Chapter 01

Part C

# Systems Auditor Control Objectives

MDIA
Malta Digital Innovation Authority

# PART C – 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: 30 October 2018

# Contents

# 1. Systems Audit Categories

| 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:<br>(a) a computer protocol; and, or<br>(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; |

# 2. Systems Audit Control Objectives

| 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.<br><br>*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 and which could be made accessible to the Authority if requested. | · | · | · |
| **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. | · | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| 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 required to identify the risks and corresponding counter measures that are implemented to mitigate those risks. | · | · | · |
| 7 | Security Assessment, Vulnerability Assessment, Penetration Testing | The Auditee has implemented adequate security measures to mitigate risks identified in a security assessment including potential vulnerabilities in key management, cryptography, consensus hijack, sidechains, permissioned chain management and wallet management. | | · | · |
| 8 | Security Assessment, Secure Code Review | The Auditee consistently applies secure coding practices in all applications developed (including smart contracts). | · | · | · |
| **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. | · | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| 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. | · | · | · |
| 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 | Information Security | The Auditee has adequate information security structures in place, including documentation, awareness as well as re-active measures to handle security incidents. | · | · | · |
| 14 | 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. | · | · | · |
| 15 | 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. | · | · | · |
| 16 | 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** | | | | | |
| 17 | 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. | · | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| 18 | 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. | . | . | . |
| 19 | ITA Description, Communication | The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties. | . | . | . |
| 20 | 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. | . | . | . |
| 21 | 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. | . | . | . |
| 22 | 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. | . | . | . |
| 23 | ITA Description, Communication | All communications should be made available in English. | . | . | . |
| 24 | 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. | . | . | . |
| **Common Criteria Related to Risk Management and Design and Implementation of Controls** | | | | | |
| 25 | 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 | . | . | . |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| | | 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. | | | |
| 26 | 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. | · | · | · |
| 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. | · | · | · |
| 28 | 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** | | | | | |
| 29 | 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. | · | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| **Common Criteria Related to Logical and Physical Access Controls** | | | | | |
| 30 | 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. | | · | |
| 31 | 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. | | · | |
| 32 | 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. | | · | · |
| 33 | 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. | | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| 34 | 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. | · | · | · |
| 35 | 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. | | · | |
| 36 | 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. | · | · | · |
| 37 | 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** | | | | | |
| 38 | 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. | · | · | · |
| 39 | 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, | · | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| | | availability, processing integrity, confidentiality and protection of personal data. | | | |
| 40 | 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. | · | · | · |
| 41 | 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** | | | | | |
| 42 | 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. | · | · | · |
| 43 | 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. | · | · | · |
| 44 | 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** | | | | | |
| 45 | Error Handling | Procedures exist to prevent, or detect and correct processing errors to meet the Auditee's processing integrity commitments and system requirements. | | · | · |
| 46 | Processing Integrity | System inputs are measured and recorded completely, accurately, and timely to meet the Auditee's processing integrity commitments and system requirements. | | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| 47 | Processing Integrity | Data is processed completely, accurately, and timely as authorized to meet the Auditee's processing integrity commitments and system requirements. | · | · | · |
| 48 | 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. | · | · | · |
| 49 | Processing Integrity | System output is complete, accurate, distributed, and retained to meet the Auditee's processing integrity commitments and system 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. | · | · | · |
| 51 | Immutability | Data stored after a consensus mechanisms was triggered with successful results is immutable. | · | · | · |
| **Additional Criteria for Confidentiality** | | | | | |
| 52 | 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. | · | · | · |
| 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. | · | · | |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| 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. | · | · | |
| 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 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** | | | | | |
| 64 | 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. | · | · | · |
| 65 | Data Disclosure | The Auditee retains a complete, accurate, and timely record of processing of personal data including a record of users performing the | · | · | · |

| Ref # | Applicable Areas | Systems Audit Control Objectives | Systems Audit Categories | | |
|---|---|---|---|---|---|
| | | | IVFAO | DLT Platforms | Smart Contracts |
| | | processing and the results of the processing. | | | |
| **Protection of Personal Data Criteria Related to Quality** | | | | | |
| 66 | 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. IVFA – Whitepaper Requirements

**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 | |

| Section | Requirement | Applicable to Systems Auditor |
|---|---|---|
| (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 | · |
| (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.*

# 4. 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 |
| **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 |