Spis treści

1. Cel i zakres dokumentu

Niniejszy dokument zawiera Opis Przedmiotu Zapytania dotyczącego przeprowadzenia audytów, stanowiących wymagania ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) z dnia 5 lipca 2018 r. art. 15 ust.1, u **dwóch** operatorów usług kluczowych. EITE oczekuje przedstawienia **czterech niezależnych ofert** na przeprowadzenie audytów w czterech spółkach (określanych dalej jako **Podmiot A, Podmiot B, Podmiot C i Podmiot D**) w oparciu o niżej przedstawione informacje i kryteria. EITE **dopuszcza** przedstawienie oferty **tylko dla jednego z podmiotów**. W ramach oferty dla jednego podmiotu oczekujemy **podania oddzielnej wyceny** dla **wariantu podstawowego** i **opcjonalnego** (opcjonalny tylko w przypadku podmiotu C). W przypadku braku możliwości realizacji audytu we wskazanych w poniższych harmonogramach terminach (kluczowym jest termin dostarczenia uzgodnionego Raportu), EITE oczekuje **od Wykonawcy podania swoich propozycji terminów** z wyraźnym zaznaczeniem braku możliwości dotrzymania kluczowego terminu.

2. Zakres zapytania dla Podmiotu A

2.1. Podstawowe informacje o podmiocie, którego dotyczy audyt

Podmiot, którego dotyczy audyt w ramach niniejszego Opisu Przedmiotu Zapytania jest spółka Grupy Energa odpowiedzialna za **wytwarzanie ciepła**, która została zakwalifikowana jako Operator Usługi Kluczowej (zwany dalej: **OUK**) w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa.

OUK posiada podpisaną umowę na świadczenie usług z zakresu cyberbezpieczeństwa ze spółką informatyczną z Grupy Energa (dalej: Podmiot Świadczący Usługi z obszaru cyberbezpieczeństwa – **PŚU; EITE)**, która posiada certyfikat ISO 27001 oraz w ramach której działa zespół CERT Energa.

OUK zatrudnia ok. 187 pracowników, w tym 3 osoby z obszaru IT / OT utrzymujące systemy informacyjne oraz posiada lokalizacje w trzech miejscowościach.

OUK zidentyfikował 2 główne systemy informacyjne z obszaru OT, które mają bezpośredni wpływ na świadczenie Usługi Kluczowej (są nimi systemy klasy SCADA/PLC), oraz jeden system z obszaru IT (system klasy ERP), który nie ma bezpośredniego wpływu na świadczenie Usługi Kluczowej.

Obszar OT zarządzany jest przez pracowników **OUK**. Większość infrastruktury oraz systemów teleinformatycznych z obszaru IT (w tym wymieniony w poprzednim akapicie systemie klasy ERP) dostarczana jest do **OUK** na podstawie umów z **PŚU (EITE).**

2.2. Wymagania EITE oraz zakres audytu

Przedmiotem zapytania jest przeprowadzenie audytu bezpieczeństwa stanowiącego wymagania ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. art. 15 ust.1 w spółce Grupy Energa świadczącej usługi **wytwarzania ciepła** zakwalifikowanej jako Operator Usługi Kluczowej.

I. **<u>Wariant podstawowy:</u>**

Zakres audytu:

- Audyt bezpieczeństwa 3 systemów informacyjnych (2 - OT, 1 - IT), które zostały zidentyfikowane przez **OUK** jako wykorzystywane do świadczenia usługi kluczowej:
  - System SCADA dla Centrum Nadzoru i sterowania iFix firmy GE (OT);
  - System SCADA dla bloku grzewczego iFix firmy GE (OT);

  - System klasy ERP Egeria firmy Comarch (IT).
- Audyt bezpieczeństwa innych systemów informacyjnych mogących mieć wpływ na świadczenie Usługi Kluczowej, które zostaną zidentyfikowane podczas prowadzonego audytu,
- Przeprowadzenie audytu w pełnym zakresie dotyczącym spełnienia wymagań wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. oraz wymagań zawartych w Rozporządzeniach do przedmiotowej ustawy,
- Przeprowadzenie audytu w dwóch lokalizacjach **OUK** – Elbląg, Kalisz
- Przeprowadzenie audytu w lokalizacji **PŚU (EITE)** – Płock.
- Przeprowadzenie audytu zgodnie z szablonem stanowiącym Załącznik nr 3 do RFI,
- Uwzględnienie zaleceń Ministerstwa Aktywów Państwowych, przedstawionych w grudniu 2019 poszczególnym operatorom usług kluczowych, takich jak:
  - Przeprowadzenie audytu zgodnie z zapisem art. 15 ust. 2 pkt 2 lit a Ustawy o KSC;
  - Metodyka wykonania audytu powinna bazować na jednej z norm: ISO/IEC 27001, ISA/IEC 62443;
  - Wykorzystanie w audycie publikacji opracowanej przez Grupę Współpracy NIS Komisji Europejskiej, która dotyczy implementacji dyrektywy NIS w sektorze energii – *Sectorial Implementation of the NIS Directive in the Energy Sector (Report – CG Publication 03/2019)* (https://ec.europa.eu/digital-single-market/en/news/eu-wide-cybersecurity-legislation-report-implementation-eu-rules-energy-sector), w szczególności zapisów z rozdziału 8 powyższej publikacji, dotyczącymi sposobów realizacji wymagań bezpieczeństwa w oparciu o międzynarodowe normy, standardy i dobre praktyki w związku z obowiązkami nałożonymi na OUK w sektorze energii;
  - Wykorzystanie narzędzia udostępnionego na stronie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dotyczącego minimalnych środków bezpieczeństwa wymaganych dla operatorów usług kluczowych, wskazujących zalecane normy i standardy a także wymagania dotyczące przeprowadzania audytów bezpieczeństwa systemów informacyjnych (https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services).

Wymagania EITE:

- Audyt musi być przeprowadzony przez osoby posiadające odpowiednie uprawnienia zgodnie z wymaganiami Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. dotyczącymi wykazu certyfikatów uprawniających do przeprowadzenia audytu,
- Audyt musi być przeprowadzony zgodnie z harmonogramem uwzględnionym w pkt. 2.3 niniejszego OPZ.

Wymagania dotyczące raportu:

- Raport musi zawierać odniesienia do wymagań wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz Rozporządzeń do przedmiotowej ustawy,
- Raport musi uwzględniać opisany stan faktyczny podczas sesji audytowych oraz wnioski i zalecenia audytowe,
- W przypadku, gdy **EITE** w ramach postępowania zakupowego uwzględni również zakres prac opisany w wariancie opcjonalnym, Wykonawca zobowiązany jest uwzględnić wszystkie informacje na temat przeprowadzonego audytu technicznego w raporcie z uwzględnieniem zidentyfikowanych podatności oraz proponowane działania naprawcze.

II. Wariant opcjonalny:

- Przeprowadzenie audytów technicznych zidentyfikowanych 3 systemów informacyjnych w zakresie skanowania podatności,

- Audyt techniczny w pomieszczeniach **PŚU (EITE)** - Płock (spełnienie wymagań z Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 w sprawie warunków organizacyjnych i technicznych).

2.3. Harmonogram

Harmonogram realizacji prac audytowych		
Lp.	**Zadanie**	**Termin**
1.	Realizacja prac audytowych zgodnie z ustalonym zakresem	09.03.2020 - 10.04.2020
2.	Przygotowanie raportu z przeprowadzonego audytu	13.04.2020 – 26.04.2020

Termin 26.04.2020 r. jest ostatnim możliwym dniem na dostarczenie przez Wykonawcę uzgodnionego z EITE raportu końcowego z przeprowadzonego audytu.

3. Zakres zapytania dla Podmiotu B

3.1. Podstawowe informacje o podmiocie, którego dotyczy audyt

Podmiot, którego dotyczy audyt w ramach niniejszego Opisu Przedmiotu Zapytania jest spółka Grupy Energa odpowiedzialna za **sprzedaż energii elektrycznej**, która została zakwalifikowana jako Operator Usługi Kluczowej w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Spółka posiada zatrudnionych ok. 1 000 pracowników oraz rozproszoną strukturę składającą się z oddziałów oraz Biur Obsługi Klienta.

Spółka zidentyfikowała 11 systemów informacyjnych, które mają bezpośredni wpływ na świadczenie Usługi Kluczowej są to m.in. systemy billingowe, systemy klasy CRM, hurtownie danych, systemy wykorzystywane do obsługi klienta (w tym platformy udostępniane w sieci publicznej).

Większość infrastruktury oraz systemów teleinformatycznych dostarczana jest do spółki na podstawie umów ze spółką informatyczną, która również wchodzi w skład Grupy Energa oraz posiada certyfikat ISO 27001.

3.2. Wymagania EITE oraz zakres audytu

Przedmiotem zapytania jest przeprowadzenie audytu bezpieczeństwa stanowiącego wymagania ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. art. 15 ust.1 w spółce Grupy Energa świadczącej usługi sprzedaży energii elektrycznej zakwalifikowanej jako Operator Usługi Kluczowej.

I. **Wariant podstawowy:**

Zakres audytu:

- Audyt bezpieczeństwa 11 systemów informacyjnych, które zostały zidentyfikowane przez EITE jako wykorzystywane do świadczenia usługi kluczowej,
- Audyt bezpieczeństwa innych systemów mogących mieć wpływ na świadczenie Usługi Kluczowej, które zostaną zidentyfikowane podczas prowadzonego audytu,

- Przeprowadzenie audytu w pełnym zakresie dotyczącym spełnienia wymagań wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. oraz wymagań zawartych w Rozporządzeniach do przedmiotowej ustawy,
- Przeprowadzenie audytu w siedzibie EITE w Gdańsku,
- Przeprowadzenie audytu w Biurze Obsługi Klienta w Gdańsku (pobranie próbki audytowej ze względu na powtarzalność działalności w innych lokalizacjach),
- Przeprowadzenie audytu zgodnie z najlepszymi praktykami rynkowymi, zakończonego raportem zgodnym z szablonem stanowiącym Załącznik nr 3 do RFI,
- Uwzględnienie zaleceń Ministerstwa Aktywów Państwowych, przedstawionych w grudniu 2019 poszczególnym operatorom usług kluczowych, takich jak:
  - Przeprowadzenie audytu zgodnie z zapisem art. 15 ust. 2 pkt 2 lit a Ustawy o KSC;
  - Metodyka wykonania audytu powinna bazować na jednej z norm: ISO/IEC 27001, ISA/IEC 62443;
  - Wykorzystanie w audycie publikacji opracowanej przez Grupę Współpracy NIS Komisji Europejskiej, która dotyczy implementacji dyrektywy NIS w sektorze energii – *Sectorial Implementation of the NIS Directive in the Energy Sector (Report – CG Publication 03/2019)* (https://ec.europa.eu/digital-single-market/en/news/eu-wide-cybersecurity-legislation-report-implementation-eu-rules-energy-sector), w szczególności zapisów z rozdziału 8 powyższej publikacji, dotyczącymi sposobów realizacji wymagań bezpieczeństwa w oparciu o międzynarodowe normy, standardy i dobre praktyki w związku z obowiązkami nałożonymi na OUK w sektorze energii;
  - Wykorzystanie narzędzia udostępnionego na stronie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dotyczącego minimalnych środków bezpieczeństwa wymaganych dla operatorów usług kluczowych, wskazujących zalecane normy i standardy a także wymagania dotyczące przeprowadzania audytów bezpieczeństwa systemów informacyjnych (https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services).

Wymagania EITE:

- Audyt musi być przeprowadzony przez osoby posiadające odpowiednie uprawnienia zgodnie z wymaganiami Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. dotyczącego wykazu certyfikatów uprawniających do przeprowadzenia audytu,
- Audyt musi być przeprowadzony zgodnie z harmonogramem uwzględnionym w pkt. 3.3 OPZ.

Wymagania dotyczące raportu:

- Raport musi zawierać odniesienia do wymagań wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz Rozporządzeń do przedmiotowej ustawy,
- Raport musi uwzględniać opisany stan faktyczny podczas sesji audytowych, obserwacje i niezgodności ustalone podczas badania audytowego oraz wnioski i zalecenia audytowe,
- W przypadku, gdy EITE w ramach postępowania zakupowego uwzględni również zakres prac opisany w wariancie opcjonalnym, Wykonawca zobowiązany jest uwzględnić wszystkie informacje na temat przeprowadzonego audytu technicznego w raporcie z uwzględnieniem zidentyfikowanych podatności oraz proponowane działania naprawcze.

II. Wariant opcjonalny:

- Przeprowadzenie audytów technicznych zidentyfikowanych 11 systemów informacyjnych w zakresie przeskanowania podatności,
- Audyt techniczny w/w systemów informacyjnych przeprowadzony w siedzibie spółki informatycznej świadczącej usługi dla Operatora Usług Kluczowych. Audyt przeprowadzony w lokalizacjach – Gdańsk

oraz Płock.

3.3. Harmonogram

Harmonogram realizacji prac audytowych		
Lp.	**Zadanie**	**Termin**
1.	Realizacja prac audytowych zgodnie z ustalonym zakresem	02.03.2020 - 03.04.2020
2.	Przygotowanie raportu z przeprowadzonego audytu	03.04.2020 – 17.04.2020

Termin 17.04.2020 r. jest ostatnim możliwym dniem na dostarczenie przez Wykonawcę raportu końcowego z przeprowadzonego audytu i nie podlega negocjacjom.

4. Zakres zapytania dla Podmiotu C

4.1. Podstawowe informacje o podmiocie, którego dotyczy audyt

Podmiot, którego dotyczy audyt w ramach niniejszego Opisu Przedmiotu Zapytania jest spółka Grupy Energa odpowiedzialna za **wytwarzanie energii elektrycznej** i **wytwarzanie ciepła**, która została zakwalifikowana jako Operator Usługi Kluczowej (zwany dalej: **OUK**) w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa.

OUK posiada podpisaną umowę na świadczenie kilku wybranych usług z zakresu cyberbezpieczeństwa ze spółką informatyczną z Grupy Energa (dalej: Podmiot Świadczący Usługi z obszaru cyberbezpieczeństwa – **PŚU; EITE**), która posiada certyfikat ISO 27001 oraz w ramach której działa zespół CERT Energa.

OUK zatrudnia do **600** pracowników, w tym do **10** osób z obszaru IT / OT utrzymujących systemy informacyjne oraz posiada **jedną** lokalizację.

OUK zidentyfikował **9** głównych systemy informacyjnych z obszaru IT / OT (2 – IT, 7 – OT), które mają bezpośredni wpływ na świadczenie Usługi Kluczowej (wymienione w pkt 4.2 poniżej).

Obszar OT zarządzany jest przez pracowników **OUK**. Część infrastruktury teleinformatycznej oraz systemów teleinformatycznych z obszaru IT dostarczana jest do **OUK** na podstawie umów z **PŚU (EITE).**

4.2. Wymagania EITE oraz zakres audytu

Przedmiotem zapytania jest przeprowadzenie audytu bezpieczeństwa stanowiącego wymagania ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. art. 15 ust.1 w spółce Grupy Energa świadczącej usługi **wytwarzania energii elektrycznej i wytwarzania ciepła** wyznaczonej jako Operator Usługi Kluczowej.

III. <u>Wariant podstawowy:</u>

Zakres audytu:

- Audyt bezpieczeństwa 9 systemów informacyjnych z obszaru IT / OT, które zostały zidentyfikowane przez **OUK** jako wykorzystywane do świadczenia usługi kluczowej,

- Audyt bezpieczeństwa innych systemów informacyjnych mogących mieć wpływ na świadczenie Usługi Kluczowej, które zostaną zidentyfikowane podczas prowadzonego audytu,
- Przeprowadzenie audytów technicznych 2 systemów informacyjnych z obszaru OT w zakresie skanowania podatności:
  - Zintegrowany system zarządzania chemicznym laboratorium przemysłowym (obszar OT);
  - Zintegrowany system ważenia (obszar OT).
- Przeprowadzenie audytu w pełnym zakresie dotyczącym spełnienia wymagań wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 5 lipca 2018 r. oraz wymagań zawartych w Rozporządzeniach do przedmiotowej ustawy,
- Przeprowadzenie audytu w jednej fizycznej lokalizacji **OUK** – województwo mazowieckie,
- Przeprowadzenie audytu w lokalizacji (innej niż OUK) **PŚU (EITE)** – województwo mazowieckie (o ile na podstawie analizy podpisanych umów na usługi cyberbezpieczeństwa pomiędzy **OUK** a **PŚU** zajdzie taka potrzeba),
- Przeprowadzenie audytu zgodnie z szablonem stanowiącym załącznik nr 1 do OPZ,
- Uwzględnienie zaleceń Ministerstwa Aktywów Państwowych, przedstawionych w grudniu 2019 poszczególnym operatorom usług kluczowych, takich jak:
  - Przeprowadzenie audytu zgodnie z zapisem art. 15 ust. 2 pkt 2 lit a Ustawy o KSC;
  - Metodyka wykonania audytu powinna bazować na jednej z norm: ISO/IEC 27001, ISA/IEC 62443;
  - Wykorzystanie w audycie publikacji opracowanej przez Grupę Współpracy NIS Komisji Europejskiej, która dotyczy implementacji dyrektywy NIS w sektorze energii – *Sectorial Implementation of the NIS Directive in the Energy Sector (Report – CG Publication 03/2019)* (https://ec.europa.eu/digital-single-market/en/news/eu-wide-cybersecurity-legislation-report-implementation-eu-rules-energy-sector), w szczególności zapisów z rozdziału 8 powyższej publikacji, dotyczącymi sposobów realizacji wymagań bezpieczeństwa w oparciu o międzynarodowe normy, standardy i dobre praktyki w związku z obowiązkami nałożonymi na OUK w sektorze energii;
  - Wykorzystanie narzędzia udostępnionego na stronie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dotyczącego minimalnych środków bezpieczeństwa wymaganych dla operatorów usług kluczowych, wskazujących zalecane normy i standardy a także wymagania dotyczące przeprowadzania audytów bezpieczeństwa systemów informacyjnych (https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services).

Wymagania EITE:

- Audyt musi być przeprowadzony przez osoby posiadające odpowiednie uprawnienia zgodnie z wymaganiami Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. dotyczącymi wykazu certyfikatów uprawniających do przeprowadzenia audytu,
- Audyt musi być przeprowadzony zgodnie z harmonogramem uwzględnionym w pkt. 2.3 niniejszego OPZ.

Wymagania dotyczące raportu:

- Raport musi zawierać odniesienia do wymagań wynikających z ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz Rozporządzeń do przedmiotowej ustawy,
- Raport musi uwzględniać opisany stan faktyczny podczas sesji audytowych oraz wnioski i zalecenia audytowe,
- W przypadku, gdy **EITE** w ramach postępowania zakupowego uwzględni również zakres prac opisany w wariancie opcjonalnym, Wykonawca zobowiązany jest uwzględnić wszystkie informacje na temat przeprowadzonego audytu technicznego w raporcie z uwzględnieniem zidentyfikowanych podatności oraz proponowane działania naprawcze.

IV. Wariant opcjonalny:

- Przeprowadzenie audytów technicznych 7 systemów informacyjnych z obszaru IT / OT w zakresie skanowania podatności (**z terminem realizacji sierpień 2020**):
  - System klasy ERP (obszar IT);
  - System wymiany dokumentacji, odczyt i wymian danych pomiarowych, udział w rynku energii (obszar IT);
  - System sterowania blokiem energetycznym (obszar OT);
  - System sterowania stacją rozładunku (obszar OT);
  - System sterowania mocą i rozdzielniami elektrycznymi (obszar OT);
  - System wizualizacji procesów technologicznych (obszar OT);
  - System monitorowania parametrów spalin (obszar OT).

4.3. Harmonogram

Harmonogram realizacji prac audytowych		
Lp.	**Zadanie**	**Termin**
1.	Realizacja prac audytowych zgodnie z ustalonym zakresem	16.03.2020 - 14.04.2020
2.	Przygotowanie raportu z przeprowadzonego audytu	15.04.2020 – 30.04.2020

Termin 30.04.2020 r. jest ostatnim możliwym dniem na dostarczenie przez Wykonawcę uzgodnionego z EITE raportu końcowego z przeprowadzonego audytu.

5. Zakres zapytania dla Podmiotu D

5.1. Podstawowe informacje o podmiocie, którego dotyczy audyt

Podmiot, którego dotyczy audyt w ramach niniejszego Opisu Przedmiotu Zapytania jest spółką Grupy Energa świadczącą usługi wytwarzania energii elektrycznej, która na podstawie decyzji została wyznaczona jako Operator Usługi Kluczowej (zwany dalej: **OUK**) w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa.

OUK posiada podpisaną umowę na świadczenie kilku wybranych usług z zakresu cyberbezpieczeństwa ze spółką informatyczną z Grupy Energa (dalej: Podmiot Świadczący Usługi z obszaru cyberbezpieczeństwa – **PŚU; EITE**), która posiada certyfikat ISO 27001 oraz w ramach której działa zespół CERT Energa.

Obszar OT zarządzany jest przez pracowników **OUK**. Część infrastruktury teleinformatycznej oraz systemów teleinformatycznych z obszaru IT dostarczana jest do **OUK** na podstawie umów z **PŚU (EITE).**

5.2. Wymagania EITE oraz zakres audytu

Przedmiotem zapytania jest przeprowadzenie audytu bezpieczeństwa zgodnie z dyspozycją art. 15 ust. 1 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa w spółce Grupy Energa świadczącej usługi **wytwarzania energii elektrycznej** wyznaczonej jako Operator Usługi Kluczowej.

III. Wariant podstawowy:

Zakres audytu:

- Audyt bezpieczeństwa **18** systemów informacyjnych w **6** różnych lokalizacjach, które zostały zidentyfikowane przez **OUK** jako wspierające świadczenie usługi kluczowej:
  - 6 systemów w lokalizacji nr 1 – woj. zachodniopomorskie,
  - 6 systemów w lokalizacji nr 2 – woj. kujawsko-pomorskie,
  - 2 systemy w lokalizacji nr 3 – woj. zachodniopomorskie,
  - 2 systemy w lokalizacji nr 4 – woj. pomorskie,
  - 1 system w lokalizacji 5 – woj. pomorskie,
  - 1 system w lokalizacji 6 – woj. pomorskie.
- Przeprowadzenie audytu w lokalizacji **PŚU (EITE)** – Płock (o ile na podstawie analizy podpisanych umów na usługi cyberbezpieczeństwa pomiędzy **OUK** a **PŚU** zajdzie taka potrzeba),
- Uwzględnienie zaleceń Ministerstwa Aktywów Państwowych, przedstawionych w grudniu 2019 poszczególnym operatorom usług kluczowych, takich jak:
  - Przeprowadzenie audytu zgodnie z zapisem art. 15 ust. 2 pkt 2 lit a Ustawy o KSC;
  - Metodyka wykonania audytu powinna bazować na jednej z norm: ISO/IEC 27001, ISA/IEC 62443;
  - Wykorzystanie w audycie publikacji opracowanej przez Grupę Współpracy NIS Komisji Europejskiej, która dotyczy implementacji dyrektywy NIS w sektorze energii – *Sectorial Implementation of the NIS Directive in the Energy Sector (Report – CG Publication 03/2019)* (https://ec.europa.eu/digital-single-market/en/news/eu-wide-cybersecurity-legislation-report-implementation-eu-rules-energy-sector), w szczególności zapisów z rozdziału 8 powyższej publikacji, dotyczącymi sposobów realizacji wymagań bezpieczeństwa w oparciu o międzynarodowe normy, standardy i dobre praktyki w związku z obowiązkami nałożonymi na OUK w sektorze energii;
  - Wykorzystanie narzędzia udostępnionego na stronie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) dotyczącego minimalnych środków bezpieczeństwa wymaganych dla operatorów usług kluczowych, wskazujących zalecane normy i standardy a także wymagania dotyczące przeprowadzania audytów bezpieczeństwa systemów informacyjnych (https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services).

Wymagania EITE:

- Audyt musi być przeprowadzony przez osoby posiadające odpowiednie uprawnienia zgodnie z wymaganiami Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. dotyczącymi wykazu certyfikatów uprawniających do przeprowadzenia audytu,
- Audyt musi być przeprowadzony zgodnie z harmonogramem uwzględnionym w pkt. 2.3 niniejszego OPZ.

Wymagania dotyczące raportu /sprawozdania:

- EITE nie narzuca szablonu w zakresie zawartości raportu / sprawozdania; formę określi Wykonawca.

5.3. Harmonogram

Harmonogram realizacji prac audytowych		
Lp.	**Zadanie**	**Termin**
1.	Przeprowadzenie i zakończenie audytu, wraz z przekazaniem raportu / sprawozdania do OUK (podmiotu D)	Do dnia **30.04.2020**