Sarbanes-Oxley 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 areas of the Sarbanes-Oxley Act (“SOX”) that require the retention of audit records and where penalties may be assessed for malicious destruction or alteration of such records. The assessment examines the ability of the EMC Data Domain system with DD (Data Domain) Retention Lock Compliance to support meeting the requirements of the record retention and record protection areas of SOX.

Cohasset’s conclusion is that the DD Retention Lock Compliance software supports meeting the requirements in the areas of SOX that relate to record retention and to providing protection against malicious destruction of records that could mitigate criminal penalties.

The capabilities that support meeting these requirements are: a) a non-erasable, non-rewriteable records storage environment that uses integrated control codes to provide for record retention and to prevent destruction or alteration of electronically stored records; b) setting a “read-only” status for and assigning a retention period to each record, c) protecting records against deletion or alteration for the assigned retention period, 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 Sarbanes-Oxley Act – Records Management Requirements ............................................................... 3  
   1.2 Data Domain Retention Lock Compliance Software Overview ........................................................... 4  
   1.3 Assessment and Technical Report ............................................................................................................ 5  

2. SOX Compliance Assessment ............................................................................................................................ 6  
   2.1 Storage-related SOX Requirements ........................................................................................................ 6  

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

4. Matrix of DD Retention Lock Compliance Edition Capabilities ................................................................. 14  
   4.1 Establishing a DD Retention Lock Compliance Capable  
       EMC Data Domain Storage System .................................................................................................... 15  
   4.2 Administrative Security .......................................................................................................................... 16  
   4.3 Assessment and Technical Report ........................................................................................................ 16  
   4.4 Creating a Duplicate or Backup Copy for Recovery ........................................................................... 17  

End Notes ............................................................................................................................................................ 18  

About Cohasset Associates, Inc. ........................................................................................................................ 19
1. Introduction

This section sets the context for this technical assessment. It identifies the foundation, as set forth in SOX that relates to the retention and protection of electronically stored records. It then provides an overview of the storage system that is the subject of Cohasset’s assessment.

1.1 Sarbanes-Oxley Act – Records Management Requirements

The Sarbanes-Oxley Act of 2002 (SOX) is a United States federal law which sets new or enhanced standards for all U.S. public company boards, executive management, and public accounting firms. It was enacted as a result of the wave of corporate crime in the 1990’s and early 2000’s. Most notable of this wave was the Enron scandal, but criminal activities of companies such as Worldcom, Adelphia, and Global Crossing also provided impetus for a new law.

The purpose of SOX is to ensure that the financial records of publicly traded companies could be trusted, and that shareholders would be better protected against potential embezzlement and greed. Private companies are not affected by the provisions in SOX.

The focus of SOX is on the procedures, controls, accountability, and records of both accounting firms that audit public companies and investment management firms and on the procedures, controls and accountability of public companies and investment management companies themselves.

To oversee the ongoing implementation of SOX, the federal government created a new quasi-public agency called the Public Company Accounting Oversight Board (PCAOB) to act as a “watchdog” over auditors of public companies.

SOX is comprised of 11 sections – with each section defining certain requirements. These requirements, in turn, are augmented by related new rules or modifications of existing rules by the Securities and Exchange Commission (SEC) – as required by SOX.
Storage systems or storage media are not addressed specifically as an integral part of meeting any of the SOX requirements. However, there are two major areas of SOX where meeting the law's requirements can be supported by using advanced digital storage capabilities:

- **Record Retention** – SOX and associated, supporting SEC rules additions stipulate that accounting firms retain all audit workpapers as official records for 7 years. This requirement encompasses both paper and electronic records.

  A storage system that ensures electronic records are preserved for the required period of retention would facilitate achieving this SOX requirement.

- **Record Protection** – Certain sections of SOX state that malicious (willfully and knowingly) destruction or alteration of records may result in substantial financial and criminal penalties for corporate officers of issuing companies or investment companies or the accounting firms that audit these entities.

  A storage system that protects electronically stored records against destruction or unauthorized alteration (for the required retention period) can mitigate the potential for such penalties.

### 1.2 Data Domain Retention Lock Compliance Software Overview

EMC offers a software product named 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 prevents 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 retention requirements, such as those in SOX, and

- **Governance environment:** where the actions allowed by client application or administrative functions would not meet SOX retention 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 edition’s (“Retention Lock Compliance Storage”) capabilities relative to meeting the two pertinent requirement areas of SOX, 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 now regulated by SOX regarding 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 the DD Retention Lock Compliance to meet the pertinent requirements and conditions of SOX, 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 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 SOX requirements that could be met or supported by digital storage systems. In addition, accounting firms or audited entities who 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 SOX.

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. SOX 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 SOX.

The term “record” is utilized to describe all information content that must be retained under SOX and related SEC regulations in order to be consistent with regulatory terminology.

2.1 Storage-related SOX Requirements

There are two functional elements of SOX that can be affected or supported by the capabilities of the DD Retention Lock Compliance:

1. **Records Retention** – meeting the requirements for retaining audit records, and
2. **Destruction Protection** – preventing malicious destruction or alteration of records and thereby mitigating the potential for financial and criminal penalties for corporate officers of issuing companies and registered investment companies.

The following sections present:

- The requirement areas of SOX related to records retention and destruction prevention,
- The capabilities of DD Retention Lock Compliance that support meeting the requirements, and
- Cohasset Associates’ assessment of the degree to which DD Retention Lock Compliance capabilities support meeting the two SOX requirements.
2.1.1 Record Retention

2.1.1.1 Compliance Requirement

SOX requires a seven-year retention of the records produced when a public accountant conducts an audit of the financial records for any publicly traded (issuing) company or registered investment company.

The following are the specific SOX requirements and related SEC rulemaking regarding the retention of records.

SEC. 103. AUDITING, QUALITY CONTROL, AND INDEPENDENCE STANDARDS AND RULES.

(2) RULE REQUIREMENTS – In carrying out paragraph (1), the Board –

(A) shall include in the auditing standards that it adopts, requirements that each registered public accounting firm shall –

(i) prepare, and maintain for a period of not less than 7 years, audit work papers, and other information related to any audit report, in sufficient detail to support the conclusions reached in such report;

SEC. 802. CRIMINAL PENALTIES FOR ALTERING DOCUMENTS.
§1520 Destruction of corporate audit records

(2) The Securities and Exchange Commission shall promulgate, within 180 days, after adequate notice and an opportunity for comment, such rules and regulations, as are reasonably necessary, relating to the retention of relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review, which is conducted by any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j–1(a)) applies.
With reference to SEC. 802, §1520 (2) above, the Securities and Exchange Commission added a rule on January 24, 2003 in 17 CFR Chapter II Part 210 that specifically addresses the record retention requirements of SOX Section 103. It states:

Final Rule: Retention of Records Relevant to Audits and Reviews

January 24, 2003

17 CFR Chapter II Part 210

§ 210.2-06 Retention of audit and review records.

(a) For a period of seven years after an accountant concludes an audit or review of an issuer’s financial statements to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j-1(a)) applies, or of the financial statements of any investment company registered under section 8 of the Investment Company Act of 1940 (15 U.S.C. 80a-8), the accountant shall retain records relevant to the audit or review, including workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents, and records (including electronic records), which:

(1) Are created, sent or received in connection with the audit or review, and

(2) Contain conclusions, opinions, analyses, or financial data related to the audit or review.

(b) For the purposes of paragraph (a) of this section, workpapers means documentation of auditing or review procedures applied, evidence obtained, and conclusions reached by the accountant in the audit or review engagement, as required by standards established or adopted by the Commission or by the Public Company Accounting Oversight Board.

(c) Memoranda, correspondence, communications, other documents, and records (including electronic records) described in paragraph (a) of this section shall be retained whether they support the auditor’s final conclusions regarding the audit or review, or contain information or data, relating to a significant matter, that is inconsistent with the auditor’s final conclusions regarding that matter or the audit or review. Significance of a matter shall be determined based on an objective analysis of the facts and circumstances. Such documents and records include, but are not limited to, those documenting a consultation on or resolution of differences in professional judgment.

The seven-year retention rule was reinforced in the Public Company Accounting Oversight Board Release No. 34-50012; File No. PCAOB-2004-05 dated July 14, 2004.
2.1.1.2 Overview of Retention Lock Compliance Capabilities

DD Retention Lock Compliance has multiple capabilities that support the retention of electronic audit workpaper records produced as a result of an accounting firm complying with SOX. They are summarized below. A more detailed description of these capabilities and their support for retention of SOX records is provided in Section 4.

DD Retention Lock Compliance capabilities:

- A Compliance MTree (a volume of virtual file systems that meets compliance requirements) can be configured that provides a non-erasable, non-rewriteable record file management environment.
- 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 – 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 set that is lower than the Minimum nor higher than the Maximum.
- 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 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.

2.1.1.3 Compliance Assessment

It is Cohasset Associates' opinion that the DD Retention Lock Compliance provides the capabilities that support meeting the record retention requirements of SOX Section 103 and SEC rule 210.2-06.
2.1.2 Preventing Destruction or Alteration of Records

2.1.2.1 Compliance Requirement

There are a number of areas in SOX and related SEC rulemaking that delineate certain monetary and incarceration penalties for officers of issuing companies or investment companies if audit-related records are maliciously destroyed or altered. A storage system that protects electronically stored audit records against malicious (or inadvertent) destruction or alteration would, in turn, mitigate the potential for such penalty situations from occurring. The following titles or sections of SOX describe the situations and penalties related to the destruction or alteration of records.

TITLE VIII—CORPORATE AND CRIMINAL FRAUD ACCOUNTABILITY
SEC. 802. CRIMINAL PENALTIES FOR ALTERING DOCUMENTS.

(a) IN GENERAL.—Chapter 73 of title 18, United States Code, is amended by adding at the end the following: 

§ 1519. Destruction, alteration, or falsification of records in Federal investigations and bankruptcy. Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.

§ 1520. Destruction of corporate audit records

(a)(1) Any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934 (15 U.S.C. 78j-1(a)) applies, shall maintain all audit or review workpapers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.

(b) Whoever knowingly and willfully violates subsection (a)(1), or any rule or regulation promulgated by the Securities and Exchange Commission under subsection (a)(2), shall be fined under this title, imprisoned not more than 10 years, or both.

TITLE XI—CORPORATE FRAUD ACCOUNTABILITY
SEC. 1101. SHORT TITLE.

This title may be cited as the Corporate Fraud Accountability Act of 2002.
SEC. 1102. TAMPERING WITH A RECORD OR OTHERWISE IMPEDING AN OFFICIAL PROCEEDING.

Section 1512 of title 18, United States Code, is amended – (1) by redesignating subsections (c) through (i) as subsections (d) through (j), respectively; and (2) by inserting after subsection (b) the following new subsection: (c) Whoever corruptly (1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both.

2.1.2.2 DD Retention Lock Compliance Capabilities

The DD Retention Lock Compliance has multiple capabilities that prevent the malicious (or inadvertent) destruction or alteration of electronically stored audit work paper records produced as a result of an accounting firm complying with SOX. They are summarized below and more detailed descriptions of these capabilities and their support for protection of SOX records is provided in Section 4.

DD Retention Lock Compliance capabilities:

- A Compliance MTree volume can be configured to establish a non-erasable, non-rewriteable file management environment.

- Any attempt to delete 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 result in an error condition in the system.

- If a DD Retention Lock Compliance 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.

- Should the primary copy of SOX 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.
2.1.2.3 Compliance Assessment

Cohasset believes that DD Retention Lock Compliance, when deployed on a Data Domain system, provides strong capabilities for protecting electronically stored audit records against malicious destruction or alteration – thereby mitigating the potential for executive management of an auditor, issuing company or registered investment company from incurring the monetary and criminal penalties as cited in Sections 802, 1102 and 1103 of SOX.
3. Conclusions

Cohasset’s conclusion is that the EMC Data Domain Retention Lock Compliance edition on an EMC Data Domain system supports meeting requirements in the two areas of SOX that relate to electronic records storage: the retention of records and the mitigation of penalties related to the malicious destruction of audit records.

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

- A records management environment can be established that uses integrated control codes to provide for record retention and to prevent malicious destruction or alteration of electronically stored records.
- Each record can be set to a “read-only” status and a retention period can be associated with each record.
- 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 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 the DD Retention Lock Compliance capabilities that enable it to support meeting certain record retention requirements and providing protection against malicious destruction or alteration of SOX records.

The column labeled “Retention” denotes (with an ✔️) those capabilities of DD Retention Lock Compliance on a Data Domain system that support meeting the requirements for record retention.

The column heading “Protection” denotes (with an ✔️) those capabilities of Retention Lock Compliance on a Data Domain system that support protecting records against malicious (or inadvertent) destruction or alteration.
### 4.1 Establishing a DD Retention Lock Compliance Capable EMC Data Domain Storage System

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- In order to activate the record retention and protection capabilities of DD Retention Lock Compliance, the regulated entity must purchase a unique DD Retention Lock Compliance edition license, which ensures that the “compliance” features of DD Retention Lock are activated.
  - During administrative setup of the DD Retention Lock Compliance, one or more MTrees can be defined as being under Compliance control, thereby allowing retention management to be applied to recorded 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 a 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 an 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 set. The time-based retention expiration date is set when the client application: a) issues a file protocol instruction with an a-time 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 and less than the Maximum defined retention period. The following situations result in an error condition:
  - If the atime retention expiration date supplied by the client application is less than the current date/time, 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 and currently contains locked record files with unexpired retention periods, then the delete command results in an error condition.
### 4.2 Setting a Retention Period

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<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.

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- 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 only be performed by a client application, not by a system administrator.

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- 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.

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- 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.

### 4.3 Administrative Security

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- A Compliance MTree cannot be deleted under any circumstances, not even with Security Officer authorization.

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<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>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

- 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. The primary administrative actions that require a dual 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 Security Officer “dual”
sign-on is allowed for error correction purposes such as the scenario where a 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 Security Officer
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 Security Officer dual sign-on is required to reset the
clock to current time.

### 4.4 Creating a Duplicate or Backup Copy for Recovery

<table>
<thead>
<tr>
<th>Retention</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

• 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 Data Domain system.
  • Should a major error occur that makes the original file system or MTree inac-
cessible, then the record files can be recovered from the replicated copy of
the MTree.
End Notes

1. DD Retention Lock currently supports only 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 DD Retention Lock Compliance enabled MTrees, this attribute is utilized to establish the retention expiration date for a record file.
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.