ST3 - Specyfikacja kompetencji, kryteriów i metodyka oceny dla profilu ACE-CRL (osoby zarządzające podmiotami KSC)

[NASK-PIB DOKUMENT NR: ST3/1.2]

Egzemplarz dla Klienta (wyciąg z egzemplarza nadzorowanego)

Podpisany elektronicznie przez
NASK - PIB
30.06.2025
14:51:59 +02'00'

NASK-PIB
ul. Kolska 12
01–045 Warszawa

standard@nask.pl
+48 22 380 82 00 / 01

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

www.certyfikacja.nask.pl

Spis treści

1. Cel i zakres dokumentu

1 Celem specyfikacji jest zapewnienie prawidłowego, rzetelnego i powtarzalnego postępowania podczas procesu oceny kompetencji w ramach profilu certyfikacji osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa (Profil ACE-CRL).

2 Niniejszy dokument określa szczegółowe specyfikacje, które wraz z Programem Certyfikacji SEK-CYBER stanowią wymagania dla profilu eksperckiego ACE-CRL – kompetencje w zakresie cyberbezpieczeństwa osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa (KSC).

3 Specyfikacja dotyczy kryteriów i metodyki oceny egzaminu pisemnego oraz spełniania wymagań wstępnych i oceny oświadczeń kandydata.

2. Dokumenty powiązane

Dyrektywa Parlamentu Europejskiego I Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (NIS 2).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r poz. 913, 1703 z późn. zm.).

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).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000 z późń. zm.).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2005 nr 64 poz. 565 z późn. zm.).

Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 poz. 773 z późń. zm.).

Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (CSA).

Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (Dz.U. z 2023 r. poz. 122 z późń. zm.).

Ustawa Prawo bankowe z dnia 29 sierpnia 1997 (Dz.U. z 2021 r. poz. 2439 z późń. zm.).

Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 r. (Dz.U. z 2022 r. poz. 1648 z późń. zm.).

Ustawa Prawo energetyczne z dnia 10 kwietnia 1997 r. (Dz.U. z 2022 r. poz. 1385 z późń. zm.).

Ustawa Prawo pocztowe z dnia 23 listopada 2012 r. (Dz.U. z 2023 r. poz. 1640 z późń. zm.).

Ustawa o systemie ubezpieczeń społecznych z dnia 13 października 1998 r. (Dz.U. z 2023 r. poz. 1230 z późń. zm.).

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. z 2023 r. poz. 1703 z późń. zm.).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 nr 88 poz. 553 z późń. zm.).

Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz.U. 1974 nr 24 poz. 141 z późń. zm.).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228 z późń. zm.).

3. Definicje

4 Definicje są określone w Programie Certyfikacji Kompetencji Cyberbezpieczeństwa SEK-CYBER.

4. Zakres certyfikacji

5 Certyfikacja kompetencji w zakresie profilu eksperckiego ACE-CRL skierowana jest do osób zaangażowanych w zarządzanie podmiotami KSC, w tym w szczególności: członków zarządów, dyrektorów zarządzających, członków rad nadzorczych, dyrektorów generalnych, dyrektorów pionów, departamentów, biur, członków organu zarządzającego w podmiotach administracji publicznej, sekretarzy w jednostkach samorządu terytorialnego.

6 Pełna nazwa kwalifikacji potwierdzonych certyfikatem w Programie Certyfikacji Kompetencji Cyberbezpieczeństwa SEK-Cyber o profilu ACE-CRL brzmi: Attested Cybersecurity Expert – Cyber Resilience Leadership.

4.1 Opis zakresu zastosowania i zadań osoby posiadającej certyfikat ACE-CRL

4.1.1 Opis zakresu zastosowania certyfikatu

7 Zakłada się, że osoba posiadająca certyfikat o profilu ACE-CRL, potwierdzający kompetencje w zakresie cyberbezpieczeństwa osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa (KSC), ma wiedzę i umiejętności oraz jest odpowiedzialna za:

a) budowanie odporności podmiotu Krajowego Systemu Cyberbezpieczeństwa;

b) zapewnienie zgodności z wymaganiami formalno-prawnymi;

c) motywowanie do wdrażania i nadzorowanie stosowania dobrych praktyk dotyczących zarządzania podmiotami KSC;

d) nadzór nad systemem ciągłości działania podmiotu KSC ze szczególnym uwzględnieniem systemów informatyczno-komunikacyjnych;

e) nadzór nad system zarządzania bezpieczeństwem informacji;

f) nadzór nad zarządzaniem ryzykiem w obszarze cyberbezpieczeństwa;

g) organizowanie i nadzór nad komunikacją w sytuacjach kryzysowych.

8 Uzyskany certyfikat jest potwierdzeniem merytorycznego przygotowania do zarządzania w obszarze cyberbezpieczeństwa w podmiotach objętych przepisami Ustawy o krajowym systemie cyberbezpieczeństwa.

4.1.2 Opis zadań

9 Osoba posiadająca certyfikat ACE-CRL potwierdzający kompetencje w zakresie cyberbezpieczeństwa osób zarządzających podmiotami Krajowego Systemu Cyberbezpieczeństwa (KSC) wykonuje następujące zadania:

10

a) zapewnia budowanie odporności podmiotu KSC na zagrożenia z zakresu cyberbezpieczeństwa;

b) zapewnia ciągłość działania systemów teleinformatycznych;

c) nadzoruje wdrażanie wymagań formalno-prawnych dotyczących podmiotu KSC (wynikających z przepisów krajowych i europejskich) oraz dobrych praktyk;

d) nadzoruje proces identyfikacji zagrożeń i ochrony przed atakami cybernetycznymi;

e) nadzoruje proces zarządzania bezpieczeństwem informacji;

f) organizuje proces zgłaszania incydentów cyberbezpieczeństwa;

g) wdraża procedury komunikacji kryzysowej;

h) wdraża działania prewencyjne zwiększające cyberbezpieczeństwo;

i) wdraża środki zarządzania ryzykiem w cyberbezpieczeństwie;

j) zatwierdza wyniki szacowania ryzyka w obszarze cyberbezpieczeństwa.

4.2 Tematyka objęta egzaminem w profilu ACE-CRL i opis kompetencji

11 Osoba certyfikowana w profilu ACE-CRL posiada wiedzę z zakresu formalno-prawnych regulacji krajowych i Unii Europejskiej z obszaru cyberbezpieczeństwa, w tym w szczególności:

a) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

b) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

c) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

d) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2);

e) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

f) 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);

g) PN-EN ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

h) PN-EN ISO 22301 Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania.

12 Dodatkowo wskazana jest znajomość następujących aktów prawnych:

a) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie);

b) Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r.;

c) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny;

d) Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej;

e) Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne;

f) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

g) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.

13 Osoba certyfikowana w ACE-CRL posiada kompetencje do sprawowania nadzoru i koordynacji zadań w obszarze cyberbezpieczeństwa, w tym identyfikacji i reakcji na zagrożenia. Wie, jak zorganizować i nadzorować proces zgłaszania incydentów, zapewnić proces ciągłości działania sieci i systemów informacyjno-komunikacyjnych oraz nadzorować proces zarządzania bezpieczeństwem informacji.

14 Ponadto osoba certyfikowana posiada wiedzę w zakresie tworzenia strategii komunikacji kryzysowej oraz potrafi rozpoznać i zweryfikować informacje dotyczące ryzyka w obszarze cyberbezpieczeństwa. Zna metody i techniki związane z szacowaniem ryzyka.

15 Osoba certyfikowana zna dobre praktyki w zakresie zapewnienia bezpieczeństwa teleinformatycznego i sposoby ich wdrażania.

16 Weryfikacja kompetencji następuje poprzez ocenę spełnienia przez kandydata wymagań wstępnych i przeprowadzenie egzaminu.

5. Zasady certyfikacji

5.1 Warunki ubiegania się o certyfikację

5.1.1 Wymagania wstępne dla profilu ACE-CRL

17 Kandydat do certyfikacji powinien spełniać następujące warunki:

a) wykształcenie wyższe;

b) co najmniej 5-letni okres zatrudnienia na podstawie umowy o pracę, powołania, wyboru, mianowania, spółdzielczej umowy o pracę lub świadczenia usług na podstawie innej umowy lub wykonywania działalności gospodarczej na własny rachunek;

c) co najmniej 3-letnie doświadczenie na stanowiskach kierowniczych lub samodzielnych albo wynikające z prowadzenia działalności gospodarczej na własny rachunek albo ukończone studia podyplomowe na kierunku zarządzanie i co najmniej 2-letni staż pracy na stanowiskach jak określono powyżej;

Uwaga 1: Jako równorzędne dla ukończenia studiów podyplomowych na kierunku zarządzanie są traktowane studia Master Bussines of Administration, zarządzanie projektami, zarządzanie w administracji publicznej, zarządzanie projektami informatycznymi.

d) co najmniej roczne doświadczenie na stanowisku kierowniczym w podmiocie KSC: członek zarządu, członek rady nadzorczej, dyrektor generalny, dyrektor pionu, departamentu, biura, kierujący lub pełniący funkcję sekretarza w jednostce samorządu terytorialnego;

e) brak skazania prawomocnym wyrokiem sądu za przestępstwo umyślne.

5.2 Ocena

5.2.1 Egzamin

18 Egzamin dla profilu eksperckiego ACE-CRL jest przeprowadzany w formie pisemnej i trwa 80 minut. Składa się z 30 pytań testowych jednokrotnego lub wielokrotnego wyboru i 7 pytań otwartych, na które odpowiedź jest udzielana w formie opisowej. Egzamin zawiera pytania z każdego niżej wymienionego modułu:

- Wymaganie prawne dotyczące podmiotu KSC
- Cyberbezpieczeństwo - podstawy
- Budowanie odporności podmiotu KSC
- Ciągłość działania systemów teleinformatycznych
- Zarządzanie bezpieczeństwem informacji
- Komunikacja kryzysowa
- Szacowanie ryzyka w obszarze cyberbezpieczeństwa.

19 Można uzyskać maksymalnie 44 punkty tj. 1 punkt za prawidłową odpowiedź z części testowej oraz 2 punkty za każdą pełną prawidłową odpowiedź z części pytań opisowych (w przypadku częściowej odpowiedzi można uzyskać 1 punkt za pytanie otwarte).

20 Aby zdać egzamin, kandydat powinien uzyskać nie mniej niż 70% prawidłowych odpowiedzi (31 punktów).

5.3 Decyzja w sprawie certyfikacji

21 Zgodnie z programem certyfikacji SEK-CYBER.

5.4 Ważność wydawanych dokumentów

22 Certyfikat w programie SEK-Cyber o profilu ACE-CRL jest ważny 2 lata. Data wydania i data ważności podane są na certyfikacie.

5.5 Ponowna certyfikacja

23 Możliwość przedłużenia na kolejne 2 lata ważności certyfikatu jest warunkowana wymaganiami określonymi w programie SEK-Cyber (złożenie wniosku, opłata) i spełnieniem przedstawionych poniżej wymogów kształcenia ustawicznego i praktyki zawodowej:

a) Odbycie szkolenia lub szkoleń o tematyce określonej poniżej (w co najmniej w jednym z modułów) w wymiarze łącznym co najmniej 5 godzin rocznie lub 10 godzin w ciągu dwóch lat:

- Wymaganie prawne dotyczące podmiotu KSC
- Cyberbezpieczeństwo - podstawy
- Budowanie odporności podmiotu KSC
- Ciągłość działania systemów teleinformatycznych
- Zarządzanie bezpieczeństwem informacji
- Komunikacja kryzysowa
- Szacowanie ryzyka w obszarze cyberbezpieczeństwa

b) Praktyka zawodowa na stanowisku/stanowiskach związanym z wykonywaniem zadań w ramach podmiotu KSC określonych w sekcji 4.1.2 w okresie co najmniej pół roku, liczonego dla pełnego etatu umowy o pracę.

6. Kompetencje

24 Kompetencje osoby certyfikowanej wynikają z przeprowadzanej oceny indywidualnej uwzględniającej wiedzę, doświadczenie oraz umiejętności.

25 Tabela 2. zawiera spis wymaganych kompetencji określonych dla profilu ACE-CRL.

Lp.	Kategoria	Kompetencja / wymaganie
1	wiedza	Znajomość kluczowych pojęć z zakresu ciągłości działania.
2	wiedza	Znajomość struktury oraz wymagań dotyczących wdrożenia i utrzymania systemu zarządzania ciągłością działania.
3	wiedza	Znajomość rodzajów dostępności systemów i usług IT.
4	wiedza	Znajomość metod, sposobów oraz celów zarządzania ryzykiem i oceny ryzyka.
5	wiedza	Znajomość metod zapewniania ciągłości działania.
6	wiedza	Znajomość zapisów prawnych (w odpowiednich ustawach, rozporządzeniach, dyrektywach lub normach) odnoszących się do ciągłości działania, ciągłości działania usługi kluczowej oraz systemu informacyjnego wspierającego realizację usługi kluczowej.

7	wiedza	Znajomość definicji krajowego systemu cyberbezpieczeństwa.
8	wiedza	Znajomość znaczenia procesów głównych, zarządczych i pomocniczych.
9	wiedza	Znajomość cyklu PDCA oraz jego poszczególnych elementów.
10	wiedza	Znajomość obowiązków najwyższego kierownictwa w kontekście SZCD.
11	wiedza	Znajomość kluczowych zagadnień związanych z analizą wpływu biznesowego (BIA).
12	wiedza	Znajomość grup podmiotów KSC określonych w ustawie KSC.
13	wiedza	Znajomość podstawowych obowiązków podmiotu publicznego określonych w odpowiednich ustawach, rozporządzeniach, dyrektywach lub normach.
14	wiedza	Znajomość procedury obsługi i zgłaszania incydentu.
15	wiedza	Znajomość definicji incydentu, incydentu w podmiocie publicznym i incydentu krytycznego zdefiniowanych w ustawie KSC.
16	wiedza	Znajomość procedury oraz poszczególnych kroków zarządzania incydentem w podmiocie publicznym.
17	wiedza	Znajomość podstawowych pojęć i zagadnień z zakresu cyberbezpieczeństwa i jego wpływu na organizację.
18	wiedza	Znajomość zasad, metod i sposobów ochrony prywatności w cyberprzestrzeni.
19	wiedza	Znajomość cyberzagrożeń i podatności na ataki.
20	wiedza	Znajomość operacyjnych skutków naruszeń cyberbezpieczeństwa.
21	wiedza	Znajomość i rozumienie metod stosowanych przez cyberprzestępców.
22	wiedza	Znajomość metod i sposobów zapewnienia wysokiego poziomu cyberbezpieczeństwa.
23	wiedza	Znajomość podstawowych zasad postępowania z urządzeniami oraz w internecie.
24	wiedza	Znajomość zasad tworzenia silnych i bezpiecznych haseł.
25	wiedza	Znajomość obowiązków kierownika podmiotu kluczowego określonych w ustawie KSC2 i dyrektywie NIS2.
26	wiedza	Znajomość kluczowych zagadnień związanych z ryzykiem.
27	wiedza	Znajomość zapisów (w odpowiednich ustawach, rozporządzeniach, dyrektywach, normach lub standardach) odnoszących się do zarządzania ryzykiem.
28	wiedza	Znajomość schematu zarządzania ryzykiem.
29	wiedza	Znajomość klasyfikacji w zastosowaniu do ochrony informacji.
30	wiedza	Znajomość ról w zarządzaniu ryzykiem.
31	wiedza	Znajomość podprocesów i wariantów analizy ryzyka.
32	wiedza	Znajomość podstawowych metod szacowania ryzyka.
33	wiedza	Znajomość metod minimalizacji ryzyka.
34	wiedza	Znajomość zabezpieczeń tworzących system ochrony informacji oraz zasad ich budowy.
35	wiedza	Znajomość podstawowych reguł organizacyjnych wspierających zabezpieczenia techniczne.
36	wiedza	Znajomość definicji akceptacji ryzyka szczątkowego.
37	wiedza	Znajomość podstawowych zadań w administrowaniu ryzykiem.
38	wiedza	Znajomość kluczowych wskaźników ryzyka.

39	wiedza	Znajomość wybranych zapisów aktualnie obowiązujących aktów prawnych (ustaw, rozporządzeń, dyrektyw, norm) związanych z cyberbezpieczeństwem.
40	wiedza	Znajomość schematu krajowego systemu cyberbezpieczeństwa.
41	wiedza	Znajomość podstawowych obowiązków operatora usługi kluczowej określonych w odpowiednich ustawach, rozporządzeniach, dyrektywach lub normach.
42	wiedza	Znajomość środków technicznych i organizacyjnych oraz środków zapobiegających i ograniczających wpływ incydentów na ciągłość działania usługi kluczowej.
43	wiedza	Znajomość zakresu podmiotów, które są objęte regulacjami dyrektywy NIS2 oraz KSC.
44	wiedza	Znajomość obowiązków podmiotów kluczowych i ważnych.
45	wiedza	Znajomość środków minimalnych, które muszą być stosowane przez podmioty kluczowe i ważne.
46	wiedza	Znajomość uprawnień i obowiązków organów nadzorczych.
47	wiedza	Znajomość procesu zgłaszania incydentów cyberbezpieczeństwa.
48	wiedza	Znajomość kluczowych pojęć i zasad określonych w ustawie o ochronie danych osobowych i RODO.
49	wiedza	Znajomość metod ochrony informacji i regulacji z nimi związanych.
50	wiedza	Znajomość obowiązujących Krajowych Ram Interoperacyjności.
51	wiedza	Znajomość podstawowych przepisów określonych w akcie o usługach cyfrowych, akcie o rynkach cyfrowych i akcie o sztucznej inteligencji.
52	wiedza	Znajomość kluczowych pojęć z zakresu cyberkryzysu.
53	wiedza	Znajomość aktualnych rekomendacji ENISA w zakresie cyberbezpieczeństwa.
54	wiedza	Znajomość podstawowych zadań systemu zarządzania kryzysem komunikacyjnym.
55	wiedza	Znajomość metod prewencji oraz procesu zarządzania cyberkryzysem.
56	wiedza	Znajomość zasad właściwej i efektywnej komunikacji w czasie kryzysu.
57	wiedza	Znajomość zapisów odnoszących się do SZBI w odpowiednich ustawach, rozporządzeniach i normach.
58	wiedza	Znajomość struktury oraz wymagań dotyczących wdrożenia i utrzymania systemu zarządzania bezpieczeństwem informacji.
59	wiedza	Znajomość głównych obszarów normy ISO 27001.
60	wiedza	Znajomość ról i zadań kierownictwa określonych w normie ISO 27001.
61	wiedza	Znajomość metod zapewnienia skuteczności SZBI.
62	wiedza	Znajomość metod zapewniania świadomości w kwestii bezpieczeństwa wśród kierownictwa i personelu.
63	wiedza	Znajomość zasad inwentaryzacji aktywów i ich konfiguracji.
64	umiejętność	Umiejętność wskazania korzyści płynących z wdrożenia systemu zarządzania ciągłością działania.
65	umiejętność	Umiejętność interpretacji zapisów prawnych związanych z obowiązkiem prowadzenia SZCD.
66	umiejętność	Umiejętność wskazania proporcjonalnych środków technicznych, operacyjnych i organizacyjnych mających na celu zarządzanie ryzykiem dla bezpieczeństwa sieci i systemów informatycznych.

67	umiejętność	Umiejętność rozróżnienia sektorów kluczowych i ważnych, określonych w dyrektywie NIS2.
68	umiejętność	Umiejętność identyfikacji zainteresowanych stron zewnętrznych i wewnętrznych istotnych dla Systemu Zarządzania Ciągłością Działania w organizacji.
69	umiejętność	Umiejętność formułowania prostych strategii i rozwiązań w zakresie ciągłości działania.
70	umiejętność	Umiejętność wskazania aktów prawnych zawierających zapisy związane z budowaniem odporności podmiotu KSC.
71	umiejętność	Umiejętność tworzenia zasad zgodnych z ustalonymi celami w zakresie bezpieczeństwa systemu.
72	umiejętność	Znajomość metod uwierzytelniania wieloskładnikowego, autoryzacji i kontroli dostępu.
73	umiejętność	Znajomość procesów zarządzania ryzykiem.
74	umiejętność	Umiejętność opisywania i prezentacji ryzyka.
75	umiejętność	Umiejętność rozróżnienia różnych rodzajów podatności.
76	umiejętność	Umiejętność identyfikacji ryzyka, podatności i zagrożeń.
77	umiejętność	Umiejętność wskazania organów właściwych do spraw cyberbezpieczeństwa dla sektorów kluczowych i ważnych.
78	umiejętność	Umiejętność wskazania działań niedozwolonych podlegających odpowiedzialności karnej, cywilnej, zawodowej lub administracyjnej.
79	umiejętność	Umiejętność wskazania podmiotów zobowiązanych do wdrożenia i utrzymywania systemu zarządzania bezpieczeństwem informacji (SZBI).
80	umiejętność	Umiejętność kierowania zespołem ekspertów ds. bezpieczeństwa IT.
81	umiejętność	Umiejętność interpretowania i stosowania przepisów prawa, regulacji, polityk i wytycznych istotnych dla cyberbezpieczeństwa organizacji.
82	umiejętność	Umiejętność komunikowania się z osobami na wszystkich szczeblach kierowniczych.
83	umiejętność	Umiejętność określenia zasobów niezbędnych do realizacji celów i zadań związanych z bezpieczeństwem technologii informacyjnej.
84	umiejętność	Umiejętność definiowania i/lub wdrażania polityk i procedur w celu zapewnienia odpowiedniej ochrony infrastruktury o kluczowym znaczeniu.
85	umiejętność	Umiejętność oceny jakości cyberberpieczeństwa w organizacji.

Tabela 2. Spis wymaganych kompetencji

7. Metodyka oceny

7.1 Wymagania wstępne

26 Wnioskujący o certyfikację w Jednostce Certyfikującej Osoby NASK-PIB powinien przedstawić dowody na spełnienie wymagań wstępnych poprzez załączenie do wniosku:

a) kopii dyplomu ukończenia studiów wyższych I lub II stopnia;

b) kopii umowy o pracę, spółdzielczej umowy o pracę, świadectwa pracy, zaświadczenia o prowadzeniu własnej działalności gospodarczej lub innego dokumentu poświadczającego wymagane doświadczenie;

c) zakresu obowiązków i/lub kopii dyplomu ukończenia studiów podyplomowych na kierunku zarządzanie, studia Master Bussines of Administration, zarządzanie projektami, zarządzanie w administracji publicznej, zarządzanie projektami informatycznymi;

d) kopii umowy o pracę lub kopii dokumentu powołania/mianowania na stanowisko w podmiocie KSC;

e) poprzez złożenie oświadczenia o niekaralności (we wniosku o certyfikację).

7.2 Egzamin

27 Egzamin służy weryfikacji kompetencji, a jego pozytywne ukończenie jest niezbędne do uzyskania certyfikatu. Egzamin przeprowadzany jest przez bezstronny zespół Egzaminatorów. Podczas egzaminu obecna może być również osoba nadzorująca egzamin.

28 Egzamin jest przeprowadzany zdalnie, za pomocą środków teleinformatycznych służących do połączeń audio i video, w formie pisemnej i trwa 80 minut. Składa się z dwóch bloków:

a) 30 pytań jednokrotnego lub wielokrotnego wyboru – 1 punkt za prawidłową odpowiedź;

b) 7 pytań otwartych – wymagających odpowiedzi w formie opisowej – 2 punkty za prawidłową odpowiedź.

7.2.1 Pytania zamknięte

29 Pytanie testowe jednokrotnego wyboru z zaznaczoną jedną prawidłową odpowiedzią egzaminator ocenia jako poprawne i przyznaje 1 punkt.

30 Pytanie testowe jednokrotnego wyboru z niezaznaczoną odpowiedzią egzaminator ocenia jako błędne i przyznaje 0 punktów.

31 Pytanie testowe jednokrotnego wyboru z zaznaczoną więcej niż jedną odpowiedzią egzaminator ocenia jako błędne i przyznaje 0 punktów.

32 Pytanie testowe wielokrotnego wyboru z zaznaczonymi wszystkimi prawidłowymi odpowiedziami egzaminator ocenia jako poprawne i przyznaje 1 punkt.

33 Pytanie testowe wielokrotnego wyboru z zaznaczonymi wszystkimi prawidłowymi odpowiedziami i jedną lub więcej nieprawidłowymi egzaminator ocenia jako błędne i przyznaje 0 punktów.

34 Pytanie testowe wielokrotnego wyboru z zaznaczonymi nie wszystkimi prawidłowymi odpowiedziami egzaminator ocenia jako błędne i przyznaje 0 punktów.

35 Uzyskanie pozytywnej oceny możliwe jest, gdy z egzaminu pisemnego kandydat uzyska minimum 70% punktów (31 na 44 możliwych do zdobycia).

7.2.2 Pytania otwarte

36 Egzaminator może przyznać 2 punkty za prawidłową odpowiedź – ma również możliwość przyznania 1 punktu, jeżeli odpowiedź jest niepełna. Ocenie egzaminatora podlega:

a) poprawność merytoryczna odpowiedzi – przede wszystkim odniesienia w odpowiedzi do przepisów prawnych, norm, procedur i dobrych praktyk w zakresie zagadnienia;

b) stosowanie nomenklatury zagadnienia i profesjonalnego osądu;

c) spójność odpowiedzi.

Tabela 2. Progi egzaminacyjne

Progi wymagane do uzyskania wyniku pozytywnego	Część pisemna
Punkty	31/44
Procenty	70%