Response to the Network Computing Survey

HDS views information and data life cycle management as two different functions that are complementary.

Information Lifecycle Management (ILM) – The function(s) necessary to manage information through the workflow or business process from creation of an information object to its completed state. This can be described in the context of a contract process or purchase order process where a document must proceed through a set of defined review/approval gates. The final gate in the process is a final and approved document. ILM typically exists at the application layer and is most often associated with document/content management and collaboration software, e.g. Documentum, FileNET, Open Text, etc.

Data Lifecycle Management (DLCM) – The function(s) necessary to manage a data object or collection of objects within the storage environment based on the prescribed value or access requirements associated with the life cycle of the data object. Data that has value, needs to be retained in a secure, recoverable (backup), monitored storage environment. The criticality of the data determines the type of storage environment required. As the activity against a valued data object decreases, it may be moved to lower cost, secondary or tertiary levels of storage, to optimize the cost of storing that data object, and to improve the efficiency of the primary storage. As storage leases expire, technology refreshes occur, ownership changes, and business processes are replaced, new storage needs to be acquired and provisioned for migration or replication of the valued data. DLCM management also means deleting data that has no value and destroying data that can pose a liability. DLCM is a function of the storage management layer that must provide open interfaces to higher-level applications for integration with ILM software services.
It is important to note that ILM and DLCM are complementary and integration is necessary for customers to more intelligently manage the information ecosystem. DLCM is a core component and represents the foundation for developing fully integrated solutions.

Usage Scenarios

In addition to Capacity Utilization Efficiency, Capacity Allocation Efficiency, DR and Business Continuity, HDS things that Operational Efficiency and Operational Risk Preparedness should also be considered when evaluating the effectiveness of ILM and DLM solutions.

Operational Efficiency. DLM solutions, often in conjunction with ILM solutions, can increase operational efficiency. This can result in the increase or elimination of quota restraints, reduce or eliminate backup and recovery times, improve data access by eliminating scans and flat file searches, offload processor cycles with off host movement of data, reduce software licenses through consolidation of server based licenses to storage based licenses, and consolidation of management interfaces across a multi-tier pool of storage.

Operational Risk Preparedness. DLM solutions can increase operational risk preparedness. A centrally managed DLM solution will provide an organized storage environment, in which the value of data is assessed and assigned to the appropriate level of protection, where Recovery Point and Recovery Time Objectives are defined. DLM deploys the appropriate level of authorization, authentication, integrity, immutability, and confidentiality to address operational threats like theft, fraud, processing errors, maintenance errors, hardware/software errors or failures, disasters, liability exposures, and invasion of privacy. Logging, monitoring, and reporting provide validation and forensics when data is exposed, corrupted, or deleted. These functions result in lower insurance rates, lower capital reserves, improved corporate governance, and improved trust.

Questions

Comment: We will be answering these questions from the context of our DLM solution. Some of these questions like "Data Naming Scheme" are more relevant to ILM than DLM, in which case we will say it does not apply, N/A. Other questions imply a single solution. There is no single solution that can address all the different types of data, such as structured, Semi Structured, and Unstructured. Even for a single data type, there may be may different ILM solutions that can be ported to our DLM solution.

Development Status
HDS has made its Open LDEV Guard feature available for the 9900V platform and is completing development of the feature for its 9500V platform. This feature provides the ability to create WORM volumes on disk to meet regulatory compliance requirements as specified in SEC 17a4.

Through its partnership with IXOS (detailed below), HDS introduced two message archiving products as part of its DLM development programs - these are the Message Archive for Email and the Message Archive for Compliance. Both products are currently available.

Future development will focus on optimizing the storage and management of other unstructured data types – from check images to PDF files to Microsoft Office documents, HDS will continue development efforts to offer the broadest support for its customers.

Development Partners
Today HDS is partnered with IXOS Software AG, which provides capabilities for archiving various data types. In keeping with HDS' stated policy for an open platform other ISVs will also be engaged to integrate with its Open LDEV Guard Data Retention Manager.

Data Naming Scheme
N/A

Access Frequency
N/A

Storage Platform Characterization
N/A

End of Useful Life
The LDEV Guard solution supports a user-definable retention period. It can be paused during a discovery action. After the retention period expires, the data may be shredded using third party software or maintained in a non-locking archive depending on customer need. If the data is destroyed following the mandated retention period, or moved to another device for replication or migration, the storage capacity it occupied can be recovered for new use.

Policy Articulation
N/A

Device support
Hitachi Data Systems 9900V and 9500V storage arrays

Resource Consumption
As far as storage consumption goes, HDS' DLM solutions can share the same multi-tier storage pool as other applications. It does not require a dedicated, or niche device. Excess capacity can be utilized by other applications.

Flexibility
HDS' DLM offering is designed to utilize a standard storage environment and does not require single-purpose archive storage devices. This allows data to easily be migrated from one storage platform to another under unified management. It also leverages common storage based functionality such as TrueCopy, for remote replication, which is another requirement for regulations such as SEC 17a-4.

The Open LDEV Guard feature is implemented in microcode on the controller itself. In addition to providing a WORM lock for disk media it also maintains the retention period such that the lock cannot be disabled until that period expired. This provides additional security in addition to a period set at the application layer to ensure that the lock cannot be disabled by a simple software command. The lock remains in place on the storage device itself. The lock function also remains with the protected data even if that data migrates to other storage platforms.

Speeds and Feeds.
The speeds and feeds are the same as the rest of the storage pool. It is Fibre Channel attached and is not limited by IP speeds or overheads.

Interconnect Support.
LDEV Guard storage arrays are Fibre Channel attached. This is currently 2MB/s Fibre Channel on both the 9900V and 9500V.

Protocol Support.
FCP. iSCSI and IFCP through gateway products, NFS and CIFS through a NAS gateway and an Embedded NAS blade (available in Japan)

Data Type Support.
The data types and granularity supported depend on the ILM application that front ends our storage. HDS' current solution offering supports data types found in traditional file systems, SAP, Siebel, content from Microsoft SharePoint as well as integration capabilities with other 3rd party software and homegrown applications**.**

Cost:
Not Available

Standards:
Open Archival information System Reference Model – A Common Foundation (ISO 14721)

CIM SMI-S for management