* 1. **Differences between data lifecycle and a Systems Development Lifecycle (SDLC)- As Described in DAMA-DMBOK**

Here is a **detailed comparison** of the **Data Lifecycle** and the **Systems Development Lifecycle (SDLC)** based on **DAMA-DMBOK V2**, including **realistic use cases and scenarios** to illustrate the differences and how they interrelate in practice:

**1. Purpose and Definition**

* **Data Lifecycle**: Describes how data is handled from creation to disposal. It ensures that data is accurate, secure, and used appropriately throughout its life.
* **SDLC**: Describes the process of designing, building, testing, deploying, and maintaining software systems that support business processes.

**Use Case**:

A healthcare organization builds a patient management system.

* **SDLC** covers the design and development of the application.
* **Data Lifecycle** manages patient data inside that system: from data entry at registration to archival after patient discharge and eventual deletion.

**2. Scope**

* **Data Lifecycle**: Cross-functional and system-agnostic. Applies to all organizational data, regardless of the application or technology.
* **SDLC**: Project-specific and time-bound. Applies only to a given system being developed or maintained.

**Scenario**:  
A retailer uses multiple systems (e.g., inventory, customer loyalty, POS).

* Each system has its own SDLC.
* The **data lifecycle** ensures that customer data (which may span all systems) is consistently validated, governed, and archived across them.

**3. Key Stages**

**Data Lifecycle Stages (DAMA-DMBOK V2):**

1. Create or Capture
2. Store and Maintain
3. Use
4. Share or Distribute
5. Archive
6. Dispose or Destroy

**SDLC Typical Stages:**

1. Requirements Gathering
2. System Design
3. Development
4. Testing
5. Deployment
6. Maintenance

**Scenario**:  
A bank creates a loan application system.

* During **SDLC**, the IT team gathers requirements, builds interfaces, and tests workflows.
* In **data lifecycle**, they define how applicant data is collected (step 1), validated, stored securely (step 2), used for credit decisions (step 3), shared with third-party verification agencies (step 4), archived after 7 years (step 5), and securely deleted (step 6).

**4. Focus and Outcomes**

* **Data Lifecycle**: Ensures data is of high quality, used ethically, retained appropriately, and deleted securely.
* **SDLC**: Ensures the system is functional, meets user needs, is delivered on time, and performs well.

**Scenario**:  
In an insurance claims portal:

* SDLC focuses on delivering the system with workflows for submitting and reviewing claims.
* The data lifecycle ensures the submitted claim data is validated, protected, used only for its intended purpose, and retained in compliance with legal requirements.

**5. Stakeholders Involved**

* **Data Lifecycle**: Data owners, stewards, governance teams, compliance officers, business analysts.
* **SDLC**: Project managers, system analysts, developers, testers, users.

**Scenario**:  
In an HR onboarding system:

* **SDLC** involves IT staff building the workflows.
* **Data lifecycle** involves HR compliance staff ensuring sensitive employee data (e.g., tax ID, personal contact info) is collected lawfully, stored securely, and eventually deleted according to retention schedules.

**6. Time Horizon**

* **Data Lifecycle**: Ongoing, as long as the data exists. Can span decades depending on legal and business requirements.
* **SDLC**: Has a start and end date for each project phase, although systems may go through multiple cycles over time.

**Scenario**:  
A university stores student records:

* The **SDLC** might run for one year to launch the system.
* The **data lifecycle** of student records spans enrollment to graduation, alumni engagement, and eventual deletion — potentially over 10–20 years.

**7. Compliance and Risk**

* **Data Lifecycle**: Directly tied to compliance regulations like GDPR, HIPAA, and retention policies. Failure impacts legal standing and customer trust.
* **SDLC**: Can indirectly impact compliance by how systems are built (e.g., ensuring access controls are implemented).

**Scenario**:  
A fintech app collects user data for digital wallets.

* If the SDLC skips implementing encryption, the data lifecycle is compromised.
* If the data lifecycle lacks policies for disposal, user data may be retained longer than allowed, violating GDPR.

**Summary Table**

| **Aspect** | **Data Lifecycle** | **Systems Development Lifecycle (SDLC)** |
| --- | --- | --- |
| Focus | Managing data over time | Building and evolving systems |
| Scope | Organization-wide | Project/system-specific |
| Key Phases | Create, Store, Use, Share, Archive, Dispose | Requirements, Design, Build, Test, Deploy |
| Timeframe | Ongoing | Temporary (per project/system) |
| Compliance Risk | High – tied to privacy & retention laws | Moderate – linked to how features are implemented |
| Stakeholders | Data stewards, owners, compliance teams | Developers, analysts, project managers |