REQUEST FOR PROPOSAL (RFP)

Financial Consumer Protection Compliance Monitoring

with Automated Collection, Processing and Advanced Analytics

Project: Development of a solution for automating monitoring and analyzing consumer complaints ("the Project") for a financial authority (the "Agency").

Description: A solution for the Agency to monitor consumer complaints submitted to supervised entities, correlate this data with complaints escalated to the Agency, provide near-real time statistical analysis from structured and unstructured data sources, and develop AI/ML model for assessing market risk.

Contracting Entity: University of Cambridge, Judge Business School

Countries and Agencies: Undisclosed until after project award

Grant Value: USD TBD

Publication Date: 24 July 2024

Submission of Proposal Deadline: 5 August 2024 23:59 GMT Time (UTC +0)

Project Implementation Dates

- **Phase 1:** September 2024– December 2024
- **Phase 2:** January 2025 – April 2025

Procurement Process Managed by: Cambridge SupTech Lab Launchpad at the Cambridge Centre for Alternative Finance (CCAF), the University of Cambridge Judge Business School

Submission: Submit all documents as detailed in Section III below.

Queries: email suptech-launchpad@jbs.cam.ac.uk with any queries with RFP Complaints in the subject.

Language: All submissions must be written in English. All data products must be processed and presented in English and Arabic.

I. Project Description

This Project requires a solution provider who can communicate and produce data products in Arabic and English, with the capacity, relevant experience, and resources to design, develop, and implement a production-ready IT and/or AI solutions. The objective is to create a comprehensive complaint monitoring and analysis suptech suite for flagging non-compliance and market risks of supervised banks, by automating the collection and analysis process (Use Case A) and augment supervisory insights with additional granular consumer complaints data and advanced technology needed for data-driven regulation (Use Case B).

The proposals including cost and timelines to develop **either Use Case A, or Use Case B, or both** use cases per the requirements listed in "Key Technical Requirements" in **2 phases**:

1) **Phase 1:** A proposal for a production-ready solution citing requirements in Table 1 to deliver a working prototype **by December 2024**.

    - By default, it should be assumed that the entirety of the solution will be developed in the vendor's environment, then transferred to the Agency's on-prem environment for testing and acceptance of the prototype source/object code.
    - The proposals should describe how the technology and source code can be transferred to the financial authority as part of the delivery of the prototype project, per the expressed intention of the Agency to transition to in-house maintenance and development. The solution provider will document all the requirements needed for full implement in a production roadmap developed in this phase.
    - Throughout the course of the project, the Lab will facilitate conversations between the solution provider and Agency (via the regular Project Team meetings) to more granularly assess which components will be transitioned to in-house development and at what point in the product lifecycle this transition is expected to occur. The solution provider will be expected to maintain and share up-to-date documentation with the Agency and the Lab reflecting the results of such conversations throughout the project.

2) **Phase 2:** A proposal to support participation and support to facilitate deployment and transition of the prototype code and related processes to a live production environment, including facilitating complete onboarding plan, training, knowledge transfer, documentation and technical support **by April 1, 2025.** This portion of the proposal will be used to obtain the necessary funding.

1. Basic Requirements

Through this tool, the Agency will be able to:

- Access near real-time granular complaints data from banks' databases.
- Correlate complaints escalated to the Agency's the original banks' complaints
- Include complaints made on paper forms and government portal in the analysis
- Identify strengths and weaknesses in banks' operations.
- Have visibility and notifications of market risk indicators and detect emerging concerns/risks
- Update or enforce policy informed by consumer complaints data
- Generate reports/analytics swiftly, saving time and workforce resources.
- Easily assess supervised entities' compliance with consumer protection and market conduct standards.
- Quickly identify concentrations of complaints.

2. High-level requirements

The main deliverable for this collaboration will be a suptech application with the following core components:

1) Automated data collection:

Facilitate direct access to banks' databases via APIs to extract and analyse data directly, in near real-time, with minimal manual intervention with a supervisory reporting API designed to automate the secure and standardized collection of data from banks' complaints databases.

2) Automated data validation & processing

Integrated validation mechanisms to ensure data accuracy and consistency by automatically checking for errors, inconsistencies, and compliance with predefined rules. This will reduce the need for manual data verification and improve the reliability of the data.

3) Data storage:

A robust database management system to securely store vast amounts of structured and unstructured data. This system will need to support efficient data retrieval and processing, ensuring quick access to relevant information, including assessments and recommendations of capacity needs.

4) Statistical analysis

Effective complaints management is vital for monitoring banks' compliance relating to consumer protection. Automation of statistical reports will provide real-time monitoring to anticipate potential crises. By surfacing early warning signals and actionable insights, the tool will enable the Agency to respond swiftly and effectively to emerging threats, minimizing their impact on the financial system.

5) Advanced-technologies processing and analytics

Artificial intelligence (AI) can assist in analyzing unstructured data by automating the extraction of information from PDFs and performing sophisticated text analysis. This includes tasks such as identifying key phrases, sentiment analysis, and categorizing content, enabling more effective utilization of data for decision-making and insights generation.

Integrated advanced technologies such as Natural Language Processing (NLP) and Large Language Models (LLM) – either Arabic or with accurate translation - Optical Character Recognition (OCR), topic modeling, machine learning and other emerging technologies will facilitate incorporation of unstructured data into the overall analysis and interactive business intelligence dashboards.

6) Interactive business intelligence (BI) dashboard

Business intelligence tools designed to enhance data visualization and reporting including customizable dashboards and automated reporting tools for real-time and periodic analysis to provide the Agency with a clear and comprehensive view of the market conduct landscape, facilitating better oversight and more informed decision-making. Additionally, the real-time reporting capabilities will ensure that the Agency has up-to-date information at all times, improving the efficiency and effectiveness of its supervisory functions. the Agency currently uses Tableau. While the Agency would like to leverage this platform, proposals may offer other options for comparison of impact, value, and time to delivery.

7) Integration into the Agency on-premise environment

The development effort will take place on the vendor environment. Iterative unit testing will be conducted throughout the prototype phase. However full acceptance testing will require integration of the code into the Agency on-premise environment (cloud solutions cannot be supported). This should be planned and scheduled periodically to ensure the prototype is functioning as expected before the end of the project.

8) Production Roadmap

The deployment process includes testing and certifying the software in a pre-production environment (phase 1) before deploying it to production (phase 2). Throughout phase 1, the vendor will capture and document a production roadmap to plan the go-live phase requirements. The vendor will specify all required licenses and provide license scheme for solution modules and user access based on business requirements provided in production roadmap.

9) Key lessons documented and disseminated

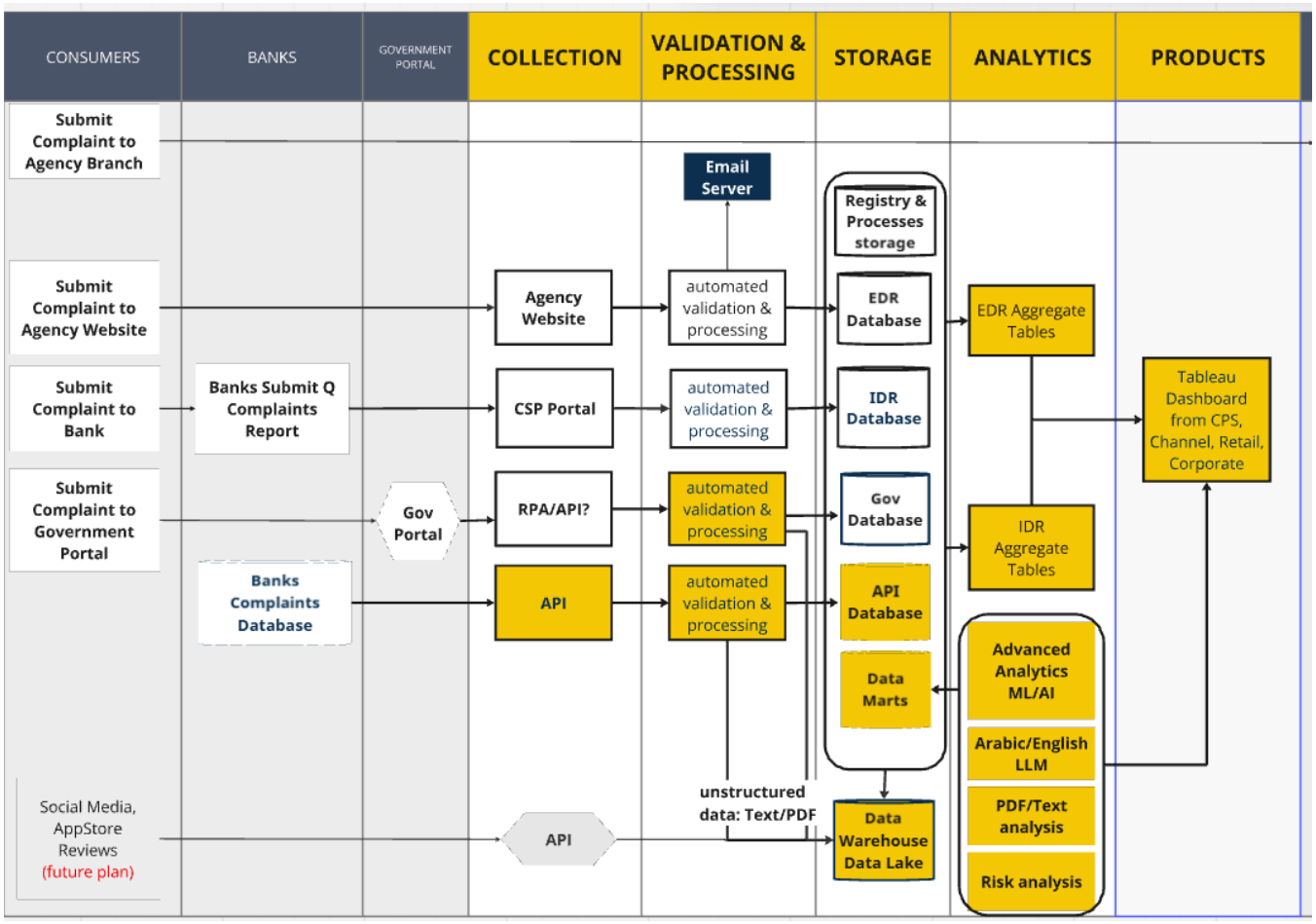
One of the high-level requirements for the project is the systematic documentation and dissemination of key lessons learned throughout the project lifecycle. This process involves capturing insights, challenges, and successes encountered during the development and implementation phases. These documented lessons are crucial for informing and refining future project designs, ensuring continuous improvement and the application of best practices.

A high-level architecture diagram and granular breakdown of the technical requirements follow.

3. Key technical requirements

The proposed solution and all collaterals and products must **support both Arabic and English languages**, and should include the following key elements:

Figure 1. Architecture and data flow diagram (Yellow = Project components)



The suptech blueprint below highlights various suptech opportunities. This project will focus on the components labelled 1-9.

- Navy - regulatory compliance reporting and monitoring (IDR)
- Teal - complaints made to the Agency (EDR inhouse .Net/Oracle solution)
- Yellow - advanced technology integrated within the supervisory process

Core Functions	Platforms				
	Collection	Validation & Processing	Storage	Analysis	Products
Currently without suptech	Manually submitted: Emails, phone, walk-in paper forms file transfer	Manual or no validation rules after receipt of data read, scan, email	Physical media, Excel, laptops, file servers	manual aggregates, Excel macros	Minimal statistical summaries, Ad-hoc, proprietary
REGULATORY COMPLIANCE IDR monitoring Complaints made to banks	Web portal FSP Push API FSP Pull API	Format validations Content validations OLAP/OLTP, RPA	Relational databases Other processes Db Agency registries Db API hooks Data warehouse	Descriptive analysis (historical, aggregates)	Case Management System (CMS) User Interface (UI) Canned/ad-hoc reports Statistical dashboards
	Web-scrapers API	AI - incoming tagging and classification	Data Lake	Predictive & Prescriptive analysis (AI/ML)	Interactive AI-BI Dashboards
COMPLAINTS EDR process Complaints made to Agency	Web portal	Format validations Content validations OLAP/OLTP, RPA	Relational databases Other processes DB Agency registries API hooks Data warehouse	Descriptive analysis (historical, aggregates)	Case Management System (CMS) Canned/ad-hoc reports Statistical dashboards
	AI-Chatbot Web-scrapers API	Tagging and classification	Data Lake	Predictive & Prescriptive analysis (AI/ML)	Interactive AI-BI Dashboards

In scope:

Use Case A: Compliance monitoring platform (API & .Net)

1. Data collection channels used to monitor bank compliance to regulations (Portal, push API and/or pull API)
2. Automated validation and Processing rules
3. Relational databases to store the data collected by the API, and data warehouse to collect additional data from other sources or processes to be included in analytics
4. Statistical analysis – software development to design and develop aggregate tables per the Agency requirements.
5. Case Management System (CMS) role-based user interface to manage workflow and statistical analysis
6. Integration of EDR data to correlated escalated complaints to original complaints

Use Case B: Advanced analytics (AI)

7. Data Lake storage for unstructured data
8. AI/ML –AI-PDF Extraction, AI-Text analysis, and other AI techniques and methodologies to advance supervisory insights such as risk assessment.
9. BI Dashboard, user interface and visualization

Out of scope:

- The EDR database and workflow management has been developed by the Agency IT. A chatbot project may be explored in the future.
- Social media scraping, web scraping and sentiment analysis were noted as a future enhancement consideration and are out of scope of this project.
- Subsequent phases of this project should explore additional AI capabilities to augment supervisory oversight with advanced analytics tools and techniques.

Table 1. General Requirements

COMPONENT	ID	FEATURE	DESCRIPTION	PRIORITY
Use Case A Data Collection	1.1	API Server & Clients	Develop server and client-side API using open standards to maximize interoperability such as Restful, SOAP integrated with a .Net/Oracle backend. The vendor will work with the project team to assess appropriate solution Push/Pull and near-real time vs periodic data needs, automated validation, processing (See **Proposed Data Points in Appendix 1**)	HIGH
	1.2	Alternate channel	Develop an alternate method of compliance reporting must be in place for banks that require more time for onboarding to the API	HIGH
	1.4	Validation & Processing	Validate file metadata and content to ensure they meet expected criteria. Develop algorithms for automated validation and processing	
	1.3	Security	The proposal should address the **Information Security team requirements in Appendix 2** and **Cybersecurity requirements in Appendix 3**	HIGH
Use Case A Centralized Storage	2.1	Design	Create a data dictionary and design database schemas for optimum security and efficiency for storage, processing and analysis	HIGH
	2.2	Access Controls	The storage mechanism must provide for varying levels of access controls with default access expiration dates. The solution needs to support user access rights to configure users, their position/organization and roles/responsibilities that define allowed access and access type to functions and reports where each group of reports can be viewed by specific group of users.	
	2.3	Scalability	The proposed solution should be expandable to support increase number of users using the system and will be sustainable with the increased amount of data over the years	
	2.4		Solution needs to support archiving capability for historical data and files per entity/function based on	

		Archive/Retention	configurable defined criteria and archived data need to be accessible by specific users based on granted access. Data retention policies and mechanism in place to comply with data retention policies	
	2.5	Capacity	Provide complete infrastructure requirements and sizing including H/W, computing power, storage, network and connectivity for solution environments (Production, Testing, development, training and DR) Details shall include all required hardware component types, computing power, storage capacity and infrastructure prerequisites covering three years of operations considering solution performance and capacity. It shall also include network components requirements, connectivity matrix, topology, network prerequisites and any relevant considerations and rules. All hardware components must be compatible with the Agency environment and must be accepted from the Agency IT teams	
Use Case A Transactional Analytics	3.1	Aggregate Reports	Up to 10 aggregate tables of complaints data, metadata, and market risks developed in .Net	MED
Use Case B Advanced Analytics	4.1	AI-Text Analysis	Analysis of unstructured data within complaints such as the complaint details (text or PDF) and the bank resolution notes to categorize, summarize, correlate and validate narrative compared to metadata compliance metrics, and resolution compared to text narrative using Natural Language Processing and other AI technologies. (**See sample text in Appendix 4**)	HIGH
	4.2	AI-PDF Extraction	A tool that extracts relevant data from PDF documents and transposes it into structured data to be included in overall statistical analysis including handwritten Arabic and English documents. Solution provided to demonstrate capabilities of accurate Arabic PDF extraction during proposal evaluation phase (sample PDFs will be provided)	MED

	4.3	AI/ML Risk modelling and analysis	Leverage AI/ML to streamline thematic reviews and periodic reports to include predictive analysis using complaint reports, products and services reviews, financial literacy/themed reviews, payments and supervision sectors, and other relevant sources identified in the design stage.	MED
Use Case A & B 5. Data Products	5.1	Dashboard	Interactive BI dashboard in Tableau or vendor proposed BI dashboard solution with recommendations detailing benefits, impact, time to market of new dashboard vs Tableau.	
	5.2	User Experience/User Interface	The solution should provide best user interface and user experience matching the latest versions of the famous browsers (Chrome / Edge / Safari)	
	5.3	Integration	Ability to integrate with the Agency needed systems through APIs, Database adaptors, XML & CSV files	
Use Case A & B 6. Integration	6.1	Strategy & Planning	Provide infrastructure and network requirements for test, production and DR protocols along with connectivity requirements.	
	6.2	Code Delivery	Source code shall be delivered to the Agency technical teams through handover detailed sessions with full handover of the system including all configurations, customizations and operational activities. Provide source Code documentation: This document will include the source code explanation and libraries configuration.	
Use Case A & B 7. Testing	7.1	Strategy & planning	provide testing strategy and criteria and to lead end-to-end UAT of the solution and manage UAT issue list resolution. Provide production launch prerequisites, activity plan and deployment runbook along with optional proposal for production launch phase to be conducted by solution provider	
	7.2	Testing	Develop test plans including test scenarios based on solution details to be used as reference for all phases of testing and UAT. Perform/responsible for all solution unit testing, security testing, integration testing, performance testing and end to end UAT	
	7.3	Test Environment	All solution components of testing and production environment shall be hosted inside on the Agencys' premise. In addition to not transfer any data to cloud sites.	
Use Case A & B		Data Dictionary	Data Dictionary for all critical data stores across the whole solution that would enable InfoSec team put	

8. Documentation			proper security controls for such data's confidentiality & Integrity	
	8.1	Deployment guide	Deployment Guide: This document will include the solution deployment manual for administrators for basic solution initial setup and configuration. Provide full rollout roadmap plan and runbook along with optional proposal for full rollout with all banks	
	8.2	Admin Manual	Availability of Administration Manual ongoing configuration, maintenance and ops support	
	8.3	User's Manual	User Guides for end users and business administrators, business documentation and related training documents in both English and Arabic languages including process for maintaining/ updating /versioning documentation, update notifications and process for accessing any supplied online documentation.	
	8.4	Architecture documentation	Provide architecture design and operational technical documentation and troubleshooting guide for all system components, including full descriptive details of all components, customizations and configurations applied detailed architecture documentation, data flow and databases and Entity relationship diagrams (ERDs). High level and low-level architecture documents for both Solution and infrastructure in addition to detailed design for customizations if any including Network Diagram shall be documented with all protocols and integrations	
	8.5	Design Specification	Design Specifications will explain solution components and its specifications against its functionality technology stack, technology concepts used, location of implementation	

Applicable Laws & Regulations

The engagement may require the Agency to share certain data with the Lab and one or more vendors or innovators working as part of the Lab team. While the solution primarily requires publicly available data, any non-public data can be shared conditionally on the same confirming with the provisions of extant I laws and regulations. Following, non-exhaustive, laws and regulations may apply in the collection, processing, and sharing of financial and personal information. A confidentiality agreement will be circulated and executed along with a project agreement defining all legal terms and conditions.

II. Project Structure

Phase 1

This phase has three stages, where stage 2 is the parallel development of IT and AI functionality, elaborated below:

1. Kickoff and interface design, including technical integration specifications

2a. Development of the API/.Net working prototype (Use Case A)

2b. Development of the AI working prototype (Use Case B)

3. Integration, testing and signoff of the working prototypes

Throughout all project stages, vendors are expected to meet weekly with key stakeholders of the Agency as well as the Lab's Launchpad team, to ensure close coordination and agility.

1. Kickoff and interface design, including technical integration specifications

During the first phase, the selected vendor, in coordination with the Lab's Launchpad team will gather requirements from the Agency and produce an initial Design Document that includes integration and user interface specifications. This document will explain the scope that will be implemented in the solution. This is the main reference document that will be used to develop, test, and deliver the solution for acceptance. It is a must that it has accurate and correct information about the business needed requirements.

This living document should include specifications for the client-facing portion of the prototype, communicated in a manner such that clients of the prototype can understand how to integrate with systems and processes, submit data, and use the system without necessarily understanding the entire architecture behind the software. It should include a traceability matrix listing all solution modules / functions / features, this matrix is the source of requirements and establishes criteria for user acceptance testing for use during the testing phase.

This Document is to be shared as needed with any other key stakeholders (e.g., vendors of relevant software used by the Agency, any financial institutions needing to integrate) to allow them to develop integrations and/or adapt existing software during the development phase. The vendor will also provide project plan/schedule detailing high level project schedule listing

start and end dates of main phases, milestones, and activities. The schedule will be following the chosen project lifecycle chosen for the project.

2a) Development of Use Case A (API/.Net)

The vendor will swiftly move from design/documentation to mockups and/or begin coding the solution with iterative review/feedback work sessions with the project team. Selected supervised entities will be available to participate in the prototype development and pilot as needed and advised by the vendor.

The project team including IT, the Lab and vendor will meet weekly to co-create the solution. discuss design and requirements, documenting user stories and key performance indicators, reviewing and iterating on mockup, then testing and iterating the features and functionality with hands-on live test application.

The project team and vendor will work asynchronously between meetings to make progress on development, testing and documentation iteratively building on each week's progress.
The vendor will track progress, timelines, next steps, meeting minutes, decisions/agreements, and other project management responsibilities.

2b) Development of Use Case B (AI)

The AI components will be developed in parallel through interactive sessions with the project team. The selected vendor should (i) assess the needs of the Agency to understand which dashboards, reports, and statistics are most useful and/or difficult to produce under the current web-based market monitoring system; and then (ii) propose and develop a prototype mechanism for extracting and visualizing this information from data consumed, processed, and produced by the working prototype. This could involve creating custom queries, scheduling the generation of reports, and outputting them in various formats. The final UI of the prototype must be done before the final tests .

3) Integration, testing and signoff of the working prototype

The development effort will take place on the vendor environment. Iterative unit testing will be conducted throughout the prototype phase. However full acceptance testing will require integration of the code into the Agency on-premise environment (cloud solutions cannot be supported). This should be planned and scheduled periodically to ensure the prototype is functioning as expected before the end of the project.

The working prototype will be tested with the Agency and pilot banks, based on user acceptance criteria defined during the design stage, to allow the vendor to ensure that the prototype is functional with real data before it is scaled into full production. This approach also minimizes the risk of interruption due to unforeseen technology failure and serves to inform estimates of the cost to scale the prototype to a production-grade service.

A cyclical final test of the prototype and improvements by the developers must be done until the product is adherent to the functional specification document as reflected through the completion of the user acceptance testing criteria.

As the working prototype is being developed and tested, the vendor will document all components and requirements necessary for deploying the solution to a live environment in a production roadmap. Once UAT is complete, the project package will be expected to be delivered, including training materials, project documentation including BRD, technical detailed design, operational workbook, maintenance workbook and user guide, and other items to be specified in the Project Agreement with the selected vendor.

Phase 2

Following successful delivery of the prototype, the Agency may opt to engage with the vendor for assistance in deploying the solution to a production environment. The production roadmap will inform Phase 2 with the necessary requirements to transition the working prototype to a live solution. In this phase, the vendor will support the Agency's IT team with a deployment plan that includes all necessary support and documentation and resources needed for a full implementation. The solution provider will be expected to conduct business user training and technical training along with handover and documentation of the solution. Should the Agency opt to engage the vendor for this effort, it will be funded through a separate Project Agreement.

Timeline

Work commences upon vendor selection and execution of the project agreement targeted to be completed in August, with a targeted **project kickoff September 2024.** This Project will ultimately deliver a **production-ready prototype by December 2024 (phase 1)**, that will be deployed, tested and accepted by the Agency. Upon completion of the prototype, the Agency may opt to own operations maintenance thereafter and not pursue further engagements. Or they may opt to continue working with the vendor full implementation roll out, knowledge transfer and support of the prototype to a **live solution by April 2025 (phase 2).**

III. Vendor Selection

1. Project Award

The successful applicant will:

- Be awarded a grant from the Bill & Melinda Gates Foundation to develop and test the required solution. This is a fixed-sum contract to cover all the applicant's expenses related to the development and testing work, including staff time, hardware, software, travel, and all other project-related expenses.
- Be listed in the Lab's online Vendor Database, a dynamic, web-based platform to explore and connect with solution providers who have been active in the global suptech market.
- Be invited to the Lab's SupTech Week - the largest gathering of the suptech community globally, where you will have the opportunity to demo the prototype to potential clients and connect with funders.
- Be recognised in a case study the Lab will write following the successful completion of this project, distributed through the Lab's direct newsletter to a list of over 20,000 global contacts in the suptech space, and on LinkedIn.
- Engage with the suptech community through the Lab's hackathons and tech sprints and receive tailored coaching from the Lab on coordinating suptech projects with Financial Authorities.
- Enhance your platform with new tools developed through this engagement.

2. RFP review and selection process

- Blind review process: A panel of expert reviewers will score anonymised proposals without knowing the name of the vendor submitting them
- Competitor scorecard: Applications will be assessed by the panel using a set of scoring metrics and weighing the relative importance of each attribute
- Rapid turnaround time: We will select the winning vendor and award 50% of the grant within 48 days from submission of the final proposal. The last 50% of the award will be granted in one installment upon completion of the deliverables according to projected timelines.

3. Rules and guidelines

a. Submission Requirements

Selected vendors must demonstrate that their proposed solution meets the needs of the Project, both in terms of technical topic responsiveness, execution, and innovative approach.

Please submit your RFP via the **RFP Submission Form.** In the 'Proposal' section, please upload your proposal following the prescribed structure below:

Part 1 - Brief company background:

- Technical and Arabic language expertise to effectively implement the project
- List of representative projects portfolio of relevant experience in similar implementations.
- Managerial capabilities and relevant experience to effectively implement the project
- Adequate resources to devote to the successful implementation
- Identify if the vendor has any partners local to the Middle East/N.Africa (MENA) region

This section should be no longer than 4 pages (font Century Gothic, size 11, line spacing 1.15)

Part 2 – Technical proposal:

1. **Detailed technical specification and architecture** that address components of the key technical requirements in Section I, including high-level overview of integration & interface requirements and capabilities with other systems. This section should be no longer than 8 pages and should reference the ID# of the corresponding requirement(s) as applicable. A technical architecture diagram, licenses, infrastructure, network, connectivity for all technical aspects and layers should be included in the production roadmap. This section should be no longer than 8 pages (font Century Gothic, size 11, line spacing 1.15)

2. **Execution plan and resourcing. Indicative development / implementation schedule** based on the timeline parameters set out above and the project structure set out in Section II along with resourcing plan for key contributors to the project. A Gantt chart or other diagram to visualize the implementation timeline should be included. This section should be no longer than 4 pages (font Century Gothic, size 11, line spacing 1.15)

3. **Additional element for consideration.** A free-form response to elaborate on the innovative aspects of the solution you propose and why your agency should be awarded this competition. This should be no longer than 1,500 characters.

4. **Information needed for due diligence.** . The Agency may be interested in continuing a long-term engagement with the vendor beyond the prototyping scope and will consider estimated cost of annual support of implemented solution after going live for 3 years, daily rate for software development enhancements, warranty periods, maintenance contracts. Solutions that involve platforms or licensed products must be supported for at least 5 years with no End of Life (EOL) or End of Support (EOS) announcements. The proposal should include descriptions of

license model or details of all required licenses of the solution environments of all solution layers, project bill of material and Support Level Agreement.

Any questions and requests for clarification should be sent via email to Cambridge SupTech Lab Launchpad at suptech-launchpad@jbs.cam.ac.uk with subject line "RFP: Complaints Monitoring Launchpad".

b. Tips for applicants

- Your proposal must demonstrate an innovative approach that meets all stated goals and complies with all restrictions and guidelines.
- Personal and organizational information should be provided separately from the proposal. Proposals will be sent to reviewers without personal or organizational information. Do not include any identifying information directly in your proposal.
- In addition to subject matter experts, your proposal will be reviewed by a panel with broad expertise and a track record in identifying innovations – these reviewers may not be deep domain experts in your field. You must describe your ideas in unambiguous language without the use of jargon unique to your field.
- The work proposed in your application must include a clear set of key activities required to develop and test the prototype solution. Proposals with vague descriptions or vague methodologies will not be funded.

Criteria to Be Considered for Vendor Choice:

- Ease of use for non-technical users.
- Ensuring feasibility of integration with the Suptech system.
- Ensuring on-prem implementation and not cloud-based.
- Scalability of usage considering 3 Vs (volume, variety, velocity).
- Security, Flexibility of updates of tool and add-ons over time.

c. Disclaimer

The Lab reserves the right to edit, invalidate, terminate, and/or reissue this RFP at any time and for any reason. The Lab also reserves the right to select a vendor through an alternate method and/or adopt an alternate timeline for vendor selection that differs from the method and/or timeline described in this document, the websites of the Lab and Launchpad, and any other communications related with the process. Furthermore, the Lab expressly disclaims responsibility for any costs incurred by any vendor in responding to this RFP, regardless of whether the RFP is edited, invalidated, terminated, and/or reissued at any time and for any reason.

Appendix 1: Proposed Data Points

1	Bank Complaint's Reference
2	Client/Non-Client
3	Client Type
4	Client Gender
5	Date of Birth
6	SMEs Type
7	ID TYPE
8	Customer National ID/Passport Number
9	Commercial Register Number
10	Company Sector
11	If other, describe
12	ISIC company code (activity)
13	If other, describe
14	Customer Branch
15	Governorate
16	Receiving Channel
17	If other, describe
18	Complaint Type
19	Complaint Reference #
20	If reopened, re-opened date
21	Complaint Details
22	Main Product/Service

23	If other, describe
24	Sub Product/Service
25	If other, describe
26	Nature of Complaint
27	If other, describe
28	Complaint Resolution
29	Complaint Root Cause
30	If other, describe
31	Source of Root Cause /Concerned Party
32	If other, describe
33	Complaint Submission Date
34	Due date extension…
35	Date of Resolving the complaint
36	SLA
37	SLA Breaching Reasons
38	If other, describe
39	SLA Breaching Reasons description
40	Compliant Internal Escalation
41	Closing Complaint Details (after resolution)
42	Redress/ Exemption Yes/No
43	Redress Amount
44	Corrective Action Taken

Appendix 2. Information Security Requirements

	Requirements
IS 1.0	**Authentication and Authorization**
	APIs should prevent leaking and not expose any sensitive information, such as the API key, session tokens, credentials. Passwords, security tokens, and API keys should not appear in the URL.
IS 1.1	Support using external authentication servers (e.g. standalone ldap, AD...)
IS 1.2	System using a proper authentication mechanism Describe the applied authentication mechanism
IS 1.3	All solution portals must be authenticated, and multi-factor authentication (MFA) must be enforced if it will be published over internet, with MFA enabled for Administrators and privileged accounts.
IS 1.4	Configurable password policy that allow: - Complexity. - Lockout threshold. - Password age/history. the applied password policy shall be mentioned in details
IS 1.5	All users / Admins must be created on the basis of "Need to Know" and "Least Privilege". Segregation of duties Principle must be applied
IS 1.6	Segregation of duties for in scope system should be implemented and verified regarding but not limited to access matrix, escalation matrix and cycle of approvals.
IS 1.7	Privileged access of the application to the database such as (drop and delete permission) must be with strong, defined, documented and approved business justification
IS 1.8	User Management Role should be separated from any other administrative role
IS 1.9	Role-based access control (RBAC) must be enforced to limit user privileges based on their job responsibilities, and all user accounts must be configured with the least privileges necessary and audited regularly to detect unauthorized activity. Implement access controls to restrict who can upload files and who can access uploaded files, based on roles and permissions.
IS 1.10	Ability to create custom roles/group of permissions with the following characteristics: - Separate page for permission/role/group assigning. - By default new users shall not have any permission till admins assign permissions. - Solution shall have following levels of permissions to assign: - System Functionality. - Screen Access. - Sub-Screen level Access. - Workflow. - Reports.
IS 1.11	Critical functions of the application must be based on the Maker & Checker principle for execution
IS 1.12	All solution portals must be authenticated and multi-factor authentication must be enforced if it will be published over internet
IS 2.0	**Security validation**

IS 2.1	"Positive" validation approach must be used for all parameters using strict format (white list)
IS 2.2	Application must be configured to validate user input at client & server side (Server side is a must)
IS 2.3	Uploaded Files must be scanned by sandbox for security vulnerabilities before usage
IS 2.4	Data output must be validated to ensure the processing of stored information is correct and appropriate
IS 2.5	Use data integrity controls at the application level to ensure that data being input, viewed, or manipulated undergoes a validation and integrity check
IS 2.6	Validation checks must be incorporated into applications to detect any corruption
IS 2.7	the integrated
IS 3.0	**Data Confidentiality, Integrity & Encryption**
IS 3.1	When transmitting sensitive information, at any tier of the application or network architecture, encryption-in-transit should be used. DB security such as Encryption, DAM shall be considered.
IS 3.2	All Sensitive Data should be encrypted or hashed at rest (Database, Files…etc.)
IS 3.3	Encryption key management and Key recycle policies should be defined i.e., Key generation, distribution, deletion, and expiration.
IS 3.4	Encryption Keys should be Secured.
IS 3.5	Form fields for sensitive data must be masked while typing
IS 3.6	Configure the database to only allow encrypted connections. All backup data must be encrypted at rest using secure encryption algorithms. All data used and stored in the solution's database must be encrypted at rest and in transit.
IS 3.7	Do not disclose sensitive information in error responses, including system details, session identifiers or account information. Describe encryption methodology including key management cypher Solution shouldn't store any sensitive information in logs without proper encryption, including unnecessary system details, session identifiers or passwords
IS 3.8	Encrypt files during transmission and storage to protect them from unauthorized access
API 22	All encryption algorithms/ciphers/key length shall be configurable.
API 23	All intercommunication between applications and API should be secured (Dual Certificates, authentication, network level)
API 24	Support Communications' Encryption
API 25	Use data integrity controls for sensitive data transmission.
IS 4.0	**Session Management**
IS 4.1	Cookies must not store any confidential information
IS 4.2	Session cookies must have a reasonable expiration time
IS 4.3	Secure session management techniques must be implemented to prevent session hijacking: i. The solution must generate session tokens by secure random functions and must be of sufficient length. ii. The solution must limit the session number per user to only one session unless the application requires multiple simultaneous sessions for a single user. iii. The solution must require the user to re-enter the password or re-activate the terminal if the session has been idle for more than 15 minutes. iv. The solution must have a reasonable expiration time for session cookie. Non-expiring session cookies should be avoided.

	v. The solution must destroy the session and corresponding data on the server when the user logs out of the application. vi. The solution must not store any confidential information or PII in cookies.
IS 4.4	Require user to re-enter the password or re-activate the terminal if the session has been idle for more than 15 minutes
IS 4.5	The solution must provide ability to log all session requests and responses incoming or outgoing including service number and IDs
IS 5.0	**Technical Security Controls**
IS 5.1	System shall be published through WAF integrated with sandbox for files submission with a suitable period be allocated for the learning mode to ensure all actions will be considered
IS 5.2	Compatibility with inspections devices(FW,Ips,NextGen FW,DLP,FIM…etc.) without restrictions to intercept and inspect all incoming traffic
IS 5.3	Application should be securely developed according to and comply with the latest OWASP's top 10 API Security verification standard. **a Penetration Test will be performed to confirm that
IS 5.4	all intercommunication between applications and api should be secured (Dual Certificates, authentication, network level)
IS 5.5	system shall be deployed on hardened environment (OS, Database, Web Servers…etc.)compliance report shall be conducted against CIS standard
IS 5.6	shall have specific software development lifecycle standards that accounts for such the following security, planning, testing, acceptance, and deployment
IS 5.7	all unused dependencies, unnecessary features, components, files shall be removed
IS 5.8	No Vulnerable and Outdated Components shall be used and the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies shall be mentioned and approved. Solution provider is responsible for resolving all issues resulting from vulnerability scanning and penetration testing and communicating to the Agency in case any vulnerabilities raised by either other customers or vendors' security self-assessments
IS 5.9	Application shall have ongoing plan for monitoring, triaging, and applying updates or configuration changes for the lifetime of the application or portfolio.
IS 5.10	in case system have db links, the Database link security controls shall be implemented and the vendor should recommend/document security controls (administrative and technical) that will be needed for Suptech solution
IS 5.11	Application development should follow Secure Coding Guidelines, incorporating industry leading practices for secure development and
API14	API should have no Excessive Data Exposure through ensuring the responses from the API contain only legitimate data by determining the consumer of data and ensuring they are allowed to access such data
API15	Implementing a rate Limiting on the API as below: • Execution timeouts • Number of requests per client/resource • Number of records per page to return in a single request response
API16	Define an appropriate request size limit and reject requests exceeding the limit.
API17	Respond with generic error messages - avoid revealing details of the failure unnecessarily.
IS 6.0	**Audit Trail**
IS 6.1	Application should be supported with configurable audit trail and interface to trace all user actions and updates to be viewable and searchable through the application based on user access. Audit logs and alert logs shall have at least 6 months retention period.

IS 6.2	SIEM friendly logs, the vendor shall provide compatible logs mechanism with the SIEM
IS 6.3	Security logs must have the following parameters and include traceable error logging capability with configurable log level and logs archiving (allow multi-level system logging to be managed by solution technical administrator): -Users Actions. -All Administrators actions , including changes to the security configuration settings - Successful/Unsuccessful login attempts -Audit log access or modification attempts -Audit Log Stop/Start -API and 3rd parties interconnection -Privilege change activity -Privileged User IDs activity -Applications shutdowns, reboots/restarts, errors
IS 6.4	Event logs recording user activities, exceptions, faults, authentication and authorization failures, including APIs, and information security events shall be produced, kept, and regularly reviewed. The following event attributes associated with each event shall be logged: - Type of action performed; - Unique user identifier such as user ID; - Source IP address of the user's computer; - Date and time of action including login and logout details; - Details of the action performed; - Success or failure indication; - Identity or name of affected data, system component, or resource.
IS 6.5	Application Audit logs / Sensitive Data /Configuration Data location should be defined to apply proper protection. Monitors and alarms over its own components and operational flows to proactively detect any failure and accordingly automatically send the alarm to concerned teams through email and SMS
IS 6.6	Application doesn't store any sensitive information in logs, including unnecessary system details, session identifiers or passwords
IS 6.7	Enabling/Disabling of Audit logs must be appropriately restricted
IS 7.0	**System Database**
IS 7.1	System's Database shall be herded against CIS standards
IS 7.2	Remove any default accounts and databases
IS 7.3	Only allow the database's system account to connect from system application server
IS 7.4	Configure the database to only allow encrypted connections
IS 7.5	Install a trusted digital certificate on the server
IS 7.6	Ensure that the backups are protected with appropriate permissions, and ideally encrypted
IS 8.0	**Performance**
IS 8.1	implement health check and cleanup scripts for operational maintenance
IS 8.2	All solution components should be designed for performance optimization
IS 9.0	**Backups and Disaster Recovery (DR)**
IS 9.1	Production roadmap to support disaster recovery environment that is fully synched with production and ability for seamless failover and DR that meet the security controls
IS 9.2	The storage system should automatically allow for cold storage backups as part of disaster recovery

IS 9.3	A backup solution and process shall be in place and the restore procedure shall be tested at least once a year.
IS 9.4	Backup storage should be physically and logically isolated from the primary production environment, and resistant to ransomware.
IS 9.5	All backup data must be encrypted at rest using secure encryption algorithms.
IS 10.0	**General**
IS 10.1	The below controls shall be considered for the file uploading - File Type Verification: Ensure that only allowed file types are accepted for upload - File Size Limitations: Implement restrictions on the size of uploaded files to prevent denial of service attacks and server resource exhaustion - Antivirus Scanning: Integrate antivirus scanning and sandbox tools to detect and block files containing malware or viruses during the upload process - Content Disposition: Set appropriate content disposition headers - Secure Storage: Store uploaded files in a secure location with proper access controls - Logging and Monitoring: Log file upload activities and monitor for suspicious behavior or anomalies
IS 10.2	Vendor shall be committed according to agreed SLA to solve the raised issues from the penetration testing and source code review.
IS 10.3	System shall be deployed on hardened environment (OS, Database, Web Servers…etc.), implement relative CIS standards.
IS 10.4	The proposed network diagram shall be shared to review by Infosec team.
IS 10.5	Architecture and infrastructure assessments will be conducted before launching.
IS 11.0	**Authorization and Access Management**
IS 11.1	API endpoint that receives an ID of an object, and performs any type of action on the object, should implement object level authorization checks. The checks should validate that the logged-in user does have access to perform the requested action on the requested object.
IS 11.1	Implement a proper authorization mechanism that enforces segregation of duties.
IS 11.3	Use an authorization mechanism to check if the logged-in user has access to perform the requested action on the record.
IS 11.4	Use random and unpredictable values records' IDs.
IS 11.5	Validating responses from the API assuring only authorized data is transmitted by determining the consumer of data and assuring they are allowed to access such data, API should not rely on the web app/desktop app solely to perform such checks and must be implemented on the API level.
IS 11.6	Regular user should not access administrative endpoints
IS 11.7	A user should not perform sensitive actions (e.g., creation, modification, or deletion) that they should not do by simply changing the HTTP method (e.g., from GET to DELETE)
IS 11.8	No user account shall gain control to other users' accounts in the system, read their personal data, and perform sensitive actions on their behalf.
Input sanitization (Code Injection Security Controls)	
IS 12.1	Client-supplied data should be validated & filtered by the API by applying whitelisting for legitimate characters only.

IS 12.2	Client-supplied data should not be directly used or concatenated to SQL/NoSQL/LDAP queries, OS commands
IS 12.3	When parsing the incoming XML messages ensure that the API is not vulnerable to XXE and similar attacks.
Is 12.4	Data output must be validated to ensure proper processing of stored information and not processing malicious content
IS 12.5	Validate input length, range, format and type.

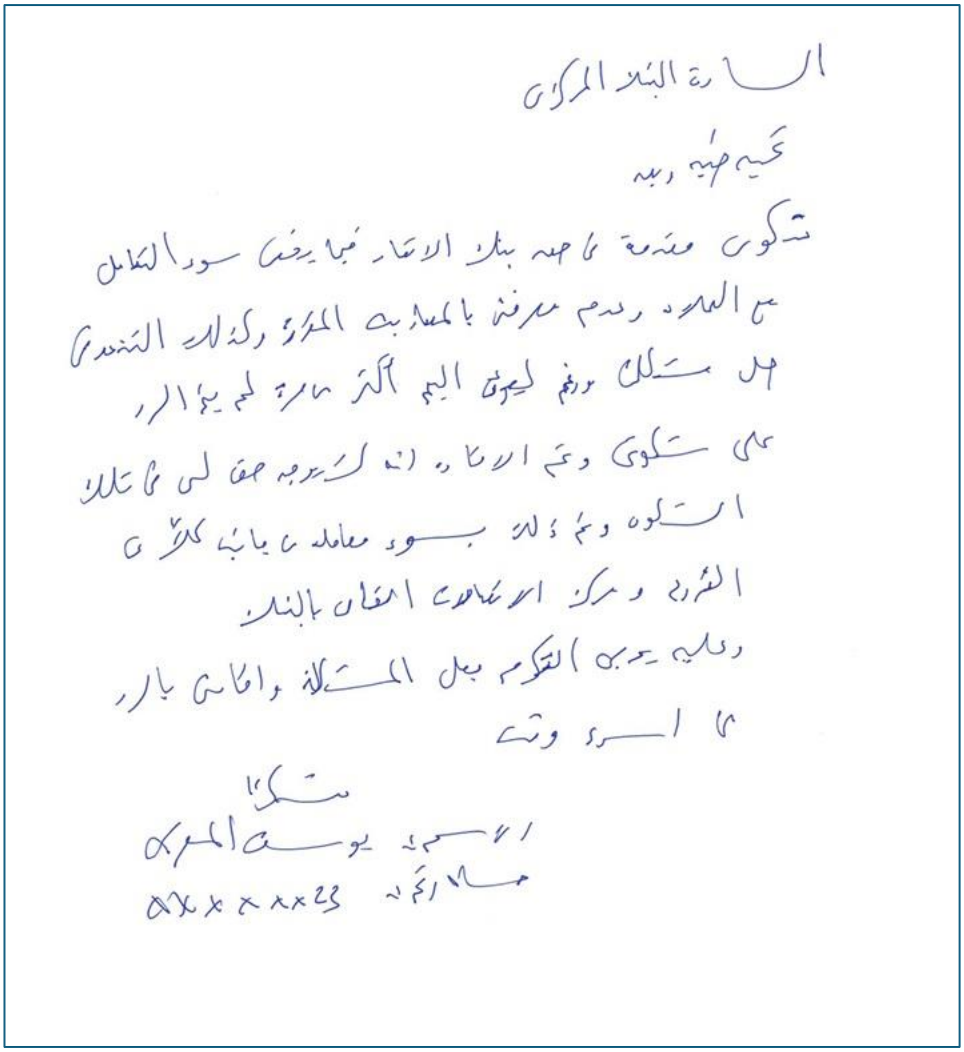
Appendix 3. Cybersecurity API Requirements

CS1	All messages and payloads between banks and the agency must be signed and encrypted on the network level and on APIs and message signature shall be verified.
CS2	The default permission for all users for all resources must be configured to deny access.
CS3	All used signed APIs must be validated before execution on solution backend.
CS4	Message headers and payload must be verified to be trustworthy and not modified in transit by requiring strong encryption for transport (TLS only) and per-message digital signatures.
CS5	All used APIs must be authenticated as per most common standards such as but not limited to OAuth and JWT.
CS7	All input data should be strictly defined such as schemas, types, string patterns - and should be enforced at runtime.
CS8	All used APIs (from testing to production) must be documented including who can access each item and what data it contains, and which API functions access them or are hosted by them, and all integrations with API.
CS9	Only secure protocols such as HTTPS or SSL/TLS must be used for authentication, and any web portals must run explicitly under HTTPS and enforce certificate pinning. Use secure communication protocols such as HTTPS and SSL/TLS to encrypt traffic between the workstations and other components such as servers or databases
CS10	The solution must be implemented on-premises and no cloud implementation or integration shall occur starting from the UAT phase.
CS11	It's not allowed for any kind of integration between banks and vendor side.
CS12	Solutions back-ends must be deployed behind appropriate security devices such as firewalls and WAFs. Any Firewall and WAF must be configured in blocking mode in production.
CS13	Servers shall be hardened according to international standards such as CIS or similar.
CS14	An anti-virus and anti-malware program endpoint protection platform (EPP) should be used on all servers, devices, and operating systems and should be able to deal with malicious software without intervention.
CS15	A detailed Network flow diagram including all network and security components (e.g. FWs, WAFs, IPSs, Load Balancer, authentication servers, etc..) shall be provided.
CS16	All Cryptographic keys for the solution infrastructure must be generated and saved on HSMs or similar tamper proof devices.
CS17	The solution must list all communications between the proposed solution and other systems.
CS18	The solution must support network segmentation and access control lists.

CS19	The solution must allow changes to the configurations with privileged access only, and apply the segregation of duties matrix (maker and checker).
CS20	In case of, any uploaded documents must be checked first by Sandbox before uploading.
CS21	▪ Apply the following restriction from the backend for file uploading: i- Allow only the whitelisted file extension extensions like (TXT, jpg or pdf) ii- Prohibited any executable or blacklisted extensions like and not limited to (exe,dll,hta,…..) iii- Make sure the filename doesn't contain any substrings that may be interpreted as a directory or a traversal sequence (../) iv- Do not upload files to the server's permanent filesystem until they have been fully validated v- Set a maximum name length and maximum file size
CS22	In case the solution is deployed in a containerized environment, the following requirements must be followed: i. Solution provider shall mitigate all risks and implement all countermeasures listed in the NIST SP 800-190 Application container security guide. ii. Solution provider shall perform a gap assessment between the security measures implemented and the security measures required to protect against MITER AT&CK Matrix for Containers, in addition to documenting the assessment and the implementation of all measures and the document shall be delivered to the Agency. iii. Solution provider shall use an antivirus and antimalware compatible with container environment and capable of recognizing running containers, with the ability to deal with malicious software without intervention, as well as dealing with all known threats and stopping exploits (exploit prevention). iv. Solution provider shall avail a design to set the access list rules at the services/pods level, not just at the worker nodes level.
CS23	All components of the solution must refrain from utilizing library versions that contain known vulnerabilities, and the vendor must ensure support for security patching of developed components. A patch management solution and process shall be in place.
CS24	SLA with all application, software, and hardware providers must be in place to address the mitigation of any discovered vulnerabilities that affect the current solution. Mitigation time for critical and high-priority vulnerabilities must be within industry standards and best practices.
CS25	Threat Modeling reports shall be performed before going live and be submitted to the agency cyber security sector.
CS26	All solution components at banks' side must be tested before implementation.
CS27	Credentialed Vulnerability assessment compatible with containerized environments (if exists) shall be performed before launch, after any change, and periodically at least once every 3 months. A report for system's servers shall be communicated and vendor shall be committed according agreed SLA to solve any vulnerability related to their system.
CS28	A gray penetration testing shall be performed before launch, after any change, and periodically at least once a year, and results submitted to the agency cyber security sector including the following: All use-cases/scenarios of data input (manually, automated, …), All solution components, and middleware including all integration and portals. The assessor should have a digital certificate to decrypt traffic and sign it
CS29	Secure Software Development Life Cycle (SSDLC) must be followed in any in-house/developed solution component for the agency.

CS30	A secure code audit review shall be performed and submitted to the cybersecurity sector for any developed/customized components.
CS31	Any cybersecurity incident shall be reported to EG-FinCIRT within 1 hour of discovery.
CS32	Cybersecurity requires full results of the prototype regarding the technology stack, technology concepts used, location of implementation and implemented security controls.

Appendix 4: Sample complaint text


السادة البنك المركزي
تحية طيبة وبعد
شكوى مقدمة تجاه بنك الاتحاد فيما يخص سوء التعامل
مع العملاء وعدم معرفة بالمعاملات البنكية وكذلك التهديد
من مشاكل ورفض لحقوق العميل أكثر من مرة لم يتم الرد
على شكوى وتم الرد بأنه لا يوجد حق لي في تلك
الشكوى وتم ذلك بسوء معاملة من ناحية كلا من
الفرع ومركز الاتصالات الخاص بالبنك
وعليه يجب التحكم بحل المشكلة وإفادتي بالرد
في أسرع وقت
شكراً
الاسم/ يوسف المهدي
م/ الرقم: 01xxxxx23