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

|  |
| --- |
| **Annex AX05: Digital Operational Resilience Assessment**  |
|  |
| **High Level Guidelines** |
|  |
|  |
| 1. **General**

This form, **Annex AX05:** **Digital Operational Resilience 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 ability to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.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 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’), and any other National and/or European Regulatory Frameworks, or other binding regulation as may be applicable at the time of Application. 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**

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.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **‘microenterprise’** | means a financial entity, other than a trading venue, a central counterparty, a trade repository or a central securities depository, which employs fewer than 10 persons and has an annual turnover and/or annual balance sheet total that does not exceed EUR 2 million. |
|  |  |
| **‘small enterprise’** | means a financial entity that employs 10 or more persons, but fewer than 50 persons, and has an annual turnover and/or annual balance sheet total that exceeds EUR 2 million, but does not exceed EUR 10 million. |
|  |  |
| **‘medium-sized enterprise’** | means a financial entity that is not a small enterprise and employs fewer than 250 persons and has an annual turnover that does not exceed EUR 50 million and/or an annual balance sheet that does not exceed EUR 43 million. |
|  |  |
| **‘small institution for occupational retirement provision’** | means an institution for occupational retirement provision which operates pension schemes which together have less than 100 members in total. |
|  |  |
| **‘electronic money institution exempted pursuant to Directive 2009/110/EC’** | means an electronic money institution benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC. |
|  |  |
| **‘small and non-interconnected investment firm’** | means an investment firm that meets the conditions laid out in Article 12(1) of Regulation (EU) 2019/2033 of the European Parliament and of the Council. |
|  |  |
| **‘payment institution exempted pursuant to Directive (EU) 2015/2366’** | means a payment institution exempted pursuant to Article 32(1) of Directive (EU) 2015/2366. |
|  |  |

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. **NOTE:** Referring to Article 16(1) of the DORA Regulation, inter alia,* small and non-interconnected investment firm(s),
* payment Institution exempted pursuant to Directive (EU) 2015/2366,
* money institutions exempted pursuant to Directive 2009/110/EC and
* small institutions for occupational retirement provision (pension schemes which together have less than 100 members in total)

are subject to regulatory obligations emanating from the Simplified ICT Risk Management Framework of the DORA Regulation. **For Sections 3 to 8:**Applicants **not** falling within scope of the Simplified ICT Risk Management Framework should complete **only Part A** of the following sections. 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 – General Identification Details**  |
|  | Registered Name *(if not yet Formed, provide proposed name)* | Enter text |
|  | Registered Number(*if applicable)* | Enter text |
|  | AU Person Code(*if applicable*) | Enter text |
|  | Authorised Person Size*In accordance with the DORA Regulation.* *Consider ‘Other’ as larger then medium-sized enterprises* | Select item |
|  | The Applicant classifies as: |
|  | A small and non-interconnected investment firm | Select item |
|  | Payment Institution exempted pursuant to Directive (EU) 2015/2366 | Select item |
|  | Electronic money institutions exempted pursuant to Directive 2009/110/EC | Select item |
|  | Small institutions for occupational retirement provision (pension schemes which together have less than 100 members in total) | Select item |
|  | The Applicant should provide a thorough description and statement as to how the proportionality element has been implemented in line with Article 4 of the DORA Regulation (EU) 2022/2554 |
|  | Enter text |

| 1. ICT Risk Management Governance and Organisation
 |
| --- |
|  | **ICT Governance – General Details***The Applicant is expected to provide information in line with Article 5 of the DORA Regulation* |
|  | For Applicant’s, other than Micro-Enterprise, to explain how an effective formal governance structure for managing and overseeing ICT risks is achieved according to the three lines of defence model, or an internal risk management and control model, including a description of all relevant functions, the assurance of achieving appropriate independence and segregation of the functions and reporting lines |
|  | Enter text |
|  | For Applicant’s that are considered a Micro-enterprise, to explain how an effective formal governance structure for managing and overseeing ICT risks is achieved, including a description of all relevant functions |
|  | Enter text |
|  | The Applicant should specify the identified roles and responsibilities for the development, implementation and maintenance of ICT security policies, procedures, protocols, and tools |
|  | Enter text |
|  | **Attachment | Organogram**Organogram – the Applicant should present the answers to section 2.1, 2.2, 2.3 in an organogram |
|  | With regards to your arrangements related to the ICT risk management framework, does the management body: |
|  | Define, approve, oversee and act responsible for the implementation of the Applicant’s ICT Risk Management Framework, including any strategies, policies, procedures, plans and mechanisms issued thereunder? | Select item |
|  | Bear the final responsibility when dealing with ICT risks | Select item |
|  | Review and approve the development and maintenance of policies relating to ensuring confidentiality, integrity and availability standards of data quality? | Select item |
|  | Review and approve the development and the maintenance of ICT Business Continuity Policy and ICT response and recovery plans? | Select item |
|  | Set clear governance roles and responsibilities for all ICT-related functions? | Select item |
|  | Establish the governance arrangements for effective communication, cooperation and coordination among all the ICT functions? | Select item |
|  | Review and approve the development and maintenance of a digital operational resiliency strategy | Select item |
|  | Periodically review and approve the development and outcome of the ICT internal audit plans/programs and ICT audits? | Select item |
|  | Allocate and periodically review the Applicant’s appropriate budget allocated to sustain the digital operational resilience objectives, including training and awareness? | Select item |
|  | How has the Applicant ascertained that at least at a management body level sufficient knowledge and skills are achieved to understand and assess ICT Risks and information security? |
|  | Enter text |
|  | Will members of the management body receive regular training about ICT risks, ICT risk management and information security, commensurate to the ICT risk being managed? |
|  | Enter text |
|  | **Additional Comments (Optional)**The below to be completed by the Applicant to add any additional comments for explanation to the answers above |
|  | Enter text |

| 1. ICT Risk Management Framework
 |
| --- |
|  | **Part A** *Note: Not to be completed by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Does the Applicant have a sound, comprehensive and well-documented ICT Risk Management Framework in place? | Select item |
|  | The Applicant should provide a thorough overview of the information and components (strategies, policies, procedures, ICT protocols and tools) captured within its documented ICT Risk Management Framework. |
|  | Enter text |
|  | The Applicant should thoroughly explain the developed, documented and implemented procedures and methodology for the, inter alia, conduct of ICT Risk Assessments, identification, implementation and documentation of ICT Risk Treatment measures for all identified ICT Risks, including residual risk. |
|  | Enter text |
|  | The Applicant should thoroughly explain the developed, documented and implemented procedure for the monitoring of the evolution of the ICT Risks, including any changes in the cyber threat landscape, threats and vulnerabilities that the entity might be exposed too. |
|  | Enter text |
|  | Does the Applicant intend to review its ICT risk management framework: |
|  | At least once a year (for entities other than micro-enterprise)? |  Select item  |
|  | Periodically (for entities that are a micro-enterprise)? | Select item |
|  | Does the Applicant intend to review its ICT risk management framework: |
|  | After the occurrence of a major ICT-incident? | Select item |
|  | Following the conclusions derived from relevant digital operational resilience testing? | Select item |
|  | following the conclusions derived from relevant audit processes? | Select item |
|  | Has the Applicant developed and implemented a digital operational resilience strategy? | Select item |
|  | If Yes to the above, the Applicant should thoroughly explain the objectives and contents of the strategy and how it implements the ICT risk management framework. |
|  | Enter text |
|  | **Part B** *Note: To completed only by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | The Applicant should provide a thorough overview of the information and components captured within its sound and well documented ICT Risk Management Framework:  |
|  | Enter text |
|  | Does the Applicant intend to review its ICT risk management framework: |
|  | Periodically?  |  Select item  |
|  | Upon the occurrence of a major ICT-incident?  | Select item |
|  | **Additional Comments (Optional)***The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. ICT Risk Identification, Control and Monitoring
 |
| --- |
|  | **Part A***Not to be completed by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation.* |
|  | Has the Applicant established and defined its risk tolerance level for ICT Risk | Select item |
|  | Has the Applicant identified all sources of ICT risks that it is exposed to in accordance with its ICT Risk Management Framework? | Select item |
|  | For Applicant’s other than Micro-Enterprise, has an ICT risk assessment been conducted on all legacy ICT systems? | Select item |
|  | As part of the ICT risk management framework has the Applicant identified, classified and documented the following: |
|  | All ICT supported business functions? | Select item |
|  | Roles and responsibilities of these functions? | Select item |
|  | Information and ICT assets supporting these functions? | Select item |
|  | The functions’ relationship and dependencies of the above to the identified ICT risks? | Select item |
|  | As part of the above, does the Applicant intend to review as needed, and at least yearly the adequacy of this classification and of any relevant documentation? | Select item |
|  | For the purpose of the above, has the Applicant developed an inventory that it intends to keep updated? | Select item |
|  | Explain how the Applicant will continuously monitor threats and vulnerabilities that it might impact the ICT Risks it is exposed too and are relevant to their critical or important functions, and information assets and ICT assets: |
|  | Enter text |
|  | **Attachment | A copy of the inventory retained by the Applicant for the purpose of identifying, classifying and documenting all ICT Supported Business functions, roles and responsibilities, the information assets and ICT assets supporting those functions and the dependencies to the identified ICT Risks.**  |
|  | **Part B** *Note To completed only by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Has the Applicant established and defined its risk tolerance level for ICT Risk? | Select item |
|  | Has the Applicant identified all sources of ICT risks that it is exposed to in accordance with its ICT Risk Management Framework? | Select item |
|  | Explain how the Applicant will continuously monitor threats and vulnerabilities that it might impact the ICT Risks it is exposed too and are relevant to their critical or important functions, and information assets and ICT assets: |
|  | Enter text |
|  | Define as to how the Applicant will manage risks related to outdated, unsupported or legacy ICT Assets: |
|  | Enter text |
|  | **Attachment | A copy of the assessment conducted to identify all ICT Risks that the Applicant is exposed to.** |
|  | **Additional Comments *(Optional)****The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. ICT Asset Management
 |
| --- |
|  | **Part A***Note: Not to be completed by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Has the Applicant developed, documented and implemented an ICT Asset Management policy relating to the management of ICT Assets including the monitoring and management of the lifecycle of the ICT Assets? | Select item |
|  | If Yes to the above, provide a thorough overview of the documented and implemented ICT Asset Management policy |
|  | Enter text |
|  | Has the Applicant developed, documented and implemented an ICT Asset Management procedure? | Select item |
|  | If Yes to the above, provide a thorough overview of the developed, documented and implemented procedure ICT Asset Management Procedure: |
|  | Enter text |
|  | Has the Applicant identified all information assets and ICT assets including those on remote sites, network resources and hardware equipment? | Select item |
|  | Does the Applicant keep records of: |
|  | The unique identifier of each ICT asset | Select item |
|  | Information on the location, either physical or logical, of all ICT assets | Select item |
|  | The identity of ICT asset owners | Select item |
|  | the business functions or services supported by the ICT asset | Select item |
|  | The ICT business continuity requirements, including recovery time objectives and recovery point objectives | Select item |
|  | Whether the ICT asset can be or is exposed to external networks, including the internet | Select item |
|  | The links and interdependencies among ICT assets and the business functions using each ICT asset | Select item |
|  | Has the Applicant linked and mapped the configuration of the information assets and ICT assets? | Select item |
|  | Has the Applicant linked and mapped the interdependencies between all different information assets and ICT assets, making a difference between those considered critical? | Select item |
|  | For the purpose of the above, has the Applicant developed a relevant inventory that it intends to keep updated? | Select item |
|  | **Attachment | A copy of the above-referenced inventory.** |
|  | **Part B** *Note To completed only by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Has the Applicant identified, classified and documented all: |
|  | Critical or important functions? | Select item |
|  | Information Assets supporting the critical or important functions? | Select item |
|  | ICT Assets supporting the critical or important functions? | Select item |
|  | Has the Applicant mapped the interdependencies of all its critical or important functions to the information assets and ICT assets supporting them? | Select item |
|  | Thoroughly explain as to how the Applicant will monitor and manage the lifecycle of all ICT Assets, including those supported by ICT third-party providers | Select item |
|  | **Additional Comments (Optional)***The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. ICT Asset Management
 |
| --- |
|  | **ICT Systems, Protocols and Tools***Note: Not to be completed by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | How is the Applicant’s ICT Infrastructure: |
|  | Proportionality appropriate to handle the magnitude of forecasted business operations and activities requirements? |
|  | Enter text |
|  | Reliable? |
|  | Enter text |
|  | Equipped with sufficient capacity to accurately process the necessary data, as needed? |
|  | Enter text |
|  | **Additional Comments (Optional)**The below to be completed by the Applicant to add any additional comments for explanation to the answers above:  |
|  | Enter text |

| 1. Security, Protection and Prevention
 |
| --- |
|  | **Part A***Note: Not to be completed by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Has the Applicant developed and documented: |
|  | An Information Security Policy | Select item |
|  | Policy(ies) and procedure(s) for management of physical and logical accesses to information assets and ICT assets, including access rights management | Select item |
|  | Policy(ies) and protocol(s) for the implementation of strong authentication mechanisms | Select item |
|  | Policy(ies) and protocol(s) for the implementation of encryption and cryptographic controls and cryptographic key management | Select item |
|  | Policy(ies) and procedures for ICT Operations Security | Select item |
|  | Policy(ies) and procedure(s) for ICT Change Management | Select item |
|  | Policy(ies) for patches and updates | Select item |
|  | **Attachment | A copy of the above-mentioned policies (ticked yes to).** |
|  | Are there any plans to align the information security framework with any internationally recognised standard/framework? |
|  | Enter text |
|  | Has the Applicant, on a risk-based approach, designed a sound network connection and infrastructure management structure | Select item |
|  | Describe the ICT security monitoring tools that the Applicant has implemented |
|  | 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 |
|  | The Applicant should thoroughly describe as to how the above-mentioned policies, procedures, protocols and tools |
|  | Enter text |
|  | Ensure resilience, continuity and availability of ICT systems, specifically for those supporting critical or important functions |
|  | Enter text |
|  | Ensure the security of networks |
|  | Enter text |
|  | Ensures the security of the means of transfer of data |
|  | Enter text |
|  | Safeguards against intrusion and data misuse |
|  | Enter text |
|  | Preserve the availability, authenticity, integrity, and confidentiality of data (at rest, in transit or in use), including via the use of cryptographic techniques |
|  | Enter text |
|  | Guarantee an accurate and prompt data transmission without major disruptions and undue delays |
|  | Enter text |
|  | Does the Applicant monitor (on a continuous basis) the security and functioning of the ICT systems and tools? | Select item |
|  | Enter text |
|  | Describe the controls in place that aim at ensuring the continuity of ICT systems, especially those supporting a critical or important function |
|  | Enter text |
|  | Do you have a strong authentication mechanism in place? | Select item |
|  | If Yes to the above, describe the implemented authentication mechanisms |
|  | Enter text |
|  | Define the encryption and cryptographic controls that the Applicant has implemented for: |
|  | Data at rest |
|  | Enter text |
|  | Data in transit |
|  | Enter text |
|  | Data in use (where necessary) |
|  | Enter text |
|  | Internal network connections and traffic with external parties |
|  | Enter text |
|  | If the implemented cryptographic controls do not adhere to leading practices, standards or reliable techniques, what are the mitigation and monitoring measures the Applicant has implemented to ensure resilience against cyber threats? |
|  | Enter text |
|  | Describe the controls in place that aim at targeting cryptographic key management, including losses or when keys are damaged or compromised |
|  | Enter text |
|  | In relation to Cryptographic Key Management, does the Applicant maintain an up-to-date register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions? | Select item |
|  | Does the Applicant make use of automated mechanisms to isolate affected information assets in the event of cyber-attacks? | Select item |
|  | Does the Applicant segregate network to minimise and prevent contagion in the event of cyber-attacks? | Select item |
|  | Describe the controls in place for ICT Project and Change Management, including changes to software, hardware, firmware components, systems or security parameters |
|  | Enter text |
|  | Are all changes to ICT systems recorded, tested, assessed, approved, implemented and verified in a controlled manner?  |
|  | 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, even at an ICT third-party provider level (as applicable)? |
|  | 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, even at an ICT third-party provider level (as applicable)? |
|  | Enter text |
|  | Describe the ICT security awareness programmes and digital operational resilience training intended to be performed |
|  | Enter text |
|  | **Part B***Note: To completed only by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Are there any plans to align the information security framework with any internationally recognised standard/framework? | Select item |
|  | Describe the ICT security monitoring tools that the Applicant has implemented |
|  | Enter text |
|  | Describe the logging procedures, protocols and tools that the Applicant has implemented |
|  | Enter text |
|  | Does the Applicant monitor (on a continuous basis) the security and functioning of the ICT systems and tools? | Select item |
|  | Describe the controls in place that aim at ensuring the continuity of ICT systems, especially those supporting a critical or important function |
|  | Enter text |
|  | Describe the controls in place for ICT Project and Change Management, including changes to software, hardware, firmware components, systems or security parameters |
|  | Enter text |
|  | Describe as to how the policies, procedures, protocols and tools mentioned above: |
|  | Ensure resilience, continuity and availability of ICT systems, specifically for those supporting critical or important functions |
|  | Enter text |
|  | Ensure the security of networks |
|  | Enter text |
|  | Ensures the security of the means of transfer of data |
|  | Enter text |
|  | Safeguards against intrusion and data misuse |
|  | Enter text |
|  | Preserve the availability, authenticity, integrity, and confidentiality of data (at rest, in transit or in use) |
|  | Enter text |
|  | Guarantee an accurate and prompt data transmission without major disruptions and undue delays |
|  | Enter text |
|  | Are all changes to ICT systems recorded, tested, assessed, approved, implemented and verified in a controlled manner? | Select item |
|  | What measures and/or mechanism will the Applicant put in place to ensure that physical access to ICT Systems is controlled and restricted, even at an ICT third-party provider level (as applicable)? |
|  | 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, even at an ICT third-party provider level (as applicable)? |
|  | Enter text |
|  | Describe the established ICT security testing plan to validate the effectiveness of the ICT security measures |
|  | Enter text |
|  | **Additional Comments (Optional)***The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. Business Continuity Management
 |
| --- |
|  | **Part A***Note: Not to be completed by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Has the Applicant developed and documented an: |
|  | ICT Business Continuity Policy? | Select item |
|  | ICT Business Continuity Plan? | Select item |
|  | ICT Response and Recovery Plans? | Select item |
|  | **Attachment | A copy of the above-mentioned policies and plans (ticked yes to).** |
|  | Has the Applicant performed a Business Impact Assessment (BIA) to assess its exposure to severe business disruptions? | Select item |
|  | Does the BIA: |
|  | Use both quantitative and qualitative criteria to assess the potential impact of disruption? | Select item |
|  | Use internal and external data in its analysis? | Select item |
|  | Include scenario analysis in its assessment? | Select item |
|  | Consider the criticality of business functions? | Select item |
|  | consider third-party dependencies? | Select item |
|  | Consider the interdependencies of critical business functions? | Select item |
|  | When developing the ICT Business Continuity Policy and Plans, were the results of the conducted BIA taken into consideration? | Select item |
|  | Do the ICT Business Continuity, Response and Recovery Plans cater for scenarios of potential disruptions of ICT Services provided by ICT Third-Party Providers, and which specifically relate to critical or important functions? | Select item |
|  | Does the crisis communication plan include: |
|  | The transmission of relevant information to the internal staff? | Select item |
|  | The transmission of relevant information to the external stakeholders | Select item |
|  | The reporting to the competent authorities? | Select item |
|  | Exhaustively explain the Applicant’s intended testing arrangements of its ICT Business Continuity, Response and Recovery Plans, including plans with ICT Third-Party Providers (as applicable) and frequency |
|  | Enter text |
|  | Exhaustively explain the Applicant’s intended testing arrangements of its crisis and communication plans |
|  | Enter text |
|  | For Applicant’s other than micro-enterprise, does the Applicant include cyber-attacks and switchovers scenarios in the ICT Business Continuity testing plans? | Select item |
|  | For Applicant’s other than micro-enterprise, was a crisis management function established? | Select item |
|  | Exhaustively describe the Applicant’s documented backup policy and procedure, also specifying the scope of the data that is subject to the backup and the minimum frequency of the backup |
|  | Enter text |
|  | Is the backup policy based on the criticality of information or the confidentiality level of the data? | Select item |
|  | Exhaustively describe the Applicant’s documented restoration and recovery procedures and methods |
|  | Enter text |
|  | Does the backup policy specify measures with regards to integrity or confidentiality of data during restoration? | Select item |
|  | Identify the Applicant’s backup system arrangements |
|  | Enter text |
|  | When restoring backup data, do you use ICT systems that are physically and logically segregated from the source ICT system? | Select item |
|  | Are the ICT systems used for backup and restoration securely protected from any unauthorized access or ICT corruption? | Select item |
|  | When recovering from ICT-related incidents, do you have a formal procedure in place that checks data correctness and integrity after resolution? | Select item |
|  | When reconstructing data from external stakeholders following an ICT-related incident, do you have a procedure in place to ensure data integrity or consistency? | Select item |
|  | For Applicants other than micro-enterprises, do you maintain redundant ICT capacities to ensure business continuity needs? | Select item |
|  | For Applicants considered to be a micro-enterprise, do you assess the need to maintain redundant ICT capacities based on your risk profile? | Select item |
|  | **Part B** *Note: To completed only by Applicant’s that are subject to the Simplified ICT Risk Management Framework of the DORA Regulation* |
|  | Has the Applicant developed and documented an ICT Business Continuity Plan? | Select item |
|  | **Attachment | A copy of the above-mentioned plan (if ticked yes to).** |
|  | Has the Applicant conducted a Business Impact Assessment (BIA) to assess its exposure to severe business disruptions? | Select item |
|  | Does the BIA: |
|  | Use both quantitative and qualitative criteria to assess the potential impact of disruption? | Select item |
|  | Use internal and external data in its analysis | Select item |
|  | Include scenario analysis in its assessment? | Select item |
|  | Consider the criticality of business functions? | Select item |
|  | Consider third-party dependencies? | Select item |
|  | Consider the interdependencies of critical business functions? | Select item |
|  | Do the ICT Business Continuity Plans cater for scenarios of potential disruptions of ICT Services provided by ICT Third-Party Providers, and which specifically relate to critical or important functions? | Select item |
|  | Does the crisis communication plan include:  |
|  | The transmission of relevant information to the internal staff? | Select item |
|  | The transmission of relevant information to the external stakeholders? | Select item |
|  | The reporting to the competent authorities? | Select item |
|  | Exhaustively describe the Applicant’s intended testing arrangements of its ICT Business Continuity, Response and Recovery Plans, including plans with ICT Third-Party Providers (as applicable) and frequency |
|  | Enter text |
|  | Exhaustively describe the Applicant’s intended testing arrangements of its crisis and communication plans | Select item |
|  | For Applicant’s other than micro-enterprise, does the Applicant include cyber-attacks and switchovers scenarios in the ICT Business Continuity testing plans? | Select item |
|  | Thoroughly describe the Applicant’s back up procedures, measures and arrangements, also specifying the scope of the data that is subject to the backup and the minimum frequency of the backup |
|  | Enter text |
|  | Thoroughly describe the Applicant’s restoration and recovery measures and arrangements |
|  | Enter text |
|  | **Additional Comments (Optional)***The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. ICT-Related Incident Management, Classification and Reporting
 |
| --- |
|  | **ICT- Related Incident Management, Classification and Reporting** |
|  | Define the mechanisms in place that detect: |
|  | Anomalous activities |
|  | Enter text |
|  | ICT network performance issues |
|  | Enter text |
|  | ICT-related incidents |
|  | Enter text |
|  | Material single points of failure |
|  | Enter text |
|  | Do the detection mechanisms, 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 regularly tested? | Select item |
|  | Do you have resources and capabilities in place that monitor user activity, occurrence of ICT anomalies and ICT-related incidents (particularly cyber-attacks)? | Select item |
|  | Has the Applicant defined, established and implemented: |
|  | An ICT-related incident management process to detect, manage and notify ICT-related incidents | Select item |
|  | Procedures and processes for follow-up of ICT- related incidents to ensure that root causes are identified, documented and addressed to prevent re-occurrence | Select item |
|  | Do you conduct a post ICT-related incident review after major ICT incidents? | Select item |
|  | Does the review lead to the improvements to the ICT operations or business continuity plans, as applicable? | Select item |
|  | **Attachment | To provide a copy of the ICT-related incident management process** |
|  | Are all ICT-related incidents and significant cyber-threats recorded? | Select item |
|  | Thoroughly identify the criteria considered by the Applicant to classify ICT-related incidents and determine their impact |
|  | Enter text |
|  | Thoroughly identify the criteria considered by the Applicant to classify cyber threats as significant |
|  | Enter text |
|  | For major ICT-related incidents, has the Applicant implemented the necessary measures to ensure that: |
|  | An initial report is submitted to the Competent Authority as early as possible within 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the moment the financial entity has become aware of the incident | Select item |
|  | An intermediate report is submitted to the Competent Authority the latest within 72 hours from the submission of the initial notification | Select item |
|  | The final report is submitted to the competent authority no later than one month from the submission of the latest updated intermediate report | Select item |
|  | **Additional Comments (Optional)***The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. Management of ICT Third-Party Risk
 |
| --- |
|  | **Management of ICT Third-Party Risk** |
|  | In instances of when arrangements with ICT third-party providers (ICT TPPs) are in place for the use of ICT Services, the Applicant should thoroughly explain as to how it ensures that at all times it will remain fully responsible and compliant with, and the discharge of, all applicable obligations under the DORA Regulation |
|  | Enter text |
|  | With regards to internal reporting channels, is the management body informed of: |
|  | The arrangements concluded with ICT TPPs? | Select item |
|  | Any relevant planned material changes regarding the ICT TPPs? | Select item |
|  | The potential impact of such changes, including a risk analysis summary, a response, recovery and corrective measures? | Select item |
|  | For Applicant’s other than micro-enterprise, has the Applicant established a role, or identified a member of senior management, to act responsible for the monitoring and overseeing of the arrangements with ICT third-party service providers? | Select item |
|  | Do the responsibilities of this role, or appointed member of senior management, include the overseeing of the related and relevant documentation? | Select item |
|  | For Applicant’s other than micro-enterprise, has the Applicant established a formal strategy on ICT third party risk? | Select item |
|  | Does it consider the multi-vendor strategy? | Select item |
|  | Does the formal strategy on ICT third party risk include a written policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers? | Select item |
|  | Is the policy reviewed by the management body at least once a year and updated where necessary? | Select item |
|  | **Attachment | A copy of the written policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers** |
|  | Has the Applicant identified and documented all processes that are dependent on ICT TPPs and identified interconnections with the ICT TPPs that provide services that support critical or important functions? | Select item |
|  | For the purpose of the above, has the Applicant developed a relevant inventory that it intends to keep updated? | Select item |
|  | Do you manage the ICT third party risk according to:  |
|  | The nature and relevance of the ICT related dependencies the ICT third party services introduce? | Select item |
|  | The criticality or importance of the respective service, process or function they support? | Select item |
|  | Does the management body review the ICT third party risks on regular basis? | Select item |
|  | Does the management body regularly review the risks identified in respect to contractual arrangements on the use of ICT services concerning critical or important functions? | Select item |
|  | Does the Applicant maintain, and intend to keep updated, a register of information identifying all contractual arrangements, and relevant supply chains, on the use of ICT Services provided by ICT TPPs? | Select item |
|  | Does the Applicant have process in place to inform the Authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important? | Select item |
|  | Does the Applicant have process in place to, upon request, make available to the Authority the full Register of Information and any other related information necessary for supervision? | Select item |
|  | The Applicant shall thoroughly explain as to how is ensures that for any contractual arrangement it can terminate contractual arrangements on the use of ICT services, in any relevant circumstance as defined by the DORA Regulation Article 28(7) |
|  | Enter text |
|  | For each contractual arrangement for the use of ICT services related to critical or important functions, does the Applicant have in place a comprehensive documented exit strategy? | Select item |
|  | Does the Applicant test and review exit plans on a regular basis? | Select item |
|  | Do exit plans include: |
|  | The identification of alternative solutions? |  Select item  |
|  | Transition steps/actions to move the ICT services to alternative providers or on premise? | Select item |
|  | Measures about the security and integrity of data? | Select item |
|  | **Attachment | AX50 ICT Third-Party Arrangement** *An Annex needs to be compiled and provided for* ***each*** *contractual arrangement held with an ICT TPP for ICT Services supporting critical or important functions, or material parts thereof* |
|  | **Additional Comments (Optional)***The below to be completed by the Applicant to add any additional comments for explanation to the answers above* |
|  | Enter text |

| 1. Digital Operational Resilience Testing
 |
| --- |
|  | Define the established digital operational resilience testing programme |
|  | Enter text |