To ensure the integrity of the **Conflict of Interest (COI)** vetting process and the **Project Resource Management System (PRMS)**, the solution will incorporate **mandatory data segregation** and a strict **Role-Based Access Control (RBAC)** model. This approach ensures that multiple auditors can manage distinct services for the same client across overlapping or different timelines while maintaining confidentiality 1-3.

Updated Security and Data Segregation Logic

The system architecture will be configured to enforce the following visibility and access restrictions:

- **Requesters (Auditors/Directors):**
- When initiating a request, the auditor selects a client from a **drop-down list populated by the PRMS Client Master** 4, 5.
- Auditors are restricted to a **"My Requests" view**, where they can only see the files and data they have personally submitted 6, 7.
- Even if a client has **2–3 different auditors** catering to different services, the system ensures that **no auditor can view the submissions, files, or service scopes** of another, unless they are part of the same assigned team 7.
- **Compliance Team (Approvers):**
- The Compliance Department is provided with a **full COI workspace** to review project details, ownership structures, and potential conflicts 6, 7.
- To maintain functional independence, the **Compliance Team sees only project-related details** (description, scope, and conflict justifications) and is strictly **blocked from viewing commercials** or pricing information 7, 8.
- **Finance Team:**
- The Finance Team manages the **engagement code module** and remains responsible for entering financial parameters, assessing credit risk, and automating finance coding 7, 9.
- **Super Admins:**
- A dedicated **Super Admin role** is established with unrestricted access to the entire system, including all historical data, commercial terms, and cross-team submissions 7, 10.
- **Assigned Partners:**
- Partners receive a **one-click dashboard** providing a high-level tracking report of all active and past proposals, COI decisions, and engagement codes relevant to their oversight, ensuring visibility into the **engagement track** 11-13.

Managing Overlapping Services for a Single Client

The system is designed to handle the complexity of a client being served by multiple auditors simultaneously:

1. **Service Distinction:** If multiple proposals are requested for the same client within the same timeline, the **Compliance Department** assesses whether the services are **conflicting or non-conflicting** 10.
2. **Duplicate Detection:** The system performs **Automated Duplication Checks** against the entity, its parents, and its subsidiaries 14, 15. If a conflict is identified between two different auditors' requests, the system **blocks submission** until a justification is provided for compliance review 15, 16.

3. **Audit Trail:** Every action, from initiation to final execution, is recorded in a **centralized audit trail**, ensuring a clear record of which auditor handled which service 17, 18.

Analogy for Data Segregation: The system operates like a **High-Security Professional Services Hub**. Each **Auditor** has a private, key-card-accessed office (their own submissions) and can only see common area directories (client list from PRMS). The **Compliance Team** acts as the safety inspector; they can enter the office to check for safety hazards (conflicts of interest) but are forbidden from looking inside the financial safes (commercials). Only the **Super Admin** holds the master key to every room and every safe in the building.