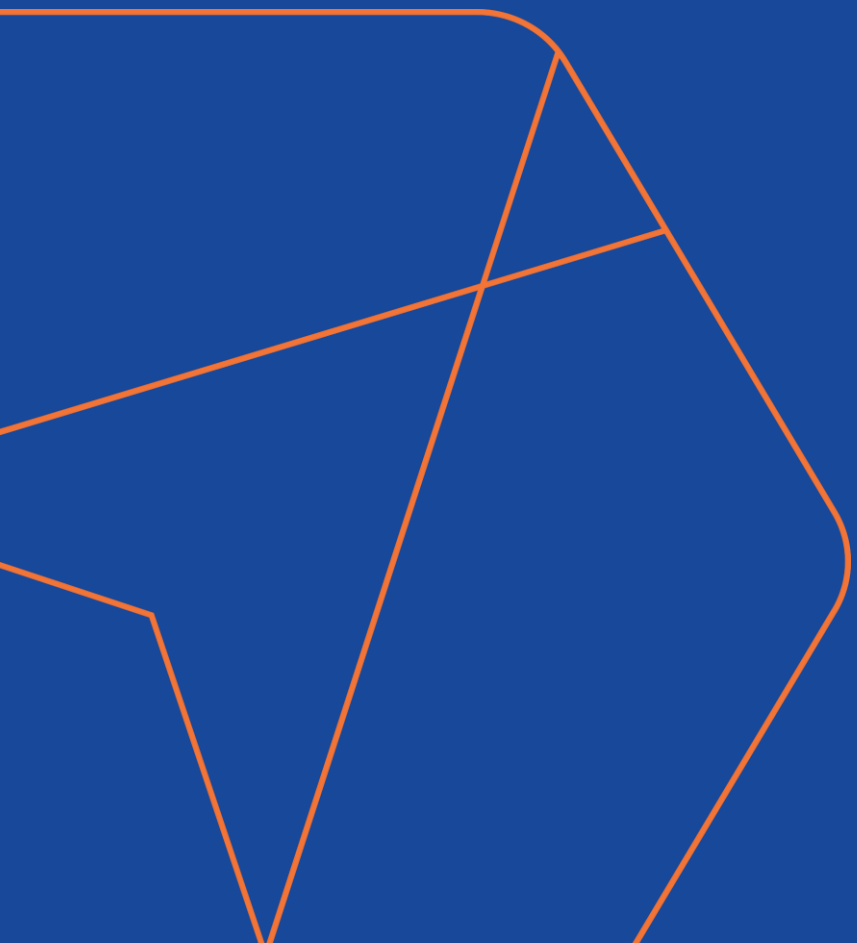
TECHNOLOGY ASSESSMENT RECOGNITION FRAMEWORK

GUIDELINES FOR APPLICANTS, ASSESSORS AND OTHER STAKEHOLDERS

Guidelines

G-SPG-012
Rev. 1
29th November 2023



Contents

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

1 Definitions

1.1 Abbreviations

DIDPS	Deployed Innovative Digital Product or Service
IDPS	Innovative Digital Product or Service
MDIA	Malta Digital Innovation Authority
NCA	National Competent Authority, also referred to as "Lead Authority"
SA	Systems Auditor
TARF	Technology Assessment Recognition Framework
TE	Technical Expert

1.2 Definitions of Key Terms

"**Act**" shall mean the Malta Digital Innovation Authority Act (Chapter 591 of the Laws of Malta).

"**Applicant**" refers to an individual and/or legal organisation, that applies for the MDIA TARF for an IDPS that the individual and/or legal organisation have legal rights to own or operate. In case of a legal organisation, the Applicant must ensure to have a representative being a natural person who will be responsible for liaising with the Authority and the operation of the IDPS. Ideally this is fulfilled by an individual with a technical understanding of the IDPS.

"**Application**" and "**Application Form**" shall mean the request and set of documents submitted by the Applicant for the purposes of participating in the MDIA TARF and found though the website of the MDIA.

"**Assessment**" refers to the action through which Applicants shall obtain their Recognition, in accordance with the TARF, that can be either a self-assessment performed by the Applicant for Assessment Level 0, a review of the IDPS performed by a Technical Expert for Assessment Level 1 and 2, or an ISAE 3000 reasonable assurance engagement performed by a Systems Auditor for Assessment Level 3.

"**Assessment Level**" refers to one of four (4) levels of assessment that form part of TARF, and their applicable IDPSs, and control types. Assessment Levels are designated by a number and a higher number implies a more intensive Assessment.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

"**Assessor**" refers to the individual or legal organisation conducting the Assessment, which can be either the Applicant, a Systems Auditor or a Technical Expert, depending on the relevant Assessment Level. For Assessment Level 1-3 the Assessor must be approved by the MDIA as described in the guidelines for each respective role prior to any TARF-related appointments. A Systems Auditor may also carry out work of a Technical Expert, however a Technical Expert may not carry out the work of a Systems Auditor.

"**Assurance**" refers to an ISAE 3000 reasonable assurance engagement carried out by a Systems Auditor. This applies solely for TARF Assessment Level 3 recognitions.

"**Authority**" refers to the Malta Digital Innovation Authority ('MDIA'), as established by the Act.

"**Control Type**" refers to the five (5) categories that the Applicant may select from one (1) to five (5) for certification purposes, which map to thematic control objectives for the relevant Assessment Level.

"**Deployed Innovative Digital Product or Service (DIDPS)**" refers to an IDPS which has completed its development lifecycle and has been (or is ready to be) deployed into the market as a product or service.

"**Governance Function**" refers to an internal department within the MDIA that is responsible for carrying out due diligence on Applicants and IDPSs for the purposes of issuing TARF recognitions, acknowledgments, and certifications.

"**Innovative Digital Product or Service (IDPS)**" refers to an innovative technological product, solution or service being provided by the Applicants. This generally refers to any applications and solutions (or parts thereof) which include software, code, computer protocols and other architectures which are used in the context of innovative technology.

"**Materiality**" or "**Material**" in the context of 'changes' within TARF refers to any modifications that necessitate updates or revisions to the Blueprint as provided by the Applicant to the Authority. The Authority may define any other aspects that it deems appropriate within the context of a specific IDPS as part of the onboarding process.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

"**National Competent Authority (NCA)**" or "**Lead Authority**" refers to an authority which has the necessary powers to oversee and regulate a specific area or sector.

"**Recognition**" means any form of recognition including a licence, registration, permission, authorisation, approval, acknowledgment, certification, attestation, or mark of credit, granted or issued by the Authority in accordance with the powers of the Authority.

"**Qualifying Shareholder**" refers to a person who directly or indirectly owns a percentage equivalent to twenty-five (25%) or more of the share capital and / or voting rights in a legal organisation or directly or indirectly controls a legal organisation.

"**Qualifying Transfer**" refers to the transfer of ten per cent (10%) or more of the share capital and / or voting rights in a legal organisation or the direct or indirect control of the organisation by a Qualifying Shareholder.

"**Regulations**" shall refer to the laws relating to the MDIA.

"**Resident Agent**" refers to an individual or legal organisation who is habitually resident in Malta that is appointed by an Applicant when the Applicant does not habitually reside in Malta.

"**Systems Audit**" refers to an ISAE 3000 reasonable assurance engagement. It is conducted by a Systems Auditor and whose report (ISAE 3000) is made available to the Authority by the Applicant.

"**Systems Auditor (SA)**" refers to the legal organisation, recognised and with active approval by the Authority, in accordance with the "System Auditor Guidelines". Refer to the MDIA's official website for a list of approved Systems Auditors.

"**TARF Controls**" refers to the list of control objectives that the IDPS shall be assessed against. The list of controls may vary based on the Assessment Level, the nature of the IDPS, and Control Types identified. The MDIA may also add/remove control objectives for an IDPS depending on the specific circumstances of the IDPS.

"**Technical Expert (TE)**" refers to the individual or legal organisation, recognised and with active approval by the Authority to conduct Assessments (in the form of

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

IDPS reviews) for the attainment of TARF recognition in Assessment Levels 1 and 2, in accordance with the "Technical Expert Guidelines". Refer to the MDIA's official website for a list of approved Technical Experts. A recognised Systems Auditor is automatically recognised to carry out the obligations of a Technical Expert.

"**Technological Domains**" refer to the different IDPS domains that the Assessment may be focused on. While some domains are quite specific, TARF also defines a generic IDPS domain that enables any IDPS to obtain Recognition. The MDIA is open to adding further IDPS domains to TARF depending on industry feedback on an ongoing basis.

"**Technology Assessment Recognition Framework**" and "**TARF**" refers to the current framework for recognition, certification or acknowledgement offered by the Authority as defined in this document, or any other documents referenced within.

"**Tri-party Meeting**" refers to a meeting between the Technical Expert, the Applicant, and the Authority that is applicable for Assessment Level 1 and 2. It is usually called upon submission of an Assessment but may be called by the Authority at any point.

> ***Note:*** *All other terms shall have the definition afforded to them as defined in other guidelines by the Authority or by the Act and Regulations.*

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

2 Introduction to TARF

The Technology Assessment Recognition Framework (TARF) is a tiered technology review framework by the MDIA that is designed to assess IDPS implementations from a holistic standpoint to provide varying degrees of recognition for a broad spectrum of IDPS. TARF is designed to cater for IDPS to be aligned with industry best practices. The framework is being set up with future scalability in mind such that new IDPS may be seamlessly introduced as deemed necessary by the Authority from time to time. TARF is an entirely voluntary framework, unless otherwise mandated by other NCAs or other bodies.

TARF is intended for owners and/or operators of IDPSs. It provides the IDPS with Recognition in relation to the IDPS-related controls they implement when developing and operating their IDPS. More specifically, the Assessment is meant to look into the implementation, control design and/or operating effectiveness of controls around risks IDPS holistically. Additionally, the TARF Recognition aims to provide a level of comfort to the IDPS stakeholders which may include NCAs (and other applicable sector regulators), investors, developers, suppliers, end-users, and the public.

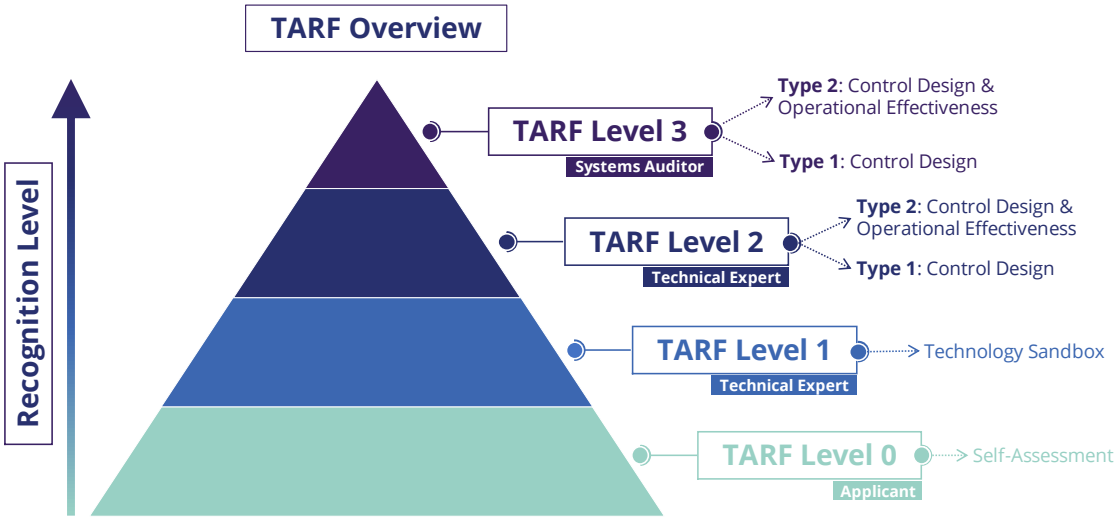


Figure 1 - An overview of the structure of TARF, with different Assessment Levels building on each other for higher Assessment Levels

Further to the Assessment Levels, TARF has been designed to be flexible to give the opportunity to Applicants to determine what they want to be assessed against, as illustrated in the Figure below, and described in the following sub-sections.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

> ***Note:*** *The Authority will be reviewing the framework on a continuous basis in view of various EU legislations that are on the horizon as well as feedback from the industry. TARF may be updated from time to time to align with such legislations.*

2.1 High-level Process

Figure 2 - The three (3) main stages of TARF

At a high level, the TARF process is split into three (3) main stages:

- **#1 Apply**: This is the stage where the Applicant reviews the guidelines and material, selects the type and attributes of the Recognition that apply to the IDPS, initiates contact with the MDIA, prepares the necessary documentation, submits the Application to the Authority and appoints an Assessor (for Assessment Levels 1-3). The Authority will carry out due diligence as applicable. This is detailed in section 3.5.
- **#2 Assess**: During this stage, the Assessor carries out the Assessment in line with the specific requirements of the identified Assessment Level, compiles the report, which is then submitted to the Authority (in line with the requirements of the respective Assessment Level). The Authority then reviews it and decides on whether to award the Recognition. This is detailed in the respective section for each Assessment Level.
- **#3 Recognition**: At this stage, provided the Authority is satisfied with the Assessment, the Authority issues the Recognition to the Applicant, and any associated conditions if and when applicable. This is detailed in each of the respective Assessment Level details, and in section 9.4.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

2.2 Assessment Level Overview

There are four (4) Assessment Levels in TARF, which increase in complexity and the level of Recognition they provide. These are:

- **Assessment Level 0**: This is in the form of a self-assessment utility that allows the Applicant to identify the maturity level of the IDPS through a quantitative assessment. It is primarily meant as an aid or educational tool for identification of gaps in relation to best practices. TARF Level 0 Assessments are domain-specific and cannot be applied for independently.
- **Assessment Level 1**: This is in the form of a Sandbox programme in which typically the Technical Expert can help carry out reviews over a period of time in line with the specific Sandbox programme.
- **Assessment Level 2**: This is in the form of an Assessment performed by a Technical Expert, typically through interviews and evidence-based analysis and verification that is qualitative in nature. The assessment may either consider the design implementation on their own or together with operating effectiveness, in relation to the controls specified by the Authority for the relevant IDPS domain.
- **Assessment Level 3**: This is the highest level of TARF Assessment that may be obtained and is typically meant for an IDPS that has a high level of maturity in place and wants or requires a high level of compliance to the relevant controls. The Assessment is conducted by a Systems Auditor in the form of an ISAE 3000 engagement, to analyse and verify that the control design, and/or operating effectiveness of the controls are aligned with those established by the Authority for such a solution, as at date of assessment and these are re-validated periodically.

Each Assessment Level adopts unique due diligence requirements as defined in each respective Assessment Level section, which is commensurate to the levels of Recognition provided by the selected Assessment Level.

The below table illustrates the qualities and features for each Assessment Level.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	TARF Level 0	TARF Level 1	TARF Level 2	TARF Level 3
Assessor	Applicant	Technical Expert		Systems Auditor
Methodology	Self-Assessment	Sandbox Programme	Technology Review	Reasonable Assurance Assessment (ISAE 3000)
IDPS Domains	Sector Specific	○ General Innovative Technology ○ Cloud Computing ○ Internet of Things ○ Artificial Intelligence ○ Blockchain		
Control Types	Specific to each Initiative	○ Accountability ○ Availability ○ Confidentiality ○ Integrity ○ Privacy		
Due Diligence	Monitoring	Prior to Onboarding		
IDPS Blueprint	Not required	Required		
Nature of Assessment	Questionnaire	Programme-specific	IDPS Review Report	ISAE 3000
Assessment Scope	Maturity Assessment	Maturity development	○ **Type 1**: Control Design Implementation ○ **Type 2:** Control Design Implementation & Operating Effectiveness	

2.3 IDPS Domains

For Assessment Levels 1 (when applicable in line with the respective Sandbox programme), 2 and 3 the Applicant will be asked to identify the IDPS domains to be assessed as part of the application. TARF currently supports the below IDPS domains:

- **General IDPS**: refers to digital technology in the form of on-premises computing systems and services, including servers, storage, databases, networking, software, analytics, and automation.
- **Cloud Computing**: refers to the computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet (also defined as "the cloud"). These controls may be further

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

classified into controls for Cloud Service Providers or controls for IDPS that utilise cloud technologies.

- **Internet of Things (IoT)**: refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.
- **Artificial Intelligence (AI)**: refers to innovative technology that leverages computers and machines to mimic the problem-solving, decision-making, and cognitive capabilities of the human mind.
- **Distributed Ledger Technologies (DLT)**: refers to a distributed technology that maintains a continuously growing list of ordered records, called blocks, including blockchain and smart contracts. A DLT is a decentralized, distributed, and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.

These domains are meant to be complimentary, and the Applicant may choose multiple domains depending on their objectives when applying for TARF.

> ***Note:*** *The Authority will be constantly open to feedback in parallel with monitoring the industry and may amend or add new IDPS domains at any time throughout the lifetime of TARF. Furthermore, while the Applicant is required to identify the relevant IDPS domain, the Authority reserves the right to require a particular domain it deems applicable to be included in scope.*

2.4 Control Types

The Control Types are divided into five (5) categories. The Applicant may select from the combination of any one (1) to five (5) categories, to identify which control objectives are deemed in-scope for the Assessment.

More specifically, the control types are:

- **Accountability** is the principle that an individual is entrusted to safeguard and control information and keying material, while being responsible / liable to proper authority for the loss of, or misuse of that information.
- **Availability** relates to providing authorized subjects timely and uninterrupted access to objects.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

- **Confidentiality** is the concept of the measures used to ensure the protection of the secrecy of data, objects, or resources.
- **Integrity** is the concept of protecting the reliability and correctness of data.
- **Privacy** is the active prevention of unauthorized access to information that is personally identifiable.

> ***Note:*** *While Applicants may choose which of the above Control Types to include or exclude from scope of the Assessment (and Recognition), the Authority reserves the right to request Applicants to amend their application or otherwise reject it if it deems that the identified Control Types are not suitable and sufficient in relation to the risk exposed by the IDPS.*

2.5 MDIA Recognition

TARF Recognition is tailored to the needs of the IDPS and varies depending on the nature of the IDPS and the Assessment Level, typically:

- **Acknowledgement**: This is provided for by TARF Assessment Level 0 and while primarily meant to indicate participation, may also include additional information specific to the Assessment. This acknowledgement is typically issued automatically but may be revoked at the discretion of the Authority for non-compliance or any other reason.
- **Mark of Credit**: This is provided for by TARF Assessment Level 1 and 2 and demonstrates that the Applicant satisfactorily underwent the appropriate level of Assessment. This is issued at the discretion of the Authority when it agrees that any issues reported by the Technical Expert, if any, were of a minor or non-critical nature.
- **Certification**: This is provided for by TARF Assessment Level 3 and demonstrates that the Applicant satisfactorily underwent an Assessment by a Systems Auditor. This is issued at the discretion of the Authority when it agrees that any issues highlighted by the Systems Auditor, if any, were of a minor or non-critical nature.

Recognitions issued by the MDIA under TARF shall be strictly limited to the aspects of the IDPS and its use as identified by the Applicant. The Authority shall not be certifying the fitness and propriety of the Applicant or other entities related to the IDPS (or any of their directors, shareholders or employees). Any due diligence checks that may be performed by the Authority are strictly for administrative purposes.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

A Recognition issued by the MDIA is not meant to be interpreted as a guarantee that the IDPS is unable to fail but is merely to serve as proof that a certain level of maturity has been achieved in developing, deploying and operating an IDPS.

Note 1: *The provision of recognitions by the MDIA under the TARF framework may not necessarily mean the same recognition as defined by the MDIA Act, Chapter 591 of the Laws of Malta or the ITAS Act, Chapter 592 of the Laws of Malta.*

Note 2: *The Authority reserves the right to withdraw a Recognition should the terms of these Guidelines, including those highlighted in section 10.1 be violated, or new information surface after issuance and the Applicant fails to provide a satisfactory response.*

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

3 Application

This section provides information about the application process. It is aimed towards helping prospective applicants in preparing for the Application and the TARF process.

Prospective applicants are encouraged to contact the MDIA with any questions they may have.

3.1 Eligibility

Any individual or legal organisation that develops, operates, or otherwise has rights to an IDPS may apply for the TARF (the Applicant). The Applicant must have a reasonable element of substance in connection to Malta (as defined in the *Guidelines on the definition of In or from Malta*) and may apply for Recognition following the successful completion of the Application form and procedures in line with the requirements established in this section.

> ***Note:*** *The Authority may, from time to time, publish additional documents, guidelines, or other material to cater for the Recognition of other technology domains in addition to the ones current established in TARF. In such instances the eligibility criteria defined in such additional guidelines will also apply to the eligibility criteria listed in these TARF guidelines, unless otherwise specified in the newly issued guidelines.*

3.2 Applicant Obligations

TARF provides the Applicant with flexibility to identify which Assessment Level, Control Types, and Technology Domains are to be in scope in obtaining their Recognition, and the Authority will tailor the process depending on the selections.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

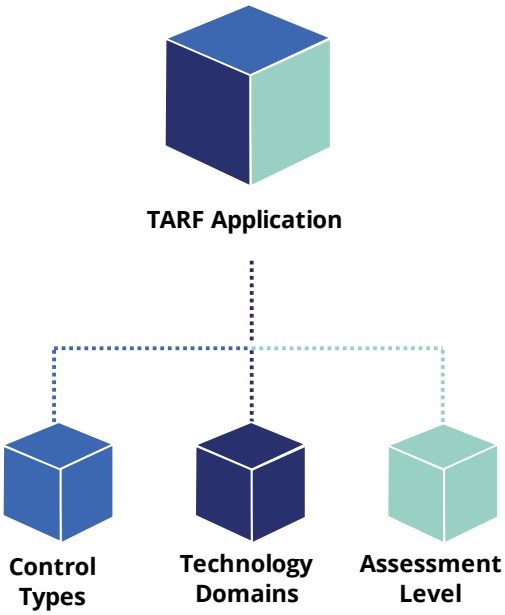


Figure 3 - TARF Application Components

While the TARF Recognition process varies depending on the Assessment Level selected, prospective Applicants for TARF Assessment Levels 1 (when required by the respective Sandbox programme), Levels 2, and 3 must submit a *TARF Application Form* to the Authority, including the IDPS Blueprint and other supporting documentation required.

3.3 Application Processing

When processing the Applicant's request, the Authority will:

- Review and assess the information provided in the TARF Application Form.
- Review the documentation submitted as detailed in these guidelines (such as, but not limited to, the IDPS Blueprint), as well as any additional documentation that the Authority may request on a case-by-case basis.
- Carry out the necessary due diligence on the Applicant, in accordance with the Applicant's selected Assessment Level.
- Assess whether the appointed Assessor is sufficiently competent to fulfil its role with respect to the Application, and according to the selected Assessment Level, Technology Domains and Control Types.
- Assess whether the Applicant is sufficiently competent to fulfil its role with respect to the Application and conduct necessary due diligence.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

The Authority reserves the right to respond to the submission of an Application Form by recommending alterations to the Assessment Level, Technology Domains and/or Control Types identified. Without prejudice to any other right which the Authority has when refusing an Application Form in terms of these Guidelines. the Authority further reserves the right to turn down the Applicant's Application Form on the basis that the type of Recognition selected in the Application Form does not align to the risks presented by the IDPS. In such cases, the Authority will provide its reasons in writing.

The Due Diligence procedures carried out by the Applicant vary depending on the selected Assessment Level. Details are provided in the section detailing each respective Assessment Level.

3.4 IDPS Blueprint

The Blueprint is a document, created by the Applicant, which highlights all of the critical and important information and features relevant to an IDPS when submitting an Application Form to the Authority. This document will also be used by the Assessors to understand their scope of work.

For an Application Form to be considered by the MDIA, the Applicant must include justification on why the Recognition is being sought in the IDPS Blueprint, clearly indicating:

- The mandate that entitles the Applicant to submit such an Application Form, and
- The governance structures of the owners of the IDPS.

At a minimum, the submitted IDPS Blueprint document must follow the template provided by the Authority in section 13.3, which also specifies live logging requirements (refer to section 9.5).

A sample Blueprint that presents an example of how a Blueprint can be tackled (for a hypothetical system) is presented in section 14.

3.4.1 IDPS Logging Mechanism

The Blueprint must clearly document the implementation of a logging mechanism as further described in section 9.5. This requirement applies to any Applicant undergoing Assessment Levels 1-3.

In this regard, the IDPS Blueprint must include:

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

- Clear identification of the datasets and events which will be collected and retained in the logs. If the Applicant believes there is justification for any key datasets or event logs not to be included, clear justification must also be provided.
- Clear description of the security measures and mechanisms in place to ensure that data stored in the logs cannot be tampered with and to ensure appropriate protection against unauthorised access, unlawful processing or loss of data.
- Privacy and retention policies justifying the storage, deletion and access parameters of the logs in order to ensure compliance with applicable laws, including data protection laws. This is to include security and access control considerations to ensure legal compliance.
- Detailed documentation of how the purpose of the logs, as defined in section 9.5 of the TARF Guidelines, is achieved by the IDPS infrastructure.
- Clear information on the physical aspects of the logging infrastructure, including the location of the server and the hardware used.
- Access control procedures in place to identify who can access the data and to ensure that only authorised personnel can access information and intervene when legally bound to do so. Procedures must also specify how direct access may be provided to relevant authorities and law enforcement agencies if necessary.

3.5 TARF Application Procedure

The process for applying for TARF approval and associated activities is outlined in step-by-step milestones below:

1. The Applicant may engage with the MDIA to establish preliminary communication channels as well as to enquire on assistance related to a TARF application. This step is optional but recommended.
2. The Applicant obtains and reviews all necessary information, documentation and the Application Form(s) related to a TARF from the MDIA website.
3. The Applicant obtains all information required by the Applicant (including documentation mentioned in these guidelines), and compiles the application, including supporting documentation. The Applicant must submit:
    a. The relevant TARF Application Form,

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

   b. The identification of Assessment Level, Technology Domains, and Control Types for which certification is being sought,
   c. The IDPS Blueprint in line with the template provided,
   d. Fit and Proper Questionnaires,
   e. The applicable documentation required for the due diligence process, as defined in the Application Form and fit-and-proper requirements.
4. The Applicant submits the compiled documentation to the MDIA, together with the relevant application fee. Documentation may be submitted as either soft or hard copies, however in case of soft-copy submission the Authority reserves the right to request hard-copy documents, with relevant wet-ink signatures to the MDIA offices.
5. The Authority processes the application by:
   a. Verifying the completeness of the application.
   b. Performing due diligence checks on the Applicant and any necessary IDPS personnel.
   c. Reviewing and evaluating the relevance of the selected Assessment Level, Technology Domains, Control Types and IDPS Blueprint.
   d. If deemed necessary, recommending alterations to the Assessment Level, Technology Domains, Control Types, or requesting revisions to the submitted IDPS Blueprint.
6. The Authority may conduct interviews with the Applicant or any one or more individuals subject to the fit-and-proper assessment.
7. The Authority notifies the Applicant of its decision on whether to accept or reject the application. In case of a rejection at this stage, the process stops here.
8. If accepted, the Applicant formally engages an approved Assessor (Technical Expert for Assessment Levels 1 or 2, and Systems Auditor for Assessment Level 3).
9. The Assessor reviews the IDPS and upon acceptance of engagement by the Applicant notifies the Authority.
10. The Authority reviews the Assessor's competency in view of the Application and notifies the Applicant and Assessor to proceed with the Assessment, or alternatively, to engage a different Assessor with competency in the subject matter of the requested Certification.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

The Assessment process then proceeds in line with the identified Assessment Level, as described in the section detailing the Assessment Level Methodology.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

4 Assessors

Assessors play a pivotal role in TARF, as they are tasked with meticulously reviewing or auditing the IDPS in alignment with the Applicant's submission, as approved by the Authority. This determines the Assessment Level and thus controls that are in scope. There are two main types of Assessors: Technical Experts and Systems Auditors.

Technical Experts (in the context of TARF Level 2 Assessments) or Systems Auditors (in the context of TARF Level 3 Assessments) may be required to carry out one of two different types of assessments:

- **Type 1**: This assessment focuses on the design and implementation of the technology solution.
- **Type 2**: This assessment delves deeper, covering both the design implementation and the effectiveness of controls in place.

In the absence of an available MDIA approved Systems Auditor or Technical Expert for any of the identified technology domains, the Authority reserves the right to identify any other person to carry out such an assessment.

> ***Note:*** *Detailed requirements for each Assessor are further defined in the respective Assessment Level in sections 6, 7, and 8.*

4.1 Technical Expert

Technical Experts are individuals that have secured approval and have a valid authorization from the Authority to act as a Technical Expert. The Technical Expert must be approved by the Authority prior to the undergoing of an Assessment for an Applicant.

The role of a Technical Expert revolves around conducting specialized technology reviews at Assessment Levels 1 or 2. They assess and report on technology solutions based on the guidelines set by the MDIA. Their evaluations, while detailed, might not carry the same weight as those conducted by Systems Auditors due to the absence of international standards, although they are still responsible to abide by the MDIA's guidelines, terms and conditions.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

4.2 Systems Auditor

Systems Auditors are legal organizations that have secured approval and have a valid authorization from the Authority to act as Systems Auditors. The Systems Auditors must be approved by the Authority prior to the undergoing of an Assessment for an Applicant.

In the context of TARF, their primary responsibility is to evaluate technology solutions for Applicants wishing to obtain Recognition at Assessment Level 3. This must be conducted in line with the ISAE 3000 international standard, specifically for reasonable assurance engagements.

> ***Note**: Systems Auditors with a valid authorization from the MDIA are also able to adopt the role of a Technical Expert to carry out engagements at Assessment Level 1 or 2.*

4.2.1 Applicability of the '*Systems Auditor Guidelines*' document

Without prejudice to the below table, the Systems Auditor Guidelines document, published under the ITAS framework applies to the TARF. This means that Systems Auditors recognised under ITAS will be able to carry out Assessments at Level 3 under TARF, subject to the TARF-specific conditions being met.

Any new Systems Auditors may apply under the ITAS Systems Auditor guidelines.

In addition to the Systems Auditor Guidelines published under the ITAS framework, ITAS Recognised Systems Auditors must meet the below criteria to be able to conduct Assessments at Level 3 under TARF:

1	Within the context of the *ITAS Systems Auditor* guidelines, the standalone term '*ITAS*' may be understood to carry the same meaning as an '*IDPS*'.
2	The execution of the ISAE 3000 report must be conducted in accordance with the relevant provisions of the Accountancy Profession Act (Cap. 281) and in adherence to the standards and ethical requirements as prescribed by the Accountancy Board of Malta.
3	The Systems Auditor under TARF are not responsible to carry out Security Testing. The Subject Matter Experts are therefore exempted from holding certification in information security assessment.
4	The report must be submitted to the Authority by the Applicant.
5	For the avoidance of doubt, the Systems Audit engagement and report must follow the ISAE 3000 reasonable assurance standard.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

6	The Systems Auditor and Applicant's agreement for the Assessment must include a provision for the MDIA to have the right to access the ISAE 3000 report when completed, as well as to communicate with the Systems Auditor for the purposes of verifying the authenticity of the report or obtaining clarifications.
7	The applicable Control Objectives are in line with the TARF Control Objectives, published in a separate document to these Guidelines.
8	The role of a Technical Administrator is not required for TARF, unless specifically mandated by the Authority.
9	The Fee Structure has been revised as published within the TARF Administrative Fee Guidelines.
10	The Enhanced Systems Auditor is not applicable to TARF.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

5 Level 0: Self-Assessment

The TARF Assessment Level 0 (hereinafter referred to simply as Level 0) provides an easy-to-access and easy-to-use quantitative and qualitative self-assessment programme, that provides immediate feedback and is meant to be primarily utilised as an educational tool, with Recognition in the form of a merit provided to the applicants for participation.

This aspect of TARF creates a structure around which the MDIA or other NCAs (in conjunction with the MDIA), may release programmes from time-to-time. As a result, it is important to note that an Applicant cannot directly apply for a Level 0 Assessment, unless it is through a designated programme.

> ***Note:*** *An example of such a TARF Assessment Level 0 programme is the Mind the Gap initiative (https://www.mdia.gov.mt/schemes/mind-the-gap), which provides a tool for e-commerce service providers to carry out a self-assessment and identify their maturity levels in relation to cybersecurity best practices..*

5.1 Target Audience

While each TARF Assessment Level 0 initiative may vary in domain and scope, depending on the specific programme on initiative that is launched by the Authority, Level 0 initiatives are intended to appeal to a wide range of audience.

Level 0 initiatives are intended to provide a low barrier to entry. They are designed for Applicants to be able to undergo the Assessment themselves, providing they have knowledge of IT Systems, by scoring a set of questions in the form of a questionnaire. However, for maximum flexibility Applicants are also able to engage 3rd parties to carry out the self-assessment for them (unless otherwise stated in the specific Level 0 initiative guidelines or terms and conditions).

TARF Level 0 initiatives may optionally be accompanied by incentives and/or grants by other government entities to further encourage the uptake, promote educational awareness and incentivise Applicants who wish to improve their maturity levels.

5.2 Due Diligence

A TARF Level 0 Applicant must provide identification information and documentation necessary to identify the Applicant, both when the Applicant is

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

applying in his personal capacity as well as when doing so in representation of a legal organisation (if applicable).

While TARF Level 0 is a self-assessment and is meant to be completed from start to finish at the Applicant's convenience, the Authority will be monitoring the information provided and reserves the right to request further documentation to verify any claims made.

5.3 Controls

While Level 0 initiatives vary between Technology Domains, they take a quantitative approach that is based on providing an answer to identify a maturity score for each applicable control, and controls are grouped in control categories. The control categories are presented in Appendix 13.1. The Authority may choose to add additional domain-specific control categories depending on the initiative.

For ease of use, each control will be presented in the form of a question and will have six (6) specific answers associated to it, each linked to a specific maturity level, so that the Applicant may easily select the answer that best applies to their IDPS. As part of these six (6) options, the Applicant has the option to mark the question as not applicable to their IDPS, which will not negatively affect the overall maturity level. The Applicant will also have the option of answering a question as 'Do not know', which allows Applicants to still undergo a Level 0 assessment even when they are unable to adequately assess the maturity level of specific controls.

The specific controls (questions), and the corresponding answers (maturity levels) will be published as part of the guidelines for each TARF Level 0 initiative that the Authority publishes.

5.4 Report

Upon completion of the self-assessment, the Applicant will be presented immediately with the overall maturity level and the maturity level per category, with each maturity level typically ranging from zero to five (0-5). This will enable the Applicant to determine what their maturity levels are, and by extension where their strengths and weaknesses lie. The overall maturity level descriptions are presented in Appendix 13.2.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

5.5 Methodology

While TARF Level 0 Assessment is in the form of a self-assessment, the Applicant must ensure that they read and accept the conditions laid down in the guidelines, terms and conditions and any other material published as part of that specific TARF Level 0 initiative.

TARF Level 0 initiatives will be made available through an online portal for an easy and seamless experience. This is intended to allow the Applicant to register and undertake the self-assessment immediately by answering the questionnaire. Responses provided are saved securely against the registered account and the Applicant may also choose to complete their self-assessment at a later date.

Once the Applicant completes the self-assessment, they will be provided with the maturity levels based on their responses, which can be analysed by the Applicant to identify particular strengths and weaknesses across the control categories. At this point, the Applicant may also opt to obtain Recognition by the Authority as further detailed in section 5.6.

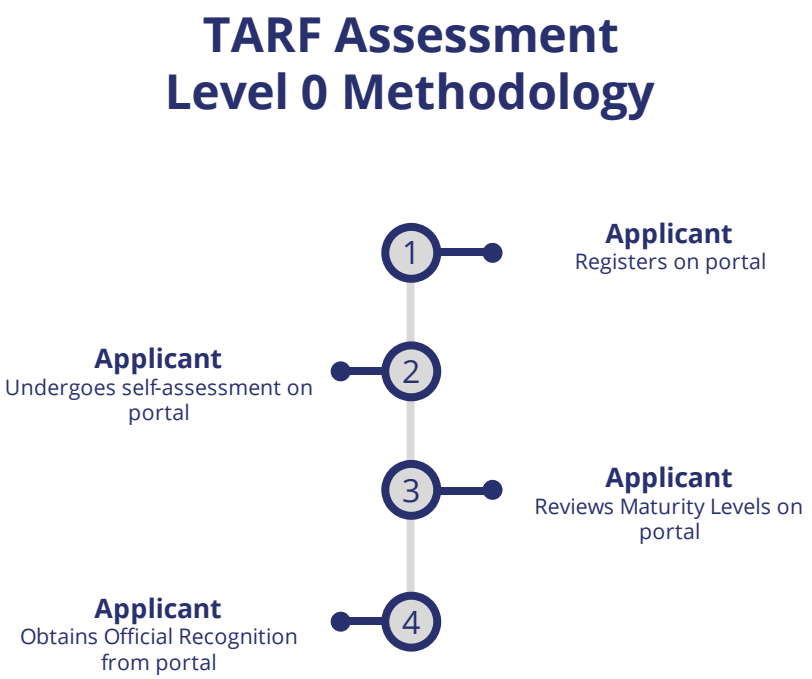


Figure 4 - TARF Assessment Level 0 Methodology

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

> ***Note:*** *While the Authority does not necessarily conduct specific on-boarding due-diligence for TARF Level 0, the Authority will still carry out due-diligence and compliance through monitoring of the information provided by the Applicant and reserves the right to take appropriate action in case of misuse or violation of any terms or conditions.*

5.6 Recognition

Once the TARF Level 0 self-assessment is completed and the Applicant is presented with the assessment outcomes, the Applicant may optionally choose to obtain the Recognition issued by the Authority in the Applicant's name.

The Recognition for TARF Level 0 will be in the form of a digital acknowledgement that serves to highlight participation in the TARF Level 0 initiative and may be shared digitally on the Applicant's appropriate channels. The Recognition for TARF Level 0 is meant to be used to publicly demonstrate initiatives undertaken by the Applicant in improving their innovative technology maturity levels.

While the TARF Level 0 Assessment is meant to be as hands-off as possible, the Authority will conduct random checks and reserves the right to withdraw the Recognition, for reasons such as (but not limited to) evidence indicating abuse or misuse of the programme, or non-compliance with requirements set out by the specific initiative.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

6 Level 1: Technology Sandbox

The TARF Assessment Level 1 (hereinafter referred simply as Level 1) refers to Technology Sandbox programmes published by the Authority. The Level 1 Assessment is meant to provide the Applicant with an opportunity to develop the IDPS controls over time and at their own pace to increase the levels of maturity to the desired targets.

The Authority may offer various Technology Sandbox programmes under TARF Assessment Level 1. As a result, it is important to note that an Applicant cannot directly apply for a TARF Level 1 Assessment, unless it is through a designated programme.

The MDIA currently has a "Technology Assurance Sandbox" programme in place that supports all the different technology domains in line with TARF. More information may be found on https://www.mdia.gov.mt/technology-assurance-sandbox/.

> ***Note:*** *The Authority may launch or update new Sandbox programmes from time-to-time that may tackle different niches, such as but not limited to specific industries, technology domains, or user-base.*

6.1 Target Audience

TARF Level 1 is intended for Applicants whose IDPS is in early stages of maturity and would like to identify any potential weaknesses or areas to strengthen through an independent Assessment over a specified period of time, which is defined by the specific programme itself. While this is typically envisaged to be start-ups or small-to-medium sized operations, it may apply to any Applicant that wishes to develop their maturity and obtain Recognition by the Authority to show that they have looked and considered certain aspects of the IDPS.

6.2 Due Diligence

Due diligence requirements for Assessment Level 1 are specific to the specific Sandbox Programme.

Typically, they focus on establishing that the Applicant and key stakeholders within the Applicant's legal organisation are fit and proper, and that any documentation that is required, such as a blueprint and a residency plan, is provided and contains adequate level of detail.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Once the programme-specific onboarding procedure is completed, the Authority will inform the Applicant about the acceptance or rejection of the Application in writing within 30 days.

> ***Note 1**: When the Applicant is a Government of Malta entity or a company with a Government of Malta majority shareholding, it shall only be requested to provide a Board Resolution or a confirmation from a legal representative or a similar document authorising the said entity to submit an Application and to be bound by the terms of the MDIA TARF and authorising the signatory to sign on its behalf.*
>
> ***Note 2**: When an Applicant is already licensed by another National Competent Authority that carries out similar Due Diligence, the MDIA may provide exemptions from pertinent Due Diligence Requirements, subject to any confirmation required by the MDIA.*

6.3 Controls

Control requirements for Assessment Level 1 are specific to each Sandbox Programme.

Please refer to the specific Sandbox programme for more information.

6.4 Report

For the purposes of obtaining TARF recognition, an independent Technical Expert Assessment that documents the Applicant's journey through the Sandbox programme and documents the progress together with any outstanding issues must be submitted to the Authority for evaluation prior to issuance of TARF Recognition.

In sandbox programmes, such as TAS, where Technical Expert Assessments are an integral part of the programme itself, the final Technical Expert Assessment may be utilised to obtain TARF Recognition, subject to the Authorities positive evaluation in this regard.

6.5 Assessment Process

The Assessment Process for Assessment Level 1 is specific to each Sandbox programme.

Please refer to the specific Sandbox programme for more information.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

6.6 Recognition

Recognition for TARF Level 1 will be in the form of a mark of credit issued in an electronic document to the Applicant that among others identifies the Applicant, as well as the applicable Sandbox Programme, period of validity, and any other details deemed relevant by the Authority. The mark of credit is valid for two (2) years from the date of issuance.

The mark of credit will be published on the Authority's website during its period of validity. Additionally, there is also an obligation on the Applicant to link to the Authority issued mark of credit on its website and, if applicable, refer to it on its IDPS.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

7 Level 2: Technology Review

The TARF Assessment Level 2 is a qualitative Assessment carried out by a Technical Expert on an IDPS. The Technical Expert (or Systems Auditor) must be approved by the MDIA and must be independent from the Applicant or IDPS.

TARF Level 2 Assessment may be in the form of two (2) types:

- **Type 1**: The Technical Expert reviews the design implementation of the controls, as of a specific point in time.
- **Type 2**: The Technical Expert evaluates the design implementation of the IDPS as well as the effectiveness of the controls over a specific period.

Applicants are encouraged to start with a Type 1 Assessment and then moving onto a Type 2 Assessment.

TARF Level 2 Assessments are also carried out via interviews and evidence-based collection and analysis carried out by the Technical Expert, which evidence must include material supporting the findings. For TARF Level 2 Assessments, the Technical Expert must draft a report outlining their findings and any recommendations, prior to discussion with the MDIA in a tri-party meeting.

For TARF Level 2 Type 2 Assessments, the Applicant must specify the period within which the operating effectiveness review is in scope. This must be a minimum of 6 months but may be adjusted subject to the Authority's approval.

7.1 Target Audience

TARF Assessment Level 2 targets Applicants who wish to obtain a Recognition subject to a Technology Review conducted by an independent Technical Expert. This is meant to assist the Applicant in identifying strengths and weaknesses of the IDPS in the control design and implementation (Type 1), and subsequently also provide insight on how those controls performed during operation (Type 2). The Recognition for TARF Level 2 presents a balanced opportunity for Applicants who wish to review their operation and provide a higher peace of mind to their stakeholders than TARF Level 1, without undergoing an in-depth rigorous audit (see TARF Assessment Level 3).

The TARF Level 2 Assessment is carried out by an independent Technical Expert in the form of an innovative technology review, with a Recognition (in the form of

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

a mark of credit) issued by the Authority should the Assessment be satisfactory to the Authority for issuing of such.

7.2 Due Diligence

Due diligence requirements for Assessment Level 2 focus on establishing that the Applicant and key stakeholders within the Applicant's legal organisation are fit and proper.

As part of the application form, the Applicant is required to submit the requested documentation which will include, but shall not be limited to:

- Memorandum and Articles of Association, Certificate of Registration, Certificate of Incumbency or Equivalent Documents, required to ascertain the ownership and control/governance of the Applicant.
- The organisational structure chart of the Applicant which clearly indicates the key stakeholders within the legal organisation.
- Valid passport or identity documentation necessary to verify the identity of the Applicant.
- Proof of address of the Applicant.
- Valid Police Conduct Certificate of the Applicant.
- When the Applicant is a legal organisation, a Board Resolution by the legal organisation's Board of Directors/Administrators, or a similar document, resolving that the legal organisation is to submit an application and is to be bound by the terms of the TARF and authorising the signatory to sign on its behalf.

Once all the requested documents have been received, the Authority will inform the Applicant about the acceptance or rejection of the Application in writing within 30 days.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

***Note 1**: When the Applicant is a Government of Malta entity or a company with a Government of Malta majority shareholding, it shall only be requested to provide a Board Resolution or a confirmation from a legal representative or a similar document authorising the said entity to submit an Application and to be bound by the terms of the MDIA TARF and authorising the signatory to sign on its behalf.*

***Note 2**: When an Applicant is already licensed by another National Competent Authority that carries out similar Due Diligence, the MDIA may provide exemptions from pertinent Due Diligence Requirements, subject to any confirmation required by the MDIA.*

7.3 Controls

TARF Level 2 Assessments, including the scope of the Assessment carried out by the Technical Expert are based on the Technology Domains (refer to section 2.3) and Control Types (refer to section 2.4) selected by the Applicant (and subject to review by the Authority) at application stage (refer to section 3).

7.4 Report

The Technical Expert must draft the report in line with the relevant Controls (depending on the Technology Domains and Control Types selected by the Applicant). A Report template is provided in the separate Technology Review Report Template.

Upon completion of the TARF Level 1 Assessment report by the Technical Expert, the report is submitted to the Authority for review and a follow-up discussion will take place during a tri-party meeting between the Authority, IDPS/Applicant, and the Technical Expert.

In view of this information, the Authority, through the information documented by the Technical Expert, will take a decision on whether to issue the Official Recognition to the IDPS, with or without conditions (such as, to remediate designs within a stipulated period), or whether to reject issuance of the Official Recognition, particularly in cases of significant deficiencies.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

7.5 Assessment Process

The below steps describe the steps involved in the TARF Level 2 Assessment:

1. The Technical Expert schedules the review(s) with the Applicant.
2. The Technical Expert conducts the review, with full cooperation from the Applicant and any stakeholders necessary and drafts the Assessment (report).
3. The Technical Expert may request additional follow-ups and/or evidence to be provided or reviewed.
4. The Technical Expert notifies the Authority and the Applicant that the Assessment has been conducted, and the report has been prepared, and issues the report to the Applicant for submission to the Authority.
5. After an initial review the Authority schedules the Tri-Party meeting.
6. In the Tri-Party meeting stakeholders discuss the outcome of the Assessment. The MDIA may request further clarifications, if deemed necessary, in which case the Assessment needs to be updated by the Technical Expert until the MDIA is satisfied that the report has adequately addressed any outstanding matters.
7. In case the Assessment identifies non-conformities of a material nature, the Authority may at its discretion provide the Applicant with a specified period of time to remediate them (no longer than 6 months).
8. The Authority issues the Recognition to the Applicant.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

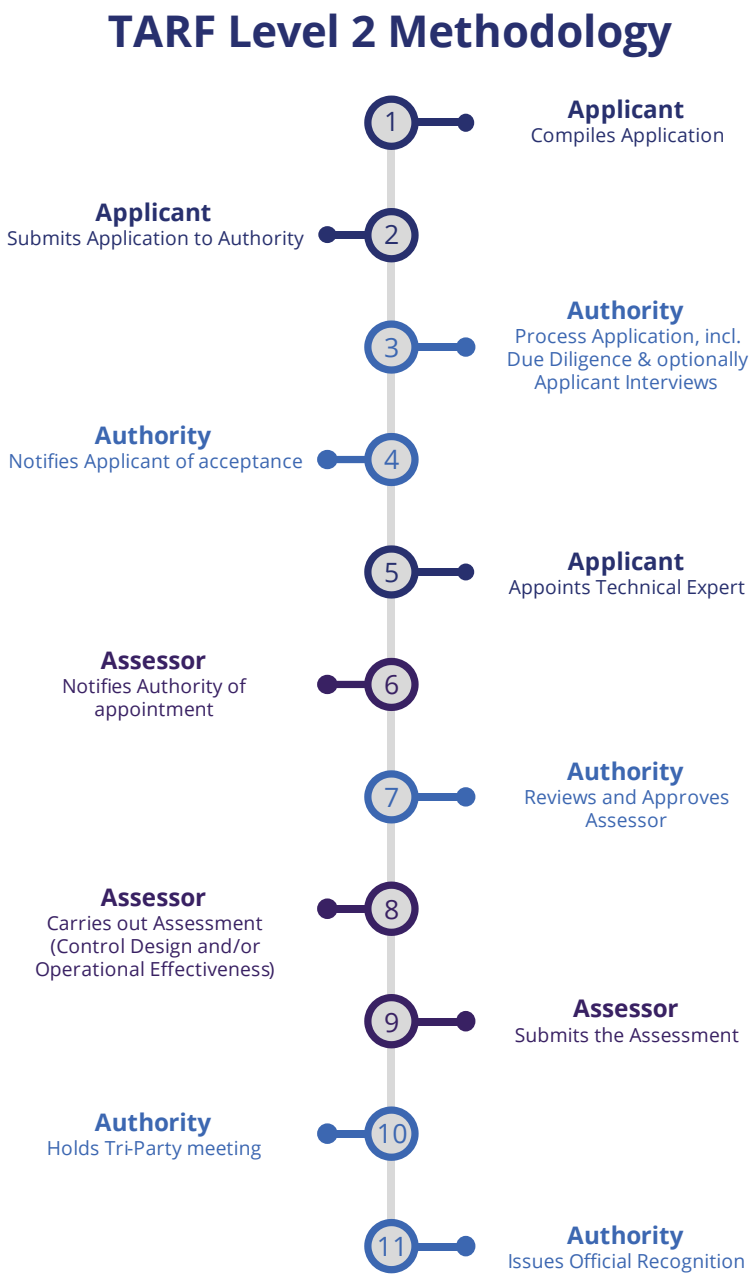


Figure 5 - TARF Assessment Level 2 Process

> ***Note**: The Applicant may also choose to nominate a Technical Expert at application stage, rather than after the application has been processed and accepted.*

7.6 Recognition

Recognition for TARF Level 2 will be in the form of a mark of credit issued in an electronic document to the Applicant that among others identifies the Applicant, as well as the Technology Domain, and Control Types subject to Assessment,

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

period of validity, and any other details deemed relevant by the Authority. The mark of credit is valid for two (2) years from the date of issuance.

The mark of credit will be published on the Authority's website during its period of validity. Additionally, there is also an obligation on the Applicant to link to the Authority issued mark of credit on its website and, if applicable, refer to it on its IDPS.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

8 Level 3: ISAE 3000 Reasonable Assurance Engagement

A TARF Assessment Level 3 (hereinafter referred simply as Level 3) represents the highest level of Recognition possible within TARF. It is primarily intended for more mature and large-scale IDPS. It offers a qualitative set of control objectives ranging from control design to control operating effectiveness to ensure robustness and a high-level of technology preparedness against sophisticated threats.

A TARF Level 3 Assessment may only be conducted by an MDIA approved Systems Auditor, through an ISAE 3000 reasonable assurance engagement between the Systems Auditor and the Applicant.

TARF Level 3 Assessment may be in the form of two (2) types:

- Type 1: The Systems Auditor expresses an opinion on whether the description of the IDPS is fairly presented and whether the control objectives that are in-scope are suitably designed to meet the applicable criteria.
- Type 2: In addition to the opinion expressed in a Type 1 Assessment, the Systems Auditor will also express an opinion on both the control design and operating effectiveness of the controls during the period covered by the audit, which may be between 6 months and 1 year, unless otherwise agreed to with the Authority in writing. This type of audit may be carried out periodically during the operational lifetime of the IDPS, or on the request of the Authority.

The indicative minimum period between a Type 1 and a Type 2 report is 6 months.

8.1 Target Audience

TARF Level 3 is aimed towards Applicants who are looking for the highest level of Recognition from TARF on their IDPS, by undergoing a Systems Audit by an MDIA-approved Systems Auditor. TARF Level 3 is primarily intended to apply to mature large-scale IDPS, such as one that has a large user base or IDPS in which the Applicants want to obtain the maximum level of comfort by ensuring a higher level of adherence to industry standards. Because of this, TARF Level 3 Assessments require the highest level of preparation and maturity due to the detailed nature of a Systems Audit.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

8.2 Due Diligence

Due diligence requirements for TARF Level 3 are the most onerous due to the higher level of Recognition provided.

It focuses on establishing that the Applicant and key stakeholders within the Applicant's legal organisation are fit and proper. Such stakeholders may include the Managing Director (Chairperson), the Chief Executive Officer (CEO) or equivalent roles and any other individual responsible for the roll-out and upkeep of the innovative technology (such as Chief Technology Officer (CTO) or the Chief Information Officer (CIO) or equivalent roles).

As part of the application form, the Applicant is thereby required to submit the requested documentation which will include, but shall not be limited to:

- Applicant organisation's Memorandum and Articles of Association, Certificate of Registration, Certificate of Incumbency or Equivalent Documents, required to ascertain the ownership and control/governance of the Applicant.
- The organisational structure chart of the Applicant's legal organisation which clearly indicates the Managing Director (Chairperson) or the Chief Executive Officer (CEO) or equivalent roles responsible for the roll-out and upkeep of the innovative technology within the legal organisation.
- Valid passport or identity documentation necessary to verify the identity of the Applicant, the Managing Director (Chairperson) or the Chief Executive Officer (CEO) or equivalent roles.
- Proof of address of the Applicant, the Managing Director (Chairperson) or the Chief Executive Officer (CEO) or equivalent roles.
- Valid Police Conduct Certificate of the Applicant, the Managing Director (Chairperson) or the Chief Executive Officer (CEO) or equivalent roles.

Once all the requested documents have been received, the Authority will inform the Applicant about the acceptance or rejection of the Application in writing within 30 days.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

***Note 1**: When the Applicant is a legal organisation, a Board Resolution by the legal organisation's Board of Directors/Administrators, or a similar document, resolving that the legal organisation is to submit an application and is to be bound by the terms of the TARF and authorising the signatory to sign on its behalf.*

***Note 2**: When the Applicant is a Government of Malta entity or a company with a Government of Malta majority shareholding, it shall only be requested to provide a Board Resolution or a confirmation from a legal representative or a similar document authorising the said entity to submit an Application and to be bound by the terms of the MDIA TARF and authorising the signatory to sign on its behalf.*

***Note 3**: When an Applicant is already licensed by another National Competent Authority that carries out similar Due Diligence, the MDIA may provide exemptions from pertinent Due Diligence Requirements, subject to any confirmation required by the MDIA.*

8.3 Controls

TARF Level 3 Assessments, including the scope of the Assessment carried out by the Systems Auditor are based on the Technology Domains (refer to section 2.3) selected by Applicant (and subject to review by the Authority) at Application stage (refer to section 3).

While there is still a degree of flexibility in identifying the technology domain(s), all the Control Types are considered to be in scope (unless otherwise agreed to by the Authority and the Systems Auditor) due to the higher level of Recognition provided by the Authority for TARF Level 3 Assessments.

The Authority reserves the right to impose any specific Technology Domains or Control Types it deems necessary at application stage.

8.4 Report

The TARF Level 3 Assessment is in the form of an ISAE 3000 reasonable assurance engagement carried out by a Systems Auditor and which is compiled into an ISAE 3000 report. Once compiled, this report is submitted to the Applicant who then submits it to the Authority for review. The Authority reserves the right to hold separate follow-up discussions with the Applicant and/or the Systems Auditor in

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

correspondence or a meeting for further clarifications, such as to confirm the authenticity of the submitted report.

While the report is written for the Applicant, it must provide the Authority the right to access the report. In this regard, the Systems Auditor must ensure that conditions to allow the Authority to have access to the report is provided for in the Letter of Engagement as well as in the report itself. Furthermore, the Applicant must give the Auditor the authorization to provide answers to any clarifications the Authority may require.

Following submission of the report, the Authority will take a decision on whether to issue the Recognition for TARF Level 3 to the IDPS, with or without conditions (such as to add or improve controls within a stipulated period), or whether to reject issuance of Recognition, particularly in cases of significant deficiencies.

8.5 Assessment Process

The below steps describe the steps involved in the TARF Level 3 Assessment:

1. The Systems Auditor and Applicant make logistical arrangements for the ISAE 3000 reasonable assurance engagement. The Applicant must agree to terms that give the Authority access to the report and the facility to engage directly with the Auditor for matters of clarification if required.
2. The Systems Auditor carries out the ISAE 3000 reasonable assurance engagement and issues the report to the Applicant.
3. The Applicant submits the report to the Authority.
4. The Authority reviews the document and determines if it requires any clarifications on the report.
5. In case the Assessment identifies non-conformities of a material nature, the Authority may at its discretion provide the Applicant with an opportunity to provide a remediation plan within 1 month.
6. The Authority issues the Recognition to the Applicant.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

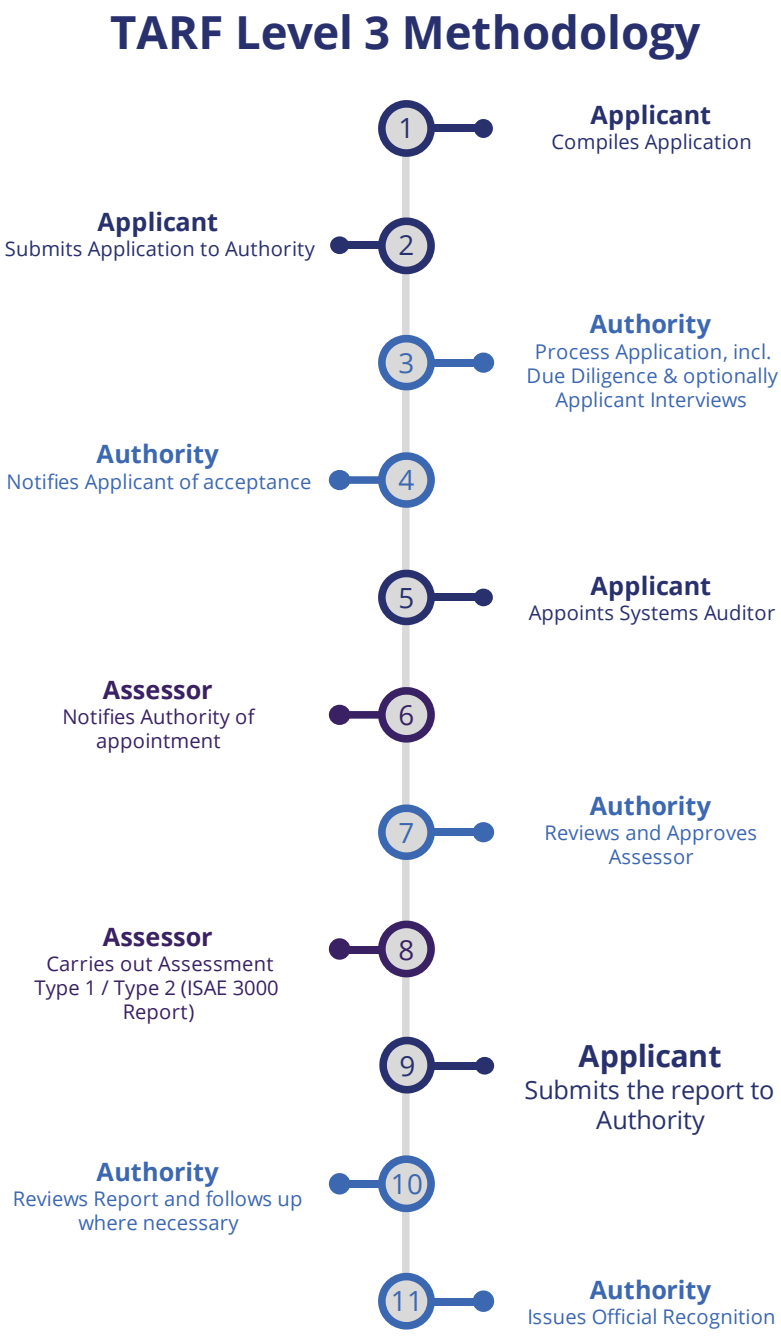


Figure 6 - TARF Assessment Level 3 Process

***Note**: The Applicant may also choose to nominate a Technical Expert at application stage, rather than after the application has been processed and accepted.*

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

8.6 Recognition

Recognition for TARF Level 3 will be in the form of certification issued to the Applicant, that among others identifies the Applicant, as well as the Technology Domain, and Control Types subject to Assessment, period of validity, and any other details deemed relevant by the Authority. For TARF Level 3, it will also highlight whether the Assessment was of Type 1, or Type 2.

The Recognition for TARF Level 3 is valid for one (1) year from the date of issuance, but the Authority reserves the right to add conditions and/or alter the validity period at its discretion.

The Recognition will be published on the Authority's website during its period of validity. Additionally, there is also an obligation on the Applicant to publish the Recognition on its website and, if applicable, refer to it on its IDPS.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

9 General Conditions

This section outlines some general conditions related to TARF.

9.1 Compliance with the Cyber Security Act

Where a European Cybersecurity Certification Scheme is in force in terms of Article 57 of REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) and the said scheme covers the TARF, the related scheme will supervene.

9.2 Recertification Procedure

The recertification procedure applies to TARF Assessment Levels 2–3.

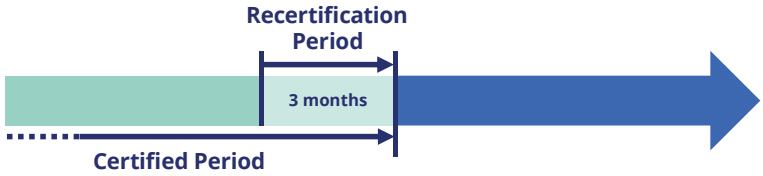


Figure 7 – Graphical representation of Recertification timeline

The Applicant may apply for a renewal of the existing Recognition no earlier than four (4) months before its expiration. The process of recertification shall be identical to the first-time certification process, unless otherwise agreed to in writing by the Authority.

It is the duty of the Applicant to ensure that the Recognition is kept valid and effective and that subject to the confirmation by the Authority, the Recognition will be renewed at least within the last four months of its duration and, in any case, prior to expiry.

9.3 Processing Fees

Payments shall be processed in accordance with the TARF Administration Fee Guidelines accessible to through the official website of the MDIA.

9.4 Recognition

If the Authority is satisfied with the outcome of the Assessment, it will proceed to issue a Recognition to the Applicant for its IDPS. The Recognition may include

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

information from the IDPS Blueprint (such as the features, qualities, and attributes of the IDPS), as well as the IDPS name and description, key IDPS stakeholders, as well as the Assessment Level, Technology Domain, and Control Types that were part of the Assessment. The Authority reserves the right to add any other information it deems pertinent to the Recognition.

The validity of the Recognition shall be tied to the terms and obligations that will be published by the Authority as an integral part of the Recognition itself.

The period of validity of any Recognition shall start to run from the date of issue irrespective of any milestones or go-live date. Note, that in accordance with section 10.1, the Applicant has an obligation to notify the Authority when the IDPS goes live, if it was not yet deployed when the Assessment took place.

The Applicant must publish the Recognition on its website, by linking to the recognition posted on the MDIA's website.

> ***Note:*** *The Authority reserves the right to withdraw the recognition at any time should new information surface about the validity of any material, statements or information that contributed to the Authority's decision to issue the recognition.*

9.5 Logging

Unless otherwise exempted to in writing by the Authority, all IDPS opting for Assessment Level 1-3 need to have a logging mechanism in place which may be used for regulatory and compliance purposes should the Authority need to launch an investigation for any reason.

The requirements for a logging mechanism are inherent in individual controls and the IDPS Assessment will be likely to fail without adequate logging in place. However, centralized live logging that takes steps to prevent tampering with is nonetheless considered a critical mechanism for ensuring the security and compliance of an IDPS that has Recognition.

Note that due to the all-encompassing and possibly sensitive and/or personal nature of the information to be stored within the logs, this data must be stored securely.

The purpose of retainment of this information is to keep an audit trail of the system runtime behaviour which is to be stored in a faithful manner. This primarily helps to ensure that:

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

a) any request for information regarding legal compliance and the operational behaviour of the system by the MDIA or any other NCA concerned with the functionality of the IDPS can be acted upon;
b) sufficient information is available to enable an intervention to take place in case of unexpected behaviour leading to material cause of loss to any user or a material breach of the law; and
c) sufficient information is available to enable Assessors to evaluate operating effectiveness of the controls.

9.5.1 Requirements

Logging implementations may vary between IDPS implementations. However, it must be considered an essential part of the IDPS's infrastructure. It must be designed to satisfy the below requirements:

a) All relevant events and data are recorded faithfully in near real-time (i.e., as quickly as reasonably possible), so that there is no risk of omission or corruption.
b) 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, that is, ensuring that no data or information may be deleted or changed.
c) Processes are in place to ensure timely access to this information by the Authority in a manner that can be demonstrated to be faithful to the original events and data which were recorded on the logs.
d) Procedures detailing how responsible persons may access the logs are documented, and such documentation stored securely and with limited access. This documentation must include information on decrypting data (if the data is stored in encrypted form), as well as outlining procedures on how access shall be granted to relevant authorities and, or law enforcement agencies upon order or request.

Details of how logging is to be implemented must be contained in the IDPS Blueprint, as specified in section 3.4.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

10 Legal and Regulatory Requirements

10.1 Recognition Conditions

A Recognition issued by the Authority is specific to the Applicant and the IDPS referenced in the application. It cannot be assigned or transferred. The Authority is to be notified where any transactions which have the effect of the assignment or transfer of ownership are to take place.

The Authority shall be empowered to conduct any due diligence and/or audit (at a fee) on the legal organisation acquiring or merging with the original Applicant and matters of relevance to the Recognition.

Any conditions mentioned in a report or otherwise communicated to the Applicant, and on the basis of which the Authority issues its Recognition, shall be binding on the Applicant as a condition of the Recognition. The Authority reserves the right to specify these conditions on the Recognition at its own discretion. The Applicant must provide the Authority with a remedial plan to bring their IDPS in line with any and all communicated conditions within a period of 1 month from issuance of the Recognition. The remedial plan must be actioned on within a maximum period of 6 months unless otherwise agreed to with the Authority in writing.

Any breaches of the conditions relating to the Recognition may lead to the Authority taking any of the remedies allowed for in the Act in relation to the Applicant.

A Recognition is issued on the basis of the information submitted to the Authority by the Applicant, the IDPS employees and other stakeholders, and the Assessor. If any of this information is found to be incorrect or false, the Authority may revoke, cancel, or suspend the Recognition and take any other remedies the Authority deems necessary.

Should throughout the Application stage or the lifetime of a Recognition, any material changes to the information submitted in the process leading to the Recognition arise, the Applicant or its delegate shall immediately notify the Authority of this change. The Authority shall examine the relevance of this change to the Recognition that was issued and may, where deemed appropriate, suspend the Recognition until such time as it carries out this review. Where the Authority concludes that the change in circumstances warrants further clarification,

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

information, examination and/or analysis, it shall issue a demand to this effect. Should the said demand not be satisfied in the stipulated timeframe by the Applicant or their delegate, the Authority may revoke, cancel, or suspend the Recognition and take any other remedies allowed for in the Act in relation to the responsible party.

Should the Authority be of the view that the change in circumstances warrants the immediate revocation, cancellation, or suspension of the Recognition or the carrying out of any other remedial action, the Authority shall inform the Applicant, and the Assessor and act accordingly.

In view of the above, the following changes should not be implemented by the Applicant without the prior written approval of the Authority:

a) changes to the Managing Director (Chairperson) or the Chief Executive Officer (CEO) or equivalent roles (in case of TARF Level 3 Assessment Type), or the appointed Technical Expert (in case of TARF Level 1 or 2) or Systems Auditor (in case of TARF Level 3),
b) changes to the individuals that occupy the roles that were the subject of due diligence or fit-and-proper evaluation by the Authority,
c) any alterations to any solutions or part thereof which include software, code or computer protocols save for upgrades, maintenance, innovative evolution, or the mere replacement of any supporting software which do not materially change the functionality or have a material impact on the users of the IDPS or are not in breach of the regulatory principles of the Act or of the Recognition,
d) any development altering the rights of users of the IDPS, and
e) changes to any information provided to the Authority as part of the TARF application which have been relied upon by the Authority in issuing the Recognition.

> ***Note:*** *The request to notify the Authority of a change shall not be satisfied merely by the fact that the information which ought to be notified to the Authority is included in a standard annual return or publicly available.*

The above limitations and requirements may be expanded or modified in the event that the Recognition is a pre-requisite for the Applicant to be able to provide IDPSs in a regulated environment or context.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Where prior notification of, or authorisation to any envisaged changes is not required according to the above provisions, the Applicant to whom Recognition has been granted, shall provide the Authority with particulars of any changes in the IDPS or to the information that had been provided to the Authority in the application processes, within thirty (30) days of such changes occurring.

In determining whether the Applicant is fit and proper, the Authority may, in addition to the due diligence requirements referred to in the *Due Diligence* requirements for each respective Assessment Level, request any information and documentation deemed necessary and examine the structure of the Applicant, its directors, administrators, shareholders, beneficiaries, ultimate beneficial owners and their equivalent, to ensure that they are of clean conduct and sufficiently competent to operate and/or offer the IDPS to third parties.

Moreover, in accordance with its powers at law, the Authority may deem it necessary to carry out further checks or investigations to ensure that the IDPS obtaining the Recognition is compliant with ad-hoc legal requirements and ensures the necessary levels of transparency, integrity, and accountability.

The Authority will assess all the documentation and information provided in the Application and throughout the recognition, certification, or acknowledgement process. The Authority may request the Applicant or any of its relevant staff or stakeholders or the Assessor to provide further documentation, information and detail as may be required by the Authority.

10.2 Resident Agent

In terms of applicable law and in accordance with the *Resident Agent Guidelines* the Authority requires the Applicant to appoint a resident agent when the Applicant is not habitually resident in Malta. The appointed resident agent must meet the following criteria:

a) is habitually resident in Malta,
b) is not interdicted or incapacitated or is an undischarged bankrupt,
c) has not been convicted of any of the crimes affecting public trust or of theft or of fraud or money laundering or of knowingly receiving property obtained by theft or fraud and
d) has satisfied the Authority that he is a person capable of carrying out the functions stated under applicable law.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Notwithstanding the above, a Resident Agent is subject to the same fit-and-proper evaluation as the Applicant.

If an Applicant is a legal organisation, it shall be considered as not being habitually resident in Malta for the purposes of applicable law if none of the below are habitually resident in Malta:

a) the members of its board of administrators or secretary; and
b) its senior officers, being the chief executive officer, the chief operations officer or its chief technology officer.

10.3 Outsourcing

The Applicant may need to outsource some functions in view of resource constraints. In granting a Recognition, the Authority must be made aware of material functions that are being outsourced.

Material functions are those functions that are central for the IDPS to meet the generic and specific requirements of the certification being issued and its legal obligations. In this respect the Applicant needs to demonstrate, by fully disclosing the details in the IDPS Blueprint (see section 3.4) to the Authority, how the process to operate the material functions will be managed and by whom, and the Authority may carry out its analysis, including a fit and proper test, of the legal organisation to which the material functions are outsourced in the same manner as it does with the Applicant. It shall be the Applicant's responsibility to obtain the full cooperation of the legal organisation to which the material functions are being outsourced.

The Authority reserves the right to request copies of outsourcing agreements.

The Recognition Conditions (section 10.1) shall further apply to changes in and/or to the legal organisation to which the material functions are outsourced. The Applicant shall not terminate the outsourcing agreement or outsource the functions to another legal organisation without the prior approval in writing of the Authority. Should the legal organisation to which material functions are outsourced be the subject of changes, as mentioned in section 10.1 above, the Authority may act in the manner described in the same section 10.1, and request the mentioned information from the said legal organisation and/or the Applicant.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

11 TARF as a tool for National Competent Authorities

Part of the reason behind the flexibility of TARF in providing Recognition by the MDIA at various levels, and across various Technology Domains and Control Types, is to enable TARF to be leveraged by other NCAs. This allows other government entities to utilise the TARF when technology-related Recognitions are required, either as special conditions or to facilitate or make for a smoother licensing process, instead of defining and operating a new and separate recognition programme on innovative technologies.

Such programmes will be defined jointly between the MDIA and the relevant NCA and will be published as a separate set of guidelines. These programmes will be compatible with specific TARF Assessment Levels and will specify which Technology Domains and Control Types and control objectives are applicable. The Authority, in conjunction with the NCA may also add any custom controls when necessary. All details will be published in the corresponding programme guidelines.

Beyond the original scope of TARF to provide general Recognition related to an IDPS, this Recognition may also be used either to ensure a degree of quality in relation to a specific deployment within the same government entity, or for regulatory purposes. Such Recognition can be either on a voluntary or obligatory basis as defined by the same requesting NCA.

Upon successful completion, the Authority will provide the Applicants of such schemes with a Recognition, which Recognition shall be jointly recognised by the MDIA as well as the requesting NCA.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

12 Alignment to other frameworks

TARF is designed to align with current MDIA offerings, and either supersede them or bring them in line to it.

MDIA Service	TARF Alignment
ITA Systems Audit for DLT solutions	This is replaced by TARF Assessment Level 3, focussed on the DLT domain
Technology Assurance Sandbox (TAS)	The TAS fits under TARF Assessment Level 1.
Mind the Gap	This was designed from the start to be TARF Level 0 compliant.

Note: *The Authority is actively involved in a number of EU working groups on upcoming regulations. The Authority expects to update TARF from time-to-time once any of these regulations are in force to align to European regulations that are currently in the pipeline to ensure alignment.*

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

13 Appendices

13.1 TARF Assessment Level 0 Control Categories

Categories	Description
Identity & Access Management (IAM)	Identity and Access Management refers to the processes associated with managing the entire lifecycle of digital identities and profiles for people, processes, and technology.
Incident Response	The Incident Response category defines the formal function for reporting and responding to incidents that may adversely impact the legal organisation's assets, operations, reputation, financial position, intellectual capital, or confidential information.
Operational Metrics	The Operational Metrics category encompasses any defined, repeatable measurement activity that aids the legal organisation in understanding the various technology components and how it supports the business strategy.
Network Security	The Network Security category captures the policies, processes, tools, and technologies that are used to maintain security at the network level.
Operations	The Operations category encompasses all risks associated to change management, configuration management, communications and operations management, backup, physical and environment security, system planning and acceptance, operations access control.
Policies	This Policies category refers to the Information Security Policies that the IDPS has in place, to enable standardization and best security practices.
Privacy	The Privacy category captures how data is collected, disclosed to third parties, retained, and used and shared across a legal organisation.
Logging & Monitoring	This category relates to the successful monitoring of logs from network devices, hosts,

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

	files, databases, and privileged user access so as to identify or be alerted of events that require further investigation due to the potential of being security events.
Software Security	The Software Security category encompasses how security is integrated with the Development lifecycle and software configuration of an organisation.
Vendor Risk Management	This category is associated with the process for managing vendors, and the transfer and exchange to, or storage of information/data by the vendors.
Vulnerability Management	Vulnerability Management refers to the existing capabilities of an organisation to identify, prioritize and remediate vulnerabilities and apply security patches.
Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.
Architecture	The architecture category is associated with the management of information security solutions and technologies that promote interoperability and manageability while meeting the organisation's risk management needs.
Asset Management	IT Asset Management encompasses the infrastructure and processes necessary for the effective management, control and protection of the hardware and software assets within an organisation, throughout all stages of their lifecycle.
Awareness	This category is associated with an organisation's security awareness program consisting of all staff within an organisation, including self-employed staff, contractors, and third-party service providers.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

BCP/ DR	This category covers business continuity and disaster recovery concepts such as senior management support for Business Continuity Management, adequate skilled resources, process definition, business impact analysis, testing of plans, and metrics reporting.
Cloud Computing	This category is associated with the fundamental risks deriving from the usage of Cloud Computing.
Data Protection	This category focuses on protecting data and heavily relates to an enterprise's goal to effectively manage data loss risks.
Host Security	This category covers the protection mechanisms and controls in place at the host level. Topics in scope for this section are anti-virus, full disk encryption, malware protection, hardware access control and patch management.
Human Resources	This category covers the risk controls related to the human element, as per the existing governance best practices.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

13.2 TARF Assessment Level 0 Maturity Levels

Maturity Level	Description
0 - Limited	Limited to negligible technology and controls are in place, deployed in a non-consistent manner. No local processes are in place.
1 - Initial	Basic technology and controls are in place, deployed in a non-consistent manner. Limited local processes are in place with limited organisational support.
2 - Managed	Partial technological maturity is in place with a combination of some technology and tools; local processes covering some regions/business units or processes are repeatable.
3 - Defined	A defined maturity is in place with significant technology and tools for some key resources and people; processes defined for some regions and/ or business units.
4 - Quantitatively Managed	A mature capability is in place with advanced technology and tools for some key resources and people, consistent processes exist for some regions and/or business units.
5 - Optimised	An advanced capability is in place which is leading-edge technology and tools for all key resources and people, consistent process across regions, business units, and effective governance is in place.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

13.3 Blueprint Template

The Blueprint is an essential document within the context of TARF, not just at application stage but throughout the entire lifecycle of the Technology Assessment as it defines the IDPS in detail. It is the basis upon which the Authority accepts an Applicant, and more importantly it defines what the Recognition is issued for.

The Blueprint is expected to contain the below sections. While the level of detail may vary depending on the maturity of the IDPS, they must be covered in a level of detail that allows the reader to gain a good and thorough understanding of the IDPS.

- **Purpose and Objectives**: Define the primary goals and objectives of the IDPS.
- **Responsibilities**: Provide an organogram that show the structure and key roles in relation to the IDPS.
- **Functional Specifications**: List the IDPS's features and functionalities, including their purpose and expected behaviour.
- **Non-functional Requirements**: List non-functional requirements of the IDPS such as performance, scalability and reliability expectations and requirements.
- **Dependencies**: Provide a comprehensive list of 3rd party dependencies, be they software, hardware, or services utilised by the IDPS.
- **Technical Architecture**: Provide a detailed diagram of the system's structural design, showcasing the relationships between the various system components, including interactions with 3rd party systems and components.
- **Data Flow Diagrams**: Define a visual representation of how the data flows through the system.
- **Deployment Architecture**: Detail the IDPS's hosting and deployment environments.
- **Test Strategy and Results**: Define how the IDPS is tested prior to deployment.
- **Policies and Procedures**: Describe the documented policies procedures that are established for routine operations, troubleshooting, cybersecurity and emergency procedures, as well as who is responsible for them.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

- **Compliance and Standards**: Define any regulatory or industry standards that the IDPS is aligned with.
- **Alignment with AI Act**: Specify whether: i) The IDPS is recognised as High-Risk AI System under the EU AI Act, and why; ii) Declaration that the AI system is not prohibited under the EU AI Act. Where the IDPS does not contain or make use of AI Systems, a statement to that effect must be included in this section.
- **Risks, Known Issues and Limitations**: Provide a list of risks, any known issues, and limitations of the IDPS.
- **Logging Mechanism**: Provide a detailed overview of the logging mechanism in line with the logging requirements laid down by TARF.

***Note**: If section not applicable to an IDPS, ensure you provide a detailed enough justification on why this is not the case.*

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

14 Sample Blueprint – Digital Health System

The Digital Health Platform (DHP) represents a paradigm shift in how healthcare data is accessed, managed, and utilized. As healthcare becomes increasingly digital and patient-centric, the need for an integrated platform that aggregates data, offers insights, and facilitates remote interactions between healthcare professionals and patients becomes paramount.

14.1 TARF Context

This Blueprint is being submitted to the Malta Digital Innovation Authority for the purposes of obtaining recognition at Assessment Level 3, Type 2.

The applicable technology control domains are: General Innovative Technologies, Cloud Computing and Artificial intelligence.

14.2 Purpose

The DHP is designed to:

- Centralize and streamline access to patient health data, making it easily accessible for both patients and healthcare professionals.
- Offer real-time health monitoring, aiding early detection of potential health issues.
- Act as a bridge between patients and healthcare professionals, promoting preventive healthcare and timely interventions.

14.2.1 Objectives

1 **Real-time Monitoring**: Ensure patients' health data, from wearable devices and manual inputs, is updated in real-time.
2 **Remote Consultation**: Provide a secure platform for patients and doctors to interact without physical appointments unless necessary.
3 **Data Centralization**: Create a unified repository for health records, making them accessible anytime, anywhere.
4 **Predictive Analysis**: Use AI-driven models to predict potential health issues or trends based on the accumulated data.

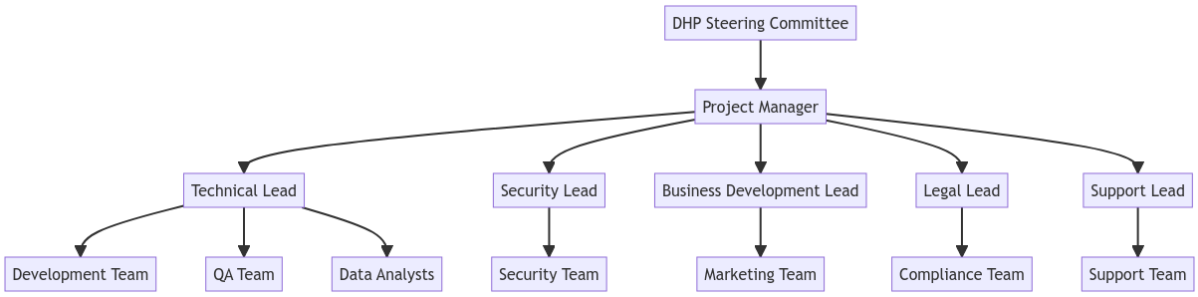
14.3 Responsibilities

The DHP's implementation and ongoing management involve a multitude of roles, each with distinct responsibilities.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt



14.3.1 DHP Steering Committee

The DHP Steering Committee oversees the strategic direction of the platform, ensuring alignment with long-term organizational goals. They engage with key stakeholders, ensuring that their concerns and needs are met, and are also responsible for approving and overseeing budget allocations for the DHP project.

14.3.2 Project Manager

Tasked with the comprehensive management of the DHP project, the Project Manager ensures all components run smoothly, timelines are met, and budgetary constraints are adhered to. Their role acts as a bridge between strategy and execution.

14.3.3 Technical Lead

The Technical Lead determines the platform's technical direction, tools, and methodologies. Under their purview is the Development Team, responsible for building and maintaining the DHP platform and addressing software glitches. The QA Team ensures the platform's functionality and performance meet set benchmarks. Meanwhile, Data Analysts delve into health data, transforming it into actionable insights and continuously refining AI-driven models.

14.3.4 Security Lead

Guiding the platform's security posture, the Security Lead sets forth the security protocols and standards for DHP. Their Security Team actively monitors the DHP for threats, ensures timely application of security patches, and conducts periodic in-depth reviews to ascertain the platform's security health.

14.3.5 Business Development Lead

The Business Development Lead examines market needs, making adjustments to the platform's features and positioning as necessary. They also nurture relationships with healthcare providers and institutions to expand DHP's footprint. Complementing their efforts, the Marketing Team strategizes and executes campaigns to raise DHP's profile and drive user adoption.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

14.3.6 Legal Lead

The Legal Lead oversees the platform's alignment with various healthcare regulations and legal standards. Under them, the Compliance Team works diligently, ensuring DHP's steadfast adherence to standards like HIPAA and GDPR and conducting audits to identify and mitigate potential compliance risks.

14.3.7 Support Lead

Championing the end-user's experience, the Support Lead dictates the support protocols and response timelines. Their Support Team is the frontline, assisting users with queries, conducting training sessions for platform acclimation, and collecting feedback to further refine the user experience.

14.4 Functional Specifications

14.4.1 User Management System

The DHP's user management system is designed with a focus on security and user experience. It offers a multi-step registration process, ensuring data accuracy and security. Once registered, users can fine-tune their profiles, setting preferences, and managing their health data. The system also incorporates role-based access controls, which ensure that specific features and data are available only to authorized personnel. For instance, while a patient can view their medical history, they might not access another patient's data or administrative tools meant for healthcare providers. An in-built password recovery mechanism, fortified with multi-factor authentication, guarantees user access continuity.

14.4.2 Integrated EHR System

Integration with Electronic Health Records is central to the platform's functionality. The DHP can communicate in real-time with various EHR systems using standard medical data protocols. This ensures that every time a healthcare provider accesses a patient's profile, they see the most recent and comprehensive health data, making their diagnostic and therapeutic decisions better informed.

14.4.3 Patient Portal

The patient portal stands as a testament to the platform's commitment to patient empowerment. Through this portal, patients can not only view their health records but also schedule or reschedule appointments, chat with healthcare assistants for queries, and even manage their insurance details. It also provides a platform for telemedicine consultations, connecting patients with their doctors

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

through integrated video or voice calls, ensuring they get medical advice irrespective of geographical boundaries.

14.4.4 AI-Driven Health Insights

Harnessing the power of artificial intelligence, the DHP can analyse vast amounts of health data to provide both macro and micro insights. On a broader scale, it can highlight health trends in a community, aiding public health decisions. On an individual level, by analysing a patient's health history combined with real-time data, it can provide personalized health recommendations, alerting them of potential health risks.

14.4.5 Prescription Management

Incorporating digital efficiency into medical prescriptions, DHP allows doctors to generate digital prescriptions. These can be instantly dispatched to patients or associated pharmacies. This digitization ensures clarity in medication instructions and significantly reduces medication discrepancies.

14.5 Non-Functional Requirements

The below are the main non-functional requirements pertinent to the DHP.

- **Performance**: The DHP aims to maintain a load time under two seconds for primary functionalities and has the capacity to support thousands of concurrent users.
- **Scalability**: The DHP utilizes a microservices architecture, allowing it to scale horizontally. This design ensures the system can manage increasing users and data volumes effectively.
- **Reliability**: The DHP is designed for an uptime of 99.9%. It has redundant systems in place, ensuring swift recovery in the event of unexpected failures with minimal data loss.
- **Security**: Given the importance of safeguarding health data, the DHP uses advanced encryption both during data transmission and while stored. The system undergoes regular security audits, penetration testing, and continuous threat monitoring.
- **Interoperability**: The DHP adheres to recognized healthcare data protocols like HL7 and FHIR. This standardization ensures data consistency when interacting with various EHR systems and health devices.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

- **Usability**: The user interface of the DHP is designed to be intuitive. Comprehensive user documentation, tutorials, and support mechanisms are available to aid users.
- **Accessibility**: The DHP complies with the Web Content Accessibility Guidelines (WCAG) 2.1. Features integrated to support this include screen reader compatibility, keyboard-only navigation, and high-contrast themes.
- **Backup and Recovery**: The platform undergoes regular data backups, both incremental and full. A systematic recovery procedure exists to address data loss or system interruptions, prioritizing data integrity and prompt availability.
- **Data Retention and Archiving**: The platform adheres to a specified data retention policy, retaining data for legally defined durations. After this duration, data is moved to secure archives, from which it can be retrieved if necessary.
- **Regulatory Compliance**: The DHP is designed to comply with the General Data Protection Regulation (GDPR) guidelines, especially concerning the handling, storage, and processing of health data. Detailed specifications regarding GDPR, and other relevant regulations will be addressed comprehensively in the "Compliance and Standards" section.

14.6 Dependencies

For the DHP to function effectively and offer its services, it relies on several third-party dependencies, including software, hardware, and external services.

14.6.1 Software Dependencies

- **Database Management Systems (DBMS)**: The DHP employs PostgreSQL for data storage, querying, and retrieval.
- **Cloud Service Providers**: The infrastructure is hosted on AWS, leveraging its suite of services for storage, computing, and analytics needs.
- **Middleware Software**: Kafka is used for real-time data streaming and RabbitMQ for asynchronous message queuing.
- **Authentication Services**: User authentication is managed through OAuth with integration from providers like Auth0.

14.6.2 Hardware Dependencies

- **On-Premises Server Hardware**: While much of the platform's operations are cloud-based, certain sensitive processes and data storage occur on Dell

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

PowerEdge servers situated on-premises. This setup provides an added layer of security and control over critical health data.

- **Backup Systems**: In addition to cloud backups, dedicated HP StoreOnce systems are used on-premises for data redundancy. This dual backup approach ensures swift data recovery in various scenarios, be it system failure or potential cloud service interruptions.
- **Networking Equipment**: To maintain a robust connection between on-premises hardware and cloud services, and to support the internal network for the DHP, high-quality Cisco routers and switches are utilized.

14.6.3 External Services

- **SMS and Email Gateways**: Twilio handles the platform's SMS notifications, while SendGrid manages email notifications.
- **Telemedicine Integration**: The platform integrates with Doxy.me for its telemedicine functionalities.
- **Payment Gateways**: Stripe is integrated for handling any potential payments or transactions.
- **Geolocation Services**: The platform uses the Google Maps API for features related to location, such as finding nearby healthcare providers.

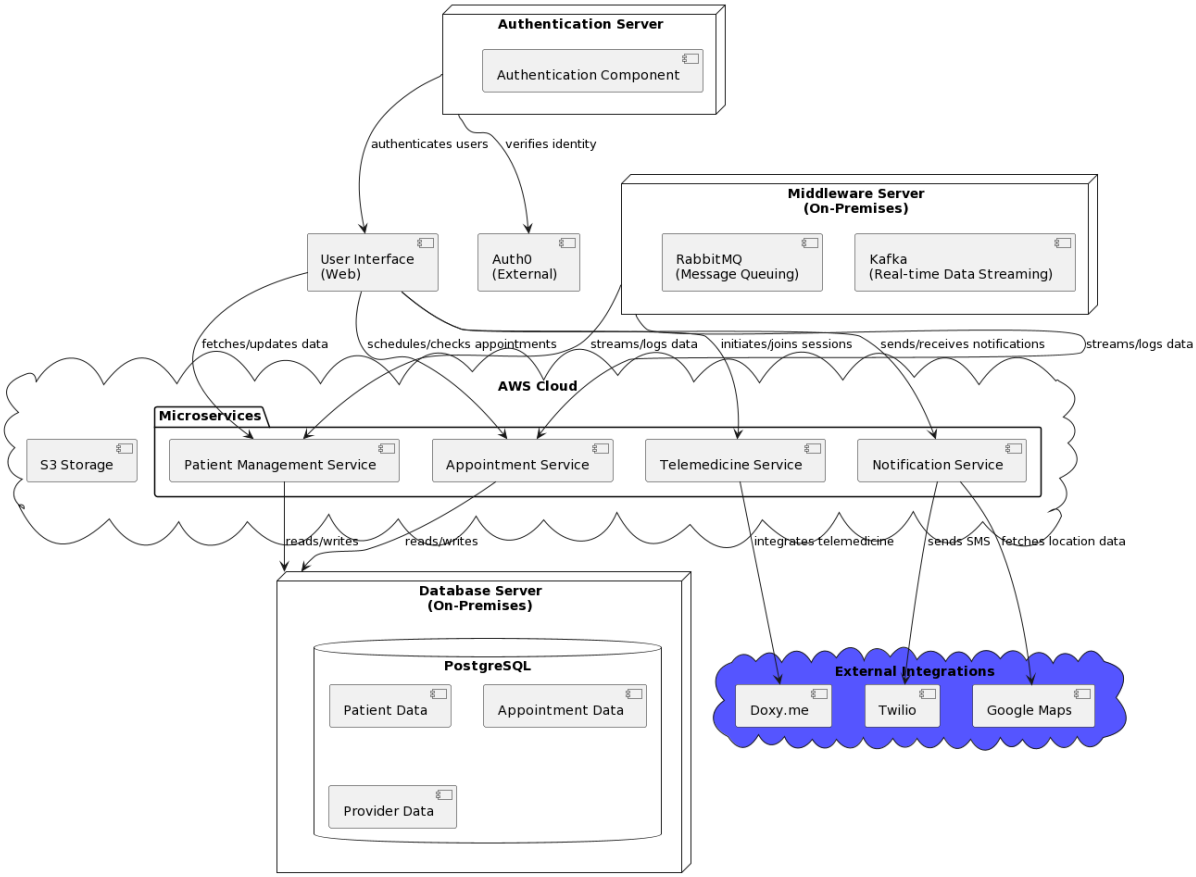
14.7 Technical Architecture

The Technical Architecture provides an overview of the system's structural design, emphasizing the relationships between its components and interactions with third-party systems.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt



14.7.1 System Components

- **User Interface (UI)**: A web-based interface for patients, healthcare professionals, and system administrators.
- **Backend Services**: Comprising of microservices handling different functionalities such as patient data management, appointment scheduling, and telemedicine integration.
- **Database**: PostgreSQL is utilized for secure storage, retrieval, and management of data.
- **Authentication Server**: Utilizing OAuth and integrated with Auth0 for secure user authentication and authorization.
- **Middleware**: Kafka handles real-time data streaming while RabbitMQ takes care of message queuing.
- **External Integrations**: This encompasses services like Google Maps for geolocation, Doxy.me for telemedicine, and Twilio for SMS services.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

14.7.2 Interactions with Third-Party Components

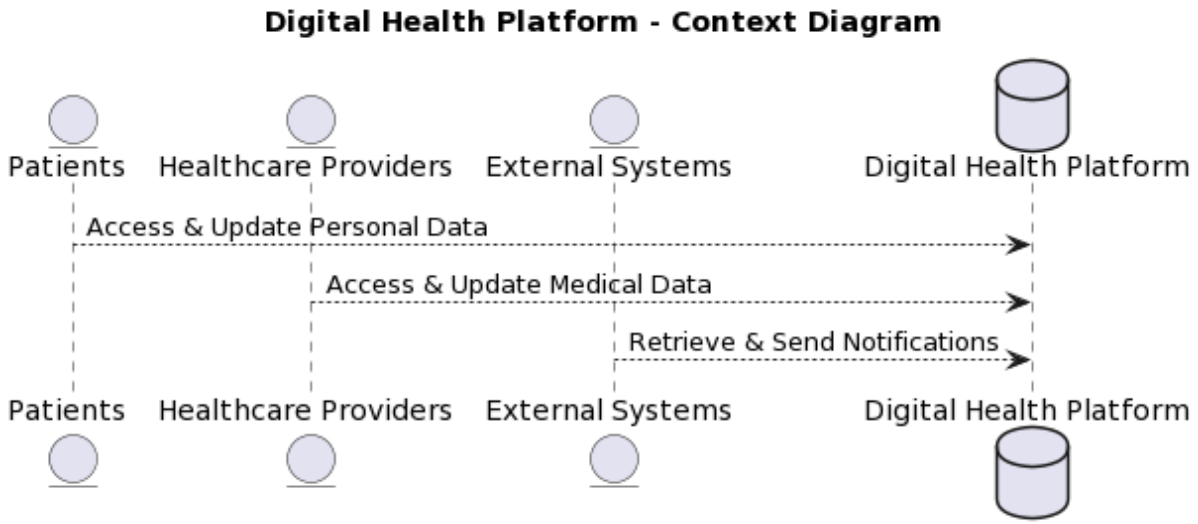
- **Cloud Services**: The AWS suite provides storage, computing, and analytics resources. The on-premises systems interact with AWS to fetch or store data and to scale resources as needed.
- **Telemedicine**: For telemedicine sessions, the platform integrates directly with Doxy.me.
- **Notifications**: Twilio and SendGrid manage SMS and email notifications, respectively, triggered by events within the DHP.
- **Geolocation Services**: For location-based features, the platform queries the Google Maps API.

14.8 Data Flow Diagrams

The Context Diagram (often referred to as a Level 0 Diagram) and the Level 1 Data Flow Diagram (DFD) represent different levels of granularity and detail when visualizing a system's data flows. Here's a breakdown of their differences.

14.8.1 Level 0 DFD

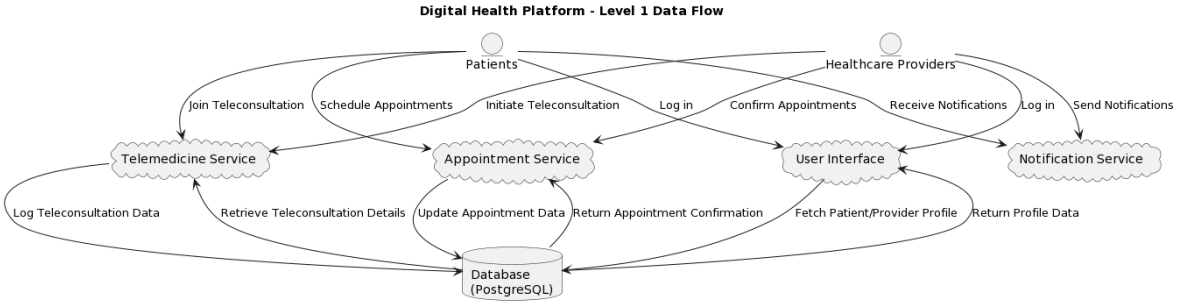
The context diagram provides a high-level overview of the entire system. It focuses on the external entities that interact with the system and the data flows between them. Its primary purpose is to define the boundaries of the system and to give a clear, broad picture of what the system does and with whom it communicates.



Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050
+356 2182 8800 info@mdia.gov.mt
www.mdia.gov.mt

14.8.2 Level 1 DFD

The Level 1 DFD illustrates the main processes or functions of the system, their data interactions, data stores, and how data flows between them. Its primary purpose is to give stakeholders a more detailed understanding of a system's operations and data flows without delving into the nitty-gritty of every individual function.



14.9 Deployment Architecture

The Digital Health Platform (DHP) leverages a hybrid infrastructure, combining the scalability and flexibility of cloud services with the robustness and control of on-premises hardware.

The deployment architecture ensures that the DHP remains agile in its operations, scalable to accommodate growth, and robust enough to provide consistent, high-quality service to its users. It strikes a balance between the benefits of cloud infrastructure and the security and control of on-premises hardware.

14.9.1 Cloud Infrastructure (AWS)

- **Compute**: The primary application servers, running the backend services and the frontend, are hosted on Amazon Elastic Compute Cloud (EC2) instances. These instances are auto-scalable based on the incoming traffic, ensuring smooth operation even during peak loads.
- **Database**: The platform's primary database is hosted on Amazon RDS with PostgreSQL as the database engine. Regular backups are stored in Amazon S3 buckets, and the database is set to run in multiple availability zones to ensure high availability.
- **Storage**: Static assets, including user-uploaded files and system-generated reports, are stored in Amazon S3 buckets. The assets are delivered to end-users via Amazon CloudFront, a content delivery network (CDN) service, to speed up content delivery.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050
+356 2182 8800 info@mdia.gov.mt
www.mdia.gov.mt

- **Network**: The DHP is housed within a Virtual Private Cloud (VPC) with clearly defined public and private subnets. This setup ensures that sensitive components, like the database, are not directly accessible from the public internet, while frontend services are accessible to users.

14.9.2 On-Premises Infrastructure

- **Backup Server**: An on-site server is dedicated to storing backups of critical data from the AWS infrastructure. These backups are encrypted and serve as a contingency against catastrophic data loss scenarios in the cloud.
- **Direct Connect**: To ensure faster and more secure data transfer between the on-premises hardware and AWS, a Direct Connect link has been established. This dedicated connection ensures optimal performance and security for data-in-transit.
- **Gateway Server**: This server acts as an intermediary for all incoming and outgoing traffic from the on-premises infrastructure. It includes firewalls and intrusion detection/prevention systems to safeguard against potential threats.

14.9.3 Deployment Strategy

- **Development Environment**: Before any deployment to the main system, changes are first deployed to a development environment. This isolated AWS environment mirrors the production setup but is solely for testing and development purposes.
- **Continuous Integration/Continuous Deployment (CI/CD)**: Using AWS CodePipeline and Jenkins, the DHP maintains a CI/CD pipeline. Once code is committed to the repository, it undergoes automated testing. If tests are successful, the changes are deployed to the development environment, and subsequently, after further testing, to the production environment.
- **Monitoring & Maintenance**: Amazon CloudWatch is employed to monitor the system's health, performance, and operational metrics. Alerts are set up for any unusual activities or potential system failures.

14.10 Test Strategy

The Digital Health Platform (DHP) follows a comprehensive testing strategy to ensure the software is robust, reliable, and provides a seamless experience to users.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

14.10.1 Unit Testing

Unit testing is an essential initial phase where we validate each individual component of the software. We utilize tools like JUnit and pytest to conduct these tests, aiming for robustness and depth in our evaluations. A critical metric for our team is code coverage, and with our current approach, we've managed to achieve a coverage of around 85%. This high coverage ensures that the majority of our code is tested for possible bugs or vulnerabilities.

14.10.2 Integration Testing

Following unit testing, integration testing becomes the focus to ensure that various modules or services of the application work seamlessly together. Employing tools like Postman for API endpoint testing and TestNG, we've created test scenarios that, for instance, validate the successful communication of data from the patient registration form to the database and back to the user.

14.10.3 System Testing

In the system testing phase, we gauge the software's overall functionality. To simulate real-world usage, tests are conducted in an environment that closely mimics the production setting. A typical test scenario would include simulating the entire patient journey from registration to appointment booking, and finally to receiving notifications.

14.10.4 User Acceptance Testing (UAT)

UAT is a pivotal stage where the software is evaluated against the expectations and needs of the users. By involving a select group of users, stakeholders, and QA specialists, we gather invaluable feedback about the system's usability and overall experience. Their insights not only validate the software's readiness but also guide further refinements.

14.10.5 Performance Testing

To ensure the DHP's responsiveness and stability, especially during high-demand periods, performance testing is executed. By leveraging tools like Apache JMeter and LoadRunner, we measure key metrics like response time and system stability under different loads.

14.10.6 Security Testing

With the sensitivity of healthcare data, security is paramount. We employ tools such as OWASP ZAP and Burp Suite to assess the system's vulnerability to threats like SQL injections or other potential security breaches. Our aim is to pre-

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

emptively identify and rectify any security weaknesses before they become critical issues.

14.10.7 Compatibility Testing

Given the vast array of devices, operating systems, and browsers available today, compatibility testing becomes essential. We ensure that our platform operates smoothly on major browsers like Chrome, Firefox, and Safari, and across mobile platforms such as iOS and Android, as well as desktop environments including Windows, MacOS, and Linux. This expansive testing guarantees a consistent user experience regardless of the access point.

14.11 Summary of Test Results

The below is a summary of the latest state of testing results:

- **Unit Testing**: Achieved 87% code coverage, surpassing the target of 85%.
- **Integration Testing**: All 120 defined scenarios passed without issues.
- **System Testing**: 3 minor bugs identified and resolved.
- **UAT**: Feedback from 40 users collected; 90% found the platform intuitive and user-friendly. Two enhancement requests have been logged for the next iteration.
- **Performance Testing**: System supported up to 10,000 concurrent users without significant degradation in response time.
- **Security Testing**: 5 potential vulnerabilities identified and patched.
- **Compatibility Testing**: The platform was found to be compatible across all targeted devices and browsers with a few minor UI issues on older Android devices, which were addressed.

14.12 Policies & Procedures

This section documents the pertinent policies and procedures that are currently in place.

- **Routine Operations**: For the smooth functioning of the Digital Health Platform, we have established a set of standardized procedures. These encompass guidelines for daily system checks, regular data backups, and updates. All personnel are trained to follow these standard procedures, ensuring consistent platform performance and user experience.
- **Troubleshooting**: In the event of system anomalies or user-reported issues, a structured troubleshooting protocol is in place. It starts with an

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

initial diagnosis by the frontline support team. If unresolved, issues escalate to the technical team for a deeper dive. A comprehensive knowledge base and issue logs assist in faster resolution. Importantly, users are kept informed about the status of their reported problems and expected resolution times.

- **Cybersecurity**: Given the sensitivity of health data, cybersecurity is paramount. Our cybersecurity policy encompasses regular system audits, threat identification, and immediate rectification. There are also protocols for handling potential data breaches, ensuring swift action and communication to all stakeholders. All staff undergoes mandatory cybersecurity training annually to stay updated on the latest threats and best practices.
- **Emergency Procedures**: For unforeseen crises, such as natural disasters or large-scale cyber-attacks, we have an emergency response plan. This includes data recovery from secure offsite backups, temporary system shutdowns if required, and a communication protocol to inform users about service disruptions and expected restoration timelines. An emergency response team, trained specifically for crisis scenarios, is on standby 24/7.
- **Roles and Responsibilities**: Clear delineation of roles ensures that there's no ambiguity in responsibilities. From database maintenance to user support, every function has a designated expert. This structure not only enhances efficiency but also ensures accountability. Team leads for each department coordinate closely with the Project Manager to ensure seamless operations and swift issue resolution.

14.13 Compliance & Standards

The Digital Health Platform is diligently aligned with both global and European regulatory and industry standards concerning health data and digital health platforms. Our adherence to these standards underscores our unwavering commitment to our users, championing data privacy, security, and trust.

- **General Data Protection Regulation (GDPR)**: Operating within a European framework, strict adherence to the GDPR is paramount. The Digital Health Platform ensures all personal data of patients and users are processed in line with GDPR provisions. Clear consent for data collection,

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

transparent data utilization policies, and assured rights to data deletion or portability are fundamental pillars of our GDPR compliance.

- **Health Level Seven (HL7)**: While HL7 is a set of global standards for the interoperable exchange of clinical and administrative data, its significance is well recognized in Europe. Many European countries and healthcare entities adopt HL7 standards either exclusively or alongside other regional specifications. This ensures interoperability and facilitates a seamless exchange of data with various healthcare systems within the European landscape.
- **Integrating the Healthcare Enterprise (IHE)**: In the European context, IHE is another crucial standard, providing detailed specifications for interoperability. The Digital Health Platform aligns with IHE protocols, further strengthening our interoperable capabilities within the European healthcare ecosystem.
- **ISO 27001**: Information Security Management: ISO 27001, an international standard, is pivotal for structured information security management. Our platform conforms to the ISO 27001 framework, safeguarding all data, particularly sensitive health records, through encryption and robust defence mechanisms against potential breaches.
- **Local Health Data Standards**: Beyond international standards, the platform is also compliant with country-specific health data regulations and standards within Europe. This encompasses adherence to localized patient data protection laws, electronic health record standards, and other region-centric regulations.

Through continuous monitoring, periodic audits, and educational sessions, the platform consistently maintains its compliance with evolving regulations. Updates or modifications in regulatory frameworks are expeditiously integrated, ensuring the platform's consistent legality and credibility within the European domain.

14.14 Alignment with the proposed EU AI Act

In this section, we address the alignment of the Digital Health Platform (DHP) with the proposed European Union Artificial Intelligence Act, specifically focusing on whether the DHP's use of AI systems is categorized as high-risk and ensuring it does not fall under the scope of banned AI practices.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

14.14.1 High-Risk AI System Assessment

The DHP employs AI systems primarily for predictive health analytics and patient data analysis. According to the criteria set forth in the proposed EU AI Act, these systems may be classified as high-risk due to their application in the field of health. The AI functionalities in the DHP are designed to support healthcare providers in making informed decisions, rather than replacing human decision-making. These systems undergo rigorous testing, validation, and are subject to continuous oversight to ensure accuracy and reliability.

This consideration shall be included in the assessment of control objective GEN-4-AI.

14.14.2 Compliance with Prohibitions Under the EU AI Act

We declare that AI systems in use by the DHP are not prohibited under the proposed EU AI Act.

14.15 Risks, Known Issues and Limitations

The Digital Health Platform, like all complex software systems, has its inherent risks, known issues, and certain limitations. While we continually work to address and mitigate these, it's essential to acknowledge and understand them for complete transparency and informed decision-making.

14.15.1 Risks

- **Data Breaches**: Even with top-tier security measures, the platform, like any other digital system, is at risk of data breaches. Regular security audits, penetration tests, and cybersecurity updates help minimize this risk, but it cannot be entirely eradicated.
- **System Downtime**: Unforeseen circumstances, such as server failures or large-scale network issues, might lead to unplanned downtimes. While our redundancy measures and backup systems minimize this risk, occasional outages are a possibility.
- **Regulatory Changes**: As the European regulatory landscape evolves, there's always a risk that sudden changes or amendments may affect the platform's compliance status. We actively monitor legislative updates to ensure rapid alignment.

14.15.2 Known Issues

- **Integration Challenges with Older Systems**: Some older healthcare systems may not be fully compatible with modern interoperability

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

standards. This can sometimes lead to integration challenges or require custom solutions.

- **Mobile App Performance on Older Devices**: The platform's mobile app may experience performance issues on outdated mobile devices due to hardware limitations.

14.15.3 Limitations

- **Limited Support for Non-European Languages**: Currently, the platform primarily supports European languages. Expansion to include a broader range of global languages is in the roadmap, but it's a limitation as of now.
- **Dependence on Third-Party Services**: Some platform features rely on third-party services, which means their performance and availability are subject to those third parties' operational statuses.
- **Data Storage Constraints**: While our storage capabilities are expansive, there are upper limits. Clients with exceptionally large datasets might need to explore additional storage solutions.

14.16 Logging

Logging is a fundamental aspect of ensuring the accountability, transparency, and security of the Digital Health Platform. This section delves into the specifics surrounding our logging infrastructure, its purpose, and the measures taken to secure it.

14.16.1 Datasets and Events Collection

The Digital Health Platform logs several datasets and events to ensure transparency and aid in system diagnostics. This includes:

- User access times and activity.
- API calls and responses.
- System errors and warnings.
- Transaction records for data retrieval or modification.

While some datasets like raw patient data aren't directly logged to ensure patient privacy, their access timestamps and the identities of the accessing users are recorded. This approach balances transparency with patient confidentiality.

14.16.2 Security Measures for Log Data

Logs are encrypted both in transit and at rest. Multi-factor authentication and strict role-based access controls are in place to prevent unauthorized access.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt

Regular audits and integrity checks are performed to ensure that the data in the logs remains tamper-proof.

14.16.3 Data Retention Policies

Log data is retained for a period of 24 months, striking a balance between historical analysis needs and data minimization principles. After this period, logs are securely deleted. Data deletion processes are tested regularly to ensure irrecoverability. These retention policies are crafted in accordance with data protection laws, including GDPR, ensuring both security and legal compliance.

14.16.4 Purpose of the Logs

As stipulated in section 8.4 of the TARF Guidelines, the logs serve to:

- Diagnose and troubleshoot system issues.
- Audit and monitor system and user activity.
- Ensure transparency in data access and modifications.
- Aid in cybersecurity measures by tracing unauthorized or suspicious activities.

The Digital Health Platform's infrastructure upholds these purposes by employing advanced log collection, monitoring, and analysis tools.

14.16.5 Physical Aspects of Logging Infrastructure

The logging infrastructure is hosted in a dedicated server cluster within the AWS environment in Frankfurt, Germany. This ensures that the data remains within the European jurisdiction, abiding by European data laws. The servers are high-end, designed for large-scale data processing, ensuring efficient log data storage and retrieval.

14.16.6 Access Control Procedures

Access to the logs is restricted to a select group of system administrators and cybersecurity personnel. A clear hierarchy and role-based access control ensure that only those with the necessary clearance can view or analyse the logs. In scenarios where direct access is required by authorities or law enforcement, a formal request procedure is in place, ensuring legal compliance and data security.

Twenty20 Business Centre, Triq l-Intornjatur, Zone 3,
Central Business District, Birkirkara CBD 3050

+356 2182 8800 info@mdia.gov.mt

www.mdia.gov.mt