

Annex 4 - List of Documents and Information to Confirm Compliance with the Contracting Authority's Qualification, Technical, and Other Requirements/

Додаток 4. - Перелік документів та інформації для підтвердження відповідності кваліфікаційним, технічним та іншим вимогам Замовника

INFORMATION AND DOCUMENTS TO BE SUBMITTED BY BIDDERS TO CONFIRM THEIR COMPLIANCE WITH THE QUALIFICATION CRITERIA AND WITH THE TECHNICAL AND OTHER REQUIREMENTS OF THE CONTRACTING AUTHORITY

ПЕРЕЛІК ІНФОРМАЦІЇ ТА ДОКУМЕНТІВ, ЩО ПОДАЮТЬСЯ УЧАСНИКАМИ ДЛЯ ПІДТВЕРДЖЕННЯ ЙОГО ВІДПОВІДНОСТІ КВАЛІФІКАЦІЙНИМ КРИТЕРІЯМ ТЕХНІЧНИМ ТА ІНШИМ ВИМОГАМ ЗАМОВНИКА

1. Information and documents confirming the bidder's compliance with the qualification criteria established in Article 16 of the Law:

1.1. A free-form certificate confirming that the bidder has the equipment, material and technical resources, and technologies necessary to provide the services that are the subject of procurement, with mandatory indication of the address of the immovable property (Data Processing Center) that the Participant intends to use in delivering these services.

1.2. A free-form certificate confirming the bidder's (subcontractor's) right to provide cloud services using VMware hypervisor software, which the bidder plans to use when delivering the services that are the subject of procurement in Ukraine. To support this, the bidder shall provide a link to the relevant website of the hypervisor software manufacturer, where the participant (subcontractor) must be listed among cloud service provider partners (with a location in Ukraine).

The VMware by Broadcom website (https://expert.broadcom.com/cloud_svcs) must contain confirmation that the participant (subcontractor) holds the status of a VMware Cloud Services Provider partner at a level not lower than PREMIER PARTNER, as well as the Sovereign Cloud status. The Participant's cloud infrastructure must be created in full compliance with the technological, functional, reliability, and fault-tolerance requirements of the VMware by Broadcom reference system architecture and must ensure full and exclusive compliance with Ukrainian legal requirements regarding confidentiality, data location, access, and control in accordance with the Sovereign Cloud Provider program.

A participant that intends to engage a cloud service provider partner as a subcontractor shall additionally submit a copy of a valid agreement with the subcontractor (without confidential information), granting the participant the right to provide the services that are the subject of procurement, including ensuring access to round-the-clock technical support from the hypervisor software manufacturer.

2. Information and documents confirming that the participant's tender proposal meets the required technical, qualitative, and quantitative characteristics of the procurement item:

2.1. A description of the Cloud Data Processing Center (ХЦОД) architecture indicating the hypervisor software and confirming compliance with the technical requirements specified in Annex 3 (Technical requirements) to the tender documentation.

1. Інформація та документи, що підтверджують відповідність учасника кваліфікаційним критеріям, встановленим у статті 16 Закону:

1.1. Довідку в довільній формі про наявність в учасника обладнання, матеріально-технічної бази та технологій, необхідних для надання послуг, які є предметом закупівлі, з обов'язковим зазначенням адреси нерухомого майна (Центру Обробки Даних), яке Учасник планує залучити для надання відповідних послуг.

1.2. Довідку в довільній формі про право учасника (співвиконавця) надавати хмарні послуги з використанням ПЗ гіпервізора VMware, яке учасник планує використовувати при наданні послуг які є предметом закупівлі, на території України. На підтвердження надати посилання на відповідний сайт виробника ПЗ гіпервізора, де серед партнерів-постачальників хмарних сервісів (з локацією в Україні) має бути учасник (співвиконавець).

На сайті VMware by Broadcom (https://expert.broadcom.com/cloud_svcs) повинно бути підтвердження наявності в учасника (співвиконавця) статусу партнера у наданні хмарних послуг (VMware Cloud Services Provider) не нижче PREMIER PARTNER та статусу Sovereign Cloud.

Хмарна інфраструктура Учасника повинна бути створена у повній відповідності до вимог технологічності, функціональності, надійності та відмовостійкості еталонної системної архітектури VMware by Broadcom та забезпечувати повну та виключну відповідність нормам української юрисдикції стосовно конфіденційності, розміщення, доступу та контролю над даними відповідно до вимог програми «Sovereign Cloud Provider».

Учасник, який планує залучити партнера-постачальника хмарних сервісів, як співвиконавця, додатково повинен надати копію чинної угоди з співвиконавцем (без конфіденційної інформації), яка надає учаснику право надавати послуги, які є предметом закупівлі, включаючи забезпечення доступу до цілодобової технічної підтримки виробника програмного забезпечення гіпервізора.

2. Інформація та документи про відповідність тендерної пропозиції учасника необхідним технічним, якісним та кількісним характеристикам предмета закупівлі:

2.1. Опис архітектури ХЦОД з зазначенням ПЗ гіпервізора та підтвердженням технічних вимог, наведених у *додатку 3 (ТЕХНІЧНІ ВИМОГИ)* до тендерної документації.

3. Other:

3.1. A valid Certificate of Conformity for the Comprehensive Information Security System (CISS/KC3I) for the existing cloud infrastructure intended for processing official information. Such cloud infrastructure must belong to the participant and be located in the Data Processing Center at the address indicated in the certificate confirming the availability of equipment, material and technical resources, and technologies required under p. 1.1 of this Appendix, or

a valid organizational and technical solution for deploying a comprehensive information security system of a standard private cloud infrastructure intended for processing official information.

- If the Participant submits a Certificate of Conformity: The CISS Certificate of Conformity must be issued by a business entity holding a license to conduct economic activities in providing services in the field of cryptographic information protection (except electronic digital signature services) and technical information protection, in accordance with the list defined by the Cabinet of Ministers of Ukraine. The contracting authority shall independently verify the validity of the license at: <https://data.gov.ua/dataset/97852d93-dd32-4771-a1a8-351a1fadd0e>.

The participant's existing ICS CISS Certificate may be submitted without the documents that form its integral parts (at the participant's discretion).

To confirm compliance with the technical requirements, the participant shall also provide: the title page of the expert report accompanying the Certificate of Conformity; the pages of the expert report containing information on the location/address of the technical site (DPC) / object of examination (OE); information on the virtualization platform software on which the participant's ICS operates.

The software on which the participant's ICS operates must comply with the requirements of these technical specifications and the participant's tender proposal.

If the pages of the expert report containing the location/address of the technical site (DPC) / OE and/or information on the virtualization platform software include confidential information, such information may be redacted, provided that this does not affect the perception of other essential data required to confirm compliance with procurement requirements.

3.2. A valid positive expert report confirming that the Data Processing Center, whose address is indicated in the certificate regarding the availability of equipment, material and technical resources, and technologies (required under p. 1.1 of this Appendix), or its individual premises (modules), complies with the requirements of technical information protection and is registered with the Administration of the State Service for Special Communications and Information Protection of Ukraine (submitted without the documents that form its integral parts), or

a valid CISS (Comprehensive Information Security System) Certificate of Conformity for the information system of the Data Processing Center (whose address is indicated in the certificate regarding the availability of equipment, material

3. Inше:

3.1. Чинний атестат відповідності комплексної системи захисту інформації (КСЗІ) на існуючу хмарну інфраструктуру для обробки службової інформації. Така хмарна інфраструктура має належати учаснику та розміщуватись в Центрі обробки даних за адресою, яка вказана в довідці про наявність обладнання, матеріально-технічної бази та технологій, надання якої вимагається в п.1.1 цього додатку або

чинне організаційно-технічне рішення на розгортання комплексної системи захисту інформації типової приватної хмарної інфраструктури для обробки службової інформації.

- у випадку надання Учасником Атестації відповідності:

Атестат відповідності КСЗІ має бути виданий суб'єктом господарювання, що має ліцензію на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України. Замовник самостійно перевіряє чинність ліцензії суб'єкта господарювання за посиланням <https://data.gov.ua/dataset/97852d93-dd32-4771-a1a8-351a1fadd0e>.

Атестат відповідності КСЗІ на існуючу ІКС учасника може надаватися без документів, які є його невід'ємною частиною (на розсуд учасника).

Також, на підтвердження відповідності вимог технічного завдання, учасник повинен надати титульну сторінку експертного висновку до наданого атестації відповідності, сторінки експертного висновку, на яких зазначено інформацію, про місцезнаходження/місцезнаходження технічного майданчика (ЦОД)/об'єкта експертизи (ОЕ) та інформацію про програмне забезпечення платформи віртуалізації на базі якого функціонує ІКС учасника. Програмне забезпечення на базі якого функціонує ІКС учасника повинно відповідати вимогам даного технічного завдання та тендерної пропозиції учасника. В разі якщо на сторінках експертного висновку, на яких зазначено інформацію, про місцезнаходження/місцезнаходження технічного майданчика (ЦОД)/об'єкта експертизи (ОЕ) та інформації про програмне забезпечення платформи віртуалізації на базі якого функціонує ІКС учасника міститься конфіденційна інформація, вона може бути прихована (заретушована) у наданих документах за умови, що це не вплине на сприйняття інших суттєвих даних, необхідних для підтвердження відповідності вимогам закупівлі.

3.2. Чинний позитивний експертний висновок про відповідність Центру обробки даних, адреса якого вказана в довідці про наявність обладнання, матеріально-технічної бази та технологій (надання якої вимагається в п.1.1 цього додатку) або його окремих приміщень (модулів) вимогам технічного захисту інформації, зареєстрований в Адміністрації Державної служби спеціального зв'язку та захисту інформації України (без документів, які є його невід'ємною частиною) або чинний атестат відповідності КСЗІ на інформаційну систему Центру Обробки Даних, (адреса якого вказана в довідці про наявність обладнання, матеріально-технічної бази та технологій, надання якої вимагається в п.1.1 цього додатку), який засвідчує, що КСЗІ

and technical resources, and technologies required under p. 1.1 of this Appendix), confirming that the CISS of the information and communication system of this Data Processing Center complies with the requirements of regulatory documents on technical information protection. The CISS Certificate of Conformity may be submitted without the documents that form its integral parts (at the participant's discretion).

The participant shall also provide the pages of the expert report containing information on the location/address of the technical site (DPC) / object of examination (OE). If these pages contain confidential information, such information may be concealed (redacted) in the submitted documents, provided that this does not affect the perception of other essential data required to confirm compliance with procurement requirements.

The participant shall provide the pages of the expert report indicating that the following subsystems are included in the certified ICS:

- access control system;
- video surveillance system;
- engineering infrastructure monitoring system (air conditioners, UPS units, temperature sensors);
- diesel generator monitoring system;
- fire alarm system and automatic gas fire extinguishing system;
- network equipment complex.

3.3. Copies of valid certificates confirming compliance of the Participant's information security management systems and personal data management systems with the requirements of the international standard ISO/IEC 27001:2022 or ISO/IEC 27001:2013 extended by ISO/IEC 27701:2019, issued for the provision of cloud services or cloud provider services to clients. Such certificates must be issued by a conformity assessment body accredited by an accreditation authority that is a member of the IAF (International Accreditation Forum).

3.4. Copies of valid certificates confirming compliance with international standards in the field of cloud computing — ISO/IEC 27017:2015 and ISO/IEC 27018:2019. These certificates must be issued in the Participant's name.

інформаційно-комунікаційної системи даного ЦОД відповідає вимогам нормативних документів з технічного захисту інформації.

Атестат відповідності КСЗІ може надаватися без документів, які є його невід'ємною частиною (на розсуд учасника).

Також учасник повинен надати сторінки експертного висновку, на яких зазначено інформацію, про місцезнаходження/місцезнаходження технічного майданчика (ЦОД)/об'єкта експертизи (ОЕ). В разі якщо на сторінках експертного висновку, на яких зазначено інформацію, про місцезнаходження /місцезнаходження технічного майданчика (ЦОД)/об'єкта експертизи (ОЕ) міститься конфіденційна інформація, вона може бути прихована (заретушована) у наданих документах за умови, що це не вплине на сприйняття інших суттєвих даних, необхідних для підтвердження відповідності вимогам закупівлі.

Учасник повинен надати сторінки експертного висновку, на яких зазначено що до складу даної атестованої ІКС, входять наступні підсистеми:

- система контролю доступу;
- система відеоспостереження;
- система моніторингу інженерної інфраструктури (кондиціонери, ДБЖ, датчики температури);
- система моніторингу дизель-генераторів;
- система пожежної сигналізації та система автоматичного газового пожежогасіння;
- комплекс мережевого обладнання.

3.3. Копії чинних сертифікатів відповідності вимогам міжнародного стандарту ISO/IEC 27001:2022 або ISO/IEC 27001:2013 в розширеній редакції ISO/IEC 27701:2019 систем управління інформаційною безпекою Учасника та систем управління персональними даними для надання клієнтам хмарних сервісів або послуг хмарного провайдера Учасника, виданих органом з оцінки відповідності, що акредитований одним з органів акредитації. Орган акредитації повинен бути членом IAF (International Accreditation Forum).

3.4. Копії чинних сертифікатів відповідності вимогам міжнародних стандартів у сфері хмарних обчислень ISO/IEC 27017:2015 та ISO/IEC 27018:2019. Такі сертифікати повинні бути видані на ім'я Учасника.