Abstract

This technical report is an assessment of the EMC Data Domain Retention Lock Compliance edition capabilities relative to selected requirement areas of ISO 15489, Part 1:2001(E) International Standard ("ISO 15489-1") and ISO/TR 15489 Technical Report Part 2 Guidelines ("ISO/TR 15489-2") that can be met or supported by advanced electronic storage systems.

Cohasset’s conclusion is that the DD Retention Lock Compliance edition, when installed, configured, and enabled on the EMC Data Domain system, supports meeting ISO 15489-1 and ISO/TR 15489-2 requirements in the areas of: authoritative and authentic records, retention and disposition and storage and handling.

The capabilities that support meeting these requirements are: a) establishing a records storage environment that supports the storage and handling of authoritative records through the use of integrated control codes that prevent alteration or destruction of electronically stored records for the required retention period, b) setting a “read-only” status for and assigning a retention period to each record, c) assigning a unique identifier and date/time stamp that makes the records accessible, and d) creating a duplicate or backup copy of all records – with the associated retention period and protection controls – for the purpose of disaster recovery.
# Table of Contents

1. Introduction ........................................................................................................................................................ 3  
   1.1 ISO 15489 ............................................................................................................................................................ 3  
   1.2 EMC Data Domain Retention Lock Compliance Edition Overview ...................................................... 5  
   1.3 Assessment and Technical Report............................................................................................................ 5  
2. ISO 15489-1 Compliance Assessment ............................................................................................................. 7  
   2.1 Storage-related ISO 15489 Requirements ............................................................................................... 7  
   2.2 Authoritative Records ...................................................................................................................................... 8  
   2.3 Retention and Disposition .......................................................................................................................... 10  
   2.4 Storage and Handling................................................................................................................................. 11  
3. Conclusions ....................................................................................................................................................... 13  
4. Matrix of DD Retention Lock Compliance Edition Capabilities ................................................................. 14  
   4.1 Establishing an Authoritative DD Retention Lock Compliance and Data Domain Storage System .................................................................................................................. 15  
   4.2 Retention Management .............................................................................................................................. 16  
   4.3 Accuracy and Quality of Stored Records ................................................................................................. 16  
   4.4 Administrative Security ............................................................................................................................. 17  
   4.5 Backup and Recovery................................................................................................................................. 19  
End Notes ............................................................................................................................................................. 20  
About Cohasset Associates, Inc. ........................................................................................................................ 21
1. Introduction

This section sets the context for this technical assessment. It provides an introduction to ISO 15489 Parts 1 and 2 and sets the foundation for identifying certain areas of requirements for electronic record systems that can be met or supported by advanced electronic storage systems. It then provides an overview of the storage system that is the subject of Cohasset's assessment.

1.1 ISO 15489

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. ISO 15489 was prepared by Technical Committee ISO/TC 46, Information and documentation, Subcommittee SC 11, Archives/Records Management.

ISO 15489 Part 1: General Information and documentation – Record Management was published in September 2001. It was developed in response to a consensus among participating ISO member countries to standardize international best practices in records management using the Australian Standards AS 4390, Records management, as its starting point.

The ISO 15489 Part 1 (“ISO 15489-1”) International Standard is accompanied by a Technical Report, ISO/TR 15489 Part 2 Guidelines (“ISO/TR 15489-2”), also published in September 2001. The standard and guidelines are recommended for combined use. The purpose of ISO/TR 15489-2, is explained in Section 1, Scope:

It gives an overview of the processes and factors to consider in organizations wishing to comply with ISO 15489-1.

1.1.1 Report Focus

This report on EMC Data Domain Retention Lock Compliance edition focuses primarily on ISO 15489-1 since it provides the foundational principles and functional requirements for a records system environment. ISO 15489-1 defines a “records system” as an “information system that captures, manages and provides access to records through time.” Further, while ISO 15489-1 encompasses
all types of records systems, whether hardcopy, micrographic or electronic, this report focuses only on the storage-related requirements related to the electronically stored records using an electronic storage system.

ISO/TR 15489-2 provides one methodology for establishing a records system – whether hardcopy, micrographic or electronic – that considers the processes and factors related to the implementation of a records system that meets the principles and requirements of ISO 15489-1. Selected implementation factors from ISO/TR 15489-2 are referenced in this report where they specifically relate to the electronic storage of records.

**1.1.2 ISO 15489 Requirements Overview**

This section provides an overview of selected requirements areas of ISO 15489-1 and selected guidelines of ISO/TR 15489-2 that relate to the storage of electronic records.

The scope of ISO 15489-1 is defined in Section 1, Scope, which states, among other items, that:

This part of ISO 15489 provides guidance on managing records of originating organizations, public or private, for internal and external clients.

All elements outlined in this part of ISO 15489 are recommended to ensure that adequate records are created, captured and managed. Procedures that help ensure the management of records according to the principles and elements outlined in this part of ISO 15489 are provided in ISO/TR 15489-2 (Guidelines).

This part of ISO 15489

*****

– provides guidance on the design and implementation of a records system, . . .

*****

The principles of records management programs are stated in ISO 15489-1, Subsection 7.1, Principles of records management programmes. The introductory paragraph of this section states:

. . . To support the continuing conduct of business, comply with the regulatory environment, and provide necessary accountability, organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required. . . .

Regarding the storage and handling of records using electronic systems, ISO 15489-1, Section 9.6, Storage and handling, states:
Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention.

The processes and factors related to the implementation of a records system as described in ISO/TR 15489-2 are of a general nature since they were developed to apply to hardcopy, micrographic or electronic records systems.

ISO 15489-1 and ISO/TR 15489-2 contain certain requirements and guidelines, such as, maintaining authentic and reliable records and protecting them against alteration or destruction for the assigned period of their retention, that can be met or supported, in whole or in part, by advanced storage systems. These requirements and guidelines are described and assessed in section 2 of this report.

1.2 EMC Data Domain Retention Lock Compliance Edition Overview

EMC offers a software product named EMC Data Domain Retention Lock that can be applied to any MTree (a logical volume in a virtual file system) on a Data Domain system. When an MTree is configured to support DD Retention Lock software, a retention period can be set for individual record files that prevent them from being deleted before the retention period has expired. The DD Retention Lock software capability can be configured for either of two retention management environments:

- **Compliance environment** designed to meet a more strict set of records management requirements, such as those in ISO 15489-1 and ISO 15489-2, and
- **Governance environment** where the actions allowed by the client application or certain administrative storage functions may not meet certain requirements of ISO 15489-1 and ISO 15489-2.

This assessment report focuses only on the Compliance edition of DD Retention Lock software.

1.3 Assessment and Technical Report

To obtain an independent and objective assessment of the EMC Data Domain Retention Lock Compliance edition (“Retention Lock Compliance Storage”) capabilities relative to meeting the pertinent requirement areas of ISO 15489-1, EMC (“EMC”) engaged Cohasset Associates, Inc. (“Cohasset”).

Cohasset (www.cohasset.com) is a highly respected records management consulting firm with recognized expertise and more than 40 years of experience serving companies that are guided by ISO 15489 regarding records management practices. Additional information about Cohasset Associates is provided at the end of this report.
Cohasset’s assignment was to:

- Assess the ability of the DD Retention Lock Compliance to meet the pertinent requirements of ISO 15489, and
- Prepare this technical report regarding that assessment.

This assessment represents the professional opinion of Cohasset Associates and should not be construed as an endorsement or rejection by Cohasset of the DD Retention Lock Compliance edition and its capabilities or other EMC products. To conduct this assessment, Cohasset relied upon four types of information provided by EMC regarding the DD Retention Lock Compliance: a) oral discussions, b) system requirements documents, c) user guides, and d) other directly related materials.

This assessment addresses only those ISO 15489-1 requirements and ISO 15489-2 guidelines that could be met or supported by digital storage systems. Public and private entities who utilize digital storage systems with the goal of being compliant with ISO 15489 must ensure that a combination of procedures, controls, and application capabilities (operating in conjunction with the storage management capabilities addressed in this assessment) are met.

The content and conclusions of this assessment are not intended and should not be construed as legal advice. Relevant laws and regulations are constantly evolving, and legal advice must be tailored to the specific circumstances of the laws and regulations for each organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel.
2. ISO 15489-1 Compliance Assessment

This section presents Cohasset’s assessment of the DD Retention Lock Compliance capabilities that are relevant to meeting the relevant electronic records management requirements of ISO 15489-1.

This assessment uses the terms “record” and “record file” (versus “file”) to be consistent with ISO 15489-1 terminology.

2.1 Storage-related ISO 15489 Requirements

There are three functional requirement areas of ISO 15489-1 and ISO 15489-2 that are assessed to determine the degree to which they can be met or supported by the capabilities of DD Retention Lock Compliance:

1) **Authoritative Records** – managing records so as to make them authentic and reliable and to preserve their integrity against unauthorized alteration or deletion,

2) **Retention and Disposition** – retaining records for as long as required prior to disposition, and

3) **Storage and Handling** – storing records on media that ensures their reliability, authenticity and preservation for as long as they are needed.

Each assessment of the three requirement areas are structured into three sections:

- **Compliance Requirements** related to a specific requirement or guideline area,
- **DD Retention Lock Compliance Capabilities** that meet or support meeting the compliance requirements, and
- **Compliance Assessment** which summarizes Cohasset Associates’ assessment regarding the degree to which DD Retention Lock Compliance capabilities support meeting the compliance requirements.
2.2 Authoritative Records

2.2.1 Compliance Requirements

An “authoritative record” as defined in ISO 15489-1 is described as having the characteristics of:

- authenticity,
- integrity,
- reliability, and
- usability.

Among other attributes of an authoritative record as stated in ISO 15489-1 is that it:

- can be depended on because its contents can be trusted as a full and accurate representation of the transactions, activities or facts to which it attests, and
- is complete and unaltered.

The characteristic of “authenticity” for a record is described in ISO 15489-1, Section 7.2.2:

... To ensure the authenticity of records, organizations should . . . . ensure . . . . that records are protected against unauthorized addition, deletion, alteration, use and concealment.

The characteristic of record “integrity” is described in ISO 15489-1, Section 7.2.4:

The integrity of a record refers to its being complete and unaltered.

It is necessary that a record be protected against unauthorized alteration. . . .

The definition of records system characteristics that achieve “reliability” is defined in ISO 15489-1, Section 8.2.2:

A records system should

*****

c) protect the records from unauthorized alteration or disposition,

*****

In addition, ISO/TR 15489-2, Section 4.3.3 Registration defines the records management process of “Registration” with its purpose “to provide evidence that a record has been created and captured into the record system.” In defining specific characteristics of “registering” a record, Section 4.3.3 in ISO/TR 15489-2 states:
Registration specifies the following metadata as a minimum:

a) a unique identifier assigned from the system;

b) the date and time of registration;

*****

2.2.2 DD Retention Lock Compliance Capabilities

DD Retention Lock Compliance has multiple capabilities that meet or support meeting the ISO 15489-1 and ISO 15489-2 requirement that records must be authoritative, including preserving record integrity and completeness when stored and retrieved and protecting records against alteration or destruction during the assigned retention period. The capabilities that can meet this requirement are summarized below.

DD Retention Lock Compliance capabilities:

• A non-erasable, non-rewriteable record management environment is established by configuring a MTree with DD Retention Lock Compliance software.

• At the time each record is stored the following actions occur:
  ▪ Each record is set to a “read-only” status and a retention period is assigned,
  ▪ A unique identifier, including a date/time of recording, is assigned to the record,
  ▪ Each record is read back and validated to verify its quality and accuracy prior to being accepted as error free.

• At the time each record is retrieved and periodically during the retention period for the record, the record is checked for errors and error correction capabilities are employed to correct errors as required.

• Any attempt to erase, overwrite or alter a record file or the complete record file system during the assigned retention period, whether by a client application, a local user, or a file system administrator, will be rejected and will result in an error condition in the system.

• If a DD Retention Lock Compliance license expires or is deleted from the Data Domain system, the integrity of record files currently stored will continue to be protected for the established retention period.

• Should the primary copy of records be compromised or destroyed, DD Retention Lock Compliance provides for setting up a second Compliance MTree where a duplicate copy of all records (with their associated retention and protection codes) can be stored and used for disaster recovery.
More detailed descriptions of these capabilities and their support for ensuring that stored records are authoritative are provided in Section 4 of this report.

### 2.2.3 Compliance Assessment

It is the opinion of Cohasset Associates that the DD Retention Lock Compliance, when deployed on the Data Domain system, provides strong capabilities for meeting the ISO 15489-1 requirement that records be authoritative at the time of recording, during the retention period and upon retrieval.

### 2.3 Retention and Disposition

#### 2.3.1 Compliance Requirements

The general requirements for retention and disposition are stipulated in ISO 15489-1, Section 8.3.7, Retention and Disposition, which states:

*Records systems should be capable of facilitating and implementing decisions on the retention and disposition of records.*

The need for retention management is also expressed in ISO 15489-1, Section 9.6, Storage and Handling:

*Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention.*

#### 2.3.2 DD Retention Lock Compliance Capabilities

The DD Retention Lock Compliance has multiple capabilities that support the retention and disposition of electronic records. The capabilities that can meet this requirement are summarized below.

DD Retention Lock Compliance capabilities:

- A non-erasable, non-rewriteable record management environment is established by configuring an MTree with DD Retention Lock Compliance software.
- Within a Compliance MTree, a retention period can be set and a read-only status can be activated for each record file – thereby establishing the time period during which specific records would be protected against erasure, overwrite, or alteration.
- Any attempt to delete a record file or the complete file system prior to the expiration of the assigned retention period – whether by a client application, a local user, or a file system administrator – will be rejected and will result in an error condition.
• Minimum and Maximum retention period attributes can be set to ensure that no retention period is set that is lower than the Minimum attribute value nor higher than the Maximum attribute value.

• The retention period for individual record files can be extended, but not lowered. This addresses the need for potentially longer retentions that may result from litigation or investigative holds.

• If the DD Retention Lock Compliance edition is either uninstalled or expired from the Data Domain system, all record files currently stored will continue to be protected for their designated retention periods.

• Once the retention period for a record has expired, DD Retention Lock Compliance allows the client application to delete the record. The record cannot be deleted via the system administration interface, even using dual sign-on.

Detailed descriptions of these capabilities and their support for retention and disposition of records are provided in Section 4 of this report.

2.3.3 Compliance Assessment

It is Cohasset Associates' opinion that the DD Retention Lock Compliance provides capabilities that support meeting the record retention and disposition requirements of ISO 15489-1.

2.4 Storage and Handling

2.4.1 Compliance Requirements

The general requirements for the storage of records is defined in ISO 15489-1, Section 9.6, Storage and Handling. An electronic record storage system can meet or support meeting the following selected set of these requirements:

Records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed.

*****

Storage conditions and handling processes should be designed to protect records from unauthorized access, loss or destruction, and from theft and disaster.

*****

Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention.
In addition, ISO 15489-2, Section 4.7.7.3, Digital Storage, addresses backup and recovery of records:

The storage of records in electronic form necessitates the use of additional storage plans and strategies to prevent their loss:

a) Backup systems are a method of copying electronic records to prevent loss of records through system failures. Such systems ought to include a regular backup schedule, multiple copies on a variety of media, dispersed storage locations for the backup copies, and provisions for both routine and urgent access to backup copies.

2.4.2 DD Retention Lock Compliance Capabilities

DD Retention Lock Compliance has multiple capabilities that support the proper storage and handling of electronic records, including protection against unauthorized access, destruction or disaster.

DD Retention Lock Compliance capabilities:

- Inadvertent or malicious record destruction is prevented during the designated retention period because any attempt to erase, overwrite or alter a record file or the complete file system – whether by a client application, a local user, or a file system administrator – will be rejected and will result in an error condition notification to the system administrator.

- Even if a DD Retention Lock Compliance software license expires or is deleted from the Data Domain system, all record files currently stored will continue to be protected for the established retention period.

- DD Retention Lock Compliance provides for setting up a second Compliance MTree where a duplicate copy of all records (with their associated retention and protection codes) can be stored so that in the event of a disaster that comprises the primary copy of records, the records and associated metadata can be fully recovered.

More detailed descriptions of these capabilities are provided in Section 4 of this report.

2.4.3 Compliance Assessment

Cohasset believes that the DD Retention Lock Compliance, when deployed on the Data Domain system, provides strong storage and handling capabilities for protecting electronically stored records from unauthorized destruction and against disaster.
3. Conclusions

Cohasset’s conclusion is that the DD Retention Lock Compliance edition configured on a Data Domain system supports meeting requirements in the three requirements areas of ISO 15489-1 and ISO 15489-2 described in Section 2, above.

The capabilities of DD Retention Lock Compliance that support meeting these requirements are:

- A records management environment can be established that uses integrated control codes to ensure that the stored records are authoritative – that they are reliable and that their integrity will be preserved during the required period of retention.

- Once the retention period and read-only status are established in the system, a record cannot be deleted until the retention period has expired – thereby protecting stored records from erasure, overwrite, or alteration during the retention period.

- When a duplicate or backup copy of the records (with the associated retention periods and protection) is created, it can be used to recover records in the case of a disaster.
4. Matrix of DD Retention Lock Compliance Edition Capabilities

The following table provides greater detail of DD Retention Lock Compliance capabilities that enable it to support meeting the three areas of ISO 15489-1 and ISO/TR 15489-2 records system requirements described in Section 2, above.

The column labeled “Authentic Record” denotes (with an “✔”) those capabilities of the DD Retention Lock Compliance on a Data Domain system that support meeting the requirements for keeping records that are authoritative - where reliability and integrity are ensured and the records are protected against malicious (or inadvertent) destruction or alteration.

The column heading “Retention/Disposition” denotes (with an “✔”) those capabilities of the DD Retention Lock Compliance on a Data Domain system that support setting a retention period and allowing extensions, but not reductions, of the retention period.

The column heading “Storage & Handling” denotes (with an “✔”) those capabilities of the DD Retention Lock Compliance on a Data Domain system that provide protection against unauthorized access, destruction or disaster.
# 4.1 Establishing an Authoritative DD Retention Lock Compliance and Data Domain Storage System

<table>
<thead>
<tr>
<th></th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
</table>
| • In order to activate the record retention and protection capabilities of the DD Retention Lock Compliance, the organization must purchase a unique Retention Lock Compliance software license that ensures that the compliance features of Retention Lock are activated.  
  • During administrative setup of DD Retention Lock Compliance edition, one or more Compliance MTrees can be defined, thereby allowing compliance capabilities to be applied to record files.  
  • After an MTree has been configured with DD Retention Lock Compliance, it cannot be disabled, or overridden. | ✔ | ✔ | ✔ |
| • A Minimum and Maximum time-based retention period for each MTree must be established during the administrative setup of DD Retention Lock Compliance on a Data Domain system. This ensures that the "atime" retention expiration date for a record is not set below the Minimum or above the Maximum. Once set, the Minimum and Maximum retention periods cannot be reduced; they can only be extended. | ✔ | ✔ |  |
| • For a Managed Tree (MTree) that is DD Retention Lock Compliance enabled, a new record file can be placed under Compliance control and a time-based retention expiration date (retention period) set. The retention period is set when the client application: a) issues a file protocol instruction with an atime retention attribute that is set into the future (beyond the date/time of recording) and b) where the retention expiration date is greater than the Minimum defined retention period per MTree and less than the Maximum defined retention period per MTree. The retention period is then managed as follows:  
  • Any atime value that is less than or equal to current time – and therefore not a valid retention period – is ignored since it is assumed to be an update to the “time last accessed” value.  
  • If the atime retention expiration date supplied by the client application less than the Minimum retention period or greater than the Maximum retention period, then an error condition will be returned to the client application.  
  • If an attempt is made to delete a record file where the retention period has not expired, then the delete command results in an error condition.  
  • If an attempt is made to delete an MTree, that is DD Retention Lock Compliance enabled, which contains record files, then the delete command results in an error condition. | ✔ | ✔ | ✔ |
### 4.2 Retention Management

<table>
<thead>
<tr>
<th></th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A retention period is set when an atime retention expiration date (the retention period) is set by the client or user application sending the record to DD Retention Lock Compliance.</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>• Once the retention period has been set for an individual record file, it cannot be deleted or overwritten until the retention period expires. Once the retention period has expired, deletion of the record file may be performed by an authorized client application or system administrator.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>• An existing retention expiration date cannot be reduced. The DD Retention Lock Compliance will return an error condition to the client application when the new atime retention expiration date is received that is earlier in time than the current atime retention expiration date.</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>• The retention expiration date for a record file under DD Retention Lock Compliance control may be extended by recording a new a-time retention attribute for the record file that is later in time than the current retention expiration date and less than the Maximum retention.</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

### 4.3 Accuracy and Quality of Stored Records

<table>
<thead>
<tr>
<th></th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>The objective of these capabilities is to provide the utmost confidence that all records read from the storage media are precisely the same as those recorded.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Initial Recording Process*

• DD Retention Lock Compliance provides an exceptionally strong capability for verifying quality and accuracy for each container of record file data that is written. An inline read verification at the time of recording is performed before being accepted as error-free. This method goes beyond the minimum acceptable reliance on state-of-the-art magnetic disk recording error checking and detection/correction capabilities. | ✔ | | ✔ |
### Post Recording Process
- Record file data is packaged and written in containers (multi-megabyte units). A strong checksum value is calculated from the data in each container and stored with that container. The write verification process involves reading back the data in the stored containers and verifying that the checksums are accurate. After the containers are verified, the files contained in them are verified by reading the metadata of the files and verifying that each segment of a file exists in the container identified by the metadata.
- During verification, if the checksum does not match for any container, RAID 6 is used to correct the errors and recover the container. If the container cannot be recovered using RAID 6, an alert is raised to the client application whereupon the administrative support personnel can recover the data from a replicated or duplicate copy.
- During read-back of a record file, whether by the client archiving application or by the Data Domain file system, the checksums are verified and, when errors are encountered, RAID 6 error correction is applied as required, thereby ensuring that the record remains complete and accurate.
- Periodic “scrubbing” of the record file data on the DD Retention Lock Compliance MTree is performed to find and correct any defects that may occur. This is particularly important for those record files that have not been read back for an extended period of time.

<table>
<thead>
<tr>
<th></th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

### 4.4 Administrative Security
- A Compliance MTree cannot be deleted under any circumstances, not even with dual sign-on authorization.

<table>
<thead>
<tr>
<th></th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

- When a DD Retention Lock Compliance license has expired or is cancelled for any reason, no new Compliance MTrees can be defined. However, all of the record files in all existing Compliance MTrees will continue to be protected. Also any new files that are stored in existing Compliance MTrees with a retention period atime later than the day stored will continue to be protected.

<table>
<thead>
<tr>
<th></th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
- Additional administrative security is provided via the DD Retention Lock Compliance to ensure that certain administrative functions or actions that could potentially compromise the integrity of record files prior to expiration of the retention period are not under the control of just one administrative person. This additional administrative security is provided in the form of a “dual” sign-on, i.e., sign-on by the regular system administrator plus the requirement for second sign-on by an authorized person. The primary administrative actions that require a dual or sign-on in a DD Retention Lock Compliance enabled Data Domain system are:
  - Extending Minimum or Maximum retention periods.
  - Renaming an MTree.
  - Deleting a DD Retention Lock Compliance license.
  - Other system support or maintenance actions that could potentially compromise the integrity of stored record files where the retention period has not expired.

- No logical access (via a software user interface) without dual sign-on security is allowed for error correction purposes such as the scenario where the Data Domain system experiences a system error or corruption. For the extreme scenario where the full Data Domain operating system will not start up, the only means to start or restart the system is through single user access to the system via a physical USB drive which must be protected and available only with dual sign-on authorization.

- The accuracy of the system clock in DD Retention Lock Compliance is critical for determining whether the retention expiration date of a record file has expired. Situations can occur, such as a power outage, maintenance downtime, etc., which may affect the accuracy of the system clock and require it to be adjusted or reset. Additional statistics are gathered, analyses are performed and certain restrictions are placed on ensuring the accuracy of the system clock to meet retention compliance requirements.
  - The accuracy of the system clock and variations of the system clock with current actual time is regularly monitored.
  - The system clock is only allowed to vary by a maximum of two weeks in a year.
  - Should the system clock vary beyond the two-week maximum during a year, then the administrative dual sign-on is required to reset the clock to current time.
4.5 Backup and Recovery

<table>
<thead>
<tr>
<th>The intent of this capability is to provide an alternate storage source for maintaining retention and protection and for accessing the electronic record should the primary source be compromised, i.e., lost or damaged.</th>
<th>Authentic Record</th>
<th>Retention/Disposition</th>
<th>Storage &amp; Handling</th>
</tr>
</thead>
<tbody>
<tr>
<td>The DD Retention Lock Compliance provides for an MTree to be replicated to a second Data Domain system configured with DD Retention Lock Compliance, either locally or remotely. During replication, all record files and associated metadata, including retention metadata, are replicated to the file system or MTree on the destination DD Retention Lock Compliance enabled Data Domain system.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Should a major error occur that makes the original file system or MTree inaccessible, then the record files can be recovered from the replicated copy of the MTree.</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>
End Notes

1. DD Retention Lock software currently supports time-based retention (i.e., retain for a specified period from the time after the file is recorded). Event-based retention (i.e., indefinite retention once the file is recorded until a specified event occurs, followed by a fixed, final retention period) is not currently supported.

2. The “atime” attribute in standard file protocol instructions represents the “time last accessed” for a file. For Retention Lock Compliance enabled MTrees, this attribute is utilized to establish the retention expiration date for a record file.

3. Redundant Array of Independent Disks (RAID): A method for recording data to magnetic disk devices that provides for various levels of error correction and read or write performance improvements. RAID 6 employs striped disks with dual parity and combines four or more disks in a way that provides for correction of detected errors for up to as many as two full disk units of data during read-back.
About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com), is one of the nation’s foremost consulting firms specializing in records and information management. Now in its fourth decade of serving clients throughout the United States, Cohasset Associates provides award-winning professional services in three areas: management consulting, education and legal research.

Management Consulting: The focus of Cohasset Associates’ consulting practice is improving the programs, processes and systems that manage document-based information. Cohasset works to provide its clients with cost-effective solutions that will both achieve their business objectives and meet their legal/regulatory responsibilities. This ranges from establishing effective corporate records management programs to planning state-of-the-art electronic records systems.

Education: Cohasset Associates is renowned for its longstanding leadership in records management education. Today, Cohasset’s educational work is centered on its annual National Conference for Managing Electronic Records (MER), which addresses the operational, technical and legal issues associated with managing the complete life cycle of electronic records (www.merconference.com). The MER sessions also are available to anyone, anytime, anywhere via streaming video through RIM on Demand, (www.rimeducation.com/videos/rimondemand.php)

Legal Research: Cohasset Associates is nationally respected for its leadership on records management legal issues – from retention schedules to the use of alternative media to paper for storing document-based information.

For more than twenty years, Cohasset Associates has been a “thought leader” in records and information management. Cohasset has been described as the only management consulting firm in its field with its feet in the trenches and its eye on the horizon. It is this blend of practical experience and a clear vision of the future that, combined with Cohasset Associates’ commitment to excellence, has resulted in Cohasset Associates’ extraordinary record of accomplishments and innovation.

This technical assessment and the information contained in it are copyrighted and are the sole property of Cohasset Associates, Inc. Selective references to the information and text of this technical assessment are welcome, provided such references have appropriate attributions and citations. Permission is granted for in-office reproduction so long as the contents are not edited and the “look and feel” of the reproduction is retained.