W celu ułatwienia wypełniania w Zintegrowanym Rejestrze Kwalifikacji elektronicznego formularza „Wniosku o włączenie kwalifikacji do ZSK" zapraszamy zainteresowane podmioty do zapoznania się z formularzem pomocniczym do przygotowania wniosku o włączenie kwalifikacji rynkowej do ZSK. Jest on wzorowany na elektronicznym formularzu wniosku o włączenie kwalifikacji do ZSK, który musi wypełnić wnioskodawca w systemie informatycznym Zintegrowanego Rejestru Kwalifikacji. Formularz umożliwia zapoznanie się z treścią i strukturą docelowego formularza w ZRK. Jest w pełni edytowalny, co pozwala na przygotowanie w nim wszystkich wymaganych treści, a następnie ich przekopiowanie do elektronicznego formularza w systemie informatycznym ZRK. Przy czym należy pamiętać, że niemożliwe jest automatyczne zaciągnięcie informacji z formularza pomocniczego do formularza w ZRK – należy je każdorazowo skopiować do odpowiedniego pola w formularzu ZRK.

Formularz pomocniczy
do przygotowania wniosku o włączenie kwalifikacji rynkowej do ZSK,

opracowany na podstawie ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji[1] oraz elektronicznego formularza „Wniosek o włączenie kwalifikacji do ZSK" w ZRK

TYP FORMULARZA W ZRK: Wniosek o włączenie kwalifikacji do ZSK

I. INFORMACJE OGÓLNE O KWALIFIKACJI

1. Nazwa kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2a)
Należy wpisać pełną nazwę kwalifikacji, która ma być widoczna w ZRK i być umieszczana na dokumencie potwierdzającym jej uzyskanie. Nazwa kwalifikacji (na ile to możliwe) powinna:
- jednoznacznie identyfikować kwalifikację,
- różnić się od nazw innych kwalifikacji,
- różnić się od nazwy zawodu, stanowiska pracy, tytułu zawodowego, uprawnienia,
- być możliwie krótka,
- nie zawierać skrótów,
- być oparta na rzeczowniku odczasownikowym (np. gromadzenie, przechowywanie, szycie).

Maksymalna liczba znaków: 300

Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji

2. Skrót nazwy

Pole nieobowiązkowe. Pole wprowadzone w celu zapewnienia przejrzystości informacji gromadzonych w ZRK. Uwaga: jeżeli nazwa kwalifikacji nie ma skrótu pole należy pozostawić puste!

[1] Tekst jednolity, Dziennik Ustaw RP z 16 listopada 2018 r., poz. 2153, z późniejszymi zmianami

Maksymalna liczba znaków: 150

3. Rodzaj kwalifikacji*

Wskazanie, czy kwalifikacja jest: kwalifikacją pełną, czy kwalifikacją cząstkową. Należy wskazać, że kwalifikacja jest cząstkowa.

Kwalifikacja cząstkowa

4. Proponowany poziom Polskiej Ramy Kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 4.
Należy wpisać swoją propozycję poziomu PRK. Ostatecznie poziom PRK nada minister.

5 PRK

5. Krótka charakterystyka kwalifikacji, obejmująca informacje o działaniach lub zadaniach, które potrafi wykonywać osoba posiadająca tę kwalifikację oraz orientacyjny koszt uzyskania dokumentu potwierdzającego otrzymanie danej kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2d) oraz pkt 5.
Należy podać wybrane informacje o kwalifikacji skierowane do osób zainteresowanych uzyskaniem kwalifikacji oraz do pracodawców, które pozwolą im szybko ocenić, czy dana kwalifikacja jest właśnie tą, której poszukują.
Ponadto należy podać orientacyjną wysokość opłaty za przeprowadzenie walidacji i wystawienie dokumentu potwierdzającego otrzymanie danej kwalifikacji.

Maksymalna liczba znaków: 4000

Osoba posiadająca kwalifikację „Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji" jest przygotowana do wykonywania zadań związanych z zabezpieczaniem rozwiązań chmurowych. Identyfikuje wymagania w zakresie bezpieczeństwa, wynikające z regulacji prawnych, specyfiki działalności oraz wymagań właścicieli procesów biznesowych, którym 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).

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

Uwaga: Pole sumuje się automatycznie po wypełnieniu pól dotyczących zestawów efektów uczenia się.

7. Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2f)
Należy podać informacje na temat grup osób, które mogą być szczególnie zainteresowane uzyskaniem danej kwalifikacji (np. osoby zarządzające nieruchomościami, specjaliści z zakresu telekomunikacji, osoby powracające na rynek pracy itp.).

Maksymalna liczba znaków: 4000

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.

Kwalifikacja ta jest przeznaczona przede wszystkim dla osób specjalizujących się w projektowaniu i wdrażaniu rozwiązań chmurowych oraz zarządzania nimi. Może być również uzupełnieniem innych kwalifikacji dotyczących rozwiązań chmurowych.

7a. Należy zaznaczyć poniższe pole jeśli dotyczy (pole wprowadzone od 1.09.2019 r.)

☐ **Kwalifikacja może być przydatna dla uczniów szkół branżowych lub techników kształcących się w określonych zawodach** Rozporządzenie MEN z dnia 16 maja 2019 r.

W szkole prowadzącej kształcenie zawodowe kształcenie odbywa się w oparciu o podstawy programowe określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego (Dz. U. poz. 991). Część godzin zajęć może zostać przeznaczona na realizację obowiązkowych zajęć edukacyjnych przygotowujących uczniów do uzyskania kwalifikacji rynkowej funkcjonującej w ZSK, związanej z nauczanym zawodem (§ 4 ust 5 pkt 2 rozporządzenia Ministra Edukacji Narodowej z dnia 3 kwietnia 2019 r. w sprawie ramowych planów nauczania dla publicznych szkół (Dz. U. poz. 639)). Należy wskazać zawody (zgodnie z klasyfikacją zawodów szkolnictwa branżowego określoną w załączniku nr 2 do rozporządzenia Ministra Edukacji Narodowej z dnia 15 lutego 2019 r. w sprawie ogólnych celów i zadań kształcenia w zawodach szkolnictwa branżowego oraz klasyfikacji zawodów szkolnictwa branżowego (Dz. U. poz. 316)), w przypadku których zasadne jest przygotowywanie uczniów do uzyskania kwalifikacji rynkowej objętej wnioskiem.

7b. Wskazanie zawodów szkolnictwa zawodowego, z którymi związana jest kwalifikacja

Jeżeli w punkcie 7a wskazano przydatność kwalifikacji, to z rozwijanej listy branż i zawodów należy wybrać te zawody, z którymi związana jest wnioskowana kwalifikacja.

8. Wymagane kwalifikacje poprzedzające

Pole nieobowiązkowe.
Jeżeli są wymagane konkretne kwalifikacje pełne lub cząstkowe, które musi posiadać osoba ubiegająca się o nadanie kwalifikacji (np. dyplom ukończenia studiów medycznych albo dyplom potwierdzający kwalifikacje zawodowe w zawodzie np. „technik rachunkowości" albo świadectwo potwierdzające kwalifikację w zawodzie np. „naprawa zegarów i zegarków" itp.), należy je wpisać.

Maksymalna liczba znaków: 2000

Nie dotyczy

9. W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji*

Pole obowiązkowe Art. 15 ust.1 pkt 2g)

O ile dotyczy, należy podać warunki, które musi spełniać osoba, żeby przystąpić do walidacji i móc uzyskać kwalifikację (np. wymagany poziom wykształcenia – wyższe, podstawowe itp.; zaświadczenie o niekaralności; orzeczenie lekarskie o braku przeciwwskazań itp.)
Warunki przystąpienia do walidacji określone w opisie kwalifikacji powinny być możliwe do zweryfikowania (warunki te nie są tożsame z warunkami zatrudnienia).
Kompetencje wynikające z doświadczenia zawodowego powinny być odzwierciedlone przede wszystkim w opisie efektów uczenia się wymaganych dla kwalifikacji. Dlatego doświadczenie zawodowe powinno być wskazywane jako warunek przystąpienia do walidacji, jedynie w szczególnie uzasadnionych przypadkach.
Jeżeli nie ma takich warunków należy wpisać: „Nie dotyczy".

Maksymalna liczba znaków: 25000

Nie dotyczy

10. Zapotrzebowanie na kwalifikację*

Pole obowiązkowe Art. 15 ust.1 pkt 2i)
Należy wskazać, na jakie aktualne lub przewidywane potrzeby społeczne i gospodarcze (regionalne, krajowe, europejskie) odpowiada kwalifikacja. Warto odwołać się do różnych źródeł np. opinii organizacji gospodarczych, trendów obserwowanych na rynku pracy, prognoz dotyczących rozwoju technologii, a także strategii rozwoju kraju lub regionu.

Maksymalna liczba znaków: 25000

„Zapewnianie cyberbezpieczeństwa rozwiązań chmurowych w organizacji" 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 wydobyciu surowców. Transformacja cyfrowa i związane z nią projekty wdrażania rozwiązań chmurowych, w pierwszych dwóch dekadach XXI wieku dotyczyły głownie 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 wprowadzano 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 w organizacji. 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, doborem 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 wspominanego 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 w organizacji" 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 [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 przyśpieszyć 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://barometrzawodow.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].

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

Pole obowiązkowe Art. 15 ust. 1 pkt 2k)
Należy wskazać, czym kwalifikacja różni się od innych kwalifikacji o zbliżonym charakterze. Punktem odniesienia powinny być kwalifikacje funkcjonujące w ZSK. Ponadto należy wskazać kluczowe kwalifikacje wpisane do ZRK, które zawierają co najmniej jeden wspólny, kluczowy zestaw efektów uczenia się.

Maksymalna liczba znaków: 6000

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 w organizacji" 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 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.

Powyższe kwalifikacje mogą mieć zastosowanie w przemyśle, ze szczególnym zorientowaniem na systemy informatyczne nadzorujące przebiegi procesów technologicznych lub produkcyjnych SCADA (ang. Supervisory Control And Data Acquisition). Ponadto 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 w organizacji".

11a. 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**

Dodatkowe umiejętności zawodowe

Należy wybrać z listy „dodatkowe umiejętności zawodowe" (określone w rozporządzeniu MEN z dnia 16 maja 2019 r. w sprawie podstaw programowych kształcenia w zawodach szkolnictwa branżowego oraz dodatkowych umiejętności zawodowych w zakresie wybranych zawodów szkolnictwa branżowego, załącznik Nr 33) zawierające wspólne lub zbliżone zestawy efektów kształcenia z zestawami efektów uczenia się określonymi w kwalifikacji rynkowej.

11b. Wskazanie „dodatkowych umiejętności zawodowych" w zakresie wybranych zawodów szkolnictwa branżowego zawierających wspólne lub zbliżone zestawy efektów kształcenia (Branża – Zawód – Umiejętność)

Jeżeli w punkcie 11a udzielono pozytywnej odpowiedzi, to z rozwijanej listy branż, zawodów i dodatkowych umiejętności zawodowych należy wybrać te umiejętności, które zawierają wspólne lub zbliżone zestawy efektów kształcenia z wnioskowaną kwalifikacją.

12. Typowe możliwości wykorzystania kwalifikacji*

Pole obowiązkowe Art. 15 ust. 1 pkt 2j)
Należy wskazać przykładowe możliwości zatrudnienia i dalszego uczenia się osoby posiadającej daną kwalifikację, np.:
- Do pracy na jakich stanowiskach przygotowuje dana kwalifikacja?
- Jakie perspektywy dalszego rozwoju otwierają się dla osoby, która uzyskała tę kwalifikację?

Maksymalna liczba znaków: 4000

Osoba posiadająca kwalifikację może podjąć zatrudnienie w organizacjach, w których istotne jest zapewnienie cyberbezpieczeństwa rozwiązań chmurowych. Ponadto może prowadzić działalność doradczą w powyższym zakresie.

13. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację*

Pole obowiązkowe Art. 15 ust.1 pkt 2h)
Należy podać tylko takie wymagania, które muszą obowiązywać każdą instytucję przeprowadzającą walidację, żeby zapewnić odpowiedni poziom wiarygodności i porównywalności wyników walidacji w skali całego kraju. Wskazane wymagania powinny pozwalać na tworzenie różnych scenariuszy walidacji w różnych instytucjach.
Wymagania mogą dotyczyć:
- doboru metod stosowanych w walidacji - służących weryfikacji efektów uczenia się wymaganych dla kwalifikacji, ale także (o ile to potrzebne) identyfikowaniu i dokumentowaniu efektów uczenia się;
- kompetencji osób przeprowadzających walidację;
- warunków organizacyjnych i materialnych niezbędnych do przeprowadzenia walidacji.
Odpowiednio do potrzeby wymagania te mogą dotyczyć pojedynczych efektów uczenia się i poszczególnych lub wszystkich zestawów efektów uczenia się, wymaganych dla kwalifikacji.
Należy brać pod uwagę, że spełnienie tych wymagań jest jednym z warunków uzyskania przez daną instytucję uprawnień do nadawania kwalifikacji (uzyskania statusu „instytucji certyfikującej").
Więcej na temat walidacji: "Walidacja – nowe możliwości zdobywania kwalifikacji", IBE 2016.

Maksymalna liczba znaków: 25000

1. Etap weryfikacji

1.1. Metody

Do weryfikacji efektów uczenia się mogą być stosowane następujące metody:

- test teoretyczny;
- analiza dowodów i deklaracji opcjonalnie uzupełniona wywiadem swobodnym.

1.2. Zasoby kadrowe

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 lub jednolitych studiów magisterskich);
- legitymuje się co najmniej rocznym doświadczeniem w przeprowadzaniu egzaminów w obszarze technologii cyfrowej lub cyberbezpieczeństwa osiągniętym w okresie ostatnich 6 lat.

Członek komisji walidacyjnej musi spełniać następujące warunki:

- posiada kwalifikację pełną z 6 poziomem 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

Walidacja może być prowadzona w trybie stacjonarnym, online lub hybrydowym.

W przypadku organizacji walidacji w trybie stacjonarnym instytucja certyfikująca musi zapewnić:

- pracownię wyposażoną w stanowisko komputerowe dla każdego uczestnika walidacji.

W przypadku organizacji walidacji w trybie online lub hybrydowym instytucja certyfikująca musi zapewnić:

- dostęp do systemu obsługi testów i egzaminów indywidualnie dla każdego uczestnika.

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.

Etapy identyfikowania i dokumentowania mogą być realizowane dowolnymi metodami.

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

Jeśli w danym sektorze lub branży funkcjonuje Sektorowa Rama Kwalifikacji, która jest włączona do ZSK, zgodnie z Art. 15 ust. 1 pkt 4 należy to pole wypełnić poprzez podanie nazwy odpowiedniej ramy i wpisanie swojej propozycji poziomu w tej ramie.

Maksymalna liczba znaków: 1000

Nie dotyczy

II. EFEKTY UCZENIA SIĘ WYMAGANE DLA KWALIFIKACJI

15. Syntetyczna charakterystyka efektów uczenia się*

Pole obowiązkowe Art. 15 ust. 1 pkt 3 oraz art. 9 ust. 1 pkt 1a)
Należy przedstawić w zwięzłej formie ogólną charakterystykę wiedzy, umiejętności i kompetencji społecznych poprzez określenie rodzajów działań, do których podjęcia będzie przygotowana osoba posiadająca daną kwalifikację.
Syntetyczna charakterystyka efektów uczenia się powinna nawiązywać do charakterystyki odpowiedniego poziomu PRK.
W szczególności syntetyczna charakterystyka powinna wskazać na:
- stopień przygotowania osoby posiadającej kwalifikację do samodzielnego działania,
- stopień złożoności działań, które osoba posiadająca kwalifikację może wykonywać,
- role, które osoba posiadająca kwalifikację może pełnić w grupie pracowników.

Maksymalna liczba znaków: 9000

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

16. Wyodrębnione zestawy efektów uczenia się*

Wykaz zestawów efektów uczenia się wymaganych dla kwalifikacji, zawierający: numer porządkowy (1, 2, …), nazwy zestawów, orientacyjne odniesienie każdego zestawu do poziomu PRK oraz orientacyjny nakład pracy potrzebny do osiągnięcia efektów uczenia w każdym zestawie.
Nazwa zestawu powinna:

- *nawiązywać do efektów uczenia się wchodzących w skład danego zestawu lub odpowiadać specyfice wchodzących w jego skład efektów uczenia się,*
- *być możliwie krótka,*
- *nie zawierać skrótów,*
- *gdy jest to możliwe, być oparta na rzeczowniku odczasownikowym, np. „gromadzenie", „przechowywanie", „szycie".*

Maksymalna liczba znaków - nazwa zestawu: 500

1. Analiza kontekstu zapewnienia cyberbezpieczeństwa rozwiązań chmurowych w organizacji, 5 PRK, 30 godzin, rodzaj zestawu: obowiązkowy

2. Analiza ryzyka w zakresie cyberbezpieczeństwa rozwiązań chmurowych w organizacji, 5 PRK, 80 godzin, rodzaj zestawu: obowiązkowy

3. Opracowanie koncepcji zapewnienia cyberbezpieczeństwa rozwiązania chmurowego w organizacji, 5 PRK, 80 godzin, rodzaj zestawu: obowiązkowy

17. Poszczególne efekty uczenia się w zestawach*

Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c)
Należy podać poszczególne efekty uczenia się (w zestawach) opisane za pomocą umiejętności (tj. zdolności wykonywania zadań i rozwiązywania problemów) wraz z kryteriami ich weryfikacji, które doprecyzowują ich zakres oraz określają niezbędną wiedzę i kompetencje społeczne. Poszczególne efekty uczenia się (w zestawach) powinny być jednoznaczne, niebudzące wątpliwości, pozwalające na zaplanowanie i przeprowadzanie walidacji, których wyniki będą porównywalne; realne, możliwe do osiągnięcia

przez osoby, dla których kwalifikacja jest przewidziana; możliwe do zweryfikowania podczas walidacji; zrozumiałe dla osób potencjalnie zainteresowanych kwalifikacją. *Podczas opisywania poszczególnych efektów uczenia się (w zestawach) korzystne jest stosowanie czasowników operacyjnych (np. wykonuje, demonstruje, diagnozuje).* *Maksymalna liczba znaków – nazwa efektu uczenia się: 2000* *Maksymalna liczba znaków - kryteria weryfikacji (dla jednego efektu): 5000*	
Zestaw efektów uczenia się:	01. Analiza kontekstu zapewnienia cyberbezpieczeństwa rozwiązań chmurowych w organizacji
Efekty uczenia się* *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać pełną nazwę efektu uczenia się.*	**Kryteria weryfikacji*** *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać kryteria , na podstawie których ocenia się, czy dany efekt uczenia się został osiągnięty.*
1. Identyfikuje wymagania prawne w odniesieniu do cyberbezpieczeństwa rozwiązań chmurowych w organizacji	a. Wskazuje typy działalności i danych objęte regulacjami prawnymi w kontekście cyberbezpieczeństwa rozwiązań chmurowych; b. Wskazuje aktualne regulacje prawne mogące mieć wpływ na zakres i sposób zapewniania cyberbezpieczeństwa dla rozwiązań chmurowych w organizacjach; c. Omawia wymagania względem zapewnienia cyberbezpieczeństwa rozwiązań chmurowych w organizacji na podstawie aktów prawnych.
2. Identyfikuje oczekiwania w zakresie zapewnienia cyberbezpieczeństwa rozwiązań chmurowych w organizacji	a. Formułuje pytania mające na celu zidentyfikowanie oczekiwań właścicieli procesów biznesowych w zakresie zapewniania cyberbezpieczeństwa rozwiązań chmurowych wykorzystywanych w organizacji; b. Identyfikuje uwarunkowania biznesowe i organizacyjne, wpływające na wymagania względem zapewnienia cyberbezpieczeństwa dla rozwiązań chmurowych w organizacji; c. Identyfikuje, w jaki sposób udostępniane są usługi chmurowe w organizacji.
3. Analizuje możliwości wdrożenia i stosowania w organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych	a. Formułuje pytania mające na celu zidentyfikowanie możliwości organizacyjnych, technicznych, czasowych i finansowych wdrożenia i stosowania w organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych; b. Opisuje możliwości oraz ograniczenia związane z wdrożeniem i stosowaniem w organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych na podstawie dokumentacji technicznej systemów informatycznych wykorzystywanych w organizacji;

	c. Wskazuje bariery w zastosowaniu w danej organizacji mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych wynikające z uwarunkowań biznesowych, organizacyjnych i prawnych.
Zestaw efektów uczenia się:	02. Analiza ryzyka w zakresie cyberbezpieczeństwa rozwiązań chmurowych w organizacji
Efekty uczenia się* *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać pełną nazwę efektu uczenia się.*	**Kryteria weryfikacji*** *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać kryteria , na podstawie których ocenia się, czy dany efekt uczenia się został osiągnięty.*
1. Analizuje poziom cyberbezpieczeństwa usług chmurowych	a. Opisuje rodzaje usług chmurowych, ich właściwości, słabe i mocne strony w zakresie cyberbezpieczeństwa; b. Opisuje możliwe zagrożenia dla poufności, integralności i dostępności danych i systemów informatycznych związane z wykorzystywaniem danej usługi chmurowej; c. Określa poziom cyberbezpieczeństwa usługi chmurowej oraz możliwości stosowania rozwiązań zapewniających bezpieczeństwo na podstawie dokumentacji dostawcy (np. regulaminu usługi); d. Porównuje usługi chmurowe pod kątem deklarowanego przez dostawcę poziomu cyberbezpieczeństwa oraz możliwości zastosowania rozwiązań zapewniających bezpieczeństwo.
2. Analizuje rozwiązanie chmurowe pod kątem zagrożeń dla jego cyberbezpieczeństwa	a. Wyjaśnia pojęcia poufności, integralności i dostępności danych oraz systemów informatycznych; b. Wskazuje zagrożenia dla cyberbezpieczeństwa rozwiązania chmurowego oraz poufności, integralności i dostępności przetwarzanych w nim danych na podstawie opisu architektury lub diagramu przepływu danych; c. Identyfikuje w rozwiązaniu chmurowym miejsca wystąpienia zagrożenia dla jego bezpieczeństwa na podstawie opisu jego architektury lub diagramu przepływu danych; d. Identyfikuje usługi chmurowe w organizacji, których bezpieczeństwo jest kluczowe z punktu widzenia działalności organizacji i obowiązujących ją wymagań zewnętrznych; e. Opisuje skutki dla organizacji wynikające z naruszenia cyberbezpieczeństwa rozwiązania chmurowego.

3. Ocenia ryzyko wystąpienia zagrożenia dla cyberbezpieczeństwa rozwiązań chmurowych w organizacji	a. Szacuje prawdopodobieństwo wystąpienia zagrożenia dla cyberbezpieczeństwa rozwiązania chmurowego oraz poufności, integralności i dostępności przetwarzanych w nim danych; b. Opisuje skutki wystąpienia incydentu naruszającego cyberbezpieczeństwo rozwiązania chmurowego; c. Ustala poziom i istotność ryzyka dla poszczególnych zagrożeń względem cyberbezpieczeństwa rozwiązania chmurowego.
Zestaw efektów uczenia się:	03. Opracowanie koncepcji zapewnienia cyberbezpieczeństwa rozwiązania chmurowego w organizacji
Efekty uczenia się* *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać pełną nazwę efektu uczenia się.*	**Kryteria weryfikacji*** *Pole obowiązkowe Art. 15 ust. 1 pkt 3) oraz art. 9 ust. 1 pkt 1c).* *Należy podać kryteria , na podstawie których ocenia się, czy dany efekt uczenia się został osiągnięty.*
1. Analizuje mechanizmy zapewniające cyberbezpieczeństwo rozwiązań chmurowych	a. Omawia typy, wady i zalety mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych (np. szyfrowanie danych, system zapobiegający wyciekowi danych); b. Porównuje skuteczność różnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych; c. Omawia warunki wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych; d. Opisuje zasady doboru mechanizmów zapewniających cyberbezpieczeństwo do typu usług chmurowych, zidentyfikowanych zagrożeń i oczekiwanego poziomu bezpieczeństwa; e. Wyjaśnia ograniczenia wynikające z zastosowania różnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych.
2. Analizuje koszty wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych	a. Opisuje rodzaje kosztów związanych z wdrożeniem i stosowaniem poszczególnych mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych; b. Szacuje koszty wdrożenia i stosowania mechanizmów zapewniających cyberbezpieczeństwo rozwiązań chmurowych;

	c. Ocenia efektywność zastosowania mechanizmów w odniesieniu do kosztów ich wdrożenia i stosowania, skuteczności działania i zapewnienia poziomu cyberbezpieczeństwa; d. Ocenia zasadność wprowadzenia poszczególnych mechanizmów w odniesieniu do poziomu i istotności ryzyka dla danego zagrożenia.
3. Proponuje działania zapewniające cyberbezpieczeństwo rozwiązania chmurowego	a. Przygotowuje warianty zapewnienia cyberbezpieczeństwa rozwiązania chmurowego w organizacji; b. Porównuje wady i zalety oraz warunki wdrożenia i stosowania przedstawionych wariantów zapewnienia cyberbezpieczeństwa rozwiązania chmurowego w organizacji; c. Wyjaśnia ograniczenia przedstawionych wariantów zapewnienia cyberbezpieczeństwa rozwiązania chmurowego w organizacji; d. Wskazuje działania i mechanizmy niezbędne do zrealizowania przedstawionego wariantu zapewnienia cyberbezpieczeństwa rozwiązania chmurowego w organizacji.

III. PODMIOTY

18. Wnioskodawca*
Pole obowiązkowe Art. 83 ust. 1 pkt 7 *Nazwę podmiotu wnioskującego należy wybrać z listy rozwijanej w formularzu w ZRK.*
Polskie Towarzystwo Informatyczne
19. Minister właściwy*
Pole obowiązkowe Art. 16 ust. 1 *Należy wybrać z listy nazwę ministerstwa, które zdaniem wnioskodawcy jest właściwe do rozpatrzenia wniosku.*
Minister Cyfryzacji

IV. POZOSTAŁE INFORMACJE

20. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji i warunki przedłużenia jego ważności*
Pole obowiązkowe Art. 15 ust. 1 pkt 2b) *W przypadku kwalifikacji nadawanej na czas nieokreślony, należy wpisać: „Kwalifikacja ważna bezterminowo”.*

W przypadku kwalifikacji nadawanej na czas określony, należy podać, po jakim czasie konieczne jest odnowienie ważności oraz warunki przedłużenia ważności dokumentu potwierdzającego nadanie kwalifikacji. *Maksymalna liczba znaków: 2000*
Certyfikat jest ważny 3 lata. Przedłużenie ważności certyfikatu następuje na podstawie dokumentów potwierdzających wykonywanie, w okresie ważności certyfikatu, zadań związanych z zapewnieniem bezpieczeństwa usług chmurowych w organizacji przez okres co najmniej 1 roku.
21. Nazwa dokumentu potwierdzającego nadanie kwalifikacji*
Pole obowiązkowe Art. 15 ust. 1 pkt 2b) *Z rozwijanej listy należy wybrać nazwę dokumentu np. dyplom, świadectwo, certyfikat, zaświadczenie.*
Certyfikat
22. Uprawnienia związane z posiadaniem kwalifikacji*
Pole obowiązkowe Art. 15 ust. 1 pkt 2e) *Należy podać, o jakie uprawnienia może się ubiegać osoba po uzyskaniu kwalifikacji.* *Jeśli z uzyskaniem kwalifikacji nie wiąże się uzyskanie uprawnień, należy wpisać: „Nie dotyczy".* *Maksymalna liczba znaków: 2500*
Nie dotyczy
23. Kod dziedziny kształcenia*
Pole obowiązkowe Art. 15 ust. 1 pkt. 6. *Należy wpisać kod dziedziny kształcenia, o którym mowa w przepisach wydanych na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2012 r. poz. 591, z późn. zm.).*
481 - Informatyka
24. Kod PKD*
Pole obowiązkowe Art. 15 ust. 1 pkt 7. *Należy wpisać kod Polskiej Klasyfikacji Działalności (PKD), o którym mowa w Rozporządzeniu Rady Ministrów z dn. 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz.U. 251, poz.1885, z późn. zm.).*
62 - DZIAŁALNOŚĆ ZWIĄZANA Z OPROGRAMOWANIEM I DORADZTWEM W ZAKRESIE INFORMATYKI ORAZ DZIALALNOŚĆ POWIĄZANA

Uwaga:
*Pola oznaczone * to pola obowiązkowe do wypełnienia zgodnie z ustawą z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (t.j., Dziennik Ustaw RP z 16 listopada 2018 r., poz. 2153, z późniejszymi zmianami).*