Ministerstwo Finansów

……

(nazwa ministerstwa przeprowadzającego konsultacje)

Formularz podsumowania konsultacji z zainteresowanymi środowiskami

przeprowadzonych na podstawie art. 19 ust. 1 ustawy o ZSK[1]

wniosku **Fundacji Warszawski Instytut Bankowości**

o włączenie kwalifikacji rynkowej

„Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych”

do **Zintegrowanego Systemu Kwalifikacji**

Nazwa kwalifikacji	Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych
Nazwa podmiotu, który złożył wniosek	Fundacja Warszawski Instytut Bankowości
Czas trwania konsultacji	14.12.2021r. – 13.01.2022r.
Liczba podmiotów, które wzięły udział w konsultacjach	11
Liczba głosów aprobujących wniosek	8
Liczba głosów negujących wniosek	1
Liczba głosów niejednoznacznych	2

[1] Tekst jednolity Dz. U. z 2020 r., poz. 226

Zestawienie uwag do wybranych pól wniosku

Lp.	Wybrane pole wniosku	Liczba uwag	Autorzy uwag
1.	Nazwa kwalifikacji Skrót nazwy	1	- Związek Banków Polskich
2.	Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji	5	- Związek Banków Polskich - Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa - Ubezpieczeniowy Fundusz Gwarancyjny - Związek Firm Pośrednictwa Finansowego - Polska Izba Informatyki i Telekomunikacji
3.	Wymagane kwalifikacje poprzedzające	1	- Związek Banków Polskich
4.	W razie potrzeby warunki, jakie musi spełniać osoba przystępująca do walidacji	1	- Związek Banków Polskich
5.	Zapotrzebowanie na kwalifikację	2	- Związek Banków Polskich - Związek Firm Pośrednictwa Finansowego - Kancelaria Prezesa Rady Ministrów
6.	Odniesienie do kwalifikacji o zbliżonym charakterze oraz wskazanie kwalifikacji ujętych w ZRK zawierających wspólne zestawy efektów uczenia się	1	- Związek Banków Polskich

7.	Typowe możliwości wykorzystania kwalifikacji	2	- Związek Banków Polskich - Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa
8.	Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację	4	- Związek Banków Polskich - Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa - Urząd Komisji Nadzoru Finansowego - Związek Firm Pośrednictwa Finansowego
9.	Opis efektów uczenia się, obejmujący syntetyczną charakterystykę efektów uczenia się, zestawy efektów uczenia się, poszczególne efekty uczenia się w zestawach wraz z kryteriami weryfikacji ich osiągnięcia	4	- Związek Banków Polskich - Ubezpieczeniowy Fundusz Gwarancyjny - Urząd Komisji Nadzoru Finansowego - Kancelaria Prezesa Rady Ministrów

Odniesienie się do zgłoszonych uwag

Wniosek Fundacji Warszawski Instytut Bankowości o włączenie kwalifikacji rynkowej **„Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych”** do **Zintegrowanego Systemu Kwalifikacji** został poddany konsultacjom ze środowiskami zainteresowanymi w dniach od 14 grudnia 2021 roku do 13 stycznia 2022 roku.

Zaproszenie do przedmiotowych konsultacji skierowano do 52 podmiotów oraz opublikowano na stronie internetowej www.kwalifikacje.gov.pl w dziale ogłoszenia. Odpowiedzi udzieliło 11 podmiotów, spośród których 9 odesłało wypełniony formularz konsultacji. Za dalszą pracą nad kwalifikacją opowiedziało się 8 podmiotów, natomiast 1 podmiot uznał, iż jest to nieuzasadnione i oddał głos negujący. Pozostałe 2 podmioty poinformowały o braku uwag do wniosku, jednak bez jednoznacznego określenia, czy według nich dalsza praca nad kwalifikacją jest uzasadniona, co zostało uznane jako głosy niejednoznaczne.

Obszary wniosku, które wzbudziły najwięcej wątpliwości oraz streszczenie uwag:

1) „Grupy osób, które mogą być zainteresowane uzyskaniem kwalifikacji”.

Wskazano na brak precyzyjnego określenia zakresu podmiotowego oddziaływania kwalifikacji, tj. pojęcia „pracownik”, „instytucja finansowa”, „infrastruktura finansowa” pozostają niedookreślone, co może doprowadzić do konieczności każdorazowego rozstrzygania czy dana grupa osób spełnia/nie spełnia warunków do posiadania tej kwalifikacji.

Zaproponowano ograniczenie obowiązku uzyskania kwalifikacji (w przypadku pracowników pośrednika finansowego) tylko do szczególnych stanowisk, np. dyrektora komórki odpowiedzialnej za bezpieczeństwo IT, z uwagi na to, iż nie wszyscy pracownicy pośrednika finansowego mają bezpośredni kontakt z klientem, a jeśli taki mają, to najczęściej nie wiąże się on z przekazaniem danych wrażliwych.

Wskazano inne grupy, które mogą być zainteresowane uzyskaniem kwalifikacji, mianowicie informatycy i pracownicy biurowi innych specjalizacji, czyli pracownicy instytucji finansowych pracujący na stanowiskach bezpośrednio niezwiązanych z działalnością finansową, a posiadający wykształcenie kierunkowe inne niż tylko związane z obszarem bankowości i finansów.

Zwrócono także uwagę na brak w opisie pojęcia „podatności”, gdyż technologie cyfrowe nie stwarzają cyberzagrożeń same z siebie - one mogą posiadać podatności określonego poziomu ryzyka, zaś działania klientów mogą prowadzić do powstawania podatności, które mogą zostać wykorzystane przez cyberzagrożenia.

2) „Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację”.

W zakresie wymagań wobec podmiotów przeprowadzających walidację wskazano na posiadanie szerokich kompetencji branżowych z zakresu bezpieczeństwa teleinformatycznego (specjaliści od cyberbezpieczeństwa posiadający certyfikaty – wiedzę z zakresu, np. CISSP, CEH, CPEH, OSCP, normy PN-EN ISO/IEC 27001).

W zakresie czwartego zestawu efektów uczenia się (tj. stosowanie uniwersalnych przepisów zapewniających bezpieczeństwo informacji, infrastruktury teleinformatycznej, pracowników oraz klientów w instytucji finansowej) przyjęto walidację polegającą na przedstawieniu pisemnego potwierdzenia przez pracodawcę, że uczestnik stosuje politykę bezpieczeństwa obowiązującą w jego firmie, zastępując tym test wiedzy, co nie jest uzasadnione charakterem efektu uczenia się, który odnosi się do uniwersalnych przepisów zapewniających bezpieczeństwo informacji, infrastruktury teleinformatycznej, pracowników oraz klientów w instytucji finansowej, nie zaś stosowania ich u

konkretnego pracodawcy. Zauważono, iż uczestnicy powinni jednakowo zaliczyć ten efekt uczenia się w zestawie czwartym, poprzez pytania w ramach testu teoretycznego, gdyż różnicowanie uczestników na tych z oświadczeniami od firm i na tych, którzy ich nie dostarczą, może budzić zamieszanie dla instytucji certyfikującej czy przygotowanie osobnych testów dla uczestników w ramach tego samego egzaminu, a przyjęcie walidacji polegającej na przeprowadzeniu testu teoretycznego pozwoliłoby na realną weryfikację uzyskania przez uczestnika oczekiwanego poziomu wiedzy. Nie wskazano przy tym formy poświadczania przez pracodawcę zaktualizowanych efektów uczenia się oraz zakresu, formy i miejsca szkolenia. Wskazano, iż wymóg dotyczący składu osobowego komisji w zespole walidacyjnym jest obowiązkiem zbyt rygorystycznym.

Zwrócono uwagę na fakt, iż wymagania w tym obszarze wniosku projektowane były przed pandemią koronawirusa SARS-CoV-2, dlatego proces walidacji i wymagań z nim związanych wymaga uproszczenia i dostosowania do przeprowadzenia walidacji w bezpiecznych warunkach z zachowaniem reżimu sanitarnego, w tym z możliwością formy zdalnej. Zaproponowano zastąpienie weryfikacji wskazanych we wniosku efektów uczenia się dot. obserwacji w warunkach symulowanych, formą praktycznych pytań ustnych, które można przeprowadzić zarówno w bezpiecznej formule stacjonarnej oraz zdalnie.

3) „Opis efektów uczenia się, obejmujący syntetyczną charakterystykę efektów uczenia się, zestawy efektów uczenia się, poszczególne efekty uczenia się w zestawach wraz z kryteriami weryfikacji ich osiągnięcia".

Wskazano na użycie niepoprawnego pojęcia „ryzyko cyberzagrożenia" i zaproponowano użycie sformułowania „ryzyko wystąpienia podatności" lub „materializacja cyberzagrożenia". Podniesiono, iż zagrożenia nie wynikają z powodu funkcjonowania w cyberprzestrzeni, tylko jesteśmy na nie narażeni w jej obszarze i w związku z tym sformułowanie „uświadamiać o zagrożeniach wynikających z funkcjonowania w cyberprzestrzeni" należałoby zmienić na „uświadamiać o zagrożeniach występujących w cyberprzestrzeni". W ramach zdefiniowanych umiejętności, sformułowania „opisuje" i „wymienia" powinny być zastąpione „potrafi zastosować", „umie tworzyć", aby podkreślić znaczenie i sprawdzić praktyczne umiejętności pracowników w zakresie cyberbezpieczeństwa (np. „potrafi korzystać z menadżerów haseł").

Zwrócono uwagę, iż **informacje dotyczące klientów poszczególnych instytucji finansowych chronione są zarówno w ramach przepisów regulujących przetwarzanie danych osobowych, jak i w ramach poszczególnych tajemnic związanych z działalnością na rynku finansowym.** Jako przykład tego typu tajemnicy wskazać można na obowiązującą pracowników banków tajemnicę bankową. Uwzględniając szczególną ochronę danych dotyczących klientów instytucji finansowych, zasadne pozostaje doprecyzowanie brzmienia opisu efektu uczenia się „chroni dane identyfikacyjne swoje i klientów przed ujawnieniem osobom niepowołanym", w którym wskazano, że uczestnik „wymienia zasady i warunki umieszczania informacji zawierających dane identyfikacyjne swoje lub klientów w ogólnodostępnych serwisach internetowych", aby nie sugerował dopuszczalności umieszczania danych klientów instytucji finansowych w ogólnodostępnych serwisach internetowych.

Streszczenie pozostałych uwag na temat kwalifikacji:

Pomimo zajęcia przez 8 podmiotów stanowiska, iż dalsza praca nad kwalifikacją jest uzasadniona, to większość z nich wskazało szereg istotnych uwag do wniosku. Jeden z 11 podmiotów, które wzięły udział w konsultacjach, wyraził jednoznaczny sprzeciw wobec włączenia kwalifikacji do Zintegrowanego Systemu Kwalifikacji.

Zwrócono uwagę, iż intensywny proces cyfryzacji usług finansowych oraz narastające ryzyko cyberprzestępczości w zestawieniu ze skalą potrzeb edukacji finansowej klientów, która nadal w Polsce pozostaje na niskim poziomie, włączenie kwalifikacji do ZSK należy uznać za zasadne i przyczyni się to do lepszego przygotowania pracowników instytucji finansowych do bezpiecznego funkcjonowania w cyberśrodowisku i korzystania z narzędzi oraz technologii, które stwarzają

cyberzagrożenie dla instytucji finansowych i ich klientów.

Zauważono, iż we wniosku powołano się na Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, zaś od 2019 roku obowiązuje Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024. Wskazany we wniosku Raport „Nadużycia w sektorze finansowym" jest datowany na 2017 r., a najnowsza wersja dostępna jest z 2021 roku (dostępna jest również wersja z 2019 r.). **Zwrócono uwagę, iż opublikowane zostały rozporządzenia Rady Ministrów w sprawie tzw. usług kluczowych oraz inne akty wykonawcze do ustawy o krajowym systemie cyberbezpieczeństwa, a aktualnie procedowana jest nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, a także, na poziomie unijnym, trwają ostatnie uzgodnienia dotyczące Dyrektywy NIS w wersji 2.0.**

Wskazano, iż zestaw nr 3 w kwalifikacji dotyczy zagadnień związanych z ochroną danych osobowych oraz szerzej tożsamości cyfrowej, a **nie odwołuje się w żadnym punkcie do zagadnień prawnych związanych z RODO[2], który jest podstawowym aktem prawnym regulującym te zagadnienia na obszarze całej Unii Europejskiej.**

We wniosku nie zostało doprecyzowane, których pracowników pośrednika finansowego obowiązek ma dotyczyć. Większość pracowników pośrednika finansowego nie ma kontaktu z klientem ani nie przekazuje mu danych wrażliwych.

Wskazano, iż rozważenia wymaga kwestia przyporządkowania opiniowanej kwalifikacji rynkowej do poziomu 2 Polskiej Ramy Kwalifikacji (zamiast do poziomu 3 PRK). Uwzględniając kod dziedziny kształcenia „481 – Informatyka" oraz objęcie nią kwestii związanych z cyberbezpieczeństwem, punktem odniesienia w zakresie zweryfikowania prawidłowości przyporządkowanego poziomu kwalifikacji rynkowej mogą być inne kwalifikacje z ww. dziedziny, a w szczególności dotyczące cyberbezpieczeństwa lub obejmujące częściowo zakresem pewne aspekty cyberbezpieczeństwa. Należą do nich przede wszystkim kwalifikacje: „Zarządzanie cyberbezpieczeństwem – specjalista" oraz „Certyfikat umiejętności komputerowych – poziom podstawowy". Pierwsza z wymienionych kwalifikacji została przypisana do poziomu 4 PRK, ale obejmuje zakresem dalece bardziej specjalistyczną wiedzę i umiejętności, niż kwalifikacja objęta konsultowanym wnioskiem. Poza pogłębioną wiedzą z zakresu pojęć i przepisów dotyczących cyberbezpieczeństwa, osoba uzyskująca kwalifikację „Zarządzanie cyberbezpieczeństwem – specjalista" posiada m.in. znajomość standardów z obszaru bezpieczeństwa informacji opracowanych przez organizacje standaryzacyjne; identyfikuje i opisuje zbiór najlepszych praktyk zarządzania usługami IT w odniesieniu do cyberbezpieczeństwa; omawia wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji; omawia metody odtwarzania po naruszeniach bezpieczeństwa czy też posiada wiedzę i umiejętności z zakresu informatyki śledczej dotyczącą sposobów prawidłowego zabezpieczania materiału dowodowego i postępowania z cyfrowymi śladami dowodowymi, czy charakteryzuje stosowane wytyczne dotyczące aspektów technicznych i najlepszych praktyk informatyki śledczej – certyfikat ten przeznaczony jest m.in. dla specjalistów komórek organizacyjnych odpowiedzialnych w organizacjach za ochronę informacji i cyberbezpieczeństwo oraz kształtowanie polityki bezpieczeństwa. Druga z wymienionych kwalifikacji, tj. „Certyfikat umiejętności komputerowych – poziom podstawowy" obejmuje natomiast podstawowe umiejętności i znajomości zagadnień z zakresu obsługi komputera, a jej poziom określono jako poziom 2 PRK. **Istotne jest przy tym, że zakres wiedzy i umiejętności objętych tym certyfikatem częściowo pokrywa się z kwalifikacją objętą opiniowanym wnioskiem.** Dotyczy to poniższych efektów uczenia się:

- stosuje procedury bezpiecznego logowania oraz wyjaśnia politykę i zasady bezpiecznych haseł,

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

- uzasadnia konieczność stosowania zapory (firewall) i podaje cel jej użycia,
- uzasadnia potrzebę archiwizacji danych na zewnętrznych nośnikach i potrzebę regularnego uaktualniania oprogramowania,
- definiuje pojęcie złośliwego oprogramowania i używa oprogramowania antywirusowego do skanowania komputera,
- przestrzega zasad dotyczących wysyłania załączników,
- wyjaśnia zagrożenia związane z niechcianą pocztą,
- charakteryzuje sposoby ochrony przed negatywnymi skutkami korzystania z portali społecznościowych.

Analiza treści efektów uczenia się zawartych w opiniowanym wniosku, w odniesieniu do charakterystyk efektów uczenia się dla kwalifikacji poziomów 2 i 3 Polskiej Ramy Kwalifikacji, wskazuje na zasadność rozważenia przypisania kwalifikacji „Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych" do poziomu 2 PRK.

Podmiot, który wyraził **jednoznaczny sprzeciw** wobec włączenia kwalifikacji „Stosowanie zasad cyberbezpieczeństwa przez pracowników instytucji finansowych" do Zintegrowanego Systemu Kwalifikacji, podniósł, iż włączenie tej kwalifikacji w ramy oficjalnego rejestru spowoduje nieuzasadniony wymóg legitymowania się uzyskaną kwalifikacją wobec pracowników instytucji finansowych. W następstwie tego organy nadzoru, a w dalszej kolejności partnerzy biznesowi, tacy jak banki czy dostawcy usług chmury obliczeniowej, zyskają możliwość wymagania legitymowania się certyfikatem ujętym w oficjalnym rejestrze, przy jednoczesnym braku oparcia takiego wymogu w bezwzględnie obowiązujących przepisach. **Aktualnie obowiązujące regulacje nakładają na szereg podmiotów, w tym na instytucje finansowe, obowiązki w zakresie zapewniania szkoleń na rzecz osób odpowiedzialnych w organizacji za dany obszar.** Przykładowo na podstawie art. 52 ust. 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2018 r. poz. 723 ze zm.) instytucje obowiązane powinny zapewnić osobom wykonującym obowiązki związane z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu udział w programach szkoleniowych dotyczących realizacji tych obowiązków. Wobec braku kwalifikacji w zakresie przeciwdziałania praniu pieniędzy ujętej w ZSK, organy nadzoru nie wymagają od instytucji finansowych zapewniania konkretnych szkoleń, pozostawiając dowolność w wyborze kursów najbardziej odpowiadających charakterowi danej instytucji. **Włączenie kwalifikacji do ZSK doprowadzi do powstania niepewności regulacyjnej w zakresie kolejnych wymagań wobec instytucji finansowych.** W obecnym stanie prawnym, cele stawiane przez regulacje wobec instytucji finansowych w zakresie szkoleń są możliwe do spełnienia i dlatego włączenie kwalifikacji do ZSK należy uznać za bezcelowe. **Wskazano na wysoki poziom ogólności i niedopasowania zakładanych efektów kształcenia do charakteru działalności poszczególnych instytucji finansowych.** Charakterystyka kwalifikacji jest ogólna i nie odnosi się precyzyjnie do działalności konkretnych instytucji finansowych, a kompetencje, których uzyskaniu ma służyć zdobycie kwalifikacji, powinien nabyć każdy użytkownik internetu – np. „posługiwanie się hasłami do systemów informatycznych zgodnie z zasadami bezpieczeństwa, „korzystanie z poczty elektronicznej z zachowaniem zasad bezpieczeństwa". Sama nazwa kwalifikacji, która odnosi się do „pracowników instytucji finansowych" również sugeruje, że osoba, która ją uzyska będzie posiadać kompetencje do wykonywania czynności w każdej instytucji finansowej, tymczasem specyfika szerokiego sektora instytucji finansowych wymaga uwzględnienia charakteru działalności danego podmiotu już na etapie szkoleń pracowników. Wskazano, iż zróżnicowanie sektora instytucji finansowych jest na tyle wysokie, że nawet pośród jednej kategorii podmiotów lub też pomiędzy pracownikami jednej instytucji finansowej na różnych szczeblach zachodzą różnice, które uniemożliwiają zastosowanie zamkniętego zbioru kompetencji przewidzianego w założeniach kwalifikacji do działalności tak szerokiego katalogu podmiotów. Przykładem może być działalność agentów rozliczeniowych, gdzie praktyka rynkowa pokazuje, iż usługi świadczone przez tę kategorię dostawców mogą się diametralnie różnić, tj. opierać

się zarówno na rozliczaniu transakcji kartami płatniczymi w terminalach, rozliczaniu płatności internetowych, czy też działalności w zakresie świadczenia usług wypłat gotówki z bankomatów. Różnorodność usług świadczonych przez instytucje finansowe sprawia, że odmiennie kształtują się ich potrzeby w zakresie zapewnienia pracownikom odpowiednich kompetencji. **Kwalifikacja nie uwzględnia specjalistycznych uwarunkowań, jakimi kierują się instytucje finansowe przy doborze środków mających na celu podniesienie kompetencji pracowników (szkoleń, warsztatów, certyfikatów, konferencji etc.).** Umiejętności, które pracownicy mogą nabyć na skutek uzyskania kwalifikacji będącej przedmiotem wniosku, stanowią **jedynie fragment szerszego obszaru** obejmującego wykorzystanie narzędzi informatycznych do zachowania cyberbezpieczeństwa. W skrajnych przypadkach kompetencje te mogą okazać się niezgodne z rygorystycznymi standardami cyberbezpieczeństwa stosowanymi przez instytucje finansowe, przy czym niezgodność ze standardami należy rozumieć jako przyswojenie wzorców, które nie są wystarczające z punktu widzenia standardów cyberbezpieczeństwa najwyższego szczebla, do których przestrzegania instytucje finansowe są obowiązane. Poza powyższym, sprzeciw budzi także sformułowanie jakoby kwalifikacja miała stanowić swoisty „paszport cyberbezpieczeństwa" dla pracownika instytucji finansowej. Z uwagi na szeroki charakter kwalifikacji odnoszący się do wszystkich instytucji finansowych, powinna ona zostać ograniczona do wąskich, precyzyjnie określonych rodzajów działalności wykonywanych przez instytucje finansowe na najniższym szczeblu, tj. np. w zakresie obsługi klienta w fizycznych placówkach.	
Podpis osoby odpowiedzialnej za przygotowanie podsumowania	Dyrektor Departamentu Rozwoju Rynku Finansowego **Katarzyna Przewalska** /podpisano kwalifikowanym podpisem elektronicznym/
Data	01.03.2022 r.

Załączniki:

1. Formularze uzyskane w trakcie przeprowadzanych konsultacji wniosku.