SmartOne STANDARD 5002

First Edition
2019-01

Token Generation Event – Code of practice for TGE controls

Contents

Foreword

SmartOne is established as a Foundation with the intention of serving both as a provider of legal services to Token Generating Event organisers and financial institutions, and as an umbrella organization for the promotion of research, development and creation of standards to serve the wider legal and regulatory landscapes of the crypto community.

Attention is drawn to the possibility that some elements of this document may be subject of patent rights. SmartOne shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

Introduction

0.1 The SmartOne Standards

This document is designed for organizations that are undertaking a Token Generation Event in line with the SmartOne Standard 5001.

The SmartOne Standard 5001 specifies the requirements for establishing and implementing a compliant TGE/ICO. It also includes requirements for the assessment and treatment of risk tailored to the needs of the organization. The requirements set out are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

SmartOne Standard 5002 is not really a Standard as such. You would not be audited against it like SmartOne 5001, but rather it is a discussion framework that takes each of the controls listed in 5001 and expands on options and recommends implementation approaches that may be used to meet the control requirement.

Much of the decision on which controls to use, which can be offset with other controls, will depend upon the organisations approach to risk and risk management. Furthermore, it will be dependent on the relevant legislation or regulatory guidance that is imposed on the organization and its TGE.

Some of these controls will be considered standard and mandatory, others can be discretionary but justification in all decisions must be shown and recorded. Choosing a single control may not be sufficient and compliance with regulated TGE may depend on providing defence in depth through the layering of controls.

0.2 Expanding the Standard

The SmartOne Standard should be regarded as the starting point for developing an organization-specific TGE policy. Additional controls, not included in this document, may be brought to bear for specific industry or regional zones and this is perfectly justifiable. When any certification of a Standard is sought, it is the overall effect that is important and as such, SmartOne Standard 5002 provides a framework on which to consider the crucial part of a TGE trying to go through the regulated approach.

Code of practice for TGE controls

1 Scope

The Standard gives guidelines for organization TGE standards and practices including the selection, implementation and management of controls taking into consideration the organizations risk environment.

This Standard is designed to be used by organizations that intend to:

- Select controls within the process of implementing a TGEs based on SmartOne 5001
- Implement commonly accepted TGE controls
- Develop their own TGE policy

2 Normative references

The following documents, in whole, or in part, are normatively referenced in this document and are indispensable for its application.

SmartOne 5000 – Overview and vocabulary

3 Terms and definitions

For the purposes of this document, the terms and definitions given in SmartOne 5000 apply.

4 Structure of this standard

This document is broken down into the same categories as the SmartOne 5001 Standard. It does not consider the required risk assessment and risk treatment but is an expansion of the reference objectives and controls. Where a control is discussed, it will give implementation guidance.

7 BUSINESS OBJECTIVES

7.1 MANAGEMENT

	CONTROL	IMPLEMENTATION GUIDANCE
7.1.1 Development of the TGE business model	A set of documents for the business model of the TGE shall be defined, approved by management, published and communicated to employees and relevant external third parties.	The business model is the concept of the business and how it utilizes and integrates with the blockchain. It would include: • Discussion on the need for the application or service • The concept of the blockchain application or service • The need the application or service fulfils i.e. the opportunity • A roadmap for the application or service • The TGE will be discussed in much more detail in later controls.
7.1.2 Development of the TGE economic model	A set of documents for the economics model of the TGE shall be defined, approved by management, published and communicated to employees and relevant external third parties. This shall be in alignment with the business model.	The economics model is a reflection of the underlying business, its model, market size, competitive landscape and cost base. The model should consider the following points: • The quantity of tokens being minted • The purpose of the TGE • Detailed model including business and entry and exit token positions • Token burning policy and process • Token economics

		A summary of the model may be included in the white paper, but a detailed financial model should be ratified by top level management.
7.1.3 TGE partners	Identification of TGE technology, legal, financial and regulatory partners.	• Service agreements shall be in place between the Organization and all Service Providers • All agreements should set out the jurisdiction under which they are operative • The Technical Partner should deliver 'Know Your Customer' services, and they should be in accordance with the terms and requirements set out in this document • The Organization shall sign off the delivery of services of applications as required All service agreements should consider the following: • Term of the agreement • Commitments for all parties • Pricing and payment terms • Confidentiality • Indemnifications • General provisions • Termination of the agreement • Governing law and jurisdiction

		Each Partner company must be subject to due diligence with regards to: • Legal issues and corporate structure • Management and employment • Sales and marketing activities • Financial aspects
7.1.4 Review of regulatory information	The market specific, and/or region specific, regulatory requirements shall be reviewed to ensure continuing suitability, adequacy and effectiveness of the application or service to meet the requirements.	A full review should be made by the management team of the Organization. The demands made on the application or service will vary greatly from region to region or country to country. Specialist advice should be sought from the Legal and Regulatory Intermediary Partners to ensure that the information is up-to-date. A decision must be made as to how to handle KYC requirements that are needed to be regulatory compliant. This may involve the purchase of an off the shelf product, engagement with a 3rd party or a hybrid of those options. Effective KYC management is discussed later in this control framework.
7.1.5 Review of Anti-Money Laundering Acts	Requirements to meet AMLA shall be reviewed and documented.	A full review should be made by the management team of the Organization. The demands made on the application or service will vary greatly from region to region or country to country. Specialist advice should be sought from the Legal and Regulatory Intermediary Partners to ensure that the information is up-to-date.

		A decision must be made as to how to handle AMLA requirements that are needed to be regulatory compliant. This may involve the purchase of an off the shelf product, engagement with a 3rd party or a hybrid of those options. Effective AMLA management is discussed later in this control framework.
7.1.6 Development of TGE operations model	This shall cover the use of the Regulatory Intermediary to KYC/AMLA checks, escrow services, FIAT deposits, crypto deposits.	In order to meet regulatory requirements, there are a number of services that need to be in place. This document should summarise Know Your Customer legislation demands and Anti-Money Laundering requirements for all relevant jurisdictions as discussed in section 7.1.4 and 7.1.5; the use of escrow accounts; fiat and crypto currency movements and all associated security controls.
7.1.7 Collection of critical business information	Collection of minimum information requirements to meet regulatory demands for the TGE.	The following information is considered as the minimum needed by the regulator or Regulatory Intermediary. It should be collated for later use by the Legal Partner when obtaining regulatory compliance status from the Regulatory Intermediary: • Name of the project, goals and project plan • Organization name / names of the project operators including domicile of the organization/organization's, address(es), email address(es) and website(s) • Details of all persons involved (including addresses and/or domicile of the Organization, in particular the founder(s), token issuer and token seller • Details of all service providers involved (e.g. Technical Partners, Regulatory Intermediary) • Other secondary trading participants (platform, TGE organizers) • Project description

		• Identification of which market participants (investors) the TGE targets • Any restrictions on investors • Any information regarding the project organization and project planning, including the timing of various TGE phases and milestones • Information about the technologies to be used
7.1.8 Price and Payment procedure	There shall be a formal and documented price and payment procedure for the TGE.	This procedure should include: • Offer terms • Timeline and pricing • Token distribution • Hard and soft cap policy
7.1.9 TGE security roles and responsibilities	All TGE security responsibilities shall be defined and allocated.	Allocation of information security responsibilities should be performed in alignment with the Information Security policy. It is critical that responsibility for individual assets, information or complete systems is assigned and in particular for the acceptance of residual risk. Where appropriate, responsibilities should be supplemented with more detailed guidance. • Assets and information security processes should be identified and defined • The entity responsible for each asset or information security process should be assigned and the details of that responsibility should be documented

		• Individuals or corporate entities should be verified as being competent in the area they are assign responsibility for
7.1.10 Information Security Policy	The Organization shall create and maintain an Information Security Policy for all aspects of the application or service and the project which delivers it.	The Information Security Policy should cover any aspect of the project and be applicable to the Organization, its subsidiaries and its partners. For example, where a KYC application provider is employed it should specify: • Acceptance testing for the quality and accuracy of the deliverables • Provision of evidence that security thresholds were used to establish minimum acceptable levels of security and privacy quality • Provision of evidence that sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery • Provision of evidence that sufficient testing has been applied to guard against the presence of known vulnerabilities It should also cover all aspects of Information Security related to the technical implementation, as set out in this document.
7.1.11 Development of the TGE white paper	The TGE white paper, shall be defined, approved by management, published and communicated to all relevant external third parties.	The white paper brings together all of the above sections to a degree. It would, therefore, consist of elements such as: • Proposition • Integration with the blockchain • Timeline and pricing of the TGE

		• Token distribution • Economic and business models • Organization details

8 ENGAGEMENT WITH PARTNERS

8.1 GENERAL

	CONTROL	IMPLEMENTATION GUIDANCE
8.1.1 Establish terms and conditions of all partnerships	Legal, Technical, Regulatory Intermediary and financial institution must be selected and engaged with.	Following on from section 7.1.3, contractual agreements with partner must be in place. They should state: • The Organization's responsibilities • Fees • Policies • Lines of communication • Jurisdiction and applicable law for all disputes In order to meet strict regulatory demands, every participant must comply with the applicable Anti-Money Laundering regulations and co-operate for the identification process according to the provisions for the prevention of money laundering and for the KYC check. The Organization must document how it is proposing to handle KYC/AMLA legislation. Options include:

		• In-house development of KYC/AMLA application and use of a Regulatory Intermediary • Use of approved KYC/AMLA application or service and use of a Regulatory Intermediary • Use of a Regulatory Intermediary that already employs an approved KYC/AMLA application or service KYC/AMLA applications or services are subject to extremely stringent technical and procedural controls as well as being subject to slow ratification processes within the regulator. In-house development could be elongate delivery times and delay any planned TGE. This risk must be shown to have been considered. Further details can be found in the requirements of a technical partner in section 8.3.
8.1.2 Screening	Background verification checks on partners and/or suppliers.	Background verification checks on partners and/or service providers shall be carried out in accordance with relevant laws, regulation and ethics and shall be proportional to the business requirements, the classification of the information and the perceived risks.
8.1.3 Contact with authorities	Contacts should be maintained by with regulatory bodies.	In order to facilitate efficient incident management or business continuity plans, as well as advanced notification and understanding of regulatory or legal changes, contacts with regulatory bodies should be maintained. This maintenance may take the form of subscriptions or correspondence. Procedures should be in place that define how and when to contact regulatory bodies in a timely manner and which defines information relevant to any security breach.

8.1.4 Monitoring and review of service provider service delivery	Organizations shall regularly monitor, review and audit supplier service delivery.	Where delivery of services is obtained by partners or 3rd party suppliers, the Organization should regularly monitor, review and audit their delivery. This will ensure: • Service performance levels are adhered to • Any information upon which the TGE is based, or changes in regulatory requirements, can be reviewed by senior management within the Organization • Any security incidents or events should be reviewed • Where applications or services are delivered for the TGE, operational problems should be reviewed, managed and improvements made and documented • If available, audit reports on supplier accreditation should be reviewed periodically The Organization should retain sufficient overall control and visibility for the delivery of its TGE.
8.1.5 Confidentiality or non-disclosure agreements (NDA)	Non-disclosure agreements shall be in place, if applicable.	Confidentiality or non-disclosure agreements may be applicable to employees of the TGE Organization and/or between external parties/partners. Each NDA should consider the following points:

		• A definition of the data to be protected • The expected duration of the NDA • Required actions when an agreement is terminated • Ownership of any intellectual property or information covered by the NDA • The process of notifying signatories to the NDA in the event of a breach of the terms of the NDA • Expected actions to be taken in case of a breach of the agreement The Organization should assert its right to audit and monitor any activity or data covered by the NDA. Evidence must be obtained that any NDA complies with all applicable laws and regulations for the jurisdiction to which they apply. A documented review process should be established both for the requirement of a confidentiality or non-disclosure agreement and for the contents of any such agreement.

8.2 LEGAL PARTNER

	CONTROL	IMPLEMENTATION GUIDANCE
8.2.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements shall be explicitly identified, documented and kept up to date for each system.	The Legal Partner shall provide for the Organization a summary of the relevant legislative statutory, regulatory and contractual requirements and advise accordingly on all contracts.

8.2.2 Token Sale terms	An appropriate set of Token Sale Terms shall be ratified by the Legal Partner.	Public sale terms and conditions. The detailed points of the Organization TGE and the legal obligations of all parties therein shall be set forth in a detailed Terms and Conditions document. This document is binding upon the Organization and the contributor and forms the basis under which tokens are issued and how a contributor is to pay for them.
8.2.3 Legal opinion	The Legal partner shall give its opinion on the TGE as to the category of the tokens.	Companies launching a TGE must ensure that they comply with the requirements set out in the relevant financial market laws. The Organization shall engage with a lawyer who is conversant in securities law for the applicable region. The assessment must be made in alignment with the relevant regulatory authorities and Legal Partner. The Legal Partner must provide a letter of opinion as to the status of the token which must be submitted to the Regulatory Intermediary for ratification. The relevant regulations must be identified and understood.
8.2.4 Engagement with Regulators	The relevant regulators shall be informed of the legal opinion and proof obtained of the adherence to the regulatory framework for that Token type.	Where applicable, the Legal Partner will submit to the Regulatory Intermediary, on behalf of the Organization, its legal opinion on the token type.
8.2.5 Privacy Policy	The Organization shall develop and maintain a privacy policy for all external 3rd parties, including partners and token holders.	

		The relevant legislation regarding privacy must be assessed by the Organization and evidence of this assessment recorded. Moreover, all 3rd parties involved in the scope of the project must have their own privacy policies aligned with the Companies privacy policy or subject to the controls outlined in the Companies policy. The privacy policy must be published and available to all 3rd parties, including token holders.
8.3 TECHNICAL PARTNER (GENERAL)		
	CONTROL	IMPLEMENTATION GUIDANCE
8.3.1 Identification of required blockchain contracts	Documented review of required contracts for all regions the TGE is applicable.	
8.3.2 Development of Smart Contracts	Development and publication of a smart contract on the blockchain for token. <<best practice for smart contracts>>	The technical partner shall deliver a KYC application and TGE service that integrates functionality in a Smart Contract, built on Solidity source code.
8.3.3 Blockchain integration	The Technical Partner should deliver a solution that is fully integrated with blockchain technology.	The following considerations should be met: • All application submissions should be stored on the blockchain as a content ID hash • Once a KYC submission has been approved, that approval by the Service provider shall be stored on the blockchain

		• The issuance of tokens shall be recorded on the blockchain
8.3.4 Outsourced development or delivery	The Organization shall develop and maintain a policy for outsourcing technical delivery of TGE components. The Organization shall supervise and monitor the activity of any system delivered by an outsourced software component.	Where system development is outsourced, consideration must be given to: • Licensing arrangements, code ownership and intellectual property rights related to the outsourced content • Contractual requirements for secure design, coding and testing practices • Agreement must be in place between the Organization and the Partner that cover the expected threats to the system • The Partner must deliver effective documentation on the delivered system or developed software Where applicable, the Organization shall retain the contractual right to audit development processes and controls. No matter the extent of outsourced hosting, delivery or development, the Organization remains responsible for compliance with applicable laws. To that extent, evidence must be collected by the Organization from all 3rd parties involved that sufficient testing and consideration of security in design has been undertaken.
8.3.5 Separation of development, testing and operational environments	Where the Technical Partner operates a service or application on behalf of the Organization, it must operate separate development, testing and operational environments.	Separation between operational, testing and development environments is required to minimise operational problems.

		Evidence must be sought that the Technical Partner has adopted this methodology as well as providing its operational policy for change management and testing procedures. It is preferable that development and testing personnel are separate and have restricted access to each environment. There is a clear segregation of duties issue where development and testing personnel have unrestricted access to operational systems or applications which can lead to unauthorized changes or untested code being deployed and may lead to misuse of the system. Separating the development, testing and operational environments reduces the risk of accidental change to the system or the data therein.
8.3.6 System security testing	The Organization shall develop and maintain its own acceptance testing policy. The Organization may outsource security testing to utilise technical expertise of a Partner, but it remains responsible for its delivery.	New and updated systems or applications require thorough testing and verification. The Organization should maintain an overview of security related matters and the changing threat landscape.
8.3.7 System acceptance testing	The Organization shall develop and maintain its own acceptance testing program.	New and updated systems or applications require thorough testing and verification. This should be independent to the Technical Partner, though the Technical Partner may provide evidence of its own testing program.
8.3.8 Secure development policy	The Organization shall enforce a secure development policy of its Technical Partner.	Secure development is key to creating a secure service or application. If development is outsourced, the Organization shall obtain assurances that the Technical Partner operates along the following guidelines:

		• The development environment is secure and has restricted and strongly authenticated access • Security is considered in the entire lifecycle of development, including the design phase of any project, service or application • Uses secure repositories • Is a specialist in designing and creating secure applications by utilising secure coding practices, secure operational procedures and has employees who understand the threat landscape.
8.3.9 Secure development environment	The Organization shall enforce a secure development environment of its Technical Partner.	Over and above the secure development policy, the development environment considers the people, processes and technical components that make up a development project. Evidence should be collected that demonstrates the following: • The sensitivity of the data being processed, stored or transmitted. The classification system used may be bespoke • Trustworthiness of the personnel working on the project and may include background security checks or HR interviews • Access procedures to all development environments and a full audit trail of permissions • Monitoring of changes to source code and full accountability
8.3.10 Securing application services		

	Information involved in the application must be protected against fraudulent activity, unauthorized disclosure and modification.	An assessment should be made of application services and, in particular, the protection requirements of any confidential information.
8.3.11 Information security requirements analysis and specification	The Organization shall assess all information security requirements and develop and maintain an information security policy.	Information security requirements will be driven by compliance requirements from regulators and other Organization policies. The specific controls chosen should reflect the business value, both reputational and intrinsic, of the information being protected. The policy should consider the following: • Authentication and authorisation requirements and processes • Minimum technical requirements to protect assets or information, in particular regarding availability, confidentiality and integrity • Assessment of the threat model to assets/information • Informing users and operators of their duties and responsibilities
8.3.12 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for the protection of information should be developed and implemented.	When developing a cryptographic policy, the following should be considered: • The management approach towards the use of cryptographic controls across the organization including the general principles under which business information should be protected • Based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required

		• The use of encryption for protection of information transported by mobile or removable media devices or across communication lines • The approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys • Roles and responsibilities for the implementation of the policy and the key management • The standards to be adopted for effective implementation throughout the organization

8.4 TECHNICAL PARTNER (KYC/AMLA APPLICATION)

	CONTROL	IMPLEMENTATION GUIDANCE
8.4.1 KYC Functionality	The Technical Partner shall deliver a full KYC application to meet the appropriate regulatory requirements.	As discussed in section 8.1.1, the Organization launching a TGE must ensure that they comply with the requirements set out in the relevant financial market laws. Therefore, to expedite the TGE process, they should engage with a Technical Partner to provide a KYC/AMLA application or service or use a Regulatory Intermediary Partner who already utilises an approved KYC/AMLA application or service. The service provider's KYC application shall meet the requirements of, and be approved by, the relevant Regulator. As a minimum it should collect and/or provide the following functionality as part of the KYC submission: • Set out Terms and Conditions • Name • Nationality

		• Profession • Date of Birth • Phone Number • Email address • Postal address • Payment Source Account • Payment source of proceeds • Token destination Ethereum wallet • MRZ passport/ID scanner • Liveness detection video solution • Submission content ID hash The back-end system of the KYC application should use Role Based Access Control to enforce segregation of duties and with strong multi-factor authentication of the Service Providers users. KYC pack submissions should be available to download, approval decision and the subsequent issuance of tokens to the application user via a digital process. KYC pack submissions shall be signed with a digital signature to ensure integrity. KYC pack submissions must be subject to strict privacy, confidentiality and integrity controls. Consideration should be given for utilising: • In-memory storage • Encrypted removable storage

		• Data destruction policy • Audit requirements All regulatory demands surrounding Politically Exposed Persons and/or other sanctions shall be applied by the application. The end user shall be notified via other means (email/SMS) of progress of the KYC submission and review process.
8.4.2 Information transfer policies and procedures	Formal transfer policies, procedures and controls should be in place to protect the transfer of information.	The procedures and controls to be followed for information transfer should consider: • Procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction • Personnel, external party and any other user's responsibilities not to compromise the organization • Use of cryptographic techniques to protect the confidentiality, integrity and authenticity of the information • Consideration of training for personnel to protect confidential information • Not leaving data in permanent storage
8.4.3 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Security considerations should include:

		• A risk assessment and classification of the transaction. The risk assessment drives the extent of the controls needed to protect information • Encryption of data in transit and data in storage • Protocols for communication and an assessment of any known vulnerabilities • Storage of transactions should be secure and in the case of KYC data, ephemeral • An assessment of the relevant legal and regulatory requirements in the jurisdiction(s) involved
8.4.4 KYC+AML apps and portal operations	The KYC application shall have a defined and secure process to download and approve/reject the KYC pack submission.	The Technical Partner must implement a solution compliant with the Information and Privacy controls laid out in the Organization policy, which by definition, will meet the criteria laid out by the Regulator.
8.4.5 Integration with blockchain	The KYC process shall be fully integrated with the Ethereum blockchain including app submission, approval and token issuance.	The Technical Partner shall implement a solution fully integrated to the Ethereum blockchain using smart contracts.
8.4.6 Notification process	Participants shall be informed of KYC progress through a defined set of methods.	The technical solution shall implement such methods as necessary to notify all relevant parties, but limit knowledge of, and access to, KYC information using controls outlined in this document.

8.4.7 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured.	Compliance with this policy and all relevant legislation and regulations concerning the protection of privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented.
8.4.8 Secure log-on procedures	Employee access to the KYC packs shall be secured through multi-factor authentication.	A suitable authentication technique should be chosen to substantiate the claimed identity of a user. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used. The procedure for logging into a system or application should be designed to minimise the opportunity for unauthorised access. The log-on procedure should therefore disclose the minimum of information about the system or application, in order to avoid providing an unauthorised user with any unnecessary assistance.
8.5 TECHNICAL PARTNER (TGE SERVICE DELIVERY)		
	CONTROL	IMPLEMENTATION GUIDANCE
8.5.1 Secure system engineering principles	The Organization must set out the engineering principles it requires of its Technical Partner or assess its Technical Partners own principles to ensure that they are in alignment.	The technical partner must operate within the principles laid out by the Organization.

		Secure information system engineering procedures based on security engineering principles should be established, documented and applied to in-house information system engineering activities. Security should be designed into all architecture layers balancing the need for information security with the need for accessibility. Where applicable, the defined engineering principles should be applied to outsourced companies through the use of contracts or other binding agreements. These principles should be regularly reviewed to ensure that they are fit for purpose and are contributing to secure system engineering.
8.5.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures. Formal change control procedures should be developed and maintained.	To ensure the integrity of all systems or applications, formal change control procedures should be documented and enforced. Any changes should adhere to these procedures so that there is a full trail of specification, design, documentation, testing and finally, managed implementation. The managed implementation should involve a risk assessment of the proposed changes. Change control procedures must incorporate: • An agreed definition of authorisation levels i.e. a scale of changes permitted from standard operating procedures authorised and performed by junior staff to major changes authorised by Senior management. • A defined list of authorised users who may submit and implement changes . • An independent review process for changes and the implementation plan.

		• Version control for all software changes. • An audit trail of all change requests and their authorisation party and implementation party. • A business assessment of the change control to provide oversight into the most appropriate time to implement any change. • Segregated testing of a change in a development or test environment.
8.5.3 Technical review of applications after changes	After any change, the application must be reviewed for functionality.	Whilst any change will have been subject to testing in a separate environment to ensure that there is no adverse impact on functionality or security, a plan must be developed to assess the real time state of the application after any change.
8.5.4 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented.	Where cryptographic controls are in use, which cryptographic algorithms, key lengths and usage practices should be assessed and defined by the Organization and/or its technical partner. The policy must also include operational matters such as managing keys through their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying. Equipment used to in the lifecycle of keys should by physically protected or if being used on a 3rd party environment, the 3rd party must comply with, and be audited to, ISO 27001.

		Any policy on cryptographic controls should include defined validity periods and approved public certification authorities including an assessment per jurisdiction(s) involved.
8.6 TECHNICAL PARTNER (OPERATIONS)		
	CONTROL	IMPLEMENTATION GUIDANCE
8.6.1 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated.	Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of the Organization's assets. When it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.
8.6.2 Access control policy	An access control policy shall be established, documented and reviewed based on business requirements.	Role based access control should be the preferred method. The core principles of any access control policy should be: • Everything is generally forbidden unless expressly permitted • Need-to-know – the granting of access to any information should be only to that required for the task • Need-to-use – the granting of access to any information processing facilities should only be to that required for the role The access control policy should consider:

		• Security requirements of business applications; • Policies for information dissemination and authorisation – the need-to-know principle • Consistency between the access rights and information classification policies of systems and networks • Relevant legislation and any contractual obligations regarding limitation of access to data • Management of access rights in a distributed and networked environment • Segregation of access control roles – access request, access authorisation, access administration • Requirements for formal authorisation of access requests • Removal of access rights • Archiving of records of all significant events concerning the use and management of user identities and secret authentication information • Roles with privileged access
8.6.3 Management of secret information of users	A process should be developed and maintained to protect secret information.	In this context, users may be external token holders (external users) or internal employees (internal users) of the Organization. The process should consider the following points: • Internal users should be required to sign a statement or policy to keep their own personal secret authentication information

		confidential i.e. logins. This signed statement may be included in the terms and conditions of employment • Any system should allow an internal user to create and maintain their own secret authentication information. They may be provided with secure temporary authentication information initially but should be subject to enforced change at initial logon. The system administrator should not be party to this changed secret authentication information • Where possible, the use of OTP or multi-factor authentication should be considered • Procedures should be established to verify the identity of an internal or external user prior to providing new, replacement or temporary secret authentication information • Temporary secret authentication information should be given to users in a secure manner
8.6.4 User registration and de-registration	A formal user registration and de-registration process should be implemented to enable the assignment of access rights.	Unique user IDs for both internal and external users must be implemented. A process should be created and implemented for the disabling or removing of user's IDs for Internal users who have left the Organization or external users who no longer require use of the application. The process should include a scheduled review of users in line with the Organization's security policy.
8.6.5 User access provisioning	Any application shall have defined role-based access control to participants information – access control policy.	A provisioning process for all internal users of the application should be created and maintained. The process should assign or revoke permissions

		for all user types (junior, senior and supervisory) to the system or services. It should include: • Access rights to be assigned 'Just in time'. Furthermore, they should not be granted until the authorisation process is complete • Authorisation of a user should be given by the owner of the information system who should verify the level of granted access • All access rights that are granted should be auditable • Access rights should be reviewed periodically and immediately upon changed roles or responsibilities Consideration should also be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorised access is attempted by personnel or contractors.
8.6.6 Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	Like the user access provisioning, privileged access rights should be restricted and controlled. • Access rights to be assigned 'Just in time'. Furthermore, they should not be granted until the authorisation process is complete • Authorisation of a user should be given by the owner of the information system who should verify the level of granted access • All access rights that are granted should be auditable • Access rights should be reviewed periodically and immediately upon changed roles or responsibilities

		A formal authorization process should be in place for the allocation of privileged rights. These rights should be allocated to specific users on a need-to-know basis and on an event-event basis in line with the access control policy.
8.6.7 Review of user access rights	All access and use rights should be periodically reviewed.	The review process should include: • Users access rights should be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment; • User access rights should be reviewed and re-allocated when moving from one role to another within the same organization; • Authorizations for privileged access rights should be reviewed at more frequent intervals; • Privilege allocations should be checked at regular intervals to ensure that unauthorised privileges have not been obtained; • Changes to privileged accounts should be logged for periodic review
8.6.8 Use of secret authentication information	Implementing the information security policy with regards to the use of secret authentication information.	The policy should have covered how to handle, maintain and use secret authentication information, including advice on: • Not keeping a record of secret authentication information

		• To not share secret authentication information • Not re-use the same secret authentication information across systems.
8.6.9 Information access control	Role based access control shall be used.	
8.6.10 Documented operating procedures	Operating procedures should be documented and made available to all users who need them.	All operational activities should be documented. Each documented process or procedure should be treated as a formal document and be subject to an authorized change management process itself. The operating procedures will be specific from implementation to implementation, but they should, at a minimum, cover: • The processing and handling of information • Instructions for handling errors or other exceptional conditions • Support and escalation contacts in the event of unexpected operational or technical difficulties

8.7 REGULATORY INTERMEDIARY PARTNER (RIP)

	CONTROL	IMPLEMENTATION GUIDANCE
8.7.1 Regulatory Intermediary status	The RIP shall hold the relevant intermediary requirements/licenses of regulators and shall be subject to regulatory audits as needed to maintain their status.	Dependent on the location of the TGE, and therein the legal framework, Regulatory Intermediaries may be required. Many Anti-Money Laundering Acts state that Regulatory Intermediaries can become members of a self-regulatory organization under civil law as a way of ensuring compliance

		with due diligence requirements as an alternative to direct supervision by the regulator. Where this is the case, the Regulatory Intermediary must become a member of that self-regulatory organization and evidence of this membership must be obtained. The Regulatory Intermediary must perform the stringent Know Your Customer review for each Contributor.
8.7.2 Adoption of a KYC procedure	The RIP shall adopt a KYC procedure for all TGE contributors.	To meet the identified regulatory requirements, all contributors must undergo KYC processing. The exact KYC procedure chosen may be technical or procedural but must be implemented in accordance with the requisite regulatory demands. These may include traceability of contributors, contributors' assets and non-repudiation of contributions.
8.7.3 Information transfer of the KYC	Secure transfer of information between the organizations and external parties must be enforced.	Information transfer mechanisms must be enforced that incorporate: • The minimum technical standards as laid out in the Information Security policy. • Responsibilities of all parties in relation to KYC data, including liabilities in the event of information security incidents, such as loss of data or breach of system • Any special controls that are required to protect sensitive items, such as cryptography.

8.7.4 Contact with the Regulator	Collection of minimum information requirements to meet regulatory demands for the TGE.	The following should be considered when contacting the Regulator regarding the position of the TGE: • Name of the project • Organization name including domicile of the organization/organizations, address(es), email address(es) and website(s) • Details of all persons involved, in particular the founder, token issuer and token seller • Notification of any licenses granted under financial market law • Project goals and project plan • Key features of the project • Investors being targeted and any restrictions on investors • Information about the technologies to be used • Which cryptocurrencies or legal tender with the TGE be financed and how • How much money the TGE is intending to raise • Token creation by the TGE including technical standards • At which point, by whom and in which manner will tokens be transferred to investors • The functionalities planned for the token • The rights of the investor • Details on the Regulatory Intermediary and whether they are currently subject to AMLA

		• How will tokens be transferred including technical standards • How and where tokens be acquired or sold after the issue • Will it be possible to use the tokens to buy goods or services or make payments to 3rd parties • Any plans for the project operator/issuer to buy back tokens

8.8 FINANCIAL INSTITUTION PARTNER (FIP)

	CONTROL	IMPLEMENTATION GUIDANCE
8.8.1 Financial Institution status	The FIP shall provide services approved by the Regulatory Intermediary Partner.	Dependent on the location of the TGE, and therein the legal framework, specific demands may be placed on the Financial Institution. The Financial Institution shall provide all financial services required by the Organization and the Regulatory Intermediary and hold all requisite licenses in order to do so.
8.8.2 Escrow accounts	Provision of an escrow account.	The Financial Institution shall provide the required escrow account.
8.8.3 Escrow process	Procedures for escrow account access shall be developed.	The Organization should not take deposits directly from Contributors prior to completion of the KYC and Anti-Money Laundering check being performed by a Regulatory Intermediary (the Regulatory Intermediary is defined in section 8.7) and until tokens are confirmed as delivered to the Contributor.

		Therefore, the Regulatory Intermediary, or its delegate, shall be the party to receive funds from Contributors. Such funds can arrive in the fiat currency bank account of the Regulatory Intermediary or to a cloud storage dual-wallet hardware device controlled by the Regulatory Intermediary. Only after the Contributor's KYC submission is approved should the Regulatory Intermediary inform the financial partner to transfer fiat currency from the intermediary's members account to the Organization's TGE account or, in the case of crypto deposits, make the crypto transfer of crypto currency from the intermediaries' member-controlled wallet to the Organization's wallet. A procedure shall be developed, documented and implanted to create to an escrow wallet. This should cover: • The hardware device to be used and its suitability • Confidentiality requirements • Recovery requirements and a process that maintains confidentiality • Defined escrow periods • Collection and refund procedure • Delivery procedure • Compensation to the escrow agent • Duties and rights of the Escrow agent • Handling disputes
8.8.4 Financial accounts	Provision of all bank accounts.	Subject to relevant national or regulatory law:

		• A Contributor may transfer fiat currency to exchange for TGE tokens • A bank account should be opened by the Organization and the Regulatory Intermediary. It is preferable for both accounts to be held at the same bank • A Contributor may transfer cryptocurrency in exchange for TGE tokens. A hardware wallet should be established between the Organization and the Regulatory Intermediary. The use of hardware wallets and/or multi-signature wallets may be evaluated. A risk assessment should be documented by the Organization into its use of either, and consider the following points: • Known technical flaws on certain implementations of multi-signature wallets • The use of cold storage dual-wallets must be accompanied by a defined and documented procedure for their use which maintains the integrity of the wallet • Leasing of safe-deposit boxes for storage of hardware wallets

9 REGULATIONS

9.1 REGULATORY COMPLIANCE

	CONTROL	IMPLEMENTATION GUIDANCE

9.1.1 Token Categorisation	An assessment must be made of the token type. The assessment must be agreed between the Organization and its Legal Partner.	Tokens fall broadly into three main categories: • Assets tokens – represent assets such as debt or equity claim on the issuer and may promise a share in future company earnings or future capital flows. Issuers offering to buyback-and-burn their tokens or those supplying physical goods traded on the blockchain are also Asset tokens. These tokens are most analogous to traditional equities, bonds or derivatives. • Payment Tokens – intended to be used, now or in the future, as a means of payment for acquiring the Organization's goods or services or as a means of money/value transfer and give rise to no claims on the issuer. Supply of these tokens increases over time and are investor-dilutive. These are synonymous with cryptocurrencies; • Utility Tokens – provide access digitally to a service by means of a blockchain-based infrastructure. Supply of these tokens does not increase and is not investor-dilutive. Asset and utility tokens can also be classified as payment tokens (referred to as hybrid tokens). In these cases, the requirements are cumulative; in other words, the tokens are deemed to be both securities and means of payment. The Organization must evaluate and justify its token classification. Tokens may also be put into circulation at the point of fund raising. • Pre-financing is another option that could be considered whereby investors are offered only the prospect that they will receive tokens

		at some point in the future and the tokens of the underlying blockchain remain to be developed. • Pre-sale represents another option whereby investors receive tokens which entitle them to acquire other different tokens at a later date
9.1.2 Utility Tokens	Assessment of the token as a utility token, where applicable.	Evidence must exist that the following core principles for Utility token compliance are met: • Platform must already exist and be fully operational on the blockchain; • The token must be redeemable by the blockchain on the platform on date of issue; • The tokens must be issued to each Participant in a "rolling-close" style Offering immediately upon receipt of Participant's' Contribution Amounts into Escrow; • Tokens are not entitled to a vote on how the Organization operates; • Tokens are not entitled to dividends or a profit-share from future operating profits; • Issuer may not Buyback tokens from future operating profits;

9.1.3 Status of Tokens as Securities	Assessment of the token as a security, where applicable.	Clarification must be sought from the Legal Partner and regulator as to whether tokens qualify as securities with the relevant regulator. • Payment tokens / cryptocurrencies There are various legal opinions as to whether tokens of this kind constitute securities. Some assert that all types of tokens should be considered as securities; others disagree. Given that payment tokens are designed to act as a means of payment and are not analogous in their function to traditional securities, ascertain if the regulator will not treat payment tokens as securities. Ensure that a review of method of notification to the Organization is on place if payment tokens were to be classified as securities through new case law or legislation. • Utility tokens Ascertain the regulators position on whether utility tokens will or will not be treated as securities if their sole purpose is to confer digital access rights to an application or service and if the utility token can be used in this way at the point of issue. Determine if the underlying function is to grant the access rights and the connection with capital markets, which is a typical feature of securities, is missing. Equally, if a utility token additionally or only has an investment purpose at the point of issue, the regulator may treat such tokens as securities (i.e. in the same way as asset tokens). • Asset tokens Ascertain of the regulator treats asset tokens as securities. It is probable that the regulator will view asset tokens as securities if they represent an

		uncertificated security and the tokens are standardised and suitable for mass standardised trading. An asset token may also qualify as a security if it represents a derivative (i.e. the value of the conferred claim depends on an underlying asset) and the token is standardised and suitable for mass standardised trading. In the case of the pre-financing and pre-sale phases of a TGE which confer claims to acquire tokens in the future, these claims may also be treated as securities (i.e. in the same way as asset tokens) if they are standardised and suitable for mass standardised trading. Note, securities are deemed as standardised certificated or uncertificated securities, derivatives and intermediated securities which are suitable for mass standardised trading, i.e. they are publicly offered for sale in the same structure and denomination or are placed with more than 20 clients, insofar as they have not been created especially for individual counterparties. Uncertificated securities are defined as rights which, based on a common legal basis (articles of association/issuance conditions), are issued or established in large numbers and are generically identical. Under the Code of Obligations (CO), the only formal requirement is to keep a book in which details of the number and denomination of the uncertificated securities issued and of the creditors are recorded (Art. 973c para.3 CO). This can be accomplished digitally on a blockchain. If the regulator concludes that the tokens of a TGE constitute securities, they will fall under securities regulation and the implications of this must be known.
9.1.4 Review of AMLA regulations	Documented assessment of the latest AMLA regulations and their applicability to the TGE.	The objective of the Anti-Money Laundering Act (AMLA) is to protect the financial system from money laundering and the financing of terrorism. Any Organization who provides payment services or who issues or

		manages a means of payment is a Regulatory Intermediary subject to AMLA. The issuing of payment tokens constitutes the issuing of a means of payment subject to AMLA regulation as long as the tokens can be transferred technically on a blockchain infrastructure. In the case of utility tokens, AMLA regulation may not be applicable as long as the main reason for issuing the tokens is to provide access rights to a non-financial application of blockchain technology.
9.1.5 Application of the Anti-Money Laundering Act	Documented evidence that the KYC process in place has been approved by the relevant Regulator.	Anti-money laundering regulation gives rise to a range of due diligence requirements including the requirement to establish the identity of the beneficial owner and the obligation either to affiliate to a self-regulatory organization (the Regulatory Intermediary as defined here) or to be subject to direct Regulator supervision. These requirements may be fulfilled by having funds accepted via Regulatory Intermediary who is already subject to AMLA and who exercises on behalf of the organiser the corresponding due diligence requirements. The exchange of a cryptocurrency for fiat money or a different cryptocurrency may fall under AMLA. Equally, the offering of services to transfer tokens if the service provider maintains the private key may also be covered by AMLA. Clarification of these points must be sought by the Organization via its Legal and Regulatory Intermediary Partners.

10 RISK ASSESSMENT

10.1 BLOCKCHAIN

	CONTROL	IMPLEMENTATION GUIDANCE
10.1.1 Review of blockchain risks	A risk assessment for all blockchain-related issues.	A risk assessment and planned treatment for all blockchain-related issues, including but not limited to mining attacks, lack of consensus, forks, must be performed and maintained on a minimum annual basis.

10.2 REGULATORY

	CONTROL	IMPLEMENTATION GUIDANCE
10.2.1 Review of regulatory risks	A risk assessment for regulatory-related issues.	A risk assessment and planned treatment for regulatory-related issues must be performed and maintained on a minimum annual basis.