Enhanced Systems Audit/or Guidelines

MDIA

Malta Digital Innovation Authority

Enhanced Systems Audit/or 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.

Contents

1. Definitions

“Applicant”, within the context of this document, refers to an individual and/or legal organisation applying for Certification of an Innovative Technology Arrangement (ITA) with the Authority.

“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 Chapter 2 of the MDIA Guidance Notes.

“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.

“Systems Auditor” (‘SA’) as defined in the Innovative Technology Arrangements and Services Act, 2018.

“Technical Administrator” (‘TA’) as defined in the Innovative Technology Arrangements and Services Act, 2018, and in line with further guidance issued by the Authority under Chapter 3 of the Guidance Notes.

2. Introduction and Summary

The MDIA provides voluntary certification of Innovative Technology Arrangements ensuring that they behave and have the qualities identified in their Blueprint. The latter is used by the Systems Auditor to understand and verify the implementation. The current approach is to address all Innovative Technology Arrangements with the same form of scrutiny, and it is up to the Systems Auditor to apply an appropriate degree of scrutiny in its evaluation.

The aim of this document is to define the notion of an Enhanced Systems Audit (ESA), which is obligatory for ITAs that are either deemed to be safety-critical, or operate in a domain for which the relevant Lead Authority requires additional security. The document identifies which ITAs will require an Enhanced Systems Audit, who can perform an audit, and what additional requirements are placed on the Applicant and the Systems Auditor when applying for certification of such ITAs with the MDIA.

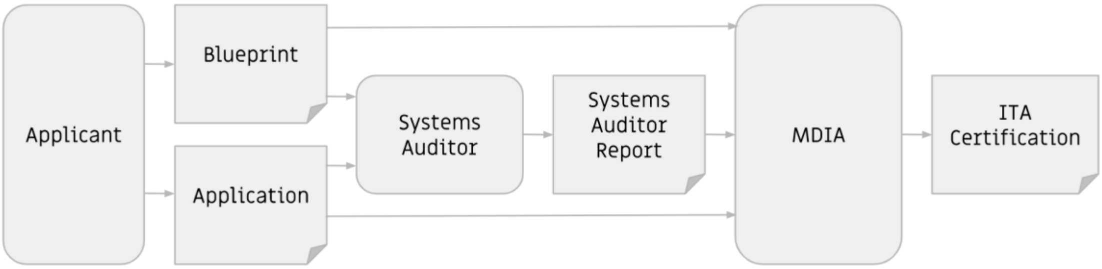
3. Rationale for Providing Enhanced Systems Audit

The Innovative Technology Arrangements and Services (ITAS) Act 2018 sets out how voluntary certification of ITAs is provided by the MDIA addressing the behaviour, qualities and attributes of the ITA as identified in MDIA guidelines. An opinion by a Systems Auditor recognized by the Authority is required for the issuing of the Certification, which opinion is based on an analysis of the ITA and its Blueprint as submitted by the ITA applicant, confirming that the ITA in question:

(i) conforms to the functionality or qualities as claimed in the Blueprint;

(ii) includes provisions for all legal requirements under the ITAS Act, including the setting up of a Forensic Node and additional functionality given to the Technical Administrator, including power to intervene in case the ITA’s behaviour results in material loss to any user or breach of law.

The process of ITA certification by the MDIA is shown in the figure below.



As specified in the MDIA ITA Blueprint Guidelines, upon an ITA's application, the submitted Blueprint must provide sufficient detail covering the ITA's:

(i) purposes (reasons for which it was created);
(ii) qualities (the characteristics offered to its users);
(iii) aspects (elements that are subject to the certification);
(iv) features (distinctive functional capabilities of the ITA);
(v) attributes (capabilities of the ITA);
(vi) behaviours (how it responds to unexpected processes and inputs); and
(vii) limitations (technical or operational restrictions).

The Blueprint thus provides documented claims regarding both the ITA's normal behaviour (the business-logic of the ITA), and measures taken to ensure that exceptional behaviour (internal or environmental) is handled appropriately.

Regarding Systems Auditors, the MDIA set out the requirements for this role in the Systems Auditors Guidelines (Chapter 01, Part A) which are in line with Article 9 of the ITAS Act. Requirements include prior experience in carrying out similar audits, subject area expertise, and experience (including the applicable laws, standards, regulations and technology).

Furthermore, a Systems Auditor is required to be covered by a Professional Indemnity Insurance (PII) policy for an amount of not less than €1,000,000, and unless habitually resident in Malta, is required to appoint a Resident Agent. Systems Auditors are only recognized after applying with the Authority and being accepted.

Currently, the Authority has two types of Systems Audits, depending solely on whether the ITA is a new one or one which has already been in production. Type 1 is performed upon application of a new ITA, in which the Systems Auditor expresses an opinion as to 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, while Type 2 is carried out periodically during the operational lifetime of an ITA and also includes an opinion on the operating effectiveness of the controls during the period covered by the audit.

It is worth noting that the Authority currently has a single approach to technological due diligence. The requirements on an ITA’s Blueprint, the requirements on the Systems Auditors who can assess the ITA, and the type of Systems Audit, are identical, whether the ITA is a small scale information storage system, or one which operates in a high-risk licensable domain.

There lies the need for requiring a higher level of technological due diligence for ITAs with a higher degree of risk associated – ensuring additional safeguards to add trust and confidence in ITAs which involve higher risk, whether it is because:

(i) they operate in a more heavily regulated area; or
(ii) because they carry out tasks which can pose a threat to human life and/or vital societal elements.

4. Enhanced Systems Audits for High-Risk Innovative Technology Arrangements

Certain ITAs will be required to follow an Enhanced Systems Audit (ESA). In this section the following are identified:

a. which ITAs will require an ESA for certification;
b. what the additional requirements are for an ESA with respect to a normal Systems Audit; and
c. who is eligible to perform an ESA.

a. ITAs requiring an ESA

The need for an Enhanced Systems Audit arises when the ITA is deemed to be high-risk, i.e. when:

(i) the ITA carries out tasks which may impact human life in a direct or indirect manner; or
(ii) another Lead Authority deems that the particular application area, class or category of the ITA may require additional scrutiny.

A new ITA will require an Enhanced Systems Audit (ESA) when either or both of the following hold:

1. the ITA is considered to be safety-critical; or

2. the activity of the ITA is regulated by another Lead Authority, and falls under an area, class or category which the Authority has identified to require enhanced scrutiny through an ESA.

Safety-critical systems are defined to be ones which may have an adverse affect on human life or health in a direct manner, or in an indirect manner through critical infrastructures.

An ITA is considered to be safety-critical if through its normal behaviour, its failure or irregularity in its functionality, and operations, poses either:

1. a direct health or safety risk for people; or
2. an indirect one by having an adverse effect on a critical infrastructure.

An infrastructure is considered critical if damage to such an infrastructure, its destruction, or disruption, may have a significant negative impact for the security of the country and the well-being of its citizens, which could result in loss of life, casualties and/or other health risks.

In cases where the ITA Applicant requests a normal Systems Audit, but the Systems Auditor appointed are of the opinion that an ESA is required due to the nature of the ITA, they are obliged to notify the Authority of this fact and include the rationale behind their opinion in their report.

b. Additional requirements for an ESA

If an ITA is deemed to require an ESA, there are additional requirements on:

(i) the Blueprint submitted by the ITA Applicant;

(ii) who can give an opinion on the Blueprint; and

(iii) the Systems Audit Report submitted by the Systems Auditor.

Every ITA applying for certification with MDIA must declare whether it requires an ESA. If it declares otherwise and the Systems Auditor is of the opinion that an ESA is required due to the nature of the ITA, the Systems Auditor is responsible for notifying the Authority promptly.

ITAs which declare that they require an ESA must also take into consideration the following requirements:

1. The Blueprint must, in addition to the requirements set out in the MDIA's ITA Blueprint Guidelines, include a risk assessment and mitigation plans appropriate for the risks of the particular ITA. Risks identified should be addressed in the blueprint through:

   a. an ongoing audit plan for Type 2 audits setting out what will be audited and with which frequency; and
   b. additional requirements on the Forensic Node providing further guarantees, security and capabilities as required.

2. Type 2 System Audits are required at least every six (6) months, although higher frequency may be proposed in the ITA Blueprint or required by the relevant Lead Authority. The frequency of the audits and what is to be audited is to be justified in the Blueprint.

3. Only Enhanced Systems Auditors recognised by the MDIA (see the next section) may audit and give an opinion on the ITA. The MDIA will not certify any ITA which is deemed to require an ESA in the Blueprint or in the System Auditor's report, unless the Systems Auditor qualifies as an Enhanced Systems Auditor.

4. Each area covered in the Systems Audit Report, is required to be signed off by **two** Subject Matter Experts with an expertise coinciding with the content of the area, and are considered jointly responsible for the opinion expressed in that section.

c. Systems Auditors Eligible to Perform an ESA

In order to be recognized by the MDIA, Systems Auditors (SAs) need to apply as defined in the Systems Auditors Guidelines published by the Authority. Stringent requirements are already in place to ensure that Systems Auditors possess the required skills and experience to form a trustworthy opinion of an ITA.

In order to be recognised as an Enhanced Systems Auditor, SAs must, in addition:

(i) be part of a legal organisation;

   a. which employs at least 100 persons; and
   b. with an annual revenue of at least €5,000,000 at least once over the previous three (3) years.

(ii) have suitable SME aggregate experience in Innovative Technology Arrangements in the fields that would be subject to audit of not less than four (4) years[1] gathered during the last three (3) years. In addition, at least one SME must have gathered not less than two (2)

[1] In these guidelines, one year of experience is considered to be at least 50% of one year's equivalent of full time employment.

years experience in the domain over the last four (4) 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; and

(iii) be covered by a Professional Indemnity Insurance (PII) policy for an amount of not less than €5,000,000.

Upon applying to be recognised as a Systems Auditor using the appropriate application form, the applicant may request to be recognised as an Enhanced Systems Auditor. In such a case, the submitted documentation must provide evidence that they satisfy the additional requirements identified in these guidelines.

A registered Systems Auditor may also request to upgrade their status to that of an Enhanced System Auditor, in which case they must apply using the relevant Application Form and supply documentation showing their eligibility.

On an annual basis, Systems Auditors are required to submit updated information to ensure their continued eligibility using the relevant form. In the case of Systems Auditors recognised as ESAs, additional information, as specified in the form, will be required.

Enhanced Systems Auditors no longer satisfying the criteria set out in these Guidelines are obliged to notify the Authority within three (3) months.

d. Updating the Risk-Vulnerability Assessment of an ITA

An ITA which was originally certified using a normal Systems Audit, may see an increase in risk-vulnerability throughout its lifetime such through an unplanned increase in volume or value of transactions. It is the responsibility of the Technical Administrator of the ITA to notify the ITA Applicant and MDIA when such an increase is observed. Once notified, it is the responsibility of the ITA Applicant to register the ITA with the MDIA within three (3) months of the notification using an Enhanced Systems Audit.

Since all ITAs are subject to regular Type 2 Systems Audits, Systems Auditors are responsible for notifying the Applicant and the Authority if, during such an audit it transpires that given unplanned changes in the form or volume of the use the ITA, it now requires an ESA. In such cases, the MDIA reserves the right to withdraw or suspend certification of the ITA until it applies with an ESA.