



Technology Assurance Sandbox v2.0 Program Guidelines

Effective Date: 1st June 2022



Contents

1	DEFINITIONS	1
2	INTRODUCTION	3
3	THE MDIA-TAS PROCESS	3
3.1	STANDARD ONBOARDING PHASE	3
3.2	MONITORING OF SANDBOX RESIDENCY	5
3.3	STANDARD OFFBOARDING PHASE	7
4	PROCESSING FEES	8
5	RESIDENCY PLAN GUIDELINES	9
6	SANDBOX BLUEPRINT GUIDELINES	9
7	SANDBOX BUSINESS PLAN GUIDELINES	10
8	FORENSIC NODE	11

1 Definitions

“Applicant”, within the context of this document, refers to an individual and/or legal organisation submitting an Application Form manifesting his/her/its wish to join the MDIA Technology Accreditation Sandbox with respect to an innovative digital product or service (“IDPS”) with the Authority. Where “he” is used with reference to the Applicant in these Guidelines, it should be deemed to refer to individual applicants of any sex, as well as to a legal organisation.

“Application” and **“Application Form”** shall mean the documents by which the Applicant registers its wish to join the MDIA Technology Accreditation Sandbox.

“Authority” refers to the Malta Digital Innovation Authority (“MDIA”).

“Control Objectives” refers to MDIA published Control Objectives or Control Objectives derived through the MDIA TAAF framework.

“Forensic Node” shall have the same meaning attributed in Section 8 of this document.

“Initial Technical Soundness Review” shall be conducted by the appointed Technical Expert identifying the current state of the IDPS.

“MDIA Technology Accreditation Sandbox”, also referred to as **“the Sandbox”** and **“MDIA-TAS”** within this document, refers to the process of providing Residents with a guided means of developing their IDPS to achieve developmental milestones set by the Residents, through a number of Technology Soundness Review iterations conducted by Technical Experts, monitored by the Authority.

“Register of Approved Sandbox Residency” is an electronic register, also referred to as **“the Register”**, of all Sandbox Residents. The Register, which shall be publicly available on the Authority’s website, shall include fields that the Authority considers necessary in order to identify the relevant Sandbox Resident and the activities being carried out by it.

“Sandbox Blueprint”, also referred to as **“the blueprint”** refers to a document that includes a technical description of the IDPS resident in the Sandbox, describing the technology, functionality and features and enabling it to be reviewed by the Technical Expert as described in [Section 6](#) of these Guidelines.

“Sandbox Business Plan” refers to a document that explains the business supporting the IDPS throughout its residency in the MDIA-TAS, as defined in [Section 7](#) of these Guidelines.

“Sandbox Residency Acceptance Notice”, also referred to as *“the Notice”*, refers to the Notice issued by the Authority to the Applicant to notify him that this Application has been accepted and he has been allowed entry in the MDIA-TAS.

“Sandbox Residency Plan”, also referred to as *“Residency Plan”* in this document, refers to the document submitted by the Applicant identifying how the IDPS will advance throughout its residency in the MDIA-TAS.

“Sandbox Residency” refers to the participation of the Sandbox Resident in the Sandbox.

“Sandbox Resident” (also referred to as *“Resident”*) refers to a successful Applicant whose application to enter and participate in the MDIA-TAS was accepted by the MDIA.

“Technical Expert” refers to specialists listed/recognised by the Authority to carry out technical reviews of the Residents’ IDPSs throughout the Residency and to produce Technical Soundness Review Reports, subject to terms and conditions applicable to the Technical Experts.

“Technical Soundness Review” refers to the technical review carried out by the Technical Experts with respect to whether the identified Control Objectives applied to the respective applicable segment of the IDPS have been successfully achieved by the IDPS as defined in the milestone within the Residency Plan.

“Technical Soundness Review Report” refers to the document produced as an outcome of the review carried out by the Technical Experts with respect to whether the identified objectives have been achieved by the IDPS as defined in the milestone within the Residency Plan.

“Technical Officer” refers to the person appointed by the Applicant to carry out the responsibilities as highlighted in the Technical Officer Terms and Conditions document.

2 Introduction

The MDIA-TAS is specifically designed to cater for start-ups, smaller players or any other entity seeking the correct development of their IDPS, through a process that consists of a number of Technical Soundness Reviews conducted by MDIA-recognised Technical Experts and is monitored by the Authority. This process supports the Applicant in identifying technological gaps, to be in conformance with the resident-identified Control Objectives and is intended to provide further confidence to stakeholders, such as investors, developers, users, and the public.

Technical Soundness Reviews would focus on functional correctness and reliability and robustness of the IDPS and the underlying operational processes in line with industry standards and best practices. The maximum permitted Sandbox Residency period is that of four (4) years. The Sandbox is not intended to serve as a certification scheme.

These Guidelines apply to any prospective Applicants and Technical Experts who may be engaged in performing Technical Soundness Reviews. These Guidelines supersede any previous version.

For the sole purpose of the Sandbox v2.0, the role of the Technical Expert can be performed by either MDIA approved Systems Auditors, or MDIA listed Technical Experts. In the case where an MDIA approved SA is acting as the Technical Expert for Sandbox v2.0, the SA will be bound by the same terms and conditions applicable to the Technical Expert.

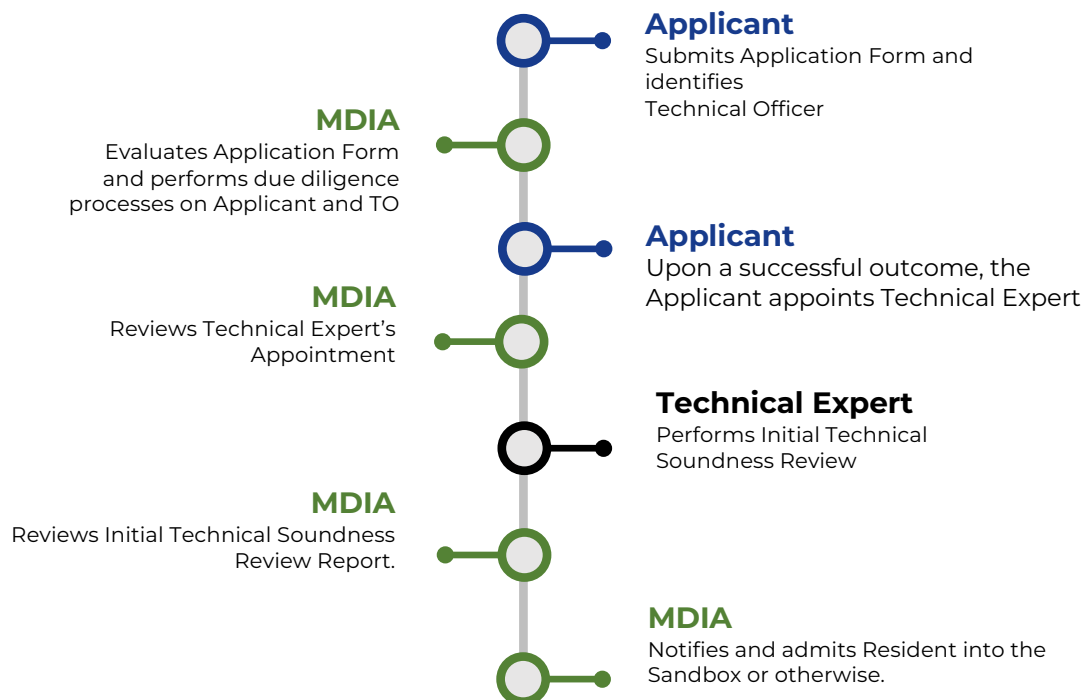
3 The MDIA-TAS Process

Residency in the MDIA-TAS will be phased in a manner which is appropriately customised for the needs of each particular Applicant. Despite the different conditions, all Sandbox Residents will go through three main phases, namely:

1. Standard *onboarding* phase,
2. Monitored *Sandbox Residency* phase,
3. Standard *offboarding* phase.

3.1 Standard Onboarding Phase

The MDIA-TAS onboarding process is shown below:



Onboarding starts when the Applicant submits a completed *MDIA-TAS Application Form*. The Applicant is, amongst others, required to submit:

- A *Residency Plan* which provides information about the IDPS, describes how the IDPS will develop throughout its Sandbox residency, planned assessments, reporting plans and residency risk assessment. For more details refer to [Section 5](#) of this document.
- A *Sandbox Blueprint* provides a description of the technology, limitations, relevant processes, security measures and technology risk assessment. Further details can be found in [Section 6](#) of this document.
- An updated *Business Plan* for the IDPS to ensure that the Sandbox Residency is aligned with the business mandate of the company making use/deploying such a technology. For more details see [Section 7](#) of this document.
- An application form of the *Technical Officer* which provides basic information on the person selected by the applicant for the role of Technical Officer. For more details refer to *MDIA-TAS Application Form* and *Technical Officer Terms and Conditions*.

The Authority shall conduct a technical evaluation of the Application Form received together with possible due diligence processes on the Applicant and Technical Officer. The Authority shall thereafter notify the Applicant of the outcome of this process. Upon a successful outcome, the Applicant must thereafter appoint a Technical Expert, who shall be approved by the Authority, before being engaged in performing the initial and subsequent Technical Soundness Reviews.

The Applicant shall trigger an Initial Technical Soundness Review of the current state of the IDPS prior to it onboarding the Sandbox. Such a report shall be received by the Authority within three (3) months of the Authority's approval of the Technical Expert. A tri-party meeting is thereafter set up between the prospective Resident, Technical Expert and MDIA to discuss the outcome of the said report. In the case of a positive Technical Soundness Review Report, or one which identifies minor issues which the Authority deems to be acceptable, the prospective resident shall be notified and admitted into the Sandbox.

Once accepted in the MDIA-TAS, the Authority will issue a Sandbox Residency Acceptance Notice (the Notice) which provides the details of how the IDPS shall be identified, including any public key or a brand name and which will carry a unique number for purposes of identification. The IDPS shall post this Notice, in a publicly accessible location which shall be specified by the Authority, in an easily accessible and legible format so it can be viewed and understood by all users of the IDPS.

3.2 Monitoring of Sandbox Residency

The Sandbox Residency Phase is shown overleaf:



The Residency Plan shall define the MDIA-issued Control Objectives that shall be evaluated against, and the respective applicable segment of the IDPS in relation to a particular stage of the Sandbox Residency referred to as Milestones.

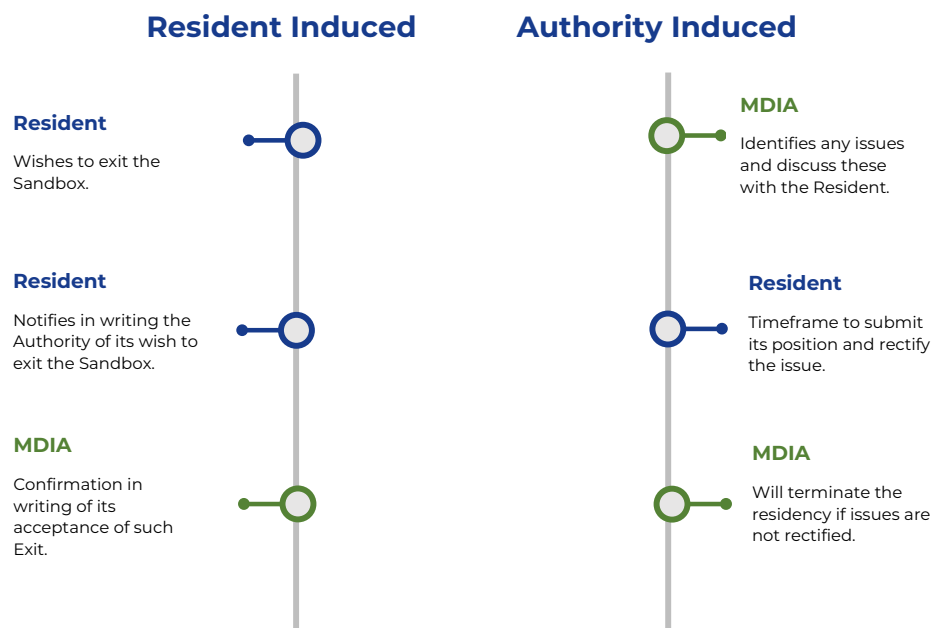
For each milestone attained by the Resident, the Technical Expert shall submit a Technical Soundness Review Report to the Resident and MDIA. Within such a report the Technical Expert shall provide visibility of the attainment or failure of the identified Control Objectives, accompanied by recommendations for potential means of rectification or the failed Control Objectives. A tri-party meeting is set up between the Resident, Technical Expert and MDIA to discuss the outcome of the said report. Within this meeting, the Residency Plan is updated to ensure that failed Control Objectives are rescheduled for re-evaluation.

Sandbox Residents are required to submit a progress report to the Authority at least every 6 months (“Progress Report”) from the date of admission into the Sandbox, or as requested by the Authority.

It is recognised that due to the nature of the IDPSs resident in the MDIA-TAS, the plans and documentation provided by the Applicant in the Application Form may require changes and updates. Approval for any changes to Application documents shall be formally requested to the Authority, which shall be

evaluated and either accepted or rejected. In addition, the Technical Officer is also required to notify MDIA of any changes in the IDPS and provide any updated documentation.

3.3 Standard Offboarding Phase



Sandbox Residents can exit or may be removed by the Authority from the Sandbox prior to completion of the Residency Plan in one of these instances:

- (i) the Resident withdraws from the Sandbox for any reason at any stage;
- (ii) the Resident proposes changes to the Application Form, Residency Plan or Technical Officer or Technical Expert which are not accepted by the Authority;
- (iii) the Authority decides to expel a Resident from the Sandbox following a violation of applicable terms and conditions;
- (iv) the Authority decides to terminate the Residency of a Resident for its failure to achieve or rectify the defined Control Objectives and scope within the milestones;
- (v) the Authority is of the opinion that the IDPS within the Sandbox may give rise to third party risks or;

(vi) the MDIA terminates or suspends the Sandbox.

Where the Resident completes the Sandbox or wishes to exit the Sandbox (Instance i), it shall notify in writing the Authority and shall not be deemed to have exited the Sandbox prior to the Authority's confirmation of such exit.

In the other cases mentioned above (Instances ii - vi) the Authority will notify the Resident, who will be given a reasonable timeframe to submit its position to the MDIA before the MDIA takes any further measures. Depending on the nature of the issue identified, the Authority may grant the Resident the opportunity to rectify the issue prior to terminating the Residency.

4 Processing Fees

The processing fees are given in the following table:

Description	Fee type	Frequency	Fee Cost
<i>Subscription fee</i> for Technical Assurance Sandbox (TAS) Residency	One-time fee	Once	€500
<i>Administrative Cost</i>	For each change necessitating due diligence checks	Per person change	€500
<i>Administrative Cost</i>	For any other change in documentation following initial submission	Per change request	€100

5 Residency Plan Guidelines

As part of the Application Form for Sandbox Residency, the Applicant must include a Residency Plan which provides information on how he envisages the IDPS to develop throughout the Residency and what information will be provided to the Authority. The Residency Plan should be closely tied to the information provided in the Blueprint, which is also to be submitted with the Application Form, as outlined below.

The Residency Plan should include a number of parts documenting:

- i. *Justification and Motivation* for participation in the Sandbox;
- ii. *IDPS Description* should specify which technologies or parts thereof are within scope of the Application Form and which are not, and also any applicable limitations (e.g. number of users or volume of transactions), which will eventually be published by the Authority in the Register;
- iii. *IDPS Progress Plan* for the duration of the Residency clearly indicating the milestones with the corresponding selected MDIA-issued Control Objectives and the respective applicable segment of the IDPS. The Applicant/Resident has to clearly indicate the intended timeframes for the attainment of each milestone;
- iv. *Applicant identified IDPS risks* in relation to the Sandbox Residency. Risks should be identified and assessed in terms of impact, severity, and probability of occurrence. The risk analysis should also include mitigation plans against the identified risks.

6 Sandbox Blueprint Guidelines

The Blueprint should describe existing and foreseen technologies, together with processes in place to develop such technology as part of the IDPS. The Blueprint is to clearly and precisely include:

- A description of *core operations* of the IDPS.
- *Functional specifications* of the IDPS, clearly defining each unit of functionality within the IDPS.
- *Activity Diagrams*, clearly defining the user, process, and data flows and interactions within the system.
- *Technical Architecture Diagrams*, clearly delineating the different logical modules of the system and interaction between them.

- An exhaustive description of any *supporting technology* which is required for the operation of the IDPS, such as external libraries.
- *Safeguards* that are in place and *limitations* within which the IDPS may operate safely (e.g. limit of the number of users, or temporary user-in-the-loop implementation) and which shall apply to its Residency within the Sandbox.
- Details of the *Forensic Node* (if the IDPS is already deployed) or plans on how the Forensic Node will be deployed (if the IDPS is still to be deployed) – see further detail in [Section 8](#)
- A list of any *foreseen technology-driven risks* and associated mitigation mechanisms.
- Details of any *other controls* or criteria (code, operational or otherwise) embedded in the system and relevant to the Sandbox Residency (e.g. Code Review policies).
- Sandbox *specific risks*, as opposed to technology or operational risks, should be covered in the accompanying Residency Plan and not in the Blueprint. Examples of sandbox-specific risks may include:
 - (i) Restrictions on the users (such as numbers of) that may be able to use the system during different milestones; and
 - (ii) Limitations on the value of the transactions that users may carry out.

Since a sandboxed IDPS may include parts which are not yet deployed, the required information is to be primarily provided for the parts already operational, but should also include any important information regarding design decisions for those parts that are not yet deployed, but which will eventually form a crucial part of the IDPS.

The above should be detailed enough such that they are not open to individual interpretation or misunderstanding. The Blueprint will be used as the basis for the Technology Soundness Review made by the Technical Expert.

7 Sandbox Business Plan Guidelines

The Applicant must include an updated Business Plan for the IDPS with the Application Form for Sandbox Residency to enable the Authority to understand the level of effort, quality and thought put into the business supporting the IDPS.

The Business Plan does not necessarily have to be written specifically for the purposes of the Sandbox Residency application to the MDIA.

The Authority understands that the maturity of the Business Plan will be commensurate with the maturity of the IDPS. In this regard, the applicant must ensure the below points are addressed, as a minimum:

- **Company/Individual:** Provide background information about your business defining aspects such as when and where it was formed, and how it is structured.
- **Business:** Provide a high-level description of the business and the solution being proposed. This need only serve for providing context.
- **Team:** Outline the team structure behind the business, as well as roles, responsibilities and experience in the field.
- **Market:** Provide a high-level description of the market(s) the solution is intended to operate in, what segments of the market are being targeted, the main competitors to the IDPS, and its unique selling points.
- **Operations:** Provide a high-level overview of how the company is anticipating to operate the IDPS. Details for this must be provided in the Blueprint.
- **Finances:** Define the financial projections for the operation of the IDPS, funding secured thus far, and how the Applicant intends securing further funding.
- **Growth plans:** Explain how the business (as a whole) is expected to grow over time.

The Business Plan will be used by the Authority for the purposes of evaluating the Application Form, and the business behind the development of the IDPS, and to ensure that the Sandbox Residency is aligned with the Applicant's business and envisioned use of the IDPS.

8 Forensic Node

- The requirements for a Forensic Node within the Sandbox Residency are as follows:
 - (i) All relevant events and data are recorded faithfully in real-time on the Forensic Node without risk of omission or corruption.
 - (ii) Information is written in a manner to ensure access to the information stored in a tamper-proof and accurate manner that is guaranteed to be faithful to the originally recorded information and that ensures that no data or information may be deleted or changed;

- (iii) Processes are in place to ensure timely access to this information by the Applicant in a manner that can be demonstrated to be faithful to the original events and data which were recorded on the Forensic Node.

It is recognised that an IDPS may apply for Sandbox Residency before it makes sense to set up a Forensic Node due to lack of data availability or due to limitations in the initial technology setup. In such cases, it is still required of the Applicant to provide information on how the above requirements will be achieved once the Forensic Node is set up. Clear milestones leading up to the setup of a Forensic Node are to be provided, including justification for the lack of a full setup until then.