IRS Rev. Procs. 98-25 & 97-22 Compliance Assessment

EMC Data Domain Retention Lock Compliance Edition

Prepared by Cohasset Associates, Inc.

Abstract

This technical report is an assessment of the EMC Data Domain Retention Lock Compliance edition capabilities relative to the requirements areas that may be met or supported by an electronic storage system as set forth in IRS Rev. Procs. 98-25 and 97-22. There are certain requirement areas of Rev. Procs. 98-25 and 97-22 that can be met or supported by DD Retention Lock Compliance, even though these revenue procedures do not specify that a particular type of storage or storage function is needed to meet the requirements.

Cohasset’s conclusion is that the DD Retention Lock Compliance edition, when installed, configured and enabled on the Data Domain system, supports meeting the requirements in the areas of IRS Rev. Procs. 98-25 and 97-22 that relate to record integrity and protection, record retention, and backup and recovery.

The capabilities of EMC Data Domain Retention Lock Compliance edition that support meeting these requirements include: a) establishing a records management environment that provides for immutability and protection of electronically stored records and thereby prevents their alteration, deletion or destruction until the retention period has expired, b) setting a “read-only” status for and assigning a retention period to each record, c) ensuring the integrity of records is maintained for the assigned retention period, and d) creating a duplicate or backup copy of all records – with the integrated retention period and protection control codes – for the purpose of disaster recovery.
# Table of Contents

1. Introduction ........................................................................................................................................................ 3  
   1.1 IRS Rev. Procs. 98-25 & 97-22 ...................................................................................................................... 3  
   1.2 EMC Data Domain Retention Lock Compliance Edition Overview ...................................................... 5  
   1.3 Assessment and Technical Report............................................................................................................. 5  

2. IRS Rev. Procs. 98-25 & 97-22 Compliance Assessment ............................................................................. 7  
   2.1 Storage-Related Rev. Procs. 98-25 and 97-22 Requirements ............................................................... 7  
   2.2 Record Integrity and Protection .................................................................................................................. 8  
   2.3 Record Retention ....................................................................................................................................... 9  
   2.4 Backup and Recovery................................................................................................................................. 11  

3. Conclusions ....................................................................................................................................................... 13  

   4.1 Authoritative and Authentic Records....................................................................................................... 15  
   4.2 Retention Management ............................................................................................................................ 16  
   4.3 Administrative Security ............................................................................................................................. 16  
   4.4 Accuracy and Quality of Stored Records ............................................................................................... 17  
   4.5 Backup and Recovery ............................................................................................................................... 18  

End Notes ............................................................................................................................................................ 19  

About Cohasset Associates, Inc. .......................................................................................................................... 20
1. Introduction

This section sets the context for this technical assessment. It identifies the foundation of requirements, as set forth in IRS Revenue Procedures (Rev. Procs.) 98-25 and 97-22, for records systems in general and identifies areas that may be met or supported by electronic storage systems. It then provides an overview of the storage system that is the subject of Cohasset’s assessment.

1.1 IRS Rev. Procs. 98-25 & 97-22

The Internal Revenue Service (IRS) is a bureau of the Department of Treasury and is the revenue service of the United States federal government. The IRS is responsible for collecting taxes and interpreting and enforcing the United States Internal Revenue Code.

In 1964, the IRS promulgated Rev. Proc. 64-12, which defined requirements for “automated data processing” systems (ADP systems). Rev. Proc 64-12 has evolved into the current Rev. Proc. 98-25.

The purpose of Rev. Proc. 98-25 is:

. . . to specify the basic requirements that the Internal Revenue Service considers to be essential in cases where a taxpayer’s records are maintained within an Automatic Data Processing system (ADP system).

An “ADP system” is defined in Section 4 as:

An “ADP system” consists of an accounting and/or financial system (and subsystems) that processes all or part of a taxpayer’s transactions, records, or data by other than manual methods. An ADP system includes, but is not limited to, a mainframe computer system, stand-alone or networked microcomputer system, Data Base Management System (DBMS), and a system that uses or incorporates Electronic Data Interchange (EDI) technology or an electronic storage system. (emphasis added)

In addition, Rev. Proc. 97-22 pertains specifically to “electronic storage systems.” Since “electronic storage systems” are also listed as a type of ADP system in the preceding definition, these systems are governed by both Rev. Procs. 98-25 and 97-22.
An “electronic storage system” is defined as follows in the Scope section of Rev. Proc. 97-22.

An electronic storage system is a system to prepare, record, transfer, index, store, preserve, retrieve, and reproduce books and records by either:

1. electronically imaging hardcopy documents to an electronic storage media; or

2. transferring computerized books and records to an electronic storage media using a technique such as “COLD” (computer output to laser disk), which allows books and records to be viewed or reproduced without the use of the original program.

The IRS has long recognized the importance of “machine sensible records” (i.e., electronic records). Explicitly, in paragraph 11.01 of Rev. Proc. 98-25, the IRS specifies that “[hardcopy] records are not a substitute for the machine-sensible records required to be retained by this revenue procedure.”

While storage systems or storage media are not addressed specifically as an integral part of meeting the requirements of Rev. Procs. 98-25 and 97-22, there are three major areas where meeting the requirements of these revenue procedures can be supported by using advanced digital storage capabilities:

• **Record Integrity and Protection**

  - Rev. Proc. 98-25 stipulates: “The [IRS] District Director may periodically initiate tests to establish the authenticity, readability, completeness, and integrity of a taxpayer’s machine-sensible records retained in conformity with this revenue procedure.” Similarly, Rev. Proc. 97-22 states: “An electronic storage system must include . . . reasonable controls to ensure the integrity, accuracy, and reliability of the electronic storage system. . . .”

  - Rev. Proc. 98-25 requires documentation that is sufficiently detailed to identify “the internal controls used to prevent the unauthorized addition, alteration, or deletion of retained records.” Similarly, Rev. Proc. 97-22 states: “An electronic storage system must include . . . reasonable controls to prevent and detect the unauthorized creation of, addition to, alteration of, deletion of, or deterioration of electronically stored books and records. . . .”

A storage system that has integrated storage and administrative controls to help protect the integrity of the records (for the required retention period) and that protects electronically stored records against unauthorized destruction or alteration (for the required retention period) would facilitate achieving these requirements.
• **Record Retention** – The IRS requires electronic records to be retained during the tax assessment period. Specifically, Rev. Proc. 98-25 stipulates: “The taxpayer must retain machine-sensible records so long as their contents may become material to the administration of the internal revenue laws . . .” Similarly, Rev. Proc. 97-22 states: “The taxpayer must retain electronically stored books and records so long as their contents may become material in the administration of the Internal Revenue laws . . .”

A storage system which ensures that electronic records are preserved for the required period of retention would facilitate achieving these requirements.

• **Backup and Recovery** – Both Rev. Procs. 98-25 and 97-22 include recommended records management practices, which include “providing a secure storage environment, creating backup copies.”

### 1.2 EMC Data Domain Retention Lock Compliance Edition Overview

EMC offers a software product, EMC Data Domain Retention Lock, which 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 support meeting a more stringent set of principles and requirements, such as those defined in Rev. Procs. 98-25 and 97-22, and

• **Governance environment** where the actions allowed by the client application or storage administrative functions may not support meeting Rev. Procs. 98-25 and 97-22 requirements.

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

### 1.3 Assessment and Technical Report

To obtain an independent and objective assessment of the EMC Data Domain Retention Lock Compliance (“DD Retention Lock Compliance”) capabilities relative to meeting the pertinent requirement areas of Rev. Procs. 98-25 and 97-22, 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 must comply with the IRS requirements with respect to their 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 DD Retention Lock Compliance to meet the pertinent requirements of Rev. Procs. 98-25 and 97-22, 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 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 Rev. Procs. 98-25 and 97-22 requirements that could be met or supported by digital storage systems. In addition, organizations that utilize these digital storage systems must ensure that a combination of procedures, controls, application capabilities (operating in conjunction with the storage management capabilities addressed in this assessment) meet all of requirements stipulated in Rev. Procs. 98-25 and 97-22.

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. IRS Rev. Procs. 98-25 & 97-22 Compliance Assessment

This section presents Cohasset’s assessment of DD Retention Lock Compliance capabilities that are pertinent to meeting the relevant electronic records management requirements of Rev. Procs. 98-25 and 97-22.

This assessment uses the terms “record” (versus “file”) to be consistent with the terminology in Rev. Procs. 98-25 and 97-22.

2.1 Storage-Related Rev. Procs. 98-25 and 97-22 Requirements

The three requirement areas of Rev. Procs. 98-25 and 97-22 that can be met or supported by the capabilities of DD Retention Lock Compliance are:

1. **Record Integrity and Protection** – storing records on media that ensures their integrity and authenticity for as long as they are needed and prevents unauthorized alteration of or deletion of electronically stored books and records,

2. **Record Retention** – meeting the requirements to retain “books and records” during the period in which their contents may become material to the administration of the internal revenue laws,

3. **Backup and Recovery** – creating a backup or duplicate copy of records and recovering records from the backup copy in the event of a disaster.

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

- **Compliance Requirements** related to a specific Rev. Procs. 98-25 and 97-22 requirement,
- **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 Record Integrity and Protection

2.2.1 Compliance Requirements

Rev. Proc. 97-22 contains requirements related to the authenticity, accuracy and reliability of requisite records, as well as requirements to prevent unauthorized alteration or deletion of requisite records. The following excerpt is from Section 4, Electronic Storage System Requirements, paragraph .01(2):

(2) An electronic storage system must include:

(a) reasonable controls to ensure the integrity, accuracy, and reliability of the electronic storage system;

In addition, paragraph three from Section 4, Electronic Storage System Requirements, states:

.03 Recommended Practices. The implementation of records management practices is a business decision that is solely within the discretion of the taxpayer. Records management practices may include the labeling of electronically stored books and records, providing a secure storage environment, creating back-up copies, selecting an off-site storage location, retaining hardcopies of books or records that are illegible or that cannot be accurately or completely transferred to an electronic storage system, and testing to confirm records integrity.

2.2.2 DD Retention Lock Compliance Capabilities

DD Retention Lock Compliance has multiple capabilities that meet or support meeting the requirements of Rev. Procs. 98-25 and 97-22, which specifies that records must have integrity and that unauthorized alteration and deletion is prevented during the assigned retention period.

DD Retention Lock Compliance capabilities that can meet this requirement are summarized below.

- A non-erasable, non-rewriteable record management environment is established by configuring an MTree with the DD Retention Lock Compliance edition.

- 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, and
  - 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.

Additional administrative security is provided via 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.

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.

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.

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

2.2.3 Compliance Assessment

It is the opinion of Cohasset Associates that the DD Retention Lock Compliance edition, when deployed on the Data Domain system, provides strong capabilities for meeting the Rev. Procs. 98-25 and 97-22 requirements that the integrity of records be protected (thereby preserving their authenticity, accuracy and reliability) and that unauthorized alteration or deletion of records is prevented, during the assigned retention period.

2.3 Record Retention

2.3.1 Compliance Requirements

The requirement to retain books and records “so long as the contents thereof may become material in the administration of any internal revenue law” is contained in paragraph 3 of the Background section of both Rev. Proc. 98-25 and 97-22, as follows:
.03 Section 1.6001-1(e) provides that the books or records required by section 6001 must be kept available at all times for inspection by authorized internal revenue officers or employees, and must be retained so long as the contents thereof may become material in the administration of any internal revenue law.

In addition, as stipulated in Section 2, paragraph .04, of Rev. Proc. 98-25, Rev. Rul. 71-20 formally establishes that electronic records need to be retained for compliance with IRS laws:

.04 Rev. Rul. 71-20, 1971-1 C.B. 392, establishes that all machine-sensible data media used for recording, consolidating, and summarizing accounting transactions and records within a taxpayer’s ADP system are records within the meaning of section 6001 and section 1.6001-1, and are required to be retained so long as the contents may become material in the administration of any internal revenue law.

As a practical matter, most organizations establish a fixed time period (e.g., 7 years, 10 years, etc.) for retaining accounting books and records, rather than assigning a retention period that is based on the expiration of the assessment period.

Further, if unusual circumstances require a longer retention period, a tax hold is issued to stop destruction of relevant records.

**2.3.2 DD Retention Lock Compliance Capabilities**

DD Retention Lock Compliance capabilities that support retention of electronic records include:

- A non-erasable, non-rewriteable records management environment is established by configuring an MTree with the DD Retention Lock Compliance edition.
- 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 parameters can be set to ensure that no retention period 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 license expires or is uninstalled from the EMC 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.

A more detailed description of these capabilities and their support for records retention and disposition are described in Section 4 of this Technical Report.

**2.3.3 Compliance Assessment**

It is Cohasset Associates’ opinion that the DD Retention Lock Compliance edition, when deployed on the Data Domain system, provides multiple capabilities that support meeting the record retention requirements of Rev. Procs. 98-25 and 97-22.

**2.4 Backup and Recovery**

**2.4.1 Compliance Requirements**

Rev. Proc. 97-22 defines recommended records management practices, which include “providing a secure storage environment, creating back-up copies.” The following is paragraph .03, excerpted from Section 4, Electronic Storage System Requirements, of Rev. Proc. 97-22:

> .03 Recommended Practices. The implementation of records management practices is a business decision that is solely within the discretion of the taxpayer. Records management practices may include the labeling of electronically stored books and records, providing a secure storage environment, creating back-up copies, selecting an off-site storage location, retaining hardcopies of books or records that are illegible or that cannot be accurately or completely transferred to an electronic storage system, and testing to confirm records integrity.

Additionally, Rev. Proc. 98-25 contains similar recommended records management practices in Section 9, paragraph .01(1).
2.4.2 DD Retention Lock Compliance Capabilities

For backup and recovery purposes, DD Retention Lock Compliance capabilities include:

- Opportunities to set 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, which comprises the primary copy of records, the records and associated metadata can be fully recovered.
  - Should a major error occur that makes the original file system or MTree inaccessible, then the record files can be recovered from the backup or duplicate copy of the MTree.

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

2.4.3 Compliance Assessment

Cohasset believes that DD Retention Lock Compliance, when deployed on the Data Domain system, provides the capabilities for creating a backup or duplicate copy of records and recovering records from the backup copy in the event of a disaster.
3. Conclusions

It is Cohasset’s conclusion that the DD Retention Lock Compliance edition, when installed, configured and enabled on the Data Domain system, supports meeting the requirements in the areas of IRS Rev. Procs. 98-25 and 97-22 that relate to record integrity and protection, record retention, and backup and recovery, as described in Section 2, above.

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

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

- A records management environment can be established that provides for the integrity of electronically stored records, and thereby prevents their alteration, deletion or destruction until the retention period has expired.

- Integrated metadata control codes can be activated for each record that includes a “read-only” status and a retention expiration date.

- Once the retention expiration date and read-only status are established, 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 meet or support meeting the three records system requirements established in Rev. Procs. 98-25 and 97-22 and described in Section 2, above.

The column labeled “Integrity & Protection” denotes (with an “✔”) those capabilities of DD Retention Lock Compliance on a Data Domain system that support meeting the requirements for ensuring the reliability and integrity of records and protects against unauthorized alteration or destruction.

The column heading “Record Retention” denotes (with an “✔”) those capabilities of 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 “Backup & Recovery” denotes (with an “✔”) those capabilities of DD Retention Lock Compliance on a Data Domain system that provide protection against unauthorized destruction or disaster.
4.1 Authoritative and Authentic Records

<table>
<thead>
<tr>
<th>• In order to activate the record retention and protection capabilities of DD Retention Lock Compliance, an organization must acquire and install a unique DD Retention Lock Compliance edition license which ensures that the compliance features of Retention Lock are activated.</th>
<th>Integrity &amp; Protection</th>
<th>Record Retention</th>
<th>Backup &amp; Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>• During administrative setup of DD Retention Lock Compliance, one or more Compliance MTrees can be defined, thereby allowing compliance capabilities to be applied to record files.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>• After an MTree has been configured with DD Retention Lock Compliance, that MTree cannot be disabled or overridden.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>• 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:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.2 Retention Management

<table>
<thead>
<tr>
<th>Integrity &amp; Protection</th>
<th>Record Retention</th>
<th>Backup &amp; Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

- 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.

- 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.

- An existing retention expiration date cannot be reduced. 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.

- The retention expiration date for a record file under DD Retention Lock Compliance control may be extended by recording a new atime retention attribute for the record file that is later in time than the current retention expiration date and less than the Maximum retention.

4.3 Administrative Security

<table>
<thead>
<tr>
<th>Integrity &amp; Protection</th>
<th>Record Retention</th>
<th>Backup &amp; Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

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

- 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.

- 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.
### 4.4 Accuracy and Quality of Stored Records

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.

<table>
<thead>
<tr>
<th>Initial Recording Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>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 sign-on in a DD Retention Lock Compliance enabled Data Domain system are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extending Minimum or Maximum retention periods.</td>
</tr>
<tr>
<td>Renaming an MTree.</td>
</tr>
<tr>
<td>Deleting a DD Retention Lock Compliance license.</td>
</tr>
<tr>
<td>Other system support or maintenance actions that could potentially compromise the integrity of stored record files where the retention period has not expired.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The accuracy of the system clock and variations of the system clock with current actual time is regularly monitored.</td>
</tr>
<tr>
<td>The system clock is only allowed to vary by a maximum of two weeks in a year.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>
### Post Recording Process

- Record file data is packaged and written in containers (multi mega-byte 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 Compliance enabled 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>Post Recording Process</th>
<th>Integrity &amp; Protection</th>
<th>Record Retention</th>
<th>Backup &amp; Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

### 4.5 Backup and Recovery

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.

- 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.

- 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.

<table>
<thead>
<tr>
<th>4.5 Backup and Recovery</th>
<th>Integrity &amp; Protection</th>
<th>Record Retention</th>
<th>Backup &amp; Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
End Notes

1. 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.

2. 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.

3. Redundant Array of Independent Disks (RAID): A method for recording data to magnetic disk devices that provides 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.