346.36

Request for Proposal for the Development and Implementation of the Investigation Module for the Vigilance Cases and Enquiry Management System (VCEMS)

VIGILANCE AND ANTI-CORRUPTION BUREAU DIRECTORATE

PMG, Vikas Bhavan P.O, Opposite KSRTC Depot,

Thiruvananthapuram, Kerala-695033, India.

Table of Contents

1. Introduction

The Vigilance and Anti-Corruption Bureau (VACB), Kerala, is committed to enhancing transparency, efficiency, and accountability in handling vigilance cases through digital transformation. As part of this initiative, VACB is seeking proposals from qualified and experienced software development firms for the design, development, and implementation of an Investigation Module as an integral component of the Vigilance Cases and Enquiry Management System (VCEMS).

2. Existing System

The Vigilance Cases and Enquiry Management System (VCEMS) is an operational web-based platform designed to support the digital handling of vigilance-related activities within the Vigilance and Anti-Corruption Bureau (VACB). The current system includes key modules such as General Diary, FIR Registration, User Management, Unit Management, and integration with various stakeholders, facilitating structured and secure data management across all vigilance units. VCEMS is actively used by approximately 1,000 registered users across 24 offices, with an average of fewer than 300 FIRs registered annually.

Despite this digital infrastructure, the investigation process is still handled manually by Investigation Officers, which creates significant challenges in terms of tracking progress, ensuring accountability, and enabling timely decision-making. Documents are often prepared and maintained in physical form, requiring manual compilation, approvals, and communication between various stakeholders. This results in delays, increased administrative workload, and potential loss or misplacement of crucial case information. To address these gaps and fully digitize the case lifecycle, the development of a robust and integrated Investigation Module is essential.

Currently, after the FIR is registered, the investigation proceeds through a series of manual steps including entrustment to an Investigating Officer (IO), field-level evidence collection, interrogation, preparation of various reports and memos, arrests (if any), and legal documentation. Each stage requires separate approvals and paper-based submissions to supervisory officers and the Directorate. Once the investigation concludes, the final report - whether it be a Charge Sheet, Further Investigation Report or Closure Report - is prepared manually and submitted physically to the court of jurisdiction. This fragmented and paper-intensive approach makes it difficult to ensure transparency, monitor case timelines, or efficiently collaborate across units and departments.

3. Objectives

- Developing further modules in VCEMS to handle investigation and other legal work flows.

- Digitize all investigation workflows to minimize manual intervention.
- Court case management and appeal & revision management.
- Enhance tracking & monitoring of cases with real-time updates.
- Ensure secure storage & retrieval of investigation-related documents.
- Facilitate role-based access control for investigators, supervisors, and administrators.
- Enable integration with external systems to improve compliance with legal and procedural requirements.
- Digitization of legacy data
- Reports & Analytics of cases.

4. Scope of Work

The Investigation Module shall be an integral component of the Vigilance Cases and Enquiry Management System (VCEMS), designed to digitally transform the end-to-end investigation life cycle within the Vigilance and Anti-Corruption Bureau (VACB). The module shall include an intuitive interface, robust tracking mechanisms, and centralized content storage to streamline investigation workflows.

It shall empower VACB users to digitally initiate, assign, monitor, and close investigation tasks, ensuring full visibility and accountability throughout the process. The module should be built on a compliant workflow engine, enabling configurable and automated investigation workflows aligned with VACB's operational standards. It shall also offer real-time status updates, automated notifications, and role-based access control to ensure data integrity and operational efficiency.

The Investigation Module will serve as a centralized hub for managing investigation-related documents, evidence, and reports, enabling seamless collaboration between investigators, supervisory officers, and administrative personnel. It will enhance transparency, minimize manual interventions, and accelerate the resolution of cases while ensuring strict adherence to legal and procedural norms.

Furthermore, the module shall be capable of secure integration with external systems and stakeholders, including the **Vigilance Court Management System (VCMS)** of Vigilance Court, **Internal Administrative Processing System (IAPS)** of VACB, **VACB SUITE, eOffice, VACB website** and other relevant platforms identified at the time of development. These integrations will ensure uninterrupted data exchange, reduce redundancy, and enable end-to-end digital case processing—from FIR registration to final reporting and legal proceedings.

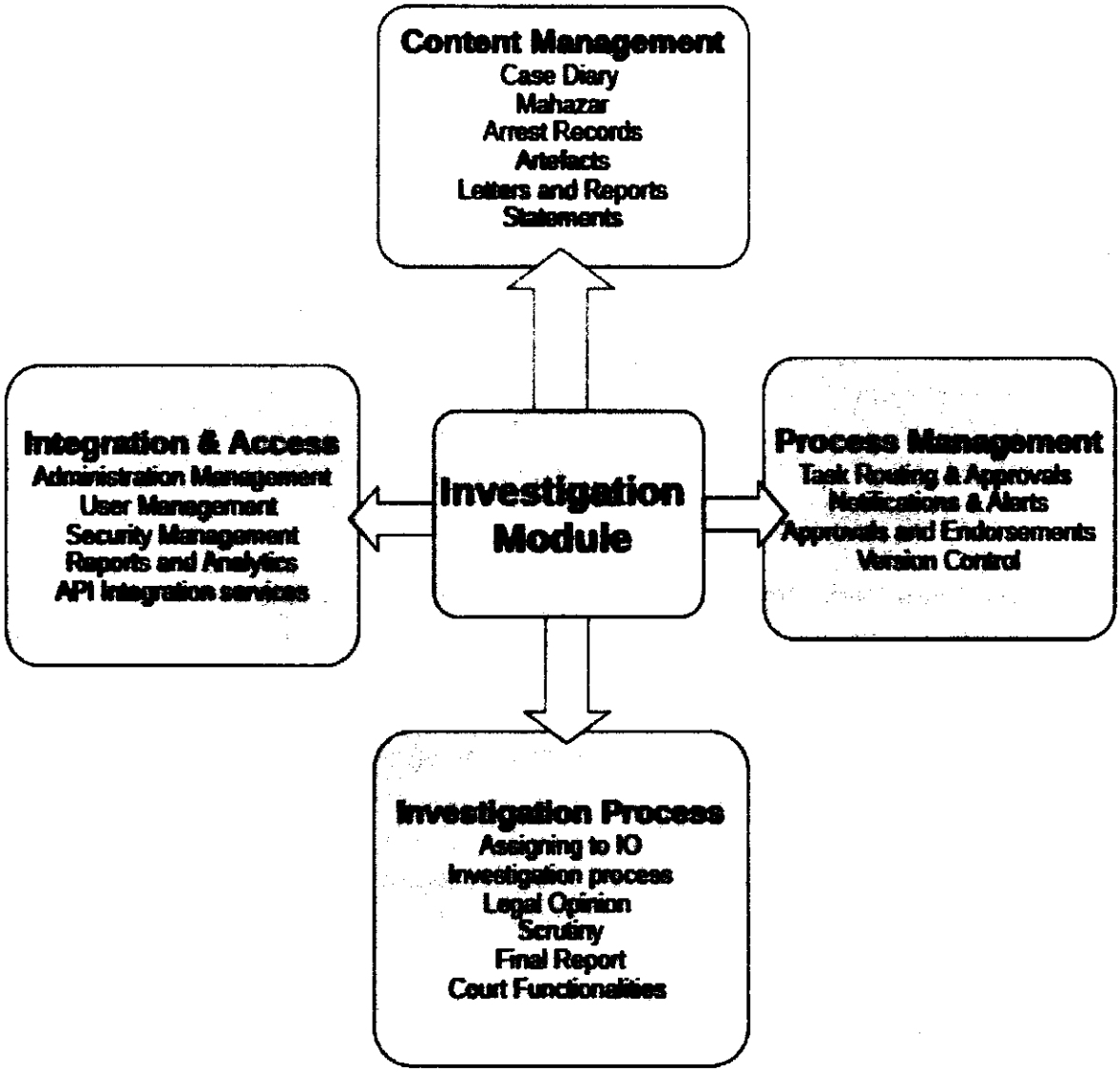
Investigation Workflow and Functional Roles

The Investigation Module will be designed to replicate and digitize the end-to-end investigation process followed by the Vigilance and Anti-Corruption Bureau (VACB),

while ensuring compliance with procedural norms and legal mandates. The workflow will be based on configurable workflow compliant processes to allow flexibility, role-based task routing, and automated alerts throughout the investigation lifecycle.

Typical Workflow (From FIR to Final Report Submission):

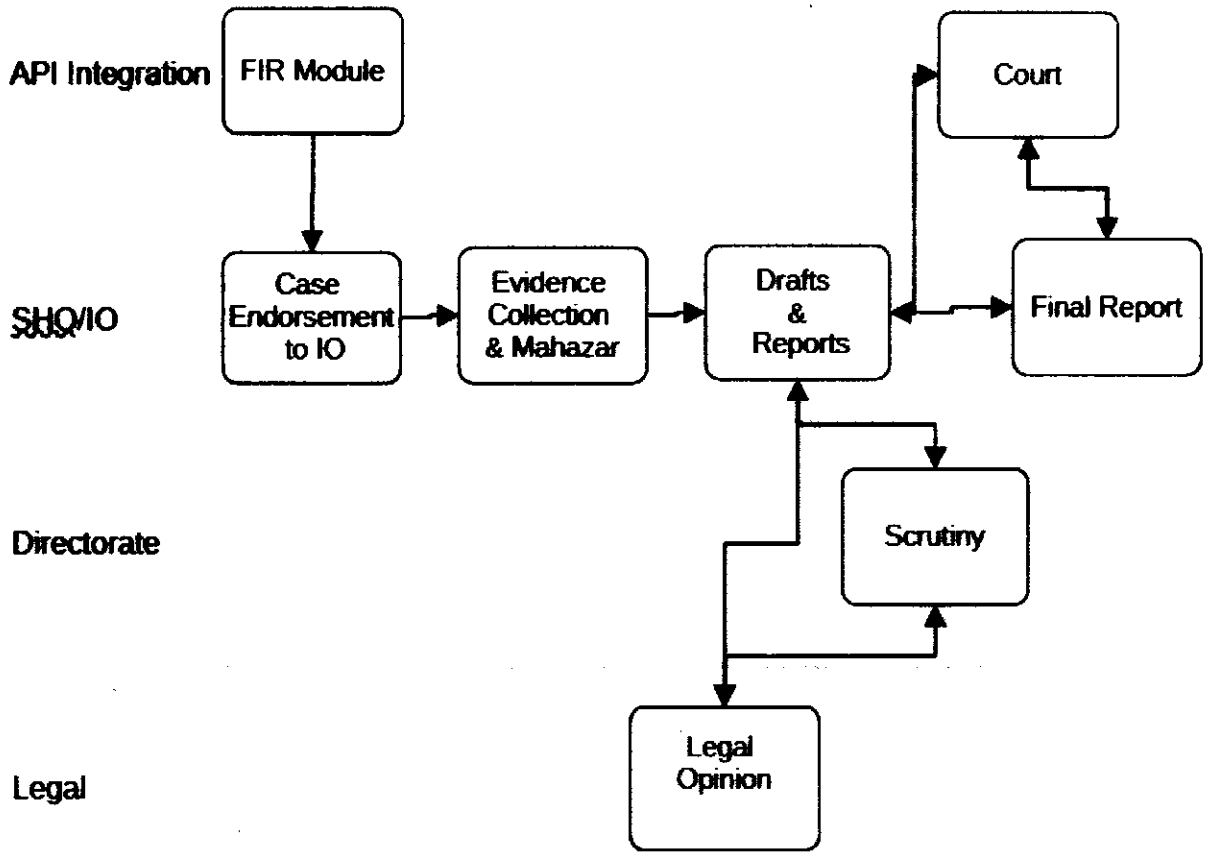
- **FIR Registration:** Registered by the SHO or authorized officer through the FIR module.
- **Case Entrustment:** Case assigned to a specific Investigating Officer (IO) by the Unit Head.
- **General Diary (GD) Entry:** IO logs investigation events chronologically in the Case Diary (KPF 24).
- **Evidence Collection & Recording:** IO performs searches, seizures, arrests, interrogations, inspections, etc., and records findings through corresponding artefacts.
- **Witness Statements:** Statements from relevant individuals are recorded and attached to the case file.
- **Supervisory Oversight:** Periodic scrutiny and approvals by the Supervisory Officer through digital endorsements.
- **Legal Review:** Legal opinion and sanction procedures (e.g., 17A, 19A) integrated into the workflow.
- **Final Report Generation:** IO prepares the Final Report (e.g., Charge Sheet, FID, Closure) based on gathered evidence.
- **Approval and Court Submission:** The report is reviewed and endorsed by the Director before being submitted digitally to the appropriate court.



Functional Roles and Responsibilities:

Role	Responsibilities
Station House Officer (SHO) / Unit Head	Entrusts investigation, approves critical actions like arrest or search, reassigns IOs, and performs first-level review.
Investigating Officer (IO)	Responsible for conducting the investigation, updating the case diary (CD), collecting evidence, recording statements, preparing various reports and memos, and submitting recommendations for final action.

Investigation Assistant (IA)	Assists the IO by preparing drafts of investigation-related documents such as case diaries, witness statements, recovery reports, and other artefacts. The IA supports data entry, formatting, and documentation tasks under the supervision of the IO.
Supervisory Officer (DySP/SP/Range Officer)	Provides oversight on case progress, endorses IO submissions, ensures adherence to timelines and legal protocols.
Legal Advisor	Offers legal opinions, verifies section applications, and ensures readiness for prosecution.
Director / Directorate Officer	Final scrutiny and approval authority for major actions including sanction recommendations and final report submission.
System Administrator	Manages user access, assigns roles, handles configurations, and ensures security compliance.



5. Proposed System

The proposed Investigation Module will serve as a centralized digital platform to manage the end-to-end investigation lifecycle, from case registration to final reporting and court submissions. The module must streamline workflows, ensure secure documentation, and facilitate seamless collaboration among investigators, supervisory officers, and legal authorities while adhering to statutory requirements and procedural norms. Low-code or no-code platforms are not acceptable. The solution must be fully custom-developed to meet the functional, technical, and security requirements specified in this RFP

The Investigation Module shall:

- Be developed as a fully integrated component of VCEMS.
- Provide intuitive UI/UX for investigators, supervisors, and administrators.

- Enable digital initiation, assignment, monitoring, and closure of investigation activities.
- Provide role-based access control and audit trails.
- Offer real-time status tracking, versioning, and digital signing.
- Support integration with digital signature solutions and Court Management Systems.
- Be accessible across devices (desktop/tablet/mobile).

6. Technical Requirements

- Role-based access control (RBAC) with multi-level approval mechanisms.
- Real-time notifications & alerts.
- Secure document management system with version control.
- Digital signature support (as per IT Act, 2000).
- Responsive UI (Web & Mobile-friendly).
- Audit logs for all user actions and system events.

6.1 Security & Compliance

- Data encryption for selected criteria (at rest & in transit).
- GDPR/Data Protection compliance.
- Multi-factor authentication (MFA).
- Disaster recovery & backup mechanisms.

7. Functional Requirements

The system shall natively support creation, editing, versioning, and secure storage of the following mandatory artefacts/forms:

7.1. Reports & Analytics of cases

A comprehensive module should be included in the system for generating various reports commonly used by the Vigilance and Anti-Corruption Bureau (VACB). This module must support both standard and customizable reporting capabilities, enabling users to generate dynamic reports based on selected parameters such as case type, status, investigation stage, officer assigned, timelines, and other relevant data fields.

The system should also include an intuitive analytical dashboard that provides real-time insights and visual representations (e.g., charts, graphs, heatmaps)

of key performance indicators and case metrics. In addition to high-level summaries, the module should support drill-down capabilities to facilitate detailed case-level analysis.

Advanced analytics features such as performance analytics, anomaly detection, and workload distribution should be considered to enhance operational decision-making. The reporting and analytics module should allow exporting of reports in multiple formats (e.g., PDF, Excel, CSV) and support scheduled report generation and distribution via email or internal notifications.

User access to reports and dashboards should be role-based to ensure data confidentiality and integrity.

8. Core Application Functionalities

- User Management
- Unit Management
- Designation Management
- Case Initiation & Assignment
- Investigation Management (creation, versioning, digital signing, export)
    - Case Diary & Progress Tracking
    - Accused and Arrest Management
    - Witness & Evidence Management
    - Case property/ evidence management
    - Search & Seizure Documentation
    - Submission/ reports to court and other stakeholders
    - Legal & Expert Opinion Integration
    - Prosecution Sanction & Court Submission
    - Final Report(Charge Sheet, FAD, etc.)
    - Document management System
- Prosecution module
    - Court trial and disposal
    - Appeal & revision
- Digital registers & Analytical reports
- Search and Vigilance Clearance reports
- Integration with other stakeholders
- Data Archiving

8.1 Case Management System

(information regarding IO, IA and draft preparation)

8.1.1 Case Registration Intimation to Directorate

Details of the cases should be intimated to VACB Directorate with relevant details at the initiation of Investigation of Vigilance Case. (details need to be elaborated).

8.2 Investigation Workflow Management

8.2.1 Assignment of Investigation

(details as paragraph- if a person assigned a case no one can transfer him from the current unit without completing his assignments like CD)

- Hierarchical entrustment workflow:
    - Unit Head → IO assignment with digital orders
    - Transfer cases (intra-unit with SHO approval)
    - Directorate-level case reassignment

8.2.2 Process Automation

- Deadline tracking for statutory timelines
- Escalation matrix for overdue tasks
- Audit trail of all reassignments

8.3. Case Diary (CD) Module – KPF 24

The Case Diary Module is a critical component of the Investigation Management System. As mandated under law and police procedural codes (KPF 24), it is the official chronological record maintained by the Investigating Officer (IO) to capture every investigative action from the time of FIR registration to final report submission. The module must be designed to facilitate daily entry, editing, and finalization of investigation notes in a secure, traceable, and legally compliant manner.The functional requirements are given below.

8.3.1. Dual Interface View

- The module shall load with:
- Calendar View: Visual timeline of CD entries mapped to specific dates.
- List View: Tabular format showing entries by serial number, date, stage, and status (draft/submitted).
- Users can toggle between views for ease of navigation and monitoring.

8.3.2. Draft Mode by Default

- All CD entries should be created and stored in draft mode until explicitly submitted by the IO.

- Drafts should be persisted across logins, preventing data loss during system outages or user timeouts.

8.3.3. Manual Date Entry

- The CD date should be manually selectable to reflect the actual date of the investigative event.
- This is to support situations where the IO was in the field and could not enter the CD in real-time.

8.3.4. Auto-Draft Generation

- Upon FIR registration, the system shall auto-generate predefined CD sections as drafts, including:
- FIR Registration
- Complainant Details
- First Information Statement (FIS)
- Witness Statements
- Document Collection
- Property Recovery
- Alterations (Sections, Accused)
- These drafts should be editable and expandable as the case progresses.

8.3.5 CD Entry Format

Each Case Diary entry must follow the standardised format laid out in Kerala Police's KPF 24 protocol. The system should present a structured interface where each key investigative detail is recorded in designated sections.

- Date of Registration: This captures the date when the FIR was formally registered. It should be a one-time entry, non-editable once the first CD entry is submitted to ensure legal and chronological integrity.
- Officer Who Registered: This section records the name, rank, and official identification of the officer who registered the case. Like the registration date, this field should be locked after the initial submission.
- Name of Accused: This field should allow the IO to record the names of one or more accused individuals related to the case. The system must support

the addition or removal of accused during the investigation while maintaining a complete audit log of any changes.

- Stolen Property Details: This section must enable entry of details about any property reported as stolen, including item description, quantity, and estimated value. These entries help trace the original complaint and track its resolution.
- Recovered Property Details: This area captures information on items recovered during the investigation. It should include specifics like the item description, the date of recovery, location, and the person or context from which the property was recovered.
- Previous CD Date: This is a system-generated field showing the date of the last CD entry. It ensures the continuity and logical progression of the investigation narrative.
- Places Visited: The IO should be able to enter a list of locations visited as part of the investigation. Each entry must include the place name, date, time, and the investigative reason for visiting.
- Persons Questioned: This section records all individuals questioned by the IO, including suspects, witnesses, and officials. It should include the person's name, their relation to the case, and a brief summary of the interaction.
- Main CD Entry (Narrative): This is the most critical part of the case diary. It must be provided as a large text field on the right-hand side of the entry screen. Here, the IO will write a comprehensive narrative of the investigative activities, findings, observations, or procedural updates for the day. The left side of the screen should simultaneously display the structured fields listed above (from date of registration to persons questioned) for easy cross-reference while drafting the main entry.

8.3.6 Submission Workflow

- Only after all mandatory fields are filled, the system will allow the IO to click Submit.
- Upon submission:
    - Entry becomes read-only and time-stamped.
    - Entry is digitally signed (or logged with officer ID and credentials).
    - Submitted entries are version-controlled and audit-logged.

- No editing is permitted once submitted. In case of errors, a supervisor-based correction workflow should be available.

8.3.7 Security and Compliance

- Access Control: Only designated IOs or authorized personnel can create/edit CD entries.
- Audit Trail: All actions (create, edit, submit, delete) must be logged with timestamp, user ID, and IP.
- Legal Compliance: Module must comply with Indian Evidence Act and CrPC for admissibility in court.
- Backup: All CD data must be backed up securely with disaster recovery capability.

8.3.8 Integration Points

- FIR Module: Auto-fetch data from FIR (accused, sections, complainant).
- Document Upload: Attach scanned evidence, statements, or supporting files to any CD entry.
- Property Recovery Module: Link to seized item records.
- User Management: Ensure only designated IOs can submit final CD entries

8.3.9 Reporting and Export

- Generate Case Diary Report (PDF/Print) for court or administrative use.
- Allow filtering by date, type, or officer.
- Export with e-signature or QR code verification for authenticity.

- Chronological digital diary with:
  - Immutable initial entry (date, registering officer)
  - Dynamic accused/property records (multiple entries)
  - Investigation timeline visualization
  - Dual-column layout (left: metadata, right: narrative)
  - Left Side: Date of Investigation, FIR Date, Name of Complainant, Name of Accused, Property Lost, Property Recovered, Prior CD Date, Places Visited, Witnessed Questioned)
  - Right Side: Narrative - Record of Investigation for that day.

- All activities on a particular day must be listed in a panel on the right side and able to be placed in the CD.
- Provision for Edit & Save multiple times and Submission
- Version control with digital signatures

8.4 Mahazar

8.4.1 Entrustment Mahazar (Mahazar taken before the arrest)

Entrustment Mahazar is typically prepared in trap cases (especially in bribery or corruption-related vigilance cases). It is done before conducting the trap, where procedures are carefully documented in the presence of independent government witnesses. This mahazar records the entrustment of trap money or marked currency notes to the complainant, along with the details of the procedure followed—such as applying phenolphthalein powder, noting serial numbers, and briefing the witnesses and complainant. The purpose is to establish a transparent, pre-trap record of the items used and the method adopted, which can be legally relied upon during trial. It includes the names and signatures of government witnesses, the complainant, vigilance officials, and detailed descriptions of the items and the roles of each person involved. This document is crucial to demonstrate the legality and fairness of the trap operation.

8.4.2 Recovery Mahazar (Mahazar after the arrest)

The Recovery Mahazar is prepared after the trap is executed and the accused is caught red-handed, or after any arrest during investigation. It documents the recovery of trap money, other incriminating items, documents, or articles from the accused or from a relevant location. It contains precise information about where and how the recovery was made, who was present, and what was seized—such as marked currency, voice/video recordings, devices, or files. This mahazar is signed by the investigating officer, independent witnesses (preferably the same government witnesses used in the trap), and may also include the accused's acknowledgment. This document is critical to establishing evidentiary linkage between the accused and the recovered material in a court of law.

8.5 Arrest & Custody Management

8.5.1 Arrest

This is the procedure of taking custody of the accused. In vigilance cases, arrest will only be conducted after the formal registration of the case (FIR). A single case may involve multiple accused, and accordingly, there may be more than one arrest

associated with the same case. These arrests can occur at different times, meaning even after one arrest is made, further arrests related to the same case may take place as the investigation progresses and more evidence emerges.

- **Inside PS or outside**
  The arrest may occur within the police station (PS) if the accused is summoned and taken into custody there, or it may happen outside, such as at the accused's residence, office, or a public place. Proper location documentation is required in both scenarios.

- **GD linking**
  The arrest event must be linked to the General Diary (GD) entry of the police station, referencing the date, time, and context of the arrest to maintain an official and chronological record.

- **Date and time**
  The exact date and time of the arrest must be recorded precisely. This timestamp is crucial for legal compliance, especially for court production within 24 hours and remand procedures.

- **Reason for arrest**
  The grounds on which the arrest is being made must be clearly stated, typically involving specific sections of the Prevention of Corruption Act or IPC, based on the evidence gathered.

- **PSR (Prison Search Register)**
  Check the details of the arrested person against the Prison Search Register (SR) to verify whether the individual has any prior history of imprisonment or detention. This involves cross-verifying with the official prison records to identify if the accused has been previously lodged in any jail for any past offences. The findings from this check should be documented and linked to the case file for reference during investigation and prosecution.

- **Arresting officer**
  The details of the officer carrying out the arrest, including name, rank, and badge number, should be documented. The officer must also be legally authorized to conduct such arrests.

- **Intimation**
  The arrested individual's family member or a nominated person must be informed about the arrest. Proof of such intimation or communication should be recorded and acknowledged.

- **Medical Examination**
  As per law, a mandatory medical examination of the accused must be conducted before and after custody to ensure that the accused's health condition is documented and to prevent false allegations of physical abuse.

- **Legal Rights**
  The accused must be informed of their legal rights, including the right to remain silent, the right to consult a lawyer, and the right to be produced before a magistrate within 24 hours. This is a constitutional safeguard.

- **Recovered items while arrest/properties**
  If any items, documents, cash, or assets are recovered from the accused during arrest, these must be listed clearly, sealed properly, and entered into the seizure memo for evidentiary use.

- **Witness while arrest (May be a police witness also; in that case, load details with pen number)**
  The presence of independent or police witnesses during the arrest is essential. Their names, designations, and identification details (like pen number for police witnesses) must be recorded to validate the legality of the arrest.

- **Photo of accused**
  A photograph of the accused at the time of arrest must be taken and preserved as part of the arrest record, useful for documentation and identification purposes.

- **Signature (Digital/Normal)**
  The accused's signature (either digital or manual) should be taken on key documents like the arrest memo, acknowledging their arrest and awareness of their rights.

8.5.2 Generating Forms after arrest

Following the arrest, several standard forms and records must be generated as part of the official arrest documentation process:

- **Arrest Memo(KPF 14(B)**
  A formal document that records details of the arrest, including District, Police Station, Crime Number (if any), Section of Law, Date and Time of Arrest, Place of Arrest, Name and Address of arrestee, Particulars of body search, (a) Wearing apparels/ Valuables/ Weapons /other items, (b)Injuries if any Any request for Medical Examination by Arrestee or Name of the police officer who took initiative to conduct Medical Examination, Name and Signature / Thump impression of Arrestee,

Signature of SHO. This is a critical legal requirement and must follow the predefined format.

- **Inspection Memo(Form 14)**
  A formal document that records details of the arrest, District, Police Station, Crime Number (if any), Section of Law, Date of Commission, Name and Address of arrestee, Taken into Custody, (a) By whom with designation, (b) Date and Time (c) Place Name and address of witness (may be more than one), Their relation to Arrestee, Information to the relative of Arrestee, Signature of Arrestee, Signature of Witness (may be one one more if more than one then numberings should be there), Signature of Police Personal, Place & Date. This is also a predefined format.

8.5.3 Custody Memo

This is also a formal document with a prescribed format containing the following fields: Police Station, District, FIR No., Crime Number, Section of Law, Name and Address of the person arrested taken to custody, Aadhar No (UID) of the person arrested taken to custody, Date time and place of arrest, Grounds for arrest, custody.

- **Intimation**
  A document that confirms that intimation has been sent to a family member or relative of the arrested person, as per legal mandate.

- **Arrest Card**
  A summary card containing key details of the arrested person, useful for internal tracking and presentation in custodial logs.

8.5.4 Arrest View

A consolidated digital or visual dashboard view of the arrest, which may include timelines, forms generated, custody status, and other critical information for administrative use or court presentation

8.5.5 Custody Monitoring

- Judicial/police custody clock
- Affidavit and custody request
- Production warrant request
- Automated remand date alerts
- Remand extension report
- Bail bond tracking with court calendar sync

8.6 Accused details (Name, Address, PEN , official address, Phone number, Identification mark, Father name, AADHAR, Date of retirement, check box for government and private person, photo, dossier number if any)

8.7 Evidence Management

8.7.1 Digital Evidence Repository

- Chain-of-custody tracking for:
  The investigation process must ensure proper handling and documentation of seized property, records, and documents through mahazars or inventories supported by geo-tagged photographs. Forensic submissions should include detailed lab requests, report tracking, forwarding notes, and standard requisition forms to maintain evidentiary integrity. Document recovery should utilize Form 15 with OCR capabilities to digitize and preserve recovered evidence. Property recovery must be documented using KPF 151 A. The discovery of BSA under relevant provisions, along with the issuance of Certificates under Section 63(4)(c) Part A and Part B of the BSA and 65B certificates, must be meticulously recorded. A robust Chain of Custody form should be maintained at every transfer stage to ensure authenticity. Additionally, expert opinions—whether civil or mechanical—should be sought and documented as needed to support the investigation

8.8 General Letters/Reports

8.9 Investigative Actions

- Dynamic section/accused modification log
- Site inspection toolkit:
  - Sketch mapping tools
  - Multimedia annotation
  - Team assignment records

8.10 Supervision & Legal Processing

8.10.1 Approval Workflows

- Multi-level review system:
  - IO → Supervisor endorsement with e-sign
  - Investigation report
  - Legal opinion
  - Director's scrutiny dashboard
  - Prosecution sanction
  - Sanction tracking (17A/19) with G2G integration

8.10.2 Prosecution Preparation

- Charge sheet assembler with:
  - Automatic form population
  - Witness list manager
  - Evidence cataloging

8.11 Court Integration

8.11.1 Judicial Interface

- Automated Court document packager:
  - Summons/Warrant Generator

- 84/85 BNSS procedural checklist
- Judgment digest system

8.11.2 Post-Submission Tracking

- Further investigation tasking module
- Appeal case cloning feature
- Convict management system

8.11.3 Timeline of Activity

This feature displays the complete chronological sequence of events for each case, beginning from the date of registration (FIR) and including every subsequent update, such as evidence collection, arrest, statements, forensic results, remand actions, and report submissions. The timeline should be rendered in a graphical interface (e.g., linear chart or vertical flow) for easy understanding. Upon selecting a case, this timeline must be automatically displayed at the front, ensuring the investigating officer or supervisor gets an immediate overview of the case progress.

8.11.4 Draft

This section acts as a workspace for investigators to record and save work-in-progress data before formal submission or approval. All entries—including notes, interim reports, suspect details, statements, and other evidence—should remain intact and unchanged, even if the user logs out unexpectedly or the session ends. This ensures data is not lost and investigators can resume from where they left off.

8.12 Accused (Name in English)

This module shall handle the management of accused individuals in an investigation, ensuring accuracy, consistency, and auditability.

8.12.1 Standardization of Names

All names of accused individuals must be entered and displayed in **English** to maintain standardization and uniformity across all documents, reports, and database entries.

8.12.2 Auto-Fetch from FIR

If the **First Information Report (FIR)** already includes details of any accused persons, the system shall automatically fetch and populate this information into the investigation module. This reduces redundancy and ensures data consistency with the FIR.

8.12.3 Manual Addition of Accused

The system must allow investigators to **manually add** new accused individuals who are identified during the course of the investigation but were not originally listed in the FIR. The following details must be captured:

- Full name and alias (if any)
- Gender and age
- Permanent and current address
- Contact details
- Identity proof
- Photograph
- Profession and department (if public servant)
- Role in the offence
- FIR linkage and case connection

8.12.4 Edit Functionality

Investigators must be able to **edit or update** existing information about accused individuals as new details emerge. All modifications must be:

- Logged with timestamps
- Tagged with the editing user's identity
- Maintained as part of an **audit trail** for legal and procedural accountability

8.12.5 Deletion of Accused Entries

The system must allow authorized users to **delete** an accused entry if it was mistakenly added or wrongly associated with the case. Such deletion must:

- Require system confirmation or administrative authorization
- Be recorded in the system logs for **transparency and traceability**

8.12.6 Retrieval of Previous Case History

The system shall automatically **search and retrieve previous case history** of any accused individual from the vigilance records, if available. This includes:

- Previous FIR numbers
- Charges and case status
- Court outcomes
- Investigation remarks

This functionality aids in identifying **repeat offenders** and facilitates **pattern analysis** to strengthen ongoing investigations.

8.12a Digitalization of Legacy Data

A digitization module should be integrated into the system to support the capture of legacy cases and documents, alongside real-time case management. The digitization process must ensure comprehensive, parameterized data capture consistent with the standards used in the new modules. Additionally, the data entry screen should be user-friendly and designed in such a way that users can input all necessary information on a single screen for efficiency and ease of use.

8.13 Requests and response

- All types of official requests and letters related to the investigation process should be managed through this module. Some of these documents can be generated and sent directly through the portal using digital signatures, enabling fast, secure, and paperless communication with other departments, officials, or authorities.

  For requests or letters that require physical signatures, the system should allow users to download the document, get it manually signed, and then upload the signed copy back into the portal for record-keeping and further processing.

  In addition to outgoing letters, reply tapals (incoming official communications or responses to previous requests) should also be handled in the same structured way—either directly through the portal (if received digitally) or scanned and uploaded (if received in physical form).

  Each request or report—whether sent or received—should be properly categorised, time-stamped, and linked to the respective case file, with an option to track its status (e.g., sent, awaiting response, received, replied). This ensures a complete audit trail of communication and improves accountability throughout the investigation process.

- Forwarding Note for Scientific Examination of Records — Sends samples to the forensic lab for examination.
- Site Inspection Report — Findings and observations made during the site visit.
- Notice Submission (Sec. 91 CrPC) / KPF 41(A) — Legal notice to produce documents or for appearance under CrPC.
- Expert Opinion — Opinion from subject-matter experts (technical/forensic/etc.).
- Legal Opinion — Formal advice on legal aspects from VACB Legal Advisor.
- Factual Report — Summarized fact-based report prepared during investigation.
- IO Recommendation — Recommendation by IO regarding prosecution or case closure.
- Forwarding Endorsement by Supervisory Officer — Supervisor's remarks and approvals on investigation progress.
- Scrutiny by Director — Final scrutiny and direction by the Director VACB.
- Prosecution Sanction (19(A)) — Government's sanction to prosecute public servants.
- Court Submission: WPC/Criminal MC/Statement of Facts — Court-bound documents including writs, case facts, etc.
- 17(A) Sanction — Prior approval required to initiate investigation against public officials.
- Summons to Witness — Order to appear in court as witness.
- Summons to Official Witness — Court order to official departments or staff to testify.
- Warrant — Legal document for arrest/search.
- Steps u/s 82, 83 CrPC (Proclamation & Attachment) — Court-ordered steps when accused is absconding.

8.14 Search

This module is designed to digitally manage and document all processes related to the search and seizure operations conducted during the investigation. It ensures that

all legal and procedural requirements are recorded systematically, including the preparation of mahazars, recovery reports, and document seizures.

8.14.1 Search / Search Memorandum

This section captures the details of the search operation, including:

- The place (house, property, office) being searched.
- The legal authority/sections under which the search is being conducted.
- The name of the person searched and/or the owner of the premises.
- Reason or basis for the search (e.g., warrant, suspicion, FIR link).
- Date and time of the search.
- Presence of witnesses and whether the owner or representative was present.
- Signatures of all parties involved including the searching officer and witnesses.

A digital version of the Search List (as in the physical format used today) should be auto-generated and stored, with an option to download, print, or digitally sign.

8.14.2 Inventory / Seizure Mahazar / 3-ാം സ്ഥാനം കൂട്ടിച്ചേർക്കൽ

This records the inventory of items seized during the search operation, also known as Seizure Mahazar. It includes:

- A detailed list of all items seized (articles, valuables, materials).
- Description, quantity, and estimated value.
- Where and how each item was found.
- Names and signatures of witnesses and the responsible officer.
  This document serves as legal evidence and must be signed and time-stamped.

Recovery Report (Items)

This part of the module focuses on the reporting of recovered physical items and includes the following fields:

1. List of items recovered (e.g., money, materials, electronics).

2. When and from whom seized, and from where found – this links the recovery to a person, place, and time.

3. Signature of the officer conducting the recovery, confirming authenticity and accountability.

All entries are to be linked to the case file and timestamped.

Recovery of Documents

This section is dedicated to seizure and documentation of written or digital documents relevant to the investigation. It includes:

1. Date of the document – original date of issuance or creation of the seized document.

2. List of documents recovered – title, type (letter, file, report), issuing authority.

3. Points sought to be – the specific information or evidence being targeted within the document (e.g., financial proof, instructions, correspondence).

4. By whom seized and when – officer name, designation, date/time of seizure.

5. Signature with date and place – confirming authenticity and proper handling.

This ensures a legally valid chain of custody and enables linking documentary evidence to persons and events in the case.

9. Technical Specifications & Requirements

9.1 Core Architecture

- Framework: Modern Frameworks are acceptable.
- Database: MySQL / PostgreSQL with temporal tables for versioning
- Security: FIPS 140-2 compliant encryption

9.2 Integration Requirements

- The system shall support integration with the following **mandatory APIs**: the **Vigilance Court Management System (VCMS)** for case status synchronization, a **Digital Signature Certificate (DSC) provider** for enabling eSign functionality, the **Court Registry System** for document exchange, the **Internal Administrative Processing System (IAPS)** for internal coordination, and access to **DOSSIER details via the DSMS** platform. All data exchanges must adhere to **NIEM 3.0 compliance** standards to ensure interoperability, data integrity, and security across platforms

9.3 Document Management System

A well equipped document management system should be integrated in the system to manage all documents and media files stored in the VCEMS application.

- **Document Capture:**
  Methods for importing, exporting or creating documents, including scanning and importing.
- **Storage:**
  Secure and organized storage of documents, often in a centralized repository.
- **Indexing and Metadata:**
  Assigning keywords, tags, and other metadata to documents for easier search and retrieval.
- **Search Functionality:**
  Robust search capabilities, including full-text search, to quickly locate documents.
- **Version Control:**
  Tracking and managing different versions of documents, allowing users to revert to previous versions if needed.
- **Security:**
  Features like access control, encryption, and audit trails to protect sensitive information

9.4 Compliance Features

- Audit Trail: Immutable blockchain-style logs
- Access Control: ABAC (Attribute-Based Access Control)
- Disaster Recovery: Geo-redundant backups with 15-min RPO

9.5 Additional Requirements

- Mobile Offline Capability: Field data collection sync
- Accessibility: WCAG 2.1 AA compliant UI
- Analytics: Investigation timeline visualization
- Localization: Malayalam Unicode support

9.6. Technical Requirements

- Web-based responsive application using secure MVC architecture.
- Role-based user access with encrypted storage and audit trail.
- Integration APIs for VCMS, IAPS, and DSC providers.
- Search and version control for all forms.
- Export options: Print, PDF, Digital Signature.
- Data backup and disaster recovery mechanisms.

9.6.1 Technical Stack (Preferred)

The proposed solution should be compactable with existing system - VCEMS with following requirements

- Cloud Ready Application
- RESTful API architecture
- Support for microservices (if applicable)
- Scalable Architecture
- Secure authentication (OAuth 2.0/JWT)
- High-performance transaction processing
- Responsive design (mobile/desktop compatible)
- Accessibility compliance (WCAG 2.1)

Database Requirements:

- ACID compliance
- Data encryption at rest for selective data
- Ensure high availability
- Audit logging and temporal tables for versioning
- Scalability for high-volume transactions

Workflow Engine Requirements:

- Visual workflow designer
- Role-based task assignment
- Audit trails for process instances
- Integration with backend APIs

Hosting & Deployment

- Preferred: Kerala State Data Centre (SDC)
- Requirements:
    - 99.9% uptime SLA
    - Multiple environment for development, staging and production
    - CI/CD pipeline for deployment
    - On-premise Source code management
    - Log monitoring system
    - Disaster recovery (geo-redundant backups)
    - Compliance with Kerala Government's IT infrastructure policies

Additional Technical Expectations

- Security:
    - FIPS 140-2 encryption
    - Regular penetration testing
    - GDPR/Data Protection compliance
- Integration:
    - API-first design (OpenAPI/Swagger)
    - Support for SOAP/REST protocols

10. Project Deliverables

- Functional Requirement Document (FRD)
- Software Requirement Specification (SRS)
- Application Design Document
- System Architecture
- Source Code & Deployment Scripts
- Test Cases and UAT Reports
- Training for master trainers
- Training Manuals and User Documentation
- Deployment of application in SDC infrastructure
- Post-deployment support for 1 year

11. Timeline & Milestones

Milestone	**Expected Duration**
Requirement study	45 days
FRD, SRS & Other documentation	30 days
Development & Testing	6 months
UAT & Deployment	1 month

Capacity Building	14 days
Go-Live & Handover	7days

12. Vendor Qualifications & Experience

- Minimum 5 years in developing government/compliance-based web applications.
- Expertise in secure document management & digital signatures.
- Preferable expertise in legal framework.

13. Proposal Submission Guidelines

- Technical Proposal (Approach, Architecture, Compliance)
- Financial Proposal (Cost breakdown, Payment terms)
- Company Profile & Case Studies
- Project Team & Roles

14. Evaluation Criteria

Standard evaluation criteria for IT project as per the startup mission guidelines

15. Terms & Conditions

- All ownership and Intellectual Property (IP) rights will vest with VACB.
- Penalty clauses for delays (1% of project cost per week of delay).
- Warranty & support for 1 year post-deployment.

16. Service Level Agreements (SLAs)

- 99.5% Uptime guarantee.
- 24x7 Support for critical issues.
- Bug Fixing: Critical (24 hrs), Major (72 hrs), Minor (7 days).
- Detailed SLA need to signed at the time of agreement

17. Budget & Payment Terms

- Payment Milestones:
    - 20% on SRS Approval
    - 30% on Module Completion

    - 30% on UAT Sign-off
    - 20% on Go-Live

18. Annexures

- Annexure A: Detailed List of Investigation Artefacts
- Annexure B: Existing System Architecture (VCEMS)

Annexure A

Sl. No.			Form Name / Artefact	Form Code / Reference	Description / Purpose
1			Case registration and Information report to Directorate (circular 12/96)	Crl no 12/96	
	1.1		VC No Generation and Tracking		
	1.2		Sections of Law		
	1.3		Date of Registration		
	1.4		Directorate reference, if applicable		
	15		Name and designation of Accused		
	1.6		In case of public servant designation, department, PEN/ Employee Number and Date of retirement		
2			Hierarchical entrustment Entrustment of Investigation to IO		
	2.2		Change of Investigating Officer		Records reassignment of case to a different IO. Done by SHO/Unit Head

	2.3		Transfer of Investigation Unit		Records transfer of investigation between units or ranges. Done from the Directorate only.
3			General Report to Court		
4			Case Diary		Daily chronological record of investigation maintained by the Investigating Officer.
	4.1		Date of Registration	KPF 24	only one time and could not edit the tab when next GD entry
	4.2		The Officer who registered		only one time and could not edit the tab when next GD entry
	4.3		Name of Accuse		May be more than one accused
	4.4		Property recover		Stolen Property
	4.5		Property recover		Recovered Property
	4.6		CD prior date		Date which previous CD entry
	4.7		Places Visited		Places visited during the investigation
	4.8		Persons questioned		
	4.9		Brief of the case and the details to enter in the CD		From 2.1 to 2.8 should get in the lest side of the page and this should be in the right side with bigger coloumn
5			Mahazar		

	5.1		Entrustment Mahazar		
	5.2		Recovery Mahazar		
6			Arrest		
	5.1		Inspection Memo	KPF 14(B)	Report of inspection of places/persons/items.
		1	District		
		2	Police Station		
		3	Crime Number (if any)		
		4	Section of Law		
		5	Date and Time of Arrest		
		6	Place if Arrest		
		7	Name and Address of arrestee		
		8	Particulars of body search (a) Wearing apparels/ valuables/weapons/other items (b) Injuries if any		
		9	Any request for Medical Examination by Arrestee or Name of the police officer who took initiative to conduct Medical Examination		

		10	Name and Signature/ Thumb impression of the Arrestee		
		11	Signature of SHO		
	6.2		Arrest Memo	KPF 14	Formal document recording the arrest of the accused.
		1	District		
		2	Police Station		
		3	Crime Number(if any)		
		4	Section of Law		
		5	Date of Commission		
		6	Name and Address of the arrestee		
		7	Taken into Custody (a) By whom with designation (b) Date and Time (c) Place		
		8	Name and address of witness (may be more than one)		
		9	Their relation to arrestee		
		10	Information to the relative of Arrestee		
		11	Signature of the Arrestee		Vacant space for signature in the bottom of the page according to the given order.
		12	Signature of witness (may be one or more if more than one then numberings should be there)		

		13	Signature of the police personal		
		14	Place and Date		At the top left of the form
	6.3		PSR (Prisoner Search Register)		
	6.4		Custody Memo		Details of accused persons in police/judicial custody.
		1	Police Station, District, Fir Number		On the top of the form.
		2	Crime number and section of Law		
		3	Name and Address of the person arrested taken to custody		
		4	Date time and place of arrest		
		5	Grounds of arrest, custody		
		6	AADHAR number of the person arrested		
	6.5		Intimation		Intimation to the relatives and make this as record
	6.6		Bail Bond		Bond for temporary release if the accused pending trial
	6.7		Medical report		Medical examination report of the accused of victim
			Arrest Check LIst		
	6.8		Remand report		Request submitted for judicial remand of the accused

	6.9		Letters to the authorities		
7			Witness statement/Witness notice	CrPC 160	Statement given by individuals related to the case
8			Alteration of section		Changing the section(s) of law applied during investigation
9			Alteration of Accused		Addition or removal of accused persons
10	10.1		Search / Search Memorandum		Records the search operation and items searched / seized
	10.2		Inventory / Seizure Mahazar / 3-ാം സാക്ഷി		Documentation of seized property with witness signatures.
	10.3		Recovery Report (Items)	KPF 151(A)	Form used to record specific item recovery during search.
		1	List of items		In the first column include full list of properties downloaded in serial numbers
		2	When and from whom seized and from where found		According to the corresponding serial numbers
		3	Signature of the officer		
	10.4		Recovery of Documents	Form15	(Rule 253, Criminal rules of Practice)List of documents Produced
		1	Date of document		
		2	List of document		

		3	Points sought to be		
		4	By whom seized and when		
		5	Signature with date and place		
11			Forwarding Note for Scientific Examination of records/ Standard requisition form		Sends sample to forensic lab for examination
12			Site Inspection Report		Findings and observations made during the site visit
13			Notice Submission (Sec. 91 CrPC) / KPF 41(A)	KPF 41(A) / CrPC 91	Legal notice to produce documents or for appearance under CrPC.
14			Expert Opinion		Opinion from subject-matter experts (technical/forensic/etc.).
15			Legal Opinion		Formal advice on legal aspects from VACB Legal Advisor.
16			Factual Report/ Investigation report		Summarized fact-based report prepared during investigation.
17			IO Recommendation		Recommendation by IO regarding prosecution or case closure
18			Forwarding Endorsement by Supervisory Officer		Supervisor's remarks and approvals on investigation progress.
19			Scrutiny by Director		Final scrutiny and direction by the Director VACB.
20			Prosecution Sanction	19(A)	Government's sanction to prosecute public servants.

21			Court Submission: WPC/Criminal MC/Statement of Facts		Court-bound documents including writs, case facts, etc.
22			17(A) Sanction		Prior approval required to initiate investigation against public officials
23			Final Report (Charge Sheet/FAD/etc.)		Conclusion of investigation (charge sheet/FID/discharge/mistake of fact).
24			Summons to Witness		Order to appear in court as witness
25			Summons to Official Witness		Court order to official departments or staff to testify.
26			Warrant		Legal document for arrest/search.
27			Steps u/s 82, 83 CrPC (Proclamation & Attachment)	CrPC 82/83	Court-ordered steps when the accused is absconding.
28			Court Case Diary (CD)		Compilation of investigation submitted to the court.
29			Judgment		Final decision pronounced by the court.
30			Further Investigation Order		Issued when more evidence or clarification is required post submission.
31			Appeal Documentation		Records related to appeal proceedings.
32			Convict Warrant		Court order for execution of sentence.