Risk Identification Exercise: Database Systems

Company Name: *Infotech Dynamics Ltd.*
Industry: Software Development and IT Services
Location: United Kingdom

---

1. Vulnerability: Weak Authentication Mechanisms

Description:
Database systems use only basic username/password authentication without multi-factor authentication (MFA). Password policies are not strictly enforced, and user credentials are not rotated regularly.

Business Impact:

- Unauthorised access to sensitive customer and proprietary data.
- Breach of data protection regulations (e.g., UK GDPR), leading to regulatory fines.
- Reputational damage resulting in client loss and decreased trust.

Severity: **High**
Likelihood: **Medium to High**

Countermeasures:

- **Implement Multi-Factor Authentication (MFA)** for all database access points.
- **Enforce strong password policies**, including minimum length, complexity, and expiration rules.
- **Integrate identity and access management (IAM)** tools for consistent enforcement.

Implementation Timeline:

- 0–3 months (short term)

Resource Requirements:

- £8,000–£12,000 for IAM/MFA solutions (e.g., Azure AD, Okta)
- IT security personnel for configuration and training
- Minimal downtime for deployment

---

2. Vulnerability: Unsecured Internal Network Access

Description:
Internal databases are accessible over the company's intranet without proper segmentation or encryption. There is no use of Virtual Private Networks (VPNs) or network-level firewalls between departments.

Business Impact:

- Increased exposure to insider threats and lateral movement in the event of a breach.
- Possibility of unauthorised data access from compromised internal devices.
- Loss of confidential R&D or financial data affecting competitive advantage.

Severity: **Medium to High**
Likelihood: **Medium**

Countermeasures:

- **Implement network segmentation** to isolate database servers from general access.
- **Use VPNs and encrypted communication protocols** (e.g., TLS) for all database traffic.
- **Deploy internal firewalls and intrusion detection systems (IDS)**.

Implementation Timeline:

- 3–6 months (medium term)

Resource Requirements:

- £15,000–£25,000 for network upgrades, firewall licences, and IDS tools
- Network engineers and security consultants
- Scheduled downtime for reconfiguration and testing

---

3. Vulnerability: Poor Data Handling and Logging Procedures

Description:
Data queries and transactions are not logged effectively. Sensitive information is stored in plain text, and no routine audits are conducted. There is also no data classification strategy in place.

Business Impact:

- Inability to detect suspicious activity or trace data leaks.
- Breach of compliance obligations (e.g., ISO 27001, UK GDPR).
- Risk of data corruption or manipulation without traceability.

Severity: **Medium**
Likelihood: **High**

Countermeasures:

- **Implement role-based access control (RBAC)** and **audit logging** for all database transactions.
- **Encrypt sensitive data at rest and in transit** using industry-standard algorithms.
- **Introduce data classification and handling policies**, including regular audits.

Implementation Timeline:

- 6–9 months (long term)

Resource Requirements:

- £10,000–£18,000 for encryption tools, audit systems, and training
- Policy development and compliance team involvement
- Ongoing operational support for audits and reviews

Risk Ranking Summary

Risk	Severity	Likelihood	Overall Priority
Weak Authentication Mechanisms	High	Medium-High	**1 (Highest)**
Unsecured Internal Network Access	Medium-High	Medium	**2**
Poor Data Handling and Logging	Medium	High	**3**
