Q&A for Lawyers & Clients :

For a vendor due diligence meeting, I'd prioritize legal, commercial and operational aspects for a highly confidential data repository – with following k**ey questions**:

1. Commercial model and contract terms.
2. Data hosting location and jurisdiction.
3. Data retention (50-year requirement) and backup.
4. Business Continuity Plan, Disaster Recovery, and SLA uptime.
5. Security (encryption, MFA, access controls, audit logs).
6. Compliance certifications (e.g., ISO 27001, SOC 2).
7. Support model and incident response.
8. Data exit and migration process.

1. Commercials & Contractual Terms

- What is the pricing model for the system?
    - Is pricing based on the number of clients, users, storage capacity, transactions, or another metric?
    - Are there any implementation, onboarding, migration, training, or support fees?
    - Are there additional charges for increased storage, premium support, or future enhancements? Ie when the volume of data increases – how is volume is by client?
- What is the contract term?
    - What are the renewal terms (automatic or manual)?
    - Is there an annual price escalation or CPI adjustment?
    - What are the termination and notice period requirements? JUST /IF there is a requirement – good to understand.
    - Is there an exit plan, including data export and migration support if we decide to move to another platform?

2. Data Hosting & Jurisdiction

- Where is the system hosted (cloud provider and data centre location)?
- Which jurisdictions are used for data storage and backup?
- How are client-specific data residency requirements managed, particularly where regulatory or Chinese Wall restrictions apply? Ie we have Local and Foreign clients with assets in different jurisdiction – is there a cross border data record being flagged up – esp India Resident with assets recorded in Pakistan..

3. Data Storage, Retention & Backup

- What is the data retention policy?
- Can retention periods be customised? Our business requires data to be retained for **at least 50 years**.
- How frequently are backups performed?
- Are backups encrypted?
- Where are backup copies stored?
- Is there a secondary backup location?
- Can deleted data be recovered, and if so, within what timeframe?

4. Business Continuity & Disaster Recovery

- Is there a documented Business Continuity Plan (BCP) and Disaster Recovery (DR) plan?
- What are the Recovery Time Objective (RTO)?
- What is the maximum accepted downtime under the SLA?
- How frequently are BCP and disaster recovery tests conducted?
- Is there automatic failover to a secondary environment in the event of an outage?

5. IT Support & Service Levels

- What are the support hours?
- Is support provided during Asia business hours only, or is 24×7 support available?
- Where is the support team located?
- What are the response and resolution times for:
    - Critical (Priority 1)
    - High
    - Medium
    - Low priority incidents?
- What is the escalation process for critical incidents? IE missing fields, system loading delays – reworks,
- Is a dedicated account manager or technical support contact assigned?

6. Security & Access Controls (Highly Recommended)

- Is Multi-Factor Authentication (MFA) supported and mandatory?
- Is all data encrypted both at rest and in transit?
- Who has administrator access to the system?
- Can administrators access client data?
- Are all user and administrator activities fully audited?
- Can access be restricted by user role and business function?

7. Compliance & Governance (Highly Recommended)

- Does the platform comply with relevant standards such as ISO 27001 or SOC 2?
- Has the platform undergone recent penetration testing?
- How are security vulnerabilities managed and remediated?
- What is the incident notification process in the event of a security breach?
- Can audit logs be exported for compliance purposes?

8. Data Exit Strategy

- If the contract ends, how can all data be exported?
- In what format will the data be provided?
- Are there any fees for data extraction?
- How long is customer data retained after contract termination before permanent deletion?