AI System Auditor Control Objectives

MDIA
Malta Digital Innovation Authority

PART C – AI-ITA Systems Audit Control Objectives

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: 03 October 2019

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.

"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.

"Authority" refers to the Malta Digital Innovation Authority ('MDIA'), as defined by the Malta Digital Innovation Authority Act, 2018 ('MDIA Act).

"Blueprint" refers to a document that includes a description of the qualities, attributes, features, behaviours or aspects of an ITA as defined in the 'ITA Blueprint Guidelines'.

"Innovative Technology Arrangement", also referred to as 'ITA' within this document, as defined within the First Schedule of the Innovative Technology Arrangements and Services Act, 2018.

"AI-ITA" refers to Innovative Technology Arrangements that exhibit features or qualities of Artificial Intelligence as recognised by the Authority and described in the 'AI Innovative Technology Arrangements Guidelines'.

"ITAS Act" refers to the Innovative Technology Arrangements and Services Act, 2018.

"Systems Auditor" ('SA') as defined in the Innovative Technology Arrangements and Services Act, 2018, and in line with further guidance issued by the Authority within the 'Systems Auditor Guidelines'.

"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.

"Ethical and Trustworthy AI Framework" refers to the *Malta Towards Trustworthy AI: Malta Ethical AI Framework* guidelines, published by the *Malta.AI* Taskforce on https://malta.ai/

2. Systems Audit Control Objectives

The below table lists the objectives which should be covered as part of the Systems Audit report. The Systems Audit is a reasonable assurance engagement to be performed using the framework defined in the MDIA's 'AI-ITA Systems Auditor Guidelines', and the term audit in the context of those guidelines is not equivalent to the scope of an audit under International Standards on Auditing issued by the International Auditing and Assurance Standards Board. As the objectives are broad in nature, the Systems Auditor may, as part of the specific AI-ITA for which they are the appointed practitioners performing the assurance engagement, clarify further any of the objectives listed below as part of the engagement scoping. In the event that the Auditee and/or the Systems Auditor believe(s) that one or more objective(s) cannot be included for a specific AI-ITA, the Auditee would be required to discuss with the Authority to determine whether that/those objective(s) should be removed and/or amended as appropriate. In addition, as AI-ITAs differ substantially between one another, these objectives are designed to give the Auditee the facility to design controls that, while adhering in substance to these objectives, are tailored to each AI-ITAs specific requirements.

#	Applicable Areas	Systems Audit Control Objectives
Common Criteria Related to Functionality and Compliance with Regulatory Requirements		
1	AI-ITA Functionality & Blueprint Review	The Auditee documents the AI-ITA core functionality in a Blueprint and maintains a register specifying how: (i) Each aspect of functionality defined in the Blueprint is developed and implemented mapping out relative references to the Blueprint and the underlying AI-ITA code; (ii) The underlying AI-ITA code is tested to confirm it reflects the stated Blueprint function; and (iii) The register is maintained and kept up to date whenever changes in the functionality or the Blueprint take place.
2	AI-ITA Blueprint alignment with Ethical & Trustworthy AI Framework	The Auditee's Blueprint defines measures that the AI-ITA implements, maintains and monitors on an ongoing basis as deemed appropriate to ensure compliance with the Ethical & Trustworthy AI Framework.
3	AI-ITA Technical Administrator	The AI-ITA must have the necessary mechanisms defined in the Blueprint and implemented to provide the Technical Administrator with power of intervention, as defined in the AI-ITA MDIA Technical Administrator Guidelines.
4	Forensic Node	The Auditee implements a Forensic Node in line with the MDIA Forensic Node Guidelines hosted in the Maltese jurisdiction that is available 24/7 logging all transactions being relevant to the AI-ITA and which could be made accessible to relevant national competent authorities upon request.
Common Criteria Related to System Operations		

#	Applicable Areas	Systems Audit Control Objectives
5	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.
6	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 the Auditee's established incident response procedures to meet its commitments and system requirements.
7	Security Assessment	The Auditee has implemented adequate security measures to mitigate risks identified in a security assessment including potential vulnerabilities
8	Secure Code Review	The Auditee has documented and implemented policies and procedures in place to adopt secure coding practices as clarified in the Guidelines or otherwise accepted by the MDIA.
Common Criteria Related to Organization and Management		
9	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.
10	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.
11	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.

#	Applicable Areas	Systems Audit Control Objectives
12	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.
13	Staff Training	The Auditee has established procedures to evaluate, implement and monitor training requirements as deemed appropriate by the management for internal employees in interacting with the AI-ITA as it directly impacts their job role and responsibilities.
Common Criteria Related to Communications		
14	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.
15	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.
16	ITA Description, Communication	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.
17	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.
18	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.
19	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.
20	ITA Description, Communication	Policies, procedures, documentation, alerts and other formal interaction internally within the Auditee's organisation, the AI-ITA users, stakeholders, or other parties external to the Auditee's organisation, is to be done in the English language or translated in English, with the interpretation of the English version prevailing.
21	AI-ITA Description, Communication	Identify, document and implement a policy for evaluating the direct and indirect adverse effects of the AI-ITA on its internal and external users and third parties. Evaluate and monitor these effects, and communicate to affected parties or responsible stakeholders.
22	AI-ITA Risks Communication	The Auditee considers the risks related to the provision of the AI-ITA to customers, documents them, and informs the AI-ITA users and other parties

#	Applicable Areas	Systems Audit Control Objectives
		accordingly on what precautions the Auditee took in addressing them and what further considerations need to be undertaken by the user.
Common Criteria Related to Risk Management and Design and Implementation of Controls		
23	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.
24	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.
25	Risk Management	The Auditee designs, implements and operates mechanisms to identify, document and evaluate the risks related to the application of the AI-ITA internally within the organisation as well as on external users, and communicates these policies to the parties that may be potentially affected by these risks.
26	AI-ITA Ethical & Trust Risks	The Auditee identifies risks and provides explanations and mitigation mechanisms related to the impact the AI-ITA might have on the Ethical and Trustworthy key principles as specified in the Blueprint Guidelines. The Auditee must make public the risks, explanations and mitigation mechanisms that affect the external users and other third parties.
27	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.
Common Criteria Related to Monitoring of Controls		
28	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.

#	Applicable Areas	Systems Audit Control Objectives
Common Criteria Related to Logical and Physical Access Controls		
29	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.
30	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.
31	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.
32	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.
33	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.
34	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.
35	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,

#	Applicable Areas	Systems Audit Control Objectives
		availability, processing integrity, confidentiality and protection of personal data.
36	Detection 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		
37	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.
38	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.
39	Change Management	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified by the Auditee 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.
40	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		
41	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.
42	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.
43	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		

#	Applicable Areas	Systems Audit Control Objectives
44	Error Handling	Procedures exist to prevent, or detect and correct processing errors to meet the Auditee's processing integrity commitments and system requirements.
45	Processing Integrity	System inputs are measured and recorded completely, accurately, and timely to meet the Auditee's processing integrity commitments and system requirements.
46	Processing Integrity	Data is processed completely, accurately, and timely as authorized to meet the Auditee's processing integrity commitments and system requirements.
47	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.
48	Processing Integrity	System output is complete, accurate, distributed, and retained to meet the Auditee's processing integrity commitments and system requirements.
49	AI-ITA Processing Integrity	The Auditee documents the data requirements for the AI-ITA including the quality, source, timeliness, retention requirements, and use of data. In addition, the Auditee also documents methods to implement and monitor such requirements.
50	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.
Additional Criteria for Confidentiality		
51	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.
52	Confidentiality	The Auditee identifies and defines confidential information in a policy. Access to confidential information as defined in this policy is securely logged in accordance with the policy.
53	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.
54	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.
55	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.
56	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.

#	Applicable Areas	Systems Audit Control Objectives
57	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.
58	Confidentiality	The Auditee retains confidential information to meet the Auditee's confidentiality commitments and system requirements.
59	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		
60	Personal Data	The Auditee retains personal data consistent with the Auditee's objectives related to protection of personal data.
61	Data Retention	The Auditee securely disposes of personal data to meet the Auditee's objectives related to protection of personal data.
Protection of Personal Data Criteria Related to Access		
62	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.
63	Personal Data	The Auditee is able to restrict access rights associated with the viewing, modifying, inserting, copying, and deleting of personal data to a person or groups of persons specifically authorised to access and process such data.
Protection of Personal Data Criteria Related to Disclosure and Notification		
64	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		
65	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.

3. Blueprint Requirements

The Blueprint is a document which highlights all of the critical and important features which an AI-ITA should include in the information submitted to the Authority during the application for the ITA certification. This document will also be used by the Systems Auditor to understand and verify the implementation of the control objectives described in Section 2. Systems Audit Control Objectives.

Refer to the 'AI-ITA Blueprint Guidelines' for more information on requirements related to the Blueprint document.

4. Applicable Areas

Common Criteria	Applicable Areas
Functionality and Compliance with Regulatory Requirements	AI-ITA Functionality & Blueprint Review, AI-ITA Blueprint alignment with Ethical & Trustworthy AI Framework, AI-ITA Technical Administrator, Forensic Node
System Operations	Vulnerabilities Management, Incident Management, Security Assessment, Secure Code Review
Organization and Management	Organisational Structures, Staff Training
Communications	AI-ITA Description, AI-ITA Risks Communication, Formal Documentation, Communication
Risk Management and Design and Implementation of Controls	Risk Management, AI-ITA Ethical & Trust Risks, Monitoring of Sub-Contractors
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, (AI-ITA) Processing Integrity, Modification of Data
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