TAAF Guidelines

Document for Public Consultation

Contents

1 Public Consultation

This document is presented to obtain feedback from stakeholders prior to finalisation of the document.

The fees associated with TAAF are being published in a separate document as part of this public consultation exercise.

These draft TAAF Guidelines ('the Guidelines') are being published by the MDIA for consultation strictly in relation to the subject matter of technology assurance.

The laws governing the MDIA and innovative technology are currently going through a re-drafting exercise. These draft TAAF Guidelines that are being consulted on make reference to laws which are currently being amended as though such amendments have already entered into force. Applicable legislation may change further by the time the Guidelines are published in their final format. Such amendments may introduce modifications that affect the contents of this technical document. Once the amendments come into force, this document may be revised, amended, or updated accordingly to ensure compliance and alignment with the updated legal framework.

Any feedback must be submitted to the MDIA on taaf@mdia.gov.mt by the 30th June 2023.

Malta Digital Innovation Authority

19th May 2023

2 Definitions

2.1 Abbreviations

CIO	Chief Information Officer
CTO	Chief Technology Officer
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	System Auditor
TAAF	Technology Assurance Assessment Framework
TE	Technical Expert

2.2 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 TAAF programme for an IDPS that they have legal rights to own or operate. The Applicant also refers to the person within the legal organisation, with executive powers, and who will be responsible for liaising with the Authority and the operation of the IDPS. Ideally this is fulfilled by a technical role, such as a CTO or a CIO.

"**Application**" and "**Application Form**" shall mean the request and set of documents submitted by the Applicant for the purposes of participating in the TAAF programme.

"**Assessment**" refers to the action through which Applicants shall obtain their Official Recognition, in accordance with the TAAF, that can be either a self-assessment performed by the Applicant, an innovative technology review performed by a Technical Expert, or an assurance assessment performed by a Systems Auditor.

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

"**Assessor**" refers to the individual or legal organisation conducting the Assurance Assessment, which can be either a Systems Auditor or a Technical Expert. The Assessor must be approved by the MDIA as described in the guidelines for each respective role prior to any TAAF-related appointments.

"**Assurance**" refers to the result of the Assessment documented in a report, developed by the Assessor for a specific IDPS. Use of the term 'Assurance' in the context of TAAF should not be misconstrued as a guarantee of certainty or complete protection.

"**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 TAAF recognitions, acknowledgments, and certifications.

"**Information Security**" refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

"**Innovative Digital Product or Service (IDPS)**" refers to an innovative technological product, solution or service being provided in line with the Innovative Technology Arrangements and Services (ITAS) Certification Regulations. 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.

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

"**Official Recognition**" in the context of TAAF refers to the acknowledgements, certificates, or other forms of recognition or validation issued by the Authority upon satisfactory completion of the TAAF programme.

"**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 governing the MDIA and innovative technology.

"**Resident Agent**" refers to the Resident Agent as defined in Article 13 of the Regulations. This is generally 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 Auditor (SA)**" refers to the individual or 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.

"**TAAF 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 Assurance Assessments for the attainment of TAAF Certifications in 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.

"**Technological Domains**" refers to the different technology domains that the Assessment may be focussed on. While some domains are quite specific, TAAF also defines a generic technology domain that enables any IDPS to obtain Official Recognition.

"**Technology Assurance Assessment Framework**" and "**TAAF**" refers to the current framework for recognition, certification or acknowledgement offered by the Authority as defined in this document.

"**Tri-party Meeting**" refers to a meeting between the Assessor, the Applicant, and the Authority. It is usually called upon submission of an Assessment by the Assessor 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.*

3 Introduction to TAAF

The Technology Assurance Assessment Framework (TAAF) is a tiered Assurance framework by the MDIA that is able to provide varying degrees of technological assurances for a broad spectrum of technologies operating at varying risk levels. TAAF is designed to cater for innovative technologies to be aligned with international standards and industry best practices. The framework has been designed with future scalability in mind such that new technologies may be seamlessly introduced as deemed necessary by the Authority.

TAAF is intended for owners and/or operators of IDPSs, by providing Applicants with Assurance in relation to the technology-related controls they implement in developing and operating their IDPS. More specifically, the Assessment is meant to look into the implementation and operational effectiveness (when applicable to the identified Assessment Level) of controls to mitigate and manage the information security and operational risk. Additionally, the TAAF Official Recognition aims to provide a level of comfort to their stakeholders which may include Lead Authorities (and other applicable sector regulators), investors, developers, suppliers, end-users, and the public.

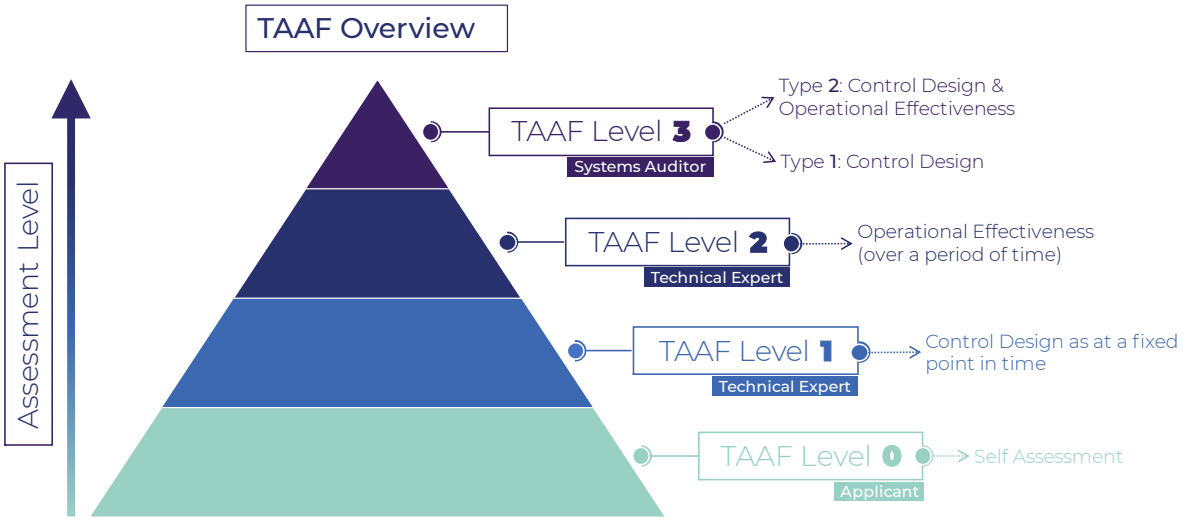

Figure 1 - An overview of the structure of TAAF, with different Assessment Levels building on each other for higher Assessment Levels

Further to the Assessment Levels, TAAF 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.

3.1 High-level Process

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

At a high level, the TAAF 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 Official 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 4.5.
- **#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, submits it to the Authority which reviews it and decides on whether to award the Official 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 Official Recognition to the Applicant. This is detailed in each of the respective Assessment Level details, and in section 9.3.

3.2 Assessment Level Overview

There are four (4) Assessment Levels in TAAF, which increase in complexity and the level of Assurance 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. TAAF Level 0 Assessments are domain-specific and cannot be applied for independently.
- **Assessment Level 1**: 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 considers the design of the controls in place by the IDPS as of a specific date in relation to those specified by the Authority for the relevant technology domain.
- **Assessment Level 2**: This, too, 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 considers the design as well as operational effectiveness of the controls in place by the

IDPS throughout a specified period of time, in relation to those specified by the Authority for the relevant technology domain.

- **Assessment Level 3**: This is the highest level of TAAF Official Recognition that may be obtained and is typically meant for an IDPS that is deployed within a risky or critical environment or otherwise requires a high level of compliance to the relevant controls. The Assessment is conducted by a Systems Auditor in the form of an interview and an evidence-based verification, to analyse and verify that the control design, existing documentation and operational effectiveness of the controls designed for high-risk technological deployments are in line 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, that is commensurate to the levels of risk and scrutiny relevant to the chosen Assessment Level.

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

	TAAF Level 0	TAAF Level 1	TAAF Level 2	TAAF Level 3
Assessor	Applicant	Technical Expert		Systems Auditor
Methodology	Self-Assessment	Technology Review		Assurance Assessment (ISAE3000)
Technology Domains	Sector Specific	o General Innovative Technology o Cloud Computing o Internet of Things o Artificial Intelligence o Blockchain		
Control Types	Specific to each Initiative	o Accountability o Availability o Confidentiality o Integrity o Privacy		
Due Diligence	Monitoring	Prior to Onboarding		
IDPS Blueprint	Not required	Required		
Risk Level	Low	Medium		High
Nature of Assessment	Questionnaire	Technology Review Report		ISAE 3000
Assessment Scope	Maturity Assessment	Control Design	Control Design & Operational Effectiveness	o **Type 1**: Control Design o **Type 2**: Control Design & Operational Effectiveness

3.3 Technology Domains

For Assessment Levels 1-3, the Applicant will be asked to identify the technology domains to be assessed as part of the application. TAAF currently supports the below technology domains:

- **General Innovative Technologies**: 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").
- **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 TAAF.

> *Note: The Authority may amend or add new technology domains at any time throughout the lifetime of TAAF. Furthermore, while the Applicant is required to identify the relevant technology domain, the Authority reserves the right to require a particular domain it deems applicable to be included in scope.*

3.4 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.
- **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 Official 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.

3.5 MDIA Official Recognition

TAAF Official 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 TAAF 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.
- **Recognition**: This is provided for by TAAF 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 TAAF 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.

Official Recognitions issued by the MDIA under TAAF shall be strictly limited to the aspects of the innovative technology 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.

An Official Recognition, be it an acknowledgement, recognition or certification, is not meant to be interpreted as a guarantee that the innovative technology is unable to fail but is merely to serve as proof that a certain level has been achieved in developing, deploying and operating an IDPS.

Note: The Authority reserves the right to withdraw an Official Recognition should the terms highlighted in section 10.1 be violated, or new information surface after issuance and the Applicant fails to provide a satisfactory response.

4 Application

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

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

4.1 Eligibility

Any individual or legal organisation that develops, operates, or otherwise has rights to an IDPS may apply for the TAAF (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 Official 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 Official Recognition of other technology domains in addition to the ones current established in TAAF. In such instances the eligibility criteria defined in such additional guidelines will also apply to the eligibility criteria listed in these TAAF guidelines, unless otherwise specified in the newly issued guidelines.*

4.2 Applicant Obligations

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

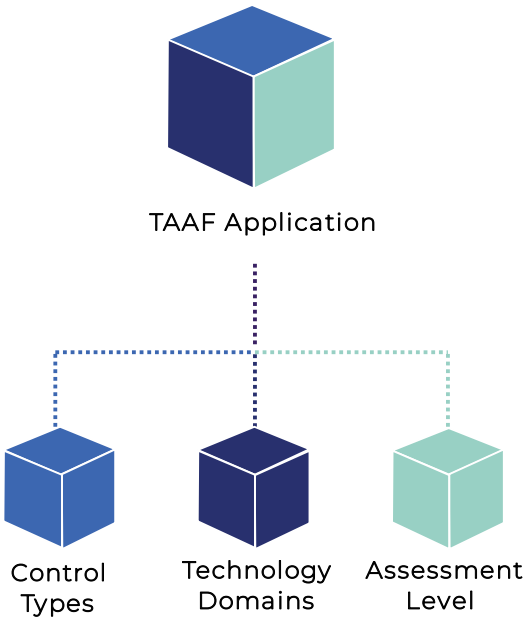

Figure 3 - TAAF Application Components

While the TAAF certification process varies depending on the Assessment Level selected, prospective Applicants for TAAF Assessment Levels 1, 2, and 3 must submit a *Technology Assurance Assessment Application Form* to the Authority, including the IDPS Blueprint and other supporting documentation required.

4.3 Application Processing

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

- Review and assess the information provided in the TAAF 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 their 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 their role with respect to the Application and conduct necessary due diligence.

The Authority reserves the right to respond to the submission of an application by recommending alterations to the Assessment Level, Technology Domains and Control Types identified. The Authority further reserves the right to turn down the Applicant's request on the basis that the type of Official Recognition selected in the application does not align to the risks presented by the IDPS. In such cases, the Authority will provide its reasons in writing, and should the Applicant disagree with the Authority's decision, it may challenge the decision through the remedies provided for in the Act.

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.

4.4 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 to the Authority. This document will also be used by the Assessors to understand their scope of work.

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

- The mandate that entitles the Applicant to submit such an application, 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, which also specifies Forensic Log requirements (refer to section 9.4).

4.4.1 Forensic Logging

The manner in which the purposes of the Forensic Node are to be achieved are to be documented in the IDPS Blueprint, including:

- 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.
- Data 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 9.4 of the TAAF 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.

4.5 TAAF Application Procedure

The process for applying for TAAF 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 TAAF 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 TAAF from the MDIA website.
3. The Applicant obtains all information required by the application (including documentation mentioned in these guidelines), and compiles the application, including supporting documentation. The Applicant must submit:
    a. The relevant TAAF Application Form,
    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.

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

5 Level 0: Self-Assessment

The TAAF Assessment Level 0 (hereinafter referred to simply as Level 0) provides an easy-to-access and easy-to-use quantitative self-assessment programme, that provides immediate feedback and is meant to be primarily educational in nature.

This aspect of TAAF creates a structure around which the MDIA or other Lead Authorities (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.

An example of such a TAAF 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 TAAF Assessment Level 0 initiatives 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).

TAAF 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 TAAF Level 0 Applicant must provide identification information and documentation necessary to identify the Applicant, both when the Applicant is applying in his personal capacity as well as when doing so in representation of a legal organisation (if applicable).

While TAAF 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 TAAF 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.

Further to the above, the Applicant will also have the option to obtain an Official Recognition as described in section 5.6.

5.5 Methodology

While TAAF 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 TAAF Level 0 initiative.

TAAF 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 Official Recognition by the Authority as further detailed in section 5.6.

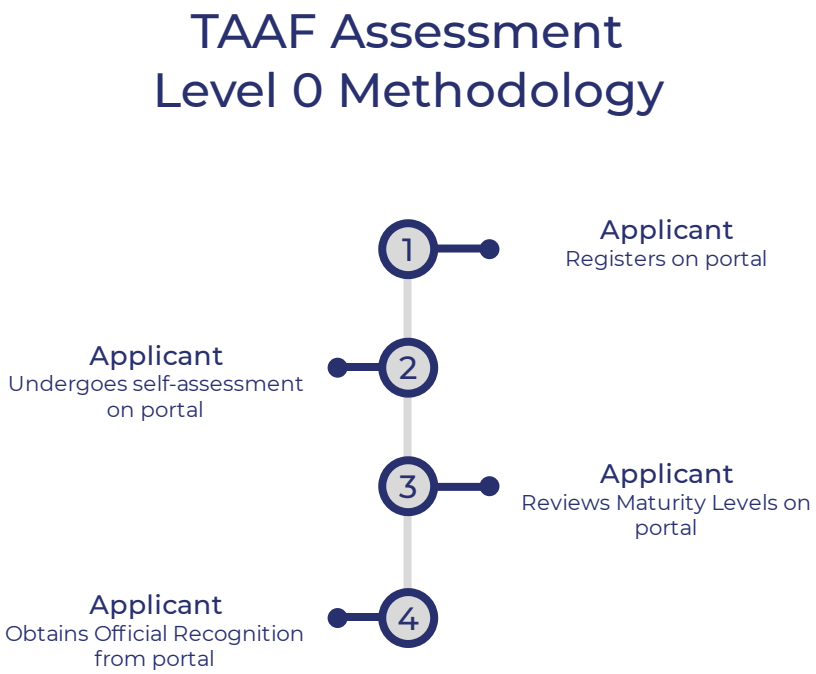

Figure 4 - TAAF Assessment Level 0 Methodology

> ***Note:*** *While the Authority does not necessarily conduct specific on-boarding due-diligence for TAAF Level 0 (due to the inherently low risk nature of the Assessment Level type), 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 Official Recognition

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

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

While the TAAF 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 Official 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.

6 Level 1: Technology Controls Design Review

The TAAF Assessment Level 1 (hereinafter referred simply as Level 1) is a qualitative Assessment carried out by a Technical Expert on an IDPS. The Technical Expert must be approved by the MDIA and must be independent from the Applicant or IDPS.

The Level 1 Assessment is meant to evaluate whether the controls in place by the IDPS are suitably designed, as of a specific point in time, in view of the control objectives specified by the Authority, and the risk(s) exposed by the IDPS.

TAAF Level 1 Assessments are primarily carried out via interviews and evidence-based collection and analysis carried out by the Technical Expert. For TAAF Level 1 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.

> ***Note:*** *While TAAF Level 1 Assessments are similar in many ways to TAAF Level 2, they differ in that Level 1 strictly considers the design of the controls as at a point in time, while TAAF Level 2 also considers operational effectiveness over a specified period of time.*

6.1 Target Audience

TAAF Level 1 is intended for Applicants whose IDPS either has a lower risk footprint, or which is starting out and would like to identify any potential weaknesses or areas to strengthen through an independent Assessment. While this is typically envisaged to be start-ups or small-to-medium sized operations, it may apply to any Applicant that wishes to obtain Official Recognition by the Authority to show that they have a reasonable level of suitably designed controls in place, without necessarily looking at the operational effectiveness of such controls over a period of time (see TAAF Assessment Level 2) or undergoing an in-depth rigorous audit (see TAAF Assessment Level 3).

While TAAF Level 1 necessitates the appointment of a Technical Expert to independently conduct the Assessment in the form of a technology review, Level 1 Assessments are intended to provide an IDPS with an opportunity to obtain tailored Official Recognition at a lower cost than subsequent levels, since the Technical Expert review is only intended to look at the design of controls as of a specific point in time.

However, it is important to note that Level 1 still necessitates a degree of scrutiny. Therefore, Applicants must ensure that their IDPS has the necessary controls designed prior to undertaking the Assessment to obtain Official Recognition.

6.2 Due Diligence

Due diligence requirements for Assessment Level 1 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 TAAF 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.

Note: When the Applicant is a Government of Malta entity, it shall only be requested to provide a Board Resolution or a similar document authorising the said entity to submit an Application and to be bound by the terms of the TAAF and authorising the signatory to sign on its behalf.

6.3 Controls

TAAF Level 1 Assessments, including the scope of the Assessment carried out by the Technical Expert, are based on the Technology Domains (refer to section 3.3) and Control Types (refer to section 3.4) selected by the Applicant (and subject to review by the Authority) at Application stage (refer to section 4).

6.4 Report

Upon completion of the TAAF 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. The report itself may identify any control designs that must be improved and might also make recommendations where applicable on control designs.

In view of this information, the Authority, together with any additional insight from the Technical Expert if deemed necessary, 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.

6.5 Assessment Process

The below steps describe the steps involved in the TAAF Level 1 Assessment stage:

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.
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.
8. The Authority issues the Official Recognition to the Applicant.

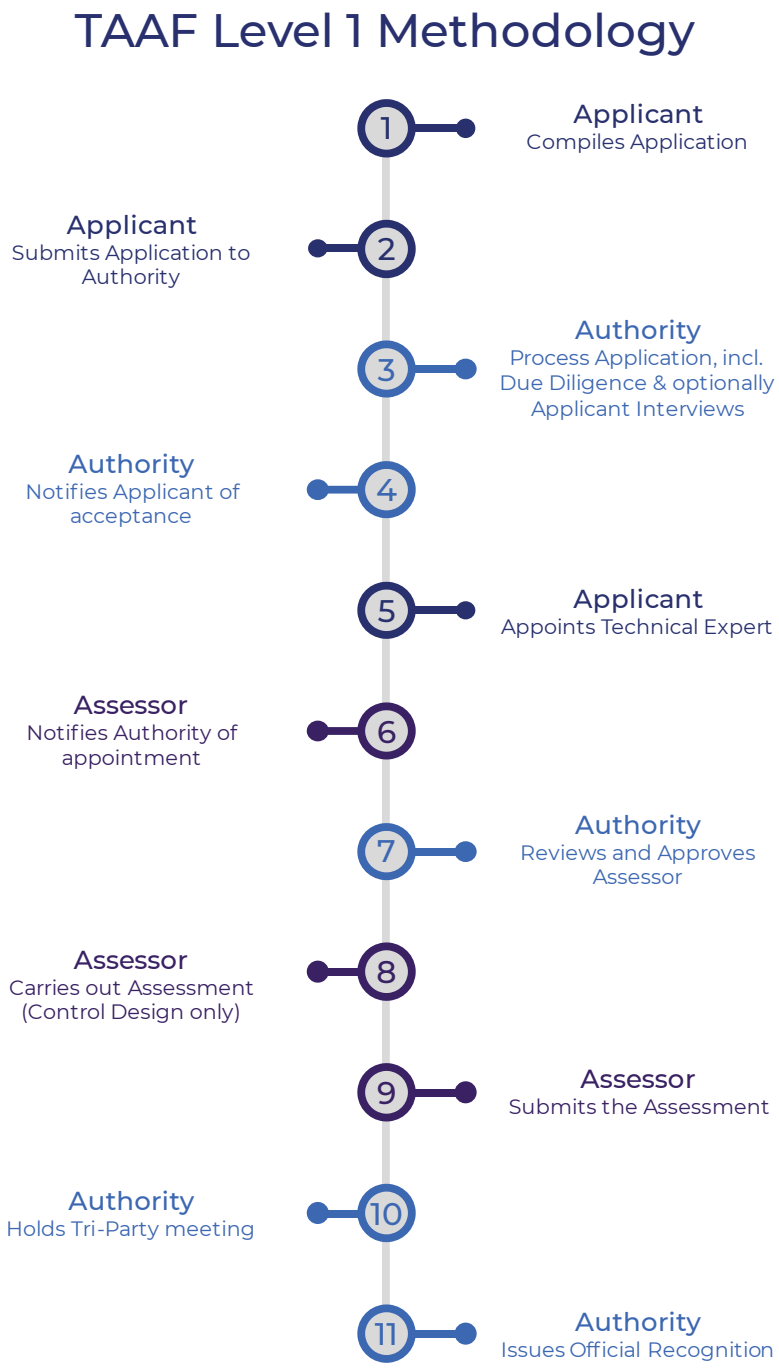

Figure 5 - TAAF Assessment Level 1 Process

6.6 Official Recognition

Official Recognition for TAAF Level 1 will be in the form of an electronic document 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. The Official Recognition for TAAF Level 1 is valid for two (2) years from the date of issuance.

The Official Recognition for TAAF Level 1 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 Official Recognition on its website and, if applicable, refer to it on its IDPS.

> ***Note:*** *The Authority reserves the right to withdraw the Official Recognition at any time should new information surface about the validity of any material that contributed to the submitted Assessment, including (but not limited to) information disclosed in the Technical Expert interviews, or provided as evidence.*

7 Level 2: Technology Controls Effectiveness Review

The TAAF Assessment Level 2 (hereinafter referred simply as Level 2) is a qualitative Assessment carried out by a Technical Expert on an IDPS. The Technical Expert must be approved by the MDIA and must be independent from the Applicant or IDPS.

The concept behind TAAF Level 2 Assessments is very similar to TAAF Level 1 with one key difference: further to evaluating whether the controls in place by the IDPS are suitably designed, Level 2 also looks at the operational effectiveness of those controls over a specified period of time.

TAAF 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 operational effectiveness (such as, but not limited to, internal logs or reports). For TAAF 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.

7.1 Target Audience

TAAF Level 2 targets Applicants who are looking for an increased level of analysis on their IDPS, by considering the effectiveness of controls over a period of time. While this also applies to IDPS with a lower risk footprint, it may be more suitable for an IDPS with medium risk, such as one that has a large user base, or one that has been in operation for a while. More than just identifying strengths and weaknesses in the control design, Level 2 Assessments also provide insight on how those controls performed during operation. The Official Recognition for TAAF Level 2 presents a balanced opportunity for Applicants who wish to review their operation over a period of time and provide a higher peace of mind to their stakeholders than TAAF Level 1, without undergoing an in-depth rigorous audit (see TAAF Assessment Level 3).

The TAAF Level 2 Assessment is carried out by an independent Technical Expert (similar to Level 1) in the form of an innovative technology review, with an Official Recognition issued by the Authority should the Assessment be satisfactory to the Authority for issuing of such.

As TAAF Level 2 has a higher degree of scrutiny, in view of the Assessment considering operational effectiveness over a period of time, Applicants should make sure that their IDPS not only has the necessary controls designed, but they also have been operating for enough time to put these controls into use.

7.2 Due Diligence

Due diligence requirements for Assessment Level 2 focuses 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 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 TAAF 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.

Note: When the Applicant is a Government of Malta entity, it shall only be requested to provide a Board Resolution or a similar document authorising the said entity to submit an Application and to be bound by the terms of the TAAF and authorising the signatory to sign on its behalf.

7.3 Controls

TAAF Level 2 Assessments, including the scope of the Assessment carried out by the Technical Expert are based on the Technology Domains (refer to section 3.3) and Control Types (refer to section 3.4) selected by the Applicant (and subject to review by the Authority) at Application stage (refer to section 4).

7.4 Report

The outcomes of TAAF Level 2 are also similar to those of TAAF Level 1.

Upon completion of the TAAF Level 2 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. The report itself may make recommendations and identify any control designs that must be improved also due to analysing how they performed throughout the time period under Assessment.

In view of this information the Authority, together with any additional insight from the Technical Expert if deemed necessary, will take a decision on whether to issue the Official Recognition to the IDPS, with or without conditions (such as to add or improve controls within a stipulated period), or whether to reject issuance of Official Recognition, particularly in cases of significant deficiencies.

7.5 Assessment Process

The below steps describe the steps involved in the TAAF Level 1 Assessment stage:

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.
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.
8. The Authority issues the Official Recognition to the Applicant.

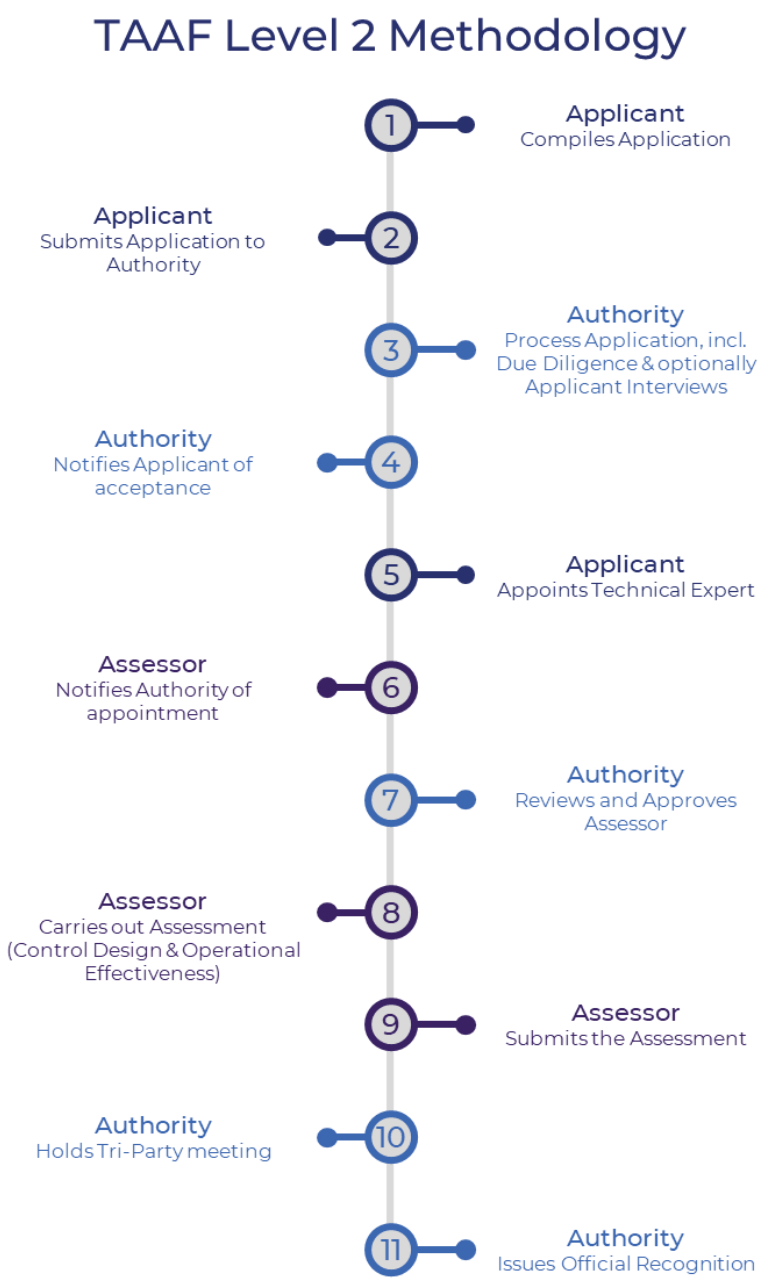

Figure 6 - TAAF Assessment Level 2 Process

7.6 Official Recognition

Official Recognition for TAAF Level 2 will be in the form of an electronic document 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. The Official Recognition for TAAF Level 2 is valid for two (2) years from the date of issuance.

The Official 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 Official Recognition on its website and, if applicable, refer to it on its IDPS.

Note: The Authority reserves the right to withdraw the Official Recognition at any time should new information surface about the validity of any material that contributed to the submitted Assessment, including (but not limited to) information disclosed in the Technical Expert interviews, or provided as evidence.

8 Level 3: Technology Assurance Assessment

A TAAF Assurance Assessment Level 3 (hereinafter referred simply as Level 3) represents the highest level of Assurance possible within TAAF. While it is primarily intended for more mature and large-scale IDPS, it is also designed for use as a compliance utility for IDPS operating in high-risk environments. It offers a qualitative set of control objectives ranging from control design to control operational effectiveness to ensure robustness and a high-level of technology preparedness against sophisticated threats.

A TAAF Level 3 Assessment may only be conducted by an MDIA approved Systems Auditor, through rigorous interviews and detailed evidence-based verification. This high-level of rigour serves to ensure (as much as reasonably possible) that the design and operating effectiveness of the controls designed for such IDPS operations is of a high-quality.

TAAF 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 operational effectiveness of the controls during the period covered by the audit. This type of audit may be carried out periodically during the operational lifetime of the IDPS, or on the request of the Authority.

8.1 Target Audience

TAAF Level 3 is aimed towards Applicants who are looking for the highest level of Official Recognition from TAAF on their IDPS, by undergoing a Systems Audit by an MDIA-approved Systems Auditor. TAAF Level 3 is primarily intended to apply to mature large-scale IDPS, such as one that has a large user base and that may have significant high-risk features. Such high-risk may, among others, be due to financial aspects, data-privacy, or IDPS that can adversely affect human health.

TAAF Level 3 provides Applicants with an opportunity to ensure that their IDPS is secure, reliable, and compliant with industry standards, and to provide the maximum level of comfort to their stakeholders in their operation. Because of this, TAAF Level 3 Assessments require the highest level of preparation due to the detailed nature of a Systems Audit.

8.2 Due Diligence

Due diligence requirements for TAAF Level 3 are the most onerous due to the higher levels of Assurance the Official Recognition provides.

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 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.

> *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 TAAF and authorising the signatory to sign on its behalf. Note: When the Applicant is a Government of Malta entity, it shall only be requested to provide a Board Resolution or a similar document authorising the said entity to submit an Application and to be bound by the terms of the TAAF and authorising the signatory to sign on its behalf.*

8.3 Controls

TAAF Level 3 Assessments, including the scope of the Assessment carried out by the Systems Auditor are based on the Technology Domains (refer to section 3.3) selected by Applicant (and subject to review by the Authority) at Application stage (refer to section 4).

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 risk associated with TAAF Level 3 Assessments. Exemptions to this may be most pertinent when the Level 3 Official Recognition is mandated by another NCA (refer to section 11).

8.4 Report

The TAAF Level 3 Assessment is in the form of a Systems Audit carried out by a Systems Auditor and which is compiled into an ISAE3000 (or equivalent standard)

report. Once compiled, this report is submitted to the Authority for review and a follow-up discussion will be held during a tri-party meeting between the Authority, IDPS/Applicant, and the Systems Auditor and its appointed Subject Matter Experts (all of whom must be approved by the Authority).

Once the report is submitted to the Authority and the tri-party meeting has taken place, the Authority will take a decision on whether to issue the Official Recognition for TAAF 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 Official Recognition, particularly in cases of significant deficiencies. Further to the official tri-party meeting, the Authority may require further follow-ups with the IDPS, Systems Auditor, or both, to reach its decision.

8.5 Assessment Process

The below steps describe the steps involved in the TAAF Level 1 Assessment stage:

1. The Systems Auditor and Applicant make logistical arrangements for the Audit. For Level 3, this is more likely to require multiple sessions with different stakeholders.
2. The Systems Auditor collects the information through interviews, documentation review, collection of evidence or any other means they deem necessary and draft the Assessment (ISAE3000 report).
3. The Systems Auditor may request additional follow-ups and/or evidence to be provided or reviewed.
4. The Systems Auditor notifies the Authority and the Applicant that the Assessment has been conducted, and the report has been prepared.
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 Systems Auditor 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 to remediate them.
8. The Authority issues the Official Recognition to the Applicant.

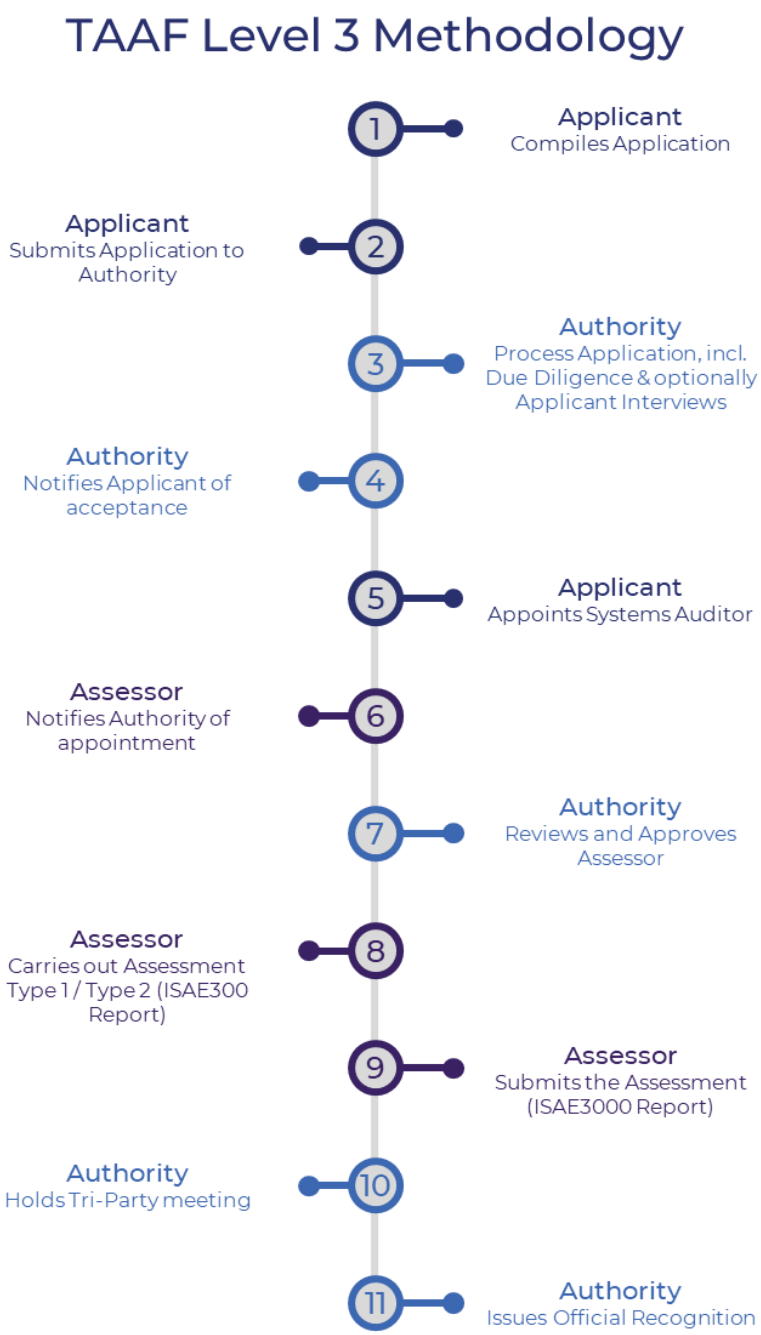

Figure 7 - TAAF Assessment Level 3 Process

8.6 Official Recognition

Official Recognition for TAAF Level 3 will be in the form of an electronic document 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 TAAF Level 3, it will also highlight whether the Assessment was of Type 1, or Type 2.

The Official Recognition for TAAF 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 Official 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 Official Recognition on its website and, if applicable, refer to it on its IDPS.

> ***Note:*** *The Authority reserves the right to withdraw the Official Recognition at any time should new information surface about the validity of any material that contributed to the submitted Assessment, including (but not limited to) information disclosed in the Systems Auditor interviews, or provided as evidence.*

9 General Conditions

This section outlines some general conditions related to TAAF.

9.1 Recertification Procedure

The recertification procedure applies to TAAF Assessment Levels 1–3.

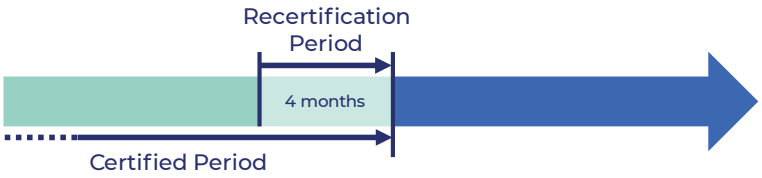

Figure 8 Graphical representation of Recertification timeline

The Applicant may apply for a renewal of the existing Official 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 Official Recognition is kept valid and effective and that subject to the confirmation by the Authority, the Official Recognition will be renewed at least within the last three months of its duration and, in any case, prior to expiry.

> *For TAAF Assessment Level 0, the Applicant may undergo the self-assessment again at any point before or after the Official Recognition expires.*

9.2 Processing Fees

Payments shall be processed in accordance with the payment schedule.

9.3 Official Recognition

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

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

The period of validity of any Official 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.

9.4 Forensic Logs

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. This is equivalent to what was previously referred to as the *Forensic Node*.

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 logging that takes steps to prevent tampering with is nonetheless considered as a critical mechanism for ensuring the security and compliance of an IDPS that has Official Recognition.

Note that due to the all-encompassing and possibly sensitive and/or personal nature of the information to be stored on the Forensic Log, this data must be stored securely, and with appropriate audit logs to prevent tampering.

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:

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.

9.4.1 Requirements

Forensic 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 Forensic Logs.
d) Procedures detailing how responsible persons may access the Forensic 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 Forensic Logging is to be implemented must be contained in the IDPS Blueprint, as specified in section 4.4.

10 Legal and Regulatory Requirements

10.1 Official Recognition Conditions

An Official 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 (when the Applicant is a legal organisation) are to take place. A transfer of ownership is considered to take place when the transfer is a Qualifying Transfer and this may only take place with the prior approval of the Authority.

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 Official Recognition.

Any conditions mentioned by the Assessor in the report, and on the basis of which the Authority issues its Official Recognition, shall be binding on the Applicant as a condition of the Official Recognition. The Authority reserves the right to specify these conditions on the Official Recognition at its own discretion.

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

An Official 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 Official Recognition and take any other remedies allowed for in the Act.

Should throughout the Application stage or the lifetime of an Official Recognition, any material changes to the information submitted in the process leading to the Official 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 Official Recognition that was issued and may, where deemed appropriate, suspend the Official Recognition until such time as it carries out this review. Where the Authority concludes that the change in circumstances warrants further clarification, 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 Official 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 Official Recognition or the carrying out of any other remedial action within the powers afforded to it by law, it 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 TAAF Level 3 Assessment Type), or the appointed Technical Expert (in case of TAAF Level 1 or 2) or Systems Auditor (in case of TAAF 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 Official Recognition;
d) any development altering the rights of users of the IDPS.
e) changes to any information provided to the Authority as part of the TAAF application which have been relied upon by the Authority in issuing the Official 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 Official Recognition is a pre-requisite for the Applicant to be able to provide innovative technology products, solutions or services in a regulated environment or context.

Where prior notification of, or authorisation to any envisaged changes is not required according to the above provisions, the Applicant to whom an Official 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 innovative technology obtaining the Official 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.

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 an Official 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 4.4) 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 Official 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.

11 TAAF as a tool for Lead Authorities

Part of the reason behind the flexibility of TAAF in providing Official Recognition by the MDIA at various levels, and across various Technology Domains and Control Types, is to enable TAAF to be leveraged by other Lead Authorities. This allows other government entities to utilise the TAAF when technology-related Assurances are required, 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 TAAF 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 TAAF to provide general Assurance, this custom certification may also be used either for a specific deployment within the same government entity, or for regulatory purposes. Such certification 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 an Official Recognition, which Official Recognition shall be jointly recognised by the MDIA as well as the requesting NCA.

12 Alignment to legacy MDIA Offerings

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

MDIA Service	TAAF Alignment
ITA Systems Audit for DLT solutions	This is replaced by TAAF Assessment Level 3, focussed on the DLT domain
Technology Assurance Sandbox (TAS)	The TAS fits under TAAF Assessment Level 1. It is effectively a set of TAAF Assessment Level 1's spread across a number of milestones (depending on the Residency Plan).
Mind the Gap	This was designed from the start to be TAAF Level 0 compliant.

13 Appendices

13.1 TAAF 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, 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.
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.

13.2 TAAF 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.