CCU Queries

1. Infrastructure and Hosting

1. **Will FBR provide physical or cloud infrastructure for hosting the CCU, or is the vendor expected to provision and manage this entirely?**
   Vendors are expected to procure, install and operate the required infrastructure, including hardware and software as part of the end-to-end CCU implementation.

2. **Kindly share the intended location(s) for the CCU(s).**
   FBR HQ

3. **Will there be one Central Control Unit (CCU) or multiple CCUs?**
   There will be one CCU at FBR HQ. However, the architecture must be modular and scalable to accommodate distributed control units in future phases.

4. **Will FBR's existing server infrastructure be used, or is the vendor expected to provision a separate server?**
   Yes, vendors are expected to propose and provide all required infrastructure for the CCU setup.

5. **Should the compute infrastructure be hosted in your data center or an external environment?**
   Hosting of both hardware and software compute infrastructure will be on-prem at designated FBR sites. Existing FBR data center infrastructure may serve as a connectivity node, but not for primary hosting.

6. **Is the "technical support and data storage entity" internal to FBR or external?**
   This entity is to be internal to FBR.

7. **Is there a preference for cloud (e.g., AWS, Azure), on-premise, or hybrid architecture?**
   The solution should be on-premise.

8. **Kindly provide a generic list/specification of required hardware so that we can analyze and propose accurate castings.**
   Vendors are expected to size hardware needs based on the scope and sizing parameters mentioned in the RFP (refer to hardware requirements in the RFP document).

9. **Is FBR open to a complete open-source solution given the mention of Postgres and RabbitMQ and the preference stated on page 117?**

FBR is open to the use of open-source tools where feasible and secure. Vendors are welcome to propose a complete open-source solution, provided it meets all technical and performance requirements outlined in the RFP.

10. **Will FBR provide infrastructure (power, cooling, racks, PDUs, servers, storage, switches, firewalls, screens) at the CCU site, and can a site survey be arranged?**
    The FBR will provide power and backup power, however the vendor is responsible for provisioning all other required infrastructure at the FBR-designated CCU site. This includes networking, computing equipment, and monitoring screens. Site surveys can only be facilitated by FBR upon contract award, since the CCU room is currently under construction.

11. **Is the vendor responsible for sizing hardware from FBR/PRAL data center to CCU?**
    Yes, the scope of hardware sizing for the vendor pertains to infrastructure required at the CCU site (FBR HQ) and its integration with the data center. The data center infrastructure itself is not in vendor scope, but compatibility must be ensured by the vendor for smooth data transmission.

12. **Will the FBR infrastructure include SAN or any other shared storage system?**
    Yes, it will include SAN. This is subject to future revision, and it is the responsibility of the vendor to ensure secure, high-volume and fast retrieval of data from the storage system.

13. **Is the existing power infrastructure (Genset, Transformers) at FBR HQ sufficient for the CCU setup?**
    Yes, the existing power infrastructure is sufficient to accommodate the CCU setup. Vendors are expected to propose their own sizing and equipment plan, but the baseline facilities—including transformer capacity and space allocation—are already provisioned by FBR.

14. **Are there specific HA/DR (high availability/disaster recovery) requirements?**
    Yes, redundancy and automated failover mechanisms must be built in to ensure system uptime and uninterrupted operations. As per the RFP, the bidder is expected to submit a complete Disaster Recovery and Business Continuity Plan, which includes redundant infrastructure, off-site backups, and fallback operations. PRAL/FBR sites can be leveraged for hosting off-site backups. The DR provisions must ensure minimal disruption and continuity of CCU operations, which could require more than just server infrastructure depending on the proposed architecture

2. Integration with Existing and Future Systems

15. **Which systems (IRIS, e-Invoicing, POS, SECP, NADRA, etc.) must the CCU integrate with initially?**

The solution should not integrate with FBR internal systems (i.e. IRIS or NADRA), but should integrate with FBR digital integrations, including Track & Trace, production monitoring for sugar and cement, Digital Invoicing (DI), Faceless Customs, CRMs, Traditional and Social Media Scraping, and tracking FBR vehicles through the Vehicle Management System. As more interventions go live, they will also need to be integrated into the CCU.

16. **Will APIs be made available for these systems, or is the vendor expected to develop them?**
    Vendors are expected to develop and manage standardized APIs and data pipelines to enable integrations. If developed already for digital interventions such as production monitoring, these shall be made available to the CCU vendor.

17. **Is there a middleware or integration platform already in place?**
    Vendors must ensure modular architecture and interoperability through their own integration strategy.

3. Data Ingestion and Access

18. **What is the estimated daily/weekly volume of incoming data from digital interventions?**
    Data will be ingested in both real-time and periodically (daily, weekly, monthly), primarily as structured summaries such as diagnostics, logs, and analytics outputs as well as real-time data from factory sites. These will be pre-computed by vendor dashboards hosted with respective intervention owners' infrastructure and accessed by the CCU through targeted pulls. As such, the CCU will not handle large historical data volumes directly, with its role focused on coordinating access and standardizing outputs across multiple vendor formats. The data load from this is currently expected to be in order of MBs per day but gradually increase over time as additional interventions are integrated.
    In select cases the CCU may request camera footage for specific time windows. This footage will be uploaded to and stored within FBR infrastructure and made temporarily available for viewing by the CCU, without requiring long-term storage on the CCU side.

19. **Will historical data be shared? If yes, in what format and through which delivery mechanism (e.g., APIs, FTP, DB dump)?**
    Vendors must support structured migration of historical data with data integrity checks. Formats and mechanisms will be finalized in coordination with FBR. Where available and as needed, APIs shall be made available to the CCU vendor.

20. **What is the volume, format, and source of historical data? Will CCU have its own historical repository?**

Historical data provided for training and baseline analytics will primarily include structured data (e.g., formats could include JSON, CSV, etc.). FBR and PRAL will store and manage this data, while CCU is expected to pull data from specified historical periods whenever necessary (e.g. the capacity to display a dashboard from a specific date by sending a request to PRAL). FBR will provide only the storage capacity, and the interfaces needed for access and data transfer; all processing must be handled by the vendor. FBR might be asked to occasionally store GB large video files from on-site cameras (not en masse). Retention and archival strategies should follow the rolling 90-day cycle outlined in the RFP.

21. **Does the phrase "Support local access" in page 101 refer to access at node/terminal level only?**
    Yes. "Support local access" refers to the ability for designated terminals at enforcement or monitoring nodes (e.g., CCU, regional tax offices) to securely access dashboards and insights generated from CCU without depending on external cloud services.

22. **Are there any restrictions in accessing third-party data sources (e.g., telcos, banks)?**
    Access to external data sources will be coordinated by FBR where necessary. Vendors must design for modular integration readiness. While access to third-party data sources such as telcos or banks is not part of the initial scope—which currently includes only digital interventions deployed or planned by FBR—such integrations may be added at any point based on evolving requirements.

4. Analytics and AI

23. **Are vendors expected to develop AI/ML models, or only provide a framework for analytics?**
    In Phase 1, vendors are not required to develop AI/ML models. Instead, they must provide an analytics platform capable of rule-based anomaly detection and basic predictive functionalities. For example, the system should be able to flag deviations such as a sudden drop in production (e.g., more than 20% compared to the same time on the previous day). Requirements for more advanced AI/ML-driven analytics may be introduced in subsequent phases.

24. **Can you share tentative alerts for each intervention?**
    Most alerts will originate from the dashboards, with the vendor mainly responsible for linking them to the CCU. However, vendors may also be required to set up basic alerts using available data from intervention sites. (See Section V.2.A of the RFP, p. 91, for details.)

Intervention name	Alerts required (tentative and not exhaustive)

Production Tracking & Track and Trace	- Abnormal drop in production count - Detection failure or missing product entries - Discrepancy between physical and reported counts - Camera or system malfunction alert - Tampering or obstruction in monitored area
Point of Sales	- Sudden drop in transaction volume - High-volume sales with no tax invoice - Unusually high discounts or voided sales - POS terminal offline or non-reporting - Transactions outside registered hours/geography
Digital Invoicing	- Failed invoice submission - Duplicate invoice entries - Unregistered buyer/seller detected - Delayed or backdated invoices - Integration failure with DI portal
Cargo Tracking System	- Route deviation from EWB route - EWB not generated for priority goods - Stalled or idle cargo beyond acceptable time - Unauthorized checkpoint crossing - GPS disconnection or tampering
Digital Enforcement Station	- Unverified cargo at checkpost - Suspicious vehicle detected - Vehicle bypassed checkpoint without clearance - Impounded vehicle flag - Inspection skipped or incomplete
Faceless Assessment	- Document discrepancy/mismatch alert - Risk flag on valuation or HS code - Repeated submission errors - Unusual clearance time spikes - Excessive document call-ups
CRM and Litigation dashboards	- Missed legal or procedural deadlines - Case inactivity beyond threshold - Escalation required but not initiated - Repeated adjournments or procedural lapses - Unlinked litigation with enforcement case
3rd party Data Integrations	- Non-filer identified via external data - Under-declared revenue vs 3rd party reported data - Missed response to notices - Delayed submission of required returns - Mismatch between declared and external asset ownership

Journeys	- Incomplete return submissions - Session abandonment before filing - Portal system errors or downtime - Duplicate registrations - Missing document uploads or validation failures
Social Media Scraping	- Spike in negative sentiment regarding tax policies or FBR performance - Surge in mentions of potential tax evasion or smuggling - Geo-tagged posts highlighting suspicious economic activity - Viral public complaints related to tax enforcement or administration - Flagged keywords associated with tax fraud, non-compliance, or protest activity - Repeated reports of enforcement officer misconduct or bribery
Chatbot	- Surge in unresolved or escalated queries - Drop in user satisfaction score below threshold - High volume of repeat queries on the same issue (indicating ineffective resolution) - Detection of query types indicating systemic technical issues (e.g., portal login failures) - Service downtime or unavailability detected via inactivity logs
Vehicle Management System	- Excessive idle time or under-utilization of vehicles - Unauthorized travel outside designated routes or areas - Low frequency of field visits by tax officers - Discrepancy between scheduled and actual site visits - Repeated use of vehicle by unauthorized personnel

25. **Are existing models or datasets already available from FBR?**
    Vendors should be prepared to build their own datasets and models as required by the CCU.

5. Communication System

26. **What is the projected volume of SMS, WhatsApp, or email notifications?**
    Vendors should ensure systems can support scalable messaging volumes. Example notifications may include SMS or WhatsApp alerts for data outages, daily summaries of enforcement interventions, or real-time compliance alerts. Email notifications may also deliver periodic reports or exception logs to relevant stakeholders.

27. **Will government gateways be provided for these channels?**

Where necessary and available, FBR will facilitate use of government gateways. However, the CCU should be standalone in this regard, and vendors must ensure support for integration with commercial gateways to enable uninterrupted communication capability.

28. **Is multilingual communication (e.g., English, Urdu) required?**
    Yes, the communication system should support multilingual messaging such as English and Urdu.

6. Web and Mobile Interface

29. **Is a dedicated mobile application required or is a responsive web interface sufficient?**
    A responsive web interface with role-based dashboards is sufficient to meet the current requirements. However, a dedicated mobile application that ensures secure and user-friendly access would be considered a value-added feature. Vendors may also leverage cross-platform frameworks (e.g., React Native Web) that allow a unified codebase to support both web and mobile interfaces, which would be viewed favorably

30. **Should the interface meet any accessibility or compliance standards (e.g., WCAG)?**
    Interfaces should be user-friendly and designed with responsive and inclusive principles in mind.

7. Security and Regulatory Compliance

31. **Must all data at rest and in transit be encrypted (e.g., AES-256, TLS 1.2)?**
    Yes, encryption of data both at rest and in transit is required.

32. **Will the system undergo third-party penetration testing?**
    Yes.

33. **Will FBR arrange an independent third-party vendor for Penetration and Vulnerability testing, or is the selected vendor expected to include this in their scope and pricing?**
    Penetration and vulnerability testing is within the vendor's scope and must be included in their pricing. The selected vendor is responsible for ensuring data security during transmission and storage through encryption, RBAC, and tamper detection mechanisms and sharing results of the third-party tests.

34. **Can the 5% Performance Bank Guarantee be released after delivery and acceptance of the system instead of being held through the SLA period?**
    No, the 5% Performance Bank Guarantee must remain valid throughout the contract duration to ensure system uptime and SLA adherence. The guarantee covers vendor obligations beyond initial delivery, including support and maintenance.

8. Dashboard and visualization

35. Are there predefined KPIs and visual metrics expected in the initial version of the dashboards?

As outlined in Section V.1 of the RFP (p. 90), the following (non-exhaustive) KPIs and visual metrics are anticipated to be part of the dashboards.

Intervention name	Description	KPIs and visualizations (not exhaustive)
Production Tracking & Track and Trace	Counting of goods produced at various manufacturing sites across key industries	Count of produced items (bags, bales etc.), no. of taxpayer sites with solution deployed, Alerts (e.g., for hardware, production drops), Production count (filterable by line, period, SKU), scanner status, deviations, potential manipulations
Point of Sales	Integration of FBR system with POS solution of provinces (restaurants, services)	Number of transactions (filterable by geography, tax-office, period), deviations, national heatmap, revenue collection
Digital Invoicing	E-invoicing across FMCG, public sector, and other priority sectors	Integrations status by Licensed integrator, number of invoices generated and invoice value (filterable by taxpayer, period, invoice type, jurisdiction), integration status, API uptime, tax return comparison
Cargo Tracking System	Tracking movement of priority goods via e-way billing for suppliers, transporters, buyers	EWBs generated, route heatmap, integration status, vehicle risk status, value triangulation to DI
Digital Enforcement Station	Checkposts across major chokepoints in Indus and Balochistan to counter smuggling	Inspections and impounded vehicles at key checkpoints, enforcement coverage
Faceless Assessment	Automated and anonymous clearance of goods	Number of GD's filed, number of documents called (vs. exempted), average clearance time, revenue collection
CRM and Litigation dashboards	Tracking of litigations across of onboarded law firms across all courts e.g., ATIR, SC, HC	CRM cases status, litigation process updates, deadlines (filterable by court, tax-office)

3rd party Data Integrations	Tracking of return filing and enforcement status for priority high value non-filing individuals	Notices status, notice deadlines, taxpayer filing status, null filing instances (filterable by tax-office, tax-officer)
Journeys	Tracking of return filing portal and simplified registration module	Development and deployment status of simplified registration and return filing modules
Traditional and Social Media Scraping	Access to major news channels / social media platforms and collection and analysis of data from various social media platforms	Social media trends and sentiments, digital campaign performance, traditional media coverage, trending keywords related to tax, enforcement, or public complaints. Volume of posts or mentions related to tax, Sentiment analysis of public commentary (positive, neutral, negative), Geo-tagged content showing location-specific buzz, Screenshots or flagged posts routed as alerts to enforcement teams
Chatbot	AI assistant for taxpayer facilitation for return filing and tax related queries	Number of queries raised (filterable by category, period), user satisfaction level
Vehicle Management System	Tracking utilization of ~1000 cars deployed to FBR officers through a vehicle management system	Utilization per vehicle, utilization per tax office, utilization per unit, locations visited

36. **Are 5 different prototypes with each having some dashboards required and views OR is one prototype having 5 different dashboards with views required?**
    Vendors are required to submit a single prototype consisting of 5 distinct dashboards/views. These should include Executive Overview, Sector-Wise Compliance, and Enforcement Monitoring among others. The evaluation will be based on clarity of layout, functionality, usability, and analytics features (e.g., alerts)

37. **The list of interventions is marked as non-exhaustive. Is there a roadmap for future interventions with FBR that could be shared with the vendor/ bidder?**
    The list of digital interventions provided in the RFP is indicative and non-exhaustive. FBR anticipates future expansion but does not have a detailed roadmap at this stage. However, vendors are encouraged to ensure modularity and flexibility in their architecture to accommodate future interventions.

38. **Regarding social media scraping and sentiment analysis using AI**
    a. **How much historical data Is required?**
    b. **Do you have an existing data repository or preferred sources for scraping (e.g., news channels)?**

    The vendor must be capable of integrating with major social media and news platforms and conducting sentiment analysis. FBR does not currently maintain a proprietary historical social media dataset. Vendors are encouraged to propose sourcing strategies and analytics capabilities using public APIs and sentiment models to deliver insights such as geotagged alerts, volume of mentions, and sentiment trends.

39. **The required quantity of GPS tracking devices has not been mentioned in the REQ. Kindly confirm the exact number. Please clarify the platform/environment where the GPS integrations are to be implemented. Are GPS coordinates required to be tracked in real-time or at periodic intervals?**

    GPS tracking is not required at this stage but may be needed in a future phase. Vendors should ensure the system can integrate real-time or periodic GPS data from field operations if required later. The integration environment will depend on the final deployment architecture (e.g., on-premise or cloud).

40. **Should dashboards support role-based access control and alert configuration?**

    Details regarding this can be found on p.112 of the RFP.

    Yes, the dashboards must support role-based access control and alert configuration. The CCU should provide tailored real-time dashboards for different user groups—including enforcement teams, operators, analysts, and senior leadership—based on their roles and responsibilities.

    Each dashboard should:

    - Display relevant content such as compliance summaries, sector trends, alert logs, and performance metrics.
    - Allow alert configuration and filtering based on user needs.
    - Support both interactive terminal views and large-screen visualizations (e.g., for video walls).
    - Enable real-time updates, filter controls, and data export in multiple formats.

    Examples of dashboard types include:

Dashboard Type	User Persona	Core Features
Executive Overview	FBR Leadership	High-level compliance summaries, risk scores, top alerts, real-time metrics.
Sector-Wise Compliance	CCU Analysts	Industry-specific data (e.g., beverage, cement), variance tracking, flagging.

Enforcement & Investigations	Enforcement Officers	Drilldowns on factories, past visits, open/closed alerts, compliance timelines.
Alert Monitoring Panel	CCU Operators	Live status of alerts (e.g., hardware failure, production drop), response logs.
System Health	Technical Admins	Queue health, server status, camera uptime, intervention diagnostics.
Data Quality Monitor	Analytics Teams	Missing data flags, system lag visualizations, source consistency monitoring.

9. Knowledge Management

41. **Should the Knowledge Portal support multimedia (e.g., videos, documents, PDFs)?**
    Yes, the Knowledge Portal must support various formats including videos, PDFs, and documents.

42. **Is AI-powered document tagging and semantic search required?**
    Vendors may include AI-based tagging and semantic search capabilities as value-added features.

10. Deployment and Operations

43. **Is 24/7 operational support required from day one?**
    Yes, vendors are responsible for 24/7 operation of the CCU with adequate staffing.

44. **Can the timelines for Phase 1 (8 weeks), Phase 2 (10 weeks), and Phase 3 (8 weeks) be extended?**
    The timelines outlined are indicative. FBR may consider vendor-proposed adjustments during contract finalization, provided they are well justified and do not compromise the implementation pace across digital interventions.

45. **Is there a specific target timeframe or a defined milestone for FBR to assume full operational ownership of the CCU system, and what level of vendor support will be required after this transition?**
    According to the tentative plan, the FBR may assume full operational ownership of the CCU system after three years of the Run Phase i.e., upon full delivery of the contract. The contract may be renewed for the vendor to continue providing support to maintain the CCU system. However, this has not been finalized and will be further discussed during the contract award and signing stage.

46. **Is an alert mechanism already in place through any VMS system (for CCTV) or NMS Systems (For Network & Security Infra)? If so, will that need to be pulled to CCU System for consolidation?**

The CCU system must be able to forward alerts generated by digital intervention vendors and create its own alerts using available data. While integration with existing VMS/NMS may support this, the vendor is responsible for developing alert protocols and ensuring automated detection, escalation, and triage within the CCU.

47. **Please clarify the number of required nodes, their functions, and the number of POS devices currently operational or planned.**
Nodes can be inferred the various interventions listed in the RFP, with sub-nodes for specific interventions such as production counting, for which there is separate node for each sector (and site within each sector). Regarding POS, the vendors will not have to directly link the CCU with each POS device, but rather they'll have to link the CCU system with existing dashboards that are already linked to and displaying data on POS devices.

48. **Please clarify if "Post-Warranty Maintenance: Support services for three years" on page 115 refers to a period beyond the initial three-year contract duration (i.e., years 4-6), or if it applies to specific components whose warranty might expire earlier within the three-year contract period.**
The "post-warranty maintenance" refers to support services provided after the initial one-year warranty period. The vendor is expected to offer an additional three years of support covering system updates, patches, technical assistance, and performance optimization beyond the base contract period

49. **Is the vendor expected to follow up with original vendors in case a component failure is flagged by the CCU?**
No, the vendor is not responsible for resolution of issues originating from third-party digital intervention vendors. However, the vendor must build alert-forwarding mechanisms to bring these issues to the attention of the CCU and provide first-level diagnostics as per the functional requirements outlined in the RFP.

50. **What SLA metrics will apply post-deployment (e.g., response time, uptime)?**

As outlined in Section V.2.D of the RFP (p. 93), the following (non-exhaustive) metrics will apply post-deployment. Vendors are expected to have reviewed these requirements in detail:

Example responsibilities	**Example required Performance Standard**	**Example penalty for Non-Compliance**
System uptime	≥ 99.5% uptime for CCU software and interfaces	5% deduction in monthly payment per

Example responsibilities	Example required Performance Standard	Example penalty for Non-Compliance
		incident of unplanned downtime
Integration with FBR Systems	Real-time data sync	Contract review if repeated failures occur
Data Ingestion & Synchronization	≥ 98% of expected data received from connected locations	Written notice for first breach; penalty on recurring violations
Alert accuracy	≥ 95% accuracy and completeness of alerts generated	Mandatory system review and tuning at vendor's expense
Dashboard Responsiveness	Key dashboards load within 3 seconds	2% deduction per week of continued non-compliance
Reporting & Submissions to FBR	Weekly performance reports delivered on time	Deduction per missed submission
Data Backup & Retention Compliance	≥ 99% of required data retained and restorable	10% holdback on milestone payments until compliance confirmed
User Access & Security Logs	All administrative and role-based access logged properly	Escalation to FBR with formal audit if gaps are detected

11. Training and Capacity Building

51. What is the expected audience size and frequency for training (e.g., IT teams, enforcement officers)?

Training must be provided to FBR IT teams, enforcement officers, and relevant users as per the deployment plan. The vendor team will not be replaced following the training and will continue to operate the CCU. Training will be conducted in phases, beginning with the central enforcement team, followed by rollout to tax offices across the country.

While the exact audience size is currently being finalized, all Assistant Commissioners (ACs), Deputy Commissioners (DCs), and above are expected to participate.

52. **In what formats should training be delivered—video, in-person, LMS, manuals?**
Training should be delivered through a combination of formats, including videos, in-person sessions, manuals, and LMS modules. In-person training should be conducted for staff based at FBR Headquarters, while remote training sessions should be arranged for regional and field offices. All training materials—including session recordings, manuals, and guides—must be systematically documented and stored in the CCU Knowledge Base for future reference and ongoing capacity building.

12. Hardware and Human Resource Requirements

53. **How many operator screens, video walls, or monitoring terminals are required at the CCU?**
The vendor must deploy necessary operator terminals, screens, and control equipment as per their design proposal. The vendor must plan for an initial setup of approximately 25 industrial-grade display screens, with the capacity to scale up to a maximum of 50 screens over the course of the contract period based on operational needs.

54. **What is the maximum number of on-site staff required to be deployed by the vendor for CCU operations (e.g., analysts, engineers, support staff)?**
The CCU will operate continuously with two rotational shifts:
    - Day Shift operators covering full dashboard monitoring and alert triage.
    - Night Shift operators ensuring minimal downtime and alert response readiness.

Vendors are encouraged to propose their own staffing plans and team sizes aligned with their operating model, while ensuring uninterrupted CCU functionality and performance.

55. **Will FBR deploy any staff, or is the vendor responsible for full operational staffing?**
Vendors are responsible for full operational staffing of the CCU to ensure uninterrupted monitoring, system performance, alert triage, and technical support. However, FBR will deploy CCU teams to provide ongoing oversight of vendor operations through daily coordination and check-ins. These FBR teams will also analyze data and compare with tax records to identify non-compliance, and liaise with other FBR departments (e.g., Operations, tax offices) to route validated alerts for enforcement action.

56. **Are any qualifications or certifications required for CCU staff?**
Yes. Staff must be appropriately qualified and experienced for their respective roles, and vendors are required to provide CVs of key personnel aligned to CCU needs. The following role-specific qualifications are expected:
    - **System Administrators, Network Engineers, and Database Managers:** Must have **certified expertise** in relevant IT infrastructure, system security, and

database tools (e.g., certifications in Linux/Windows administration, Oracle, or SQL databases, etc.), and **3–5 years of hands-on experience**.

- **Real-time Monitoring & Operations Staff:** Should have **prior experience operating centralized control rooms or monitoring platforms**, with familiarity in working across shifts and handling escalations.
- **Enforcement Analysts and Data Scientists:** Should have a background in **data analytics**, enforcement systems, or tax compliance, with **experience using anomaly detection tools and enforcement dashboards**.
- **Managers and Team Leads:** Must demonstrate **strong managerial oversight capabilities**, preferably with a history of managing multi-role technical teams on similar projects.

Vendors will be evaluated based on the mapping of proposed team members to these roles and must clearly demonstrate the qualifications, certifications, and relevant past experience for each key function.

13. Edge Computing and Remote Site Requirements

57. Is the vendor required to install edge computing devices (gateways, microservers) at digital intervention sites to pre-process or propagate data to the central CCU?

If necessary to ensure real-time data transmission, vendors may have to install edge computing devices. However, this may not be required at the initial stage, with edge computing already occurring by the respective vendors assigned to digital interventions.

58. If yes, how many such sites are currently operational or planned?

The number of sites will expand over time across sectors such as sugar, textile, cement, and beverages. Under the initial scope for production counting, the following sites are planned:

- Sugar: 82 sites
- Cement: 27 sites
- Textile: 301 sites
- Beverages: 55 sites

These sites will be integrated into the CCU in phases. Vendors must design their systems to support scalable onboarding, real-time data transmission, and centralized monitoring. Additional sectors and sites will be added over time as FBR continues to roll out digital interventions across other industries.

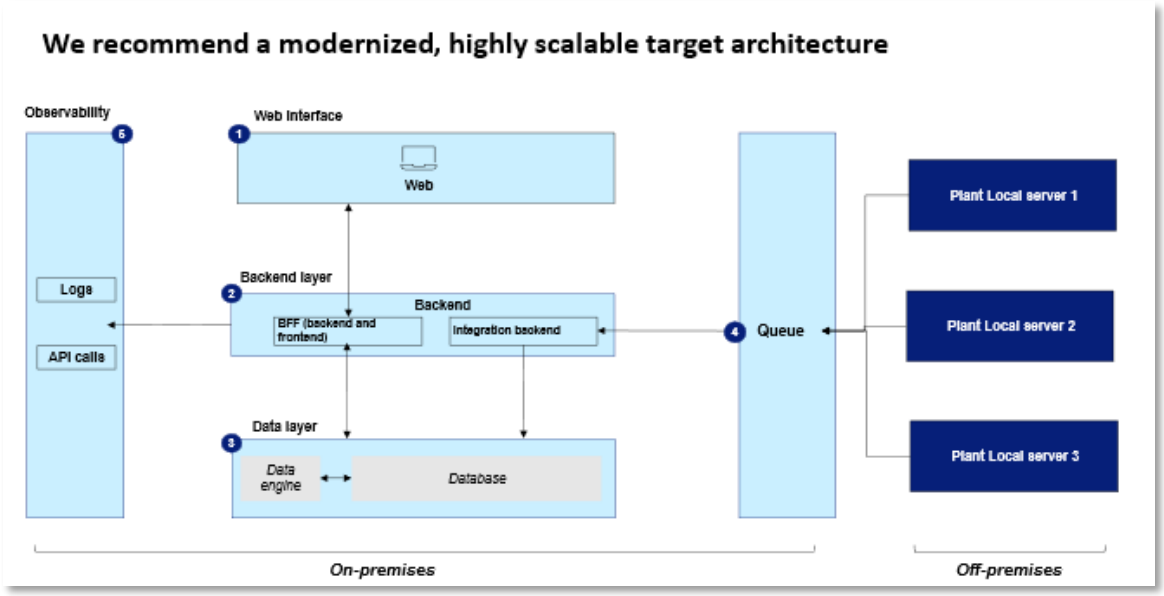
59. What is the preferred mode of connectivity from these remote sites to the central repository (e.g., 4G, fiber, VPN, leased line)?

The preferred connectivity approach is API-based integration over a secure and stable internet connection, enabling structured data to be transmitted efficiently from remote sites to FBR's central repository. However, for remote sites where internet connectivity is not secure and stable, a fiber-based option would be preferred. This mode allows real-

time or near-real-time communication while maintaining modularity and scalability across vendor solutions.

For sensitive data transfer (such as real-time analytics or logs), the API calls must be secured via HTTPS and token-based authentication, and where required, a VPN layer may be added for additional encryption.

Please refer to the below tentative architecture diagram (listed in appendix A of the RFP), which outlines the proposed data flow and integration model:



Behind this setup will be a multi-layered technical architecture, comprising:

1. **Web Interface:** A user-facing web app using best-in-class technologies, allowing CCU operators to view dashboards, access alerts, and interact with enforcement data in real time.
2. **Backend Layer:** A monolithic backend consisting of two engines—
    a. BFF (Backend for Frontend) to generate and render dashboards, charts, and reports.
    b. Integration Backend to collect messages from the queue and populate the CCU database with structured data.
3. **Data Layer (Database & Data Engine):** A centralized on-premise system hosted by PRAL (Pakistan Revenue Automation Limited), responsible for storing, processing, and managing data from all deployed digital interventions.
4. **Message Queue:** An asynchronous messaging system to transfer data from plant servers to the CCU for real-time ingestion and alerting.

5. **Observability Layer:** A module that continuously tracks system health, logs events, and monitors error traces to ensure uninterrupted system performance and rapid fault detection.