**Data Risk Identification**

**Data risks** refer to any potential threat or issue that may affect the quality, security, availability, integrity, compliance, or value of data. These risks can impact business operations, regulatory compliance, decision-making, and reputation.

**1. Security Risk**

**Definition**: Unauthorized access, theft, tampering, or loss of data.

**Scenario**: A hacker breaches a system and downloads sensitive customer records.

**Use Case**: A retail company must implement role-based access control and encryption to prevent unauthorized access to customer data.

**2. Privacy Risk**

**Definition**: Exposure or misuse of personal or sensitive data in violation of data protection laws (e.g., GDPR, CCPA).

**Scenario**: A healthcare provider shares patient information with a third party without proper consent.

**Use Case**: A hospital establishes a consent management platform and logs data sharing activities to ensure compliance with privacy regulations.

**3. Quality Risk**

**Definition**: Poor data quality that affects decision-making and operations.

**Scenario**: Duplicate customer records lead to multiple marketing emails sent to the same person.

**Use Case**: A marketing department implements data profiling and cleansing tools to remove duplicates and standardize contact data.

**4. Availability Risk**

**Definition**: Data is not available when needed due to system outages, delays, or lack of access.

**Scenario**: An outage in the sales data warehouse prevents real-time reporting for executives.

**Use Case**: The IT department implements high-availability architecture and regular backups to ensure 24/7 data access.

**5. Integrity Risk**

**Definition**: Data is incorrectly entered, processed, or altered, leading to incorrect results.

**Scenario**: Financial figures are accidentally overwritten due to poor version control.

**Use Case**: A finance team implements a workflow for data entry and approval, and enforces audit logs for changes.

**6. Compliance Risk**

**Definition**: Non-compliance with laws, regulations, or internal policies related to data management.

**Scenario**: A company fails to retain transaction data for the required 7-year period under financial regulations.

**Use Case**: The legal team implements a data retention schedule and automated archival tools based on regulatory needs.

**7. Operational Risk**

**Definition**: Risks that arise from failures in internal processes, people, or systems.

**Scenario**: An employee uploads incorrect product prices to the website, affecting sales and customer trust.

**Use Case**: A retail company integrates data validation rules and approval workflows into their product information system.

**8. Strategic Risk**

**Definition**: Data is not aligned with business strategy, leading to poor investment or misinformed decisions.

**Scenario**: Executives make product development decisions based on outdated customer insights.

**Use Case**: The business intelligence team sets up real-time dashboards that reflect up-to-date customer behavior trends.

**9. Ethical Risk**

**Definition**: Use of data in ways that are unethical, even if legal.

**Scenario**: An AI model uses biased historical hiring data, leading to discrimination.

**Use Case**: A company reviews training datasets for bias and applies fairness metrics in their algorithms.

**Summary Table**

| **Risk Type** | **Description** | **Scenario Example** | **Control/Response** |
| --- | --- | --- | --- |
| Security | Unauthorized access or theft | Hacker steals customer data | Encryption, access control |
| Privacy | Misuse of personal data | Data shared without consent | Consent management, masking |
| Quality | Inaccurate or duplicate data | Duplicate customer records | Data cleansing, validation rules |
| Availability | Data not accessible when needed | System outage halts reporting | Backup, high availability systems |
| Integrity | Data tampering or errors | Financial data overwritten | Audit logs, version control |
| Compliance | Breach of legal requirements | Missing records for audits | Retention policies, compliance audits |
| Operational | Internal process failures | Incorrect product data uploaded | Workflow automation, training |
| Strategic | Misaligned or outdated data use | Wrong market decisions based on old data | Real-time analytics, governance |
| Ethical | Unethical use of data | AI discrimination in hiring | Fairness reviews, ethical oversight |