

Warszawa, dnia 03.07.2026 r.

Znak sprawy: P.261.71.2026.P2

ZAPYTANIE OFERTOWE 4/2026

1. Zamawiający, Transportowy Dozór Techniczny w Warszawie zaprasza do złożenia oferty w postępowaniu na: **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Transportowym Dozorze Technicznym.**
2. Określenie przedmiotu zamówienia:
 - 1) Przedmiotem zamówienia jest usługa polegająca na wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w Transportowym Dozorze Technicznym;
 - 2) Opis przedmiotu zamówienia stanowi Załącznik nr 1 – Opis przedmiotu zamówienia;
 - 3) Wspólny Słownik Zamówień CPV:
79.21.20.00-3 Usługi audytu
72.15.00.00-1 Usługi doradztwa w zakresie audytu komputerowego oraz sprzętu komputerowego
3. Termin realizacji zamówienia:
Okres realizacji zamówienia: w nieprzekraczalnym terminie do 20.12.2026 r.
4. Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny ich spełnienia:
 - 1) spełniają warunki udziału w postępowaniu dotyczące **zdolności technicznej lub zawodowej**
 - a) **odnoszącej się do doświadczenia:**

Zamawiający wymaga, aby Wykonawca wykazał, że w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał należycie co najmniej:

 - I. 2 usługi polegające na opracowaniu, przeglądzie, aktualizacji, wdrożeniu, tj. kompleksowym przygotowaniu do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (zwane dalej SZBI). Zamawiający pod powyższym zapisem rozumie analizę stanu obecnego, analizę luk, analizę ryzyka, rejestr aktywów lub aktywów informacyjnych (zwany inaczej klasyfikacją aktywów informacyjnych), plan postępowania z ryzykiem, opracowanie dokumentacji SZBI, procedurę zarządzania incydentami (w tym obsługa incydentów, raportowanie incydentów), bezpieczeństwo łańcucha dostaw lub nadzoru nad dostawcami usług ICT¹, deklarację stosowania albo dokument równoważny oraz elementy zarządzania ciągłością działania SZBI w jednostkach sektora finansów publicznych, określonych w Ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, obejmujące wymagania:

– norm PN-EN ISO/IEC 27001:2023-08 lub normy równoważnej oraz

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego

- norm PN-EN ISO 22301:2019 w zakresie ciągłości działania lub normy równoważnej,
- Dyrektywą 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 (zwana dalej NIS 2)
- Ustawą o krajowym systemie cyberbezpieczeństwa (zwaną dalej UKSC)

oraz

- II. 1 usługę polegającą na opracowaniu lub aktualizacji Systemu Zarządzania Ciągłością Działania (zwane dalej SZCD), w tym co najmniej: analizę wpływu na działalność, identyfikację procesów krytycznych, określenie parametrów RTO/RPO, opracowanie strategii ciągłości działania, planów ciągłości działania lub planów odtworzeniowych oraz scenariuszy testów lub ćwiczeń.

Każda jedna z powyższych trzech usług powinna mieć wartość co najmniej 70 000,00 zł brutto – zgodnie z Załącznikiem nr 3.

Wykonawca zobowiązany jest przedstawić dowody potwierdzające należyte wykonanie usług wykazanych na potwierdzenie spełnienia warunków udziału w postępowaniu. Dowodami mogą być w szczególności referencje, poświadczenia, protokoły odbioru, zaświadczenia, oświadczenia odbiorców usług lub inne dokumenty potwierdzające zakres, termin, wartość i należyte wykonanie usługi. Jeżeli ze względu na zobowiązania poufności, charakter odbiorcy lub szczególną wrażliwość projektu Wykonawca nie może ujawnić pełnej nazwy odbiorcy, dopuszcza się przedstawienie zanonimizowanej referencji lub oświadczenia Wykonawcy, pod warunkiem że dokument umożliwia ocenę zakresu, wartości, terminu i rezultatu usługi.

b) odnoszące się do zdolności technicznej:

Wykonawca posiada wdrożony i certyfikowany system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001 lub równoważny, obejmujący zakresem działalność doradczą, audytową, konsultingową, bezpieczeństwo informacji, cyberbezpieczeństwo, usługi IT lub inne usługi odpowiadające przedmiotowi zamówienia.

Za dokumenty potwierdzające można uznać aktualny certyfikat ISO/IEC 27001 wystawiony przez akredytowaną jednostkę certyfikującą albo dokumenty równoważne potwierdzające wdrożenie, utrzymywanie, audytowanie i doskonalenie systemu zarządzania bezpieczeństwem informacji u wykonawcy.

c) odnoszące się do dysponowania osobami, które będą brały udział w realizacji niniejszego zamówienia:

- i. osobę pełniącą funkcję Kierownika projektu / koordynatora wdrożenia (odpowiada za harmonogram, komunikację, jakość, odbiory i koordynację zespołu), która:
- posiada co najmniej dwa certyfikaty lub kwalifikacje, z których co najmniej jeden dotyczy audytowania albo wdrażania SZBI, a co najmniej jeden dotyczy audytu bezpieczeństwa informacji, cyberbezpieczeństwa, zarządzania ryzykiem, ciągłości działania albo audytu systemów informacyjnych lub równoważne,
 - posiada minimum 2-letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa oraz
 - posiada minimum 3-letnie doświadczenie w prowadzeniu projektów z zakresu SZBI, cyberbezpieczeństwa, compliance, audytu lub ciągłości działania oraz

- uczestniczyła w co najmniej 2 projektach dotyczących przeglądu, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach sektora finansów publicznych określonych w Ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U.z 2024r. poz. 1530 z późn. zm.) w zakresie ISO 27001, UKSC/NIS2, KRI lub ISO 22301
- ii. osobą pełniącą funkcję Eksperta SZBI / ISO 27001 Lead Implementer, który:
 - posiada minimum 2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa zgodnie z normą ISO/IEC 27001;
 - uczestniczył w co najmniej 2 projektach dotyczących przeglądu, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach sektora finansów publicznych określonych w Ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U.z 2024r. poz. 1530 z późn. zm.) w zakresie ISO 27001, UKSC/NIS2, KRI lub ISO 22301
- iii. osobą pełniącą funkcję Audytora wiodącego ISO 27001, który:
 - posiada certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025r. poz. 568), w zakresie certyfikacji osób lub równoważnym;
 - posiada minimum 2 letnie doświadczenie w przeprowadzaniu audytów bezpieczeństwa zgodnie z normą ISO/IEC 27001;;
 - uczestniczył w co najmniej 2 projektach dotyczących przeglądu, aktualizacji i wdrożeniu Systemu Zarządzania Bezpieczeństwem Informacji w jednostkach sektora finansów publicznych określonych w Ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U.z 2024r. poz. 1530 z późn. zm.) w zakresie ISO 27001, UKSC/NIS2, KRI lub ISO 22301
- iv. osobą pełniącą funkcję Eksperta ISO 22301, który
 - posiada minimum 2 letnie doświadczenie w zakresie zgodnie z normą ISO/IEC 27001;
 - uczestniczył w co najmniej 2 projektach w zakresie BIA, RTO/RPO, planach ciągłości działania, planach odtworzeniowych i testach ciągłości zgodnie z normą PN-EN ISO 22301.
- v. osobą pełniącą funkcję eksperta cyberbezpieczeństwa technicznego / KRI / UKSC, który:
 - posiada rozległą wiedzę techniczną z zakresu bezpieczeństwa systemów i sieci potwierdzoną co najmniej jednym z certyfikatów (np.: VA - Certified Vulnerability Assessor, CSSA - Certified Cybersecurity Systems Auditor, CompTIA Security+) lub równoważnym;
 - posiada minimum 3 letnie doświadczenie w audytach technicznych IT, bezpieczeństwie sieci, architekturze bezpieczeństwa, zarządzaniu podatnościami lub ocenie zabezpieczeń technicznych zgodnie z przepisami KRI, UKSC/NIS2.
- vi. osobą pełniącą funkcję pełnomocnika posiadającą poświadczenia bezpieczeństwa oraz aktualne przeszkolenie w zakresie ochrony informacji niejawnych zgodnie z ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209 tj.).

Zamawiający dopuszcza łączenie maksymalnie dwóch ról przez jedną osobę, pod warunkiem spełnienia przez tę osobę wszystkich wymagań przewidzianych dla łączonych ról. Funkcja kierownika projektu nie powinna być łączona z więcej niż jedną funkcją ekspercką.

Przez równoważne kwalifikacje zawodowe Zamawiający rozumie możliwość wykazania posiadania innych certyfikatów niż wskazane przez Zamawiającego, pod warunkiem że potwierdzają one kwalifikacje w zakresie odpowiadającym wymaganiom określonym dla danego stanowiska.

W przypadku powołania się na certyfikaty równoważne Wykonawca zobowiązany jest do wskazania nazwy certyfikatu oraz nazwy instytucji certyfikującej – zgodnie z wzorem stanowiącym załącznik nr 4 do niniejszego zapytania (Wykaz osób).

Zamawiający uzna za równoważne certyfikaty, które łącznie spełniają następujące warunki:

- a) potwierdzają posiadanie wiedzy i umiejętności w zakresie audytu systemów zarządzania bezpieczeństwem informacji lub ciągłości działania, co najmniej odpowiadających wymaganiom określonym w normach ISO/IEC 27001 oraz ISO 22301;
- b) zostały wydane przez niezależną jednostkę certyfikującą (osoby), działającą zgodnie z zasadami oceny zgodności, w szczególności w oparciu o wymagania określone w ustawie z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku lub równoważnych regulacjach;
- c) umożliwiają weryfikację zakresu certyfikacji oraz podmiotu wydającego.

Wykonawca wraz z ofertą złoży poświadczony za zgodność z oryginałem kopie ww. certyfikatów.

- 2) spełniają warunki udziału w postępowaniu dotyczące **sytuacji ekonomicznej lub finansowej**:

Zamawiający wymaga, aby Wykonawca wykazał, że posiada ubezpieczenie odpowiedzialności cywilnej zawodowej z tytułu prowadzonej działalności gospodarczej związanej z przedmiotem zamówienia, obejmującej działalność doradczą, audytową, konsultingową, informatyczną lub z zakresu bezpieczeństwa informacji, na sumę gwarancyjną nie mniejszą niż 2 000 000,00 zł.

Zakres ochrony ubezpieczeniowej powinien obejmować odpowiedzialność za szkody wskutek błędów, zaniedbań lub nieprawidłowości powstałych w trakcie świadczenia usług informatycznych wynikające w szczególności z nieprawidłowych działań doradczych, audytowych, organizacyjnych, naruszenia obowiązku zachowania poufności, prywatności oraz odpowiedzialności internetowej (w tym wycieku danych / informacji), nienależytego wykonania usług lub innych zdarzeń pozostających w związku z realizacją przedmiotu zamówienia.

Na potwierdzenie spełnienia warunku Wykonawca zobowiązany jest przedłożyć kopię aktualnej polisy ubezpieczenia odpowiedzialności cywilnej lub inny dokument wystawiony przez ubezpieczyciela potwierdzający posiadanie ważnego ubezpieczenia na wymaganą sumę gwarancyjną.

5. Kryteria oceny ofert

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami:
Cena –100%

W - Cena za realizację zamówienia – waga 100 %.

Oferta z najniższą ceną otrzyma maksymalną liczbę punktów – 100 pkt.

Pozostałe oferty zostaną przeliczone według poniższego wzoru

$$W = \frac{\text{najniższa cena oferty brutto}}{\text{cena oferty badanej brutto}} \times 100$$

Maksymalna liczba punktów jakie można uzyskać wynosi 100.

Najwyższa liczba punktów wyznaczy najkorzystniejszą ofertę.

6. Informacje dotyczące przygotowania i składnia ofert:

- 1) Wykonawca przystępujący do postępowania zobowiązany jest do przygotowania i złożenia oferty w sposób zgodny z wymaganiami opisanymi w niniejszym zapytaniu pod rygorem odrzucenia oferty;
- 2) Ofertę należy sporządzić w języku polskim;
- 3) Wykonawca może złożyć tylko jedną ofertę;

- 4) oferta musi być podpisana przez osobę(y) uprawnioną(e) do reprezentowania Wykonawcy;
 - 5) ofertę należy złożyć zgodnie z załączonym wzorem formularza oferty stanowiącym załącznik nr 2 do niniejszego zapytania, w którym Wykonawca podaje cenę za wykonanie przedmiotu zamówienia;
 - 6) cena winna obejmować wszystkie koszty jakie Wykonawca będzie musiał ponieść w celu prawidłowej realizacji przedmiotu zamówienia;
 - 7) cena za wykonanie przedmiotu zamówienia musi być podana w złotych polskich cyfrowo i słownie z uwzględnieniem wszystkich opłat i podatków (w tym VAT) oraz ewentualnych upustów i rabatów;
 - 8) wraz z ofertą i szczegółowym formularzem cenowym Wykonawca zobowiązany jest złożyć następujące dokumenty:
 - a) odpis lub informacja z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, sporządzona nie wcześniej niż 3 miesiące przed jej złożeniem, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
 - b) pełnomocnictwo upoważniające do złożenia oferty – (o ile ofertę składa pełnomocnik) Pełnomocnictwo do złożenia oferty musi być złożone w formie elektronicznej opatrzone podpisem kwalifikowanym. Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie (t.j. Dz.U.2024 poz. 1001).
 - c) Załącznik nr 3 – Wykaz usług. Do Wykazu należy załączyć dowody potwierdzające, że wskazane usługi zostały wykonane w sposób należyty.
 - d) Załącznik nr 4 – Wykaz osób.
 - e) kopie certyfikatów poświadczone za zgodność z oryginałem przez Wykonawcę.
 - f) kopię aktualnej polisy ubezpieczenia odpowiedzialności cywilnej lub inny dokument wystawiony przez ubezpieczyciela.
 - 9) Wykonawca jest związany ofertą 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert;
 - 10) Ofertę wraz z załącznikami należy złożyć:
 - a) w postaci elektronicznej – jako dokument opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, albo
 - b) w formie dokumentowej – jako skan oferty podpisanej własnoręcznie.
 - 11) **Ofertę należy przesyłać w nieprzekraczalnym terminie do: 14.07.2026 r. na adres poczty elektronicznej e-mail: przetargi@tdt.gov.pl**
6. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.
 7. Dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
 8. Osoby uprawnione do porozumiewania się z Wykonawcami:
 - w sprawach dot. przedmiotu zamówienia – Mariusz Sagan, tel. 728 333 019, email: mariusz.sagan@tdt.gov.pl
 - w sprawach dot. procedury – Wioletta Waszczuk, email: przetargi@tdt.gov.pl
 9. Postanowienia końcowe:
 - 1) niniejsze zapytanie nie stanowi oferty w myśl art. 66 Kodeksu Cywilnego, jak również nie jest ogłoszeniem w rozumieniu ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych;

- 2) Zamawiający zastrzega sobie przed wyborem oferty prawo do ewentualnych negocjacji z Wykonawcami treści istotnych postanowień umowy, w tym ceny oferowanej przez Wykonawców;
- 3) Zamawiający zastrzega sobie prawo do rezygnacji z udzielenia zamówienia bez podania przyczyny;
- 4) Zamawiający zastrzega, że Nazwa i adres Wykonawcy oraz oferowana cena będzie stanowić informację publiczną;
- 5) Zamawiający zawiadomi wszystkich Wykonawców biorących udział w postępowaniu o wyborze Wykonawcy lub o unieważnieniu postępowania;
- 6) Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę na warunkach określonych w Załączniku nr 5 do niniejszego zapytania – Projektowane Postanowienia Umowy.
- 7) Komunikacja z Wykonawcą prowadzona będzie w języku polskim.

Klauzula informacyjna RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, Transportowy Dozór Techniczny informuje, że:

- 1) administratorem Pani/Pana danych osobowych jest **Dyrektor Transportowego Dozoru Technicznego; dane kontaktowe: ul. Puławska 125, 02-707 Warszawa tel. 22 490 29 02, info@tdt.gov.pl ;**
- 2) kontakt z Inspektorem Ochrony Danych w Transportowym Dozorze Technicznym możliwy jest pod adresem e-mail: dane.osobowe@tdt.gov.pl;
- 3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b RODO w celu związanym z zapytaniem ofertowym w postępowaniu na **Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Transportowym Dozorze Technicznym**;
- 4) Pani/Pana dane osobowe nie będą przekazywane innym podmiotom/osobom trzecim;
- 5) Pani/Pana dane osobowe będą przechowywane przez okres oraz w zakresie wymaganym przez przepisy powszechnie obowiązującego prawa;
- 6) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- 7) posiada Pan/Pani:
 - a) na podstawie art. 15 RODO prawo dostępu do Pani/Pana danych osobowych;
 - b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
 - c) na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania Pani/Pana danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
 - d) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO;
- 8) w przypadkach, o których mowa w art. 17 ust. 3 lit. b, d lub e RODO nie przysługuje prawo do usunięcia Pani/Pana danych osobowych;
- 9) w przypadkach, o których mowa w art. 20 RODO nie przysługuje prawo do przenoszenia Pani/Pana danych osobowych;
- 10) w przypadkach, o których mowa w art. 21 RODO nie przysługuje prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. b RODO.

Załączniki:

Załącznik nr 1 – Opis przedmiotu zamówienia

Załącznik nr 2 – Formularz oferty wraz ze szczegółowym formularzem cenowym

Załącznik nr 3 – Wykaz usług

Załącznik nr 4 – Wykaz osób

Załącznik nr 5 – Projektowane Postanowienia Umowy

*Dokument podpisany elektronicznie
Agnieszka Zawadzka
p.o. Dyrektor
Transportowego Dozoru Technicznego*