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

|  |
| --- |
| **Annex AX04: ICT and Security Risk Assessment** |
|  |
| **High Level Guidelines** |
|  |
|  |
| 1. **General**

This form, **Annex AX04:** **ICT and Security Risk 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 Information and Communications Technology (‘ICT’) infrastructure and arrangements, including the management of ICT and security risk management and outsourcing 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 Acts, 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
 |
| --- |
| * 1. #
 | **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 Governance and Strategy
 |
| --- |
|  | **ICT Governance and Strategy**  |
|  | Is the Applicant's ICT Strategy aligned with the overall business strategy? | Select item |
|  | Thoroughly define the Applicant’s ICT Strategy. |
|  | Enter text |
|  | Define the Applicant’s implemented action plans and measures to acquire the objectives of the ICT Strategy.  |
|  | Enter text |
|  | 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 |
|  | How has the Applicant ensured that at least at Senior Management Level, including the Management Body, have sufficient ICT risk and information security knowledge, skills and expertise to establish an effective ICT and security risk management framework. |
|  | Enter text |
|  | Will members of the management body receive regular training about ICT and security risk management and information security? | Select item |
|  | **ICT and Security Risk Management**  |
|  | **Governance Arrangements** |
|  | Does the Applicant intend to adopt a Three Lines of Defence Model to identify and manage their ICT and security risks? | Select item |
|  | If ‘*No*’: Outline alternative arrangement(s) the Applicant will put in place |
|  | Enter text |
|  | If a Three Lines of Defence Model is adopted, what measures will the Applicant put in place to ensure that all functions are segregated and act independently? |
|  | Enter text |
|  | How has the Applicant ensured that sufficient ICT risk and Information Security knowledge, skills and expertise are held across all ICT operational, control and internal audit functions to establish an effective ICT and security risk management framework. |
|  | Enter text |
|  | **ICT Operational Function (1LoD)** |
|  | Does the Applicant have, or intend to establish, an ICT Operational Function? | Select item |
|  | If ’*Yes*’: Provide an overview of the structure of the Applicant's ICT Operational Function, including its resources and respective reporting lines, arrangements with ICT Third-Party Providers (if applicable), in line with the proposed volume and value of business being proposed. |
|  | Enter text |
|  | Define the roles and responsibilities assigned to the ICT Operational Function.  |
|  | Enter text |
|  | **ICT Operational Function Holder***This sub-section is only applicable if the Applicant has or intends to establish an ICT Operational Function.* |
|  | Title | Select item |
|  | Name | Enter text |  | Surname | Enter text |
|  | Does the IT Operational Function Holder hold or intend to hold any other positions within the Applicant? | Select item |
|  | Does the IT Operational 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 |
|  | Is the Applicant’s ICT Operational Function Holder acting for and on-behalf of an ICT Third-Party Provider? | Select item |
|  | **ICT Control Function (2LoD)** |
|  | Does the Applicant have, or intend to establish, an ICT Control Function? | Select item |
|  | If ’*Yes*’: Provide an overview of the structure of the Applicant's ICT Control Function, including its resources and respective reporting lines, arrangements with ICT Third-Party Providers (if applicable), in line with the proposed volume and value of business being proposed. |
|  | Enter text |
|  | Define the roles and responsibilities assigned to the ICT Control Function.  |
|  | Enter text |
|  | **ICT Control Function Holder***This sub-section is only applicable if the Applicant has or intends to establish an ICT Control Function.* |
|  | Title | Select item |
|  | Name | Enter text |  | Surname | Enter text |
|  | Does the ICT Control 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 |
|  | Is the Applicant’s ICT Control Function Holder acting for and on-behalf of an ICT Third-Party Provider? | Select item |
|  | **Internal Audit Function (3LoD)** |
|  | Does the Applicant have, or intend to establish, an Internal Audit Function? | Select item |
|  | If ’*Yes*’: Provide an overview of the structure of the Applicant's Internal Audit Function, including its resources and respective reporting lines, arrangements with ICT Third-Party Providers (if applicable), in line with the proposed volume and value of business being proposed. |
|  | Enter text |
|  | **ICT Internal Auditor Function Holder***This sub-section is only applicable if the Applicant has or intends to establish an ICT Internal Audit Function.* |
|  | Title | Select item |
|  | Name | Enter text |  | Surname | Enter text |
|  | Does the ICT Internal Audit Function Holder hold or intend to hold any other positions within the Applicant? | Select item |
|  | Does the ICT Internal Audit 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 |
|  | Is the Applicant’s ICT Internal Audit Function Holder acting for and on-behalf of an ICT Third-Party Provider? | Select item |
|  | **Information Security Function** |
|  | Does the Applicant intend to establish an Information Security Function? | Select item |
|  | If ’*Yes*’: Provide an overview of the structure of the Applicant's Information Security Function, including its resources and respective reporting lines, arrangements with ICT Third-Party Providers (if applicable), in line with the proposed volume and value of business being proposed. |
|  | Enter text |
|  | **ICT and Security Risk Management Framework** |
|  | Provide a thorough overview of the ICT and security risk management framework, and respective processes, that the Applicant has implemented to identify and manage its ICT and security risks.  |
|  | Enter text |
|  | Does the management body define, approve, oversee and act responsible for the implementation and changes of the Applicant’s ICT and Security Risk Management Framework, including any strategies, policies, procedures, plans and mechanisms issued thereunder? | Select item |
|  | **ICT and Security Risks Identification, Control and Monitoring**  |
|  | Has the Applicant established and defined its risk appetite for ICT and security risks? | Select item |
|  | Has the Applicant conducted a preliminary risk assessment to identify all ICT and security risks that it is exposed too? |
|  | Enter text |
|  | Does the above-mentioned assessment also consider risks stemming from outdated or unsupported ICT Assets? |
|  | Enter text |
|  | Does the above-mentioned assessment also consider risks stemming from outsourcing arrangements with ICT Third-Party Providers, including sub-outsourcing? |
|  | Enter text |
|  | As part of the ICT and security risk management framework has the Applicant identified, documented and mapped the following: |
|  | 1. all ICT supported business functions, including roles and supporting processes?
 | Select item |
|  | 1. all information and ICT assets supporting the above-mentioned business functions and supporting processes?
 | Select item |
|  | Has the Applicant classified, according to criticality, the identified business functions, supporting process, information and ICT assets? | Select item |
|  | Has the Applicant identified, documented and mapped the ICT and security risks, that it is exposed too, and that impact the identified and classified business functions, supporting processes, information assets and ICT assets (according to their criticality)? | Select item |
|  | Provide a thorough overview of the measures that the Applicant has implemented to mitigate all ICT and security risks that it is exposed too.  |
|  | Enter text |
|  | Define the measures and/or mechanisms that the Applicant will have in place to ensure adequate and continuous monitoring of cybersecurity threats and vulnerabilities. |
|  | Enter text |
|  | For the purpose of ICT and security risk identification, control and monitoring has the Applicant developed a register/inventory that it intends to keep updated? | Select item |
|  | **Attachment | ICT and Security Risk Register / Inventory***(If the answer is ‘Yes’ to Q2.2.9.10****)*** |

|  |
| --- |
| 1. Information Security
 |
|  | **Information Security** |
|  | Explain whether there are any plans to align the information security framework with any internationally recognised standard/framework. |
|  | Enter text |
|  | Will the Applicant establish an information security policy and procedures based on its predefined information security objectives? | Select item |
|  | **Attachment | Information Security Policy***(If the answer is ‘Yes’ to Q3.1.1.3****)*** |
|  | Thoroughly define the implemented measures and/or mechanism that the Applicant put in place to ensure physical security from unauthorised access and environmental hazards.  |
|  | Enter text |
|  | Thoroughly define the implemented measures and/or mechanism that the Applicant put in place to ensure logical security (identity and access management) from unauthorised access. |
|  | Enter text |
|  | Thoroughly define the encryption techniques the Applicant will adopt to preserve the availability, authenticity, integrity, and confidentiality of data (at rest, in transit or in use). |
|  | Enter text |
|  | What ICT security monitoring tools and/or measures will the Applicant put in place to prevent the occurrence of security breaches on ICT systems and services? |
|  | Enter text |
|  | What ICT security monitoring tools and/or measures will the Applicant put in place to protect ICT systems against malware and/or other security threats? |
|  | Enter text |
|  | Describe the logging procedures, protocols and tools that the Applicant has implemented. |
|  | Enter text |
|  | Describe the procedures and tools that the Applicant has implemented for vulnerability and patch management. |
|  | Enter text |
|  | Does the Applicant make use of automated mechanisms to isolate affected information assets in the event of cyber-attacks? | Select item |
|  | Are all changes to ICT systems recorded, tested, assessed, approved, implemented and verified in a controlled manner? | Select item |
|  | What processes and procedures would be in place to ensure that ICT third-party providers are aligned with the Applicant’s information security objectives?  |
|  | 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 |

|  |
| --- |
| 1. ICT Operations
 |
|  | **ICT Asset Management**  |
|  | Does the Applicant have in place an up-to-date inventory of all ICT assets (whether implemented on premises or in the cloud, and whether owned or leased)? | Select item |
|  | If ‘Yes’ to the above, select which of the below information can be promptly extracted from the ICT Asset inventory:  |
|  | ICT Asset Identification  | Select item |
|  | ICT Asset Location | Select item |
|  | ICT Asset Security Classification | Select item |
|  | ICT Asset IP Addresses(es) (if applicable) | Select item |
|  | ICT Asset Owner | Select item |
|  | Distinction whether ICT Asset is owned or leased | Select item |
|  | Links and interdependencies between the different ICT Assets  | Select item |
|  | Will the Applicant review the ICT asset inventory on a periodical basis, and every time there is a major change? | Select item |
|  | Define the measures implemented by the Applicant to monitor and manage the life cycle of ICT Assets to ensure that they continue to meet and support business and risk management requirements. |
|  | Enter text |
|  | **ICT Incident and Problem Management** |
|  | Has the Applicant established an incident and problem management process?  | Select item |
|  | If ‘Yes’ to the above, provide a thorough overview of the established process.  |
|  | Enter text |
|  | Has the Applicant defined and determined criteria and thresholds for classifying an event as an operational or security incident, or as an early warning indicator?  | Select item |
|  | Define the mechanisms and/or tools implemented by the Applicant to detect ICT-related incidents and/or early warning indicators.  |
|  | Enter text |
|  | Do the detection mechanisms and/or tools, referred to above, include alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alerts to staff in charge? | Select item |
|  | Are the detection mechanism and/or tools regularly tested? | Select item |
|  | Does the incident management processes cater for follow-up of ICT-related incidents to ensure that root causes are identified, documented and addressed to prevent re-occurrence? | Select item |
|  | Will the Applicant's ICT-related incident management framework include provision on incident reporting to the Competent Authority? | Select item |
|  | Are all ICT-related incidents and significant cyber-threats recorded? | Select item |

|  |
| --- |
| 1. ICT Project and Change Management
 |
|  | **ICT Project and Change Management** |
|  | Will the Applicant implement an ICT Projects Management Framework? | Select item |
|  | 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 |

|  |
| --- |
| 1. Business Continuity Management
 |
|  | **Business Continuity Management**  |
|  | Has the Applicant conducted a business impact analysis (BIA) to assess its exposure to severe business disruptions and their potential impact on the Applicant's future performance? | Select item |
|  | For conducting the BIA, has the Applicant considered the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies? | Select item |
|  | Has the Applicant established and documented ICT Business Continuity Plans (BCPs)? | Select item |
|  | Has the Applicant established and documented ICT Disaster Response and Recovery Plans (DRPs)? | Select item |
|  | Were the results of the BIA taken into consideration when establishing and documenting the Applicant’s ICT BCPs and DRPs?  | Select item |
|  | Do the Applicant’s ICT BCPs cater for scenarios of potential disruptions or failure of ICT Functions that are outsourced and relate to a critical or important function? | Select item |
|  | Provide a thorough overview of the Applicant’s established and documented BCPs and DRPs, including Recovery Time Objectives (RTOs) and a Recovery Point Objective (RPOs) and crisis communication plans.  |
|  | Enter text |
|  | 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 |
|  | Define the Applicant’s implemented data and ICT systems backup and restoration arrangements, including as to how the Applicant has ensured that the secondary site is adequately remote from the primary site. |
|  | Enter text |
|  | Will the Applicant test the ICT BCPs and DRPs at least on a yearly basis? | Select item |
|  | Will the above-mentioned tests include: |
|  | cyber-attacks and switchovers scenarios. | Select item |
|  | Governance arrangements and crisis communication plans. | Select item |
|  | The ability of third-party providers to respond to the scenarios under test in line with the Applicant’s own ICT BCPs and DRPs.  | Select item |
| 1. Outsourcing Arrangements
 |
|  | **Outsourcing Arrangements** |
|  | Has the Applicant developed and documented an outsourcing policy? | Select item |
|  | **Attachment | Outsourcing Policy***(If the answer is ‘Yes’ to Q7.1.1.1)* |
|  | In instances of when outsourcing arrangements are in place:  |
|  | Define as to how the Applicant will ensure that the Management Body retain full responsibility for compliance with all legal and regulatory requirements. |
|  | Enter text |
|  | Define the governance oversight arrangements that will be implemented by the Applicant, including documentation, management and control of outsourcing arrangements.  |
|  | Enter text |
|  | Will the Management Body be the decision-making body on outsourcing arrangements that at least relate to a critical or important function? | Select item |
|  | Define how the Applicant identifies, assess and manages conflicts of interest that may be created from outsourcing arrangements.  |
|  | Enter text |
|  | Will the Applicant retain a Register of Information on all outsourcing arrangements?  | Select item |
|  | Prior to entering into an outsourcing arrangement, define the pre-outsourcing analysis performed by the Applicant more specifically as to how it: |
|  | 1. Assess if the outsourcing arrangement concerns a critical or important function of the Applicant.
 |
|  | Enter text |
|  | 1. Identifies and assess all relevant risks of the outsourcing arrangement, and sub-outsourcing arrangements (as applicable), which the Applicant will be exposed too.
 |
|  | Enter text |
|  | 1. Undertake appropriate due diligence on prospective service providers.
 |
|  | Enter text |
|  | For each outsourcing arrangement related to critical or important function, will the Applicant define and document an exit strategy? | Select item |
|  | Does the Applicant intend to outsource any critical or important ICT systems, services, processes or functions to a third-party service 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 |
|  |
| 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***(An AX03 to be completed for each above-identified ICT Third-Party Provider)* |