|  |  |
| --- | --- |
|  |  |
| MALTA FINANCIAL SERVICES AUTHORITY |
| **Authorisation Forms - Annex** |
|  |

|  |
| --- |
| **Annex AX50: ICT Third-Party Service Provider** |
|  |
| **High Level Guidelines** |
|  |
|  |
| 1. **General**   This form, **Annex AX[XX]:** **ICT Third-Party Provider Assessment** (‘Annex’), shall be duly filled in by persons wishing to obtain authorisation from the MFSA to carry out financial services activities. This Annex shall be submitted as part of and in conjunction with the relevant Authorisation Application Form, as indicated therein.  This Annex primarily aims to capture relevant information in relation to the Applicant’s arrangement with an ICT third-party service provider (‘ICT TPP’) for ICT Services supporting a critical or important function, or material parts thereof. This Annex shall be completed for each arrangement held, or intended to be held.  In this respect, the Applicant shall to the best of its knowledge, provide information, which is truthful, accurate and complete. The Applicant shall notify the MFSA immediately if the information provided changes in any material respect either prior to or subsequent to authorisation.  The Applicant is required to make reference, and where applicable comply with, the relevant Act, the Regulations made, or Rules issued thereunder during the completion of the Application or Notification Process. The Applicant shall also refer to the respective National and/or European Regulatory Frameworks or other binding regulation as may be applicable.  The Applicant shall not tamper with, or modify in any manner, this Annex or its respective Application. Should it transpire that the documents were tampered with, or modified in any manner, the Authority shall consider the submission to be invalid. Any suggestion regarding potential improvements should be communicated to the MFSA for consideration.  The Authority may at its sole discretion request from the Applicant further information/ documentation.   1. **Definitions**   For completion of this Annex, definitions specified in Regulation (EU) 2022/2554 of the European Parliament and of the Council on 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter referred to as ‘the DORA Regulation’), shall be referred to. If not specified in the mentioned regulation, terms used in this Annex shall have the same meaning assigned to them within the respective sector application form.   |  |  |  | | --- | --- | --- | |  |  |  | | **‘ICT Third-Party Service Provider’** | | means an undertaking providing ICT services. | |  | |  | | **‘ICT Services’** | | means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services; | | **‘Critical or important function’** | | | means a function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law. |  1. **Instructions**   In order for this Annex to be considered complete, the Applicant is required to complete all the respective sections under this Annex. It is noted that the information provided should reflect the Applicant’s structure and method of operations at time of authorisation.   1. **Privacy Notice**   The MFSA ensures that any processing of personal data is conducted in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation), the Data Protection Act (Chapter 586 of the Laws of Malta) and any other relevant European Union and national law. For further details, you may refer to the MFSA Privacy Notice available on the MFSA webpage <https://www.mfsa.mt/privacy-notice/>. |

| 1. Applicant | | |
| --- | --- | --- |
|  | **Applicant – Identification Details** | |
|  | Registered Name  *(if not yet Formed, provide proposed full legal name)* | Enter text |
|  | Registered Number (*if applicable)* | Enter text |
|  | AU Person Code  (*if applicable)* | Enter text |

| 1. ICT TPP and Chain of Subcontracting | | | |
| --- | --- | --- | --- |
|  | ICT TPP and Chain of Subcontracting | | | |
|  | Registered Name of the direct ICT TPP | Enter text | |
|  | Identification Code (*LEI Code or EUID*) of the direct ICT TPP | Enter text | |
|  | Is the contractual arrangement with the direct ICT TPP considered intra-group? | | Select item |
|  | Provide a brief explanation on the rationale to classify the function(s) supported by the ICT TPP(s) as critical or important. | | |
|  | Enter text | | |
|  | Exhaustively define all ICT Services provided by the direct ICT TPP. | | |
|  | Enter text | | |
|  | Does the arrangement with the direct ICT TPP permit for the delegation of the provision of ICT service(s) supporting a critical or important function, or material parts thereof, to a subcontractor(s)? | | Select item |
|  | If ‘Yes’ to the above, has the Applicant identified all subcontractors supporting the ICT TPP with the provision of the ICT service(s), and whose disruption would impair the security or the continuity of the service provision?  Select item | | |
|  | Enter text | | |
|  | Will data be processed and stored at the direct ICT TPP, or any of the subcontractors in the supply chain? | | Select item |
|  | Has the Applicant ensured that, at all times, it shall maintain full responsibility of compliance with, and discharge of, all obligations of the DORA Regulation and the applicable legislative framework? | | Select item |

| 1. Preliminary Assessment | | | |
| --- | --- | --- | --- |
|  | **Risk Assessment** | | | |
|  | Prior to entering the contractual arrangement with the direct ICT TPP, has the Applicant: | | | |
|  | assessed if supervisory conditions for contracting are met? | Select item | | |
|  | identified and assessed all relevant risks in relation to the contractual arrangement? | Select item | | |
|  | undertaken the necessary due diligence processes? | Select item | | |
|  | identified and assessed conflicts of interest that the contractual arrangement may cause? | Select item | | |
|  | Thoroughly explain the results of the risk assessment performed on the potential impact the contractual arrangement with the ICT TPP, for the provision of ICT Services supporting critical or important function, could have on the Applicant and all of its risks. | | | |
|  | Enter text | | | |
|  | Does the above risk assessment consider, as applicable, the impact of the contractual arrangement on the Applicant’s: | | | |
|  | Operational Risks | Select item | |
|  | Legal Risks | Select item | |
|  | ICT Risks | Select item | |
|  | Reputational Risks | Select item | |
|  | Risks to the protection of confidential or personal data | Select item | |
|  | Risks linked to the availability of data | Select item | |
|  | Risks linked to where the location of the data is processed and stored | Select item | |
|  | Risks linked to where the location of the data is processed and stored | Select item | |
|  | ICT Concentration Risks | Select item | | |
|  | Explain the measures implemented for the mitigation of the risks identified to emanate/be effected as a result of the arrangement with the ICT TPP. | | | | |
|  | Enter text | | | | |
|  | Explain as to how the Applicant intends to conduct ongoing monitoring of the third-party service provider’s performance, for assurance of effectiveness of the implemented risk mitigating measures on a continuous basis. | | | | |
|  | Enter text | | | | |
|  | Should the contractual arrangement with the direct ICT TPP for ICT services supporting critical or important function permit for sub-contracting, does the Applicant’s process include additional steps to assess risks: | | | | |
|  | associated with an ICT subcontractor established in a third-country? | | Select item | |
|  | associated with insolvency law provisions that would apply in the event of the ICT TPP’s bankruptcy? | | Select item | |
|  | associated with constraints that may arise in respect to the urgent recovery of your data? | | Select item | |
|  | associated with monitoring (including compliance) potentially long or complex chains of subcontracting? | | Select item | |
|  | **Conflicts of Interest** | | | | |
|  | Has the Applicant identified conflicts of interests as a result of the contractual arrangement with the ICT TPP. | | Select item | |
|  | If ‘Yes’ to the above, define the identified conflicts of interests including the implemented mitigating measures. | | | | |
|  | Enter text | | | | |
|  | **Due Diligence** | | | | |
|  | Outline the proportionate due diligence process conducted by the Applicant on the ICT TPP, including considered characteristics, to ensure its suitability. | | | | |
|  | Enter text | | | | |

| 1. Business Continuity, Termination and Exit Strategies | |
| --- | --- |
|  | **Business Continuity** |
|  | Exhaustively define the business continuity plan established and documented by the Applicant for the ICT Services supporting critical or important functions and provided by the direct ICT TPP. |
|  | Enter text |
|  | **Exit Strategy and Termination Clauses** |
|  | Exhaustively define the termination terms established and documented by the Applicant for the ICT Services supporting critical or important functions and provided by the direct ICT TPP. |
|  | Enter text |
|  | Exhaustively define the exit plan established and documented by the Applicant for the ICT Services supporting critical or important functions and provided by the direct ICT TPP. |
|  | Enter text |

| 1. Written Contractual Obligations | | |
| --- | --- | --- |
|  | **Key Contractual Provisions** | | |
|  | Does the written contractual arrangement with the direct ICT TPP include: | | |
|  | clearly stated and written rights and obligations? | Select item |
|  | full-service level descriptions, including quantitative and qualitative performance targets within the agreed service levels? | Select item |
|  | effective monitoring to enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met? | Select item |
|  | complete description of all ICT services to be provided by the ICT TPP? | Select item |
|  | tolerance and conditions of subcontracting of an ICT service supporting a critical or important function? | Select item |
|  | data and service locations, including the ICT TPP’s obligation to notify of changes of such locations? | Select item |
|  | provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data? | Select item |
|  | obligation of the ICT TPP to provide assistance in case of an ICT-related incident related to the service provider? | Select item |
|  | obligation of the ICT TPP to fully cooperate with Competent Authorities and resolution authorities? | Select item |
|  | provisions on termination rights and related minimum notice periods for the termination of the contractual arrangements? | Select item |
|  | conditions for the participation of ICT TPP in ICT security awareness programs and digital operational resilience training? | Select item |
|  | reporting obligations of the ICT TPP to notify the Applicant of any material changes in the ICT services supporting critical or important functions? | Select item |
|  | requirements for the ICT TPP to implement and test business contingency plans? | Select item |
|  | requirements for the ICT TPP to have in place ICT security measures, tools and policies? | Select item |
|  | obligation of the ICT TPP to participate and fully cooperate in the Applicant’s TLPT, if it is the case? | Select item |
|  | rights of access? | Select item |
|  | inspection and audit rights by the Applicant, or an appointed third party, or the Competent Authority? | Select item |
|  | the obligation for the ICT TPP to fully cooperate during the onsite inspections and audits? | Select item |
|  | exit strategies that define a feasible transition period during which the ICT TPP will continue providing the respective ICT services? | Select item |
|  | exit strategies that define a feasible transition period which allow you to fully migrate to another provider or on-prem? | Select item |
|  | When negotiating contractual arrangements, are standard contractual clauses developed by public authorities made use of? | Select item |