MONITOR POLSKI

DZIENNIK URZĘDOWY RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 28 grudnia 2020 r.

Poz. 1208

OBWIESZCZENIE
MINISTRA CYFRYZACJI[1)]

z dnia 14 grudnia 2020 r.

w sprawie włączenia kwalifikacji rynkowej „Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych” do Zintegrowanego Systemu Kwalifikacji

Na podstawie art. 25 ust. 1 i 2 ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz. U. z 2020 r. poz. 226) ogłasza się w załączniku do niniejszego obwieszczenia informacje o włączeniu kwalifikacji rynkowej „Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych” do Zintegrowanego Systemu Kwalifikacji.

Minister Cyfryzacji: wz. *M. Zagórski*

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

Załącznik do obwieszczenia Ministra Cyfryzacji
z dnia 14 grudnia 2020 r. (poz. 1208)

INFORMACJE O WŁĄCZENIU KWALIFIKACJI RYNKOWEJ „KSZTAŁTOWANIE POLITYKI NIEZAWODNOŚCI I CYBERBEZPIECZEŃSTWA W PRZEMYŚLE W ZAKRESIE ZASOBÓW LUDZKICH I TECHNICZNYCH" DO ZINTEGROWANEGO SYSTEMU KWALIFIKACJI

1. Nazwa kwalifikacji rynkowej

Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych

2. Nazwa dokumentu potwierdzającego nadanie kwalifikacji rynkowej

Certyfikat

3. Okres ważności dokumentu potwierdzającego nadanie kwalifikacji rynkowej

Certyfikat jest ważny 3 lata. Przedłużenie certyfikatu następuje na podstawie dokumentów potwierdzających udział w min. jednym szkoleniu lub konferencji wskazanych przez IC w każdym roku w okresie ostatnich 3 lat. Dokumenty należy przedstawić przed upływem ważności certyfikatu

4. Poziom Polskiej Ramy Kwalifikacji przypisany do kwalifikacji rynkowej

6 poziom Polskiej Ramy Kwalifikacji

5. Efekty uczenia się wymagane dla kwalifikacji rynkowej

Syntetyczna charakterystyka efektów uczenia się Osoba posiadająca kwalifikacje „Kształtowanie polityki niezawodności i cyberbezpieczeństwa w przemyśle w zakresie zasobów ludzkich i technicznych" opracowuje plan zapobiegania zagrożeniom w organizacji. Posiada pogłębioną wiedzę dotyczącą niezawodności i cyberbezpieczeństwa oraz krajowych i europejskich regulacji prawnych w tych obszarach (m.in. zjawiska z obszaru wojny informacyjnej jak np. „fake news" oraz deepfake"). Posługuje się technikami analizy zagrożeń i analizy ryzyka. Wykorzystuje systemy IT i OT w procesach biznesowych i operacyjnych organizacji. Wyznacza obszary zagrożeń w organizacji, w tym prawdopodobieństwo wystąpienia „efektu domino". Uzasadnia wybór poziomu zagrożenia, jak również ocenia i weryfikuje szacunki nakładów na cyberbezpieczeństwo i niezawodność. Zarządza zespołem analiz incydentów IT/OT. Prowadzi politykę organizacji po skutecznym cyberataku. Tworzy scenariusze działań biznesowych i strategię upubliczniania informacji po skutecznym cyberataku. Analizuje skutki strat fizycznych lub wizerunkowych oraz przygotowuje scenariusze minimalizacji strat. Analizuje politykę bezpieczeństwa zasobów ludzkich w kontekście najnowszych osiągnięć dotyczących powyższego obszaru.

Zestaw 1. Posługiwanie się wiedzą z zakresu niezawodności i cyberbezpieczeństwa w zakresie zasobów ludzkich i technicznych	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Posługuje się pojęciami normatywnymi z obszaru niezawodności i cyberbezpieczeństwa	– omawia pojęcia niezawodności i cyberbezpieczeństwa; – omawia pojęcie cyklu życia (projekt, realizacja, eksploatacja, utylizacja) obiektu w kontekście sprzętu i oprogramowania; – określa typowe zagrożenia pochodzące z cyberprzestrzeni np. ransomware, trojany, wirusy, robaki, bots, DDoS (Distributed Denial of Service).
02. Charakteryzuje normatywne techniki analityczne	– omawia techniki analityczne (np. wstępna analiza zagrożeń (PHA), badania zagrożeń i zdolności do działania (HAZOP), procedura analizy rodzajów i skutków uszkodzeń (FMEA)); – omawia definicję „efektu domino”; – podaje przykład „efektu domino” w przedsiębiorstwie; – omawia zasady tworzenia i zastosowanie matrycy ryzyk.
03. Charakteryzuje zagadnienia związane z kształtowaniem polityki bezpieczeństwa zasobów ludzkich	– analizuje politykę bezpieczeństwa zasobów ludzkich w kontekście najnowszych osiągnięć dotyczących powyższego obszaru; – omawia elementy planu walki z „fake news” i „deep news”; – podaje przykłady zastosowania planu walki z „fake news” i „deep news”; – omawia sposoby postępowania w przypadku ujawnienia cybermolestowania i cyberstalkingu; – omawia sposoby postępowania w przypadku wystąpienia cyberprzemocy, np. wobec kobiet.
04. Charakteryzuje zagadnienia prawne związane z niezawodnością i cyberbezpieczeństwem	– wymienia nazwy regulacji odnoszące się do krajowego systemu cyberbezpieczeństwa; – omawia przepisy regulujące krajowy system cyberbezpieczeństwa; – omawia europejskie normy dotyczące systemów zarządzania ciągłością działania i bezpieczeństwa; – omawia zasady tworzenia strategii i polityki niezawodności i cyberbezpieczeństwa; – omawia zasady pracy zespołu ds. analiz incydentów IT/OT.

Zestaw 2. Opracowanie planu zapobiegania zagrożeniom w zakresie zasobów ludzkich i technicznych w organizacji	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Analizuje zagrożenia i ryzyka pod kątem niezawodności i cyberbezpieczeństwa	– identyfikuje strefy zagrożeń newralgiczne dla niezawodności i ciągłości działania na określonym obszarze/obiekcie; – ocenia ryzyko na określonym obszarze, posługując się matrycą ryzyka; – identyfikuje potencjalne społeczne cyberzagrożenia w miejscu pracy (np. cyberstalking, cybermolestowanie); – podaje przykłady rozwiązań i środków zapobiegawczych w obszarze społecznych cyberzagrożeń w miejscu pracy.

02. Przygotowuje plan zapobiegania zagrożeniom w zakresie zasobów ludzkich i technicznych w organizacji	– formułuje wnioski i zalecenia dla organizacji na podstawie analizy zapisów w rejestrze incydentów; – sporządza plan zapobiegania zagrożeniom (uwzględniający m.in. opis sytuacji, możliwe rozwiązania i scenariusze działania z uwzględnieniem obowiązujących przepisów prawa).
03. Zarządza pracą zespołu IT/OT	– określa zadania członków zespołu; – określa czas i kolejność realizacji zadań; – wskazuje kompetencje członków zespołu niezbędne do realizacji zadań; – określa sposoby monitorowania realizacji zadań; – wskazuje działy, z którymi musi podjąć współpracę w celu realizacji zadań.

Zestaw 3. Postępowanie po skutecznym cyberataku w zakresie zasobów ludzkich i technicznych w organizacji	
Poszczególne efekty uczenia się	**Kryteria weryfikacji ich osiągnięcia**
01. Wykonuje czynności wstępne po skutecznym cyberataku	– analizuje dostępne źródła informacji o cyberataku (w tym prasę i media społecznościowe); – sporządza wstępną informację dotyczącą szacunkowych strat i skutków wewnętrznych i zewnętrznych, jakie mogą wystąpić po cyberataku.
02. Prowadzi działania osłabiające skutki cyberataku	– tworzy scenariusze działań biznesowych na podstawie pozyskanych informacji (np. z prasy, od dostawców i odbiorców, partnerów biznesowych); – tworzy scenariusze upublicznienia informacji o skutecznym cyberataku; – wskazuje optymalny scenariusz dla danej sytuacji.
03. Analizuje koszty możliwych strat	– rozróżnia rodzaje strat; – sporządza wykaz strat fizycznych lub wizerunkowych oraz omawia ich skutki; – tworzy scenariusze minimalizacji strat.

6. Wymagania dotyczące walidacji i podmiotów przeprowadzających walidację

1. Weryfikacja.

Weryfikacja efektów uczenia się składa się z dwóch części: teoretycznej i praktycznej.

1.1. Metody.

Na etapie weryfikacji stosowane są wyłącznie następujące metody: Część pierwsza: test teoretyczny, Część druga: analiza dowodów i deklaracji, obserwacja w warunkach symulowanych połączona z rozmową z komisją. W części pierwszej do zestawu efektów uczenia się 01 stosuje się wyłącznie test teoretyczny. W części drugiej do zestawu efektów uczenia się 02 i 03 stosuje się wyłącznie: analizę dowodów i deklaracji w postaci portfolio oraz obserwację w warunkach symulowanych połączoną z rozmową z komisją. Metodą analizy dowodów i deklaracji weryfikowana jest umiejętność „Analizuje opracowany plan monitorowania i zapobiegania w zakresie zasobów ludzkich” z zestawu efektów uczenia się 02.

1.2. Zasoby kadrowe.

Komisja walidacyjna składa się z co najmniej trzech członków w tym przewodniczącego.

Przewodniczący komisji walidacyjnej musi posiadać:

– certyfikat CRP (Certified Reliability Professional) bądź inny z listy rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
– stopień naukowy (8 PRK);
– min. 3 lata udokumentowanego doświadczenia w przeprowadzaniu egzaminów zdobytego w okresie ostatnich 5 lat.

Każdy z pozostałych członków komisji walidacyjnej musi spełniać następujące warunki:

– kwalifikacja pełna z 7 PRK;
– min. rok doświadczenia w przeprowadzaniu egzaminów. Ponadto co najmniej jeden z członków komisji walidacyjnej musi posiadać certyfikat szkolenia międzynarodowego w ośrodku zajmującym się cyberbezpieczeństwem przemysłowym.

1.3. Sposób organizacji walidacji oraz warunki organizacyjne i materialne.

Potwierdzenie efektów uczenia się w części pierwszej pozwala na dopuszczenie do części drugiej weryfikacji. Pozytywny wynik części pierwszej jest ważny przez 3 miesiące od daty jej zaliczenia. Instytucja certyfikująca musi zapewnić: laboratorium symulujące sieć przemysłową (min. 20 komputerów połączonych w sieć imitującą instalację przemysłową klasy SCADA lub DCS); narzędzia programistyczne do obliczeń niezawodnościowych 2 lub 3 parametrycznych.

2. Identyfikowanie i dokumentowanie.

Nie określa się wymogów dla etapu identyfikowania i dokumentowania efektów uczenia się.

7. Termin dokonywania przeglądu kwalifikacji

Nie rzadziej niż raz na 10 lat