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

|  |
| --- |
| **Annex AX05: Extended ICT Questionnaire** |
|  |
| **High Level Guidelines** |
|  |
|  |
| 1. **General**   This form, **Annex AX05:** **Extended ICT Questionnaire** (‘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 Information and Communications Technology (‘ICT’) infrastructure and arrangements.  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. 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 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**   Unless otherwise specified, terms used in this Annex shall have the same meaning assigned to them within the respective Application.   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 Details | | |
| --- | --- | --- |
|  | **Applicant – Identification Details** | |
|  | Registered Name  *(if not yet Formed, provide proposed name)* | Enter text |
|  | Registered Number (*if applicable)* | Enter text |
|  | LEI Code  (*if applicable)* | Enter text |

| 1. Operational and ICT | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **ICT Governance and Strategy (GAS)** | | | | | | | |
|  | Is the Applicant's ICT Strategy aligned with the overall business strategy? | | | | | | | Select item |
|  | How will the Applicant ensure that its resources (human, physical capital / financial, technology) are adequate to support the ICT operational needs and ICT and security risk management processes? | | | | | | | |
|  | Enter text | | | | | | | |
|  | Will the established function include a designated person responsible for inter alia establishing, maintaining and overseeing the internal cybersecurity? | | | | | | | Select item |
|  | If ‘*No*’: Explain what measures will be put in place by the Applicant to ensure adequate oversight of the internal cybersecurity. | | | | | | | |
|  | Enter text | | | | | | | |
|  | **ICT Function** | | | | | | | |
|  | **ICT Function** | | | | | | | |
|  | Does the Applicant have, or intend to establish, an ICT function? | | | | | | | Select item |
|  | If ’*Yes*’: Provide an overview of the structure of the Applicant's ICT Function, including its resources and respective reporting lines, in line with the proposed volume and value of business being proposed. | | | | | | | |
|  | Enter text | | | | | | | |
|  | **Third-Party Outsourcing** | | | | | | | |
|  | Does the Applicant intend to outsource any critical or important ICT systems, services, processes or functions to a Third-Party Outsourcing Provider? | | | | | | | Select item |
|  | If ‘*Yes’*: Identify the Third-Party Outsourcing Provider/s. | | | | | | | |
|  | |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  | | --- | --- | | 1. Third-Party Outsourcing Provider | | | Name of Third-Party Outsourcing Provider | Enter text | | Registration number  *(if applicable)* | Enter text | |  | | |   *(Add multiple as applicable)* | | | | | | | |
|  | **Attachment | MFSA Annex – AX03** | | | | | | | |
|  | **ICT Function Holder**  *This sub-section is only applicable if the Applicant has or intends to establish an ICT Function.* | | | | | | | |
|  | **Identification** | | | | | | | |
|  | Title | | Select item | | | | | |
|  | Name | | Enter text |  | Surname | Enter text | | |
|  | Date of Birth | | Enter date | | | | | |
|  | Identification Document (‘ID’) Type | | Select item |  | ID Number | Enter text | | |
|  | ID Expiry Date | | Enter date |  | Country of Issuance | Select country | | |
|  | MFSA PQ Code | | Enter text | | | | | |
|  | **Other Positions** | | | | | | | |
|  | Does the IT Function Holder hold or intend to hold any other positions within the Applicant? | | | | | | | Select item |
|  | If ‘*Yes*’: Provide an explanation on the nature of the position/s | | | | | | | |
|  | Enter text | | | | | | | |
|  | **ICT Systems Acquisition and Development (SAD)** | | | | | | | |
|  | Will the Applicant's core software application be developed in-house or acquired? | | | | | | | Select item |
|  | If ‘*Developed in-house’*: Provide details regarding the segregation of the production environment from development, testing and other non-production environments | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to test the integrity of its core software application before use and after deployment on a continuous basis? | | | | | | | |
|  | Enter text | | | | | | | |
|  | **Technology Arrangements** | | | | | | | |
|  | Will the Applicant's business model utilise any type of innovative technology, including but not limited to, those listed in Question 2.5.2?[[1]](#footnote-2) | | | | | | Select item | |
|  | If ‘*Yes*’: Specify which of the following innovative technologies are being utilised | |  |  | | --- | --- | |  |  | | Application Programming Interface (APIs) | Select item | | Artificial Intelligence (AI) | Select item | | Big Data | Select item | | Biometrics | Select item | | Cloud Computing | Select item | | Data Analytics | Select item | | Deep Learning | Select item | | Distributed Ledger Technology (DLT) | Select item | | Internet of Things | Select item | | Machine Learning | Select item | | Natural Language Processing | Select item | | New Encryption Methodologies | Select item | | Quantum Computing | Select item | | Smart Contracts | Select item | | Robotic Process Automation | Select item | | Other (specify) | |  | | --- | | Enter text | |  | | *(Add multiple as applicable)* | | |  |  | | | | | | | |
|  | Provide details of how these innovative technologies are being utilised | | | | | | | |
|  | Enter text | | | | | | | |
|  | What are the technology arrangements (network, systems, applications, ICT security tools and cloud services) the Applicant will put in place? | | | | | | | |
|  | Enter text | | | | | | | |
|  | How will the Applicant's technology arrangements interface with customers? | | | | | | | |
|  | Enter text | | | | | | | |
|  | **ICT and Security Risk Management** | | | | | | | |
|  | **ICT Risk Management (RM)** | | | | | | | |
|  | Has the Applicant established a comprehensive risk management framework that includes the mechanism for the management of ICT and Security Risk? | | | | | | | Select item |
|  | Will the Applicant manage its ICT and Security Risks by applying the three lines of defence or a similar internal control framework? | | | | | | | Select item |
|  | If ‘*No’:* Outline alternative arrangement(s) the Applicant will put in place | | | | | | | |
|  | Enter text | | | | | | | |
|  | Has the Applicant conducted a preliminary ICT Risk Assessment/ICT Audit on its governance, systems and processes for its ICT and security risks? | | | | | | | Select item |
|  | Will the Applicant have measures and/or mechanisms in place to ensure adequate and continuous monitoring of cybersecurity threats and vulnerabilities? | | | | | | | Select item |
|  | Has the Applicant identified an internal auditor(s) with sufficient knowledge, skills and expertise in ICT and security risks, to provide independent assurance to the Applicant's management body? | | | | | | | Select item |
|  | **Information Security (ISE)** | | | | | | | |
|  | Are there any plans to align the information security framework with any internationally recognised standard/framework? | | | | | | | Select item |
|  | Will the Applicant establish an information security policy based on its predefined information security objectives? | | | | | | | Select item |
|  | What measures will the Applicant put in place to ensure that the function responsible for ICT security is segregated from its ICT operations and processes? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures and/or mechanism will the Applicant put in place to ensure that physical access to ICT systems is controlled and restricted? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures and/or mechanism will the Applicant put in place to ensure that logical access to ICT systems is controlled and restricted? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What encryption techniques will the Applicant adopt to provide data integrity and confidentiality of information? | | | | | | | |
|  | Enter text | | | | | | | |
|  | If the Applicant is utilising Application Programming Interface (API) to inter-operate with third-parties, what mechanisms and/or measures will the Applicant put in place to ensure security and protection of the API connections? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to prevent the occurrence of security breaches on ICT systems and services? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to protect ICT systems against malware and/or other security threats? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to ensure adequate monitoring and response to security events within the established Incident management framework? | | | | | | | |
|  | Enter text | | | | | | | |
|  | Will the Applicant implement and/or establish an information security testing framework to validate its cybersecurity posture? | | | | | | | Select item |
|  | If ‘*Yes’:* provide details on the testing framework. | | | | | | | |
|  | Enter text | | | | | | | |
|  | Will the Applicant put in place specific ICT security training and awareness campaigns/programmes? | | | | | | | Select item |
|  | Will the Applicant establish a digital platform? | | | | | | | Select item |
|  | If ‘*Yes’*: Provide the following details: | | | | | | | |
|  | 1. Explain the purpose of such platform. | | | | | | | |
|  | Enter text | | | | | | | |
|  | 1. How will the Applicant prevent unauthorised access to its platform? | | | | | | | |
|  | Enter text | | | | | | | |
|  | 1. What measures will the Applicant put in place to ensure users are aware and guided against security risks linked to its platform? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What processes and procedures would be in place in the event that security controls are not compatible with Third-Party Outsourcing Providers, as applicable? | | | | | | | |
|  | Enter text | | | | | | | |
|  | **ICT Operations Management (IOM)** | | | | | | | |
|  | Will the Applicant's incident management framework include provision on incident reporting to the Competent Authority? | | | | | | | Select item |
|  | **Business Continuity Management (BCM)** | | | | | | | |
|  | Has the Applicant established an ICT continuity policy as part of its Business Continuity Policy (BCP)? | | | | | | | Select item |
|  | Does the Applicant's BCP include identification of the data and ICT systems backup and restoration procedures, secondary/backup location, back-up site, access to ICT infrastructure, and the key software? | | | | | | | Select item |
|  | Has the Applicant conducted a potential business impact analysis (BIA) in order to assess its exposure to severe business disruptions and to assess their potential impact on the Applicant's future performance? | | | | | | | Select item |
|  | As part of the BCP, has the Applicant established a Recovery Time Objective (RTO) and a Recovery Point Objective (RPO)? | | | | | | | Select item |
|  | Will the secondary location for disaster recovery be located in a remote site different from the primary location? | | | | | | | Select item |
|  | **Attachments** | | | | | | | |
|  | **Attachment | Enterprise ICT Architecture Diagram** | | | | | | | |
|  | **Trading Platform**  *This Section is only applicable if the Applicant is implementing a Trading Platform / system.* | | | | | | | |
|  | Will the Applicant use a proprietary online trading platform or will this be developed in-house or acquired? | | | | | | | Select item |
|  | Please provide relevant details. | | | | | | | |
|  | Enter text | | | | | | | |
|  | Will the Applicant's core systems used for trading be developed in-house or outsourced? | | | | | | | Select item |
|  | If ‘*Outsourced*’: Explain how the Applicant will ensure it has access rights and audit rights to the core system. | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to ensure security of transmitted messages during trading? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to ensure effective monitoring of trading data during trading? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to ensure there is an appropriate testing of its trading algorithms and facilities? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to ensure that all employees are provided with necessary training on the trading platforms to be offered to the clients? | | | | | | | |
|  | Enter text | | | | | | | |
|  | What measures will the Applicant put in place to sufficiently deal with peak order and messages volumes during trading? | | | | | | | |
|  | Enter text | | | | | | | |

1. Where applicable, reference is to be made to the definitions falling within scope of the Innovative Technology Arrangements and Services Act (Chapter 592 of the Laws of Malta) and any Regulations issued thereunder. [↑](#footnote-ref-2)