Detailed Mini Case Study: Digital Service Portal Audit Failure (Bangladesh Context)

1. Background of the Project

As part of the Digital Bangladesh / Smart Bangladesh initiative, a government department launched an online citizen service portal to issue certificates and manage benefit-related applications. The system aimed to reduce physical visits, improve transparency, and speed up service delivery.

The portal was developed by a private IT vendor, hosted in a government-approved data center, and used nationwide. It collected sensitive citizen information such as National ID numbers, phone numbers, addresses, and service history.

2. Governance and Management Structure

The line ministry acted as the system owner, while operational responsibility rested with the department ICT cell. Technical maintenance was outsourced to a vendor. However, no data protection focal person was formally assigned, and cyber risk was treated as an IT issue rather than a management responsibility.

3. The Incident

After several months, media reports revealed that citizen data from the portal was publicly accessible through shared links and search results. The department denied responsibility, while the vendor blamed weak password practices by staff. No formal incident report or immediate containment action was taken.

4. Audit Trigger

Following media attention and public concern, senior authorities instructed an internal audit focusing on governance, controls, and accountability rather than technical hacking.

5. Audit Scope

The audit reviewed data protection practices, access control, vendor management, incident handling, and policy compliance. No system penetration testing was conducted.

6. Key Audit Findings

• No formal data classification or retention policy • Excessive and shared user access • Long-term vendor access without review • Weak contracts lacking security and breach clauses • No documented incident response procedure • Absence of prior cyber audits

7. Root Cause Analysis

The audit concluded that the incident resulted from governance and management failures rather than advanced cyber attacks.

8. Impact Assessment

Operational disruption, reputational damage, potential legal exposure, and reduced public trust in digital services were identified as major impacts.

9. Audit Recommendations

Immediate access review, assignment of a data protection focal person, contract revision, staff awareness training, and mandatory periodic cyber audits were recommended.

10. Key Lessons for Senior Officials

Outsourcing does not remove accountability. Cyber auditing is a leadership responsibility, and simple governance controls can prevent major incidents.

11. Discussion Questions

Who was accountable? What questions should senior management have asked? Which control should be prioritized first? How could this incident have been prevented without technical tools?