Chapter 01

Part A

Systems Auditor Guidelines

MDIA
Malta Digital Innovation Authority

view changes in this version (2)

PART A - Systems Auditor Guidelines

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.

Document Version: 30 July 2019

Contents

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 an owner or controller of an ITA ('ITA Owner'), 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').

"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 the 'Innovative Technology Arrangements Guidelines'.

"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.

"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.

"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.

"Register of Recognitions" is an electronic register, also referred to as "the Register", of all recognitions issued by the Authority, which recognitions shall include the certification of ITAs, and registration of Systems Auditors and s. The Register shall include all such details as the Authority shall consider necessary to identify the relevant Applicant and the activities being carried out. In addition, the Register shall be available to the public on the website of the Authority.

"Resident Agent" refers to the Resident Agent as defined in Article 15 of the Innovative Technology Arrangements and Services Act, and in line with further guidance issued by the Authority within the 'Resident Agent Guidelines'.

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

2. Systems Auditor Role

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 within 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 Reasonable Assurance 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 conduct an audit following the ISAE 3000 standard[2]. In line with Article 9(7) of the ITAS Act, 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

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

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

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, which may be held through remote means at the discretion of the Authority, 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 Reasonable Assurance 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.

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

A Systems Auditor needs to meet the requirements set by the Authority, as documented in the *Guidelines on the definition of 'in or from Malta'*.

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);
- 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 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. The Authority will ensure that this is done in a consistent and equitable manner.

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 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

[3] http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/
[4] In these guidelines, one year of experience is considered to be at least 50% of one year's equivalent of full time employment.

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.

In line with Article 15 of the ITAS Act, an Applicant that is not habitually 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.

In line with Article 15(2) of the ITAS Act, a legal organisation shall not be deemed habitually resident in Malta if none of the following are habitually resident in Malta:

- the members of its board of administrators or secretary; and
- appointed senior officers, being the Chief Executive Officer, the Chief Operations Officer, or the Chief Technology Officer.

Additional guidelines to determine when ITAs will require an enhanced systems audit, the corresponding requirements of such an audit and the eligibility criteria of the Systems Auditor to perform such an audit, will be issued by the Authority at a later stage.

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 above).

5. Subject Matter Experts

Subject Matter Experts identified in the Systems Auditor application must be bound by a contract and submit proof of the appointment with the Systems Auditor at the time of application. Such contracts may need to be disclosed to the Authority for review. The Subject Matter Expert must also include his/her CV and the subject matter expertise within the Systems Auditor Application Form.

The Subject Matter Experts do not have an obligation to be resident in Malta.

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.

6. Security Testing

The Subject Matter Experts responsible for Security Testing is expected to hold a certification in information security assessment (e.g. OSCP or SANS/GIAC GPEN Penetration Tester) or accreditation (e.g. CREST).

Security tests performed should be based on a documented risk assessment and will be likely to include an assessment of the security within the system design and the code (e.g. following the OWASP Secure Coding Principles).

The results of the security testing should be reported in a structured form promoted by recognised industry bodies (for example the SANS Institute 'Writing a Penetration Testing Report', NIST SP 800-115 or Open Source Security Testing Methodology Manual (OSSTMM)).

Security tests should be documented in line with 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 *Secure Coding Practices Quick Reference Guide* is a technology agnostic set of general software security coding practices, in a comprehensive checklist format, that can be integrated into the development lifecycle. 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,

[5] http://cve.mitre.org/about/faqs.html
[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

summary of findings and recommendations as well as a detailed description of each vulnerability identified including its recommended patching.

7. Independence of the Systems Auditor

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

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 Systems Audit team begins to perform audit services. The engagement period ends when the Systems 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 Systems Audit Report.

For the purposes of the Systems Auditor engagement for a Systems Audit, consultancy work related to the architectural design, security and implementation of the ITA (including its whitepaper, blueprint and other documentation) provided to the Auditee 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 not to be independent.

8. Systems Auditor Engagement

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

- Submit a statement informing the Authority of the appointment by the Auditee to act as its Systems Auditor. Once the Systems Auditor appointment is approved by the Authority, the audit can start;
- Submit a statement to the Authority confirming that the Systems Auditor and any Subject Matter Experts involved in the Systems Audit are independent (refer to Section 7);
- 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;
- Carry out the audit;
- Submit the final Systems Audit Report to the client as well as to the Authority, along with the respective fee.

The ITA is required to provide the Systems Auditor with all information, explanations, documentation and resources necessary to perform the audit.

A Systems Auditor is required to cover all Control Objectives as defined by the Authority – refer to Section 10 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. The Authority shall publish any updates of the System Audit Report Guidelines or System Audit Control Objectives in advance and will inform the Systems Auditors listed in the Register of Recognition.

9. Systems Audit Reports

The 'Systems Audit Report Guidelines' published by the Authority provides guidance on the content, format and objectives of the Reasonable Assurance 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. The Subject Matter Experts will declare the areas that each expert was responsible for and sign for such area. 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.

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 adequate engagement documentation to support the backing of tests and conclusions drawn from the tests performed, for a period of not less than five (5) years from the date of the Systems Audit Report.

10. 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.
- **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

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

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'. These Systems Audit Control Objectives are applicable if the ITA is backed up by a legal organization. If it is governed by an ITA itself, the Authority may vary the requirements as applicable.

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, Vulnerability Assessment, Penetration Testing, Secure Code Review
Organization and Management	Organisational Structures, Information Security, Internal Controls, Independence
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

Common Criteria	Applicable Areas
Access to Personal Data	Integrity of Data, Personal Data
Disclosure and Notification of Personal Data	Data Disclosure
Quality of Personal Data	Personal Data

The Reasonable Assurance Systems Audit Report based on the 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.

11. 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 within the Virtual Financial Assets Act (Cap. 590) in relation to the ITA, the Auditee is required to provide a copy of that Whitepaper to the Systems Auditor and the Systems Audit report if any.

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 within the ITA Application Form and the ITA Blueprint; and has all 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.

The Systems Auditor is responsible to confirm the powers and features of intervention by the Technical Administrator, or the Authority, documented within the Blueprint, should an intervention be required.

12. 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 Auditor 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 Auditor fails to report an issue relating to independence to the Authority.

13. Fee Structure

For details pertaining to the fee structure please refer to the 'Legal Notice 355 of 2018'.

14. Enhanced Systems Auditor

The objectives and description of the 'Enhanced Systems Auditor' are documented in separate guidelines titled as 'Enhanced Systems Audit/or Guidelines'.

Form related to 'Enhanced Systems Auditor' can also be found in the application form section on the website of MDIA. New applicants must apply as a 'Systems Auditor' and indicate whether they would like to be considered as 'Enhanced Systems Auditor' (and therefore meeting the requirements of ESAs) in the relevant section of the form.

Applicants who are certified 'Systems Auditor' with MDIA and wish to upgrade and be considered as an Enhanced Systems Auditor need to fill in the 'Notification to Upgrade to Enhanced Systems Auditor Application Form'.