Guidelines for Financial Institutions adopting Enabling Technologies

Central Bank of the UAE

Securities and Commodities Authority

Dubai Financial Services Authority

Financial Services Regulatory Authority

Contents

Introduction 3
Objectives 3
Structure of the Guidelines 4
Scope of Application 4
Section 1: Definitions 5
Section 2: Key Principles for adopting Enabling Technologies 11
Key Principles for all Enabling Technologies 11
Application Programming Interfaces (APIs) 11
Cloud Computing 12
Biometrics 12
Big Data Analytics and Artificial Intelligence (AI) 13
Distributed Ledger Technology (DLT) 13
Section 3: Guidelines for adopting Enabling Technologies 15
Application Programming Interfaces (APIs) 15
Cloud Computing 19
Biometrics 28
Big Data Analytics and Artificial Intelligence (AI) 30
Distributed Ledger Technology (DLT) 35
Section 4: Interpretation 41

Introduction

The Central Bank of the UAE (CBUAE), together with the Securities and Commodities Authority (SCA), the Dubai Financial Services Authority (DFSA) of the Dubai International Financial Centre and the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market, collectively referred to as "Supervisory Authorities", have issued the "Guidelines for Financial Institutions adopting Enabling Technologies" ("the Guidelines").

The Guidelines are issued pursuant to the powers vested in the respective law of the individual Supervisory Authorities, including:

- The Central Bank of the UAE under the Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities ("Central Bank Law");
- The Securities and Commodities Authority under Federal Law No. (4) of 2000 concerning the Emirates Securities and Commodities Authority and Market;
- The Dubai Financial Services Authority pursuant to the Regulatory Law - DIFC Law No. (1) of 2004 concerning Dubai International Financial Centre; and
- The Financial Services Regulatory Authority pursuant to Law No. (4) of 2013 concerning Abu Dhabi Global Market.

The increasing adoption of technology-enabled business models presents both opportunities and challenges to those carrying out Innovative Activities.

The purpose of the Guidelines is to provide a set of principles when using Enabling Technologies in financial services and accompanying guidance. The key principles are broad enough to cater to the different business models, operating models and financial services offered by existing organisations operating in, and new entrants to, the financial services sector. The key principles are accompanied by more detailed guidance for Institutions to consider when using Enabling Technologies.

The Supervisory Authorities may issue further guidance relating to the Guidelines.

Objectives

The objectives of the Guidelines are:

- To provide Institutions with best practices on risk management in respect to Enabling Technologies;
- To encourage the safety and soundness of Institutions so that relevant risks arising from innovative business models and services are adequately managed and mitigated;
- To limit the systemic risks that could arise from the use of innovative technology, thus fostering transparency and financial stability;
- To provide guidance on how to manage the risks when adopting Enabling Technologies to deliver more efficient, secure and robust solutions to Customers thereby improving organisational efficiency and financial inclusion; and
- To promote the growth and advancement of the UAE financial services sector and encourage adoption of Innovative Activities in the UAE whilst managing risks in a proportionate manner.

Structure of the Guidelines

The Guidelines are divided into the following sections:

- Section 1: Provides definitions of the key terms used throughout the Guidelines;
- Section 2: Sets out the key principles relating to the adoption and use of different types of Enabling Technologies; and
- Section 3: Provides guidance on the application of the key principles covering the use of Application Programming Interface (API), Cloud Computing, Biometrics, Big Data Analytics and Artificial Intelligence (AI), and Distributed Ledger Technology (DLT).

Scope of Application

The Guidelines are applicable to all Institutions licensed and supervised by the Supervisory Authorities that are using, or intend to use, Enabling Technologies. Institutions are expected to consider the application of the Guidelines to their business activities in a manner that reflects the size and complexity of the Institution and the nature, scope, risk level, complexity and materiality of their Institution's Innovative Activities. They are in addition to any binding regulations, standards, guidance, and other instructions issued by the relevant Supervisory Authorities, which shall take precedence over the Guidelines.

Section 1: Definitions

In the Guidelines, words and expressions have the meanings set out below. :

Term	Definition
Application Programming Interface (API)	A set of rules and specifications for software programs to communicate with each other that forms an interface between different programs to facilitate their interaction. There are various types of APIs which include: • Private APIs: used within an organisation to provide interoperability between internal applications in order to help automation and provide flexibility. • Partner APIs: used to integrate software between a company and its partner, often for a very specific purpose such as providing a product or service. • Open APIs: Designed to be easily accessible by the wider population, regardless of whether a business relationship has been established or not. This term does not have the same meaning as "Open Banking". • Composite APIs: Designed to batch API requests sequentially into a single API call combining different data and service APIs with the aim to improve efficiency.
API Lifecycle	Refers to the phases of: • Conception: the formulation and design of an API; • Production: the development and testing of an API; • Publishing: the steps taken to make an API available for use; • Consumption: the use of an API; and • Retirement: the withdrawal of an API from use.
API Provider	An organisation that makes APIs available for use by organisations or persons, including by the organisation itself.
Application	Refers to the use of an Enabling Technology in any capacity by an Institution, including where the Institution outsources part or all of the use of that Enabling Technology.
Artificial Intelligence (AI)	Refers to the theory and development of computer systems able to perform tasks that traditionally use human intelligence.

Term	Definition
Big Data Analytics	Using advanced analytics techniques in relation to a large volume of Data, generated by any means and stored in a digital format.
Biometrics	Automated recognition of individuals based on their biological and behavioral characteristics. It covers a variety of technologies in which unique, identifiable attributes of people are used for identification and authentication. These include, but are not limited to, a person's fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals. Biometric attributes are based on an individual's personal biometric characteristics and typically include the use of one of the following: • Biophysical: Biometric attributes, such as fingerprints, iris print, voiceprints, and facial recognition; • Biomechanical: Biometric attributes that are the product of unique interactions of an individual's muscles, skeletal system and nervous system, such as keystroke mechanics; or • Behavioral: Biometric attributes that consist of an individual's various patterns of movement and usage, such as an individual's email or text message patterns, mobile phone usage, geolocation patterns, file access log etc. Biometrics can be used for the following activities, amongst others: • Facilitating Customer identification and verification at on-boarding and for ongoing Customer authentication; • Supporting ongoing due diligence and scrutiny of transactions throughout the course of the business relationship; • Providing better and focused Customer services, e.g. identifying regular Customers at the point of entrance and authenticating transactions; and • Aiding transaction monitoring for the purposes of detecting and reporting suspicious transactions, as well as, general risk management and anti-fraud efforts.
Cloud Computing	Use of a network ("cloud") of hosting processors to increase the scale and flexibility of computing capacity. Such a network could be built by an Institution or made available by a service provider. This model enables on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage facilities, applications and services).

Term	Definition
Customer	Customer includes: • In respect of the CBUAE: A person who is using, or who is or may be contemplating using, any of the services provided by an Institution. • In respect of the SCA: A natural or legal person. • In respect of the DFSA: A Retail Client, Professional Client or Market Counterparty. • In respect of the FSRA - A "Customer".
Credential Service Provider	An organisation that issues and/or registers authenticators and corresponding electronic credentials (binding the authenticators to the verified identity) to subscribers. Credential Service Provider's maintain a subscriber's identity credential and all associated enrolment Data throughout the credential's lifecycle and provide information on the credential's status to verifiers.
Data	A collection of organised information, facts, concepts, instructions, observations or measurements, in the form of numbers, alphabets, symbols, images or any other form, that are collected, produced, or processed by Institutions.
Digital Channels	The internet, mobile phones, Automated Teller Machines (ATMs), Point of Sale (POS) terminals, Digital Personal Assistants (DPAs), mobile applications, or other similar means for Institutions to contact other organisations or persons.
Distributed Ledger Technology (DLT)	Processes and related technologies that enable Nodes in a network (or arrangement) to securely propose, validate, agree and record state changes (or updates) to a synchronised ledger that is distributed across the network's Nodes. Blockchain is a type of DLT which stores and transmits Data in packages called "blocks" that are connected to each other in a digital 'chain'.
Enabling Technology	One of the following types of technologies: • APIs; • Cloud Computing; • Biometrics; • Big Data Analytics; • AI; and • DLT.

Term	Definition
Fee	Any fees, charges, penalties and commissions incurred on a product and/or service.
Guidelines	Refers to these Guidelines.
Governing Body	Governing Body means an Institution's Board of Directors, partners, committee of management, or any other form of the governing body of a body corporate or partnership.
Identity Lifecycle	Refers to the phases of: • Enrolment: collecting and proofing identity data; • Issuance: issuing one or more credentials; • Use: checking identity at the point of transactions; • Management: maintaining identities and credentials; and • Retirement: removing the identity record.
Innovative Activities	Technologically enabled provision of financial services which can take various forms and encompass the different sectors of the financial industry (e.g., crowdfunding, payment services).
Institution	An Institution includes: • In respect of the CBUAE: Any licensed and supervised Financial Institution. All references to Institutions include any Outsourcing Service Providers acting on behalf of the Institution. • In respect of the SCA: Any entity that has obtained a license or approval to engage in a financial activity and / or provide a specific financial service. • In respect of the DFSA: Any licensed and supervised "Authorised Person". All references to Institutions include any Outsourcing Service Providers acting on behalf of the Authorised Person. • In respect of the FSRA: Any "Authorised Person" or "Recognised Body".
IT Assets	Any form of information technology, including software, hardware and Data.

Term	Definition
Machine Learning	Machine Learning is a sub-category of AI that is a method of designing a sequence of actions for the design and generation or development of AI models to solve a problem through learning and experience and with limited or no human intervention.
Multi-Factor Authentication	Combines use of two (2) or more of the following authentication factors to verify a user's identity: • knowledge factor - "something an individual knows"; • possession factor - "something an individual has"; and/or • biometric factor - "something that is a biological and behavioral characteristic of an individual".
Nodes	Network participants in a DLT network.
Outsourcing	An agreement with another party either within or outside the UAE, including a party related to an Institution, to perform an activity, process or service on a continuing basis which currently is, or could be, undertaken by the Institution itself. The activity, process or service should be integral to the provision of a financial service or should be provided to the market by the Outsourcing Service Provider on behalf of and in the name of the Institution.
Outsourcing Service Provider (OSP)	A third-party entity that is undertaking an outsourced activity, process or service or parts thereof, under an outsourcing arrangement. The Institution using an Outsourcing Service Provider always remains responsible and accountable for the actions of that OSP under an outsourcing arrangement and to ensure that its outsourcing arrangements comply with the principles set out in these Guidelines.
Permissioned DLT	A distributed ledger which can be updated or validated only by authorised users within set governance rules i.e. special permissions are necessary to read, access or write information on them.
Permissionless DLT	A distributed ledger which can be read or updated by anyone, such as an open-access blockchain used for some cryptocurrencies.
Personal Data	Personal Data is any information relating to an identified natural person or identifiable natural person. "Identifiable natural person" is defined as a natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their biological, physical, Biometric, physiological, mental, economic, cultural or social identity.

Term	Definition
Senior Management	Senior Management includes: • In respect of the CBUAE: The executive management of the Institution responsible and accountable to the Board/Governing Body for the sound and prudent day-to-day management of the Institution, generally including, but not limited to, the chief executive officer, chief financial officer, chief risk officer and heads of the compliance and internal audit functions. • In respect of the SCA: A director or group of executives who assume the tasks of planning the daily administrative and supervisory operations of the company's business to achieve its goals and is appointed by the company's Board/Governing Body. • In respect of the DFSA: Includes any senior management and Governing Body within an Authorised Person who take responsibility for that Authorised Person's arrangements and operations. • In respect of the FSRA: - "Senior Management".
Staff	One or more employee(s) of the Institution acting in any capacity for or on behalf of the Institution.
Subscriber	A person whose identity has been verified and bound to authenticators (credentialed) by a Credential Service Provider.
Supervisory Authorities	Refers to the following UAE authorities: • The Central Bank of the UAE (CBUAE); • The Securities and Commodities Authority (SCA); • The Dubai Financial Services Authority (DFSA) of the Dubai International Financial Centre; and • The Financial Services Regulatory Authority (FSRA) of the Abu Dhabi Global Market.
Third Party	Any person, group of persons or organisation external to and not a related party to an Institution.

Section 2: Key Principles for adopting Enabling Technologies

Key Principles for all Enabling Technologies

2.1 Data Protection: Institutions are required to comply with all applicable legislation and regulations in relation to Data protection when handling the use, transmission, and storage of Data.

2.2 Control Functions: Institutions should have effective audit, compliance and risk management functions that are equipped with the relevant expertise for reviewing and assessing the adequacy of the internal control environment for implementing the Enabling Technologies.

2.3 Independent Review: Institutions should ensure that formal, independent reviews/audits of Enabling Technologies are carried out periodically, the regularity of which will depend on the nature, scope, complexity and materiality of the Institution's technology framework. These reviews should be conducted by the internal audit function and/or third party/external auditors that can provide independent, timely assurance in respect of an Institution's Enabling Technologies, including compliance with relevant internal policies. While Institutions may co-source or outsource the audit activities surrounding their innovative technology, they are expected to ensure that the OSP has a solid understanding of their operations, an appreciation of the existing and potential risks and knowledge of the controls required to remain in compliance with all applicable laws and regulations.

2.4 Skills, Knowledge and Expertise: Institutions should ensure that their adoption of Enabling Technologies 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 and that the technologies continue to meet intended outcomes. Institutions should ensure that they continue to develop specialist expertise relative to the technologies adopted.

2.5 Training: Given the rapid developments in respect of Enabling Technologies, Institutions should ensure that adequate training is provided to the relevant staff for handling Enabling Technologies.

Application Programming Interfaces (APIs)

2.6 Governance: Institutions should establish an approved and documented governance framework for effective decision-making and the proper management and control of risks arising from the use of APIs.

2.7 Design: Institutions should ensure that APIs, whether designed in-house or by a Third Party, are designed such that the APIs can flexibly evolve and have robust controls to support cybersecurity, cyber resilience, and data protection.

2.8 Management and Monitoring: Institutions should establish an approved and documented API monitoring framework that addresses infrastructure, technology and security-related incidents and events in a timely and effective manner.

2.9 Outsourcing: Where an Institution outsources API development to an Outsourcing Service Provider, the Institution must follow the outsourcing requirements of the relevant Supervisory Authority. Institutions should ensure that the contract governing the arrangement between the Institution and Outsourcing Service Provider contains at a minimum information on the roles and

obligations of all parties, liability, dispute management, access to relevant information by the relevant Supervisory Authority, and minimum control measures to be employed by the OSP that are acceptable to the Institution.

2.10 Business Continuity: Institutions should sufficiently cover APIs and the related security controls in their business continuity plans. Institutions should also assess the criticality of different types of APIs being used and ensure that the business continuity planning scenarios reflects them.

Cloud Computing

2.11 Material Arrangements: Institutions should assess the materiality and the associated risks of their Cloud Computing arrangements and address any concerns and expectations that the relevant Supervisory Authority may have prior to implementing any material Cloud Computing arrangement.

2.12 Governance: Institutions should establish an approved and documented governance framework for effective decision-making and proper management and control of risks arising from the use of Cloud Computing and Outsourcing to Outsourcing Service Providers.

2.13 Auditability: Institutions should ensure that the Cloud Computing arrangement is auditable by maintaining appropriate evidence and records to enable the Institution's internal control functions, external auditors, regulators, and other authorities to conduct their audits and reviews.

2.14 Outsourcing: Institutions should establish an approved and documented governance framework for Outsourcing their Cloud Computing arrangements to appropriately select and monitor vendors as well as mitigate risks arising from Cloud Computing Outsourcing arrangements.

2.15 Design: Institutions should implement adequate measures that are commensurate with the materiality of the arrangement to ensure that Cloud Computing arrangements are resilient, secure, recoverable, and meet the capacity and other needs of the Institution.

2.16 Management and Monitoring: Institutions should regularly monitor their Cloud Computing arrangements, to evaluate performance, detect technology and security related incidents, and promptly take any remedial action.

2.17 Data Protection: Institutions should ensure that the use, transmission and storage of Data in a Cloud Computing arrangement complies with applicable laws and regulations and is secured from unauthorised access, use or modification to the extent commensurate with the importance of the Data.

2.18 Business Continuity: Institutions should put in place a robust and regularly tested business continuity plan for each material Cloud Computing arrangement and ensure that the plan complies with the relevant Supervisory Authority's requirements.

2.19 Exit and Resolution Planning: Institutions should define and maintain specific exit plans for their material outsourced Cloud Computing arrangements and account for these arrangements when developing recovery and resolution plans.

Biometrics

2.20 Governance: Institutions should establish an approved and documented governance framework to control and manage the broad range of risks which may arise from the use of Biometrics.

2.21 Identity Proofing and Enrolment Management: Institutions should establish appropriate identity verification and proofing mechanisms as part of the Biometrics Application's identity enrolment process.

2.22 Ongoing Authentication: Institutions should establish controls and processes to protect the customers and their credentials against vulnerabilities and unauthorised access, disclosure or use in the authentication process and throughout the Identity Lifecycle.

2.23 Management and Monitoring: Institutions should regularly monitor their Biometrics Applications throughout the Identity Lifecycle to evaluate performance, detect security-related events, ensure the adequacy of controls, and promptly take any remedial action.

2.24 Data Management: Institutions should ensure the security, confidentiality, authenticity, and integrity of Data throughout all phases of authentication and whether the Data is in use, storage, or transmission.

Big Data Analytics and Artificial Intelligence (AI)

2.25 Governance: Institutions should establish an approved and documented governance framework for effective decision-making and proper management and control of risks arising from the use of Big Data Analytics and AI.

2.26 Accountability: The Governing Body and Senior Management of the Institution should remain accountable for the outcomes and decisions of their Big Data Analytics and AI Applications including those Applications that make decisions on behalf of the Institutions.

2.27 Design: Institutions should ensure that the models for their material Big Data Analytics and AI Applications are reliable, transparent, and explainable, commensurate with the materiality of those Applications.

2.28 Management and Monitoring: Institutions should establish an approved and documented framework to review the reliability, fairness, accuracy and relevance of the algorithms, models and Data used prior to deployment of a material Big Data Analytics and AI Application and on a periodic basis after deployment, to verify that the models are behaving as designed and intended.

2.29 Ethics: Institutions should ensure that their Big Data Analytics and AI Applications promote fair treatment, produce objective, consistent, ethical, and fair outcomes and are aligned with the Institutions' ethical standards, values and codes of conduct.

2.30 Customer protection: Institutions should be transparent with Customers about their use of Big Data Analytics and AI through their conduct and through accurate, understandable, and accessible plain language disclosure.

Distributed Ledger Technology (DLT)

2.31 Governance: Institutions should establish an approved and documented governance framework for effective decision-making and proper management and control of the risks arising from the use of DLT.

2.32 Auditability: Institutions should ensure that the DLT Application is auditable by maintaining appropriate evidence and records to enable the Institution's internal control functions, external auditors, regulators, and other authorities to conduct their audits and reviews.

2.33 Design: Institutions should design their DLT Applications to be efficient and effectively secure IT Assets and any Customer assets.

2.34 Anonymity and Pseudonymity: Institutions developing Permissionless DLT Applications should ensure that users are not anonymous or pseudonymous.

2.35 Management and Monitoring: Institutions should ensure that their DLT Application are reviewed and monitored on a periodic basis to evaluate performance, detect technology and security related incidents, ensure the adequacy of controls, and promptly take any remedial action.

2.36 Business Continuity: Institutions should establish an effective business continuity plan to ensure and periodically test arrangements to maintain the continuity of the service/process performed by the DLT Application in the event of an incident that adversely affects the availability of the Application.

Section 3: Guidelines for adopting Enabling Technologies

Application Programming Interfaces (APIs)

Governance

3.1 Institutions should establish a documented governance framework for effective decision-making and proper management and control of risks arising from the use of APIs. The governance framework should:

a. Define the roles and responsibilities of the Institution, API Provider and API developer (where different), including the division of duties;

b. Establish appropriate policies, procedures, standards and controls to govern the API Lifecycle within the Institution;

c. Employ tools and technologies that enable communication, change management and performance monitoring across the API Lifecycle;

d. Establish appropriate testing strategies prior to publication and on an ongoing basis for optimal performance of APIs, for example:

i. A load testing strategy which can be used to assess how the API performs against service-level agreements and to determine what response is normal for the API. Target API test case problems that would prevent longer load tests from running correctly should be developed;

ii. Stress testing of the APIs that can be undertaken by simulating a heavy load on the API or by conducting crash point testing to identify the maximum number of users the API can handle; and

iii. A monitoring framework that can ensure critical interfaces and functions to be appropriately tested and verified for conformance to expected behavior;

e. Establish a framework to assess, monitor, report and mitigate risks associated with the APIs including developing mechanisms to ensure regular testing and implementation of coding controls, production monitoring and support post deployment, process control mapping and development of a risk control matrix; and

f. Be approved by the appropriate Governing Body.

3.2 When Outsourcing to an Outsourcing Service Provider, Institutions should ensure that access to information is adequately controlled, monitored, reviewed and audited by the Institution's internal control functions, and regulators, including the appropriate Supervisory Authority;

3.3 Business continuity plans of an Institution should cover APIs and the security controls associated with APIs. Institutions should assess criticality of the different types of APIs used and ensure that the business continuity planning scenarios cover the various types of APIs being used. The business continuity strategy and arrangements should be updated when changes are made to the operating environment, and most importantly, be tested periodically.

Architecture

3.4 Institutions should ensure that the systems and technology architecture for the APIs are designed such that the APIs can flexibly evolve. This could be done by making the architecture independent from the applications using the APIs (i.e. such that it is not over tailored to the most common use cases). The evolution of APIs should not hinder existing applications, which should be able to function without interruption.

3.5 Institutions should establish controls so that the architecture supporting the API and the API itself is secure and protected against misuse or security attacks.

Design

3.6 When determining the design of an API, Institutions may consider the following elements to deliver innovation and flexibility:

a. Accessibility: Ensure all relevant parties can access the API;

b. Interoperability: Enable exchange of Data across Institutions without any dependencies on underlying technologies;

c. Reuse: Leverage existing standards and taxonomies to avoid duplication of effort;

d. Independence: Avoid dependency on any vendors or technologies and retain various options for delivery models and implementation technologies;

e. Extensibility: Establish flexibility to extend APIs to new stakeholders and business channels and offer new functionality in existing APIs;

f. Stability: Ensure consistency in functionality and accessibility when modifying the API through appropriate governance;

g. Privacy by design: All APIs should be designed in a way to only expose relevant Data elements to any party in order to fulfil the purpose of the API;

h. Transparency: Promote transparency and clarity on the API, including environments supported, changes implemented, and standards followed; and

i. Loosely coupled: Provide flexibility and minimise impact of changes to operations of other APIs or API applications.

3.7 Institutions should have proper engagement with API Providers before API Providers can expose any Personal Data through the APIs. This engagement should cover the onboarding of and due diligence processes on the API Provider.

3.8 Institutions should undertake the following steps when designing APIs:

a. Decide on in-house vs outsourced API development;

b. Prioritise and sequence APIs to publish;

c. Consider guiding principles such as openness, usability and interoperability;

d. Ensure that adequate security and Data protection mechanisms are in place to protect Personal Data; and

e. Identify and define requirements and technical guidelines.

3.9 During the development of APIs, Institutions and API Providers should ensure that they:

a. Adopt the appropriate API design model based on the type of the API and the protocol used;

b. Develop requirements and technical specification that define the output to be achieved by the APIs and how the APIs should perform their expected functionality from a technical perspective; and

c. Document these requirements and technical specifications so that the behavior of the API is well understood and can be measured against expected behavior.

3.10 Institutions should ensure that Personal Data being transmitted or stored is encrypted to enable privacy and integrity of Data. Institutions can consider utilizing secure public/private key based encryption methods and protocols, which should comply with internationally recognised and applicable security standards.

3.11 Institutions should ensure that access management and authentication processes are used so that only authorised and authenticated individuals and organisations have controlled access to the appropriate API resources.

3.12 Institutions should ensure that authentication mechanisms are implemented effectively and securely, preventing attackers from compromising authentication tokens, or exploiting implementation flaws to assume other user identities temporarily or permanently.

3.13 Institutions should develop an appropriate infrastructure to manage and securely store access credentials.

3.14 Institutions should use Multi-Factor Authentication when a Customer initially accesses an online service that uses APIs, to provide secure access to the account.

3.15 Institutions should consider using Multi-Factor Authentication when a customer uses an API to access, process or transmit Personal Data. Multi-Factor Authentication may also be considered for the initiation or processing of transactions.

3.16 Institutions should ensure that they create clear access control policies that separate administrators and regular users and that accurately reflect the hierarchies, groups, and roles within the organisation. Institutions should review their internal hierarchies, groups, and roles to ensure that there are no gaps in the roles that could lead to unauthorized access to the APIs.

3.17 Institutions should ensure that APIs are designed to impose restrictions on the size or number of resources that can be requested by the user to prevent Denial of Service (DoS) attacks.

3.18 An independent function or external expert with adequate skills and knowledge should conduct vulnerability assessments and penetration tests on the Institution's and the API Provider's systems and infrastructure to identify weaknesses or flaws in the security processes at least on an annual basis.

Standardisation

3.19 Institutions should consider the adoption of standardised APIs that are issued either by Supervisory Authorities or the industry. Standardised APIs can, among other matters, include the following:

a. API design standards: Adopting a uniform API design model and language across the relevant financial services industry based on a broad range of design considerations;

b. Data standards: Adopting international Data standards that define the semantics and syntax of Data being transmitted using APIs, based on the type of Data being transacted and the use case, to promote interoperability; and

c. Information security standards: Adopting international information security standards to ensure information is securely transmitted through APIs.

Management

3.20 Institutions should consider establishing an API monitoring framework that addresses infrastructure, technology and security related incidents and events in a timely and effective manner. The monitoring framework should:

a. Define what constitutes an incident/event, such as unusual activity or unauthorised changes;

b. Monitor the use of APIs to rapidly and accurately detect incidents and events;

c. Report incidents and events to decision makers in a timely manner commensurate with their severity; and

d. Remediate the impact of the incidents and events in an effective manner.

3.21 Larger Institutions with important API adoption should consider establishing a security operations centre dedicated to monitoring, assessing and defending IT systems and assets such as APIs, web sites, applications, Data servers, networks, hardware and software.

3.22 Institutions should maintain an audit trail that records the appropriate metrics and security-related behavior of each API and records any breaches of security that occur. The audit trail should capture the metrics and behavior before and after such breaches to support future detection of breaches of security.

3.23 Institutions should establish incident handling procedures to swiftly detect, review, report and rectify any incidents. Institutions should only provide the necessary details of any incident when reporting incidents to the public to avoid providing attack vectors for bad actors.

Cloud Computing

Materiality

3.24 A Cloud Computing arrangement is considered material when a disruption in service or breach of security or confidentiality of systems and/or Data may have the potential to materially impact:

a. The Institution's business operations;

b. The Institution's ability to manage risks;

c. The Institution's ability to comply with applicable laws and regulations; or

d. The confidentiality or integrity of an Institution's or Customer's Personal Data (i.e. if the arrangement may lead to unauthorized access, disclosure, loss or theft of Personal Data).

3.25 Institutions should conduct an assessment to determine the materiality and the associated risks of a Cloud Computing arrangement. When conducting such an assessment, Institutions should consider:

a. The criticality and inherent risk profile of the Cloud Computing arrangement i.e. activities that are critical to the business continuity/viability of the Institution and its obligations to Customers;

b. The impact and likelihood of a service failure, security breach or other event on an Institution's business operations or reputation;

c. The impact and likelihood of a confidentiality breach, loss or theft of Customer Data or breach of Data integrity of the Institution and its Customers; and

d. The cost and other resources to support a Cloud Computing arrangement.

3.26 Institutions should engage the relevant Supervisory Authority of any material Cloud Computing plans in order to address any concerns and expectations early in the design process before implementing any material Cloud Computing arrangement. This approach must comply with existing outsourcing requirements set by the relevant Supervisory Authority, including, where appropriate, the need to seek approval for material Cloud Computing plans.

Governance

3.27 Institutions considering the use of Cloud Computing should define a clear strategy and architectural roadmap which covers the target IT environment, the transition from the current environment to the target and the operating model, including any organisational change or additional skillsets that maybe necessary.

3.28 Institutions should establish an approved and documented governance framework for effective decision-making and proper management and control of risks arising from the use of Cloud Computing and Outsourcing of Cloud Computing to Outsourcing Service Providers. The governance framework should:

a. Define the roles and responsibilities for the operation and management of the Cloud Computing arrangement, security controls and risk management controls. Where an

Outsourcing Service Provider is involved, the division of roles and responsibility between the Institution and the Outsourcing Service Provider should be clearly defined;

b. Define the process to conduct a risk-based analysis to identify and classify the IT Assets involved in or deployed by the Cloud Computing arrangement based on criticality and confidentiality;

c. Require the maintenance and updating of the log of IT Assets in the cloud environment including their ownership;

d. Establish appropriate policies, procedures, and controls to govern the use of Cloud Computing covering risk management, due diligence on the Outsourcing Service Providers and access, confidentiality, integrity, and recoverability of IT Assets outsourced; and

e. Set out the steps for management and review of the contract between the Institution and the Outsourcing Service Provider, where Cloud Computing services are outsourced.

3.29 Senior Management of the Institution should be responsible for the assessment, understanding and monitoring of the Institution's reliance on Outsourcing Service Providers for material Cloud Computing services.

3.30 Institutions should maintain up-to-date and accurate documentation pertaining to the Cloud Computing arrangement for review, audit, supervision, and other purposes, including but not limited to:

a. Rationale and an appropriate strategy for implementing the Cloud Computing arrangement;

b. Materiality and risk assessment and conclusion;

c. Outsourcing risk assessment, other initial security-related risk assessments and their conclusions (further guidance on assessments provided in subsection "Outsourcing");

d. Due diligence or suitability assessments conducted on the Outsourcing Service Provider and conclusions;

e. Description of the Cloud Computing arrangement including but not limited to:

i. Name of Outsourcing Service Provider and any sub-contractors;

ii. Level of reliance on Outsourcing Service Providers;

iii. Type of Cloud Computing service models (i.e. Software as a service - SaaS, Infrastructure as a service - IaaS etc.) and deployment models used (i.e. private, public etc.);

iv. IT Assets in scope including their criticality and ownership;

v. Services/products selected;

vi. Parties involved; and

vii. Delivery locations.

f. Contract and other legal documentation pertaining to the arrangement with the Outsourcing Service Provider (further guidance provided in subsection “Outsourcing”).

Outsourcing

3.31 Prior to engaging an Outsourcing Service Provider to provide Cloud Computing services, Institutions should perform a comprehensive Outsourcing risk assessment covering:

a. The role and materiality of the service to be outsourced in the Institution’s business operations;

b. Due diligence on prospective Outsourcing Service Providers (further guidance on the due diligence process provided in Clause Institutions should verify the maturity, adequacy and appropriateness of the prospective Outsourcing Service Provider and services selected, taking into account the intended usage of the Cloud Computing service. Institutions should consider the following specific factors when conducting due diligence on Outsourcing Service Providers providing Cloud Computing services, including but not limited to:); and

c. Assessing the benefits of the Outsourcing arrangement against the risks.

3.32 Institutions should verify the maturity, adequacy and appropriateness of the prospective Outsourcing Service Provider and services selected, taking into account the intended usage of the Cloud Computing service. Institutions should consider the following specific factors when conducting due diligence on Outsourcing Service Providers providing Cloud Computing services, including but not limited to:

a. Materiality: The results of the materiality assessment. The depth of the due diligence undertaken and risk mitigating controls established should be commensurate with the materiality of the Cloud Computing arrangement and the level of reliance the Institution places on the provider to maintain effective security controls;

b. Due diligence scope: The scope of the due diligence assessment should be appropriate and cover an adequate set of controls and individual assessments of all locations expected to be relevant in the arrangement. In particular, the Institution should consider the track record of the Outsourcing Service Provider in achieving acceptable outcomes in areas such as information security policies and awareness, due diligence and risk assessment of practices related to sub-contracting, system vulnerability assessments, penetration testing, and technology refresh management;

c. Data centers: Evaluation of whether the data centers are located in countries that the Institution deems suitable and acceptable to store and process Data (further guidance outlined in the subsection “Design”);

d. Controls: Institutions should ensure that Outsourcing Service Providers implement strong authentication, access controls, Data encryption and other security and technical controls (further guidance outlined in the subsections “Design” and “Management and monitoring”) to meet the Institutions’ requirements. Controls implemented by Outsourcing Service Providers should be at least as strong as those which the Institutions would have implemented had the operations been performed in-house;

e. Security risk assessments: Prior to implementing Cloud Computing services and undertaking an Outsourcing arrangement, Institutions should conduct an initial security and risk assessment of the service to identify any information security, cybersecurity and

other IT control weaknesses. The risk assessment will identify security threats including information security threats and operational weaknesses and develop safeguards to mitigate those threats and weaknesses. The factors considered during the risk assessment should include but not be limited to:

i. Nature of the service (including specific underlying arrangements);

ii. Provider and the location of the service;

iii. Criticality and confidentiality of the IT Assets involved;

iv. Transition process including handover from the Institution and/or other service providers to the potential Outsourcing Service Provider;

v. Target operating model; and

vi. Adherence to recognised technical security standards.

vii. Compliance with standards and external assurance: The Outsourcing Service Provider's adherence to international standards as relevant to the provision of services (for e.g. ISO/EIC etc.). Institutions may take into consideration any external assurance that has already been provided by independent auditors when conducting their own due diligence.

3.33 When conducting risk assessments of Cloud Computing services, Institutions should consider key risks including but not limited to:

a. Cybersecurity risk;

b. Operational risks, specifically information security, Outsourcing and business continuity risk. In particular, Institutions in an outsourced Cloud Computing arrangement should consider the impact of the Outsourcing arrangement on the Institution's risk profile i.e. the potential heightened operational, legal, compliance, reputational, concentration and other risks associated with the arrangement;

c. Reputational risk; and

d. Specific risks arising from the design and operating model of the Cloud Computing arrangement.

3.34 Institutions should ensure that the written contract governing the Cloud Computing arrangement between the Institution and Outsourcing Service Provider covers the following issues including, but not limited to:

a. The roles, relationships, obligations and responsibilities of all contracting parties;

b. Location of the data centres;

c. Ownership and control over IT Assets, if the Outsourcing Service Provider is expected to be given some level of control over IT Assets;

d. Liability in the event of losses or breaches in security or confidentiality;

e. Measures to protect the Institution's Data and confidential information and limits to disclosure of such information;

f. Data recovery and access to Data used for daily operational purposes as well as for contingency, disaster recovery or backups;

g. Advance notice to the Institutions regarding any changes to data centre locations;

h. Access to information held by the Institution;

i. The right to monitor, review and audit Cloud Computing arrangements by the Institution's internal control functions, and regulators, or persons employed by them, including for the purposes of supervisory reviews by the respective Supervisory Authority;

j. With respect to Outsourcing Service Providers use of sub-contracting arrangements:

    i. Disclosure of all material and service-related sub-contracting arrangements;

    ii. Advance notification of any new sub-contracting arrangements or changes to existing arrangements by the Outsourcing Service Provider;

    iii. Outsourcing Service Provider's accountability to the Institution for the provision of service and effectiveness of agreed controls;

    iv. Outsourcing Service Provider's contractual liability for the performance and risk management of any sub-contractor(s) it employs and, where this is the case, the full compliance of the sub-contractor(s) with the obligations existing between the Institution and Outsourcing Service Provider.

k. Scenarios or events in which Institutions have the right to terminate the contractual agreement, such as where new or modifications to existing sub-contracting arrangements have an adverse effect on the Institution's security or risk assessment of the Cloud Computing arrangement; and

l. The exit plan and process to be followed in the event of termination of the Cloud Computing arrangement including, but not limited to:

    i. A reasonable transition period;

    ii. Procedures for returning Data to the Institution;

    iii. Permanent Data deletion by the Outsourcing Service Provider; and

    iv. Any arrangements to transfer the outsourced service to another Outsourcing Service Provider or reincorporate it into the Institution with sufficient hand-over and support from the previous Outsourcing Service Provider.

3.35 Institutions should understand their roles and those of the Outsourcing Service Provider providing Cloud Computing services. Roles and owners should be defined and agreed upon as part of the shared responsibility model which should specifically cover roles with respect to cybersecurity, information security and related controls.

3.36 Where a material Outsourcing arrangement involves the transfer of Data, Institutions should:

a. Classify Data based on criticality and confidentiality;

b. Identify potential risks relating to outsourced Data and their impact; and

c. Agree on an appropriate level of confidentiality, integrity, and availability.

Design

3.37 Institutions should ensure that the design and architectural aspects of the Cloud Computing services, or arrangement are optimised to cater to the needs of the Institution, adhere to the Institution's internal policies and procedures and minimise risks.

3.38 Institutions and Outsourcing Service Providers should consider the following principles when developing the design and architecture of the Cloud Computing arrangement:

a. Availability: To reduce the likelihood of IT Assets becoming unavailable in the event of failure of individual components and improve the ability for users to request and use IT Assets;

b. Resilience: To improve resilience through implementation of security controls, implementation of regular testing and checks to detect security and service issues, and use of multiple data centres distributed across multiple locations, or where appropriate, use of multiple Outsourcing Service Providers to provide Cloud Computing services;

c. Recoverability: To allow for swift and effective recovery and restoration of IT Assets to a specified level of service in the event of a compromise of integrity or availability;

d. Capacity: To ensure the Cloud Computing arrangement's capacity is commensurate with the Institution's needs; and

e. Encapsulation: To ensure re-usability of network and system components.

3.39 Institutions should carefully determine and choose the type of cloud(s) deployed based on an assessment of the business operations performed on the cloud(s) and the risks associated with each type of cloud.

3.40 Institutions should evaluate and assess the location of data centres while determining the design of the Cloud Computing arrangement to select data centres appropriate to the Institution's needs. The assessment should address the location's:

a. Potential risks, including information security, legal and compliance risks;

b. Wider political and security issues; and

c. Legislation and legal framework including law enforcement and insolvency law provisions that would apply in the event of an Outsourcing Service Provider's failure.

3.41 Institutions should implement appropriate and effective network access and security controls such as firewalls, Intrusion Prevention System, advanced threat protection and web proxy so that other on-premise environments are not exposed to unauthorized access from the cloud.

3.42 Institutions should define a standard set of tools and processes to manage containers, images and release management and ensure consideration of any risks posed by shared virtual environments or Data co-mingling.

3.43 Institutions should implement preventative and detective Data controls to keep Data secure and prevent Data loss. Institutions should ensure that the Data controls including those outlined in

this section cover all Data, whether it is Data in storage, Data in transmission (i.e. Data that is actively moving from one location to another) or Data in use.

3.44 Institutions should ensure that Data processed or stored through the Cloud Computing arrangement are recoverable within a pre-defined timeframe and appropriate and secure backups of Data are maintained.

3.45 Where the Cloud Computing arrangement is using a multi-tenancy environment or Data co-mingling arrangement, Institutions should ensure its Data and information is segregated and the Outsourcing Service Provider is able to protect the confidentiality and integrity of the Data and information.

3.46 Institutions should introduce controls to prevent unauthorised access to Data and permit access to IT Assets only when appropriate.

3.47 Institutions should establish security controls to protect against attacks (e.g. network intrusion attempts, DoS attacks) including cloud specific attacks.

3.48 Institutions should introduce cryptographic key management to control access to, segregate and secure Customer's Data.

3.49 Institutions should utilise encryption or tokenisation to protect confidentiality of Personal Data, such as authentication credentials and emails etc., being processed, or in transit including Data in Data back-ups.

3.50 Institutions should introduce user identity and access management and authentication (including Multi-Factor Authentication) to provide controlled access to information systems allowing Staff and Outsourcing Service Providers to perform their business activities, while protecting Data and systems from unauthorised access.

3.51 Institutions should ensure that user access and activities are logged and reviewed on an "as needed" basis.

3.52 Institutions should develop controls to ensure confidentiality and integrity of source codes and prevent alteration of source codes and system configurations (particularly when the Institution uses models such as DevOps).

3.53 Institutions should conduct vulnerability assessments and penetration tests specific to the Cloud Computing arrangement to identify weaknesses or flaws in the security processes.

Management and monitoring

3.54 Institutions should establish change management processes to ensure any changes in the Cloud Computing arrangement by the Institution or the Outsourcing Service Provider are appropriately governed and implemented.

3.55 Institutions should ensure that they define the conditions and scenarios in which automated testing and releases can take place for changes to their Cloud Computing arrangements, and that there is a full audit trail, record of the changes and evidence of pre-approval.

3.56 Institutions should develop a mechanism by which they are notified of material changes to the Cloud Computing arrangement in a timely manner.

3.57 Institutions should develop a configuration management process which includes regular monitoring to detect unauthorised changes to the cloud environment and ensure such changes

can be appropriately remediated.

3.58 Institutions should ensure that the Cloud Computing arrangement has the capacity to run the Institution's workloads. Institutions should regularly monitor utilisation and proactively plan for upgrades or enhancements based on anticipated spikes in workloads or resulting from strategic business initiatives.

3.59 Institutions should establish a monitoring framework to define, monitor, report and remediate key infrastructure, technology and security related incidents and events in the cloud environment in a timely and effective manner to minimise detriment. The framework should:

a. Cover incidents and events that may impact the stability or availability of the Institution's applications, networks and systems or the confidentiality or integrity of cloud environments;

b. Be centralised to promote clarity of process and enable consolidation and analysis of threat intelligence, incident and event related Data;

c. Manage incidents and events according to their frequency, criticality and assigned ownership;

d. Identify, monitor and manage systemic issues;

e. Monitor and identify vulnerabilities, incidents, and events on an on-going basis by:

i. Defining a standard set of health and performance metrics;

ii. Utilising analytics and Data from previous security incidents and events to enable retrospective detection;

f. Categorise and record Data associated with incidents and events;

g. Report and escalate incidents and events to relevant stakeholders for notification or action; and

h. Ensure that incidents and events are properly reviewed and identified gaps are remediated to prevent a reoccurrence.

3.60 Institutions should be able to swiftly and safely:

a. Detect vulnerabilities in the software used in the cloud environment; and

b. Deploy security and operating system patches.

3.61 After implementation of the Cloud Computing arrangement, Institutions should re-assess the risks associated with the Cloud Computing arrangement when there is a material change to existing arrangements and on a regular basis through ongoing:

a. Outsourcing risk assessments to assess adequacy of controls in managing the risks arising from the Outsourcing arrangement; and

b. Security and risk assessments to assess the adequacy of the security and risk controls in managing the risks arising from Cloud Computing. These should include conducting vulnerability assessments and penetration tests specific to the Cloud Computing arrangement on at least an annual basis.

3.62 Institutions should establish risk mitigation controls to address any shortcomings of the Cloud Computing arrangement. The degree of risk should inform the stringency of controls and mitigation procedures implemented.

Business continuity

3.63 Institutions' business continuity management functions and crisis management teams should develop and implement a business continuity plan for material Cloud Computing arrangements. If Cloud Computing arrangements are outsourced, the Outsourcing Service Provider should have a business continuity plan in place that is acceptable to the Institution.

3.64 Institutions should define key risk indicators, performance metrics and adverse conditions that can trigger the business continuity plan for the Cloud Computing arrangement during its on-going monitoring and oversight of any services provided by the Outsourcing Service Provider.

3.65 As part of an Institution's own business continuity planning for Cloud Computing services, it should tailor the plan to:

a. Account for any dependency on one Outsourcing Service Provider;

b. Define the division of roles and responsibilities;

c. Define recovery objectives;

d. Identify alternative solutions/develop transition plans; and

e. Test their business continuity plans for their Cloud Computing arrangement (jointly with the Outsourcing Service Provider if the Cloud Computing arrangement is outsourced) on at least an annual basis.

Exit and resolution planning

3.66 Institutions should consider the possibility of a stressed exit wherein an event of disruption cannot be managed through business continuity measures.

3.67 Institutions should define and maintain specific exit plans for their outsourced Cloud Computing arrangements, taking into account, developments (such as new technology) that may change the feasibility of an exit in stressed and non-stressed scenarios.

3.68 Institutions should account for outsourced Cloud Computing arrangements when developing resolution plans or strategies to identify and address any impediments to its resolvability and to prepare for its possible resolution.

3.69 Institutions should establish procedures for Data recovery by the Institution and permanent Data deletion by the Outsourcing Service Provider in the event of a termination of services.

Biometrics

Governance

3.70 Institutions should ensure compliance with the relevant legislation and regulations in relation to Data protection.

3.71 When Outsourcing to an Outsourcing Service Provider, Institutions should ensure that access to information is adequately controlled, monitored, reviewed, and audited by the Institution's internal control functions, and regulators, or persons employed by them, including supervisory reviews by the respective Supervisory Authority.

Identity proofing and enrolment management

3.72 Institutions using Biometric Applications should ensure effective proofing of identities, including validation and verification of identities. Validation involves determining that the documentary evidence for the Biometric identity is genuine, reliable, and independent. Verification involves confirming the validated identity relates to the individual being proofed.

3.73 Institutions should obtain and store evidence of any digital identity verification (e.g., via chip or wireless technologies) performed by integrated scanners, sensors and other devices.

Ongoing authentication and Identity Lifecycle management

3.74 Institutions should establish controls and processes to protect Customers and their credentials against vulnerabilities and unauthorized access, disclosure or use in the authentication process and throughout the Identity Lifecycle.

3.75 Institutions deploying Multi-Factor Authentication at login that includes a Biometric factor should consider employing phishing-resistant authenticators where at least one factor relies on public key encryption to secure the Customer authentication process.

3.76 Institutions should implement risk-based or adaptive authentication measures that present Customers with authentication options commensurate with the risk level of the transaction and sensitivity of the information.

3.77 Institutions should implement Multi-Factor Authentication using a Biometric factor, where possible, to authorize high risk activities and protect the integrity of Customer account Data and transaction details. High-risk activities include changes to Personal Data (e.g. Customer office and home address, email and telephone contact details), registration of Third-Party payee details, high value funds transfers and revision of funds transfer limits.

3.78 For Biometric authentication of transactions, Institutions should adopt security measures to ensure the confidentiality, authenticity and integrity of authentication codes, Personal Data and transaction specific information.

Management and monitoring

3.79 Institutions should periodically monitor their Biometric Applications throughout the Identity Lifecycle to assess performance, detect security-related events, evaluate the adequacy of controls, and take any remedial action.

3.80 Institutions should ensure that all communications with individuals involving Biometric Data across the Identity Lifecycle occur over a mutually authenticated and protected channel.

3.81 Institutions should ensure the employment of physical tamper detection and resistance features appropriate for the environment in which the identity-proofing session occurs.

3.82 Across the Identity Lifecycle, Institutions should introduce processes and controls to safeguard against Data tampering, cyberattacks, security breaches and other fraudulent activities which may lead to identity theft, compromise or misuse of Data and errors.

3.83 Institutions should monitor and evaluate all the processes involved in the Identity Lifecycle including identity proofing, authentication etc. to ensure that they are secure and efficient.

3.84 As a Credential Service Provider may be an independent Third Party or may issue credentials for its own use, Institutions should ensure that they perform the requisite due diligence checks and protocols on the Credential Service Provider on a regular basis.

3.85 Institutions should monitor the performance of the Biometrics Application for inherent risks such as false acceptance rates and false rejection rates. Poorly executed algorithms may result in higher false acceptance rates and these inherent risks should be calibrated to be commensurate with the risks associated with the Biometric Application.

Data management

3.86 Institutions should ensure the security, confidentiality, authenticity and integrity of Data across all phases of authentication, whether the Data is in use, storage or transmission.

3.87 Institutions should maintain a clear trail and record of the Biometric Application's Data obtained from the Credential Service Providers.

3.88 Institutions should consider the principles of portability and interoperability when planning and implementing systems and databases for the Biometric Application.

3.89 Where Biometric Applications are used for Biometric authentication, Institutions should ensure Biometric Data and authentication credentials, whether in use, storage or transmission, are encrypted.

Outsourcing

3.90 If Biometric activities are outsourced, Institutions should ensure that:

a. They obtain the necessary Data concerning Biometric identification/verification from the Outsourcing Service Providers and take adequate steps to satisfy themselves that copies of identification Data and other relevant documentation will be made available from the Outsourcing Service Providers upon request and without delay; and

b. The Outsourcing Service Provider complies with the Institution's Customer due diligence and record-keeping requirements.

Big Data Analytics and Artificial Intelligence (AI)

Materiality

3.92 Institutions should assess their Big Data Analytics and AI Applications to determine the materiality and associated risks of each Application.

3.93 When conducting a materiality assessment of a Big Data Analytics and AI Application, Institutions should consider:

a. The purpose of the Big Data Analytics and AI Application (i.e. use case) and its role in the Institution's decision-making process;

b. The criticality and inherent risk profile of the activities (i.e. are they activities that are critical to the business continuity/viability of the Institution and its obligations to Customers); and

c. The likelihood that the activity may be disrupted and the impact of any such disruption.

Governance

3.94 Institutions should establish an approved and documented governance framework for effective decision-making and proper management and control of risks arising from the use of Big Data Analytics and AI. The governance framework should:

a. Establish a mechanism to ensure that Institutions are required to assess whether the Application is suitable for Big Data Analytics and AI implementation and define specific parameters and criteria to enable the Institution in its decision-making;

b. Establish appropriate policies, procedures and controls to govern the design, development, monitoring, review and use of Big Data Analytics and AI Applications within the Institution;

c. Ensure proper validation of Big Data Analytics and AI Applications prior to their launch, and thereafter implement on-going training, calibration and review to ensure the reliability, fairness, accuracy and relevance of the algorithms, models and Data used and the results;

d. Maintain a transparent, enterprise-wide record of Big Data Analytics and AI Applications and their underlying mechanics;

e. Establish processes to assess, monitor, report and mitigate risks associated with the Big Data Analytics and AI Application;

f. Ensure that material decisions regarding Big Data Analytics and AI Applications and their underlying models and Data are documented and sufficiently justified; and

g. Cover every stage of the model lifecycle including design, development, deployment, review, update and discontinuation.

3.95 The Governing Body and Senior Management of the Institution should be accountable for the outcomes and decisions arising from the use of Big Data Analytics and AI Applications, including those Applications that make decisions on behalf of the Institution. They should:

a. Ensure that all Staff working on or using Big Data Analytics and AI Applications are

assigned appropriate accountability for their involvement with Big Data Analytics and AI Applications and understand what they should to do meet this accountability; and

b. Ensure that technical specialists with appropriate technology skillsets (e.g. Big Data analysts, Artificial Intelligence engineers and specialists) and Application specific skillsets (e.g. credit risk modelling specialists if the Application is a credit scoring model) form part of the team actively involved in developing and implementing Big Data Analytics and AI Applications.

3.96 When Outsourcing to an Outsourcing Service Provider, Institutions should ensure that access to information is adequately controlled, monitored, reviewed, and audited by the Institution's internal control functions, and regulators, or persons employed by them, including supervisory reviews by the respective Supervisory Authority.

3.97 Big Data Analytics and AI Applications, including when the model is developed by an Outsourcing Service Provider, should be auditable and, accordingly, Institutions, where relevant and considering the type of application used, should maintain on-going and up-to-date information through:

a. Establishing audit logs and maintaining traceability of decisions and outcomes of the Big Data Analytics and AI Application;

b. Developing and maintaining design documentation (further guidance provided in Clause Institutions should maintain documentation outlining the design of the material Big Data Analytics and AI model including but not limited to, where applicable:);

c. Maintaining records of the various versions of the model including its code (further guidance provided in Clause Institutions should establish a robust system for versioning and maintain record of each version of the material Big Data Analytics and AI model including but not limited to, where applicable:);

d. Archiving original Datasets used to develop, re-train or calibrate models;

e. Tracking outcomes and performance of the Big Data Analytics and AI Application; and

f. Retaining above information for a minimum period of five (5) years, or as otherwise prescribed by applicable laws and regulations.

Design

3.98 Institutions should ensure that the models for their Big Data Analytics and AI Applications are reliable, transparent, and explainable, commensurate with the materiality of those Applications. Accordingly, Institutions, where appropriate, should consider:

a. Reliability: Implementing measures to ensure material Big Data Analytics and AI Applications are reliable and accurate, behave predictably, and operate within the boundaries of applicable rules and regulations, including any laws on data protection or cyber security;

b. Transparency: Institutions should be transparent in how they use Big Data Analytics and AI in their business processes, and (where reasonably appropriate) how the Big Data Analytics and AI Applications function; and

c. Technical Clarity: Implementing measures to ensure the technical processes and

decisions of a Big Data Analytics and AI model can be easily interpreted and explained to avoid the threat of "black-box" models. The level of technical clarity should be appropriate and commensurate with the purpose and materiality of the Big Data Analytics and AI Application (e.g. where the model results have significant implications on decision making).

3.99 Institutions should adopt an effective Data governance framework to ensure that Data used by the material Big Data Analytics and AI model is accurate, complete, consistent, secure, and provided in a timely manner for the Big Data Analytics and AI Application to function as designed. The framework should document the extent to which the Data meets the Institution's requirements for data quality, gaps in data quality that may exist and steps the Institution will take, where possible, to resolve these gaps over time.

3.100 Institutions should make regular efforts to ensure data used to train the material Big Data Analytics and AI model is representative (i.e. how relevant the Data and inferences drawn from the Data are to the Big Data Analytics and AI Application) and produces predictable, reliable outcomes that meet objectives.

3.101 Institutions should be able to promptly suspend material Big Data Analytics and AI Applications upon the Institution's discretion such as in the event of a high cyber threat, information security breach or malfunctioning of the model.

3.102 Institutions should, where relevant, conduct rigorous, independent validation and testing of material trained Big Data Analytics and AI models to ensure the accuracy, appropriateness, and reliability of the models prior to deployment. Institutions should ensure the model is reviewed to identify any unintuitive or false causal relationships. The validation may be carried out by an independent function within the Institution or by an external organisation.

3.103 Institutions should maintain documentation outlining the design of the material Big Data Analytics and AI model including but not limited to, where applicable:

a. The input Data source and Data description (types and use of Data);

b. The Data quality checks and Data transformations conducted;

c. Reasons and justifications for specific model design and development choices;

d. Methodology or numerical analyses and calculations conducted;

e. Results and expected outcomes;

f. Quantitative evaluation and testing metrics used to determine soundness of the model and its results;

g. Model usage and implementation;

h. Form and frequency of model validation, monitoring and review; and

i. Assumptions or limitations of the model with justifications.

3.104 Institutions should introduce controls to ensure confidentiality and integrity of the codes used in the material Big Data Analytics and AI Application so that the code is only accessed and altered by authorized persons.

3.105 Institutions should identify and monitor the unique risks arising from use of the material Big

Data Analytics and AI Application and establish appropriate controls to mitigate those risks.

Management and monitoring

3.106 Institutions should establish an approved and documented framework to review the reliability, fairness, accuracy and relevance of the algorithms, models and Data used prior to deployment of a material Big Data Analytics and AI Application and on a periodic basis after deployment, to verify that the models are behaving as designed and intended. The framework should cover, where relevant:

a. The various types and frequencies of reviews including continuous monitoring, re-training, calibration and validation;

b) Scenarios and criteria that would trigger a re-training, calibration, re-development or discontinuation of the model such as a significant change in input Data or external/economic changes;

a. Review of material Big Data Analytics and AI model outcomes for fairness or un-intentional bias (e.g. through monitoring and analysis of false positive and/or false negative rates); and

b. Review of continuity or contingency measures such as human intervention or the use of conventional processes (i.e. that do not use Big Data Analytics and AI).

3.107 When the use of a material Big Data Analytics and AI model results in a technical or model-related error or failure, Institutions should:

a. Be able to swiftly detect the error;

b. Establish a process to review the error and rectify it in a timely manner, which may include notifying another function; and

c. Report the error to relevant stakeholders if material.

3.108 Institutions should establish a robust system for versioning and maintain record of each version of the material Big Data Analytics and AI model including but not limited to, where applicable:

a. New Data used;

b. Revisions to the documentation;

c. Revisions to the algorithm;

d. Change in the way variables are picked and used in the model or, where possible, the names of variables; and

e. The expected outcome of the newly calibrated, re-trained or re-developed model.

Ethics

3.109 Institutions should ensure that their Big Data Analytics and AI Applications promote fair treatment, produce objective, consistent, ethical, and fair outcomes, and also, are aligned with Institutions' ethical standards, value and codes of conduct. Accordingly, they should:

a. Comply with laws against discrimination and other applicable laws;

b. Be produced using representative inputs and Data which have been tested for selection bias (further guidance provided in Clause 3.100);

c. Consider whether a human-in-the-loop mechanism is needed to detect and mitigate biases;

d. Retain the possibility of manual intervention to mitigate or reverse irresponsible and erroneous decisions;

e. Retain the possibility of modification by the Institution; and

f. Be explainable.

3.110 Institutions should consider the fairness of a Big Data Analytics and AI model through understanding the biases and noise affecting Big Data Analytics and AI decisions. Institutions should define what it means for a Big Data Analytics and AI model to be fair.

3.111 Institutions should consider and assess the impact that Big Data Analytics and AI models may have on individuals or groups of individuals to ensure that such individuals or groups are not systematically disadvantaged unless the decisions suggested by the models have a clearly documented justification. Institutions should take steps to minimize unintentional or undeclared bias.

Customer protection

3.112 Institutions should be transparent with Customers about their use of Big Data Analytics and AI through their conduct and through accurate, understandable, and accessible plain language disclosure. Institutions should:

a. Ensure that Customers are informed of products and/or services that utilise Big Data Analytics and AI and the associated risks and limitations of the technology, prior to providing the service or each time Customers interact with the service (e.g. in the case of a Customer-facing service);

b. Explain how to use the Big Data Analytics and AI Application to Customers and ensure Customers always have easy access to the instructions; and

c. Provide clear explanations of the types of Data, types of variables and decision-making process used by Big Data Analytics and AI Applications upon Customers' requests. To avoid doubt, clear explanations do not require exposure of Institutions intellectual property, publishing of proprietary source code or details on firms' internal processes.

3.113 Institutions should obtain each Customer's acceptance of the risks associated with the use of Big Data Analytics and AI prior to providing the service.

3.114 Institutions should put in place a mechanism for Customers to raise inquiries about Big Data Analytics and AI Applications and request reviews of decisions made by Big Data Analytics and AI Applications.

Distributed Ledger Technology (DLT)

Governance

3.115 Institutions should establish an approved and documented governance framework for effective decision-making and proper management and control of risks arising from the use of DLT. The governance framework should include the following, as may be relevant depending on the type of DLT:

a. Cover the following elements integral to the functioning of a DLT Application:

b. Ownership model of the DLT platform and the Nodes running on it;

c. The model used to operate and manage the distributed ledger (e.g. a consortium, a single Institution);

d. Rules to govern the ledger(s) including participant and validator rules and restrictions;

e. Approval processes and procedures to grant access to create, read, update or deactivate Data stored on the distributed ledger(s);

f. Managing public and private keys;

g. Consensus protocol; and

h. Off-chain procedures (if any) including parameters for the validity of an off-chain activity and any standards or requirements for off-chains systems are defined and complied with.

i. Define the roles and responsibilities of the key groups involved with respect to the design, development, and operation 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), such as other Institutions and miners;

iii. Participants involved in the distributed ledger(s), such as owners of cryptocurrency etc.; and

iv. Third Parties including Outsourcing Service Providers such as custodians or software developers involved in delivering the service.

3.116 Reviews of the DLT Application should be conducted with oversight from Senior Management, prior to launch and thereafter on an on-going basis to ensure its reliability and security.

3.117 Institutions should establish clear and unambiguous governing rules for participants of the distributed ledger(s) for onboarding, on-going operations and dispute resolution.

3.118 When Outsourcing to an Outsourcing Service Provider, Institutions should ensure that access to information is adequately controlled, monitored, reviewed, and audited by the Institution's internal control functions, and regulators, or persons employed by them, including supervisory reviews by the respective Supervisory Authority.

3.119 Institutions should ensure that their DLT Applications maintain appropriate evidence and records to enable the Institution's internal control functions, external auditors, regulators, and other authorities to conduct their audits and reviews. Accordingly, Institutions should:

a. Record and store the additional evidence and information to provide auditors with a complete representation of processes, internal controls, financial statements, etc., and for proper accounting treatment of the transaction;

b. Ensure that a log of records of the DLT Application is fully available and accessible to the relevant parties to audit and review;

c. In the event that the DLT is in the form of a blockchain, ensure that off-chain activities, rules and protocols associated with and any link to on-chain activities are recorded and stored; and

d. Ensure that the DLT code and subsequent updates are recorded and stored.

Design

3.120 Institutions should design their DLT Applications to be efficient and effectively secure IT assets and any customer assets. Institutions should, where possible, ensure the design and architectural aspects of the DLT are optimised to cater to the specific use of the technology and the needs of the Institution.

3.121 Institutions should consider the following principles when developing the design of a DLT Application that manages financial assets:

a. Flexibility: To define the DLT Application narrowly, which is easier to optimise, or flexibly, which may incur higher costs (more difficult protocol, less predictability, larger target for attacks, etc.);

b. Traceability: To ensure that the distributed log of records and any off-chain records are traceable and anonymity is avoided;

c. Capacity: To ensure that the DLT Application's computing and Data capacity is commensurate with the Institution's needs and is scalable depending on the intended use;

d. Security: To ensure that the activities and records on the distributed ledger(s) are secure;

e. Confidentiality: To maintain confidentiality of Data and implement adequate controls over the set-up and number of Nodes; and

f. Resilience: To ensure that the system is resistant to Data loss, loss of integrity, unavailability, or manipulation.

3.122 Institutions should define rules relating to Data and technological architecture of the DLT Application during the design phase to ensure that internal control functions, external auditors and Supervisory Authorities can effectively access the application (when applicable) and monitor compliance.

3.123 Institutions should appropriately determine the type of access, whether permissioned or permissionless, granted to participants based on an assessment of the operations performed, level of security and Data stored using DLT. For instance, Applications involving any of the following elements should use permissioned systems:

a. Customer assets, funds or other forms of ownership, rights or interests such as contracts;

b. Personal Data; or

c. Requirements for a controlled set of participants or restricted access.

3.124 Institutions should establish controls to ensure the integrity and security of the network and DLT Application. These controls may include, but are not limited to:

a. Implementing processes to limit Node processing ability and limit the potential for a Node to process an excessive number of transactions;

b. Designing the Application to allow blocking of IPs/Nodes that generate too many new transactions; and

c. Developing permissioned DLT Applications with individual Nodes that comply with security standards and requirements to guard against attacks.

3.125 Institutions should establish appropriate consensus protocols or platforms to accept and validate new records. The consensus methodology should be based on the Institution's requirements with respect to performance, scalability, consistency, Data capacity, governance, security and failure redundancy.

3.126 Institutions should avoid storing clear-text Personal Data on a blockchain and instead use sidechains or other private storage options.

3.127 Institutions should introduce cryptographic key management to control access to confidential information and Personal Data. Institutions should institute controls with respect to key generation and management and ensure an appropriate and secure storage and transmission mechanism for private keys. The key management controls should cover offline root keys (split amongst multiple owners) and online root keys (stored on hardware security modules).

3.128 With respect to the issuance of keys to Staff and other personnel:

a. Institutions should issue individual keys to Staff and other persons working on behalf of the Institution for audit, supervision and review purposes;

b. Institutions should embed internal checks and verifications on the transactions and activities executed through the distributed ledger such as Staff sign-off on requests or transactions; and

c. Institutions should ensure they can internally identify the Staff signing-off messages or requests on the distributed ledger.

3.129 Institutions should, if possible, ensure that the design of the DLT Application allows for change i.e. add new functionality or remove unwanted or incorrectly functioning features within the DLT Application.

3.130 Institutions should, if possible, introduce mechanisms to manage forks (i.e. conflicts arising from incompatible versions of the DLT that are broadcast within a short time period) and ensure that the situation is resolved quickly and the integrity of the DLT is maintained.

3.131 Institutions should, if possible, introduce user access management and authentication to provide controlled access to the DLT Application. Staff and Outsourcing Service Providers should be provided access to only those parts of the system they need to perform their responsible

business or operational activities. Institutions may consider if, in certain cases, it might be feasible to accept transactions only from selected, authorised IP addresses.

3.132 Institutions should develop controls to ensure confidentiality and integrity of code(s) and prevent alteration of code(s).

Anonymity and pseudonymity

3.133 Institutions developing Permissionless DLT Applications should ensure that users are not anonymous or pseudonymous, as allowing anonymity and pseudonymity can facilitate criminal purposes like tax evasion, bribery, money laundering or terrorism financing.

3.134 Further, Institutions should consider using mechanisms such as chain analytics to follow and monitor transactions on pseudonymous blockchains.

Management and monitoring

3.135 Institutions should ensure that their DLT Applications are reviewed and monitored on a periodic basis to evaluate performance, detect technology and security related incidents, ensure the adequacy of controls, and promptly take any remedial action.

3.136 Institutions should ensure that code is reviewed and validated on an ongoing basis at regular, predetermined intervals to identify any weaknesses. Institutions should ensure code is performing its expected functions and is secure.

3.137 Institutions should conduct vulnerability assessments and penetration tests specific to the DLT Application to identify weaknesses or flaws in the security processes.

3.138 Institutions should manage and monitor information integrity, privacy and confidentiality in the implementation of the DLT throughout its lifecycle (e.g. by conducting privacy threshold analysis, privacy impact assessment, and Data protection impact assessment). Institutions may adopt processes such as sharding and pruning during the design of the Application to further manage privacy and confidentiality mechanisms.

3.139 Institutions should further ensure adequate control and monitoring of the DLT through an even stringent focus on encryption than traditional controls with a particular focus on key management. A related control to consider is encrypting the ledger(s) with more than one key and applying on-chain encryption.

3.140 Institutions should review the distributed log of records and transactions within the ledger(s) to identify suspicious patterns and connections to monitor any anomalous behavior using analytics and testing.

3.141 Institutions should adopt operations security controls including standard infrastructure controls such as virus checking schedules, zero-day exploit remediation, maintenance schedules, capacity, and backup management.

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

3.143 Institutions should ensure that adequate human resources are put in place for implementing security controls to monitor access to the DLT Application and system. Institutions should

ensure that these controls are updated when Staff leave or change roles.

3.144 Institutions 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.

Data standardisation and interoperability

3.145 Institutions should not maintain Personal Data on the ledger(s) and such Data should be maintained off-chain.

3.146 Data retention will need to be factored into the underlying design of the network for Nodes to purge ledger information after certain defined time periods. Where Data retention rules apply to individual Data sets, destruction of keys used to encrypt the on-chain Data should be implemented.

3.147 Depending on the Application, Institutions should consider the principle of interoperability when planning the design of the distributed ledger(s). Institutions should establish processes to prune the distributed ledger(s) and remove records older than a specific time period or enable processes that allow Data stored on the ledger to be forgotten (i.e. destruction of keys used to encrypt Data).

Business continuity

3.148 Institutions should ensure appropriate business continuity planning with respect to DLT, as it covers the potential loss of Data and processing capability due to loss of servers or connectivity, and risks such as cyber-crime.

3.149 Institutions should plan, establish, and periodically test arrangements to maintain the continuity of the service/process performed by the DLT Application in the event of an incident that affects the availability of the Application

3.150 Institutions should ensure that their business continuity plan encompasses all the complex technical areas of DLT, from key storage and key regeneration in the event of catastrophic Data loss to creating new keys when a cyber-crime incident compromises Data security.

3.151 Institutions should consider DLT specific scenarios such as network malfunction or compromise of Data integrity in their business continuity plans.

3.152 The Institution's business continuity plan team should include specialists in DLT and should monitor cryptographic advances and vulnerabilities such that proactive responses can be developed to avoid system outages.

3.153 In solutions involving public key infrastructure, Institutions should ensure that the business continuity plan covers the technical integrity of the key generation mechanisms (certificate authorities, hardware security modules etc.), the business processes involved in the secure transportation of the private keys and the authorisation layer around these mechanisms.

Customer protection

3.154 Institutions should disclose the relevant governing rules to Customers participating in the distributed ledger(s).

3.155 Institutions should disclose any Fees associated with the on-going operation and management of the distributed ledger(s) including providing notice that Fees may be charged by Third Parties,

where applicable.

3.156 Institutions should advise Customers on what they should do to protect their keys from misuse. In particular, Institutions should inform Customers of the consequences of sharing their private keys and other security information.

Section 4: Interpretation

Any clarification or interpretation of the provisions of the Guidelines may be sought from the respective Supervisory Authority:

- FinTech Office of the Central Bank of the UAE (fintechoffice@cbuae.gov.ae);
- FinTech Team of the Securities and Commodities Authority (fintech@sca.gov.ae);
- Innovation Team at the Dubai Financial Services Authority (innovation@dfsa.ae); and
- Financial Technology and Innovation Unit of the Financial Services Regulatory Authority (fintech@adgm.com).