Chapter 01

Part B

Systems Auditor Report Guidelines

MDIA

Malta Digital Innovation Authority

PART B – Systems Audit Report 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 October 2018

Contents

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;
- Helps meet regulatory demands.

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

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.
- **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, in all material respects:

- 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).

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

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. The Auditee should determine whether controls over the functions performed by an organization from which it has contracted services 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 Sub-Contractor 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 Sub-Contractor to meet one or more of the applicable criteria, the Sub-Contractor activity shall be considered to be within scope for the systems audit. 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 the presentation method of such an approach to monitor the controls.

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 each sign a declaration in 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