**Opis Przedmiotu Zamówienia**

1. **Przedmiot zamówienia:**
	1. Przedmiotem zamówienia jest wykonanie usługi audytu zgodności systemu zarządzania bezpieczeństwem informacji (SZBI) w Ministerstwie Rozwoju, Pracy i Technologii (MRPiT) z normą PN-ISO/IEC 27001:2017, zewnętrzne i wewnętrzne testy penetracyjne systemów informatycznych utrzymywanych przez MRPiT oraz badanie odporności na socjotechniki użytkowników poczty elektronicznej MRPiT, w siedzibie przy Pl. Trzech Krzyży 3/5 oraz ul. Żurawiej 4a w Warszawie.
	2. Zakres przedmiotowy audytu obejmuje:
		1. określenie zgodności istniejącego SZBI MRPiT z obszarami i szczegółowymi zabezpieczeniami wskazanymi w Załączniku A do normy PN-ISO/IEC 27001:2017;
		2. weryfikację poprawności stosowanych w MRPiT zabezpieczeń w odniesieniu do wymagań zawartych w Załączniku A do normy PN-ISO/IEC 27001:2017;
		3. opracowanie rekomendacji w zakresie doskonalenia SZBI MRPiT.
	3. W ramach usługi Wykonawca przeprowadzi zewnętrzne i wewnętrzne nieinwazyjne testy penetracyjne typu black-box w środowisku produkcyjnym następujących systemów utrzymywanych przez MRPiT:
		1. Kontroler domeny;
		2. Serwer plików;
		3. Serwery EZD;
		4. Telefonię VOIP;
		5. System Firewall;
		6. Serwery pocztowe i system antyspamowy;
		7. Hosty hiperkonwergentne;
		8. System backupu;
		9. Infrastruktura sieciowa.
	4. Przeprowadzenie ewentualnych zewnętrznych i wewnętrznych inwazyjnych testów penetracyjnych typu black-box w środowisku produkcyjnym systemów utrzymywanych przez MRPiT, o których mowa w pkt. 1.3, może nastąpić wyłącznie za zgodą Zamawiającego, w wyniku uzgodnień planu audytu, po wskazaniu skutków takich testów dla systemów MRPiT.
	5. W ramach usługi Wykonawca przeprowadzi badanie odporności na socjotechniki użytkowników poczty elektronicznej MRPiT.
2. **Zobowiązania Wykonawcy**
	1. Wykonawca przygotuje plan i harmonogram audytu, który uzgodni z zamawiającym.
	2. W ramach prowadzonych czynności audytowych wykonawca zobowiązuje się do stosowania uznawanych standardów organizacji branżowych i normy, specjalistyczne urządzenia, oprogramowanie oraz uzgodnione z wykonawcą scenariusze testowe.
	3. W ramach usługi audytu Wykonawca przygotuje raport, który będzie zawierał co najmniej:
		1. temat i cel audytu;
		2. zakres podmiotowy i przedmiotowy audytu;
		3. datę rozpoczęcia audytu;
		4. opis przyjętej metodyki;
		5. syntezę wyników audytu zawierającą ustalenia z określeniem zidentyfikowanych nieprawidłowości w podziale na: systemowe i incydentalne oraz wskazaniem dobrych i złych praktyk;
		6. ustalenia, w tym:
			1. wyniki testów i ich interpretację, ogólną ocenę poziomu bezpieczeństwa (% zgodności z normą);
			2. odporności na ataki, stwierdzone słabości/nieprawidłowości ze wskazaniem systemu i krytyczności, lokalizację podatności) oraz ocenę szczegółową przygotowaną według kryteriów przyjętych w planie audytu – na każde ustalenie powinny być wskazane konkretne przypadki ewentualnych słabości/nieprawidłowości poparte zgromadzonymi dowodami audytowymi, które będą stanowiły załączniki do raportu;
			3. punktację zgodności dla każdego zabezpieczenia z Załącznika A normy ze stanem faktycznym, gdzie 0 pkt oznacza brak zgodności, 0.5 pkt oznacza częściową zgodność, a 1 pkt oznacza pełną zgodność;
			4. identyfikację potencjalnych luk, słabości lub zagrożeń w systemie, w celu określenia ryzyk związanych z zapewnieniem ciągłości realizacji zadań MRPiT, ze szczególnym uwzględnieniem procesów krytycznych;
		7. skutki/ryzyka będące konsekwencją stwierdzonych słabości/niezgodności z przyjętymi kryteriami;
		8. rekomendacje (w przypadku braku lub niefunkcjonowania zidentyfikowanych mechanizmów bezpieczeństwa, propozycje uzupełnienia dokumentacji systemu zarządzania bezpieczeństwem informacji w MRPiT o brakujące elementy), w tym wskazanie działań korygujących i usprawniających działanie systemu z uwzględnieniem ich priorytetów (tj. od najbardziej do najmniej istotnych);
		9. datę sporządzenia raportu;
		10. opis wykonanych czynności audytowych w odniesieniu do poszczególnych ryzyk, ujętych w planie audytu oraz listę zweryfikowanych dokumentów/regulacji;
		11. imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy.
	4. Ocena, ustalenia i rekomendacje powinny być ze sobą jasno powiązane i łatwo identyfikowalne.
	5. Załącznikiem do raportu będzie plan i harmonogram audytu uzgodniony z Zamawiającym.
	6. Dokumentacja audytowa zostanie przekazana łącznie z raportem dostarczonym w formie elektronicznej w formacie edytowalnym i pdf, w ostatnim dniu terminu realizacji audytu (lecz nie będzie stanowiła załącznika do raportu).
	7. Zamawiający ma prawo do zgłoszenia uwag do raportu, do których Wykonawca ustosunkuje się w terminie wskazanym przez Zamawiającego.
	8. Informacje uzyskane w trakcie realizacji audytu są znane jedynie osobom zaangażowanym w jego realizację ze strony Wykonawcy oraz przekazywane wskazanym pracownikom Zamawiającego. Dodatkowo w trakcie prac może zajść konieczność wymiany wrażliwych informacji związanych ze zrealizowaną usługą. W takim wypadku proponuje się:
		1. wykorzystanie do wymiany danych zabezpieczonych kryptograficznie mechanizmów poczty elektronicznej, przy użyciu kluczy asymetrycznych;
		2. przesyłanie danych w archiwum ZIP, zaszyfrowanym przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczonym co najmniej 8-znakowym hasłem jednorazowym, przesłanym przez alternatywny kanał komunikacji.