku XXI wieku obejmuje niemal wszystkie aspekty życia gospodarczego i społecznego. W miarę cyfryzowania się największych gospodarek światowych wzrasta presja, jaka wywierana jest na mniej rozwinięte krajowe systemy gospodarcze, dla których szybkie wejście w procesy cyfryzacji może przesądzić o możliwości konkurowania na globalnym, coraz mniej analogowym rynku. Istotnym elementem cyfryzacji jest przenoszenie danych cyfrowych, najczęściej z lokalnych serwerów prywatnych lub firmowych, na serwery dostawcy chmury, lub też przenoszenie ich pomiędzy różnymi chmurami [1]. Miejsce, na które trafiają dane to specjalnie dedykowane przestrzenie magazynów danych, pozostające w odpowiedniej konfiguracji, strukturze i rygorze bezpieczeństwa. Działania związane z takim procesem są określane jako „migracja danych do chmury”, „wdrażanie rozwiązań chmurowych” lub „wdrażanie chmury obliczeniowej”. Są one prowadzone w celu optymalizacji kosztów oraz podniesienia poziomu bezpieczeństwa, wydajności i dostępności podczas korzystania z danych. Procesy związane z transformacją cyfrową, których istotnym elementem jest wdrażanie rozwiązań chmurowych, są obecnie jednym z najistotniejszych zjawisk oddziałujących na wszystkie dziedziny gospodarki. Jak wspomniano wyżej, szybkość i jakość cyfryzacji mają fundamentalny wpływ na możliwości rozwojowe przedsiębiorstw, co dotyczy również Polski. Niestety do roku 2019 procesy te przebiegały w naszym kraju bardzo powoli, co najprawdopodobniej wynikało ze specyfiki gospodarki opartej na przemyśle rolno-spożywczym

oraz wydobywaniu surowców. Transformacja cyfrowa i związane z nią projekty wdrażania rozwiązań chmurowych, w pierwszych dwóch dekadach XXI wieku dotyczyły głównie zlokalizowanych w Polsce oddziałów zagranicznych korporacji, operujących za granicą firm softwarowych, niewielkiego grona firm przemysłu 4.0 oraz innowacyjnych startupów. Pomimo, że liczba cyfryzujących się podmiotów była niewielka, to wprowadzane w nich rozwiązania charakteryzowały się wysoką innowacyjnością. W porównaniu do krajów, gdzie podobne rozwiązania wprowadzono dużo wcześniej, oznaczało to, że w przyszłości nie będzie potrzeby likwidowania luki technologicznej. Sytuacja ta pozwalała analitykom postrzegać Polskę jako kraj dobrze rokujący w przyszłym cyfrowym świecie, posiadający istotny potencjał rozwojowy w zakresie procesów transformacji cyfrowej [2]. Jak wspomniano, aż do 2018 roku w Polsce transformacja cyfrowa nie przebiegała w sposób zbyt intensywny, co zmieniło się dopiero w wyniku następstw pandemii COVID-19. Na skutek wprowadzanych lockdownów i okresów kwarantanny, obywatele musieli przez wiele tygodni pozostawać w swoich domach, co zmieniło ich zwyczaje konsumenckie, zaś pracodawcom uzmysłowiło, że tylko firmy, które przeprowadziły cyfryzację i automatyzację części procesów, są w stanie wydajnie działać i rozwijać się w takiej sytuacji. Okazało się też, że istotne postępy w zakresie cyfryzacji poczyniono w ostatnich latach w sferze usług publicznych, co było wynikiem inwestycji państwa i realizowania przez nie polityk unijnych w tym zakresie. Świadomość tych faktów wywołała w wielu firmach wciąż rosnące zainteresowanie cyfryzacją, głównie w zakresie wdrażania usług chmurowych. Niestety obiektywnie istniejące zapóźnienia w stosunku do państw tak zwanej starej UE powodują, że mimo wysokiego potencjału i wskazanego zainteresowania, pod względem cyfryzacji gospodarki Polska wciąż jest daleko od europejskiej i światowej czołówki. Dane wskazują, że w wypadku gospodarki amerykańskiej poziom cyfryzacji wynosi 18%, w krajach Europy Zachodniej jest to 12%, zaś w Polsce jedynie 8%. Ogółem poziom cyfryzacji polskich firm wynosi jedynie 34% średniej krajów tak zwanej starej Unii oraz Wielkiej Brytanii [3]. Z danych przedstawionych przez analityków Komisji Europejskiej, dotyczących rozwoju gospodarek i społeczeństw cyfrowych wynika, iż Polska zajęła w 2021 roku, podobnie jak w roku 2020, 24 miejsce wśród 27 państw członkowskich Unii Europejskiej [4]. Analizy te opierają się na zagregowanym wskaźniku gospodarki cyfrowej i społeczeństwa Digital Economy and Society Index (dalej: DESI), umożliwiającym ocenę poziomu cyfryzacji państw UE. DESI jest tworzony w pięciu głównych kategoriach: Connectivity - infrastruktury i łączności cyfrowej, Human Capital - kapitału ludzkiego w kontekście cyfrowym, Use of Internet - wykorzystania Internetu, Integration of Digital Technologies - technologii cyfrowych obecnych w przedsiębiorstwach oraz Public Digital Services - cyfrowych usług publicznych. DESI jako najbardziej zaawansowane cyfrowo państwa europejskie wskazuje Finlandię Szwecję, Holandię i Danię, dla których wskaźnik wynosi blisko 70 punktów na 80 możliwych. Państwa te stanowią światową awangardę cyfryzacji i plasują się w tej dziedzinie zaraz za Koreą Południową, Japonią i Stanami Zjednoczonymi. W przypadku Polski, w roku 2021, DESI wyniósł 41 punktów, co było wynikiem poniżej średniej europejskiej określanej na 50,7. Polska wyprzedzała tylko Grecję, Bułgarię i Rumunię uzyskujące poniżej 40 punktów w rankingu DESI. Mimo tak niskiego wyniku, wskaźnik jednocześnie obrazuje, że od 2016 roku widoczny jest postęp w cyfryzacji Polski, zwłaszcza w obszarze wspomnianej już Public Digital Services oraz Connectivity, dla których Polska osiągnęła już poziom średniej 27 krajów UE. Dostępność połączeń cyfrowych w telekomunikacji oraz rozwój cyfrowy sektora publicznego to pozytywny trend, jeśli chodzi o dalsze postępy w cyfryzacji. Jednak potencjalny rozwój cyfryzacji, w tym zwłaszcza wdrażanie rozwiązań chmurowych, nie postępuje tak szybko, jak można by sobie tego życzyć, nawet pomimo istotnej intensyfikacji w okresie pandemii COVID-19. W środowiskach biznesowych panuje opinia, że niektóre firmy poradziły sobie z kryzysem tylko dlatego, że były w stanie w odpowiedni sposób wdrożyć cyfrowe technologie chmurowe, a następnie odpowiednio je wykorzystywać i chronić zawarte tam dane. Świadomość ich sukcesu powodowała reakcje naśladowcze u konkurencji, co spowodowało gwałtowny wzrost zapotrzebowania na usługi

chmurowe. Według DESI, w latach 2017 i 2018 z rozwiązań chmurowych, w Polsce, korzystało jedynie 7% przedsiębiorstw, natomiast w roku 2020 było to już 15% [4]. Mimo to polska gospodarka w roku 2020 nie osiągnęła średniej unijnej dla korzystania z usług chmurowych, która wyniosła w tym okresie 26%. Jak wynika z badań przytaczanych w raporcie „Chmura i cyberbezpieczeństwo w Polsce – raport 2021” powodem takiego stanu rzeczy nie są kwestie finansowe, ale braki kadrowe i obawy o możliwości zarządzania i zapewnienia cyberbezpieczeństwa w zaimplementowanej chmurze [5]. Według raportu, tylko jedna na dziesięć polskich firm mierzących się z wdrażaniem rozwiązań chmurowych posiada odpowiednie zasoby kadrowe pozwalające na samodzielne zaprojektowanie, wdrożenie, zarządzanie i zapewnienie bezpieczeństwa w opracowanym rozwiązaniu. W konsekwencji znakomita większość podmiotów i organizacji wprowadzających chmurę korzysta z usług podmiotów zewnętrznych, oferujących gotowe pakiety usług oraz ich wdrożenie. Niestety rozwiązania takie często okazują się nieadekwatnie dobrane do celów i oczekiwań danego podmiotu. Poza tym okazuje się, że opieka ze strony dostawcy usługi oraz wdrożone rozwiązania automatyzujące, nie są w stanie zastąpić stale obecnych pracowników o odpowiednich kompetencjach. Jest to szczególnie widoczne w kontekście bezpieczeństwa danych w chmurze. Według raportu „Chmura i cyberbezpieczeństwo w Polsce – raport 2021”, tylko 30% firm zatrudnia pracowników posiadających kompetencje w zakresie zgodnym z proponowaną kwalifikacją. Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych. Tymczasem są oni niezbędni na każdym etapie, od projektowania chmury, przez wdrożenie aż do jej stałego działania. Znając zakres i zasady działania organizacji, mechanizmy danego rozwiązania chmurowego oraz kluczowe kwestie związane z oceną ryzyka, analizowaniem zagrożeń, doбором narzędzi i środków przeciwdziałania, pracownicy ci są w stanie planować i podejmować kroki zapewniające cyberbezpieczeństwo chmury, w tym także jej niezawodność. Postępująca na całym świecie cyfryzacja zmienia istniejące i tworzy nowe gałęzie gospodarki, zaś jej rozwój jest warunkiem koniecznym do zapewnienia wzrostu gospodarczego również w Polsce. Będzie to jednak możliwe do zrealizowania jedynie dzięki dalszemu wzrostowi inwestycji w procesy transformacji cyfrowej w przedsiębiorstwach, w tym wdrażania i zapewnienia właściwego funkcjonowania rozwiązań chmurowych. To z kolei wymaga wykwalifikowanych pracowników posiadających szereg deficytowych dziś kompetencji, nie tylko związanych z projektowaniem i utrzymaniem działania cyfrowych chmur, ale też z zapewnieniem bezpieczeństwa dla znajdujących się w nich danych [6]. Opublikowany przez McKinsey & Company raport „Chmura 2030. Jak wykorzystać potencjał technologii chmurowej i przyspieszyć wzrost w Polsce” wskazuje, że zapewnianie cyberbezpieczeństwa rozwiązań chmurowych obejmuje szereg procedur i działań, nie tylko w zróżnicowanych środowiskach informatycznych chmur publicznych, prywatnych i hybrydowych, ale również poza nimi [7]. Wśród takich raport wymienia kontakty użytkowników, procedury kontrolne i prewencyjne skierowane na użytkowników, kontakty z dostawcami usług, organami kontrolnymi itd. Kompetencje niezbędne do prac tego typu w istotny sposób różnią się od tradycyjnie przypisanych zadaniom związanym z zapewnieniem bezpieczeństwa w systemach informatycznych. Oprócz technologicznych, związanych ściśle z IT, pracownicy zapewniający cyberbezpieczeństwo rozwiązań chmurowych w organizacjach, powinni również posiadać kompetencje planistyczne, zarządcze, prawnicze, edukacyjne i społeczne, co znajduje potwierdzenie w raporcie „Kompetencje chmurowe firm w Polsce 2020” zawierającym wyniki badań kompetencji, prowadzonych przez IDG, Oktawave i 7bulls.com [8]. Zapotrzebowanie na specjalistów z zakresu zapewniania cyberbezpieczeństwa rozwiązań chmurowych rośnie wraz z upowszechnianiem się tego typu rozwiązań. W odróżnieniu od innych ról, związanych np. z wdrożeniami chmury, wymaga on wysokich kompetencji IT, co w istotny sposób ogranicza, ale nie uniemożliwia, dostępu do tego typu zajęć dla osób niezwiązanych z IT. Warto zaznaczyć, że zjawisko zapotrzebowania na tego typu specjalistów jest tak nowe i jednocześnie tak dynamiczne, że, podobnie jak wszystkie związane z wprowadzaniem rozwiązań chmurowych,

niemal nie występuje ono w statystykach PSZ i GUS. Pierwszą zmianą w tym zakresie jest wprowadzenie, w roku 2021 do predykcji rynku pracy „Barometru Zawodów” kategorii „Specjaliści ds. projektowania, wdrażania i doskonalenia produktów i usług cyfrowych” [9]. Wysoki popyt na specjalistów cyberbezpieczeństwa rozwiązań chmurowych jest faktem, o czym informuje druga część wspomnianego raportu „Kompetencje chmurowe firm w Polsce 2020”. Braki kadrowe dotyczą zwłaszcza małych i średnich firm, które z powodu braków kompetencyjnych pracowników wybierają rozwiązania chmurowe gotowe, często nieadekwatne do ich działalności oraz oddają cały zakres bezpieczeństwa tych rozwiązań w ręce zewnętrznych podmiotów. Rozwiązanie to nie zawsze zapewnia odpowiedni stopień bezpieczeństwa i często opóźnia wprowadzanie modyfikacji i rozwój chmur. Natomiast w przypadku większych podmiotów widoczna jest rosnąca świadomość konieczności rozwijania kompetencji własnych pracowników i uzyskiwania przez nich odpowiednich kwalifikacji lub zatrudniania nowych osób, posiadających kwalifikacje w zakresie zapewnienia cyberbezpieczeństwa rozwiązań chmurowych. Z racji innowacyjnego charakteru oraz długiego cyklu edukacji formalnej, kompetencje konieczne do zapewnienia cyberbezpieczeństwa rozwiązań chmurowych nie są obecnie kształcone w obszarze edukacji formalnej w zakresie szkolnictwa branżowego. Efektów kształcenia w ich zakresie nie ma zawodach Technik Informatyk i Technik Programista. Zaczynają być one widoczne w dopiero w programach studiów kierunków informatycznych, jak również w programach dedykowanych studiów podyplomowych. Wysokie zapotrzebowanie rynku na wiedzę w zakresie zapewnienia cyberbezpieczeństwa rozwiązań chmurowych wpływa na ofertę edukacji pozaformalnej. Można tu zaobserwować rosnącą liczbę szkoleń i kursów. Należy jednak zauważyć, że realizowane kursy często nie obejmują rzetelnej walidacji rozwijanych kompetencji. W efekcie uzyskiwane zaświadczenia i certyfikaty nie zawsze potwierdzają realny poziom szkolonych umiejętności. Powoduje to, że zatrudnianie osób korzystających tylko z edukacji pozaformalnej wymaga od pracodawców weryfikacji każdego zatrudnionego pracownika na jego stanowisku pracy. W podsumowaniu należy podkreślić, że braki specjalistów wykwalifikowanych specjalistów do zapewnienia cyberbezpieczeństwa rozwiązań chmurowych stanowią zagrożenie dla konkurencyjności i rozwoju polskiej gospodarki. Kwalifikacja „Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych” umożliwi niezależną walidację rozwijanych kompetencji i potwierdzanie ich w postaci certyfikatu kwalifikacji. Korzystanie z tego rozwiązania będzie możliwe nie tylko dla osób związanych z IT, gdyż pozwoli na potwierdzanie kompetencji niezależnie od sposobu ich nabycia, zarówno w drodze edukacji formalnej, pozaformalnej, samokształcenia jak też praktyki. Certyfikat wydawany w wypadku pozytywnej walidacji będzie atrakcyjny zarówno dla pracodawców, gdyż da im pewność zatrudnienia wykwalifikowanego pracownika, jak też dla pracownika, dla którego będzie stanowił niezależne i szeroko uznawane potwierdzenie posiadanych przez niego kompetencji. Przypisy: 1. What is cloud migration?, <https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-is-cloud-migration/#definition> [20.07.2022] 2. J. Novak, M. Purta, T. Marciniak, K. Ignatowicz, K. Rozenbaum, K. Yearwood, The rise of Digital Challengers. How digitization can become the next growth engine for Central and Eastern Europe, raport opracowany przez McKinsey Company, 2018, <https://www.mckinsey.com/~media/McKinsey/Featured%20Insights/Europe/Central%20and%20Eastern%20Europe%20needs%20a%20new%20engine%20for%20growth/The-rise-of-Digital-Challengers.ash%20x> [dostęp: 20.07.2022]. 3. Digital Economy and Society Index (DESI) 2020 [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=67086](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086) [dostęp: 20.07.2022] . 4. Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) na 2021 r. Polska, 2022, <https://ec.europa.eu/newsroom/dae/redirection/document/80596> [dostęp: 20.07.2022]. 5. Kompetencje chmurowe firm w Polsce 2020, <https://oktawave.com/pl/raporty/kompetencje-potrzebne-do-transformacji-chmurowej> [dostęp: 20.07.2022]. 6. J. M. Moczydłowska, Rewolucja przemysłowa 4.0 jako źródło nowych wyzwań zarządzania kompetencjami zawodowymi, [w:] I. Stańczyk, S. Twaróg (red.), Człowiek w

organizacji, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2018, s. 25-34. 7. P. Dziadosz, E. Granosik, S. Hieronimus, T. Marciniak, J. Novak, B. Pastusiak, M. Purta, O. Sokoliński, Chmura 2030. Jak wykorzystać potencjał technologii chmurowej i przyspieszyć wzrost w Polsce, McKinsey & Company, Warszawa 2021, s. 60, <https://www.mckinsey.com/pl/our-insights/chmura-2030> [dostęp: 22.07.2022]. 8. Kompetencje chmurowe firm w Polsce 2020, <https://oktawave.com/pl/raporty/kompetencje-potrzebne-do-transformacji-chmurowej> [dostęp: 20.07.2022]. 9. Barometr zawodów. Prognoza zapotrzebowania na pracowników, Specjaliści ds. projektowania, wdrażania i doskonalenia produktów i usług cyfrowych, [https://barometrzwodow.pl/modul/prognozy-na-mapach-wyniki?province%5B%5D=%23polska&year%5B%5D=2021&forecast\\_type=relation&profession%5B%5D=326&relation=1](https://barometrzwodow.pl/modul/prognozy-na-mapach-wyniki?province%5B%5D=%23polska&year%5B%5D=2021&forecast_type=relation&profession%5B%5D=326&relation=1) [dostęp: 20.07.2022].

Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się\*

Kwalifikacje o zbliżonym charakterze ujęte w ZRK: ● Zarządzanie cyberbezpieczeństwem - specjalista ● Zarządzanie cyberbezpieczeństwem - menedżer ● Zarządzanie cyberbezpieczeństwem - ekspert Wymienione kwalifikacje obejmują umiejętności pozwalające na kompleksowe zarządzanie cyberbezpieczeństwem. Przeznaczone są one przede wszystkim dla specjalistów w zakresie cyberbezpieczeństwa odpowiedzialnych za ochronę informacji, bezpieczeństwo infrastruktury teleinformatycznej oraz kształtowanie polityki bezpieczeństwa, na różnych szczeblach organizacji. Kwalifikacja "Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych" koncentruje się natomiast na umiejętnościach związanych z zabezpieczeniem usług i rozwiązań chmurowych stosowanych w organizacjach. Ujęte w niej efekty uczenia się dotyczą znajomości specyfiki zagrożeń związanych z usługami chmurowymi oraz umiejętności doboru mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych. Kwalifikacja ta jest przeznaczona przede wszystkim dla osób specjalizujących się w projektowaniu i wdrażaniu rozwiązań chmurowych oraz zarządzania nimi. Może być również uzupełnieniem w zakresie rozwiązań chmurowych wymienionych wyżej kwalifikacji o zbliżonym charakterze, dla specjalistów z zakresu cyberbezpieczeństwa. Kwalifikacja nie posiada wspólnych zestawów efektów uczenia się z wymienionymi powyżej kwalifikacjami o zbliżonym charakterze. W kwalifikacji "Zarządzanie cyberbezpieczeństwem - ekspert" ujęto efekt uczenia się odnoszący się do ogólnej wiedzy na temat bezpieczeństwa rozwiązań chmurowych (EUS "Omawia bezpieczeństwo rozwiązań chmurowych"). Ponadto w ZRK ujęto następujące kwalifikacje: ● Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych ● Zarządzanie niezawodnością i cyberbezpieczeństwem w przemyśle w zakresie zasobów ludzkich i proceduralnych ● Zarządzanie niezawodnością i cyberbezpieczeństwem w zakresie urządzeń oraz technologii w przemyśle. Wymienione kwalifikacje dedykowane są do stosowania w przemyśle, ze szczególnym zorientowaniem na systemy informatyczne nadzorujące przebiegi procesów technologicznych lub produkcyjnych SCADA (ang. Supervisory Control And Data Acquisition). Wymienione kwalifikacje koncentrują się na zagadnieniach bezpieczeństwa w środowiskach systemów sterowania przemysłowego w zakresie przemysłu procesowego. W wymienionych kwalifikacjach nie zidentyfikowano zestawów uczenia się wspólnych dla kwalifikacji "Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych".

Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)



Kwalifikacja zawiera wspólne lub zbliżone zestawy efektów kształcenia z „dodatkowymi umiejętnościami zawodowymi” w zakresie wybranych zawodów szkolnictwa branżowego

#### Typowe możliwości wykorzystania kwalifikacji\*

Osoba posiadająca kwalifikację może podjąć zatrudnienie w firmach projektujących, dostarczających lub wdrażających rozwiązania chmurowe na stanowiskach np. projektant, doradca klienta, związanych z wdrażaniem rozwiązań chmurowych w organizacjach oraz w organizacjach wykorzystujących lub planujących wykorzystanie rozwiązań chmurowych. Ponadto może prowadzić działalność w zakresie zapewniania cyberbezpieczeństwa rozwiązań chmurowych oraz w zakresie doradztwa związanego z projektowaniem, wdrażaniem oraz zapewnianiem bezpieczeństwa rozwiązań chmurowych. Osoba posiadająca kwalifikację może również podjąć zatrudnienie w firmach zajmujących się zapewnianiem cyberbezpieczeństwa.

#### Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację\*

1. Etap weryfikacji 1.1. Metody Weryfikacja dla każdego zestawu efektów uczenia się musi być przeprowadzona: testem teoretycznym (w formie tradycyjnej lub elektronicznej) albo ● metodą analizy dowodów i deklaracji opcjonalnie uzupełnioną testem teoretycznym (w formie tradycyjnej lub elektronicznej) lub wywiadem (ustrukturyzowanym lub swobodnym). Walidacja musi być przeprowadzana w oparciu o wystandaryzowane narzędzia walidacji. W przypadku wykorzystania testu teoretycznego należy wykorzystać również pytania otwarte, oparte na opisach przypadków oraz, tam, gdzie wymagane jest to przez kryterium weryfikacji, należy udostępnić kandydatowi wraz z testem odpowiednią dokumentację. W przypadku metody analizy dowodów i deklaracji instytucja certyfikująca powinna opracować i udostępnić wykaz dowodów uznawanych za wiarygodne oraz określić warunki, jakie muszą spełniać te dowody (np. okres ważności). Za wiarygodne uznane mogą zostać: ● dokumenty potwierdzające wykonywanie przez kandydata zadań związanych z zapewnianiem bezpieczeństwa rozwiązań chmurowych (np. projekty rozwiązań w zakresie cyberbezpieczeństwa usług i rozwiązań chmurowych, raporty z wdrażania zabezpieczeń rozwiązań chmurowych, referencje, zaświadczenia, nagrody), ● dokumenty świadczące o potwierdzeniu, w wyniku wiarygodnej weryfikacji, określonych dla kwalifikacji efektów uczenia się. 1.2. Zasoby kadrowe Osoby przygotowujące narzędzia walidacji W procesie przygotowania narzędzi walidacji muszą uczestniczyć co najmniej: • osoba posiadająca aktualne (aktualnie wykonująca lub nadzorująca wykonywanie zadań związanych z kwalifikacją) doświadczenie praktyczne z zakresu objętego kwalifikacją, • osoba posiadająca doświadczenie w przygotowywaniu narzędzi walidacji. Komisja walidacyjna. 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 rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze technologii cyfrowej lub cyberbezpieczeństwa osiągniętym w okresie ostatnich 6 lat. 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 lub cyberbezpieczeństwa osiągniętym w okresie ostatnich 3 lat. Ponadto, każdy z członków komisji musi posiadać udokumentowane minimum 3-letnie doświadczenie zawodowe w obszarze projektowania, wdrażania rozwiązań chmurowych lub zarządzania nimi lub w obszarze cyberbezpieczeństwa. 1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne Obserwacja w warunkach symulowanych oraz rozmowa z komisją walidacyjną przeprowadzana jest w ośrodku egzaminacyjnym. Instytucja certyfikująca musi zapewnić: • pracownię wyposażoną w stanowisko komputerowe dla każdego uczestnika walidacji tj. stół, krzesło, komputer z dostępem do Internetu, pakietem programów biurowych i z dostępem do drukarki •

scenariusze zadań praktycznych, opisy przypadków. 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-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).

2. Etap identyfikowania i dokumentowania efektów uczenia się Instytucja certyfikująca może zapewniać wsparcie dla kandydatów w zakresie identyfikowania oraz dokumentowania posiadanych efektów uczenia się. Korzystanie z tego wsparcia nie jest obowiązkowe.

2.1 Metody Etapy identyfikowania i dokumentowania mogą być realizowane w oparciu o dowolne metody zapewniające osiągnięcie celów tych etapów walidacji.

2.2 Zasoby kadrowe Doradca walidacyjny. Zadaniem doradcy walidacyjnego jest wsparcie osoby przystępującej do procesu walidacji na każdym etapie tego procesu. Doradca walidacyjny pomaga w zidentyfikowaniu posiadanych efektów uczenia się oraz w ich rzetelnym udokumentowaniu na potrzeby walidacji. Pomaga również w określeniu innych, możliwych do potwierdzenia kwalifikacji oraz perspektyw rozwoju i dalszego uczenia się po uzyskaniu kwalifikacji. Udziela informacji dotyczących przebiegu walidacji, wymagań związanych z przystąpieniem do weryfikacji efektów uczenia się oraz kryteriów i sposobów oceny. Funkcję doradcy walidacyjnego może pełnić osoba, która posiada:

- doświadczenie zawodowe związane z bilansowaniem kompetencji,
- doświadczenie w weryfikowaniu efektów uczenia się lub ocenie kompetencji,
- umiejętność stosowania metod i narzędzi wykorzystywanych przy identyfikowaniu i dokumentowaniu kompetencji,
- wiedzę dotyczącą niniejszej kwalifikacji oraz innych kwalifikacji funkcjonujących w obszarze technologii cyfrowej.

2.3 Sposób organizacji walidacji oraz warunki organizacyjne i materialne etapu identyfikowania i dokumentowania Instytucja certyfikująca może zapewnić osobom przystępującym do walidacji wsparcie na etapie identyfikowania i dokumentowania. Etap ten może być również realizowany przez te osoby samodzielnie. Instytucja certyfikująca, która zdecyduje się na wsparcie osób w procesie identyfikowania i dokumentowania powinna zapewnić warunki umożliwiające im indywidualną rozmowę z doradcą walidacyjnym. Instytucja certyfikująca może również udzielać wsparcia zdalnie tzn. za pośrednictwem telefonu lub Internetu, w warunkach zapewniających poufność rozmowy.

Propozycja odniesienia do poziomu sektorowych ram kwalifikacji (o ile dotyczy)

Nie dotyczy

Syntetyczna charakterystyka efektów uczenia się\*

Osoba posiadająca kwalifikację zapewnia bezpieczeństwo rozwiązań chmurowych w organizacji uwzględniając zmienne, nie w pełni przewidywalne warunki, w tym związane z intencjonalnymi atakami, jak również pogorszeniem parametrów niezawodności i jakości. Identyfikuje uwarunkowania związane z zapewnieniem bezpieczeństwa usług chmurowych, w tym wynikające z przepisów prawa, oczekiwań właścicieli procesów biznesowych oraz dostępnej infrastruktury. Analizuje akty prawne oraz dokumentację techniczną. Na podstawie dokumentacji dostawcy



usług chmurowych określa poziom bezpieczeństwa usług oraz analizuje możliwości zastosowania różnych mechanizmów zapewniających bezpieczeństwo. Identyfikuje ryzyko związane z korzystaniem z poszczególnych usług i rozwiązań chmurowych oraz wskazuje potencjalne skutki wystąpienia incydentów naruszających bezpieczeństwo rozwiązań chmurowych. Proponuje koncepcję zabezpieczenia rozwiązania chmurowego z wykorzystaniem różnorodnych metod i rozwiązań. Uzasadnia przedstawione propozycje wskazując wady, zalety danego rozwiązania oraz związane z nim koszty i ograniczenia. Analizuje koszty związane z zapewnieniem bezpieczeństwa rozwiązania chmurowego oraz analizuje efektywność działań zapewniających bezpieczeństwo rozwiązania chmurowego.

### **Zestawy efektów uczenia się**

Numer zestawu w kwalifikacji\*

1

Nazwa zestawu\*

Analiza kontekstu zapewnienia bezpieczeństwa rozwiązań chmurowych w organizacji

Poziom PRK\*

4

Orientacyjny nakład pracy [godz.]\*

30

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia\*

### **Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia**

Efekt uczenia się

1. Identyfikuje wymagania prawne względem bezpieczeństwa rozwiązań chmurowych w organizacji

Kryteria weryfikacji\*

a. Wskazuje typy działalności i danych objęte szczególnymi regulacjami prawnymi w kontekście bezpieczeństwa rozwiązań chmurowych; b. Wskazuje regulacje prawne mogące mieć wpływ na zakres i sposób zapewniania bezpieczeństwa dla rozwiązań chmurowych w organizacji; c. Omawia, na podstawie aktów prawnych, minimalne wymagania względem zapewnienia bezpieczeństwa rozwiązań chmurowych w organizacji.

Efekt uczenia się

2. Identyfikuje oczekiwania w zakresie zapewnienia bezpieczeństwa rozwiązań chmurowych w organizacji

Kryteria weryfikacji\*

a. Formułuje pytania mające na celu zidentyfikowanie oczekiwań właścicieli procesów biznesowych w zakresie zapewniania bezpieczeństwa rozwiązań chmurowych wykorzystywanych w organizacji; b. Identyfikuje uwarunkowania biznesowe i organizacyjne,

które wpływają na wymagania względem zapewnienia bezpieczeństwa dla rozwiązań chmurowych w organizacji; c. Identyfikuje, w jaki sposób i w jakim celu wykorzystywane i udostępniane są usługi chmurowe w organizacji.

Efekt uczenia się

3. Analizuje możliwości wdrożenia i stosowania w organizacji mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych

Kryteria weryfikacji\*

a. Formułuje pytania mające na celu zidentyfikowanie możliwości organizacyjnych, technicznych, czasowych i finansowych wdrożenia i stosowania w organizacji mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych; b. Opisuje, na podstawie dokumentacji technicznej systemów informatycznych wykorzystywanych w organizacji, możliwości oraz ograniczenia związane z wdrożeniem i stosowaniem w organizacji mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych; c. Wskazuje bariery w zastosowaniu w danej organizacji mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych wynikające z uwarunkowań biznesowych, organizacyjnych i prawnych.

Numer zestawu w kwalifikacji\*

2

Nazwa zestawu\*

Analiza ryzyka w zakresie bezpieczeństwa rozwiązań chmurowych w organizacji

Poziom PRK\*

5

Orientacyjny nakład pracy [godz.]\*

80

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia\*

### **Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia**

Efekt uczenia się

1. Analizuje poziom bezpieczeństwa usług chmurowych

Kryteria weryfikacji\*

a. Opisuje rodzaje usług chmurowych, ich właściwości, słabe i mocne strony w zakresie bezpieczeństwa; b. Opisuje możliwe zagrożenia dla poufności, integralności i dostępności danych i systemów informatycznych związane z wykorzystywaniem danej usługi chmurowej; c. Na podstawie dokumentacji dostawcy (np. regulaminu usługi) określa poziom bezpieczeństwa usługi chmurowej oraz możliwości stosowania rozwiązań zapewniających bezpieczeństwo; d. Porównuje usługi chmurowe pod kątem deklarowanego przez dostawcę

poziomu bezpieczeństwa oraz możliwości zastosowania rozwiązań zapewniających bezpieczeństwo.

Efekt uczenia się

2. Analizuje rozwiązanie chmurowe pod kątem zagrożeń dla jego bezpieczeństwa

Kryteria weryfikacji\*

a. Wyjaśnia pojęcia poufności, integralności i dostępności danych oraz systemów informatycznych; b. Wskazuje, na podstawie opisu architektury lub diagramu przepływu danych, potencjalne zagrożenia dla bezpieczeństwa rozwiązania chmurowego oraz poufności, integralności i dostępności przetwarzanych w nim danych; c. Identyfikuje w rozwiązaniu chmurowym, na podstawie opisu jego architektury lub diagramu przepływu danych, potencjalne miejsca wystąpienia zagrożenia dla jego bezpieczeństwa; d. Identyfikuje w ramach wykorzystywanych w organizacji rozwiązań chmurowych usługi, których bezpieczeństwo jest kluczowe z punktu widzenia działalności organizacji i obowiązujących ją wymagań zewnętrznych; e. Opisuje skutki dla organizacji wynikające z naruszenia bezpieczeństwa rozwiązania chmurowego.

Efekt uczenia się

3. Ocenia ryzyko wystąpienia zagrożenia dla bezpieczeństwa rozwiązań chmurowych w organizacji

Kryteria weryfikacji\*

a. Szacuje prawdopodobieństwo wystąpienia zagrożenia dla bezpieczeństwa rozwiązania chmurowego oraz poufności, integralności i dostępności przetwarzanych w nim danych; b. Opisuje skutki wystąpienia incydentu naruszającego bezpieczeństwo rozwiązania chmurowego; c. Ustala poziom i istotność ryzyka dla poszczególnych zagrożeń względem bezpieczeństwa rozwiązania chmurowego.

Numer zestawu w kwalifikacji\*

3

Nazwa zestawu\*

Opracowanie koncepcji zapewnienia bezpieczeństwa rozwiązania chmurowego w organizacji

Poziom PRK\*

5

Orientacyjny nakład pracy [godz.]\*

80

Rodzaj zestawu

obowiązkowy

Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia\*

## Poszczególne efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia

Efekt uczenia się

1. Analizuje mechanizmy zapewniające bezpieczeństwo rozwiązań chmurowych

Kryteria weryfikacji\*

a. Omawia typy, wady i zalety mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych (np. szyfrowanie danych, system zapobiegający wyciekowi danych); b. Porównuje skuteczność różnych mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych; c. Omawia warunki wdrożenia i stosowania mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych; d. Opisuje zasady doboru mechanizmów zapewniających bezpieczeństwo do typu usług chmurowych, zidentyfikowanych zagrożeń i oczekiwanego poziomu bezpieczeństwa; e. Wyjaśnia ograniczenia wynikające z zastosowania różnych mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych.

Efekt uczenia się

2. Analizuje koszty wdrożenia i stosowania mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych

Kryteria weryfikacji\*

a. Opisuje rodzaje kosztów związanych z wdrożeniem i stosowaniem poszczególnych mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych; b. Szacuje koszty wdrożenia i stosowania mechanizmów zapewniających bezpieczeństwo rozwiązań chmurowych; c. Ocenia efektywność zastosowania mechanizmów w odniesieniu do kosztów ich wdrożenia i stosowania, skuteczności działania i zapewnienia poziomu bezpieczeństwa; d. Ocenia zasadność wprowadzenia poszczególnych mechanizmów w odniesieniu do poziomu i istotności ryzyka dla danego zagrożenia.

Efekt uczenia się

3. Dobiera działania zapewniające bezpieczeństwo rozwiązania chmurowego

Kryteria weryfikacji\*

a. Przedstawia co najmniej dwa różne warianty zapewnienia bezpieczeństwa rozwiązania chmurowego w organizacji; b. Porównuje wady i zalety oraz warunki wdrożenia i stosowania przedstawionych wariantów zapewnienia bezpieczeństwa rozwiązania chmurowego w organizacji (np. różnice w kosztach, wymagań technicznych, zapewnianego poziomu bezpieczeństwa); c. Wyjaśnia ograniczenia przedstawionych wariantów zapewnienia bezpieczeństwa rozwiązania chmurowego w organizacji; d. Wskazuje działania i mechanizmy niezbędne do zrealizowania przedstawionego wariantu zapewnienia bezpieczeństwa rozwiązania chmurowego w organizacji.

## Informacje o instytucjach uprawnionych do nadawania kwalifikacji

Wnioskodawca\*

Polskie Towarzystwo Informatyczne

Minister właściwy\*

Minister Rozwoju i Technologii

Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności\*

Certyfikat jest ważny 3 lata. Przedłużenie ważności certyfikatu następuje na podstawie przedłożenia dokumentów potwierdzających wykonywanie, w okresie ważności certyfikatu, zadań związanych z zapewnieniem bezpieczeństwa usług chmurowych w organizacji przez okres co najmniej 1 roku.

Nazwa dokumentu potwierdzającego nadanie kwalifikacji\*

Certyfikat

Uprawnienia związane z posiadaniem kwalifikacji\*

Nie dotyczy

Kod dziedziny kształcenia\*

481 - Informatyka

Kod PKD\*

Kod	Nazwa
62	DZIAŁALNOŚĆ ZWIĄZANA Z OPROGRAMOWANIEM I DORADZTWEW W ZAKRESIE INFORMATYKI ORAZ DZIAŁALNOŚĆ POWIĄZANA

Status

Dokumenty

#	Tytuł dokumentu
1	Dowód wniesienia opłaty
2	Pełnomocnictwo
3	ZRK_FKU_nie dotyczy
4	ZRK_FKU_Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych



Oświadczam, że dane zawarte we wniosku o włączenie kwalifikacji rynkowej do Zintegrowanego Systemu Kwalifikacji są zgodne z prawdą. Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia.\*

Dane o podmiocie, który złożył wniosek

Polskie Towarzystwo Informatyczne  
Siedziba i adres: Solec 38 lok. 103, 00-394 Warszawa  
NIP: 5220002038  
REGON: 001236905  
Numer KRS: 0000043879

