

WYKAZ OSÓB (dokument składa Wykonawca, którego oferta została najwyżej oceniona, w odpowiedzi na wezwanie Zamawiającego dokonane na podstawie art. 274 ust. 1 ustawy Pzp)

na potwierdzenie spełniania warunku określonego w pkt 5.1.1) SWZ w postępowaniu o udzielenie zamówienia publicznego, którego przedmiotem jest

opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w Małopolskim Urzędzie Wojewódzkim w Krakowie oraz jednostkach podległych

	Imię i nazwisko	Kwalifikacje ekspertów Uwaga należy skreślić, dla każdego z wykazywanych ekspertów, <u>kwalifikacje</u> których nie posiada	Doświadczenia ekspertów Uwaga należy skreślić, dla każdego z wykazywanych ekspertów, <u>doświadczenie</u> którego nie posiada	W odniesieniu do doświadczenia, należy przedstawić jednoznaczny opis umożliwiający ocenę spełniania warunku - zakres wykonywanych czynności - doświadczenie zawodowe (w latach)	Informacja o podstawie dysponowania przez Wykonawcę wskazaną osobą:	
					np. zobowiązanie podmiotu trzeciego tzw. dysponowanie pośrednie ¹	np. umowa o pracę/ umowa zlecenie/ umowa o dzieło tzw. dysponowanie bezpośrednie ²
1.	1) certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001	1) doświadczenie w realizacji dwóch audytów systemów zarządzania bezpieczeństwem			

¹ należy rozumieć powoływanie się na osoby zdolne do wykonania zamówienia należące do innych podmiotów tj. podmiotów, które dysponują takimi osobami, a na czas realizacji zamówienia w celu wykonywania pracy związanej z wykonywaniem tego zamówienia, np. oddelegują pracownika. W takim przypadku Wykonawca zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych osób na okres ich udziału w wykonaniu zamówienia.
UWAGA: Należy wpisać zobowiązanie podmiotu trzeciego. (W przypadku jeżeli nie dotyczy, Wykonawca powinien wpisać „nie dotyczy”).

² należy rozumieć przypadek, gdy tytułem prawnym do powoływania się przez Wykonawcę do dysponowania osobami zdolnymi do wykonania zamówienia jest stosunek prawny istniejący bezpośrednio pomiędzy Wykonawcą, osobą (osobami), na dysponowanie której (których) Wykonawca się powołuje. Przy czym bez znaczenia jest tutaj charakter prawnego takiego stosunku, tj. czy mamy do czynienia z umową o pracę, umową o świadczenie usług, czy też samozatrudnieniem się osoby fizycznej prowadzącej działalność gospodarczą. **UWAGA:** Należy wpisać odpowiednio: umowa o pracę, umowa zlecenie lub umowa o dzieło. (W przypadku jeżeli nie dotyczy, Wykonawca powinien wpisać „nie dotyczy”).

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

		<p>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 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób (lub równoważny);</p> <p>2) jeden z poniższych certyfikatów:</p> <ul style="list-style-type: none"> - Certified Information Systems Auditor (CISA), - Certified Information Security Manager (CISM), - Certified Information Systems Security Professional (CISSP). <p>3) certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób (lub równoważny).</p>	<p>informacji, zgodnych z normą ISO/IEC 27001, w okresie co najmniej dwóch lat, w tym doświadczenie w zakresie audytowania procesów bezpieczeństwa informacji w organizacjach;</p> <p>2) doświadczenie w realizacji dwóch wdrożeń SZBI w organizacji, obejmujące opracowanie polityk bezpieczeństwa, zarządzania ryzykiem oraz implementację wymagań normy ISO/IEC 27001, w okresie co najmniej dwóch lat</p>			
2.	<p>1) certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z</p>	<p>1) doświadczenie w realizacji dwóch audytów systemów zarządzania bezpieczeństwem informacji, zgodnych z normą ISO/IEC 27001, w</p>			

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

		<p>przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób (lub równoważny);</p> <p>2) jeden z poniższych certyfikatów: - Certified Information Systems Auditor (CISA), - Certified Information Security Manager (CISM), - Certified Information Systems Security Professional (CISSP).</p> <p>3) certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób (lub równoważny).</p>	<p>okresie co najmniej dwóch lat, w tym doświadczenie w zakresie audytowania procesów bezpieczeństwa informacji w organizacjach;</p> <p>2) doświadczenie w realizacji dwóch wdrożeń SZBI w organizacji, obejmujące opracowanie polityk bezpieczeństwa, zarządzania ryzykiem oraz implementację wymagań normy ISO/IEC 27001, w okresie co najmniej dwóch lat</p>			
3.	<p>1) 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, w</p>	<p>1) doświadczenie w realizacji dwóch audytów systemów zarządzania bezpieczeństwem informacji, zgodnych z normą ISO/IEC 27001, w okresie co najmniej dwóch lat, w tym doświadczenie w zakresie audytowania</p>			

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

		zakresie certyfikacji osób (lub równoważny); 2) jeden z poniższych certyfikatów: - Certified Information Systems Auditor (CISA), - Certified Information Security Manager (CISM), - Certified Information Systems Security Professional (CISSP). 3) certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób (lub równoważny).	procesów bezpieczeństwa informacji w organizacjach; 2) doświadczenie w realizacji dwóch wdrożeń SZBI w organizacji, obejmujące opracowanie polityk bezpieczeństwa, zarządzania ryzykiem oraz implementację wymagań normy ISO/IEC 27001, w okresie co najmniej dwóch lat			
4.	1) 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, w zakresie certyfikacji osób (lub równoważny); 2) jeden z poniższych certyfikatów:	1) doświadczenie w realizacji dwóch audytów systemów zarządzania bezpieczeństwem informacji, zgodnych z normą ISO/IEC 27001, w okresie co najmniej dwóch lat, w tym doświadczenie w zakresie audytowania procesów bezpieczeństwa informacji w organizacjach;			

UWAGA: Dokument należy podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

		- Certified Information Systems Auditor (CISA), - Certified Information Security Manager (CISM), - Certified Information Systems Security Professional (CISSP). 3) certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób (lub równoważny).	2) doświadczenie w realizacji dwóch wdrożeń SZBI w organizacji, obejmujące opracowanie polityk bezpieczeństwa, zarządzania ryzykiem oraz implementację wymagań normy ISO/IEC 27001, w okresie co najmniej dwóch lat			
5.						