



Solution Specification Document (Project)
Issuer Announcement Publication Service System
(IAPSS)

iQx Consult Limited

May 2024



Document Revision History

Document Version	Modification Details	Modified By	Modification Date
Version 1.0	Initial requirement specification and documentation	Oluwatoni Amusan	May 2024
Version 2.0	Reviewed and updated	Adedamola Folarin	May 2024
Version 3.0	Reviewed and updated	Simi Abudu	May 2024
Version 4.0	Reviewed	Risk and Compliance Group	May 2024
Version 5.0	Comments addressed and recommendation implemented	Oluwatoni Amusan	May 2024






N/A: Not Applicable

Contents

1	Document Information/Approvals for Business Stakeholders	5
2	INTRODUCTION	6
2.1	Purpose	6
2.2	Scope	6
2.3	Background.....	6
2.4	References.....	7
2.5	Assumptions and Constraints	7
2.6	Document Overview	7
3	METHODOLOGY	8
4	FUNCTIONAL SPECIFICATIONS	8
4.1	Context Diagram	8
4.2	Use Case Diagram	9
4.3	System Actors & Activities	9
4.4	High-Level User Requirements	10
4.5	System Utilisation	11
4.6	General System Features	12
5	FUNCTIONAL REQUIREMENTS	14
5.1	QCG ADMIN FEATURES - Profiling User Institutions & System Users	14
5.2	SYSTEM USER - INPUTTER FEATURES	20
5.2.1	Publications	20
5.2.1.1	Generating Publication (Type as Text or PDF Upload)	20
5.2.1.1.1	Use Case	20
5.2.1.2	View Publication Status	22
5.2.1.2.1	Use Case	22
5.2.1.3	User Institution Edit/Update Logo	23
5.2.1.3.1	Use Case	23
5.3	SYSTEM USER - AUTHORISER FEATURES.....	25
5.3.1	Publication.....	25
5.3.1.1	Rejection/Approval	25
5.3.1.1.1	Use Case	25
5.3.1.2	View Previous Publications (System Inputter & Authoriser)	26
5.3.1.2.1	Use Case	26
5.3.2	User Institution Logo	27
5.3.2.1	Logo Rejection/Approval	27
5.3.2.1.1	Use Case	27
5.4	QCG ADMIN FEATURES.....	29
5.4.1	Publications	29
5.4.1.1	Delete Publications	29

5.4.1.1.1	Use Case - Delete Publications	29
5.4.1.2	View All Publications	30
5.4.1.2.1	Use Case – View All Publications	30
5.4.1.3	Approve/Reject Action to Delete Publications	30
5.4.1.3.1	Use Case – Approve/Reject Publication Deletion.....	30
5.4.2	Manage User Institution/System Users	32
5.4.2.1	Deactivate/Reactivate/Delete User Institution/System User	32
5.4.2.1.1	Use Case	32
5.4.3	Audit Log	35
5.4.3.1	View and Export Audit Log	35
5.4.3.1.1	Use Case	35
6	Document Information/Approvals for iQx Consult Limited	38
7	TECHNICAL REQUIREMENTS	39
7.1	Logical Data Model/Data Dictionary	40
7.2	Interface Requirements	41
7.3	Hardware/Software Requirements	41
7.4	Operational Requirements.....	41
7.5	Security and Privacy	42
7.5.1	Audit Trail	45
7.5.2	Reliability	45
7.5.3	Data Backup and Recoverability	45
7.5.4	System Availability	45
7.6	General Performance	45
7.6.1	Audit Trail	46
7.6.2	Reliability	46
7.6.3	Data Backup and Recoverability	46
7.6.4	System Availability	47
7.6.5	Efficiency.....	47
7.6.6	Stability	47
7.6.7	Scalability	47
7.6.8	Usability	47
7.6.9	Capacity	47
7.6.10	Maintainability	47
7.6.11	Data Retention.....	48
7.6.12	Error Handling and Logging	48
7.6.13	Validation Rules	48
7.6.14	Conventions/Standards	48
8	NEED FOR DATA PROTECTION IMPACT ASSESSMENT (“DPIA”) CHECKLIST	49

1 Document Information/Approvals for Business Stakeholders

Document Information/Approvals	
<div>Prepared By</div> <div>Oluwatoni Amusan</div>	<div></div> <div>-----</div> <div>Business Interface</div> <div>May 2024</div>
<div>Reviewed By</div> <div>Adedamola Folarin</div>	<div></div> <div><small>Adedamola Folarin (May 23, 2024 19:46 GMT+2)</small></div> <div>-----</div> <div>Business Interface</div> <div>May 2024</div>
<div>Concurred By</div> <div>Simi Abudu</div>	<div></div> <div>-----</div> <div>Listings & Quotations Compliance</div> <div>May 2024</div>
<div>Concurred By</div> <div>Ebenezer Nwoji</div>	<div></div> <div>-----</div> <div>Divisional Head, Market Oversight</div> <div>May 2024</div>
<div>Approved By</div> <div>Emmanuel Alao</div>	<div></div> <div><small>Emmanuel Alao (May 27, 2024 15:06 GMT+1)</small></div> <div>-----</div> <div>Supervising Head, iQx Consult</div> <div>May 2024</div>

2 INTRODUCTION

Due to the dynamic landscape of the Nigerian Financial Markets and the growing need for innovation, FMDQ Group PLC ("**FMDQ**" or the "**Group**") is embarking on an innovative venture: the launch of an Equities market. As part of this initiative, the Listings & Quotations Compliance Group ("**QCG**") within FMDQ Exchange is introducing an Issuer Announcement Publication Service System ("**IAPSS**"). This system is designed to automate and elevate the way Equity Issuers disseminate critical information to investors and the public.

The IAPSS will serve as a self-service portal, empowering Equity Issuers, or User Institutions, to directly publish notifications, disclosures, and announcements seamlessly. Through this system, FMDQ aims to eliminate information delays commonly associated with traditional publication processes, thereby fostering greater market transparency and investor confidence.

The IAPSS represents a significant leap forward in the realm of Equity market communications. By providing a seamless platform for publication and approval, FMDQ aims to empower User Institutions and enhance the overall integrity and accessibility of the Equities market.

In this document, we will consider the features, functionalities, and operational procedures of the Issuer Announcement Publication Service System, outlining its benefits, implementation strategy, and the overarching vision for transforming Equity market information dissemination.

2.1 Purpose

The purpose of the Issuer Announcement Publication Service System ("**IAPSS**") is to automate the dissemination of critical information within the Equities market by providing User Institutions with a seamless, self-service platform for publishing notifications, disclosures, and announcements.

2.2 Scope

The system under consideration is for the development of a self-service portal tailored to the needs of Equity Issuers operating within the Equities market. This system enables User Institutions to efficiently create, upload, and manage publications, while adhering to confining approval workflow processes to be overseen by designated Authorisers. Key functionalities include the generation and previewing of publications, real-time status tracking, and seamless integration of User Institution logos. Additionally, the IAPSS will include robust Administrative features for profiling User Institutions and System Users, facilitating account management, and ensuring adherence to security protocols. With a focus on enhancing transparency, accessibility, and efficiency, the IAPSS aims to set a new standard for communication and disclosure within the Equities market landscape.

2.3 Background

The Equities market has long been a cornerstone of global finance, providing Investors with opportunities for wealth creation and capital formation. FMDQ Exchange, a leading financial market infrastructure provider, has embarked on a strategic initiative to launch an Equities market. As part of this initiative, QCG within the FMDQ Exchange has undertaken the development of the Issuer Announcement Publication Service System ("**IAPSS**"). The genesis of the IAPSS stems from the imperative to enhance the efficiency and accessibility of information dissemination within the Equities market. By introducing a self-service portal for Equity Issuers, FMDQ seeks to empower User Institutions with the tools and resources necessary to communicate critical information in a timely and transparent manner.

Traditional methods of communication often involved intermediaries and manual processes, leading to delays and potential errors in the dissemination of information. Through the IAPSS, FMDQ Exchange aims to address

these challenges by providing User Institutions with a direct channel for publishing announcements, notifications, and disclosures, thereby fostering greater market efficiency and Investor confidence.

Moreover, the development of the IAPSS aligns with FMDQ's broader mission to promote market integrity, transparency, and innovation. By leveraging technology and best practices in financial market infrastructure, FMDQ aims to set new standards for communication and disclosure within the Equities market. The IAPSS represents an incremental step towards achieving these objectives, ushering in a new era of efficiency and transparency in equity market communications.

2.4 References

This document references the Business Requirements Document ("**BRD**") for the Issuer Announcement Publication Service System ("**IAPSS**").

2.5 Assumptions and Constraints

Assumptions

- User Institutions will readily adopt the system and actively utilise its features for publishing notifications, disclosures, and announcements
- The IAPSS will comply with relevant regulatory requirements and industry standards governing the publication and dissemination of information within the Equities market. This assumption necessitates thorough adherence to regulatory guidelines and periodic reviews to ensure continued compliance with evolving regulations
- The system will be able to seamlessly integrate with the FMDQ Exchange website as notifications will be pushed to the dedicated Equities page and the corresponding Issuer pages on the FMDQ website upon their availability on the website
- User Institutions will designate appropriate personnel to fulfill the roles of Inputters and Authorisers (by a mandate form to be executed by the Managing Director and another Director of the User Institution) within the IAPSS, as outlined in the system requirements. The system will not verify the credibility of the Inputter or the Authoriser
- Stable and reliable network connectivity is available for users accessing the system (QCG System Administrators, User Institution, Investors, and the Public)

Constraints

- Unforeseen downtime with the system, including servers, networks, and bandwidth may impose constraints on the system's performance and scalability
- Compliance with data retention policies and privacy regulations may introduce constraints on data storage, archival, and deletion

2.6 Document Overview

This Solution Specification Document ("**SSD**") provides detailed description of the requirements, features, and functionalities of the IAPSS. It serves as a blueprint or a guide for the implementation team to understand what needs to be built.

3 METHODOLOGY

The major goal is to provide a system that can provide an automated and accurate system for disseminating publications/notifications within the Equities Market, to enable Investors and the General Public to make informed decisions about their investment positions. The system will be used mainly by:

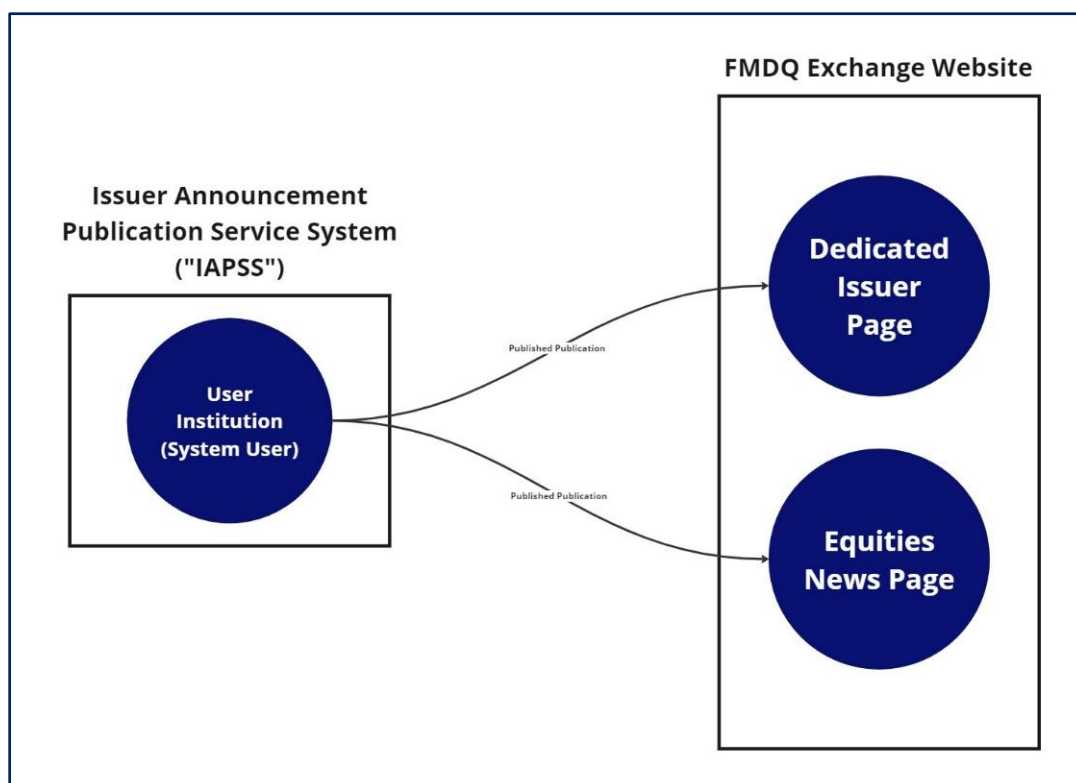
- User Institutions
- FMDQ System Administrators (“QCG”)
- Investors and the Public (they will be able to view the notifications via the Equities news page on the FMDQ Exchange website)

The system will have modules to cater for but not limited to generating or uploading publications, approving publications, and publishing notifications. The overall goal of the IAPSS is to enhance the efficiency, accuracy, turnaround time, and transparency of publications being made by User Institutions to the public and/or investors.

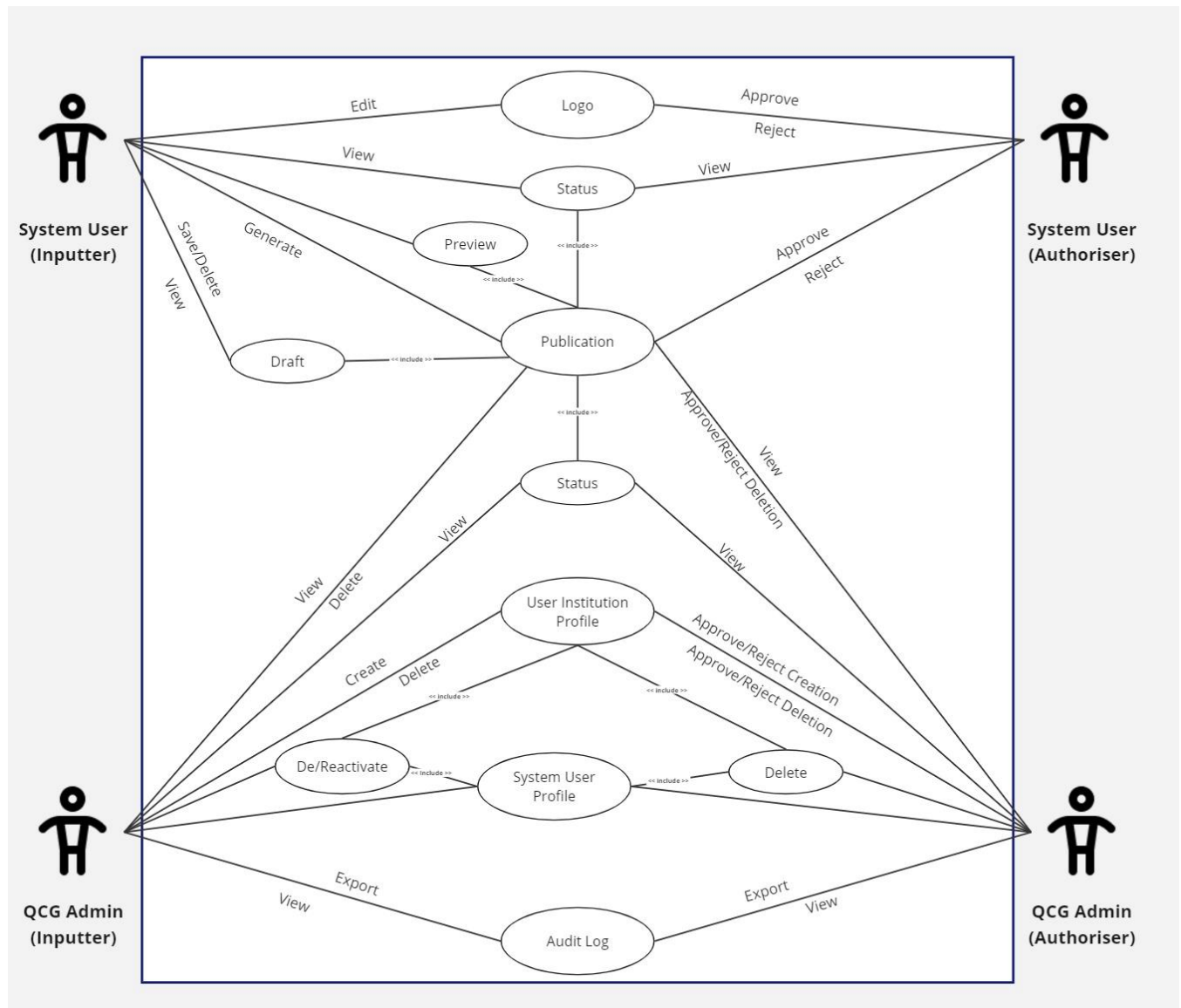
4 FUNCTIONAL SPECIFICATIONS

4.1 Context Diagram

The context diagram illustrates the interaction between the IAPSS and its external entities. At the centre of the diagram is the IAPSS, depicted as a standalone self-service portal/website. The primary external entities include FMDQ Exchange Equity Issuers (User Institutions), and the dedicated Equity news page and Issuer pages on the FMDQ website. User Institutions utilise the IAPSS to directly publish notifications, disclosures, and announcements. These publications are then pushed to two key destinations: the dedicated Equity news page and the corresponding Issuer pages on the FMDQ website (note that these pages are yet to exist on the FMDQ Exchange website. Their availability is dependent on the launch of the Equities Market). The equity news page serves as a platform for disseminating important information to investors and the public, while the Issuer pages provide specific updates relevant to each User Institution.



4.2 Use Case Diagram



4.3 System Actors & Activities

The proposed system to consist of the following major actors and their activities:

S/N	ACTORS	FREQUENCY OF USE	SECURITY/ACCESS, FEATURES
1.	User Institution – Inputter	<ul style="list-style-type: none"> Need Basis 	<ul style="list-style-type: none"> Generate New Publication (Type as Text/Upload PDF) View Previous Publication View Publication Status Save Publication as Draft View Draft Delete Draft Preview Publication Publish Publication Edit/Update Logo

2.	User Institution – Authoriser	<ul style="list-style-type: none"> Need Basis 	<ul style="list-style-type: none"> Approve Publication Reject Publication View Pending Publications View Publication Status Approve Logo Update Reject Logo Update
3.	System Admin – Inputter	<ul style="list-style-type: none"> Need Basis 	<ul style="list-style-type: none"> Profile User Institution Profile System User View System User View User Institution Delete Publication Deactivate/Reactivate/Delete User Institution Deactivate/Reactivate/Delete System User Delete Publication
4.	System Admin – Authoriser	<ul style="list-style-type: none"> Need Basis 	<ul style="list-style-type: none"> Approve Profiling of User Institution Approve Profiling of System User View System User(s) View User Institution(s) Approve/Reject Deletion of Publication Approve/Reject Deactivation/Reactivation/Deletion User Institution Approve/Reject Deactivation/Reactivation/Deletion System User Approve/Reject Publication Deletion View/Export Audit Log

4.4 High-Level User Requirements

The following are high level requirements of the proposed system, considering all major classes/categories of user:

- The system must feature a user-friendly interface that allows users, regardless of their technical expertise, to easily navigate and interact with the system
- The system shall permit users to authenticate securely into the system with role-based access control, ensuring that they only have access to functionalities relevant to their roles
- User Institutions shall be able to upload and manage their logos within the system. Any changes to the logo must require approval from designated Authorisers
- The QCG Admin shall have the ability to manage user profiles for User Institutions/System Users, including the creation, modification, deletion, deactivation, and reactivation of user accounts
- System User Authorisers shall be able to review and approve or reject publications submitted by Inputters

- System User Authorisers must provide an attestation of the accuracy of approved publications before they are published
- Inputters shall have the capability to create new publications by providing relevant details such as title and text content or upload of a PDF file. They should also be able to manage draft publications, edit existing publications, and track the status of all publications submitted through the system
- Inputters shall be able to preview publications before submission to ensure accuracy and formatting consistency. The system should support basic formatting options such as bold, italics, and underline for text content
- The system must provide quick responses and minimal latency, ensuring efficient interactions, especially during times of market volatility
- The system must be scalable to handle an increasing number of users, while maintaining performance

These high-level user requirements provide a foundation for the development and implementation of the IAPSS, ensuring that the system meets the needs of its users, while aligning with the Equity Markets information dissemination standards and user expectations.

4.5 System Utilisation

Although the Equities market is yet to launch, the system is estimated to have over five hundred (**500**) users and over two hundred (**200**) concurrent users. The system must be built to manage an increasing number of users, data upload, workflow approvals and data display. The system will be utilised by User Institutions within the Equities Market and QCG. The system will experience activity everyday including weekends and public holidays and should be always available.

4.6 General System Features

S/N	Module/Screen	Descriptions/Specifications
1.	User Access/Authorisation	<ul style="list-style-type: none"> Upon successful creation of a user's profile by the System Admin, the system shall send a notification email indicating successful profiling to the email of the designated user containing their login credentials The login credentials shall contain the user's email and a system generated temporary password to be changed upon first login to the system Upon initial login to the system, users will be presented with the FMDQ Data Privacy notice, and they must agree to its contents to proceed with interacting with the system The system shall permit all users (System Users within the User Institution & QCG Admin) to authenticate themselves using their unique credentials (email and password) to access the system The system shall strictly follow the FMDQ Group's Password Policy as defined in the 'Security and Privacy' section The system shall enforce role-based access control to restrict user access based on their assigned roles (Inputter or Authoriser) Each role shall have predefined permissions as seen in the 'Systems Actors and Activities' section in 4.3, governing the actions users can perform within the system
2.	Approval Workflow	<ul style="list-style-type: none"> The system shall always send system notifications within the notification tab and email notifications to designated Authorisers when an action is being performed by the Inputter of either the System Users within the User Institution of the QCG Admin Notifications shall include details of the pending actions, such as title, date, and time of submission, along with a link to access the publication in the IAPSS Authorisers shall have access to a dedicated interface within the IAPSS to view pending actions awaiting their approval The interface shall display pending actions in a list view, showing details such as title, date, name of Inputter and time of submission Authorisers shall have the ability to approve or reject pending actions from the designated interface

		<p>Approve</p> <ul style="list-style-type: none"> ▪ Upon approval, the action shall become authorised and approved. A system notification and an email notification shall be sent to the Inputter and Authoriser confirming their action ▪ In instances of publications approval, before approving a publication made by an Inputter of a User Institution, Authorisers shall be required to make an attestation confirming the accuracy of the information contained in the publication and their authorisation to make the publication on behalf of the institution ▪ Authorisers shall not be able to approve a publication without providing the required attestation <p>Rejection</p> <ul style="list-style-type: none"> ▪ Upon rejection, the Authoriser shall have the option to provide a reason for rejection, which will be communicated to the Inputter via email ▪ The system shall also generate a notification within the designated notifications tab and send emails to both the Inputter and Authoriser containing details of the rejected action(s)
3.	Notifications	<ul style="list-style-type: none"> ▪ Upon profile creation for a user institution or system user, a system notification should be displayed within the IAPSS notifications tab/interface, and the notification shall include details such as the successful or failed creation of the profile, the name of the user institution or system user, name of the QCG Admin who is creating the profile and any relevant identifiers ▪ In the event of a successful creation, the system shall send success notifications to the System User's alongside the QCG Admin's notifications tab and email ▪ The email notification to the System User of the User Institution should contain login credentials (username and temporary password), instructions for accessing the IAPSS, and any other pertinent information ▪ The email subject should clearly indicate the purpose of the notification, such as "IAPSS Profile Creation Confirmation", to avoid confusion ▪ In the event of a failed profile creation, the system shall send notification only to the QCG Admin's notification tab and email ▪ The email template must be professionally formatted and branded, reflecting the identity of the IAPSS, and ensuring clarity of information

		<ul style="list-style-type: none"> ▪ The content of both system and email notifications must be consistent and aligned with the information provided during the profile creation process ▪ For every action made by the Inputter or Authoriser of either the System User or QCG Admin, a notification shall be generated and sent to all responsible parties involved
4.	Audit Logs	<ul style="list-style-type: none"> ▪ The system shall capture all relevant actions performed within the IAPSS, including but not limited to User Institution profiling, System User profiling, publication generation, publication approval/rejection, and any administrative actions ▪ Each log entry shall include a timestamp indicating the date and time when the action was performed ▪ Audit logs shall identify the user who initiated the action, whether it is an Inputter or Authoriser ▪ The log entry must provide a clear description of the action performed, including details such as the type of action, the object or entity affected, and any relevant parameters ▪ The log entry shall indicate the outcome or result of the action, such as whether a publication was approved, rejected, or deleted ▪ The audit logs must be securely stored within the system to prevent unauthorised access or tampering ▪ Authorised users with appropriate permissions (only the QCG Authoriser Admins) shall be able to access, view and export audit logs within the IAPSS interface

5 FUNCTIONAL REQUIREMENTS

5.1 QCG ADMIN FEATURES - Profiling User Institutions & System Users

S/N	Screen	Requirement Definition
1.	Admin Interface	<ul style="list-style-type: none"> ▪ The system shall include a System Administrator module for the QCG Admin within FMDQ ▪ This module shall be accessible by the QCG Admin by providing their login details (valid FMDQ email address and encrypted password) ▪ The system shall verify and validate the login details and grant the user access to the QCG Admin module based on their role (Inputter or Authoriser)

S/N	Screen		Requirement Definition												
2.	User Institution Profiling	Data Capture	<ul style="list-style-type: none">▪ Upon login to the QCG Admin Inputter module, the system shall include a dashboard with a dedicated tab to profile User Institutions▪ Given that the QCG Inputter clicks on the 'Profile User Institution' tab, the system shall navigate the user to a page that displays a form with the following required fields to be filled by the QCG Inputter:<ol style="list-style-type: none">1. User Institution – Name2. Sector3. RC Number4. Registered Address5. Email Address6. Logo<table><tr><td>User Institution</td><td>XYZ Corporation Limited</td></tr><tr><td>Sector</td><td>Manufacturing</td></tr><tr><td>RC Number</td><td>192837</td></tr><tr><td>Registered Address</td><td>1, Maitama Avenue, FCT, Abuja</td></tr><tr><td>Email Address</td><td>info@xyzcorp.com</td></tr><tr><td>Upload Logo</td><td>(the "Admin" shall be able to upload a PNG file"</td></tr></table>▪ Within the profile of the User Institution, the QCG Admin shall be able to include a link to the User Institutions page on the FMDQ Exchange website (as required in Use Case-5)▪ When the QCG Inputter clicks the button to approve, the system shall prompt the QCG Inputter to select the desired QCG Authoriser▪ The system shall include a display that allows the QCG Inputter to view a list of all User Institutions that have been profiled on the system. The user shall be able to filter this data and export as a MS Excel file or PDF	User Institution	XYZ Corporation Limited	Sector	Manufacturing	RC Number	192837	Registered Address	1, Maitama Avenue, FCT, Abuja	Email Address	info@xyzcorp.com	Upload Logo	(the "Admin" shall be able to upload a PNG file"
	User Institution	XYZ Corporation Limited													
Sector	Manufacturing														
RC Number	192837														
Registered Address	1, Maitama Avenue, FCT, Abuja														
Email Address	info@xyzcorp.com														
Upload Logo	(the "Admin" shall be able to upload a PNG file"														
	Approval		<ul style="list-style-type: none">▪ Upon selection, the system shall move this action to the selected QCG Authoriser to approve the User Institution to be profiled▪ The system shall provide the QCG Authoriser with two actions: Approve:▪ If the QCG Authoriser clicks the 'Approve' action, then the system shall create a profile for the User Institution within the IAPSS and automatically send a notification email containing successful												

S/N	Screen	Requirement Definition
		<p>profiling details and log-in details to the email of the User Institution</p> <ul style="list-style-type: none"> The system shall also mirror the notification email within the 'Notifications' tab of the QCG Inputter, informing them of their action <p>Reject:</p> <ul style="list-style-type: none"> If the QCG Authoriser clicks on the 'Reject' button, then the system shall display a field for the Authoriser to input their 'Reason for Rejection' The system shall automatically send a notification email to the QCG Inputter informing them about the rejection. The email shall also include the reason for rejection The system shall also mirror the notification email within the 'Notifications' tab of the QCG Inputter and QCG Authoriser
	Manage User Institutions	<ul style="list-style-type: none"> The system shall include a tab within the QCG Inputter or Authoriser Admin interface for the "Profiled User Institutions" The system shall display a list of all user institutions that have been profiled, including details such as name, sector, RC number, and registered address The QCG Admin shall be able to utilise filter options provided by the system to refine the list based on specific criteria such as sector, RC number, or registered address The system shall apply the selected filters and updates the list accordingly The system shall present the QCG Admin with the options to export the filtered list of profiled user institutions The QCG Admin shall be able to select the export option and chooses the desired format (MS Excel or PDF) for the exported file The system shall generate the export file containing the filtered list of profiled user institutions in the selected format and automatically download the export file to the QCG Admin's local device for further analysis or sharing The QCG Inputter shall be able to edit User Institution profile

S/N	Screen		Requirement Definition										
			<ul style="list-style-type: none">▪ Upon initiation of this action, the system shall ensure approval of the action by the QCG Authoriser before the update will take place on the system▪ If there are no user institutions currently profiled in the system, the system shall display a message indicating the absence of data and offer options for the QCG Admin to return to the main dashboard or perform other actions										
3.	System User Profiling	Data Capture	<ul style="list-style-type: none">▪ Upon login to the QCG Admin Inputter module, the system shall include a dashboard with a dedicated tab to profile System Users▪ Given that the QCG Inputter clicks on the 'Profile System User' tab, the system shall navigate the user to a page that displays a form with the following required fields to be filled by the QCG Inputter:<ol style="list-style-type: none">1. First Name2. Last Name3. Email Address4. User Institution (dropdown displaying a list of all profiled User Institutions)5. Role (dropdown displaying 'Inputter' or 'Authoriser')<table><tr><td>First Name</td><td>Sharon</td></tr><tr><td>Last Name</td><td>Oyakhamoh</td></tr><tr><td>Email Address</td><td>sharon.oyakhamoh@xyzcorp.com</td></tr><tr><td>User Institution</td><td>[to be selected from a drop-down field containing all profiled User Institutions]</td></tr><tr><td>Role</td><td>[to be selected from a drop-down field containing two (2) role options – "Inputter" or "Authoriser"]</td></tr></table>▪ When the QCG Inputter clicks the button to approve, the system shall prompt the QCG Inputter to select the desired QCG Authoriser▪ The system shall include a display that allows the QCG Inputter to view a list of all Users that have been profiled on the system. The user shall be able to filter this data and export as a MS Excel file or PDF	First Name	Sharon	Last Name	Oyakhamoh	Email Address	sharon.oyakhamoh@xyzcorp.com	User Institution	[to be selected from a drop-down field containing all profiled User Institutions]	Role	[to be selected from a drop-down field containing two (2) role options – "Inputter" or "Authoriser"]
First Name	Sharon												
Last Name	Oyakhamoh												
Email Address	sharon.oyakhamoh@xyzcorp.com												
User Institution	[to be selected from a drop-down field containing all profiled User Institutions]												
Role	[to be selected from a drop-down field containing two (2) role options – "Inputter" or "Authoriser"]												
		Approval	<ul style="list-style-type: none">▪ Upon selection, the system shall move this action to the QCG Authoriser to approve the System User to be profiled▪ The system shall provide the QCG Authoriser with two actions:										

S/N	Screen		Requirement Definition
			<p>Approve</p> <ul style="list-style-type: none"> ▪ If the QCG Authoriser clicks the 'Approve' action, then the system shall create a profile for the System User for the desired User Institution within the IAPSS and automatically send a notification email containing successful profiling details and log-in details to the email of the System User to login with their email and a system generated temporary password to be changed upon first login ▪ The system shall also mirror the notification email within the 'Notifications' tab of the QCG Inputter, informing them of their action <p>Reject</p> <ul style="list-style-type: none"> ▪ If the QCG Authoriser clicks on the 'Reject' button, then the system shall display a field for the Authoriser to input their 'Reason for Rejection' ▪ The system shall automatically send a notification email to the QCG Inputter informing them about the rejection. The email shall also include the reason for rejection ▪ The system shall also mirror the notification email within the 'Notifications' tab of the QCG Inputter and QCG Authoriser ▪ The system shall include a display that allows the QCG Authoriser to view a list of all Users that have been profiled on the system. The user shall be able to filter this data and export as a MS Excel file or PDF
		Manage System Users	<ul style="list-style-type: none"> ▪ The system shall include a tab within the QCG Inputter or Authoriser Admin interface for the "Profiled System Users" ▪ The system shall display a list of all System Users that have been profiled, including details such as first name, last name, email address, user institution and role ▪ The QCG Admin shall be able to utilise filter options provided by the system to refine the list based on specific criteria such as user institution, role, name, etc ▪ The system shall apply the selected filters and update the list accordingly ▪ The system shall present the QCG Admin with the options to export the filtered list of profiled system users

S/N	Screen		Requirement Definition
			<ul style="list-style-type: none"> ▪ The QCG Admin shall be able to select the export option and choose the desired format (MS Excel or PDF) for the exported file ▪ The system shall generate the export file containing the filtered list of profiled system users in the selected format and automatically download the export file to the QCG Admin's local device for further analysis or sharing ▪ The QCG Inputter shall be able to edit the System User's profile ▪ Upon initiation of this action, the system shall ensure approval of the action by the QCG Authoriser before the update will take place on the system ▪ If there are no System Users currently profiled in the system, the system shall display a message indicating the absence of data and offer options for the QCG Admin to return to the main dashboard or perform other actions
		User Login	<ul style="list-style-type: none"> ▪ Given that the System User's profile has been successfully created on IAPSS, then the system shall send a notification email indicating successful profiling to the email of the designated System User containing their login credentials ▪ The login credentials shall contain the System User's email and a system generated temporary password to be changed upon first login to the system ▪ Upon first login to the system, the system shall display two fields: <ol style="list-style-type: none"> 1. Email 2. Password ▪ When the user clicks the login button, the system shall prompt a display with two fields: <ol style="list-style-type: none"> 1. Change Password 2. Confirm Password ▪ Upon clicking the login button, the system shall grant the System User access to the system. The system shall automatically recognise the newly changed password as the password for that System User ▪ For subsequent logins, the system shall only display only the Email and Password field

S/N	Screen	Requirement Definition
		<ul style="list-style-type: none"> The system shall also have a 'Forgot Password?' hyperlink on the login page that allows users to reset their password The system shall enforce the use of the FMDQ Group Password Policy

5.2 SYSTEM USER - INPUTTER FEATURES

5.2.1 Publications

5.2.1.1 Generating Publication (Type as Text or PDF Upload)

5.2.1.1.1 Use Case

UC-5	Generating Publication Use Case
Description	<ul style="list-style-type: none"> This use case describes the process initiated by an Inputter to generate a publication by typing the content directly into the system or PDF upload
Primary Actor(s)	<ul style="list-style-type: none"> System User – Inputter
Trigger	<ul style="list-style-type: none"> The Inputter decides to create a new publication and chooses the option to type the content as text or upload a PDF
Pre-Conditions	<ul style="list-style-type: none"> The Inputter must be logged into the IAPSS
Post-Conditions	<ul style="list-style-type: none"> The publication is transmitted to the Authoriser for approval Both the Inputter and Authoriser are notified of the publication submission
Main Success Scenario	<ol style="list-style-type: none"> The Inputter navigates to the "Generate New Publication" option within the IAPSS interface The system presents the Inputter with the choice to type the publication content directly or upload PDF The Inputter selects the option to type as text and proceeds The system prompts the Inputter to fill in the required fields for the publication, including: <ul style="list-style-type: none"> Publication Title Publication Text The Inputter inputs the publication title and text (the system ensures that the title is in all capital letters no matter how it was entered by the Inputter) and utilises any desired formatting options such as Underline, Italics, or Bold for the text



UC-5	Generating Publication Use Case
	<p>6. After completing the publication content, the Inputter reviews it for accuracy and completeness</p> <p>7. The system offers options to the Inputter:</p> <ul style="list-style-type: none">▪ Preview: Allows the Inputter to preview the publication before finalising▪ Save as Draft: Allows the Inputter to save the publication as a draft for future completion. The system shall include an interface that allows the Inputter to view or delete drafts as desired▪ Publish: Allows the Inputter to proceed with publishing the generated publication <p>8. If the Inputter chooses to preview, the system displays a preview of the publication and automatically embeds the following:</p> <ul style="list-style-type: none">▪ The User Institution's logo▪ An automatically generated IAPS number (format should be <<random 4 alphanumeric string + date (dd/mm/yyyy format) + time (24-hour format)>> e.g., 13G4/21042024/1043)▪ A link to the User Institution's page on the FMDQ website▪ The date and time of the publication <p>9. The Inputter selects the "Publish" option</p> <p>10. The system prompts the Inputter to select the desired Authoriser from a list of available Authorisers within the User Institution</p> <p>11. After selection, the system transmits the publication to the designated Authoriser for approval</p> <p>12. Both the Inputter and Authoriser receive notifications via email and the system's notifications tab about the publication submission</p>
Alternative Flow	<p>1. In Step 2 of the normal flow, if the Inputter selects the 'Upload PDF' option</p> <p>2. Then the system shall display a pop-up and an option to copy (these will be included within the System User's Publication outside of the system):</p> <ul style="list-style-type: none">▪ An automatically generated IAPS number (format should be <<random 4 alphanumeric string + date (dd/mm/yyyy format) + time (24-hour format)>> e.g., 13G4/21042024/1043)▪ A link to the User Institution's page on the FMDQ website <p>3. The System User clicks Next</p>

UC-5	Generating Publication Use Case
	<ol style="list-style-type: none"> The system prompts the Inputter to upload the PDF file containing the publication content The Inputter selects the desired PDF file from their local device and uploads it to the system The Inputter selects the "Publish" option Use Case resumes at Step 10
Exceptions	<ol style="list-style-type: none"> If there are errors in the input provided by the Inputter, such as missing mandatory fields or incorrect data formats, the system should display appropriate error messages and guide the Inputter on how to rectify them If the uploaded file is not in a valid PDF format, the system should prompt the Inputter to upload a valid PDF file and provide appropriate error messages
Special Requirements	N/A

5.2.1.2 View Publication Status

5.2.1.2.1 Use Case

UC-6	View Publication Status Use Case
Description	This use case describes how an Inputter views the status of generated or uploaded publications within the IAPSS
Primary Actor(s)	System User – Inputter
Trigger	The Inputter decides to check the status of a publication they have previously generated or uploaded
Pre-Conditions	<ol style="list-style-type: none"> The Inputter must be logged into the IAPSS The Inputter has previously generated a publication
Post-Conditions	<ol style="list-style-type: none"> The Inputter has successfully viewed the status of the publication and, if necessary, sent reminders to the designated Authoriser for pending publications The Authoriser receives the reminder notification and can take appropriate action on the pending publication
Main Success Scenario	<ol style="list-style-type: none"> The Inputter accesses the IAPSS dashboard to view the status of publications Within the publication status interface, the Inputter is presented with a list of publications that they have initiated. The system also allows the Inputter to search for the specific publication they want to check the status of The system displays the status of the publication, indicating whether it is pending, approved, rejected

	<ol style="list-style-type: none"> If the publication status is pending, approved, or rejected, the Inputter may review the publication details and associated information There shall be an option within each row/record for the Inputter to download the publication The Inputter can navigate back to the dashboard or relevant section upon completion
Alternative Flow	<ol style="list-style-type: none"> In Step 3 of the normal flow, if the publication status is pending i.e., awaiting approval: <ul style="list-style-type: none"> The Inputter is presented option to send a reminder to the designated Authoriser The Inputter can decide to send the reminder immediately or select a desired date and time to send the reminder The Inputter shall be able to configure reminders to send daily weekly at a particular time The system prompts the Inputter to confirm the action Upon confirmation, the system generates and sends a reminder notification to the designated Authoriser via email and within the system's notifications tab Use Case resumes at Step 4
Exceptions	N/A
Special Requirements	N/A

5.2.1.3 User Institution Edit/Update Logo

5.2.1.3.1 Use Case

UC-7	Logo Update (Inputter) Use Case
Description	This use case outlines the process followed by an Inputter to edit the logo associated with their User Institution on the IAPSS
Primary Actor(s)	System User - Inputter
Trigger	The Inputter wants to update or modify the logo representing their User Institution on the IAPSS
Pre-Conditions	The Inputter must be logged into the IAPSS
Post-Conditions	<ol style="list-style-type: none"> The logo associated with the User Institution has been successfully edited and updated on the IAPSS The Inputter can view the updated logo within the system's interface Any publications or communications generated by the User Institution will now display the updated logo
Main Success Scenario	<ol style="list-style-type: none"> The Inputter navigates to the "Edit Logo" section within their dashboard


UC-7	Logo Update (Inputter) Use Case
	<ol style="list-style-type: none"> The system displays the current logo associated with the User Institution The Inputter selects the option to upload a new logo or replace the existing one The system prompts the Inputter to choose a logo file from their local storage (PNG and must not be more than 2MB – these requirements should be displayed to the Inputter) The Inputter selects the desired logo file and confirms the upload action The system validates the uploaded logo file to ensure it meets the specified requirements If the uploaded logo meets the validation criteria, the system replaces the existing logo with the new one The system notifies the Inputter of the successful logo update and displays the updated logo on the interface The Inputter confirms the changes and navigates back to the dashboard or relevant section
Alternative Flow	<ol style="list-style-type: none"> In Step 6 of the normal flow, if the uploaded logo file does not meet the required format, the system shall display an error message prompting the Inputter to upload a valid logo file The Inputter uploads an appropriate logo that meets the requirement Use Case resumes at Step 7
Exceptions	<ol style="list-style-type: none"> If the uploaded logo file exceeds the maximum allowed size or is an inappropriate format (i.e., not PNG), the system should reject the upload and notify the Inputter to select a smaller PNG file System Error: If an unexpected error occurs during the logo upload process (e.g., server error, network interruption), the system should display a friendly error message and advise the Inputter to try again later
Special Requirements	N/A

5.3 SYSTEM USER - AUTHORISER FEATURES

5.3.1 Publication

5.3.1.1 Rejection/Approval

5.3.1.1.1 Use Case

UC-8	Reject/Approve Publication Use Case
Description	This use case describes the process followed by an Authoriser to review and act on publications submitted for approval by Inputters within their User Institution on IAPSS
Primary Actor(s)	System User – Authoriser
Trigger	<ol style="list-style-type: none"> 1. The Authoriser receives a notification or accesses the system to review pending publications awaiting approval 2. A reminder is triggered by the Inputter on a publication that is awaiting approval
Pre-Conditions	<ol style="list-style-type: none"> 1. The Authoriser must be logged into the IAPSS 2. The user must be an Authoriser (i.e., they must have the necessary permissions to review and approve/reject publications for their User Institution)
Post-Conditions	<ol style="list-style-type: none"> 1. The pending publication has been reviewed and either approved or rejected by the Authoriser 2. The publication status is updated accordingly in the system 3. Email notifications are sent to relevant parties (Inputter, Authoriser) to communicate the outcome of the approval/rejection process
Main Success Scenario	<ol style="list-style-type: none"> 1. The Authoriser navigates to the "Pending Publications" section within the system's interface on their dashboard 2. The system displays a list of pending publications, showing details such as publication title, date submitted, 3. Upon clicking a publication, the Authoriser will be displayed with a preview of the publication 4. The Authoriser review its content and associated details 5. If satisfied with the publication, the Authoriser selects the "Approve" action 6. The system prompts the Authoriser to provide an attestation confirming the accuracy of the information and their authorization to approve the publication 7. The Authoriser enters the attestation statement as required by the system <div>  <p>I attest to the accuracy of the information contained in this publication and confirm that I have the authorisation of the institution to make this publication.</p> </div>

UC-8	Reject/Approve Publication Use Case
	<ol style="list-style-type: none"> The system records the approval action along with the Authoriser's attestation and updates the publication status to "Approved" An email notification is sent to both the Inputter and Authoriser confirming the publication approval or rejection, including details such as publication title, date, time, and IAPS number The publication is published to the User Institution's page on the FMDQX website and the Equities page
Alternative Flow	<ol style="list-style-type: none"> In Step 5 of the normal flow, if the Authoriser identifies any issues or discrepancies in the publication, they select the "Reject" action The system prompts the Authoriser to provide a reason for rejection, which may include specific feedback or instructions for revision The Authoriser enters the rejection reason as required by the system The system records the rejection action along with the provided reason and updates the publication status to "Rejected" Use Case resumes at Step 9
Exceptions	N/A
Special Requirements	<ol style="list-style-type: none"> If the System User generates a publication by typing as text, upon successful publishing of the publication, the system shall convert the publication to a PDF both on IAPSS and the FMDQX Website

5.3.1.2 View Previous Publications (System Inputter & Authoriser)

5.3.1.2.1 Use Case

UC-9	View Previous Publications (System Inputter/Authoriser)
Description	This use case describes the process by which an Inputter and/or Authoriser accesses and views previously approved or rejected publications within their User Institution on the IAPSS
Primary Actor(s)	System User – Inputter System User - Authoriser
Trigger	The Inputter/Authoriser navigates to the "View Previous Publications" section within the system's interface on their dashboard
Pre-Conditions	<ol style="list-style-type: none"> The Inputter/Authoriser must be logged into the IAPSS The Inputter/Authoriser wants to view previous publications for their User Institution
Post-Conditions	<ol style="list-style-type: none"> The Inputter/Authoriser has successfully accessed and viewed previous publications within the IAPSS

UC-9	View Previous Publications (System Inputter/Authoriser)
	2. The Inputter/Authoriser can perform further actions based on the information being viewed while reviewing previous publications, such as data export
Main Success Scenario	<ol style="list-style-type: none"> 1. The Inputter/Authoriser selects the "View Previous Publications" option from the available menu or navigation bar 2. The system retrieves and displays a list of previous publications associated with the User Institution, sorted chronologically with the most recent publications first 3. The Inputter/Authoriser reviews the list of publications and may use filters or search functionality to locate specific publications based on criteria such as publication title, date, or status 4. The Inputter/Authoriser can decide to export the list view as MS Excel file or PDF 5. The Inputter/Authoriser can select a publication from the list to view its details and content 6. The system presents the selected publication in a readable format, including the publication title, content, date of publication, approval status 7. The Inputter/Authoriser may scroll through the publication content and review its accuracy and completeness 8. If necessary, the Inputter/Authoriser can download or print the publication for offline reference or documentation purposes 9. After reviewing the publication, the Inputter/Authoriser can navigate back to the list of previous publications to continue browsing or exit the view
Alternative Flow	N/A
Exceptions	1. If there are no previous publications available for the User Institution, the system should display a message indicating the absence of data and provide options for the Inputter/Authoriser to return to the main dashboard or perform other actions
Special Requirements	N/A

5.3.2 User Institution Logo

5.3.2.1 Logo Rejection/Approval

5.3.2.1.1 Use Case

UC-10	Logo Rejection/Approval
Description	This use case outlines the process by which an Authoriser approves or rejects the update of a User Institution's logo within the IAPSS
Primary Actor(s)	System User – Authoriser
Trigger	The Authoriser receives a notification or accesses the pending logo update request within the system

UC-10	Logo Rejection/Approval
Pre-Conditions	<ol style="list-style-type: none"> 1. The Authoriser must be logged into the IAPSS 2. The user must be an Authoriser (i.e., they must have the necessary permissions to review and approve/reject publications for their User Institution)
Post-Conditions	<ol style="list-style-type: none"> 1. If approved, the User Institution's logo is updated with the new logo, reflecting the changes in the system 2. If rejected, the Inputter and Authoriser are informed of the rejection along with the reason provided by the Authoriser 3. The system maintains a log of the approval/rejection action for auditing purposes
Main Success Scenario	<ol style="list-style-type: none"> 1. The Authoriser navigates to the designated Logo Approval/Rejection section within the system's interface 2. The system displays a list of pending logo update requests, including details such as the User Institution's name, current logo, and the proposed new logo 3. The Authoriser selects a pending logo update request from the list to review its details 4. The system presents the details of the logo update request, including the current logo and the proposed new logo for comparison 5. The Authoriser examines the proposed new logo to ensure it aligns with the User Institution's branding guidelines and standards 6. The Authoriser approves the update by selecting the "Approve" option provided by the system 7. The system updates the User Institution's logo with the approved new logo and notifies relevant stakeholders (via system's notifications tab and email), including the Inputter and Authoriser, of the approval
Alternative Flow	<ol style="list-style-type: none"> 1. In Step 5 of the normal flow, if the new logo does not meet the requirements or standards, the Authoriser rejects the update by selecting the "Reject" option provided by the system 2. The system prompts the Authoriser to provide a reason for the rejection, which may include details or suggestions for improvement 3. The Authoriser submits the rejection along with the reason provided 4. The system notifies the Inputter and Admin of the rejection, providing the reason provided by the Authoriser for further action
Exceptions	<ol style="list-style-type: none"> 1. If there are no pending logo update requests for the User Institution, the system should display a message indicating the absence of pending actions and provide

UC-10	Logo Rejection/Approval
	options for the Authoriser to return to the main dashboard or perform other actions
Special Requirements	N/A

5.4 QCG ADMIN FEATURES

5.4.1 Publications

5.4.1.1 Delete Publications

5.4.1.1.1 Use Case - Delete Publications

UC-11	Delete Publications Use Case
Description	This use case outlines the process by which the QCG Inputter views and deletes publications within the IAPSS
Primary Actor(s)	QCG Inputter
Trigger	Outside of the system, there has been a request by a User Institution's representative to delete a publication
Pre-Conditions	The QCG Inputter must be logged into the IAPSS
Post-Conditions	<ol style="list-style-type: none"> 1. The selected publication(s) have been successfully deleted from the system 2. The list of publications is updated to reflect the deletion(s)
Main Success Scenario	<ol style="list-style-type: none"> 1. The QCG Inputter navigates to the "View All Publications" section or similar functionality within the system's interface 2. The system presents a list of all publications stored within the IAPSS, including details such as publication title, inputter's name, input date, User Institution name, Authoriser's name, approval date, and publication status 3. The QCG Inputter reviews the list of publications to identify the one(s) they wish to delete 4. The QCG Inputter selects the publication(s) they want to delete from the list 5. The QCG Inputter includes a reason for deletion 6. The system prompts the QCG Inputter to confirm the deletion action 7. The QCG Inputter confirms the deletion action 8. The publication(s) to be deleted will be transmitted to the QCG Authoriser's queue for deletion. A system notification and email will be sent to the QCG Inputter and Authoriser accordingly appropriately capturing the action to be performed
Alternative Flow	N/A
Exceptions	N/A
Special Requirements	N/A

5.4.1.2 View All Publications

5.4.1.2.1 Use Case – View All Publications

UC-12	View All Publications Use Case
Description	This use case outlines the process by which the QCG Admin views all publications made by the System Users within all User Institutions
Primary Actor(s)	<ol style="list-style-type: none"> 1. QCG Inputter 2. QCG Authoriser
Trigger	The QCG Admin logs in to the IAPSS and navigates to the "View All Publications" section
Pre-Conditions	The QCG Admin must be logged into the IAPSS
Post-Conditions	<ol style="list-style-type: none"> 1. The QCG Admin has successfully viewed all publications 2. The QCG Admin has exported a view of publications data on the IAPSS
Main Success Scenario	<ol style="list-style-type: none"> 1. The QCG Admin logs in to the IAPS using their login credentials 2. The QCG Admin navigates to the "View All Publications" section 3. The system retrieves and displays a list of all publications made by User Institutions 4. The QCG Admin reviews the list, which includes details such as publication titles, authors, dates, and status 5. The QCG Admin can scroll through the list to view additional publications 6. QCG Admin can filter the list based on specific criteria, such as publication status, User Institution, or date range 7. The QCG Admin may choose to export the list as an Excel or PDF file 8. The system automatically downloads the exported view of the page to the QCG Admin's local device storage
Alternative Flow	If there are no publications available, the system displays a message indicating that there are no records to show
Exceptions	If there are technical issues or system errors preventing the retrieval of publications, the system displays an error message and prompts the QCG Admin to try again later or contact support for assistance.
Special Requirements	N/A

5.4.1.3 Approve/Reject Action to Delete Publications

5.4.1.3.1 Use Case – Approve/Reject Publication Deletion

UC-13	Approve/Reject Publication Deletion Use Case
Description	This use case describes the process by which a QCG Authoriser approves or rejects a request to delete a publication within the IAPSS
Primary Actor(s)	QCG Authoriser
Trigger	QCG Inputter has initiated the deletion of one or more publications

Pre-Conditions	<ol style="list-style-type: none"> 1. The QCG Inputter has initiated the deletion 2. The QCG Authoriser must be logged into the IAPSS
Post-Conditions	<ol style="list-style-type: none"> 1. If approved, the requested publication is deleted from the system. The system removes the selected publication(s) from the database and updates the list of publications to reflect the deletion(s) <ul style="list-style-type: none"> ▪ The system send notification to the QCG Inputter and Authoriser via the system's notifications tab and email informing them of the action which has just occurred 2. If rejected, the publication remains unchanged in the system, and the QCG Authoriser and Inputter are notified of the rejection
Main Success Scenario	<ol style="list-style-type: none"> 1. The QCG Authoriser receives a notification or accesses the pending actions section indicating a request for approval to delete a publication 2. The QCG Authoriser reviews the details of the publication deletion request, including the reason provided for deletion and the publication to be deleted 3. The QCG Authoriser assesses the validity of the deletion request based on institutional policies, regulatory requirements, and accuracy of information 4. The Authoriser selects the option to approve the deletion 5. The system prompts the Authoriser to confirm the approval action 6. The Authoriser confirms the approval 7. The system processes the deletion of the publication from the database 8. The system sends a notification to the QCG Authoriser and Inputter informing them of the approved deletion
Alternative Flow	<ol style="list-style-type: none"> 1. In Step 3 of the normal flow, if the Authoriser rejects the deletion request: 2. The Authoriser selects the option to reject the deletion 3. The Authoriser provides a reason for the rejection 4. The system prompts the Authoriser to confirm the rejection action 5. The Authoriser confirms the rejection 6. The system notifies the QCG Authoriser and Inputter of the rejection and provides the reason, if specified
Exceptions	N/A
Special Requirements	<ol style="list-style-type: none"> 1. If a publication gets deleted and approved by the QCG Authoriser, the publication shall no longer be available on the IAPSS and FMDQX website as a disseminated publication, but shall be retained in the audit log of the IAPSS, reflecting its status

	as a deleted document with relevant details such as the initial publication date, the date of deletion and reason for deletion
--	--------------------------------------------------------------------------------------------------------------------------------

5.4.2 Manage User Institution/System Users

5.4.2.1 Deactivate/Reactivate/Delete User Institution/System User

5.4.2.1.1 Use Case

UC-14	Manage User Institution/System Users Use Case
Description	This use case outlines the process by which a QCG Inputter deactivates, reactivates, or deletes User Institutions or System Users within the IAPSS
Primary Actor(s)	<ol style="list-style-type: none"> 1. QCG Inputter 2. QCG Authoriser
Trigger	<ol style="list-style-type: none"> 1. A User Institution is yet to pay their annual system usage fee, which grants them access to the system and the applicable process for access removal has been followed 2. A User Institution has requested for their representative (Inputter/Authoriser) to be deactivated or reactivated (noting that each User Institution must have always at least one Inputter and Authoriser) 3. A User Institution has requested for their data to be expunged from the system
Pre-Conditions	The QCG Inputter must be logged into the IAPSS
Post-Conditions	<ol style="list-style-type: none"> 1. If deactivated, the User Institution/System User's access and functionalities are suspended but retained in the system 2. If reactivated, the User Institution/System User's access and functionalities are restored 3. If deleted, the User Institution/System User and associated data are permanently removed from the system
Main Success Scenario	<ol style="list-style-type: none"> 1. The QCG Inputter accesses the administrative functionalities within the IAPSS 2. The Inputter navigates to the section for managing User Institutions/System Users <p>To Deactivate</p> <ol style="list-style-type: none"> 3. The Inputter selects the option to deactivate a specific user institution/system user 4. The QCG Inputter includes their reason for deactivation 5. The system prompts the Inputter to confirm the deactivation action 6. The Inputter confirms the deactivation

7. The system informs the QCG Authoriser, and the action becomes pending for the QCG Authoriser to approve
8. The QCG Authoriser assesses the reason for the requested action
 - a. The QCG Authoriser approves the deactivation of the User Institution/System User
 - i. The system updates the status of the user institution/system user to "Deactivated" in the database
 - ii. The User Institution/System User's access and functionalities are suspended but retained in the system (i.e., the User Institution/System User will not have access to the system, but their data will be retained)
 - iii. The system sends a notification to the QCG Authoriser's and Inputter's notification tab and email, containing details about successful deactivation
 - b. The QCG Authoriser rejects the deactivation of the User Institution/System User
 - i. The QCG Authoriser includes a reason for rejection
 - ii. The system sends a notification to the QCG Authoriser's and Inputter's notification tab and email, indicating why the deactivation is rejected
- To Reactivate**
9. The Inputter selects the option to reactivate a specific user institution/system user
10. The QCG Inputter includes their reason for reactivation
11. The system prompts the Inputter to confirm the reactivation action
12. The Inputter confirms the reactivation
13. The system informs the QCG Authoriser, and the action becomes pending for the QCG Authoriser to approve
14. The QCG Authoriser assesses the reason for the requested action
 - a. The QCG Authoriser approves the reactivation of the User Institution/System User
 - i. The system updates the status of the user institution/system user to "Reactivated" in the database
 - ii. The User Institution/System User's access and functionalities are restored, and they can access the system
 - iii. The system sends a notification to the QCG Authoriser's and Inputter's notification tab and email, containing details about successful reactivation

	<ul style="list-style-type: none"> b. The QCG Authoriser rejects the reactivation of the User Institution/System User <ul style="list-style-type: none"> i. The QCG Authoriser includes a reason for rejection ii. The system sends a notification to the QCG Authoriser's and Inputter's notification tab and email, indicating why the reactivation is rejected <p>To Delete</p> <p>15. The Inputter selects the option to delete a user institution/system user</p> <p>16. The system prompts the Inputter to confirm the deletion action</p> <p>17. The Inputter confirms the deletion</p> <ul style="list-style-type: none"> ▪ The system informs the QCG Authoriser, and the action becomes pending for the QCG Authoriser to approve ▪ The QCG Authoriser assesses the reason for the requested action <ul style="list-style-type: none"> a. The QCG Authoriser approves the deletion of the User Institution/System User b. The system removes the user institution/system user and associated data from the database c. The QCG Authoriser rejects the deletion of the User Institution/System User <ul style="list-style-type: none"> i. The QCG Authoriser includes a reason for rejection ii. The system sends a notification to the QCG Authoriser's and Inputter's notification tab and email, indicating why the deletion is rejected <p>18. The system sends notifications to relevant stakeholders (i.e., QCG Inputter & Authoriser) about the performed action</p>
Alternative Flow	N/A
Exceptions	N/A
Special Requirements	<ul style="list-style-type: none"> 1. If a User Institution gets deleted/deactivated, the System Users (Inputter and Authoriser) within that User Institution shall not be able to login to the IAPSS 2. All previous publications made by that User Institution shall remain on the system and the FMDQX website for record purposes

5.4.3 Audit Log

5.4.3.1 View and Export Audit Log

5.4.3.1.1 Use Case

UC-4	Audit Log Use Case
Description	This use case describes the steps for a QCG Authoriser to view and export audit logs within the system
Primary Actor(s)	1. QCG Authoriser
Trigger	The QCG Authoriser navigates to the audit logs section of the IAPSS to review or export historical actions
Pre-Conditions	The QCG Authoriser must be logged into the IAPSS
Post-Conditions	<ol style="list-style-type: none"> 1. The QCG Authoriser gains insights into the historical actions performed within the IAPSS, aiding in monitoring compliance, identifying patterns, and detecting any anomalies 2. If exported, the audit log data is saved in the desired file format (MS Excel or PDF) for future reference or external reporting requirements
Main Success Scenario	<ol style="list-style-type: none"> 1. The QCG Authoriser accesses the audit logs section within the IAPSS Admin interface 2. The system presents a list of available audit logs, organised by date, time, and type of action. The system must have audit logs for the following but not limited to: <ul style="list-style-type: none"> ▪ User Institution profiling success ▪ User Institution profiling failure ▪ System User profiling success ▪ System User profiling failure ▪ User Institution edit ▪ User Institution deletion/reactivation/deactivation ▪ System User edit ▪ System User deletion/reactivation/deactivation ▪ System User Login/Logout Activities ▪ Generate Publication Failure/Success ▪ Document upload ▪ Document generation success ▪ Document generation failure

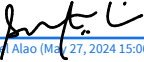


	<ul style="list-style-type: none">▪ Document upload success▪ Document upload failure▪ Document approval success▪ Document rejection success▪ Document approval failure▪ Document rejection failure▪ Document publication success▪ Document publication failure▪ Password reset success▪ Password reset failure▪ Logo upload success▪ Logo upload failure▪ Delete Publication Success▪ Delete Publication Failure <p>3. The QCG Authoriser selects the desired audit log entry to view more detailed information about a specific action</p> <p>4. If viewing detailed information:</p> <ul style="list-style-type: none">a. The system displays additional details about the selected audit log entry, including the user responsible for the action, timestamp, and description of the action performedb. The QCG Authoriser reviews the information and takes note of any relevant actions or discrepancies <p>5. If exporting audit logs:</p> <ul style="list-style-type: none">a. The QCG Authoriser selects the option to export audit logs to an external file format, such as CSV, Excel, or PDFb. The system prompts the Authoriser to specify any filtering criteria, such as date range or specific types of actions<ul style="list-style-type: none">▪ All actions from inception to date▪ All actions within a specified date range▪ All actions by a particular System User (Inputter/Authoriser) from inception to date
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<ul style="list-style-type: none">▪ All actions by a particular System User within a specified date range▪ All actions relating to a User Institution from inception to date▪ All actions relating to a User Institution within a specified date range <p>c. The QCG Authoriser confirms the export settings and initiates the export process</p> <p>d. The system generates the export file containing the requested audit log data in the specified format</p> <p>e. The QCG Authoriser downloads the export file to their local system for further analysis or archival purposes</p> <p>6. After reviewing or exporting audit logs, the QCG Authoriser may choose to return to other areas of the IAPSS interface or log out of the system</p>
Alternative Flow	N/A
Exceptions	In case of errors during the export process, such as file format compatibility issues or system constraints, the system should notify the QCG Authoriser about the error
Special Requirements	N/A



6 Document Information/Approvals for iQx Consult Limited

Document Name	Solution Specification Document
<p>Approved By</p> <p>Emmanuel Alao</p>	<p> Emmanuel Alao (May 27, 2024 15:06 GMT+1)</p> <p>-----</p> <p>Supervising Head, iQx Consult</p> <p>May 2024</p>

7 TECHNICAL REQUIREMENTS

- **Database Management:** The system must have a reliable and scalable database management system (“DBMS”) to store and manage user institution and system user details, publication data, and historical records securely. The system should also consider factors like data backup and recovery and performance optimisation
- **Data Model Design:** The system must develop a well-defined data model that accurately represents the entities, relationships, and attributes
- **Data Encryption:** The system must implement encryption mechanisms to secure sensitive data stored within the database, such as user credentials, publication content, and audit logs
- **Backup and Recovery:** The system should establish automated backup procedures to regularly backup the database and transaction logs. Implement disaster recovery mechanisms to facilitate timely restoration of data in the event of data loss or system failure
- **Data Archiving and Retention:** The system should implement data archiving and retention policies to manage the lifecycle of historical user and publication data stored within the database
- **Security Measures:** The system must implement robust security measures to protect user data, system integrity and prevent unauthorised access or malicious attacks. This includes data encryption, secure access controls, user authentication and authorisation, role-based permissions, firewall configurations, and regular security audits
- **Performance:** The system should be designed to function without any significant slowdowns or crashes
- **Scalability:** The system should be scalable, allowing it to handle an increasing number of users and data over time without requiring significant hardware upgrades
- **Availability:** The system should be highly available, with a minimum downtime or interruptions throughout the publication, user management and data management processes
- **Publication Management:** A robust publication management module should be implemented to facilitate the creation, editing, review, and approval of publications. This module should support rich text formatting, and workflow automation to streamline the publication process
- **Real-Time Communication:** The system should support real-time communication and notification mechanisms to alert users of important events such as publication submissions, approvals, and rejections
- **Usability:** The system should be user-friendly and easy to use, with a simple and intuitive user interface
- **Maintainability:** The system should be designed for easy maintenance and updates, allowing for easy bug fixes and software updates
- **Portability:** The system should be portable, meaning it can run on different hardware and software platforms without significant modification
- **Compatibility:** The system should be compatible with a wide range of devices and operating systems. This requires a responsive design that adapts to different screen sizes and resolutions, as well as support for different web browsers and mobile devices

- **Testing:** The system should undergo rigorous testing at different stages of development, including unit testing, integration testing and system testing
- **Audit Trail and Logging:** The system should maintain a detailed audit trail and logging mechanism to record all user activities, system events, and changes to publication status. This information is essential for compliance purposes, troubleshooting, and forensic analysis in case of security incidents
- **Error Handling and Exception Management:** The system should be designed to have robust error handling mechanisms to handle exceptions, edge cases, and error scenarios effectively. The system should also implement proper error logging, error messages, and exception handling to provide a smooth user experience

The above requirements are essential for IAPSS's overall performance, scalability, security, and maintainability, ensuring that the system can operate efficiently and reliably over time.

7.1 Logical Data Model/Data Dictionary

The below data requirements describe the business data needed by the system.

Entities:

- **User Attributes:** UserID, FirstName, LastName, Email, Password, RoleID
- **Role Attributes:** RoleID, RoleName
- **User Institution Attributes:** InstitutionID, InstitutionName, Sector, RCNumber, RegisteredAddress, Email, Logo
- **Publication Attributes:** PublicationID, Title, Text, DocumentID, Status, ApprovalDateTime, AuthoriserID, InputterID, InstitutionID
- **Authoriser Attributes:** AuthoriserID, UserID, InstitutionID
- **Inputter Attributes:** InputterID, UserID, InstitutionID

Relationships:

- **User - Role (One-to-Many):** Each System User can have one Role, but a Role can be assigned to many System Users or QCG Admin
- **User Institution - User (One-to-Many):** Each User Institution can have multiple System Users, but each System User belongs to only one User Institution
- **User Institution - Authoriser (One-to-Many):** Each User Institution can have multiple Authorisers, but each Authoriser belongs to only one User Institution
- **User Institution - Inputter (One-to-Many):** Each User Institution can have multiple Inputters, but each Inputter belongs to only one User Institution
- **Publication - Authoriser (Many-to-One):** Each Publication must have one Authoriser who approved it, but an Authoriser can approve multiple Publications
- **Publication - Inputter (Many-to-One):** Each Publication must have one Inputter who created it, but an Inputter can create multiple Publications

- **Publication - User Institution (Many-to-One):** Each Publication must belong to one User Institution, but a User Institution can have multiple Publications

This logical data model provides a foundation for structuring the data in the IAPSS, capturing the relationships between users and publications. The actual implementation details, including data types, constraints, and indexing, will depend on the chosen database management system.

7.2 Interface Requirements

Hardware Interfaces

The system should be able to perform with the following hardware interface requirements:

- Processor speed of 0.5ghz or more for mobile gadgets
- Processor speed of 1.5ghz or more for desktop and computer gadgets
- Ram of 500mb and above for all devices
- Free storage memory capacity of more than 100mb

Software Interfaces

The system should have a smooth performance on the following operating systems and internet browsers:

- Windows/ android/ Linux/ mac/ chrome or any other operating system
- Mozilla Firefox / Google chrome / opera mini / UC browser or internet explorer and any other browsers

Communications Interfaces

- Internet connectivity will be required for communication to occur on the system

7.3 Hardware/Software Requirements

All specifications applied in the interface requirements will be applied here also

7.4 Operational Requirements

The following requirements should be considered for system efficiency:

- **System Availability and Reliability:** The IAPSS should be always available and reliable, with a high uptime percentage. Downtime for maintenance and updates should be scheduled during off-peak hours and communicated in advance
- **User Management:** The system should provide functionality for user management, including the ability to create, and deactivate user accounts by the QCG Administrators (this action must include a maker-checker functionality)
- **Data Security and Privacy:** The system should ensure data security and privacy and other sensitive information. It should implement appropriate security measures, access controls, data encryption, and comply with relevant data protection regulations
- **Scalability and Performance:** The system should be designed to handle a growing number of users. It should be scalable and perform efficiently even with increased system usage
- **Monitoring and logging:** The system should be designed to provide real-time monitoring and logging of system activities to enable system administrators to identify and address issues promptly

- **Backup and recovery:** The system should be designed to perform regular backups and implement recovery mechanisms to ensure that data is not lost in case of system failures

7.5 Security and Privacy

- **Secure Coding Practices:** The following security and privacy requirements are critical to ensure the confidentiality, integrity, and availability of the application. The application must be compliant with industry best practices such as the OWASP Application Security Verification Standard version 4 and associated vendor recommendations (e.g., Microsoft Security Guidance, Oracle Hardening Guides, etc.). At the minimum, the application must meet the security requirements stated in here
 - a) All applications must adhere to secure coding practices, following industry standards such as OWASP (Open Web Application Security Project) guidelines
 - b) Developers must undergo training on secure coding practices and be aware of common vulnerabilities and mitigation techniques
- **Secure Development Lifecycle (SDL):**
 - a) A secure development lifecycle approach should be adopted, integrating security practices throughout the application development process
 - b) This includes security requirements gathering, threat modeling, code review, and security testing
- **Authentication and Access Control:**
 - a) Applications must implement strong authentication mechanisms, including multi-factor authentication, for user access
 - b) Access controls should be enforced based on the principle of least privilege, ensuring that users have only the necessary permissions to perform their tasks
 - c) Passwords must be securely stored using strong hashing algorithms and not transmitted in plain text. Passwords must comply with the Group's password policy. **Note** that these parameters must be configurable for flexibility.

S/N	POLICIES
1.	Users are required to change their password on first use of the application
2.	Enforce Password history for example 10
3.	Password age configuration for example 30 days
4.	Minimum password length should be set at 8 characters
5.	Password must meet complexity requirements: at least one upper case, lower case, one number (for example 0-9) and one special character (for example: ,!\$%^&*()_+ ~-=\`{}[]:~<?/.)
6.	Account lockout threshold should be set at 3 invalid login attempts
7.	Account lockout duration should be set at 30 mins

- **Input Validation and Output Encoding:**
 - a) All user inputs must be validated to prevent common vulnerabilities like SQL injection, cross-site scripting (XSS), and command injection attacks

- b) Use parameterised SQL queries: SQL queries should be crafted with user content passed into a bind variable. SQL queries should not be created dynamically using string concatenation. Similarly, the SQL query string used in a bound or parameterised query should never be dynamically built from user input. Queries written this way are safe against SQL injection attacks
- c) Output encoding should be applied to prevent HTML, JavaScript, or other malicious content injection
- **Secure Session Management:**
 - a) Applications must implement secure session management mechanisms, including the use of secure session tokens, session expiration, and session invalidation upon logout
 - b) Implement session timeout to ensure that inactive sessions are terminated after a specified time to mitigate session hijacking or fixation attacks. This helps prevent session hijacking attacks by closing the session after a certain period of inactivity
 - c) Secure Session ID Generation: Generate random and unpredictable session IDs to prevent session fixation attacks. Session IDs should be unique for each user and should not be guessable or predictable
 - d) Session Encryption: Encrypt session data and the session ID to prevent eavesdropping and session hijacking attacks. Use SSL/TLS to encrypt session data in transit and store session data in an encrypted format in the server
 - e) Cookie Security: Use secure cookies to transmit session data between the client and server. Secure cookies should have the 'secure' flag set to prevent interception by attackers, and the 'httpOnly' flag set to prevent client-side scripting attacks
 - f) Session Revocation: Implement session revocation mechanisms to terminate sessions that are suspected to be compromised or hijacked. This helps prevent further exploitation of the session by attackers
- **Data Protection and Encryption:**
 - a) Sensitive data, such as Personal Identifiable Information (PII) and financial data, must be encrypted both in transit and at rest
 - b) Encryption algorithms and key management practices must adhere to industry standards and best practices
 - c) Use Strong Encryption Algorithms: Use strong and secure encryption algorithms, such as Advanced Encryption Standard (AES) or Twofish, to encrypt sensitive data. Avoid using weak encryption algorithms that can be easily cracked
 - d) Encrypt Data in Transit: Use Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data in transit between the web application and the client browser. This helps protect against eavesdropping and man-in-the-middle attacks
 - e) Encrypt Data at Rest: Store sensitive data in an encrypted format in the database or on disk. This helps protect against data breaches and unauthorised access to the data

- f) Use Key Management Best Practices: Implement key management best practices, such as key rotation, to ensure that encryption keys are kept secure and are not compromised. Avoid hardcoding encryption keys in the application code or configuration files
- **Error Handling and Logging:**
 - a) Proper error handling mechanisms should be implemented to provide minimal error information to users while logging detailed errors for analysis and troubleshooting
 - b) Logging and auditing mechanisms must be in place to capture security-related events and incidents. The application must maintain a complete audit trail of all user activity to enable the identification of unauthorised access or data breaches
 - c) Error messages should not reveal details about the internal state of the application. For example, file system path and stack information should not be exposed to the user through error messages. Implement proper error handling mechanisms to prevent information leakage and avoid exposing sensitive information to attackers. Use custom error messages and avoid displaying detailed error messages to users. Some development frameworks or platforms may generate default error messages. These should be suppressed or replaced with customised error messages as framework generated messages may reveal sensitive information to the user
- **Software Versions and Updates:** At a minimum, the software used in and around the application must be up-to-date, and there must be no known vulnerabilities
- **Data Backup and Recovery:** The application must have a robust backup and recovery system in place to ensure that data can be restored in the event of a system failure or data breach
- **Compliance with Privacy Regulations:** The application development must ensure compliance with all relevant data protection and privacy regulations, including the Nigerian Data Protection Regulation or Act (“NDPR/A”), General Data Protection Regulation (“GDPR”), and any other applicable data protection laws. These regulations set forth specific requirements and guidelines for handling and safeguarding personal data, and it is crucial for the application to adhere to them. This entails implementing appropriate data protection measures, obtaining user consent where necessary, providing data subject rights, and maintaining the security and confidentiality of personal information in accordance with the respective regulations. By complying with these data protection and privacy regulations, the application ensures that user data is handled responsibly and in line with legal requirements
- **Vulnerability Assessment and Penetration Testing:**
 - a) Regular Vulnerability Assessments and Penetration (VAPT) testing should be conducted on applications to identify and address security weaknesses
 - b) Testing should cover both in-house developed applications and third-party applications
 - c) VAPT must be done against the OWASP Top 10 Web Application Vulnerabilities (Version 2021), and all identified vulnerabilities must be remediated
- **Security in Outsourced Development:**

- a) Where software development is wholly or partially outsourced to a third party, due care must be taken to ensure that the policies of FMDQ are still followed where possible. The same level of rigor test must be applied to outsourced software development, as the ones created in-house
 - b) Standard procurement procedures should be used in the selection and engagement of the appropriate outsourced developer. Use of the procedure should ensure the developer can meet the security requirements specified amongst other requirements as stated in the business requirement document. Use of subcontractors by the outsourced developer for any aspect of the development should be understood and an assessment of these sub-contractors is required
- **Audit:** Regular audits should be conducted to ensure adherence to application security requirements and standards
 - **Non-Compliance And Exception:** These standards serve as the foundation and are obligatory, requiring implementation across all applications. However, if there are any exceptional cases where the standards cannot be met, a risk acceptance process must be followed. In such instances, any deviations from the requirements outlined in these standards should be brought to the attention of the cybersecurity group for risk analysis. Subsequently, a risk management process must be implemented

7.5.1 Audit Trail

The system must maintain a complete audit trail of all user activity to enable the identification of unauthorised access or data breaches.

7.5.2 Reliability

The system should be able to function correctly and consistently, without any unexpected failures or errors. Regular system maintenance and testing should be conducted to identify and address any potential issues before Go-Live.

7.5.3 Data Backup and Recoverability

The system must have a robust backup and recovery system in place to ensure that data can be restored in the event of a system failure or data breach

- If the system is unavailable to users (experiencing downtime) because of a system failure, the failure must be detected, and function will be restored within thirty (30) minutes to one (1) hour
- In the event the database is corrupted, the database must be capable of being restored to its condition of no more than one (1) hour before the corruption occurred

7.5.4 System Availability

The system must be always available to users daily, including weekends and public holidays.

7.6 General Performance

Response time for queries and updates: The Server-Side Response Time should be less than 3.5 seconds, 95% of the time. The Client-Side Response Time should be less than 3.0 seconds, 95% of the time. The system shall be able to respond to user queries and updates within the following instances and response times to ensure a seamless user experience

- i) **Web Applications (loading a page):**
 - a) Acceptable: 1-3 seconds

- b) Tolerable: 3-5 seconds
- c) Poor: >5 seconds
- ii) **APIs (processing a request):**
 - a) Acceptable: 1-2 seconds
 - b) Tolerable: 2-5 seconds
 - c) Poor: >5 seconds

The system must meet these performance figures, but of importance is to take note that connectivity and infrastructure will also contribute majorly on the system performance.

Throughput: The system shall exhibit a high throughput capability, allowing for swift data input, updates, and retrieval to meet the demands of a dynamic regulatory landscape

Expected rate of user activity: The system will experience continuous activities every day with an estimate of five hundred (500) users and two hundred (200) concurrent users. Under normal circumstances, the home page must be fully rendered within three (3) seconds, for 90% of users. Under heavy load, the home page must be fully rendered within five (5) seconds. The system must load each page within three (3) seconds

7.6.1 Audit Trail

The system must maintain a complete audit trail of all user activity to enable the identification of unauthorised access or data breaches.

7.6.2 Reliability

The system should be able to function correctly and consistently, without any unexpected failures or errors. Regular system maintenance and testing should be conducted to identify and address any potential issues before Go-Live

- **Availability:** The system should always be operational and available for use. Regular system maintenance and testing shall be conducted to identify and address any potential issues before go-live. The system must maintain a high level of availability, aiming for 24/7 accessibility to accommodate users across different time zones and adhere to the demands of dynamic regulatory environments. Downtime should be minimised through proactive maintenance and robust infrastructure, ensuring that all stakeholders can rely on the system to access real-time data and receive timely notifications without disruptions. Additionally, the system should implement measures for quick recovery in the event of unforeseen incidents, guaranteeing a resilience and consistence to support informed decision-making and regulatory adherence
- **Fault Tolerance:** The system should be able to operate in the presence of hardware or software failures

7.6.3 Data Backup and Recoverability

The system must have a robust backup and recovery system in place to ensure that data can be restored in the event of a system failure or data breach

- If the system is unavailable to users (experiencing downtime) because of a system failure, the failure must be detected, and function will be restored within thirty (30) minutes to one (1) hour
- In the event the database is corrupted, the database must be capable of being restored to its condition of no more than one (1) hour before the corruption occurred

7.6.4 System Availability

The system must be always available to users daily, including weekends and public holidays.

7.6.5 Efficiency

The Page size for the system must be less than 1MB.

7.6.6 Stability

- i) Average memory usage for the second day should be less than 10% higher than the first day
- ii) Average response times for the second day should be less than 10% higher than the first day
- iii) Within a working day, the coefficient of variation for response time should be no more than 15%

7.6.7 Scalability

Average Web Service CPU time should not vary by more than 20%.

Vertical Scalability: System should have the ability to handle increased load by adding more resources (e.g., increasing the capacity of a single server).

Horizontal Scalability: System should have the ability to handle increased load by adding more instances or nodes in a distributed environment.

7.6.8 Usability

User Interface (UI) Design: Look and feel of the system should be user-friendly and meet the needs of the target audience.

7.6.9 Capacity

The system will be utilised by User Institutions within the Equities Market and the FMDQ System Administrators. The system is estimated to have an estimate of over five hundred (500) users. The system should be scalable enough to handle an increasingly large volume of users.

7.6.10 Maintainability

Code Maintainability: The system's code should be understood, modified, and maintained with ease.

Documentation: Well specified documentation should be available for code, databases, and system architecture to aid future development and maintenance

7.6.11 Data Retention

The data retention policy for IAPSS outlines the guidelines for the retention and disposal of data collected, processed, and stored within the system. The system shall retain Personal Identifiable Information ("PII"). Data archive and destruction will be conducted in a secure manner, ensuring permanent deletion or anonymisation. The policy will comply with applicable laws and regulations, provide mechanisms for employee consent and rights, maintain records of retention activities, and undergo periodic review to align with changing requirements and best practices.

7.6.12 Error Handling and Logging

Error messages should not reveal details about the internal state of the system. For example, file system path and stack information should not be exposed to the user through error messages. Implement proper error handling mechanisms to prevent information leakage and avoid exposing sensitive information to attackers. Use custom error messages and avoid displaying detailed error messages to users. Some development frameworks or platform may generate default error messages, and these should be suppressed or replaced with customised error messages as framework generated messages may reveal sensitive information to the user.

7.6.13 Validation Rules

All specified mandatory fields and business rules will be taken into considerations at the implementation phase

7.6.14 Conventions/Standards

- The system should comply with data protection and privacy laws and regulations, such as the Nigerian Data Protection Regulation or Act ("NDPR/A") and the General Data Protection Regulation ("GDPR")
- The system should adhere to industry-standard security protocols and framework

8 NEED FOR DATA PROTECTION IMPACT ASSESSMENT ("DPIA") CHECKLIST

Based on the review of the checklist, there will be no need to conduct DPIA for this project.

S/N	Does the data processing activities involve:	Yes/No
1	Evaluation or scoring of personal data (including profiling and predicting of behaviour)?	No
2	Automated decision-making with legal or significant effects?	No
3	Systematic monitoring?	No
4	Sensitive data (including special categories of personal data)?	No
5	Data processed on a large scale?	No
6	Matching or combining data sets	No
7	Data concerning differently abled people (including children)?	No
8	Innovative use or applying technological or organisational solutions?	Yes
9	Preventing data subjects from exercising their rights?	No