مصرف قطر المركزي
Qatar Central Bank
State of Qatar • دولـــة قطـــر

Distributed Ledger Technology Guideline

(Regulating the use of Distributed Ledger Technology by QCB Licensed Entities)

Table of Contents

PART A (GENERAL PROVISIONS)

1. Short Title & Commencement

The instructions set forth herein are titled the "Distributed Ledger Technology (DLT) Guideline" for 2024 and shall enter into force as of 22/07/2024.

2. Definitions

For the purpose of this guideline, the following terms are defined as follows, unless the context otherwise suggests:

S. No.	Term	Explanation
1	Blockchain	A form of DLT where transactions are recorded in blocks of data.
2	Consensus Mechanism	Set of rules used in a DLT environment to find agreement on the current status of the ledger at a specific point in time.
3	Customer	Any natural or legal person who receives services from a DLT Participant.
4	Distributed Ledger	Database where records can be synchronized and updated by a set of Participants, with no need for the central database management system used to validate such updates in traditional databases.
5	Distributed Ledger Technology (DLT) Network	A set of Nodes that share the management of a common set of information, which is recorded in a Distributed Ledger.
6	Entity	An organization regulated by the Qatar Central Bank.
7	Financial Market Infrastructure (FMI)	A systemically important Entity regulated by QCB providing an infrastructure or particular functions e.g., payments, clearing, etc. The FMI may run on existing and legacy IT technologies or any form of DLT.
8	Material DLT	DLT application which: (a) In the event of a service failure or security breach, has the potential to impact an Entity's: (i) business operations, reputation, or profitability or; (ii) ability to manage risk and comply with applicable laws and regulations. (b) Involves Customer information and, in the event of any unauthorized access or disclosure, loss or theft of Customer information, may have a negative impact on an

		Entity’s Customers.
9	Node	Any machine (such as a computer) that is connected to the DLT network.
10	Oracle	A Node of the DLT network that certifies to other Nodes the occurrence of specific events outside the network (e.g., change in asset prices, change in ownership, etc.).
11	Participant	A legal Entity or natural person that connects via a Node to use a Distributed Ledger, and the technology behind it, to manage information.
12	Permissioned Network	A DLT network which can be updated or validated only by authorized Users within set governance rules i.e., special permissions are necessary to read, access or write information on them. Non-Validator Participants must also be authorized.
13	Permissionless Network	DLT network that has no restrictions on participation. Any Entity can become a Participant and join the network as a Validator Node and validate transactions.
14	Qatar	The State of Qatar.
15	QCB	The Qatar Central Bank, which has been established as per the QCB Law.
16	QCB Law	Law of the Qatar Central Bank and the Regulation of Financial Institutions No. (13) of 2012.
17	Register	Inventory of an Entity’s DLT applications.
18	Sector-Specific-Security Regulations	QCB information security regulations that are applicable to Entities operating in a specific financial services sub-sector (e.g. Insurance or Payment Services).
19	Smart Contract	Digital contract which contains algorithms coded to update records when a set of conditions are met.
20	Token	A cryptographically secured digital representation of value, rights or obligations, which may be issued, transferred and stored electronically, using DLT or other similar technology.
21	User	A natural or legal person that has Participant rights in a DLT system.
22	Validator	A Participant that takes part in the consensus process in a DLT network to confirm the validity of an update and to synchronize the information held by its Participants.
23	Wallet (Digital, hot or cold)	Software or hardware that stores private keys used to initiate transactions and provides additional customizable services, e.g., an overview of asset balance and transaction history. Hot wallets are internet-enabled and online, cold wallets are offline and often in the form of a physical device.
24	Zero-day exploit	A Zero-day exploit is a cyberattack technique that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware.

3. Introduction

DLT (of which Blockchain is a particular form but only one of many possible DLT types) is a shared database of records that can be updated by a set of Participants using a Consensus Mechanism, with no need for the central database management system used to validate such updates in traditional databases. The entire newly created business model needs to be assessed to identify risks to an Entity; from very low risk internal administrative processes to highly complex processes.

4. Purpose

4.1 Provide requirements for the oversight of DLT applications or systems provision and usage by all Entities regulated by QCB to ensure their usage is safe, secure, and efficient.

4.2 Allow an Entity flexibility to achieve its objectives based on principles rather than rules, except where requirements are specified.

4.3 Issue specific requirements where relevant. Although this is a guideline, requirements have the same force as a requirement in a QCB issued regulation.

4.4 Set out principles or "best practice standards" that govern the conduct of an Entity who shall make every effort to comply with this guideline as part of their regulatory obligations.

4.5 Set requirements on the way that an Entity should manage its DLT activities and specific DLT types (as outlined in Annexure 1).

5. Scope

5.1 This guideline covers the interaction with or use of DLT by an Entity in any form.

5.2 This guideline is only applicable to an Entity providing or using DLT or an Entity proposing to use DLT.

5.3 QCB strongly encourages Entities to inform QCB of all potential DLT applications. Entities should present fully worked out proposals to QCB.

5.4 Currently, QCB would not permit Permissionless DLT networks.

PART B (GOVERNANCE)

6. Strategy

6.1 An Entity must create a defined DLT strategy based on the Entity's needs and risk appetite. It must also be consistent with the Entity's relevant strategies and internal policies and processes.

6.2 An Entity must conduct a periodic review of its DLT strategy on a timetable consistent with an Entity's goals and risk appetite.

6.3 An Entity should ensure that its strategy provides a business case, addresses information and communication technology requirements, information security, and operational risk management (including business continuity, disaster recovery, and resiliency framework).

6.4 An Entity's DLT strategy should define an implementation plan and architectural roadmap which covers the target IT environment, the transition from the current environment to the target environment and the operating model, including any organizational change or additional skillsets that may be necessary.

6.5 An Entity must allocate sufficient resources to handle any DLT projects and ongoing business needs.

7. Corporate Governance, Internal Controls and Risk Management

7.1 **Board Responsibility**

7.1.1 The Entity's board of directors, and senior management, are accountable for ensuring effective internal controls, audit and risk management practices are implemented to achieve security, reliability and resilience of its information and communication technologies (ICT) operating environment.

7.1.2 The board is responsible for:

7.1.2.1 Approving the level of DLT exposures to be tolerated in the overall risk framework.

7.1.2.2 Deciding whether an Entity's existing governance structures are fit for purpose.

7.1.2.3 Assigning clear lines of accountability and responsibility.

7.2 **Senior Management Responsibility**

7.2.1 Senior management should have one or more members with the knowledge to manage technology risks, ideally including understanding, designing, governing and operating DLT.

7.2.2 Senior management is responsible for the assessment, understanding and monitoring of an Entity's reliance on DLT.

7.2.3 Senior management must provide, to the board, information that is clear, consistent, robust, timely, well-targeted and contains an appropriate level of technical detail to facilitate effective oversight and challenge by the board of DLT issues.

7.2.4 Senior management should establish either a function overseeing DLT and participation in external DLT networks; or delegate its responsibility to an existing function within an Entity.

7.2.5 An Entity shall manage risks associated with the use of DLT within the enterprise Risk Management structure.

7.2.6 An Entity must ensure that DLT applications are auditable by maintaining appropriate evidence and records to enable the Entity's internal control and audit functions, external auditors, regulators, and other authorities to conduct their audits and reviews.

7.2.7 An Entity must ensure that their DLT applications are reviewed by the appropriate internal risk management function prior to launch and monitored to allow real time and periodic summaries and trends to evaluate performance, detect technology and security related incidents, ensure the adequacy of controls, and promptly take any remedial action.

7.2.8 An Entity must update its business continuity plan and periodically test arrangements to maintain the continuity of the service or process performed by the DLT application in the event of an incident that adversely affects the availability of the application.

7.2.9 An Entity must ensure that the adoption of DLT is supported by resources with the necessary skills, knowledge, and expertise specific to their roles and functions. Staff responsible for the operations, management and oversight of innovative technologies should possess the required expertise to ensure ongoing effectiveness (including adequate training and provide educational materials to the staff to strengthen the knowledge of the risks of DLT service).

7.3 <u>Technology Risk Management</u>

7.3.1 An Entity must establish policies, standards, and procedures for all DLT applications, and where appropriate, incorporate industry standards and best practices to manage technology risks and safeguard information assets. The policies, standards and procedures should also be regularly reviewed and updated, taking into consideration the evolving technology and cyber threat landscape.

7.3.2 An Entity's framework must encompass the following components:

7.3.2.1 Risk identification – Identify threats and vulnerabilities to the Entity and information assets.

7.3.2.2 Risk Assessment – Assess the potential impact and likelihood of threats and vulnerabilities to the Entity and information assets.

7.3.2.3 Risk treatment – Implement processes and controls to manage technology risks posed to the Entity and protect the confidentiality, integrity, and availability of information assets.

7.3.2.4 Risk monitoring, review, and reporting – Monitor and review technology risks, which include risks that Customers are exposed to, changes in business strategy, IT systems, environmental or operating conditions, and report key risks to the board of directors and senior management.

7.3.3 An Entity must establish an approved and documented DLT governance framework for effective decision-making as well as proper management and control of risks arising from the use of DLT. The governance framework should:

7.3.3.1 Define the roles and responsibilities of the key groups involved with respect to the design, development, operation, and management of the Distributed Ledger(s). Key groups may include:

i. Core group who will design, govern, and operate the Distributed Ledger(s).

ii. Qualified Users of the Distributed Ledger(s).

iii. Participants involved in the Distributed Ledger(s), such as other regulated Entities.

iv. Third parties including outsourcing service providers such as custodians or software developers involved in delivering the service.

7.3.4 An Entity may use DLT products sourced through a third party, and they will be subject to the DLT assessment process in Section (9):

7.3.4.1 If the third party stores, processes or transmits confidential or sensitive Customer information, the Entity must ensure it is compliant with privacy regulations and its own data controls.

7.3.4.2 If the DLT process is outsourced, compliance with privacy regulations and data controls will apply.

7.3.5 An Entity must adopt a robust set of security and privacy practices:

7.3.5.1 An Entity must conduct vulnerability assessments and penetration tests specific to the DLT application to identify weaknesses and flaws in the security processes.

7.3.5.2 An Entity must manage and monitor information integrity, privacy, and confidentiality in the implementation of the DLT and throughout its lifecycle.

7.3.5.3 An Entity must further ensure adequate control and monitoring of the DLT through a focus on encryption and with a particular focus on key management.

7.3.5.4 An Entity must review the distributed log of records and transactions within the ledger(s) to identify suspicious patterns and connections to monitor any anomalous activity.

7.3.5.5 An Entity must adopt operations security controls including standard infrastructure controls such as virus checking schedules, Zero-day exploit remediation, maintenance schedules, capacity, and backup management.

7.3.5.6 An Entity must adopt security incident management controls that describe the processes around reporting, escalation, and response to any breaches. Entities should monitor the cause if one of the Nodes increases processing power and is executing a significantly higher number of transactions.

7.3.5.7 An Entity should maintain and monitor physical and environmental security through use of hardware security modules, physical security measures such as CCTVs, physical barriers, traditional key security, and access controls.

7.3.6 Internal governance structures and measures shall ensure robust oversight over an Entity's use of DLT. An Entity's existing internal governance structures can be adapted, and new structures can be implemented, if necessary.

7.3.7 An Entity shall manage risks associated with the use of DLT within the enterprise risk management structure.

8. Register

8.1 An Entity must develop a Register with a complete inventory of all DLT applications and maintain it on a regular basis.

8.2 An Entity must disclose the full Register to QCB on an annual basis, and upon request by QCB.

8.3 An Entity should prove its own compliance with its own policies and any externally imposed regulations by recording all relevant activity on an immutable audit trail.

8.4 The Register for each DLT application must include:

8.4.1 Whether each DLT application is built, purchased, licensed, or outsourced.

8.4.2 The Entity will affirm for each DLT application:

8.4.2.1 The nature of the DLT arrangements.

8.4.2.2 The Entity's role.

8.4.2.3 Whether the application is material.

8.4.2.4 A category assigned by the Entity that reflects the nature or functional use of the DLT application.

8.4.3 If the application is purchased, licensed, or outsourced:

8.4.3.1 The name of the provider or outsourcer.

8.4.3.2 The country of registration, local corporate registration number, LEI (where available).

8.4.3.3 Registered address and relevant contact details.

8.4.3.4 Name of its parent company (where applicable).

8.4.3.5 The creation date of the application and all subsequent upgrades.

8.4.3.6 The contract start date (where applicable).

8.4.3.7 The next contract renewal date.

8.4.3.8 Governing law of the provider.

8.4.4 A detailed description of all Material DLT applications.

8.4.5 The date of the most recent risk assessment or audit of each of the Material DLT application together with details of the external audit provider (if any), scope covered, a brief summary of the main results, and the date of the next planned risk assessment or audit.

8.4.6 In relation to finding an alternate provider, if relevant, an Entity must:

8.4.6.1 Assess the DLT's substitutability as easy, difficult, or impossible.

8.4.6.2 Identify an alternate service provider (where possible).

9. DLT Assessment

It is essential that Entities conduct a proper risk assessment when developing, providing, using, or implementing a DLT system. These risks must be clearly identified, mitigated, and monitored throughout the entire life cycle of the DLT use. The Entity must demonstrate that prudential and regulatory requirements are met when using a DLT and that Sector-Specific Security Regulations are followed. When a DLT model is selected, the Entity's control function must:

9.1 Evaluate the model used to operate and manage the Distributed Ledger (e.g., a consortium, a single firm) including:

9.1.1 Rules to govern the ledger(s), including Participant and Validator rules, and restrictions.

9.1.2 Consensus Mechanism approval processes and procedures to grant access to create, read, update or deactivate data stored on the Distributed Ledger(s).

9.2 Ensure integrity of the governance framework in place to manage changes at the DLT level:

9.2.1 The Entity must assess its ability to extend control to the DLT parameters and rules required in order to define the governance model in a consistent manner with its risk management framework.

9.2.2 The Entity must assess the impact of a change of governance on the service delivery.

9.3 Review regulatory and legal issues:

9.3.1 The Entity must verify if any of the DLT application's activities, services or products require licensing, approval, or registration with QCB.

9.3.2 The Entity must identify who is in charge of claims or malfunctions and the applicable jurisdiction.

9.3.3 The Entity must clarify whether it bears any liability and identify the dispute resolution mechanisms that apply.

9.3.4 The Entity must have an analysis or legal opinion as to the legal effects of using this type of DLT and any related Smart Contracts or Tokens.

9.4 Review Distributed Ledger design:

9.4.1 The Entity must ensure the Consensus Mechanism has been tested and validated by qualified internal or external experts for the correctness of operation and any identified shortcomings.

9.4.2 If the DLT uses a proprietary algorithm, the Entity must obtain formal proof of the correctness using test cases under realistic conditions or other methods.

9.4.3 The Entity must assess the DLT architecture to check distribution of transaction processing capacity and that mechanisms exist to assure the sharing of capacity and the quality of service between Participants, by:

9.4.3.1 Ensuring the mechanism will prevent a monopoly or concert control of transaction validation.

9.4.3.2 Testing transaction management in a stress test environment (overload, latency) and documenting any preventive measures.

9.4.4 The Entity must ensure that any DLT application they interact with has appropriate KYC controls and does not allow any anonymous or pseudonymous Users, and that the distributed logs of records and any off-chain records are traceable, and anonymity and pseudonymity is avoided.

9.4.5 The Entity must ensure that Nodes management process is in a Permissioned Network:

9.4.5.1 The Entity must ensure the DLT Node selection and management approach conforms to internal risk management policies.

9.4.5.2 The Entity must ensure the DLT Node software design conforms to internal risk management policies.

9.5 Manage the Smart Contracts Management Process:

9.5.1 The Entity must ensure that the Smart Contract code is properly developed, audited validated and the process documented using current recognized standards and frameworks for Smart Contracts.

9.5.2 The Entity must define a contract deployment strategy considering the authorization process, the continuity and quality of service and the dispute resolution process.

9.5.3 The Entity must define management of risks linked to Oracles management by:

9.5.3.1 Defining the process for the selection and monitoring of Oracles.

9.5.3.2 Defining a remediation process and dispute resolution mechanism in case of failure/ error/ issue.

9.6 Manage the Key Management:

9.6.1 Where the Entity uses public key infrastructure, it must ensure the DLT system has a robust process for key generation to:

9.6.1.1 Generate and deliver the encryption key pairs to the Customer.

9.6.1.2 Protect the data linking the Customer real identity and its public key.

9.6.2 The Entity must analyze and understand the following:

9.6.2.1 Mechanisms for private keys storage and related tools.

9.6.2.2 The Wallet solution and the security measures to prevent theft/corruption/loss of the private keys stored in the Wallet.

9.6.3 The Entity must select or approve the internal or external security solution(s) chosen to protect private keys, whether the Entity self-custodies or appoints a qualified custodian. These solutions should be evaluated considering internal and external security risks.

9.6.4 The Entity must evaluate the appropriateness of the storage solution and consider additional controls, such as utilizing strictly controlled cold Wallets, for higher risk assets.

9.6.5 The Entity must evaluate the procedures and tools in place in case of lost keys or stolen keys and develop key recovery plans.

9.6.6 The Entity must ensure that data is secure and privacy rights are protected by:

9.6.6.1 Setting parameters for type of data that is stored inside and outside of the DLT.

9.6.6.2 Adopting security measures that ensure Customer data is protected under the Law No. (13) of 2016 on Personal Data Privacy Protection.

9.7 Assess the requirements for integrating DLT applications with non-DLT applications.

9.8 The Entity should conduct an operational readiness check, prior to solution go-live. For material risk applications, this should be performed by an independent third party. The Entity should submit this assessment report to QCB for approval.

9.9 Send written notifications to QCB:

9.9.1 An Entity must notify QCB in writing in a timely manner of any planned DLT application and must receive QCB approval prior to use. Any major change in an application is subject to the same requirement.

9.9.2 An Entity must notify QCB in writing immediately if a DLT application is not previously classified as material and becomes classified as material.

10. Outsourcing

10.1 An Entity that outsources any activity to support its operations when developing, providing, using, or implementing a DLT system should ensure regular due diligence on the outsourcing service provider is carried out (identity, legal status, activities, financial position, etc.) and obtain prior consent from QCB.

10.2 An Entity must conduct a due diligence review on the capabilities and expertise of the outsourcing service provider prior to its selection.

10.3 An Entity should conduct a risk assessment of the outsourcing service provider, including the location of the data when it is processed, stored, and transmitted, and any relevant vendor contracted by the third party.

10.4 An Entity must periodically review the suitability and performance of the outsourcing service provider.

10.5 An Entity must obtain approval from its Board of Directors to outsource any function in relation to the use of a DLT and must document it.

10.6 An Entity must put in place proper mechanisms to ensure the confidentiality and security of information that the outsourcing service provider may have access to.

10.7 An Entity must put in place proper reporting and monitoring mechanisms to ensure that the integrity and quality of work conducted by the outsourcing service provider is maintained.

10.8 The external and internal auditors of the Entity must be able to review the accounting records and internal controls of the outsourcing service provider.

10.9 An Entity must also have a contingency plan in the event that the arrangement with the outsourcing service provider is suddenly terminated.

10.10 An Entity must have a service agreement with the outsourcing service provider. The service agreement should be comprehensive and contain at a minimum the following:

10.10.1 The right to monitor and be informed about the third party's compliance with applicable laws, regulations, international standards (wherever applicable) and to require timely remediation if issues arise.

10.10.2 A clause on professional ethics and conduct in performing their duties.

10.10.3 Clearly defined roles and responsibilities of the outsourcing service provider.

10.10.4 Robust confidentiality and security procedures and controls.

10.10.5 Sound business continuity management procedures.

10.10.6 The Entity's right to terminate the services of the outsourcing service provider if it fails to comply with the conditions imposed or is directed by QCB to do so.

10.10.7 Inclusion of exit clauses that ensure any data will be wiped out upon termination of the outsourcing.

10.10.8 The QCB's right to audit the outsourcing service provider's accounts.

10.11 An Entity shall be responsible as the principal for all the acts of omission or commission of their outsourcing service providers.

PART C (COMPLIANCE WITH SECONDARY REGULATIONS)

11. Compliance with Secondary Regulations

Along with the QCB Law and this guideline, the Entity must also comply with the below mentioned secondary regulations, and their subsequent amendments, while operating in Qatar:

11.1 Regulations or guidelines issued by QCB, including those related to related to emerging technology.

11.2 Law No. (13) of 2016 on Personal Data Privacy Protection.

11.3 The Sector-Specific Security Regulations.

11.4 Know Your Customer (KYC), Anti-Money Laundering (AML), Combating Financing of Terrorism (CFT) and Financing of Weapons of Mass Destruction Proliferation:

11.4.1 The provisions of Law no. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

11.4.2 The instructions related to AML/CFT issued in May 2020.

11.4.3 Any other circulations issued by the controllers and law enforcement bodies in Qatar must be implemented by all Entities.

11.5 E-KYC Regulation, in the event an Entity on boards Customers digitally.

11.6 Technology Risks Circular of January 2018 issued by QCB.

11.7 Cloud Computing Regulation, if the Entity is looking to adopt cloud computing deployments.

Annexure 1: Taxonomy of DLT Structures in Financial Services and Related Use Cases

This Part of the guideline provides a roadmap to categorize the various types of DLT systems based on a number of key variables within an overall governance framework. The focus is firstly on the governance and control of the DLT systems and only then considers the technical issues of each system.

Annexure 1 sets out the types of DLT an Entity may run or join. For each type, it looks at the issues of concern about DLT to be addressed before the detailed technical analysis becomes the focus. These issues primarily comprise the risk assessment of the basic risk level of the type of project, which parties are running the system (solely or jointly), which parties can participate in the system at all, the basis of voting rights on the Nodes and Consensus Mechanism both for individual transactions and the DLT as a whole. Addressing these issues can be very complicated but it must be done before focusing on the technical aspects of the DLT itself.

General types of DLT applications:

- An internal tool.
- An Entity becomes a Participant in a Permissioned Network.
- An Entity sets up a Permissioned Network.
- An Entity becomes a Participant in a Permissionless Network.
- An Entity sets up a Permissionless Network.

For any use-case that does not match the types of DLT applications above, an Entity shall apply relevant principles from the closest type and demonstrate caution in the approach taken.

The following provide detailed guidelines for each of the DLT application types and further details are available in the flow chart in Annexure 2.

DLT application as an internal tool:

- The following would apply to internal tools handling administrative tasks as well tools for evaluating risk in financial assets and transaction businesses
- Any such system must go through the DLT assessment laid out in Section (9).
- From a governance perspective, rules need to be in place to determine level of access required to make entries and the controls for approving any changes (the Consensus Mechanism). Standard protocols about access and security would be applied. Where a non-DLT system would have strict access controls and multiple levels of oversight and independent validation, the DLT system has to ensure such controls are also present and effective.
- An internally developed system will have been subject to the Entity's Technology Risk Management Framework. At that point, the specific processes of Section (7) will be implemented. When deploying externally created DLT applications, a more extensive assessment, validation and testing should be applied.
- An Entity must disclose all existing applications to QCB, and QCB will determine the approval process for the continuing use or termination of existing DLT applications. In due course, it may be possible to develop preapproved lists of specific DLT applications or DLT applications based on specific technical or other parameters.
- Any new DLT application must be disclosed to QCB and approved prior to solution go-live.

Where an Entity becomes a Participant in a Permissioned Network:

- This area will cover the vast majority of external DLT activities: many will be a replication of current regulated activities, and some will be wholly novel, or with regulated Participants, or with unregulated Participants or both, and some established by an unregulated DLT administrator.
- A Permissioned Network presents three main types:
  - Type 1: Where the DLT network is part of an inherently regulated activity (e.g., an FMI).
  - Type 2: Where a single firm runs the network (Participants have no rights in the Consensus Mechanism process), that firm may be regulated or unregulated.
  - Type 3: Where the DLT network is run by one or more regulated Entities, run by unregulated firms, or both and whether the relevant Entity is a co-sponsor of the network.

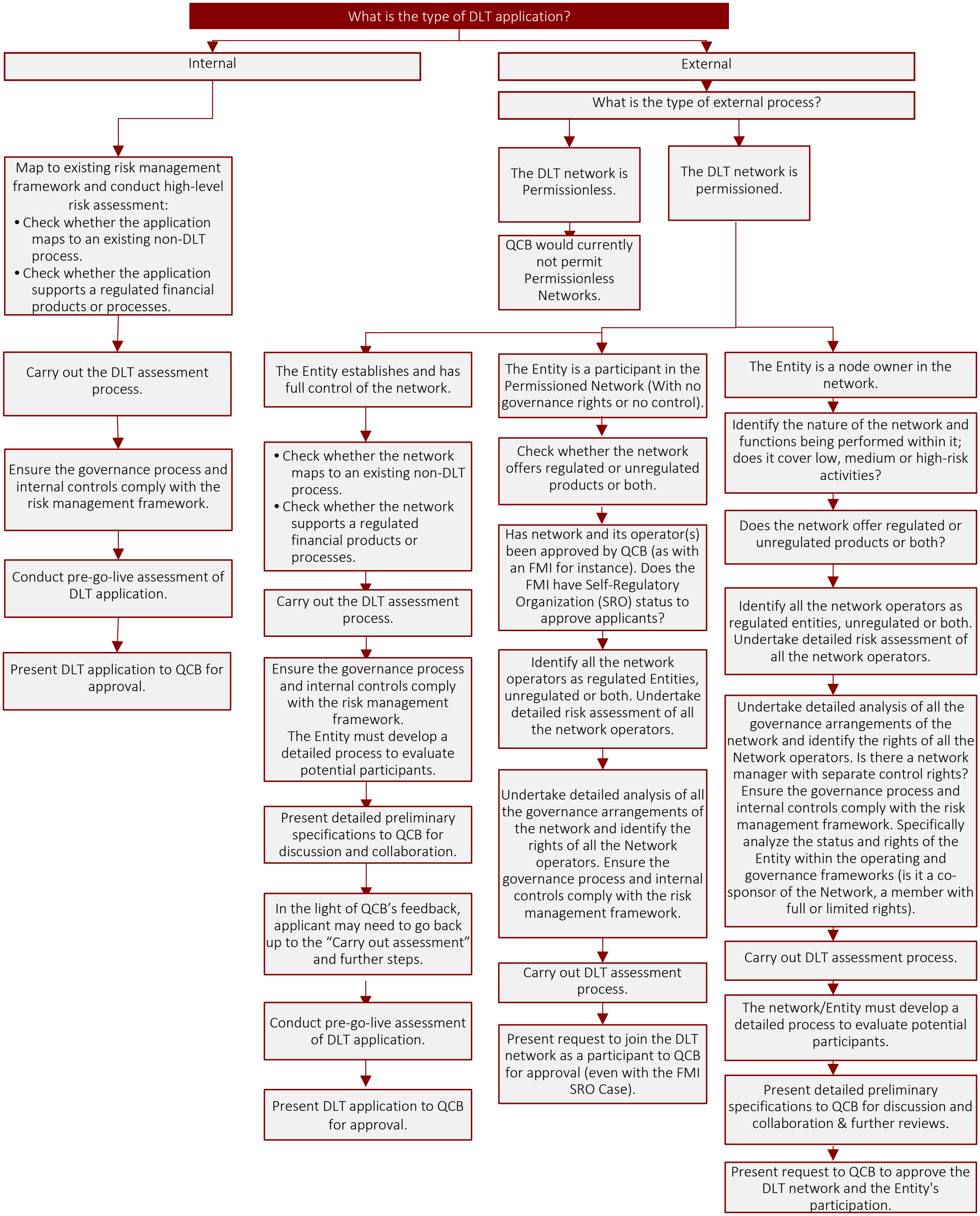
An Entity sets up a DLT network interacting with Customers:

- This is essentially a subset of "Where a single Entity sets up a Permissioned Network" and will largely be focused on putting existing Customer products and information onto DLT applications.
- It will be important in anything of this nature to closely adhere to the relevant Customer protection, privacy rights, and ensure transparency of fees and costs, technology risks and asset protection.

An Entity becomes a Participant in a Permissionless Network or sets up a Permissionless Network:

- Currently, QCB would not permit Permissionless DLT networks.

Annexure 2: DLT Assessment at an Application & Entity Level



What is the type of DLT application?

Internal

Map to existing risk management framework and conduct high-level risk assessment:
- Check whether the application maps to an existing non-DLT process.
- Check whether the application supports a regulated financial products or processes.

Carry out the DLT assessment process.

Ensure the governance process and internal controls comply with the risk management framework.

Conduct pre-go-live assessment of DLT application.

Present DLT application to QCB for approval.

External

What is the type of external process?

The DLT network is Permissionless.

QCB would currently not permit Permissionless Networks.

The DLT network is permissioned.

The Entity establishes and has full control of the network.

- Check whether the network maps to an existing non-DLT process.
- Check whether the network supports a regulated financial products or processes.

Carry out the DLT assessment process.

Ensure the governance process and internal controls comply with the risk management framework. The Entity must develop a detailed process to evaluate potential participants.

Present detailed preliminary specifications to QCB for discussion and collaboration.

In the light of QCB's feedback, applicant may need to go back up to the "Carry out assessment" and further steps.

Conduct pre-go-live assessment of DLT application.

Present DLT application to QCB for approval.

The Entity is a participant in the Permissioned Network (With no governance rights or no control).

Check whether the network offers regulated or unregulated products or both.

Has network and its operator(s) been approved by QCB (as with an FMI for instance). Does the FMI have Self-Regulatory Organization (SRO) status to approve applicants?

Identify all the network operators as regulated Entities, unregulated or both. Undertake detailed risk assessment of all the network operators.

Undertake detailed analysis of all the governance arrangements of the network and identify the rights of all the Network operators. Ensure the governance process and internal controls comply with the risk management framework.

Carry out DLT assessment process.

Present request to join the DLT network as a participant to QCB for approval (even with the FMI SRO Case).

The Entity is a node owner in the network.

Identify the nature of the network and functions being performed within it; does it cover low, medium or high-risk activities?

Does the network offer regulated or unregulated products or both?

Identify all the network operators as regulated entities, unregulated or both. Undertake detailed risk assessment of all the network operators.

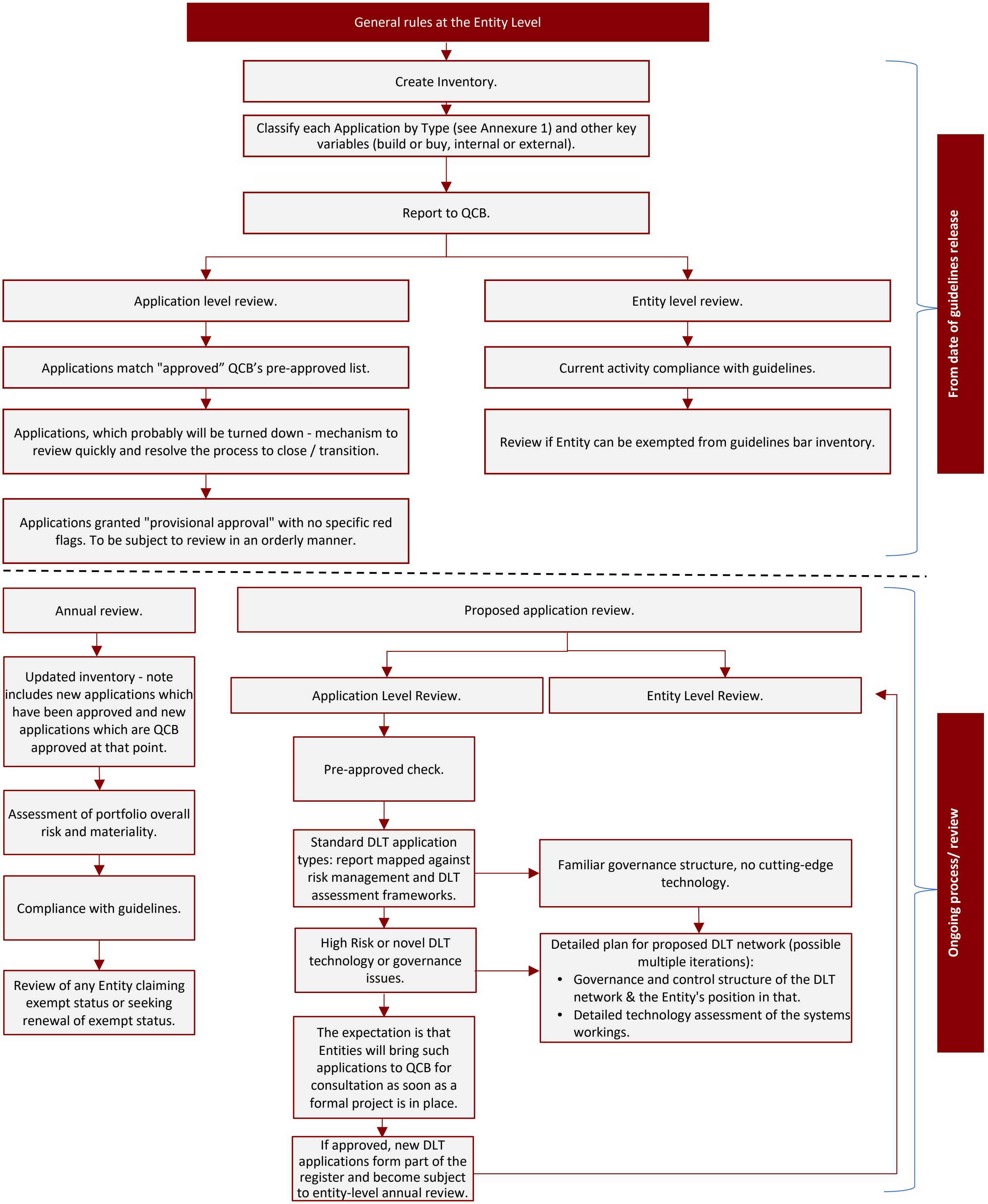
Undertake detailed analysis of all the governance arrangements of the network and identify the rights of all the Network operators. Is there a network manager with separate control rights? Ensure the governance process and internal controls comply with the risk management framework. Specifically analyze the status and rights of the Entity within the operating and governance frameworks (is it a co-sponsor of the Network, a member with full or limited rights).

Carry out DLT assessment process.

The network/Entity must develop a detailed process to evaluate potential participants.

Present detailed preliminary specifications to QCB for discussion and collaboration & further reviews.

Present request to QCB to approve the DLT network and the Entity's participation.



General rules at the Entity Level

Create Inventory.

Classify each Application by Type (see Annexure 1) and other key variables (build or buy, internal or external).

Report to QCB.

Application level review.

Applications match "approved" QCB's pre-approved list.

Applications, which probably will be turned down - mechanism to review quickly and resolve the process to close / transition.

Applications granted "provisional approval" with no specific red flags. To be subject to review in an orderly manner.

Entity level review.

Current activity compliance with guidelines.

Review if Entity can be exempted from guidelines bar inventory.

From date of guidelines release

Annual review.

Updated inventory - note includes new applications which have been approved and new applications which are QCB approved at that point.

Assessment of portfolio overall risk and materiality.

Compliance with guidelines.

Review of any Entity claiming exempt status or seeking renewal of exempt status.

Proposed application review.

Application Level Review.

Pre-approved check.

Standard DLT application types: report mapped against risk management and DLT assessment frameworks.

High Risk or novel DLT technology or governance issues.

The expectation is that Entities will bring such applications to QCB for consultation as soon as a formal project is in place.

If approved, new DLT applications form part of the register and become subject to entity-level annual review.

Entity Level Review.

Familiar governance structure, no cutting-edge technology.

Detailed plan for proposed DLT network (possible multiple iterations):

- Governance and control structure of the DLT network & the Entity's position in that.
- Detailed technology assessment of the systems workings.

Ongoing process/ review