BANKING INFORMATION LIFECYCLE

The information lifecycle for banks involves various stages through which data and information pass, from creation or acquisition to disposal or archival.

1 CREATION/ACQUISITION

- Information is generated through various channels such as customer transactions, loan applications, account openings, and internal operations.
- Data can be acquired from sources like online applications, in-person interactions, electronic transactions, and third-party providers.

2 STORAGE

- Once acquired, the information is stored in databases, servers, or other secure storage systems.
- Data storage practices in Financial Services organizations often involves adherence to regulatory requirements such as the Gramm-Leach-Bliley Act (GLBA) and other federal or regional data protection laws.

3 ACCESS & USAGE

- Authorized personnel access the stored information to perform tasks such as processing transactions, analyzing customer behavior, assessing loan applications, and managing accounts.
- Access controls and authentication mechanisms are implemented to ensure that only authorized individuals can access sensitive data.

4 TRANSMISSION/SHARING

- Information transmitted between internal departments, branches, or external partners for various purposes such as processing transactions, verifying identities, or complying with regulatory reporting requirements.
- Secure communication channels and encryption methods are employed to protect data during transmission.

5 RETENTION & ARCHIVAL

- Financial Institutions are required to retain certain types of information for specific periods to comply with regulatory requirements or legal obligations.
- Archived data may be stored in secure offline or cloud-based storage systems to ensure long-term preservation and accessibility.

6 MAINTENANCE & UPDATES

- Regular maintenance activities, including data backups, software updates, and security patches, are conducted to ensure the integrity, availability, and confidentiality of information.
- Systems and procedures are periodically reviewed and updated to adapt to changes in technology, regulations, and business needs.

7 DISPOSAL

- When information is no longer needed for operational, legal, or regulatory purposes, it is securely disposed of to prevent unauthorized access or misuse.
- Disposal methods may include shredding physical documents, degaussing or securely erasing digital media, and implementing data destruction protocols.

8 MONITORING & COMPLIANCE

- Regular maintenance activities, including data backups, software updates, and security patches are conducted to ensure the integrity, availability, and confidentiality of information.
- Systems and procedures are periodically reviewed and updated to adapt to changes in technology, regulations, and business needs.