Data Lifecycle Management (DLM) is a comprehensive and overarching approach which governs the way data is created, used, stored, retained and securely destroyed throughout its entire lifecycle, outlining that data is separated into phases based on specific criteria, moving through the stages as tasks are completed or certain requirements are met (IBM, n.d.). Effective DLM involves the creation of documented policies and procedures in order to ensure data security, regulatory compliance, operational efficiency, and risk mitigation is enforced at every stage of the data's lifecycle, which makes DLM a crucial aspect for organizations to incorporate in order to protect assets and support ongoing business continuity.

Importance of Data Life Cycle Plans for an Organization:

DLM is vital for organizations, such as Green Thumb Nursery, because there are a wide range of data types, from various sources, and they all must be kept secure, compliant and available through their entire lifecycle. This approach aligns with operational needs, upholds compliance requirements, provides structure to an organization's data and supports data security and data availability which reinforces the 3 tenets of the CIA Triad; Confidentiality, Integrity, and Availability of data.

Implementing DLM can ensure that the correct data is in the right place, at the right time, which allows capitalizing on data insights and the creation of new opportunities for organizations who can leverage data science to obtain a holistic view of data, as DLM makes it possible to monitor data use across all of the various stages and detect any data misuse or breaches (Kamaly, T., 2022). In the example of Green Thumb Nursery, managing data related to business operations, agricultural data, records of employees and customers, environmental sensor readings, surveillance footage and more, it's critical that DLM be incorporated in order to protect data and have a thorough understanding of the relevant stages data goes through in its lifecycle.

Generally speaking, DLM will:

- Aid in the preservation of the Confidentiality, Integrity, and Availability (CIA Triad) of all data, with safeguards in place to protect data at every stage through its lifecycle.
- Assist compliance with relevant regulations and laws, such as OSHA reporting, data privacy and security compliance, as well as Department of Agriculture expectations.
- Require the use of specific encryption protocols in order to protect the CIA Triad of all data, which can take the form of utilizing AES-256 encryption for data-at-rest and enforcing TLS 1.2 or higher for data-in-transit. Encryption is a cornerstone of data protection and organizations have a duty to make efforts to protect data security.
- Incorporate the use of access controls, including but not limited to the Principle of Least Privilege (PoLP) and Role-Based Access Control (RBAC), to mitigate the impacts of any Insider Threats as well as account/credential compromise and abuse of permissions to threaten the privacy and security of data.
- Provide guidance on clearly defined retention and disposal schedules, with secure and verifiable destruction methods used such as DoD compliant overwriting and physical destruction. Organizations must ensure that the appropriate destruction method is applied to data, based on its sensitivity tier in order to remain cost-effective while maintaining security.

Impact of Lacking a Data Life Cycle Plan:

Without formal DLM in place, organizations face the risk of significant operational, reputational, and financial harm because unmanaged data can lead to inefficiencies, security vulnerabilities and compliance or regulatory failures. Effective DLM should be paired with formal Risk Management Strategies to achieve proactive identification, assessment, and mitigation of risks that are associated with data, at every stage of its lifecycle and integrating a centralized Risk Management Strategy will uphold operational effectiveness and business continuity, provide protection of company assets, and maintain brand integrity and customer satisfaction (Vicente, V., 2024).

Lacking the implementation of DLM can result in:

- Increased risk of data breaches, unauthorized access and other security vulnerabilities as a result of ineffective/inadequate encryption, poor data monitoring practices, and weak access controls in place.
- Operational disruptions due to data loss, corrupt backups or archive data, potentially inaccessible systems (causing poor Availability), all of which will negatively impact revenue and business continuity.
- Inefficient budget allocation and wasting both money and resources, due to over-retention of unnecessary data, as well as accruing costs related to storing data in an incorrect storage type due to a poor understanding of data lifecycle stages.
- Increased exposure to Insider Threats and human error as a result of weak, or non-existent, access controls causing the organization to face reputational damage in the event of data mishandling or a publicized data breach post-disclosure which can cause loss of consumer trust and reduced revenue, leading to business sustainability issues.

Value of Data Life Cycle Plan Maintenance:

Maintaining comprehensive DLM offers organizations a strategic and operational advantage by providing ongoing visibility and control over data, which enables them to improve processes, optimize data security, compliance, and costs while improving risk response efforts (IBM, n.d.).

Continual maintenance of this plan provides:

- Improved and proactive risk mitigation capabilities, allowing adaptation to new threats, such as ransomware or supply chain vulnerabilities more effectively.
- Assurances of business continuity and improved disaster recovery through defining retention, archive, and restoration priorities of data, as a result of a clear understanding of data lifecycle stages.
- A clear audit trail and documentation regarding destruction processes in order to provide evidence of regulatory compliance and appropriate data governance, to support any required legal defense.
- Enhanced data quality, which improves data-driven decision-making capabilities that are supported by reliable and trustworthy information.
- The ability to 'right-size' storage infrastructure by understanding data lifecycle stages, which balances performance, security and costs in order to maintain security without unnecessary expenditure.

Overall, Data Lifecycle Management positions organizations to protect their data assets effectively, assists achievement of business goals, upholds regulatory compliance requirements, builds resilience against evolving risks and mitigates risks to ongoing business continuity. Particularly when combined with Risk Management Strategies, the result is proactive identification and responses to data-related risks, which ensures sustained operational stability and long-term continuity and success.

References

IBM, (n.d.). *What is data lifecycle management (DLM)?* IBM.

Retrieved on December 08, 2025 from:

https://www.ibm.com/think/topics/data-lifecycle-management

Kamaly, T., (2022). *The Importance of Data Lifecycle Management (DLM) and Best Practices.*

IEEE Computer Society.

Retrieved on December 08, 2025 from:

https://www.computer.org/publications/tech-news/trends/the-importance-of-data-lifecycle-management

Vicente, V., (2024). *10 Types of Risk Management Strategies to Follow.* AuditBoard.

Retrieved on December 08, 2025 from:

https://auditboard.com/blog/10-risk-management-strategies