**Data Risk & Security Management**

Here's a comprehensive overview of **Data Risk & Security Management** based on **DAMA DMBOK v2**, focusing on the **identification of threats** and the **adoption of defenses**—especially concerning the **protection of personal and sensitive data**.

**Objective:**

To **protect data assets** from threats (internal and external) through the implementation of **security policies, processes, and technologies**, while ensuring **compliance with laws and regulations** (e.g., GDPR, HIPAA, etc.).

**Key Concepts**

**1. Data Risk**

Data risk refers to the **potential for loss, corruption, exposure, or misuse** of data that can harm an organization or individuals.

**Sources of Data Risk:**

* **Human error** (e.g., accidental deletion)
* **Malicious insiders**
* **Cyberattacks** (e.g., ransomware, phishing)
* **Physical threats** (e.g., theft, fire)
* **Non-compliance** with regulations

**2. Types of Threats**

| **Threat Type** | **Example** |
| --- | --- |
| **Unauthorized Access** | Hacker accesses sensitive customer data |
| **Data Leakage** | Employee emails unencrypted file with PII externally |
| **Loss of Data** | System crash results in unrecoverable sales records |
| **Data Tampering** | Internal actor alters financial results |
| **Denial of Service** | Attack disables access to key data systems |

**3. Security Controls & Defenses**

**a. Technical Controls**

* **Access Control**: Role-based access, identity management, least privilege
* **Encryption**: Data-at-rest and data-in-transit encryption
* **Audit Trails**: Monitoring changes and access to sensitive data
* **Data Masking/Anonymization**: Protects personal data during testing or analysis
* **Firewalls & Intrusion Detection Systems**

**b. Organizational Controls**

* **Data classification policy** (e.g., Public, Internal, Confidential)
* **Data retention policy** and secure disposal
* **Incident response planning**
* **Third-party data sharing agreements**

**c. Governance Controls**

* **Security ownership roles** (e.g., Data Security Officer)
* **Security risk assessments**
* **Regulatory compliance** frameworks (GDPR, HIPAA, etc.)
* **Periodic audits and reviews**

**4. Focus on Personal Data Protection**

Especially under laws like **GDPR**, **CCPA**, and others:

| **Requirement** | **Description** |
| --- | --- |
| **Data Minimization** | Only collect what is strictly necessary |
| **Consent Management** | Ensure users give informed consent for personal data use |
| **Right to Access/Deletion** | Allow users to view or delete their data on request |
| **Breach Notification** | Mandatory reporting of data breaches |
| **Privacy by Design** | Integrate privacy features in system development |

**Example Scenario: E-Commerce Platform**

**Threat:**

A customer support agent accesses and copies customer credit card data for fraudulent use.

**Risk:**

* Violation of PCI-DSS compliance
* Legal penalties under GDPR
* Loss of customer trust

**Controls:**

* Mask credit card number display (only show last 4 digits)
* Restrict access by role (support cannot see full payment info)
* Encrypt payment details in database
* Log all access to sensitive customer data

**Integration with Data Governance**

Data Risk & Security is a **core function** of data governance. It must integrate with:

* **Metadata management** (e.g., tagging sensitive data)
* **Data quality** (e.g., ensure secure, valid data)
* **Lifecycle management** (e.g., retention and secure disposal)

**Summary**

| **Area** | **Description** |
| --- | --- |
| **Risk Identification** | Understand vulnerabilities and potential attack vectors |
| **Threat Management** | Prevent data misuse, theft, or loss |
| **Defenses** | Technical, organizational, and governance-based controls |
| **Privacy Compliance** | Adhere to legal regulations to protect personal and sensitive data |
| **Ongoing Monitoring** | Use audits, logs, and analytics to detect and respond to incidents |