Chapter 01

Systems Auditor Guidelines

MDIA
Malta Digital Innovation Authority

MDIA Circular No.1

Introduction

On the 04 July 2018 the Maltese Parliament enacted Malta's regulatory framework for digital innovation through the:

- Malta Digital Innovation Authority Act, 2018[1];
- Innovative Technology Arrangements and Services Act, 2018[2]; and
- Virtual Financial Assets Act, 2018[3];

By means of Legal Notice 250 of 2018, the Parliamentary Secretary for Financial Services, Digital Economy & Innovation, established on the 15 July 2018 as the date on which the provisions of the Malta Digital Innovation Authority Act is deemed to have come into force. As a result, The Malta Digital Innovation Authority (MDIA) is now formally set up.

Amongst its various duties, the MDIA is responsible for recognising Service Providers, namely Systems Auditors and Technical Administrators, as well as, certifying Innovative Technology Arrangements (ITAs) as contemplated in the Innovative Technology Arrangements and Services Act.

With this in mind, the MDIA will be issuing a set of guidance notes aimed at assisting Service Providers and ITA Applicants when approaching the MDIA for registration and certification respectively. These guidelines will be divided into four chapters as follows:

Chapter 1 Systems Auditors Guidelines
Chapter 2 Innovative Technology Arrangement Guidelines
Chapter 3 Technical Administrator Guidelines
Chapter 4 Resident Agent Guidelines

[1] Chapter 591 of the Laws of Malta
[2] Chapter 592 of the Laws of Malta
[3] Chapter 590 of the Laws of Malta

Collectively, these chapters shall be referred to as the MDIA Guidance Notes. It is the MDIA's intention to seek feedback on each chapter through public consultations.

In due course the MDIA shall also be issuing standards that it deems necessary to ensure that the ultimate objectives of the Innovative Technology Arrangements and Services Act are met, as well as, ensure that Malta's reputation in this field is not compromised. Standards issued by the MDIA may be circulated for prior public consultation depending on the subject.

In order to ensure clarity, it is worth highlighting that with respect to the Virtual Financial Assets Act, the Malta Financial Services Authority is the lead authority issuing guidance to potential applicants.

The MDIA will also be driving the issuance of subsidiary legislation under the Innovative Technology Arrangements and Services Act with respect to applicable fees when seeking any form of authorisation from the MDIA. These regulations shall also be made available for consultation.

MDIA Public Consultation Ref No. 01/18

The MDIA is making available the first set of documents for public consultation, namely Chapter 1 – Systems Auditor Guidelines.

Chapter 1 – Systems Auditor Guidelines

Chapter 1 – Systems Auditor Guidelines shall apply to all interested parties who shall seek recognition from the MDIA as Systems Auditor, as defined in the Innovative Technology Arrangements and Services Act, 2018[4] and Systems Auditors who attain a recognition from the MDIA as contemplated in the said Act.

Chapter 1 is divided into two part as follows:

- Part A – Systems Auditor Guidelines
- Part B – Systems Audit Report Guidelines

[4] Chapter 592 of the Laws of Malta

Part A – Systems Auditor Guidelines

This section focuses on the:

- Scope of the Systems Audit
- Application process and approval criteria for a Systems Auditor
- Revocation, cancellations or suspension of a Systems Auditor from the MDIA's Register or Recognised Service Providers
- Engagement of the Systems Auditor including independence criteria that must be satisfied
- Systems Audit Reports

Part B – Systems Audit Report Guidelines

This section presents the form and structure of audit reports expected to be issued by Systems Auditors approved by the MDIA which shall focus on the following five key principles areas:

- Security
- Processing Integrity
- Availability
- Confidentiality
- Protection of Personal Data

Concluding remarks

The consultation period is open to the public from 18 September 2018 until 02 October 2018. Interested parties are requested to submit their comments and feedback by email on info@mdia.gov.mt by not later than 02 October 2018.

Malta Digital Innovation Authority
18 September 2018

PART A - Systems Auditor Guidelines

Contents

Digital Innovation is, by definition, a rapidly evolving sector. These guidelines are expected to be updated to keep abreast with technology, regulatory and operational developments.

1. Definitions

"Applicant", within the context of this document, refers to an individual and/or legal organisation applying for recognition as a Systems Auditor with the Authority.

"Auditee" refers to the individual and/or legal organisation that is subject to a Systems Audit as required by the Authority in the case of a provider of an ITA ('ITA Provider'), or as required by another recognised Lead Authority, such as in the case of an Issuer of VFA (as defined in article 2(2) of the Virtual Financial Assets Act (Cap. 590)) and certain Providers of a VFA Services as defined in the Second Schedule of the Virtual Financial Assets Act (Cap. 590).

"Authority" refers to the Malta Digital Innovation Authority ('MDIA').

"Initial Virtual Financial Asset Offering", also referred to as "IVFAO" within this document, as defined in Article 2(2) of the Virtual Financial Assets Act (Cap. 590), means a method of raising funds whereby an issuer is issuing Virtual Financial Assets (VFA) and is offering them in exchange for funds.

"Innovative Technology Arrangement", also referred to as "ITA" within this document, is defined within the First Schedule of the Innovative Technology Arrangements and Services Act, 2018. For the avoidance of doubt, this definition includes, inter alia, any ITA supporting an IVFAO, Providers of VFA Services or similar arrangements.

"Subject Matter Expert" is an individual who takes a specific technical role with the Systems Auditor based on his/her expertise. A Subject Matter Expert may be an employee of the Systems Auditor or a sub-contracted individual or an employee of a sub-contracted legal organisation.

"Lead Authority" refers to the "national competent authority" as defined within the Innovative Technology Arrangements and Services Act, 2018, which has a leading role within that application of the technology arrangement.

"Resident Agent" refers to the Resident Agent as defined in Article 15 of the Innovative Technology Arrangements and Services Act.

"Systems Auditor" ('SA') as defined in the Innovative Technology Arrangements and Services Act, 2018.

"Blueprint" refers to a document that includes a description of the qualities, attributes, features, behaviours or aspects of an ITA as defined by the respective Lead Authority. As an example, in the case of an Issuer of a VFA, the Whitepaper,

or parts thereof, registered with MFSA shall serve as the Blueprint. Further information on the contents of the Blueprint is provided in Chapter 2 of the MDIA Guidance Notes.

2. Systems Audit Scope

These Guidelines apply to:

- Any individual or legal organisation that is applying for registration or holds a Certificate of Registration, to act as a registered Systems Auditor; and
- Any Subject Matter Expert employed or sub-contracted with the Systems Auditor that is applying with the Systems Auditor.

In line with Article 9 of the ITAS Act, Applicants interested in performing Systems Audits shall apply to the Malta Digital Innovation Authority for their suitability to be registered. Subject to requirements established in this document, an Auditee may engage any registered Systems Auditor of their choice to audit Innovative Technology Arrangements or parts thereof. All Systems Audits carried out by registered Systems Auditors under these Guidelines documents shall only be subject to requirements as set-out by the Authority. The Systems Audit may be one of the following types:

- Type 1 Systems Audit: the Systems Auditor expresses an opinion on whether the description of the ITA is fairly presented and whether the controls included in the description are *suitably designed* to meet the applicable criteria[1]. This type of audit is typically carried when an Innovative Technology Arrangement is in the process of applying to be certified by the Authority; or when deemed necessary by the Authority, or other Lead Authority in Malta.
- Type 2 Systems Audit: the Systems Auditor's report contains the same opinions expressed in a Type 1 report, but also includes an opinion on the *operating 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 an ITA; or on the request of the Authority or other Lead Authority in Malta.

The Systems Auditor, being an individual or a legal organisation, is responsible for the final deliverable of the Systems Audit. The Systems Auditor is responsible to

[1] Applicable criteria form part of the following five (5) Key Principles: Security, Processing Integrity, Availability, Confidentiality and Protection of Personal Data.

conduct an audit following the ISAE 3000 standard[2]. The System Auditor shall nominate Subject Matter Experts to assist in specific technical fields during the System Audit. The Subject Matter Experts may be employees of the System Auditor or sub-contracted. The Authority expects that the Systems Auditor to have a complement of at least two (2) Subject Matter Experts. All Subject Matter Experts must be recognised by the Authority as part of the Systems Auditor registration process.

When carrying out a Systems Audit, the Systems Auditor will be expected to confirm in the Audit Report that the skills necessary to perform the audit of the particular Innovative Technology Arrangement are available to the Systems Auditor through Subject Matter Experts.

Before being registered by the Authority, Systems Auditors and the respective Subject Matter Experts shall be required to undertake a Competence Assessment, which can be done through remote means at the discretion of the Authority, and that consists of a series of questions aimed at verifying their knowledge on the subject matter to be audited. In addition, Systems Auditors and their Subject Matter Experts will be required to attend an interview with an Interview Board appointed by the Authority. The interview will be used for the Systems Auditors and their Subject Matter Experts to elaborate on the experience, qualifications and other information submitted in the Innovative Technology Service Provider application; and to verify the understanding of the role of the Systems Auditor, the Authority's Systems Audit Guidelines, systems security and Audit Reports.

The Authority may register an Applicant to act as a Systems Auditor only if the Applicant satisfies the requisite criteria through the aggregate of the Subject Matter Experts included in the application. The registration is valid for two (2) years from date of issue on condition that the Systems Auditor requirements are met during the period. In line with Article 9(6) of the ITAS Act, once registered by the Authority, the Systems Auditor is required to display the Certificate of Registration, as issued by Authority, on its website.

The Systems Auditor and the Subject Matter Experts are expected to keep up to date on the subjects on which they perform Systems Audits with a minimum of 20 hours per annum of continuous professional education (CPE). Records of CPE should be kept and may be required by the Authority for compliance and monitoring of registered Systems Auditors.

[2] https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga

The Authority may carry out quality reviews of registered Systems Auditors and in the process require access to documentation from the Systems Auditor including documentation supporting the Systems Audit process and related quality procedures.

3. Systems Auditor Recognition Criteria

As set out in Article 10 (2) (a) of the ITAS Act, a Systems Auditor may be a legal organisation that:

- Is formed and existing in accordance with the laws of Malta, of a Member State of the European Union, or of an EEA State;
- Has its registered office, central administration and principal place of business within Malta, or the European Union, or the European Economic Area;
- Whereof more than fifty (50) per cent of the legal organisation is owned and effectively controlled, whether directly or indirectly through one or more intermediate legal organisation, by persons that are citizens of Malta or citizens of a Member State of the European Union or of an EEA State; and
- Has a place of residence or business in Malta, the European Union, or the European Economic Area.

In addition, a Systems Auditor may be an individual ordinarily resident in the European Union, or in an EEA State.

In satisfying the requirements of Article 10 (2) (b) of the ITAS Act, a Systems Auditor (in the case of an individual), and the Subject Matter Experts, must, in aggregate, meet all of the following criteria:

- Hold a qualification in ICT and/or Information Security at MQF level 6 or higher;
- Hold a certification in IT Audit; or IT Risk or Security Management (such as CISA[3] or similar);
- Has experience in carrying out audits and reporting based on audit established standards (such as ISAE 3000);

[3] http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/

- Has suitable experience in Innovative Technology Arrangements in the fields that would be subject to audit of not less than two (2) years[4] during the last three (3) years.
    - Such experience must be corroborated with references of past engagements carried out with established and reputable entities as may be deemed fit by the Authority;
    - The fields that would be subject to a Systems Audit are directly related to the specific technologies involving the ITA such as development and/or auditing of DLT platforms, Smart Contracts, Solidity, Ethereum, Hashing, Cryptography, Distributed Systems and other emerging technologies recognised by the Authority.

The Authority expects that ITAs can involve innovative technology that may not be widely deployed or familiar. Within this context, the Authority reserves the right to vary this requirement in particular cases.

In addition, each Subject Matter Expert is required to have suitable post-qualification experience by having worked within the fields of IT audits; or development or implementation of web/enterprise-grade applications; or Information Security; for not less than three (3) years during the last seven (7) years, or five (5) years during the last ten (10) years. Such experience can be calculated as the total across the various fields stated within this clause and will need to be corroborated by appropriate evidence that may need to be presented to the Authority on request.

The Systems Auditor and each Subject Matter Expert must be of good conduct, fit and proper. Any skillset notification change by the Systems Auditor or Subject Matter Experts shall be submitted to the Authority as to update the recognised expertise of the individual registered with the Authority.

The Systems Auditor is required to be covered by a Professional Indemnity Insurance (PII) policy for an amount of not less than Euro 1,000,000. In order to perform audits of Innovative Technology Arrangements a Systems Auditor would need to have a sound knowledge of the applicable laws; standards; regulations and guidelines relevant to the subject matter.

[4] One year of experience is considered to be at least 50% of one year's equivalent of full time employment.

In line with Article 15 of the ITAS Act, an Applicant that is not ordinarily resident in Malta is required to appoint a Resident Agent. Refer to the respective Resident Agent Guidelines as issued by the Authority for further guidance.

4. Documents required for a Systems Auditor Application

An Applicant is required to complete and submit the relevant Application Form and remit the requisite fees to the Authority along with the following documentation:

- A general description of the Systems Auditor track record: in the case of an individual, a career history; in the case of a legal organisation, a corporate profile;
- Shareholding/partnership structure if the Systems Auditor is a legal organisation;
- Organisational structure and governance processes (including units in charge of the audit team) if the Systems Auditor is a legal organisation;
- CVs of the Subject Matter Experts to meet requisite qualifications and experience requirements (as identified in Section '3. Systems Auditor Recognition Criteria' above).

5. Subject Matter Experts

Subject Matter Experts identified in the Systems Auditor application must be bound by a contract with the Systems Auditor at the time of application. Such contracts may need to be disclosed to the Authority for review.

If a Subject Matter Expert included in the Systems Auditor application is no longer available, an application to update the Systems Auditor registration, including any applicable fees, must be submitted to the Authority indicating the changes and replacement (if any) of Subject Matter Experts to meet the requisite criteria.

The role of each Subject Matter Expert and the areas of a Systems Audit covered by the Subject Matter Expert will be documented in the Systems Audit Report and the Subject Matter Expert will take responsibility for the work he/she performs.

Independence obligations applicable to the Systems Auditor on a Systems Audit assignment also apply to each Subject Matter Expert on that audit.

The Subject Matter Experts responsible for Security Testing should meet the following minimum standards:

- Hold a certification in information security assessment (OSCP or CREST)
- Assess the level of secure coding (such as the OWASP Secure Coding Principles)
- Report the result of this security assessment in the form as described by the SANS Institute ("Writing a Penetration Testing Report")
- Undertake security tests in-line with the industry good practices for information security, documenting and rating each vulnerability found in line with the CVE[5] security vulnerability online data source.

CREST (www.crest-approved.org) provides qualifications in a range of security areas such as threat analysis, attack and response including penetration testing (web applications; infrastructure), and at different levels of proficiency (practitioner; registered; certified).

OSCP (www.offensive-security.com) offers tools and certifications in various types of penetration testing and levels of proficiency (professional; expert). The *Secure Coding Practices Quick Reference Guide*[6] is a technology agnostic set of general software security coding practices, in a comprehensive checklist format.

OWASP (www.owasp.org) is an open community dedicated to enabling organisations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. The focus is on secure coding requirements, rather than on vulnerabilities and exploits.

The SANS Institute (www.sans.org) guidelines *Writing a Penetration Testing Report*[7], is one of the leading industry guidelines providing a standardised style for a security testing report. The comprehensive report structure facilitates the process of understanding and navigating the contents and findings of such an exercise. It includes an executive summary, assessment objectives, assumptions, timeline, summary of findings and recommendations as well as a detailed description of each vulnerability identified including its recommended patching.

6. Independence of the Systems Auditor

During audit engagements, the Systems Auditor, including the related Subject Matter Experts, shall be independent of the Auditee.

[5] https://www.cvedetails.com/
[6] https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf
[7] https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343

Independence from the Auditee is required both during the engagement period and the period covered by the letter of engagement. The engagement period starts when the audit team begins to perform audit services. The engagement period ends when the Audit Report is issued. When the engagement is of a recurring nature, it ends at the later of the notification by either party that the professional relationship has terminated or the issuance of the final Audit Report.

For the purposes of the Systems Auditor engagement for a Systems Audit, consultancy work, assistance in the application process, implementation of systems, book keeping, accounting and internal audit services provided to the Auditee in the preceding twelve (12) months by the Systems Auditor or affiliated entities or any one or more of its employees, Subject Matter Experts or sub-contractors who shall be involved in the performance of the Systems Audit shall be deemed to have a conflict of interest.

7. Systems Auditor Engagement

Upon being appointed to act as Systems Auditor by the Auditee, the Systems Auditor shall:

- Notify the Authority of the appointment by the Auditee to act as its Systems Auditor;
- Submit a statement to the Authority confirming that the Systems Auditor and any Subject Matter Experts involved in the Systems Audit are free from any conflict of interest (refer to Section '6. Independence of the Systems Auditor');
- Submit an 'Authorisation to Release Information' form by the Auditee (to allow the Systems Auditor to disclose any information relating to the Auditee to the Authority);
- Confirm the timeframe within which the Systems Audit will be carried out.

A Systems Auditor is required to cover all Control Objectives as defined by the Authority – refer to Section '9. Systems Audit Control Objectives' below for further guidance. From time to time, the 'Systems Audit Report Guidelines' and the 'Systems Audit Control Objectives' may be updated to cover additional areas as required by the Authority.

8. Systems Audit Reports

The 'Systems Audit Report Guidelines' published by the Authority provides guidance on the content, format and objectives of the Systems Audit Report.

The final Systems Audit Report must be signed by the Systems Auditor and by all Subject Matter Experts involved in the Audit. In the case where a Systems Auditor is a legal organisation, the authorised representative shall sign the Audit Report, stating his/her name and position in the legal organisation.

Independent of the regulatory framework under which a Systems Audit report is issued, a copy of such report shall be filed with the Authority for the sole purpose of establishing internal mechanisms to monitor the quality of registered Systems Auditors.

In addition, upon completion of each Systems Audit, the Systems Auditor is also required to collect the 'Systems Audit Report Registration Fee' from the Auditee, a fee to cover the registration of the Systems Audit Report, and remit this fee to the Authority within thirty (30) days.

The Systems Auditor must establish policies and procedures for the retention of engagement documentation for a period of not less than five (5) years from the date of the Systems Audit Report.

9. Systems Audit Control Objectives

The Systems Audit Control Objectives are designed to provide and assist the Systems Auditor with an audit framework in the field of Innovative Technology Arrangements. The Control Objectives are based on five (5) Key Principles, inspired by AICPA SOC2[8] auditing guidelines, Information Security industry good practices, and specific requirements established by the Authority:

- **Security**: Information and systems are protected against unauthorised access, unauthorised disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and protection of personal data or systems and affect the Auditee's ability to meet its objectives.
- **Processing Integrity**: Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorisation of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorised or inadvertent manipulation. Because of the number of systems used by an Auditee, processing integrity is usually only addressed at the respective system or functional level.

[8] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

- **Availability**: Availability refers to the accessibility of information used by the Auditee's systems, as well as the products or services provided to its customers. The availability objective does not set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.
- **Confidentiality**: Confidentiality addresses the Auditee's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the Auditee's control in accordance with the Auditee's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorised access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for internal personnel.
- **Protection of Personal Data**: Processes underlying the ability to process personal data in compliance with applicable legislation. Although the confidentiality applies to various types of sensitive information, Protection of Personal Data relates only to personal data.

The Systems Audit Control Objectives are provided in a separate document entitled 'Systems Audit Control Objectives'. Below is a summary of the applicable areas:

Common Criteria	Applicable Areas
Functionality and Compliance with Regulatory Requirements	Functionality Code Review, Platform Implementation, Forensic Node
System Operations	Vulnerabilities Management, Incident Management, Security Assessment, Security Assessment, Vulnerability Assessment, Penetration Testing, Security Assessment, Secure Code Review, Security Assessment
Organization and Management	Organisational Structures, Information Security, Internal Controls, Independence

Common Criteria	Applicable Areas
Communications	ITA Description, Formal Documentation, Communication
Risk Management and Design and Implementation of Controls	Risk Management, Monitoring of Sub-Contractors, Audit, Transparency
Monitoring of Controls	Internal Controls
Logical and Physical Access Controls	Logical Access, Physical Access, Transmission of Information, Detection of Malicious Software
Change Management	Systems Development, Systems Maintenance, Change Management
Availability	Processing Capacity, Availability, Disaster Recovery
Processing Integrity	Error Handling, Processing Integrity, Modification of Data, Immutability
Confidentiality	Confidentiality, Access Control, Compliance, Awareness, Data Retention
Use, Retention, and Disposal of Personal Data	Personal Data, Data Retention
Access to Personal Data	Integrity of Data, Personal Data
Disclosure and Notification of Personal Data	Data Disclosure
Quality of Personal Data	Personal Data

The Systems Audit Report based on Control Objectives is intended to provide a framework that can be applied to variety of scenarios. The innovative technology environment may envisage ITAs that are part of an eco-system such that they may use, or be used, by other ITAs to deliver services. The Systems Audit effort and focus would vary according to circumstances within the framework.

10. Functional and Security Review Guidelines

The Auditee requesting a Systems Audit must submit to the Systems Auditor the relevant documentation, including a Blueprint, to provide a good understanding of the scope, functionality and capabilities of the system. Where the Auditee has previously registered a Whitepaper with the Lead Authority under the Virtual Financial Assets Act (Cap. 590) to fund the ITA, the Auditee is required to provide a copy of that Whitepaper to the Systems Auditor.

In line with Article 8 (4) (b) of the ITAS Act, the Systems Audit opinion shall provide reasonable assurance that the ITA is fit and proper for the purpose/s declared; and has the qualities, attributes, features, behaviours or aspects declared.

The Systems Auditor is responsible to cover the various Control Objectives that are part of the Systems Audit, including the aspect of security and functional testing. These tasks shall be performed by Subject Matter Experts specialised in the respective fields. The results in the form of an expert opinion would be considered and utilised by the Systems Auditor to support the Systems Audit opinion.

11. Revocation, cancellations or Suspension of a Systems Auditor

The Authority reserves the right to remove or suspend any Systems Auditor from the registered list in case of unsatisfactory performance or any breach of the obligations related to the Systems Auditor registration with the Authority. In line with Article 35 (1) of the MDIA Act, in case of revocation, cancellation or suspension, the Authority shall give the Systems Audit no less than twenty-five (25) days to show cause for the suspension or revocation of its approval not to take place. The Authority may revoke the registration with immediate effect, by written notice to the Systems Auditor, in the following cases:

- The Systems Auditor maliciously or due to gross negligence fails to report to the Authority serious failures on the part of one or more ITAs with respect to which the Systems Audit has carried out an Audit, provided that the Authority shall, at its sole discretion, determine what amounts to a serious failure on the part of a Systems Auditor.
- Three (3) or more reprimands are issued to the Systems Auditor for failure to carry out the Audits to the standard and with the diligence desired by the Authority.
- The Systems Audit fails to report a conflict of interest to the Authority.

PART B – Systems Audit Report Guidelines

Contents

Digital Innovation is, by definition, a rapidly evolving sector. These guidelines are expected to be updated to keep abreast with technology, regulatory and operational developments.

This is a supporting document to the "Systems Auditor Guidelines" as issued by the Malta Digital Innovation Authority.

1. Introduction

This document presents the form and structure of Audit Reports expected to be issued by Systems Auditors registered with the Malta Digital Innovation Authority, and should be read in conjunction with the 'Systems Auditor Guidelines' document.

The following are the five (5) Key Principles around a system on which the Audit will focus:

- Security;
- Processing Integrity;
- Availability;
- Confidentiality;
- Protection of Personal Data.

The Authority is directing Systems Auditors to follow ISAE 3000[1] reporting standard. This standard provides Systems Auditors with guidance on how to perform the work through recommended, generally acceptable and competent procedures. This standard:

- Allows for a single deliverable to address demands from the Lead Authority for increased transparency into the Auditee's operations;
- Builds trust and transparency with customer base;
- Reduces Systems Auditor procedures;
- Helps meet regulatory demands.

2. Type of Systems Audit Reports

There are two types of Systems Audit Reports which may be issued:

- **Type 1 reports:** The Systems Auditor expresses an opinion on whether the description of the ITA is fairly presented and whether the controls included in the description are suitably designed to meet the documented applicable criteria[2]. This type of audit is typically carried out when an Innovative Technology Arrangement is in the process of applying to be certified by the Authority; or when deemed necessary by the Authority, or other Lead Authority in Malta.

[1] https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga

[2] Applicable criteria form part of the following five (5) Key Principles: Security, Processing Integrity, Availability, Confidentiality and Protection of Personal Data.

- **Type 2 reports:** The Systems Auditor's report contains the same opinions expressed in a Type 1 report, but also includes an opinion on the operating 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 an ITA; or on the request of the Authority or other Lead Authority in Malta.

The Independent Systems Auditor's Opinion

The Systems Auditor will provide an opinion, based on the controls described by Management and the Control Objectives as set out by the Authority, that:

- The description fairly presents the ITA that was designed and implemented throughout the period (or "as of [date]" in the case of a Type 1);
- The controls stated in the description were suitably designed to provide reasonable assurance that the applicable Control Objectives would be met if the controls operated effectively throughout the period (or "as of [date]" in the case of a Type 1);
- The controls operated effectively to provide reasonable assurance that the applicable Control Objectives were met throughout the period (only in a Type 2).

3. Independence

The Systems Auditor needs to state within the Systems Audit Report that the Audit was conducted and concluded in-line with independence guidelines established by the ISAE 3000 standard and specific requirements set-out by the Authority in the 'Systems Auditor Guidelines'.

4. Systems Audit Report Contents

Auditee's Assertion

The Auditee is required to provide a written assertion and that assertion is required to be attached to Auditee's description. A written assertion should be provided by the Auditee and include whether in all material respects, and based on suitable criteria:

- The Auditee's description of the Innovative Technology Arrangement fairly presents the ITA that was designed and implemented throughout the period in the case of a Type 2 Report (or "as of [date]" for a Type 1 Report);

- The controls stated in the Auditee's description of the ITA were suitably designed throughout the specified period in the case of a Type 2 Report (or "as of [date]" for a Type 1 Report) to meet the applicable Control Objectives;
- In a Type 2 Report, the controls stated in the Auditee's description of the ITA operated effectively throughout the specified period to meet the applicable Control Objectives.

Innovative Technology Arrangement Description

The Auditee is responsible for preparing the ITA description, including the completeness, accuracy, and method of presentation of the description, and ensure that such description is in line with the 'Innovative Technology Arrangement Guidelines' issued by the Authority.

The description should clearly detail the services performed at the Auditee to enable the user of the Systems Audit Report to understand the structure and processes supported.

The depth of detail should enable the report user to identify risk areas where controls that address the specific control objectives in each category have been implemented by the Auditee.

Selection of the Applicable Categories and Control Objectives

Control Objectives are set out in the "Systems Audit Control Objectives" document issued by the Authority. From time to time, the 'Systems Audit Report Guidelines' and the 'Systems Audit Control Objectives' may be updated to cover additional areas as required by the Authority. The Auditee may identify Categories and Criteria set out in the Systems Audit Control Objectives that are not applicable to the particular ITA, however, the rationale for each exclusion needs to be explained and documented in the Systems Audit Report.

The Systems Audit Report must include a section identifying the Criteria that is covered by the Systems Auditor and the Subject Matter Experts who were responsible for the Audit of those criteria.

The Auditee is responsible for designing and implementing controls to achieve the applicable criteria, identifying the risks that threaten the achievement of the applicable criteria, and evaluating the linkage of the controls to the risks that threaten the achievement of the applicable criteria. In many cases, the Systems Auditor may be able to obtain the Auditee's documentation of its identification of risks and evaluation of the linkage of controls to those risks. In these instances, the Systems Auditor may evaluate the completeness and accuracy of the Auditee's

identification of risks and the effectiveness of the controls in mitigating those risks.

Description of a Control

A Systems Auditor should consider the following types of information when assessing the description of the control:

Relevant information when describing control	Example
The frequency with which the control is performed or the timing of the occurrence	The Auditee's management reviews error reports on a monthly basis. On a daily basis, a departmental clerk reviews reconciling items identified in the comparison of the ABC report with the data feed from user entities.
The party responsible for performing the control	The security manager reviews... An input processing clerk compares...
The nature of the activity that is performed	The system compares the name of the user entity employee requesting access to the system with approved user information submitted by authorized user entity personnel.
The subject matter to which the control is applied	Program changes are reviewed by ...

Presentation of Tests of Controls in Type 1 and Type 2 Reports

The description of procedures performed identifies the Controls that were tested, whether the items tested represent all or a sample of the items in the population, and the nature of the tests performed in sufficient detail to enable Systems Audit Report users to determine the effect of such tests on user's risk assessments.

Control Activities Specified by *ABC Company*	SA's Test of Operating Effectiveness	Test Results
Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.		
1) Access to systems is provided based on user's assigned roles and responsibilities. Documented authorization from appropriate management is required prior to adding access to systems.	Extracted a system-generated list from the platform showing all the users and the respective account creation date (to determine the population of user accounts that were created in the period under review). Inspected the authorization for a sample of user access requests (retained in a centralized ticketing management system) to determine whether access was authorized by management prior to granting the user access to the system.	No Exceptions Noted
2) User access rights, privileges, functions, entitlements, roles and/or profiles within a system, database, or application are removed or disabled when notified by HR that a user has been terminated.	Extracted a system-generated list from the Human Resource system showing all individuals that terminated employment during the period under review. Inspected the listing of terminated employees and the platform user listing to determine whether the terminated employees' access to the system was removed upon termination.	No Exceptions Noted.

Results of Tests in Type 1 and Type 2 Reports

If exceptions have been identified, the description of the extent of testing performed would include the number of items tested and the number and nature of the exceptions noted, even if, on the basis of tests performed, the Systems Auditor concludes that the applicable Control Objectives were still met.

Control Activities Specified by ABC Company	SA's Test of Operating Effectiveness	Test Results
Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to them.		
1) Access to systems is provided based on user's assigned roles and responsibilities. Documented authorization from appropriate management is required prior to adding access to systems.	Inspected the authorization for a sample of user access requests to determine whether access was authorized by management prior to granting the user access to the system.	For 2 of the 25 user access requests inspected, due to a system outage, authorization for the access granted was not maintained.

If the Systems Auditor chooses to also report exceptions and include the Auditee's responses to the exceptions in a separate section, the following points should be considered:

- Auditor's responsibilities (beyond inquiry) for reviewing and testing the Auditee's response(s);
- Workpapers should include documentation of the testing performed.

Other Information Provided by the Auditee (Unaudited)

An Auditee may decide to provide Systems Audit Report users with information other than the information required to be in the description of the Control and will not be covered by the Systems Audit Report.

For example, the Auditee may be in the process of making changes to the System that will be implemented after the end of the period or the Auditee may want to describe remediation activities for identified deficiencies. This provides an opportunity for the Auditee to respond to deviations identified by the Systems

Auditor when such responses have not been subject to the procedures by the Systems Auditor.

If such other information is presented in an attachment to the description of the Control, the other information should be differentiated from the information covered by the Systems Audit Report.

When other information that is not covered by the Systems Audit Report is attached to the description, the System Auditor should read the other information to identify any material inconsistencies between the other information and the description of the ITA, Auditee's assertion, or the Systems Audit Report.

If other information is included, this should be included as an appendix to the Systems Audit Report and the Systems Auditor's opinion should be modified to include the reference to the other information.

Other Reporting Considerations: subsequent events and subsequently discovered facts

Subsequent events are those events that occur after the "period end date" and prior to the issuance of the Systems Audit Report. For example, if the "period end date" is December 31, 2018 and the Systems Audit Report issuance date is March 1, 2019, an event that occurred on February 15, 2019 that affected the Systems Audit Report would be considered a subsequent event.

The Auditee may wish to disclose such events in a separate section of the description of the Auditee's system; the disclosure may be titled, for example, "Other Information Provided by the Auditee (Unaudited)." In a format similar to the description, this section will describe what has occurred since the period end date.

Verification of Source Files and Systems Audit Report

Systems Audit Reports are to be issued in the English language. Systems Audit Reports may be submitted to the Authority on various media accepted by the Authority. The Systems Auditor must ensure the integrity of the Systems Audit Report in a manner appropriate to the media used. For example, in the case of electronic media, digitally signed files or documented hashes based on forensically-sound hashing algorithms may be used and the Systems Auditor must provide sufficient documentation to enable the Authority to verify the integrity of the electronic content submitted.

Similarly, it is expected that the Systems Auditor will use hashes or similar mechanisms to identify the version of systems being audited to be able to verify the integrity and the authenticity of the system reviewed subsequent to the Audit, for example, executable files; policy documents; source code files; and configuration files.

5. Role of Auditee's Sub-Contractors

In the context of this document, a Sub-Contractor is an individual or legal organisation that provides services to the Auditee.

An Auditee may interact with Sub-Contractors in the operation of its platform. Vendors should be evaluated to determine if they are considered Sub-Contractors. The Auditee should determine whether controls over the functions performed by an organization from which it has contracted services (the vendor) are needed to meet one or more of the Control Objectives or are otherwise relevant to the fair presentation of the description of the ITA.

If the services provided by the vendor are likely to be relevant to the Systems Audit Report user's understanding of the services provided by the Auditee as it relates to the categories included and the Auditee is relying on controls at the vendor to meet one or more of the applicable criteria, the vendor shall be considered a Sub-Contractor. The Auditee's description of its system should include a description of the role of Sub-Contractors and the Systems Auditor should perform the following steps:

- Identify the Auditee's controls that monitor the services provided by the Sub-Contractor;
- Develop an approach to assess the Auditee's monitoring controls;
- Determine presentation method of such an approach to monitor the controls.

If the vendor is determined not to affect the Auditee's system then the Auditee does not need to treat the vendor as a Sub-Contractor and may omit any description of controls at the vendor.

6. Responsibility of the Auditee

The Auditee should identify the risks that would prevent the Control Objectives from being met for the proposed ITA in the following areas:

- Products and services provided by the ITA;
- Components of the ITA used to provide the products and services;

- Environment in which the ITA operates;
- Commitments the Auditee has made to users of the ITA and parties affected by the ITA;
- ITA requirements that derive from:
    - Laws and regulations affecting how the ITA functions and products and services are provided; and
    - Business objectives of the Auditee.

The Auditee is responsible for:

- Determining the type of Audit to be performed (Type 1 or Type 2), in accordance with the requirements set out by the Authority or respective Lead Authority;
- Determining the scope of the engagement/boundaries of the system.
    - This includes:
        - The services, business units, functional areas, and activities or applications that will be of interest to users;
        - The applicable criteria that will be covered by the Systems Audit Report. This is determined based on the needs of the Systems Audit Report users;
        - The period to be covered by the description and Systems Audit Report;
        - Whether any Auditee's sub-contractors will be included in, or carved out of, the Systems Audit Report.
- Preparing a description of the ITA, including the provision of the necessary Blueprint (or equivalent) which highlights the functionality of the ITA;
- Providing a written assertion in which the Auditee confirms, to the best of its knowledge, that:
    - The ITA description is fairly presented as implemented throughout period;
    - Controls were suitably designed throughout the specified period to meet the Control Objectives;
    - Controls operated effectively throughout the reporting period (Type 2 Report only);
    - Having a reasonable basis for its assertions through monitoring or other procedures.

7. Systems Audit Report Signatures

The Systems Audit report must be signed by the Systems Auditor. In addition, Subject Matter Experts involved in the Systems Audit will sign the Systems Audit Report indicating the respective areas covered.

In the case where a Systems Auditor is a legal organisation, the authorised representative shall sign the Systems Audit Report, stating his/her name and position in the legal organisation.

8. Conclusion

Systems Auditors should comply with all the ISAE 3000 requirements and be familiar and understand the Control Objectives presented in guidelines issued by the Malta Digital Innovation Authority. The Systems Audit Report should follow the form and detail as specified in the ISAE 3000 standard from paragraph A161 onwards (ref: Appendix 1).

Appendix 1: Assurance Report Content

Title

- A161

Addressee

- A162

Subject Matter Information and Underlying Subject Matter

- A163

Applicable Criteria

- A164

Inherent Limitations

- A165

Specific Purpose

- A166
- A167

Relative Responsibilities

- A168
- A169
- A170

Applicable Quality Control Requirements

- A171

Compliance with Independence and Other Ethical Requirements

- A172

Summary of the Work Performed

- A173
- A174
- A175
- A176
- A177

The Practitioner's Conclusion

- A178
- A179
- A180 A181
- A182

The Practitioner's Signature

- A183

Date

- A184

Systems Audit Control Objectives

Systems Audit Categories	Definition
IVFAO	As defined in Article 2(2) of the Virtual Financial Assets Act (Cap. 590), an “Initial Virtual Financial Asset Offering”, also referred to as “IVFAO” within this document, means a method of raising funds whereby an issuer is issuing Virtual Financial Assets (VFA) and is offering them in exchange for funds.
DLT Platforms	As defined in Article 2(1) of the Malta Digital Innovation Authority Act (2018), "DLT", "distributed ledger technology", "decentralised ledger technology" means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof, as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, 2018, and the term "node" means a device and data point on a computer network;
Smart Contracts	As defined in Article 2(1) of the Malta Digital Innovation Authority Act (2018), a “Smart Contract” means a form of innovative technology arrangement consisting of: (a) a computer protocol; and, or (b) an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both;

Ref #	Applicable Areas	Systems Audit Control Objectives	Systems Audit Categories		
			IVFAO	DLT Platforms	Smart Contracts
Common Criteria Related to Functionality and Compliance with Regulatory Requirements					
1	Functionality Code Review	The functionality, as confirmed through a Code Review, testing and/or any other required procedures, is in line with the Blueprint (or equivalent) submitted to the Lead Authority.	✓	✓	✓
2	Platform Implementation	Depending on the Systems Audit Category, the Auditee has taken the necessary measures to implement the platform in line with the Blueprint (or equivalent) submitted to the Lead Authority. *Note: As an example, the equivalent of the Blueprint in the case of an IFVAO is the Whitepaper submitted to the Lead Authority. In this regard, refer to the 'IVFAO - Whitepaper Requirements' (attached as Appendix 1 to this document) for reference to the specific Whitepaper requirements the Systems Auditor is expected to cover as part of this Control Objective.*	✓	✓	✓
3	Forensic Node	The Auditee implements a Forensic Node hosted in Malta that is available 24/7 logging all transactions being relevant to the ITA.	✓	✓	✓
Common Criteria Related to System Operations					
4	Vulnerabilities Management	Vulnerabilities of system components to security, availability, processing integrity, confidentiality and protection of personal data breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
5	Incident Management	Security, availability, processing integrity, confidentiality and protection of personal data incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the Auditee's commitments and system requirements.	✓	✓	✓
6	Security Assessment	A security assessment is scoped and undertaken to make sure the best possible level of security by the test is achieved to both the legacy as well as emerging threats to the ITA itself.	✓	✓	✓
7	Security Assessment, Vulnerability Assessment, Penetration Testing	A security testing exercise (including a vulnerability assessment and a penetration test) should be undertaken on the system by a CREST certified security assessor or a similar recognition as approved by the Authority.		✓	✓
8	Security Assessment, Secure Code Review	For any application developed (including smart contracts), a secure code review exercise should be undertaken by a CREST certified security professional, in line with the OWASP Secure Coding Practices guide.	✓	✓	✓
9	Security Assessment	Any security reporting should be presented inline with the SANS Penetration Testing Reporting guidelines.	✓	✓	✓
Common Criteria Related to Organization and Management					
10	Organisational Structures	The Auditee has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
11	Organisational Structures	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the Auditee's system controls and other risk mitigation strategies are assigned to individuals within the Auditee with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓

Ref #	Applicable Areas	Systems Audit Control Objectives	Systems Audit Categories		
			IVFAO	DLT Platforms	Smart Contracts
12	Organisational Structures	The Auditee has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security, availability, processing integrity, confidentiality and protection of personal data and provides resources necessary for personnel to fulfil their responsibilities.	✓	✓	✓
13	Organisational Structures	The Auditee has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
14	Information Security	The Auditee has adequate information security structures in place, including documentation, awareness as well as re-active measures to handle security incidents.	✓	✓	✓
15	Organisational Structures	The Auditee has implemented governance structures and management procedures in line with the information provided in the Blueprint (or equivalent) submitted to the Lead Authority.	✓	✓	✓
16	Internal Control	The Auditee's internal control systems, produced and operational artefacts and the handling of sensitive information should be undertaken in-line with International Standards.	✓	✓	✓
17	Independence	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	✓	✓	✓
Common Criteria Related to Communications					
18	ITA Description, Formal Documentation	Information regarding the design and operation of the system and its boundaries (possibly through logical and physical architecture diagrams, design documentation, API documentation, etc.) has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	✓	✓	✓
19	ITA Description, Communication	Commitments are communicated to external users, as appropriate, and the commitments and related requirements are communicated to internal system users to enable them to carry out their responsibilities.	✓	✓	✓
20	ITA Description, Communication	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	✓	✓	✓
21	ITA Description, Communication	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, processing integrity, confidentiality and protection of personal data of the system, is provided to personnel to carry out their responsibilities.	✓	✓	✓
22	ITA Description, Communication	Internal and external users have been provided with information on how to report security, availability, processing integrity, confidentiality and protection of personal data failures, incidents, concerns, and other complaints to appropriate personnel.	✓	✓	✓
23	ITA Description, Communication	System changes that affect internal and external users' responsibilities or the Auditee's commitments and system requirements relevant to security, availability, processing integrity, confidentiality and protection of personal data are communicated to those users in a timely manner.	✓	✓	✓
24	ITA Description, Communication	All communications should be made available in English.	✓	✓	✓
25	ITA Description, Communication	Any restrictions of use of the system should be made available to the user upon accessing the main login pages of the system.	✓	✓	✓

Ref #	Applicable Areas	Systems Audit Control Objectives	Systems Audit Categories		
			IVFAO	DLT Platforms	Smart Contracts
Common Criteria Related to Risk Management and Design and Implementation of Controls					
26	Risk Management	The Auditee (1) identifies potential threats that could impair system security, availability, processing integrity, confidentiality and protection of personal data commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyses the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	✓	✓	✓
27	Risk Management	The Auditee designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	✓	✓	✓
28	Monitoring of Sub-Contractors	Any 3rd party sub-contractors involved in the development, up keeping and maintenance of the system must be documented and the relevant authority informed.	✓	✓	✓
29	Audit, Transparency	The Auditee has adequate auditability characteristics in place to facilitate the unique identification of transaction and the inter-linking between them.	✓	✓	✓
Common Criteria Related to Monitoring of Controls					
30	Internal Controls	The design and operating effectiveness of controls are periodically evaluated against the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	✓	✓	✓
Common Criteria Related to Logical and Physical Access Controls					
31	Logical Access	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.		✓	
32	Logical Access	New internal and external users, whose access is administered by the Auditee, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data. For those users whose access is administered by the Auditee, user system credentials are removed when user access is no longer authorized.		✓	
33	Logical Access	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.		✓	✓

Ref #	Applicable Areas	Systems Audit Control Objectives	Systems Audit Categories		
			IVFAO	DLT Platforms	Smart Contracts
34	Logical Access	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.		✓	✓
35	Physical Access	Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
36	Logical Access	Logical access security measures have been implemented to protect against security, availability, processing integrity confidentiality, or protection of personal data threats from sources outside the boundaries of the system to meet the Auditee's commitments and system requirements.		✓	
37	Transmission of Information	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the Auditee to meet its commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
38	Detecion of Malicious Software	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.		✓	✓
		Common Criteria Related to Change Management			
39	Systems Development	The Auditee's commitments and system requirements, as they relate to security, availability, processing integrity, confidentiality and protection of personal data, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	✓	✓	✓
40	Systems Maintenance	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
41	Change Management	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the Auditee's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality and protection of personal data.	✓	✓	✓
42	Change Management	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the Auditee's security, availability, processing integrity, confidentiality and protection of personal data commitments and system requirements.	✓	✓	✓
		Additional Criteria for Availability			
43	Processing Capacity	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the Auditee's availability commitments and system requirements.	✓	✓	✓
44	Availability	Environmental protections, software, data backup processes, and recovery infrastructure are authorized designed, developed, implemented, operated, approved, maintained, and monitored to meet the Auditee's availability commitments and system requirements.	✓	✓	✓

Ref #	Applicable Areas	Systems Audit Control Objectives	Systems Audit Categories		
			IVFAO	DLT Platforms	Smart Contracts
45	Disaster Recovery	Recovery plan procedures supporting system recovery are tested to help meet the Auditee's availability commitments and system requirements.	✓	✓	✓
Additional Criteria for Processing Integrity					
46	Error Handling	Procedures exist to prevent, or detect and correct processing errors to meet the Auditee's processing integrity commitments and system requirements.		✓	✓
47	Processing Integrity	System inputs are measured and recorded completely, accurately, and timely to meet the Auditee's processing integrity commitments and system requirements.		✓	✓
48	Processing Integrity	Data is processed completely, accurately, and timely as authorized to meet the Auditee's processing integrity commitments and system requirements.	✓	✓	✓
49	Processing Integrity	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the Auditee's processing integrity commitments and system requirements.	✓	✓	✓
50	Processing Integrity	System output is complete, accurate, distributed, and retained to meet the Auditee's processing integrity commitments and system requirements.	✓	✓	✓
51	Modification of Data	Modification of data, other than routine transaction processing is authorized and processed to meet with the Auditee's processing integrity commitments and system requirements.	✓	✓	✓
52	Immutability	Data stored after a consensus mechanisms was triggered with successful results is immutable.	✓	✓	✓
Additional Criteria for Confidentiality					
53	Confidentiality	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the Auditee's confidentiality commitments and system requirements.	✓	✓	✓
54	Confidentiality	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the Auditee's confidentiality commitments and system requirements.	✓	✓	✓
55	Access Control	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the Auditee's confidentiality commitments and system requirements.	✓	✓	
56	Confidentiality	The Auditee obtains confidentiality commitments that are consistent with the Auditee's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	✓	✓	
57	Compliance	Compliance with the Auditee's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.	✓	✓	
58	Awareness	Changes to the Auditee's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	✓	✓	
59	Confidentiality	The Auditee retains confidential information to meet the Auditee's confidentiality commitments and system requirements.	✓	✓	
60	Data Retention	The Auditee disposes of confidential information to meet the Auditee's confidentiality commitments and system requirements.	✓	✓	
Protection of Personal Data Criteria Related to Use, Retention, and Disposal					
61	Personal Data	The Auditee retains personal data consistent with the Auditee's objectives related to protection of personal data.	✓	✓	
62	Data Retention	The Auditee securely disposes of personal data to meet the Auditee's objectives related to protection of personal data.	✓	✓	

Ref #	Applicable Areas	Systems Audit Control Objectives	Systems Audit Categories		
			IVFAO	DLT Platforms	Smart Contracts
Protection of Personal Data Criteria Related to Access					
63	Integrity of Data	The Auditee is able to correct, amend, or append personal data based on information provided by data subjects to meet the Auditee's objectives related to protection of personal data.	✓	✓	
64	Personal Data	The Auditee is able to restrict processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data.	✓	✓	✓
Protection of Personal Data Criteria Related to Disclosure and Notification					
65	Data Disclosure	The Auditee is able to restrict processing (such as viewing; editing; inserting; copying, deleting) to personal data to person or groups of persons necessarily authorised to process such data.	✓	✓	✓
66	Data Disclosure	The Auditee retains a complete, accurate, and timely record of processing of personal data including a record of users performing the processing and the results of the processing.	✓	✓	
Protection of Personal Data Criteria Related to Quality					
67	Personal Data	The Auditee collects and maintains accurate, up-to-date, complete, and relevant personal data to meet the Auditee's objectives related to protection of personal data through secure processing measures.	✓	✓	

VFA Act, First Schedule, Paragraph 7

Section	Requirement	Applicable to Systems Auditor
(a)	description of the reason behind the initial virtual financial asset offering	
(b)	detailed technical description of the protocol, platform and, or application, as the case may be, and the associated benefits	✓
(c)	detailed description of the sustainability and scalability of the proposed project	
(d)	associated challenges and risks as well as mitigating measures thereof	✓
(e)	detailed description of the characteristics and functionality of the virtual financial assets being offered	✓
(f)	detailed description of the issuer, VFA agent, development team, advisors and any other service providers that may be deployed for the realisation of the project	
(g)	detailed description of the issuer's wallet/s used	✓
(h)	description of the security safeguards against cyber threats to the underlying protocol, to any off-chain activities and to any wallets used by the issuer	✓
(i)	detailed description of the life cycle of the initial virtual financial asset offering and the proposed project	
(j)	detailed description of the past and future milestones and project financing	
(k)	detailed description of the targeted investor base	
(l)	change rate of the virtual financial assets	
(m)	description of the underlying protocol's interoperability with other protocols	✓
(n)	description of the manner funds raised through the initial virtual financial asset offering will be allocated	
(o)	the amount and purpose of the issue	
(p)	the total number of virtual financial assets to be issued and their features	✓
(q)	the distribution of virtual financial assets	
(r)	the consensus algorithm, where applicable	✓
(s)	incentive mechanism to secure any transactions, transaction and/or any other applicable fees	
(t)	in the case of a new protocol, the estimated speed of transactions	✓
(u)	any applicable taxes	
(v)	any set soft cap and hard cap for the offering	*
(w)	the period during which the offer is open	*
(x)	any person underwriting or guaranteeing the offer	
(y)	any restrictions on the free transferability of the virtual financial assets being offered and the DLT exchange/s on which they may be traded, to the extent known by the issuer	✓
(z)	methods of payment	
(aa)	specific notice that investors participating in the initial virtual financial asset offering will be able to get their contribution back if the soft cap is not reached at the end of the offering and detailed description of the refund mechanism, including the expected time-line of when such refund will be completed	*
(ab)	detailed description of the risks associated with the virtual financial assets and the investment therein	✓
(ac)	the procedure for the exercise of any right of pre-emption	
(ad)	detailed description of the smart contract/s, if any, deployed including inter alia the adopted standards, its/their underlying protocol/s, functionality/-ies and associated operational costs	✓
(ae)	any smart contract/s is/are deployed by the issuer, details of the auditor who performed an audit on it/them	
(af)	description of any restrictions embedded in the smart contract/s deployed, if any, including inter alia any investment and/or geographical restrictions	✓
(ag)	the programme agents used to obtain data and verify occurrences from smart contracts (also known as 'oracles') used and detailed description of their characteristics and functionality thereof	✓
(ah)	bonuses applicable to early investors including inter alia discounted purchase price for virtual financial assets	
(ai)	the period during which voluntary withdrawals are permitted by the smart contract, if any	✓

Section	Requirement	Applicable to Systems Auditor
(aj)	description of the issuer's adopted white-listing and anti-money laundering and counter financing of terrorism procedures in terms of the Prevention of Money Laundering Act and any regulations made and rules issued thereunder	
(ak)	intellectual property rights associated with the offering and protection thereof	
(al)	the methods of and time-limits for delivery of the virtual financial assets	*

(*) Where the characteristics indicated are enforced in the code of the underlying ITA, such areas will fall under the scope of the Systems Audit as per Requirement (b) above.

MDIA

Malta Digital Innovation Authority

mdia.gov.mt