Gimmal
Information Management for Everyone®

User Guide

Compliance Suite
(Feature-Activated)

For SharePoint 2013/2016/2019

Software Version 4.14.0
December 2020

Contents

1 Introduction

Gimmal delivers market-leading content governance and compliant records solutions built on Microsoft® SharePoint®. Gimmal solutions drive user adoption and simplify information access by making information lifecycle management of content simple and transparent, ensuring consistent compliance and proactive litigation readiness enterprise-wide while lowering costs.

Gimmal's Compliance Suite combines with SharePoint to give your organization a reliable and centralized repository for collaboration and records management that is compliant with the standards of the Department of Defense (DoD) 5015.2 Records Management Program.

1.1 Compliance Suite Features

The Gimmal Compliance Suite software for Microsoft SharePoint is the only product that extends SharePoint to create a Department of Defense (DoD)-certified records management application while maintaining content in SharePoint.

The Compliance Suite features include:

- Record Relationships
  - Enable users, records managers, and administrators to create, move, and copy records
  - Associate policies with a set of records, such as a case, to process all records as a group
  - Manage and link regulatory and legal citations to multiple policies to provide legal justification for the retention process
- Event Management
  - Define and manage events
  - Use events as records disposition criteria
  - Define recurring events
  - Facilitate disposition of related records as a single entity
  - Manage related records through links, associations, and folders ● Disposition Processing
  - Provide processing and approval to start the retention period for records
  - Require approval to perform the disposition action
  - Handle disposition metadata
  - Close folders
  - Handle staged dispositions
  - Provide forensic destruction of records
- Email Record Management
  - Manage email and attachments as records

- o Automate capturing of message metadata
- o Email as single record or separately as different record categories ● Legal Holds
- o Place individual items or entire folders on hold ● Vital and Restricted Records
- o Identify record containers that contain vital records with specific attributes, including review periods and last reviewed date
- o Identify a vital record reviewer
- o Report on past and future vital record collections ● Transfers
- o Configure predefined schema for export
- o Import records into Compliance Suite
- o Export records into validated format, ensuring contextual links
- o Map custom metadata

1.2 Who Should Use this Guide

This manual identifies information that is targeted towards the following users:

- Records manager
- Compliance Suite administrator
- End user
- Local records officer

Beginning and advanced users of the Compliance Suite software should use this guide. All users must have a basic knowledge of SharePoint functionality.

1.3 Important Notes about Compliance Suite and this Manual

The following notes provide important information about the use of Compliance Suite and this manual.

- This manual contains step-by-step instructions for using Compliance Suite.
- All illustrations are for example purposes and vary according to how your installation is configured.

2 Working with Records

Working with Records functionality is available within a **SharePoint Records Center** with Compliance Suite enabled. To use the Working with Records features, Compliance Suite must be installed and the following features must be active:

- For working with Records Site Collection feature, activate these Site Collection features in this sequence:
  - o Gimmal - Record Core - Site Content Types

- o Gimmal Compliance Suite - Base Content Types
- o Gimmal Compliance Suite - Working With Records Site Columns
- For the Working with Records Site feature, activate these Site Collection and Site features in this sequence:
  - o SharePoint Server Publishing Infrastructure
  - o Gimmal Compliance Suite - Security Configuration
  - o Gimmal Compliance Suite - Record Relationship Content Types
  - o Gimmal Compliance Suite - Record Relationship Functionality
  - o Gimmal Compliance Suite - Working With Records

Working with Records builds upon standard SharePoint Records Center and Content Organizer capabilities. Enhanced records management functionality enabled through Working with Records includes:

1. Record Library Configuration

   - Prerequisite for using Working with Records
   - Selecting the **Install and configure default settings** link on the **Library Settings** page will install all Compliance Suite Content Types and enable the Record Library to be used with Working with Records.
   - You must be a Managed Metadata Administrator to perform this function.

2. Creating Record Containers (outside of File Plan Builder)

   - A Record Container is the implementation of a file plan node based on your organization's records management policies.
   - Creation of a new Record Container is enabled through the **New Container** action link within a configured Record Library or Record Container.
   - When a new Record Container is created, a corresponding Filing Location is created in the **Filing Locations** list. See 2.3 Filing Locations for more details.
   - By default you must be a member of the RMA Records Managers SharePoint group to create a new Record Container. However, additional SharePoint user and group permission can be granted on individual Record Containers by editing the Filing Location's **Create Child Containers Members** site column.

Note

System accounts cannot add a new Record Container.

3. Filing Records

- *Filing Records* is the act of creating and storing records based on your organization's records management policies.

- Electronic and Physical Records are supported.

- Creation and filing of a new Electronic Record is enabled through the **Upload Document** action link or the **+Add New Item** link within a Record Container.

- Creation and filing of a new Physical Record is enabled through the New **Non-Electronic Record** action link within a Record Container.

- When a new record is created from the Record Center site, the **Filing Location** site column of the new record determines the *Filing Location* used to apply the Content Organizer rules and the corresponding *Record Container* to store the record.

- Viewing a record's *Filing Locations* is enabled through either the **View Locations** action link under the *Records → Record Locations* heading in the Record Container header ribbon or the **View Record Locations** link on a selected record's action menu.

- Filing a record to a new location is enabled through either the **File to New Location** action link under the **Records → Record Locations** heading in the Record Container header ribbon or the **File Record to New Location** link on a selected record's action menu. *Filing a record to a new location* takes an existing record and links the record into another filing location without removing the current filing location link.

4. Retrieving Records

- Retrieving Records is the act of viewing an existing record's content and metadata.

- Viewing previous record versions is supported.

- Viewing a record's current version is enabled through either the **View Latest Version** action link under the **Records → Record Versions** heading in the Record Container header ribbon or the **View Latest Version** link on a selected record's action menu.

- Viewing all versions for a record is enabled through either the **View Versions** action link under the **Records → Record Versions** heading in the Record Container header ribbon or the **View Record Versions** link on a selected record's action menu.

- Uploading a new version for a record is enabled through either the **Upload Version** action link under the **Records → Record Versions** heading in the Record Container header ribbon or the **Upload New Record Version** link on a selected record's action menu.

5. Copying Records

- Copying Records takes an existing record and creates a duplicate record in another record category.

- Copying a record to a another filing location is enabled through either the **Copy Record** action button under the *Records* heading in the Record Container header ribbon or the **Copy Record** link on a selected record's action menu.

- Copying a record is governed by Content Organizer rules for the record's current filing location.

- When a record is copied, a new audit history is created for the duplicate record.

6. Moving Records

- Moving Records takes an existing record and files the record into another record category while removing the link to the current record category.
- Moving a record to a new filing location is enabled through either the **Move Record** action button under the *Records* heading in the Record Container header ribbon or the **Move Record** link on a selected record's action menu.
- Moving a record is governed by Content Organizer rules for the record's current filing location.
- When a record is moved, the existing record audit history is maintained.

7. Editing Record Metadata

- Editing Record Metadata is the act of updating an existing record's site column (property) values. Cs can limit which roles can edit specific record properties.
- Editing record metadata is enabled through either the **Edit Properties** action button under the *Manage* heading in the Record Container Files Ribbon or the **Edit Properties** link on a selected record's action menu.
- See Metadata Editing help for more details.

The Working with Records functionality described above utilizes Compliance Suite Record Content Types and Record Actions to support the enhanced records management capabilities.

Intended User: End User; Records Manager; Compliance Suite Administrator

2.1 Compliance Suite Record Content Types

Content types enable centralized administration of unique types of records management information. A content type is a reusable collection of metadata (site columns) for a category of record items in a SharePoint list or library. Content types enable users to specify information about an item, in addition to its policies, workflow, or other behavior based on your organization's records management policies.

Compliance Suite Record Content Types build upon standard SharePoint Content Types. The Compliance Suite Content Types include:

- Record Container
- RMA Record
- Correspondence Record
- Digital Photo Record
- Digital Photo Correspondence Record
- Email Record
- Email Upload

- Non-Electronic DoD Record
- Non-Electronic Correspondence DoD Record
- PDF Record
- PDF Correspondence Record
- Scanned Record
- Scanned Correspondence Record
- Web Record

Note

Organizations typically use File Plan Builder to create record containers. Creating a new container here inherits the retention from the parent container.

The following table lists site columns (metadata) unique to the content type.

Table 2-1   Record Container Content Types

Site Column Name	Input Type	Purpose
Specified ID	Single line of text Required: Yes	Unique identifier for each Record Container.
Description	Multiple lines of text Required: No	Descriptive statement that defines the types of records to be filed in the Record Container.
Location	Single line of text Required: No	Pointer to the record's location if is not under direct control of the SharePoint Records Center. For example, location of a file cabinet or a magnetic tape racks.
Disposition Authority	Single line of text Required: Yes	Person or group with legal authorization to manage disposition or transfer to permanent storage of records within the Record Container.
Transfer or Accession to NARA Indicator	Menu Required: Yes	Indicates if the Record Container contains permanent records that are required to be transferred or accession to the National Archives and Records Administration (NARA).

Table 2-1   (Continued) Record Container Content Types

Site Column Name	Input Type	Purpose
Disposition Instruction Name	Single line of text Required: No	Defines the disposition instructions (IMP) and actions that contain the directions for cutting off and carrying out the disposition of records within the Record Container.
Supplemental Markings	Multi-select list *Managed Metadata*: Gimmal RMA Supplemental Marking	Document markings that support the security feature that enables site column content to restrict unauthorized users from accessing records within the Record Container.
Vital Record Review Indicator	Check box and menu (Review Period) Required: Yes	Indicates that the Record Container can contain vital records which are subject to periodic review. If enabled, the Select review period cycle for the vital record(s) is displayed. The **Select review period cycle for the vital record(s)** defines the frequency of periodic reviews for vital records in the Record Container. See Vital Records help for more details.
Vital Record Indicator Inherited	Radio button *Required*: Yes, if Vital Record Review Indicator is selected.	A Record Container can inherit vital record settings from its Parent Record Container or it can specify unique vital record settings. Defaults to *Override* if the Parent Record Container does not have Vital Record Review Indicator selected. Otherwise, it defaults to Inherit from the parent. See Vital Records help for more details.
Vital Record Last Reviewer	User or Group *Required*: Yes if Vital Record Review Indicator is selected.	Person responsible for periodic review of vital records in the Record Container. See Vital Records help for more details.

Table 2-1   (Continued) Record Container Content Types

Vital Record Last Review Date	Date *Required*: Yes if Vital Record Review Indicator is selected.	Date vital records in the Record Container were last reviewed and the date from which the new review date will be calculated. Initial date defaults to the **Creation Date** of the Record Container. See Vital Records help for more details.

Site Column Name	Input Type	Purpose
Vital Record In-Review Indicator	Only displayed when viewing properties.	Indicates if a vital record review workflow is in progress for the Record Container.
Case-Based Retention	Check box Required: No	Indicates that the Record Container contains records that will be processed together for records management tasks such as disposition or holds processing.
Disposition Instructions	Only displayed when viewing properties. System generated based on retention policy.	Lifecycle stages that define duration specifications (e.g., 2 Months) and actions (e.g., Delete Record) to be performed when the duration specification is met.
Action Dates	Only displayed when viewing properties. System generated.	System coded disposition criteria for all future disposition tasks (actions) for records within the Record Container. Enables "As Of" Reporting to retrieve the record container based on its disposition criteria.
Next Action Dates	Date and Time Only displayed when viewing properties. System generated date.	Date the next disposition task (action) will occur for records within the Record Container.

Table 2-1   (Continued) Record Container Content Types

Cutoff Criteria Override	Radio button Required: Yes	Overrides inherited cutoff criteria for the Record Container. Defaults to *Override the cutoff criteria* if the Record Container has a parent Record Container. Otherwise, it defaults to *Inherit from the parent container*.
Cutoff Criteria	Custom Compliance Suite Cutoff Criteria input Required: No	Cutoff criteria for records within the Record Container. Criteria options are Enable Event, Enable Periods, Enable Relationships, Enable Scripts, or a combination of these cutoff options. A Record Container can inherit **Cutoff Criteria** from its Parent Record Container or it can specify unique **Cutoff Criteria**.
Filing Status	Only displayed when viewing properties. System generated.	Indicates if the Record Container has been successfully added to the **Filing Locations** list and is available for filing new records.

2.1.1 RMA Record

Content Type Name: RMA Record

Parent Content Type: Document

Table 2-1   (Continued) Record Container Content Types

Site Column Name	Input Type	Purpose
Subject	Multiple lines of text Required: No	Descriptive statement that defines the purpose of the record.
Date Filed	Date Required: No Displayed as Read only Defaults to the date the record was added to the system.	Date the record was filed into the system and officially became a record.
Publication Date	Date Defaults to the date the record was added or updated in the system. Required: Yes	Date the author or originator completed the development or signed off on the record.

Table 2-1   (Continued) Record Container Content Types

Author	Single line of text Required: No	Person, office or designated position responsible for the creation of the record.
Site Column Name	**Input Type**	**Purpose**
Hold Reason	Multiple lines of text Required: No Only displayed when a hold is placed on the Record Container.	Descriptive statement that defines the purpose of a hold placed on the Record Container.

Description: Represents a physical or electronic record. This is the Compliance Suite parent content type for all record content types (excluding Record Container). It contains the common set of inheritable site columns.

The following table lists site columns (metadata) unique to this content type.

Table 2-2   RMA Record Content Types

Table 2-2   (Continued) RMA Record Content Types

Site Column Name	Input Type	Purpose
Originating Organization	Single line of text Required: No	Office or business unit responsible for creation of the record.
Date Received	Date and Time Required: No	Date and time the record was received for entry into the system.
Addressee(s)	Multiple lines of text Required: No	Organization or individual to whom the record is addressed.
Other Addressee(s)	Multiple lines of text Required: No	Organization of individual to whom the record is copied (CC'd).
Location	Single line of text Required: No	Pointer to the record's location if is not under direct control of the SharePoint Records Center. For example, location of a file cabinet or a magnetic tape racks.
Most Recent Transfer Date	Only displayed when viewing properties. System generated date.	Date the record was successfully transferred into or out of the system.
Record Destruction Date	Only displayed when viewing properties. System generated date.	Date the record was set to be destroyed or retained to long term storage as a part of disposition processing.
Format Type	Managed Metadata Required: No	For electronic records, computer file format described by vendor standards or specifications. For example, Joint Photographic Experts Group (JPEG) or Microsoft Word for Windows. For physical records, physical form such as paper or microfilm.
Media Type	Managed Metadata Required: No	Material or environment on which the record is created. For example, Electronic, Paper, Web, or PDF.

Table 2-2   (Continued) RMA Record Content Types

Supplemental Markings	Multi-select list *Managed Metadata*: Gimmal RMA Supplemental Marking Required: No	Document markings that support the security feature that enables site column content to restrict unauthorized users from accessing the record.

Site Column Name	Input Type	Purpose
Filing Location	Hierarchical selection of Record Containers Required: No	Record Container where the record will be filed in the SharePoint Records Center.
Disposition Instructions	Only displayed when viewing properties. System generated based on retention policy.	Lifecycle stages that define duration specifications (e.g., 2 Months) and actions (e.g., Delete Record) to be performed when the duration specification is met.
Disposition Ready	Only displayed when viewing properties. System generated.	Indicates if the individual record is eligible for disposition. If the record is part of a case-based record container, see the **Disposition Eligible** site column listed below.
Disposition Eligible	Only displayed when viewing properties. System generated.	If the record is part of a case-based record container, this flag indicates if all records within the case-based record container are eligible for disposition.
Action Dates	Only displayed when viewing properties. System generated.	System coded disposition criteria for all future disposition tasks (actions) for the record. Enables "As Of" Reporting to retrieve the record based on its disposition criteria.
Next Action Dates	Only displayed when viewing properties. System generated date.	Date the next disposition task (action) will occur for the record.

Table 2-2   (Continued) RMA Record Content Types

Cutoff Date	Only displayed when viewing properties. System generated date.	Date the record was cutoff and closed.
Cutoff Last Review Date	Only displayed when viewing properties. System generated date. Defaults to **Creation Date**.	Date the record was last reviewed and the date from which the next review date will be calculated.

2.1.2 Correspondence Record

Content Type Name: Correspondence Record

Parent Content Type: RMA Record

Table 2-2   (Continued) RMA Record Content Types

Site Column Name	Input Type	Purpose
Cutoff Last Reviewer	Only displayed when viewing properties. System generated.	Person who was responsible for last cutoff review for the record.
Cutoff Criteria	Custom Compliance Suite Cutoff Criteria Required: No	Cutoff criteria for the record. Criteria options are Enable Event, Enable Periods, Enable Relationships, Enable Scripts, or a combination of these cutoff options. A record can inherit cutoff criteria from its Parent Record Container or it can specify unique cutoff criteria. See Cutoffs help for more details.
Cutoff Review Status	Only displayed when viewing properties. System generated.	Status of cutoff review process for the record.
Has Bulk Updates Pending	Check box Required: No	Indicates if bulk processing updates are pending processing by the RMA Bulk Processing Job.
Site Column Display Name: Confirmation Complete	Displayed only if Bulk Processing has been configured for the content type and selected Record Library.	

Description: Represents an electronic correspondence or memo. The media type for this content type is *Electronic Correspondence*.

No unique site columns (metadata) are assigned to this content type.

2.1.3 Digital Photo Record

Content Type Name: Digital Photo Record

Parent Content Type: RMA Record

Description: Represents an electronic photograph or image. The media type for this content type is *Digital Photo*.

The following table lists site columns (metadata) unique to this content type.

Table 2-3   Digital Photo Record Content Types

Site Column Name	Input Type	Purpose
Caption	Multiple lines of text Required: Yes	Descriptive statement for the digital photo.
Photographer	Single line of text Required: No	Person responsible for origination of the digital photo.
Copyright	Single line of text Required: No	Descriptive statement defining the exclusive legal right of the digital photo.
Bit Depth	Single line of text Required: No	Number of bits used to represent the color of a single pixel in the digital photo.
Image Size	Single line of text Required: No	Width and height of the digital photo.
Image Source	Single line of text Required: No	Originating source of the digital photo.
Compression	Single line of text Required: No	Amount of minimization in size (bytes) of the digital photo to reduce storage size without unacceptable degradation of the quality of the image.
International Color Consortium/Image Color Management (ICC/ICM)	Single line of text Required: No	ICC/ICM color specification.
Exchangeable Image File Format (EXIF) Information	Single line of text Required: No	Additional metadata/tags following the EXIF standard for the digital photo. For example, Manufacturer or FNumber.

2.1.4 Digital Photo Correspondence Record

Content Type Name: Digital Photo Correspondence Record

Parent Content Type: Digital Photo Record

Description: Represents an electronic photograph or image correspondence or memo. The media type for this content type is *Digital Photo*.

No unique site columns (metadata) are assigned to this content type.

2.1.5 Email Record

Content Type Name: Email Record

Parent Content Type: RMA Record

Description: Represents an email message that has been classified in the file plan (Record Category) as a record by an end user. Unlike Email Upload, an Email Record does not use the Email Header Mappings to automatically assign values to select site columns based on the email header information.

The following table lists site columns (metadata) unique to this content type.

Table 2-4   Email Record Content Types

Site Column Name	Input Type	Purpose
From **Note: This is *Author* from RMA Record**	Single line of text Required: No	Email address of the email record author.
To **Note: This is *Addressee(s)* from RMA Record**	Multiple lines of text Required: Yes	Email addresses of the primary recipients of the email record. This can be an email distribution list.
CC **Note: This is *Other Addressee(s)* from RMA Record**	Multiple lines of text Required: No	Email addresses of the secondary recipients of the email record. This can be an email distribution list.

BCC	Multiple lines of text Required: No	Email addresses of the tertiary recipients of the email record. These email addresses are invisible to other recipients. This can be an email distribution list.

Table 2-4   (Continued) Email Record Content Types

Site Column Name	Input Type	Purpose
Date Sent	Only displayed when viewing properties. System generated date.	Date and time when the email record was authored and sent to recipients.
Date Received **Note: This is** *Date Received* **from RMA Record**	Only displayed when viewing properties. System generated date.	Date and time when the email record was received by recipients.
Expanded To	Multiple lines of text Required: No	If **To** is an email distribution list, this site column will store the expanded list of all email addresses included in the email distribution list (group).
Expanded CC	Multiple lines of text Required: No	If **CC** is an email distribution list, this site column will store the expanded list of all email addresses included in the email distribution list (group).
Expanded Bcc	Multiple lines of text Required: No	If **BCC** is an email distribution list, this site column will store the expanded list of all email addresses included in the email distribution list (group).

2.1.6 Email Upload

Content Type Name: Email Upload

Parent Content Type: RMA Record

Description: Represents an email message that has been uploaded and filed into the file plan (Record Category) from the *Email DropZone* library by an end user. Email Upload uses the *Email Header Mappings* to automatically assign values to select site columns based on the email header information. The *Email Header Mappings* is configured by the Compliance Suite Administrator.

After filing as a record in the file plan, an Email Upload item should be changed to *Email Record* to enable records management capabilities.

Email Upload contains an identical set of site columns as Email Record. However, for Email Upload the **To** and **From** site columns are not required. These site column values will be automatically assigned based on the email header.

See Email Management help for more details.

2.1.7 Non-Electronic DoD Record

Content Type Name: Non-Electronic DoD Record

Parent Content Type: RMA Record

Description: Represents a physical record. The media type for this content type is Non-Electronic.

No unique site columns (metadata) are assigned to this content type.

2.1.8 Non-Electronic Correspondence DoD Record

Content Type Name: Non-Electronic Correspondence DoD Record

Parent Content Type: Non-Electronic DoD Record

Description: Represents a physical correspondence or memo. The media type for this content type is *Non-Electronic Correspondence*.

No unique site columns (metadata) are assigned to this content type.

2.1.9 PDF Record

Content Type Name: PDF Record

Parent Content Type: RMA Record

Description: Represents an Adobe PDF record. The media type for this content type is PDF.

The following table lists site columns (metadata) unique to this content type.

Table 2-5   PDF Record Content Types

Site Column Name	Input Type	Purpose
Producing Application	Single line of text Required: Yes	Application used to render content to PDF.

Producing Application Version	Single line of text Required: Yes	Application version used to render content to PDF.
PDF Version	Single line of text Required: Yes	Version of portable document format (PDF) used to render record content.
Creating Application	Single line of text Required: No	Application (including version) used to create initial record content.

Table 2-5   (Continued) PDF Record Content Types

Site Column Name	Input Type	Purpose
Document Security Settings	Single line of text Required: No	Security set in the PDF record. This is not SharePoint security, it is security set within the PDF record content.

2.1.10 PDF Correspondence Record

Content Type Name: PDF Correspondence Record

Parent Content Type: PDF Record

Description: Represents an Adobe PDF correspondence or memo. The media type for this content type is PDF.

No unique site columns (metadata) are assigned to this content type.

2.1.11 Scanned Record

Content Type Name: Scanned Record

Parent Content Type: RMA Record

Description: Represents a physical record that has been scanned to an electronic record. The media type for this content type is Scanned Image.

The following table lists site columns (metadata) unique to this content type.

Table 2-6   RMA Record Content Type

Site Column Name	Input Type	Purpose

| Image Resolution | Single line of text Required: Yes | Number of pixels in the scanned record. The higher the resolution the more image detail.

For example, 72 pixels per inch (ppi). |
| Image Bit Depth | Single line of text Required: No | Number of bits used to represent the color of a single pixel in the scanned record. |
| Scanned Image Format and Version | Managed Metadata Required: No | Image standard and version for the scanned record. For example, GIF (87a) or TIFF (4.0). |

2.1.12 Scanned Correspondence Record

Content Type Name: Scanned Correspondence Record

Parent Content Type: Scanned Record

Description: Represents a physical record that has been scanned to an electronic correspondence or memo. The media type for this content type is *Scanned Image*.

No unique site columns (metadata) are assigned to this content type.

2.1.13 Web Record

Content Type Name: Web Record

Parent Content Type: RMA Record

Description: Represents a web page that is classified as an electronic record. The media type for this content type is *Web*.

The following table lists site columns (metadata) unique to this content type.

Table 2-7   Web Record Content Type

Site Column Name	Input Type	Purpose
Web File Name	Single line of text with format validation Required: No	Name of the web record file that was published to the web site. For example, default.aspx.
Web Platform	Single line of text Required: No	Technical platform used to render the web record. For example, IIS.
Web Site Name	Single line of text Required: No	Name of the website that contains the published web record.

Web Site Uniform Resource Locator (URL)	Single line of text Required: No	Address on the world wide web of the published web record.
Capture Method	Single line of text Required: No	Process for capturing a snapshot (moment in time) of the published web page. This snapshot is the web record.
Capture Date	Date and Time Required: No	Date the snapshot (moment in time) of the web page was taken.
Contact	Single line of text Required: No	Person responsible for maintaining the published web page.

Table 2-7   (Continued) Web Record Content Type

Site Column Name	Input Type	Purpose
Content Management System	Single line of text Required: No	Authoring system used to manage the published web page.

2.1.14 Web Correspondence Record

Content Type Name: Web Correspondence Record

Parent Content Type: Web Record

Description: Represents a web page that is classified as an electronic correspondence or memo. The media type for this content type is Web.

No unique site columns (metadata) are assigned to this content type.

2.2 Initiating Record Actions

Compliance Suite Working with Records supports initiating record actions through either:

- *header ribbon*: Record action buttons on the header ribbon of configured Record Libraries and Record Containers.
- *Record Action Menu*: Contextual record action links accessible through a Record Container or Record Item action menu.

2.2.1 Files Ribbon

The **Files** ribbon displays in the top navigation of a Record Library or Record Container.

To access the **Files** ribbon:

1. Open a **SharePoint Records Center**. The *Records Center Home Page* opens.
2. Select **Libraries** from the Quick Launch and then the desired Library when Site Contents display.

   You see a list of all items contained within the selected Library.
3. Select the **Files** tab in the top navigation.
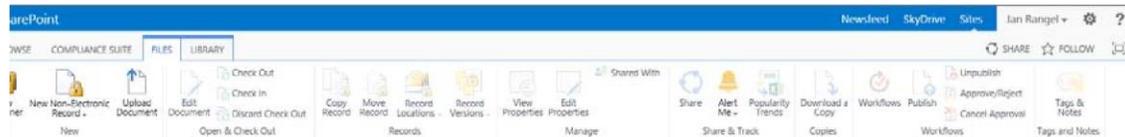
Figure 2-1 Files Tab

2.2.2 Record Action Menu

The *Record Action Menu* is displayed contextually as a list of links associated to a record item.

To access the Record Action Menu:

1. Open a **SharePoint Records Center**. The *Records Center Home Page* opens.
2. Select **Libraries** from the Quick Launch and then the desired Library when Site Contents display.

   You see a list of all items contained within the selected Library.
3. Select a *Record Container* or *Record Item* from Library.
4. Click (**…**) twice to display the Record Relationship Action Menu.
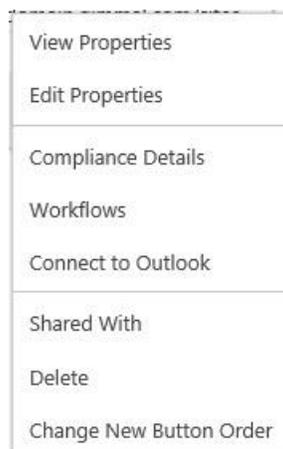
Figure 2-2 Record Action Menu

All record action links displayed for a *Record Container* are standard SharePoint actions. There are no Compliance Suite-specific record actions.

5. If a *Record Item* is selected, the following menu displays:
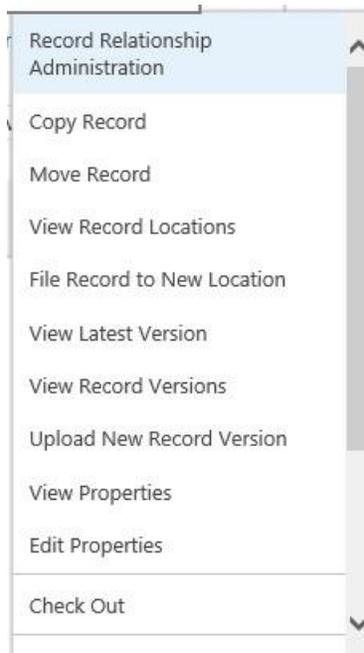
Figure 2-3 Record Relationship Administration Menu

2.3 Filing Locations

Filing Locations are SharePoint items that support the classification of records into your organization's File Plan. Classifying records correctly into the File Plan is an essential component of a successful records management program.

In addition to the classification of records, Filing Locations also support:

- Granting Access to Create Child Record Containers
- Closing of Filing Locations

Filing Locations are implemented through using *Record Containers*.

Compliance Suite uses the following for the implementation of Filing Locations:

- *Record Container*: Each Filing Location corresponds to a *Record Container* which is the actual SharePoint Records Center storage location of the record.

- *Record Item*: Filing Location: A record's **Filing Location** site column maps the record to the *Filing Location* which then maps to a corresponding *Record Container* to properly classify the record.

- *Filing Locations Items and List*: Updating and viewing Filing Locations. From this list, you can configure access for child container creation within a Filing Location's corresponding Record Container. In addition, you can close the Filing Location.

Intended User: Records Manager

To access the **Filing Locations** list:

1. Open a **SharePoint Records Center**. The **Records Center** home page opens.

2. Select **Libraries** from the Quick Launch and then the desired list when Site Contents display.

3. Select the **Filing Locations** list. You see a list view of all Filing Locations defined within your Site Collection.

The following table describes the **Filing Locations** list with a description of each heading.

Table 2-8 Filling Locations Headings

List View Heading	Description
Filing Location	Path of the corresponding *Record Container*. This is the Record Container that will contain records that use this filing location.
Is Closed	Defines if the Filing Location is closed. If a Filing Location is *Closed*, records cannot be classified into the Filing Location and new child Record Containers cannot be created within the corresponding *Record Container*.
Create Child Containers Members	List of users and/or groups that have access to create child *Record Container(s)* within the Filing Location's corresponding *Record Container*. By default, any user that is a member of *RMA Records Managers* SharePoint group can create new child *Record Containers*. This expands that access to additional selected users and/or groups.

2.3.1 Creating a Filing Location

Before records can be classified in the File Plan (Record Categories), a Filing Location must be created.

Filing Locations are system generated when a new *Record Container* item is created. There are two ways to initiate the creation of a new Record Container:

- File Plan Builder and Instantiation

- *New Container* record action button in the header ribbon Filing

Locations should **not** be manually created by a user.

2.3.2 Granting Access to Create Child Record Containers

Filing Locations support granting selected users and group access to create child *Record Container(s)* within the corresponding *Record Container*. By default, any user that is a member of *RMA Records Managers* SharePoint group can create new child *Record Containers*. This expands that access to additional selected users and/or groups.

To grant additional access to create child Record Containers, you must edit the Filing Location item:

1. From the **Filing Locations** list, select the Filing Location you want to edit. Only one Filing Location can be selected at a time.

2. Select the Items tab to display the header ribbon.
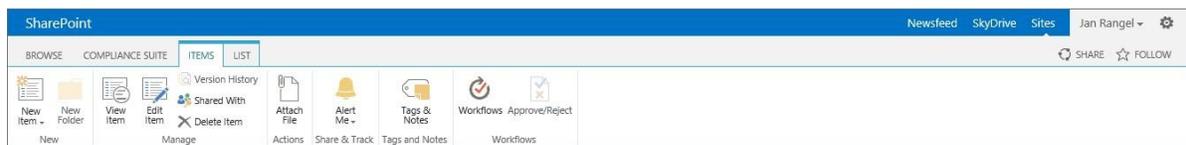
Figure 2-4 Filing Locations header ribbon

3. Select Edit Item on the header ribbon. The Filing Location Edit dialog box opens displaying the selected Filing Location details.
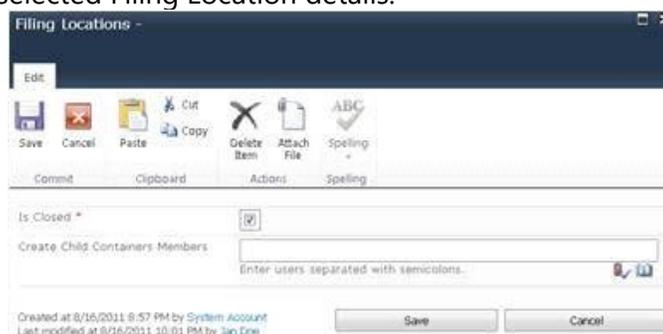
Figure 2-5 Filing Location Edit dialog box

4. Enter the Create Child Containers Members.

   There are two ways to add users or groups to **Create Child Containers Members**:

   - Semicolon-separated list
   - Standard SharePoint address book lookup

5. Click **Save** to update the Filing Location. The changes display in the *Filing Location* list. Click **Cancel** to return to the *Filing Location* list without updating the selected Filing Location.

After the Filing Location change is saved, the users and/or groups defined in the **Create Child Containers Members** field are granted permission to create new child Record Containers within the Filing Location's corresponding Record Container.

2.3.3 Closing a Filing Location

Filing Locations support closing of Filing Locations. When a Filing Location is closed, records cannot be classified into the Filing Location and new child Record Containers cannot be created within the corresponding *Record Container*.

15 January 2019

Note:

Closure of a record container can also happen during the Cutoff Process for a CBR container.

To close a Filing Location, you must edit the Filing Location item:

1. From the **Filing Locations** list, select the Filing Location you want to edit. Only one Filing Location can be selected at a time.

2. Click the **Items** tab to display the header ribbon.
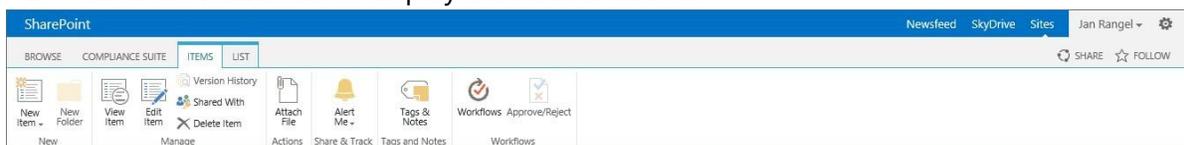
Figure 2-6 Filing Locations Header Ribbon

3. Click **Edit Item** on the header ribbon. The **Filing Location Edit** dialog box opens displaying the selected Filing Location details.
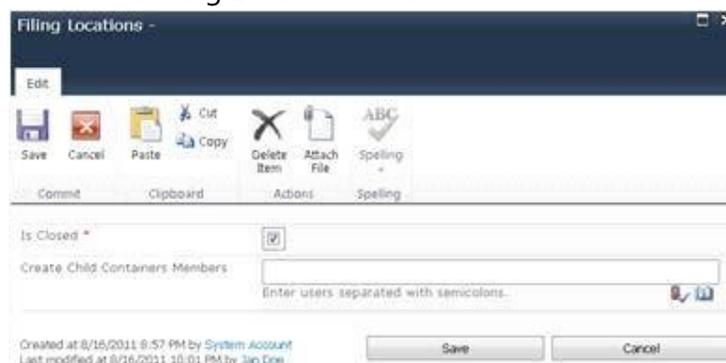
Figure 2-7 Closing a File Location

4. (**Required**) Select **Is Closed**.

5. Click **Save** to update the Filing Location. The changes display in the *Filing Location* list. Click **Cancel** to return to the *Filing Location* list without updating the selected Filing Location.

6. If **Is Closed** was selected,

   - The Filing Location does not appear as an option in the **Filing Location** field on a *Record Item*.

   - The Filing Location's corresponding Record Container updates to display a new icon, .

- New child Record Containers cannot be created within the Filing Location's corresponding Record Container.

2.4 Metadata Editing

Metadata is information about data or other information. Formal metadata help organize and maintain an organization's internal investment in data and provide information to aid data transfers. Once metadata has been created, some of the information it contains changes in time. Compliance Suite Administrators can edit an organization's metadata to change the information.

Metadata editing functionality is available within a **SharePoint Records Center** with **Compliance Suite** enabled. Compliance Suite Administrators can further secure metadata fields by adding fields to the **GimmalSoft Column Access Control** list.

Compliance Suite Administrators can add authorized metadata editors via the *GimmalSoft Column Access Control* site columns to control who can modify a record's metadata. Only users who are members of the *RMA Administrators* group can create metadata editing rules. The rule definition identifies metadata editors who can modify a record's metadata. A metadata rule is defined by three pieces of information: the Field Name; metadata editors; and list exceptions. When a rule exists for a metadata field of stored records, *GimmalSoft Column Access Control* presents the property as uneditable field on the edit screen to unauthorized users, i.e., users who are not listed in the metadata editors' field. Compliance Suite Administrators can also add Metadata Security List Exceptions. Metadata Security List Exceptions are names of lists or libraries for which the rule should be ignored. If a record has a metadata rule for a property, but it exists in a library that is part of the exclusion list, any user with write access can modify the value.

Intended User: Compliance Suite Administrator

The following table describes the **GimmalSoft Column Access Control All Items View** list with a description of each heading.

Table 2-9   GimmalSoft Column Access Control Headings

List View Heading	Description
Edit	Click the **Edit** icon to access the *GimmalSoft Column Access Control* edit dialog box.
Field Name	Unique identifier located after the Field equals sign (Field=) at the end of the column name's URL. For example, in the URL `http://mysite/FldEdit.aspx?List=%7D&Field=OriginatingOrganization`, the field name is **Originating Organization**.
Metadata Editor	Individual(s) authorized by Compliance Suite Administrators to modify the record metadata field(s). The field is uneditable to all users other than those listed in the Metadata Editor field.

Table 2-9   (Continued) GimmalSoft Column Access Control Headings

List View Heading	Description
Metadata Security List Exceptions	Identifies all lists and libraries for which the rule will not be applied. If a metadata rule for a record's field exists, but the record resides in one of these lists or libraries, the rule is ignored and the default system security is applied.

2.4.1 Adding a Field Name to the GimmalSoft Column Access Control List

Compliance Suite Administrators can edit metadata fields by adding field names to the *GimmalSoft Column Access Control* list. Field names are used because their value does not change even when the display name is altered. To identify the field name, Compliance Suite Administrators must access the Site Settings. This requires Compliance Suite Administrators to also be members of the Site Owner security group.

Note: The field name entered for access control items must be the internal name of the field.

To add a field name to the GimmalSoft Column Access Control list:

1. Open a **SharePoint Records Center**. The *Records Center Home Page* opens.

2. Click **Libraries** in the Quick Launch. When the Site Contents display, select the Library that you want to edit.

3. Click the **Library** tab in the header ribbon and click **Library Settings**.
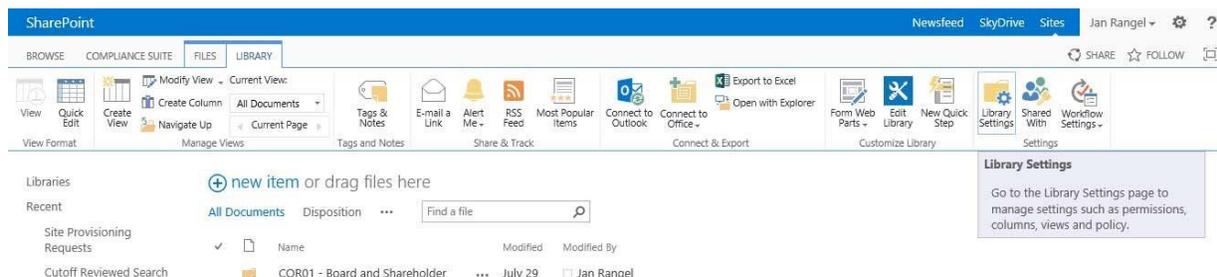
Figure 2-8 Library Settings Button

4. The *Settings* screen opens. Scroll down to the *Columns* list.

5. Find the internal column name you want to edit. To find the internal column name:

   - Maximize the browser window to increase the status bar real estate and hover over the column you want to configure. The URL of the field name of the column is displayed at the bottom of the screen in the status bar. The field name is the unique identifier located after the Field *equals* sign (*Field=*) at the end of the URL.

Figure 2-9 Columns List

- Hover over the column that you want to edit. Right-click and select **Copy Shortcut** from the menu. Open Notepad and paste the URL into the Notepad document. The field name is the unique identifier located after the Field *equals* sign (*Field=*) at the end of the URL.

- Open Notepad and paste the URL into the Notepad document. The field name is the unique identifier located after the Field *equals* sign (*Field=*) at the end of the URL.

6. Scroll to the top of the Library Settings screen and click on the **Lists** link on the left pane of the screen.

7. The **Lists** window displays. Click the **GimmalSoft Column Access Control** link.

Figure 2-10 GimmalSoft Column Access Control

8. The *GimmalSoft Column Access Control - All Items* screen opens. There are two ways to add a new field name.

- Click **+Add new item** from the bottom of the list.

- Click the **Items** tab.

- In the header ribbon, select **New Item** and then **New Item** again.

9. The GimmalSoft Column Access Control - New Item dialog box opens with fields for creating a new GimmalSoft Column Access Control item.

Figure 2-11 GimmalSoft Column Access Control - New Item Dialog Box

10. (**Required**) Enter the field name in the **Field Name** field.

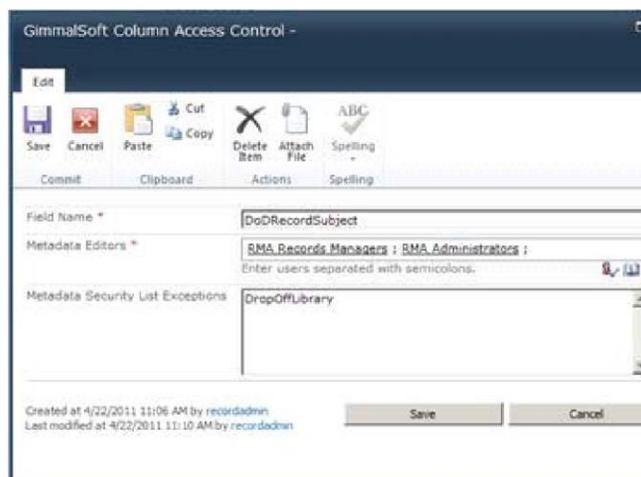11. (**Required**) Enter the metadata editor(s) in the **Metadata Editors** field by adding name(s) or group(s) via the People Picker. Metadata editors can designate fields in the *GimmalSoft Column Access Control* Field Name edit screen as noneditable to unauthorized users.

12. Enter the metadata security list exceptions in the **Metadata Security List Exceptions** field. Metadata Security List Exceptions will exclude the rule definitions from being applied, which will allow users who are not editors to update a column. The list or library name is contained in the library's URL located in the *Library Settings* screen. The list or library name directly follows the web address. For example, the list or library name of the URL `https://sp2013.yourcompany.com/DropOffLibrary/Forms/AllItems.aspx` is *DropOffLibrary*. You must enter the list or library name exactly as it is displayed in the URL. *DropOffLibrary* is the default exception.

Note:

Any custom columns added directly to libraries must also be added to the *DropOffLibrary* if you want them to appear during initial record creation.

---

13. Click **Save** to create the new GimmalSoft Column Access Control item. It is displayed in the *GimmalSoft Column Access Control - All Items* list.

    Or

    Click **Cancel** to return to the *GimmalSoft Column Access Control - All Items* list without creating a new item.

2.4.2 Editing Record Metadata

Metadata editors previously added to edit selected fields in the *GimmalSoft Column Access Control* Edit Field dialog box can edit those fields in the record's *Edit Properties* dialog box.

1. There are two ways in which you can access the *Edit Properties* dialog box.

   - From the target Library's *All Documents* screen, select the record you want to edit. Only one item can be selected at a time. Click the **Files** tab and then click the **Edit Properties** button.
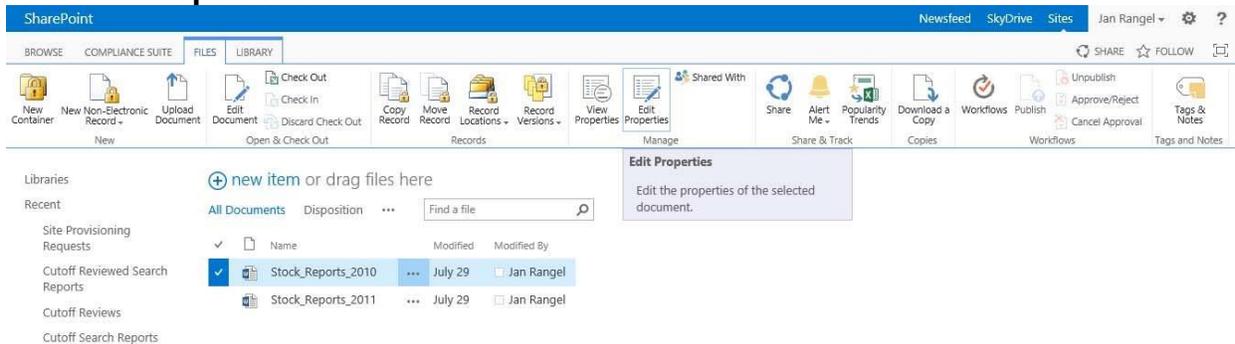

Figure 2-12 Edit Properties Selection

   - Select **Edit Properties** from the action menu for the record.
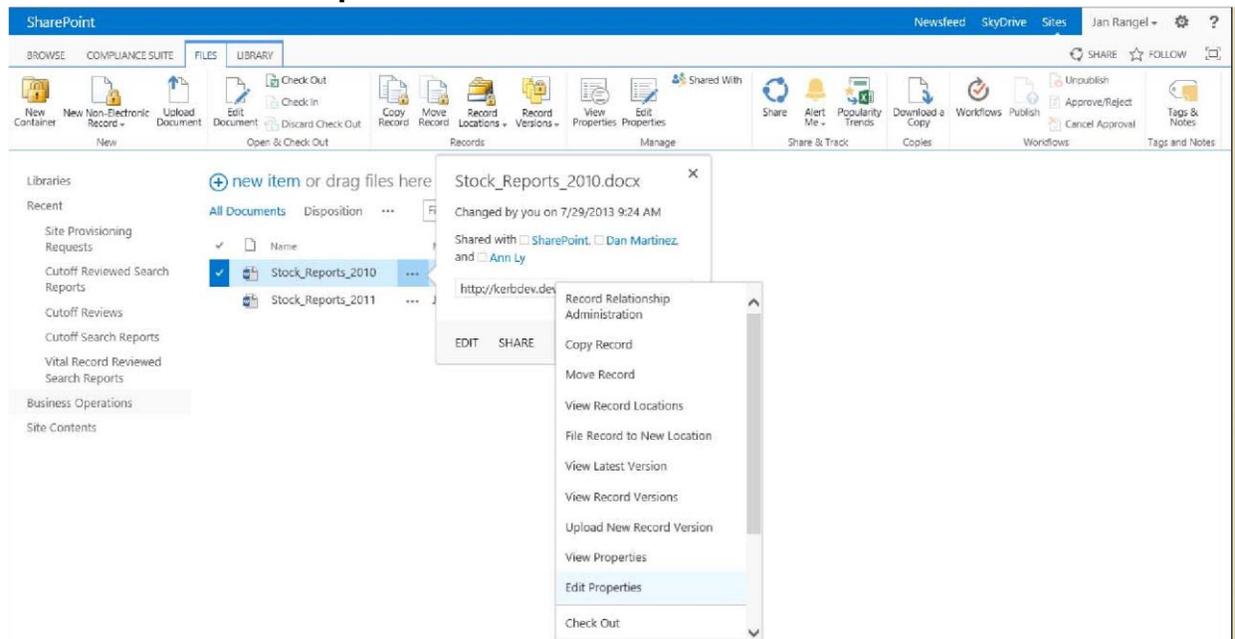
Figure 2-13 Action Menu: Edit Properties

2. The **Edit Properties** dialog box opens. Update the information in the fields that you want to change. Field names that Compliance Suite Administrators have designated in the **GimmalSoft Column Access Control** list are displayed on the edit screen as noneditable fields to unauthorized users. These users can alter any value except the one that is secured by GimmalSoft Column Access Control.

Figure 2-14 Edit Properties dialog box

3. Click **Save** to update the item. It is displayed in the GimmalSoft Column Access Control list. Click **Cancel** to return to the GimmalSoft Column Access Control list without updating the selected item.

2.4.3 Viewing Details of a GimmalSoft Column Access Control List Item

To view the details of an existing GimmalSoft Column Access Control list item, you must view the item.

1. From the **GimmalSoft Column Access Control** list screen, select the list item you want to view. Only one list item can be selected at a time. Then click the **Items** tab.
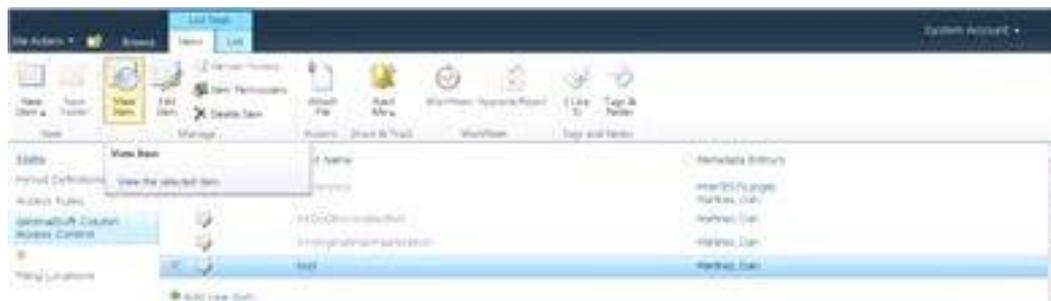
Figure 2-15 Items Tab

2. Click the **View Item** button on the header ribbon. The **GimmalSoft Column Access Control View** dialog box opens displaying the list item details in read-only mode.

Figure 2-16 Viewing the GimmalSoft Column Access Control

3. From the **GimmalSoft Column Access Control View**, Compliance Suite Administrators can edit, delete, or manage permissions of the selected list item.

4. Click **Close** to return to the **GimmalSoft Column Access Control** list dialog box.

2.4.4 Deleting a GimmalSoft Column Access Control Item

To remove an existing list item from the *GimmalSoft Column Access Control* list, you must delete the item.

1. From the *GimmalSoft Column Access Control* screen, select the list item(s) you want to delete; then click the **Items** tab.
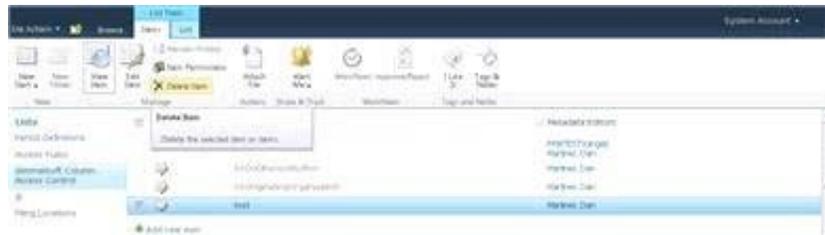
Figure 2-17 Items Tab

2. Select **Delete Item** button on the header ribbon. A prompt opens asking **Are you sure you want to send the item(s) to the site Recycle Bin**?

3. Click **OK** and the list item(s) is deleted and removed from the **GimmalSoft Column Access Control** list or click **Cancel** to return to the **GimmalSoft Column Access Control** list without deleting the selected item(s).

Note:

If a metadata rule definition is removed, users who have write access to the item that contains a field that was managed by the deleted rule will be able to modify its value.

3 Restricted Records Access

Restricted Records Access functionality is available within a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Restricted Records Access features, Compliance Suite must be installed and the Gimmal Compliance Suite - Restricted Records Access feature must be active.

Restricted Records Access provides the functionality to define custom security for Record Container(s) and/or Record Item(s) based on the content of SharePoint site columns. It supports userdefined Access Rules to grant only authorized users access to Record Container(s) and/or Record Item(s) based on the content of SharePoint site columns.

Restricted Records Access functionality is used to support:

- Supplemental Markings
- Access-Constrained Columns

Compliance Suite uses *Access Rules* items to implement Restricted Records.

SharePoint site columns used in Restricted Records Access must be of type *Access Constrained* or *Supplemental Markings* and use Access Rules items for content validation. By default, the SharePoint site column Supplemental Markings, which is a Supplemental Markings type, is available. SharePoint site columns used as Access-Constrained Columns are defined by the Compliance Suite administrator based on your organization's record management policies.

Intended User: Records Manager, Compliance Suite Administrator

3.1 Supplemental Markings

Supplemental Markings are security features to restrict unauthorized users from accessing Record Container(s) and/or Record Item(s) based on the content of a SharePoint site column. When Supplemental Markings are assigned to Record Container(s) and/or Record Item(s), the Supplemental Markings restricts access to only authorized users based on the item's Supplemental Markings site column value(s) even if the unauthorized user had access to the specific item under normal circumstances.

Supplemental Markings are unique from Access-Constrained Columns through the implementation of the access restriction rules and the SharePoint site column type assigned as follows.

- SharePoint Site Column

    o The Supplemental Markings site column is installed on Record Container and Record Item content types.

    o Supplemental Markings site column type. This site column type allows a user to select multiple values based on Access Rules configured for each Supplemental Markings managed metadata term.

- Access Rules

  - Supplemental Markings access restrictions settings are configured through a SharePoint Access Rules content type.

  - A Records Manager creates an Access Rule item for each Supplemental Markings Site Column Value and Authorized Users combination as described in 3.4 Access Rules.

- Site Column Metadata Assignment

  - An authorized user assigns values for a Record Container and/or Record Item Supplemental Markings site column.

  - The displayed Supplemental Markings site column value options are based on the Access Rules configured for each Supplemental Markings managed metadata term.

3.1.1 Supplemental Markings Access Restriction Rules

When a Record Container and/or Record Item has more than one Supplemental Markings value assigned, the user must be an authorized user for all Supplemental Markings values to access the records.

For Record Containers and Record Items that are assigned Supplemental Markings values, the access restrictions are applied as follows:

1. Record Containers

   - Applied to the Record Container itself

   - Applied to all Record Items within the Record Container

   - Access restrictions not applied to Record Containers within the selected Record Container

2. Record Items

   - Applied to the Record Item itself

   - Supplemental Markings applied to the Record Item further restrict any access restrictions applied on the Record Item's Record Container

3.1.2 Supplemental Markings Example

This example describes records' access restrictions based on Access Rules applied to Supplemental Markings values assigned to example Record Containers. The example is broken into two parts:

- Access Rules: Supplemental Markings Values and Authorized Users

- Record Container Assignment: Values and Access Restriction

Access Rules: Supplemental Markings Values and Authorized Users

Table 3-1 defines the Access Rules for the Supplemental Markings values and Authorized Users for this example. Each row in the table represents an Access Rule item.

Table 3-1 Access Rule Supplemental Markings and Authorized Users

Access Rule Name	Supplemental Markings Value	Authorized Users
Restricted Data Access Rule	Restricted Data	Jan Doe
Formerly Restricted Data Access Rule	Formerly Restricted Data	Jan Doe; Jim Brown
Originator Controlled Access Rule	Originator Controlled	Jan Doe; John Smith; Jane Smyth

These Access Rules allow only the Authorized Users access to any Record Containers assigned the corresponding Supplemental Markings value. For Supplemental Markings, an Authorized User must be assigned to the Access Rule for all corresponding Supplemental Markings values to be granted access to the Record Container.

Record Container Assignment: Values and Access Restriction

Building on the Access Rules created for the example Supplemental Markings values listed in Table 3-1, Table 3-2 defines the example Record Containers and subsequent access restrictions based on the assigned Supplemental Markings for each Record Container. Each row in the table represents a Record Container.

Table 3-2 Record Container Access Restrictions

Record Container Name	Assigned Supplemental Markings Value(s)	Users with Authorized Access
Record Container A	Originator Controlled	Jan Doe, John Smith, and Jane Smyth
Record Container B	Restricted Data; Formerly Restricted Data; Originator Controlled	Jan Doe; Jim Brown **Note**: Only Jan Doe is granted access because she is the only user assigned as an Authorized User for Restricted Data, Formerly Restricted Data, and Originator Controlled Access Rules.

Only *Users with Authorized Access* are granted permission to access the Record Container and the Records within the Record Container.

3.2 Access-Constrained Columns

Access-Constrained Columns provide a security feature to restrict unauthorized users from accessing Record Container(s) and/or Record Item(s) based on the content of SharePoint site column(s). When Access-Constrained Columns are assigned to Record Container(s) and/or Record Item(s), the Access-Constrained Column restricts access to only authorized users. This restriction is based on the item's Access-Constrained Site Column value(s), even if the unauthorized user had access to the specific item under normal circumstances.

Access-Constrained Columns are unique from Supplemental Markings through the implementation of the access restriction rules and the SharePoint site column type assigned.

In Compliance Suite, Access-Constrained Columns are implemented through the following functionality:

1. SharePoint Site Column

   - Access-Constrained Columns are SharePoint site columns defined by the Compliance Suite Administrator.

   - Access-Constrained Columns can be applied to *Record Container* and/or *Record Item* content types.

   - *Access-Constrained* site column type allows a user to select single or multiple values based on *Access Rules* configured for each Access-Constrained site column managed metadata term.

2. Access Rules

   - Access-Constrained Columns access restrictions settings are configured through a SharePoint *Access Rules* content type.

   - A Records manager creates an Access Rule item for each Access-Constrained Column Site Column Value and Authorized Users combination as described in the Access Rules help documentation.

3. Site Column Metadata Assignment

   - An authorized user assigns values for a Record Item Access-Constrained Site Column Name.

   - The displayed Access-Constrained Site Column Name value options are based on the Access Rules configured for each Access-Constrained site column managed metadata term.

3.2.1 Access-Constrained Columns Access Restriction Rules

When a *Record Container* or *Record Item* has more than one value assigned for a single **Access-**

Constrained Site Column Name, the user must be an authorized user for only one of the Access-Constrained **Site Column Name** values to access the records. **This is a critical difference between how Supplemental Markings and Access-Constrained Columns work.**

When a *Record Container* or R*ecord Item* has values assigned to more than one **Access-Constrained Site Column Name**, the user must be an authorized user for at least one value for each of the **Access-Constrained Site Column Name** site columns to access the records.

For *Record Containers* and *Record Items* that are assigned Access-Constrained Columns values, the access restrictions are applied as follows:

1. Record Containers

   - Applied to the Record Container itself

   - Applied to all Record Items within the Record Container

   - Access restrictions *not* applied to Record Containers in the selected Record Container

2. Record Items

   - Applied to the Record Item itself

   - Access-Constrained Columns applied to the Record Item further restrict any access restrictions applied on the Record Item's Record Container

3.2.2 Access-Constrained Columns (ACC) Example

This example describes records' access restrictions based on Access Rules applied Access-Constrained Columns values assigned to example Record Containers. The example is broken into two parts:

   - Access Rules: Access-Constrained Columns Values and Authorized Users

   - Record Container Assignment: Values and Access Restriction

Access Rules: Access-Constrained Columns Values and Authorized Users

Table 3-3 defines the Access Rules for the Access-Constrained Columns values and Authorized Users for this example. Each row in the table represents an Access Rule item. The Access-Constrained Site column in this example was added to the Record Container content type.

Table 3-3 Access Rule Constrained Columns and Authorized Users

Access Rule Name	ACC Name	ADD Value	Authorized Users
Florida Access Rule	State	Florida	Jan Doe
New York Access Rule	State	New York	Jan Doe; Jim Brown
Texas Access Rule	State	Texas	Jan Doe; John Smith; Jane Smyth

Compliance Suite Access Rule	Project	Compliance Suite	Jan Doe; Jim Brown
Governance Suite Access Rule	Project	Governance Suite	Jan Doe; John Smith; Jane Smyth

These Access Rules are used to allow only the Authorized Users access to any Record Containers assigned the corresponding Access-Constrained Columns name and value pairs.

Record Container Assignment: Values and Access Restriction

Building on the Access Rules for the example **Access-Constrained Columns** names and values listed in Table 3-3, Table 3-4 defines the example Record Containers and subsequent access restrictions based on the assigned **Access-Constrained Columns** for each example Record Container. Each row in the table represents a Record Container.

Table 3-4 Record Containers and Access-Constrained Columns

Record Container Name	Assigned State Column Values	Assigned Project Column Values	Users with Authorized Access
Florida Access Rule	State	Florida	Jan Doe
New York Access Rule	State	New York	Jan Doe; Jim Brown
Texas Access Rule	State	Texas	Jan Doe; John Smith; Jane Smyth
Compliance Suite Access Rule	Project	Compliance Suite	Jan Doe; Jim Brown
Governance Suite Access Rule	Project	Governance Suite	Jan Doe; John Smith; Jane Smyth

Only *Users with Authorized Access* are granted permission to access the Record Container and the Records within the Record Container.

3.3 Supplemental Markings and Access-Constrained Columns

If a *Record Container* or *Record Item* is assigned both **Supplemental Markings** and **Access-Constrained Columns** values, access restriction rules for both features must be met for an authorized user to have access to the *Record Container* or *Record Item*. See the Supplemental Markings and Access-Constrained Columns help sections for more details on feature specific access restriction rules.

3.4 Access Rules

Compliance Suite supports user-defined Access Rules. Access Rules are the SharePoint items that support the implementation of Restricted Records Access for *Supplemental Markings* and *AccessConstrained Columns*. Access Rules are used to grant only authorized user's access to *Record Container(s)* and/or *Record(s)* based on the content of SharePoint site columns.

Compliance Suite provides the ability to create, edit, view, or delete access rules using a SharePoint list.

Intended User: Records Manager

To access the **Access Rules View** list:

1. Open a Compliance Suite-enabled SharePoint Records Center. The Records Center Home Page opens.
2. Select **Site Contents** and then **Access Rules** in the Quick Launch.

   The Access Rules page displays with any access rules defined in your Site Collection.

Table 3-5 describes the **Access Rules View** list with a description of each heading.

Table 3-5 Access Rules View

List View Heading	Description
Title	Descriptive name that differentiates the Access Rule from other Access Rules in the **Access Rules View** list.
Description	Descriptive statement used to further differentiate the Access Rule from other Access Rules
Access Rule	SharePoint Site Column and Site Column Value combination for the Access Rule item. It is displayed as Site Column=Site Column Value. The Site Column defines the SharePoint site column that will be used to restrict records access. The valid site columns are of the type Supplemental Markings or Access-Constrained. The Site Column Value defines the Managed Metadata value that restrict records access for the selected Site Column. Example: Supplemental Markings=Restricted Data

Authorized Users	List of users or groups that have access to view Record Container(s) and/ or Record Item(s) that have metadata equal to the Access Rule as described previously. Only users in this list can select the Access Rule: Site Column and Value combination when creating or editing Record Container(s) and/or Record Item(s).
	The rules for Authorized Users access varies based on the type (Supplemental Markings or Access-Constrained) of the Access Rule: Site Column. For more details, see the Supplemental Markings and AccessConstrained Columns help.
Modified	When the access rule was last modified.
Modified By	Compliance Suite user name of the user who last modified the rule.

Note

Do not change the name of a site column that is referenced as part of an access rule; the rule will not reflect the change. If renaming a site column is necessary, all access rules, along with the site column values, must be recreated to reflect the change.

3.4.1 Creating an Access Rule

Before access restrictions are applied to a Record Container or Record Item through Supplemental Markings or Access-Constrained Columns, an Access Rule must be created. To create an access rule:

1. From the **Access Rules View**, click **Add new item**.

   The **Access Rules - New Item** dialog box opens with fields for creating a new Access Rule.

Figure 3-1 Access Rules New Item Dialog Box

2. (**Required**) Enter the **Title**. The **Title** is a **descriptive** identifier for the new Access Rule.

3. Enter a **Description**. The Description is a descriptive statement that defines the purpose of this Access Rule.

4. (**Required**) Select the **Access Rule: Site Column**. The **Access Rule: Site Column** defines the SharePoint site column used to restrict records access based on this Access Rule. The selection list is populated with all SharePoint site columns that are of the type *Supplemental Markings* or *Access-Constrained*. By default, site column *Supplemental Markings* are available.

5. (**Required**) Select the **Access Rule: Site Column Value** that must be unique across all Access Rules. The **Access Rule: Site Column Value** defines the Managed Metadata term that restricts records access for the selected **Access Rule: Site Column**. The selection options are defined by SharePoint Managed Metadata Terms. Only terms directly below the term set are supported; subterms display but cannot be used.

There are two ways to add an Access Rule: Site Column Value:

- Enter *Site Column Value* in text field. The type ahead feature is enabled to support immediate value matches for the selected **Access Rule: Site Column** as you type.
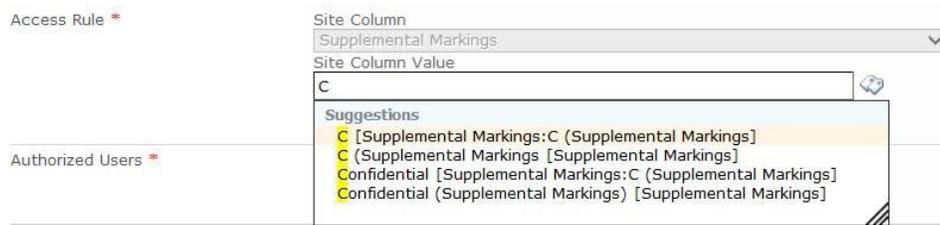
Figure 3-2 Access Rules Add Site Column Value

- Click **Browse**. The *Select: Add Terms* dialog box opens with valid terms for the selected **Access Rule: Site Column**.

  Only terms directly below the term set are supported; subterms cannot be used. If you attempt to use a subterm and click **Save**, an error is generated.
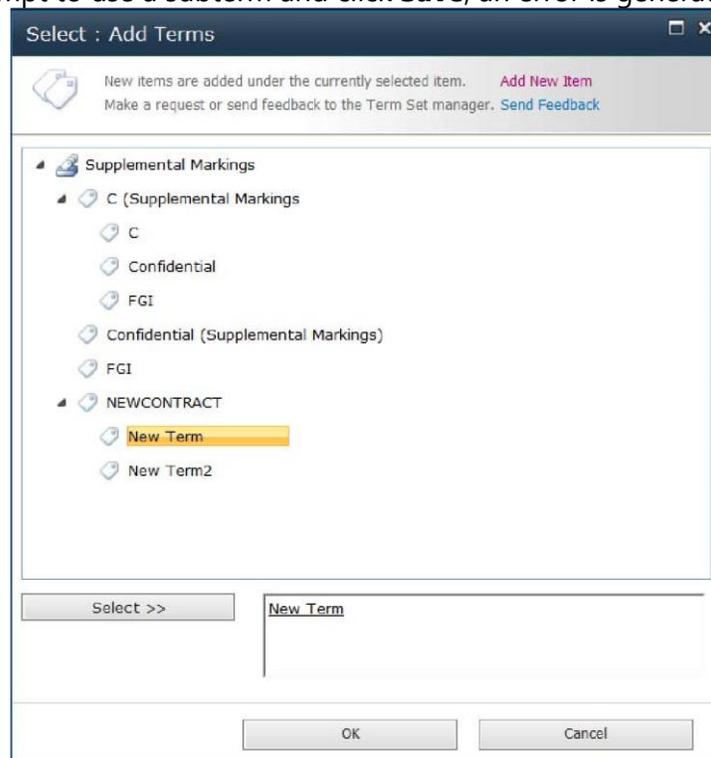

Figure 3-3 Access Rules Add Terms Dialog Box

- Select the term from the displayed list. Click **Select** →→ to add the term. Click **OK** and the selected term is set in the **Access Rule: Site Column Value** field or click C**ancel** to return to the **Access Rules - New Item** dialog box without adding the selected term.

- In addition to selecting an existing term, you can add a new term to the Managed Metadata Terms for the selected Access Rule: Site Column by clicking **Add New Item** at the top of the screen.

6. (**Required**) Enter the **Authorized Users**. The **Authorized Users** identify users that have access to view Record Container(s) and/or Record Item(s) that have metadata content equal to the **Access Rule: Site Column** and **Access Rule: Site Column Value**

combination as described above. The rules for A**uthorized Users** access varies based on the type (Supplemental Markings or Access-Constrained Column) of the **Access Rule: Site Column**. For more details, see 3.3 Supplemental Markings and Access-Constrained Columns.

There are two ways to add authorized users:

- Semicolon-separated list

- Standard SharePoint address book lookup

7. Click **Save** to create the new Access Rule. The new rule is displayed in the **Access Rules View** list.
   or
   Click **Cancel** to return to the **Access Rules View** list without creating a new Access Rule.

8. After the new Access Rule is saved:

- The **Access Rule: Site Column Value** defined in the new Access Rule is a selection in the **Access Rule: Site Column** field for **Record Container(s)** and/or **Record Item(s)** dialog boxes as applicable

- For the **Access Rule: Site Column Value** defined in the new Access Rule to be applicable, the **Access Rule: Site Column** must be a valid SharePoint site column for the Record Container and/or Record Item content type. In addition, the user accessing the record item must be included in the **Authorized Users** list for the new Access Rule.

3.4.2 Editing an Access Rule

To change an existing Access Rule, you must edit the Access Rule item by following these instructions.

1. From the **Access Rules View**, select the Access Rule that you want to edit.

2. Click **Items** to display the ribbon.

Figure 3-4 Access Rules Edit Item

3. Select **Edit Item** on the header ribbon. The **Access Rules Edit** dialog box opens displaying the selected Access Rule details.
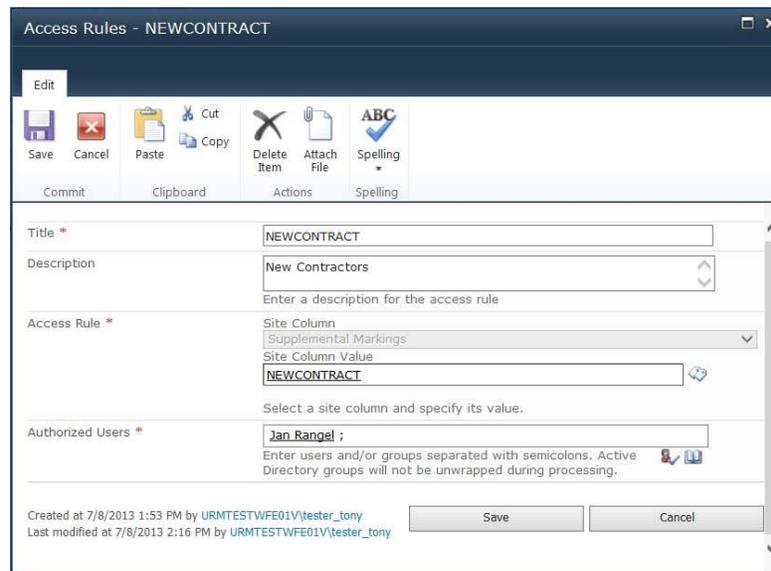
Figure 3-5 Access Rules Edit Item Dialog Box

4. Update the information in the fields you want to change.

    ● (**Required**) **Title**: Enter a title.

    ● **Description**: The **Description** is a descriptive statement that defines the purpose of this Access Rule.

    ● (**Required**) **Access Rule: Site Column** updates refresh the valid options for **Access Rule: Site Column Value** field. Updates that affect existing Record Container(s) and Record Item(s) are applied when you click **Save**. You cannot edit the **Site Column**. See 3.4.1 Creating an Access Rule for details on setting the **Access Rule: Site Column**.

    ● (**Required**) **Access Rule: Site Column Value** must be unique across all Access Rules. Updates that affect existing Record Container(s) and Record Item(s) are applied upon **Save**. See 3.4.1 Creating an Access Rule for details on setting the **Access Rule: Site Column Value.**

    ● (**Required**) **Authorized Users** updates that affect existing Record Container(s) and Record Item(s) are applied upon **Save**. See 3.4.1 Creating an Access Rule for details on setting the **Authorized Users**.

5. Click **Save** and the Access Rule updates and displays in the **Access Rules View** list. Click **Cancel** to return to the *Access Rules View* list without saving the selected Access Rule.

6. After the Access Rule change is saved:

    ● For Supplemental Markings, if the updated Access Rule is currently used by one or more R*ecord Container(s)* or *Record Item(s)* and is updated in a such a way that the previous **Access Rule: Site Column Value** is no longer valid, all user permission for the affected record items except the *System Account* user are removed. *Please update with caution.*

- For Access-Constrained Columns, if the updated Access Rule is currently used by one or more *Record Container(s)* or R*ecord Item(s)* and is updated in such a way that the previous **Access Rule: Site Column Value** is no longer valid and no other Access Rules apply for the affected Record Container(s) or Record Item(s).

- If the **Access Rule: Site Column Value** was updated, the updated value displays as a selection in the **Access Rule: Site Column** field on the **Record Container(s)** and/or **Record Item(s)** dialog boxes as applicable based on **Access Rule: Site Column** availability and the **Authorized Users** list. In addition, the previous value is removed as a selection in the **Access Rule: Site Column** field on the **Record Container(s)** and/or **Record Item(s)** dialog boxes.

3.4.3 Viewing an Access Rule

To view the details of an existing Access Rule, you must view the Access Rule item. To view an access rule:

1. From the **Access Rules View**, select the Access Rule that you want to view.

2. Select **Items** to display the ribbon.

Note:

You can only select one Access Rule at a time.

Figure 3-6 Access Rules View Item

3. Select **View Item** button on the header ribbon. The **Access Rules View** dialog box opens displaying the Access Rule details in read-only mode.
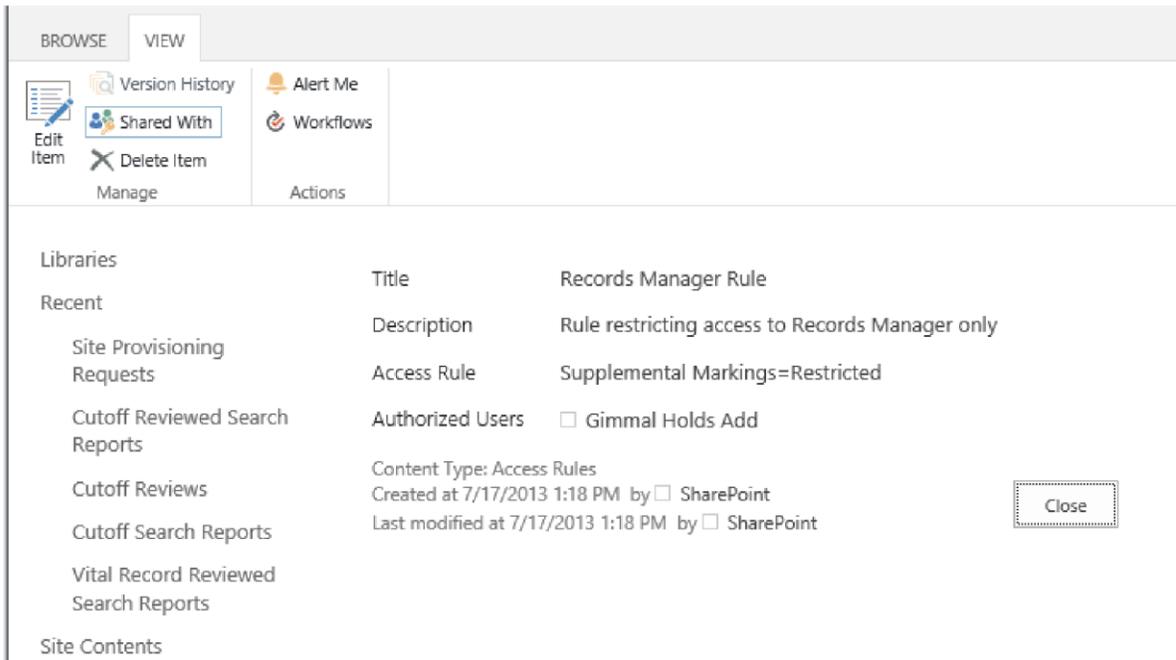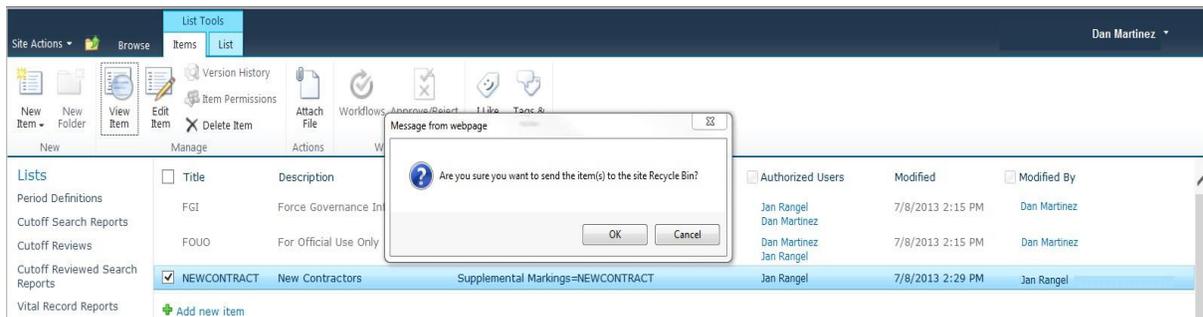

Figure 3-7 Access Rules View Item Dialog Box

4. From the **Access Rules View** dialog box, you can edit or delete the selected Access Rule.

5. Click **Close** to return to the **Access Rules View** list.

3.4.4 Deleting an Access Rule

To remove an existing Access Rule from your site, you must delete the Access Rule item.

To delete an access rule, follow these steps.

1. From the **Access Rules** view, select the Access Rule(s) that you want to delete. Select **Items** to display the ribbon.

Figure 3-8 Access Rules Delete Item

2. Click **Delete Item** on the header ribbon. A prompt dialog box opens asking '*Are you sure you want to send the item(s) to the site Recycle Bin?*'

3. Click **OK** and the Access Rule(s) is deleted from the Access Rules View list. Click **Cancel** to return to the **Access Rules View** list without deleting the selected Access Rule(s).

   - For Supplemental Markings, if the deleted Access Rule(s) is currently used by one or more **Record Container(s)** and/or **Record Item(s)**.

   - "For Access-Constrained Columns, if the deleted Access Rule(s) is currently used by one or more **Record Item(s)** and no other Access Rules apply for the affected *Record Item(s)*.

   - The **Access Rule: Site Column Value** as defined in the deleted Access Rule(s) are removed as a selection in the **Access Rule: Site Column** field on the **Record Container(s)** and/or **Record Item(s)** dialog boxes.

3.5 Restricted Records Cleanup Timer Job

There is a Gimmal Compliance Suite Restricted Records Cleanup Timer Job that you can set to automatically reset and evaluate the permissions on restricted records and folders to ensure they are consistent with current access rules. You must manually activate this timer job.

3.5.1 Activating the Restricted Records Cleanup Timer Job

Follow these steps to activate the Restricted Records Cleanup Timer job:

1. Go to **Central Administration > Application Management > Manage web applications**. The Web Applications display.

Figure 3-9 Web Applications

2. Select the web application where the Restricted Records Timer Job is located and click **Manage Features** in the header ribbon. The **Manage Web Features** dialog box displays.
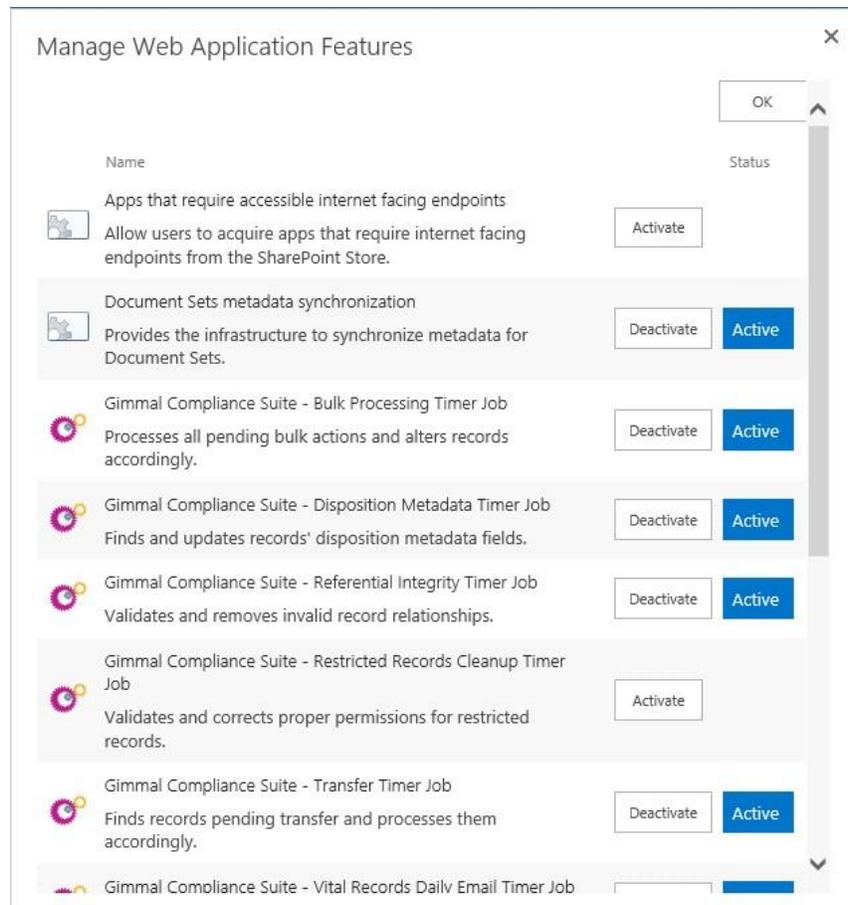
Figure 3-10 Manage Web Application Features

3. Click **Activate** next to **Gimmal Compliance Suite - Restricted Records Cleanup Timer Job**. The timer job immediately activates.

4. Click **X** in the top right corner to close the dialog box.

4 Record Relationship Management

Record Relationship Management functionality is available in a SharePoint Records Center with Compliance Suite enabled. To use the Record Relationship Management features, Compliance Suite must be installed and the Gimmal RMA Record Relationship Content Type and Gimmal RMA Record Relationship Functionality features must be active.

Compliance Suite allows the creation of relationships between records in one or more record centers. However, if records are in different record centers, they are *unidirectional*; that is, the records exist only on the record where they were created.

Compliance Suite supports user-defined relationships between records. A Record Relationship is an association that links two or more independent records. Records can be related for a variety of reasons, such as:

- *Supporting Information*: Supporting and reference materials can be contained in multiple records.
- *Cross-Reference*: Records can contain cross references to other records.
- *Version Management*: A record can have multiple iterations.
- *Rendition Management*: A record can be stored in multiple media formats.
- *Disposition Management*: Disposition of a record can be dependent on another record's disposition status.

Creating a relationship between records enables a user to easily find all related information through search or browse. In addition, it enables the application to support business processes and maintain integrity across related records.

Three views support Record Relationships:

1. Relationship Type View

   - **Records Center → Libraries → Relationship Type**

2. Record Relationship Administration

   - Click **...** next to a record to display the **Record Relationship Administration** menu.

3. Related Records (Record Relationships) View

   - **Records Center → Libraries → Related Records**

4.1 Relationship Types

Relationship Types define the behavior of the relationship between records. The Relationship Types are either Hierarchical or Non-Hierarchical, which is defined in the **Relationship Form Type** field for a Relationship Type.

- *Hierarchical*: Relationships that are structured as parent to child. One record in this relationship is the parent record to one or many children records. An example of a Hierarchical relationship is a master record that is related to many other records that contain only supporting information.
- *Non-Hierarchical*: Relationships that are structured as peer-to-peer. Records in this type of relationship are on the same level with no record serving as the primary or parent. An example of a Non-Hierarchical relationship is multiple records that crossreference each other with each record being equally dependent on the other records.

Compliance Suite provides several out-of-the-box Relationship Types:

- *Version*: Non-Hierarchical
- *File to New Location*: Hierarchical
- *Cross Reference*: Non-Hierarchical
- *Superseded*: Hierarchical

- *Supporting*: Hierarchical
- *Rendition*: Non-Hierarchical

The Relationship Types are extensible. Compliance Suite provides the ability to create, edit, view, or delete Relationship Types using a SharePoint list.

Intended User: Records Manager, Compliance Suite Administrator

To access the Relationship Types View list:

1. Open a **SharePoint Records Center**. The Records Center Home Page opens.
2. Select **Libraries** from the Quick Launch. All lists available in your **SharePoint Records Center** display.
3. Select the **Relationships Types** list. A list of all Relationship Types defined in your Site Collection displays.

The following table describes the Relationship Types list with a description of each heading.

Table 4-1 Relationship Types

List View Heading	Description
Title	Unique name that differentiates the Relationship Type from other Relationship Types. The **Title** is used in **Related Records** dialog boxes as the selection list for the **Relationship Title** menu. Example: Supporting/Supported Document

Table 4-1 Relationship Types

List View Heading	Description
Relationship Type	Defines the record relationship behavior. The **Relationship Type** determines the displayed fields in the Related Records dialog boxes. The **Relationship Type** is referred to as the **Relationship Form Type** on the Relationship Types dialog boxes as described in the subsequent sections. Values: Hierarchical (parent to child) or Non-Hierarchical (peer-topeer)
Relationship Members	Name for each member of the Relationship Type. For Hierarchical, two member names are listed. For Non-Hierarchical, a single member name is listed. The **Relationship Members** are used on the **Record Relationship Administration - Define a New Relationship** dialog box to identify Relationship Types that can be created. Example: Create a new **Supporting** relationship

Authorized Users	List of users or groups that have access to use the Relationship Type. Only users in this list are able to select the Relationship Type when creating or editing Record Relationships.

4.1.1 Creating a Relationship Type

Before a new relationship between records can be created, a Relationship Type must be created:

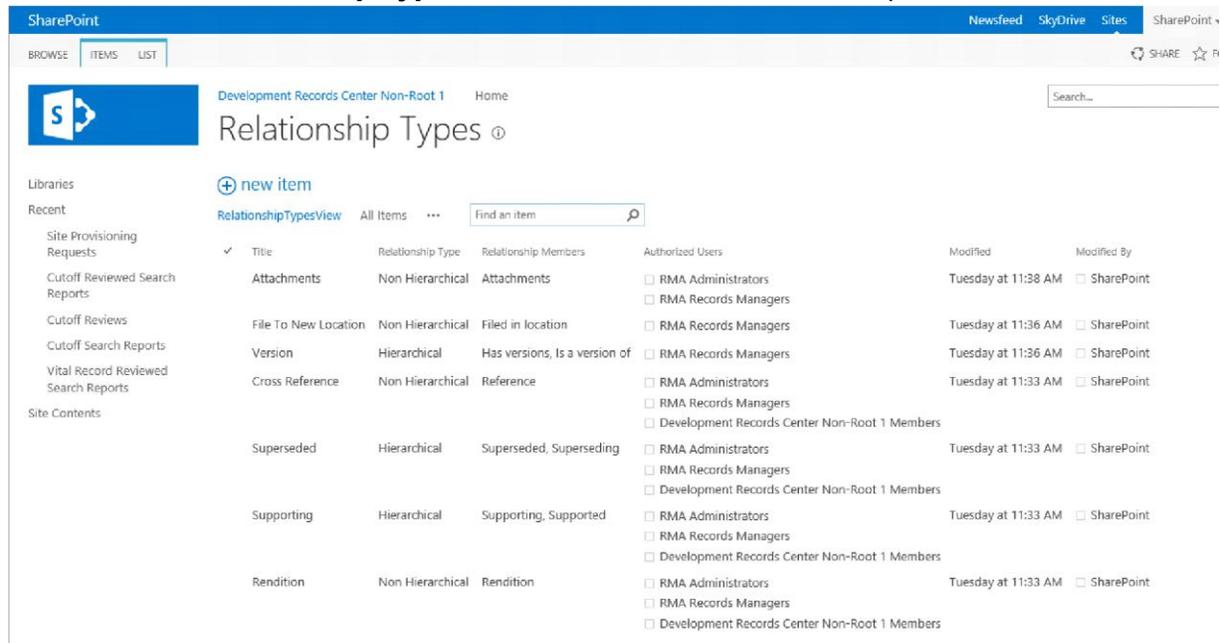1. From the **Relationship Types View**, click **+ new item** at the top of the list.

Figure 4-1 Record Relationship Types

A **Relationship Types - New Item** dialog box opens.

Figure 4-2 Relationship Types - New Item Dialog Box

2. (**Required**) Enter the **Title**. The **Title** is a unique identifier for the new **Relationship Type** and is used to populate the **Relationship Title** menu in **Related Records** and R**ecord Relationship Administration: Define a New Relationship**.

3. (**Required**) Enter the **Relationship Form Type** for the relationship. The **Relationship Form Type** defines the behavior of the relationship. There are two options: Hierarchical or Non-Hierarchical. The required fields vary based on type selected.

4. If the **Relationship Form Type** is *Hierarchical*:

    ● (**Required**) Enter the **Name** of the parent member of the relationship. The **Name** is used in **Record Relationship Administration: Define a New Relationship** to list available parent relationship types.

    ● (**Required**) Enter **Description** of the parent member of the relationship. The **Description** is used in **Record Relationship Administration: Relationships** to list existing parent relationships.

    ● (**Required**) Enter the **Name** of the child member of the relationship. This is located below the dotted line as shown on the previous screen. The **Name** is used in **Record Relationship Administration: Define a New Relationship** to list available child relationship types.

- (**Required**) Enter **Description** of the child member of the relationship. This is located below the dotted line as shown on the screen above. The **Description** is used in Record Relationship Administration: Relationships to list existing child relationships.

5. If the **Relationship Form Type** is Non-Hierarchical:

   - (**Required**) Enter the **Name** of the peer members of the relationship. The **Name** is used in **Record Relationship Administration: Define a New Relationship** to list available peer relationship types.

   - (**Required**) Enter **Description** of the peer members of the relationship. The **Description** is used in **Record Relationship Administration: Relationships** to list existing peer relationships.

6. (**Required**) Enter the **Authorized Users**. The **Authorized Users** identify users and groups that have access to create record relationships based on this new Relationship Type. It is recommended to add user groups such as Records Managers instead of individual user names.

   There are two ways to add **Authorized Users**:

   - Semicolon-separated list
   - Standard SharePoint address book lookup

7. Click **Save** to create the new Relationship Type. The item displays in the **Relationship Types View** list. Click **Cancel** to return to the Relationship Types View list without saving the new Relationship Type.

8. After the new Relationship Type is saved, the new Relationship Type displays as a selection in the **Relationship Title** menu for **Authorized Users** in the Related Records dialog boxes.

4.1.2 Editing a Relationship Type

To edit an existing Relationship Type, follow these steps:

1. From the **Relationship Type View**, select the Relationship Type that you want to edit. Only one Relationship Type can be selected at a time.

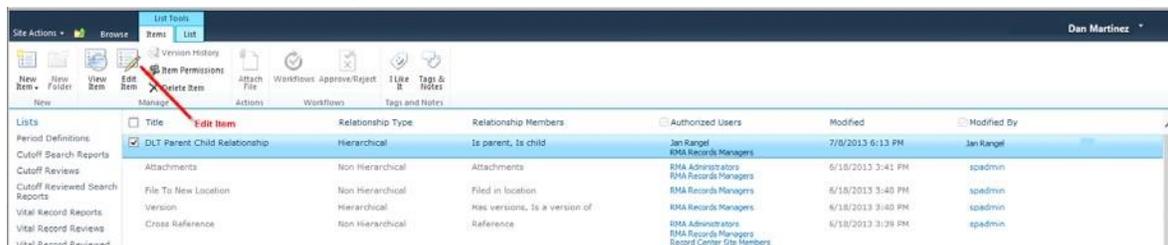   - Select **Items** to display the ribbon.

Figure 4-3 Relationship Types - Edit Item

Select

2. **Edit Item** on the header ribbon. If the selected Relationship Type is based on a Hierarchical **Relationship Form Type**, the dialog box displays with the following fields:

Figure 4-4 Hierarchical Relationship Types Edit Dialog Box

If the selected Relationship Type is based on a Non-Hierarchical **Relationship Form Type**, the dialog box updates with the following fields:

Figure 4-5 Non-Hierarchical Relationship Type Edit Dialog Box

3. Update the information in the fields that you want to change.

    -   (**Required**) **Title** must be unique across all Relationship Types.

    -   **Relationship Form Type** is not editable. A new Relationship Type must be created to change this value.

4. Click **Save** to update the Relationship Type. It displays in the **Relationship Type View** list. Click **Cancel** to return to the **Relationship Type View** list without updating the selected Relationship Type.

5. After the Relationship Type change is saved, the updated Relationship Type displays as a selection in the **Relationship Title** menu for **Authorized Users** in the Related Records dialog boxes.

4.1.3 Deleting a Relationship Type

To remove an existing Relationship Type from your site, you must delete the Relationship Type item.

To delete a relationship type:

1. From the **Relationship Type View**, select the Relationship Type that you want to delete. You can select only one Relationship Type at a time.

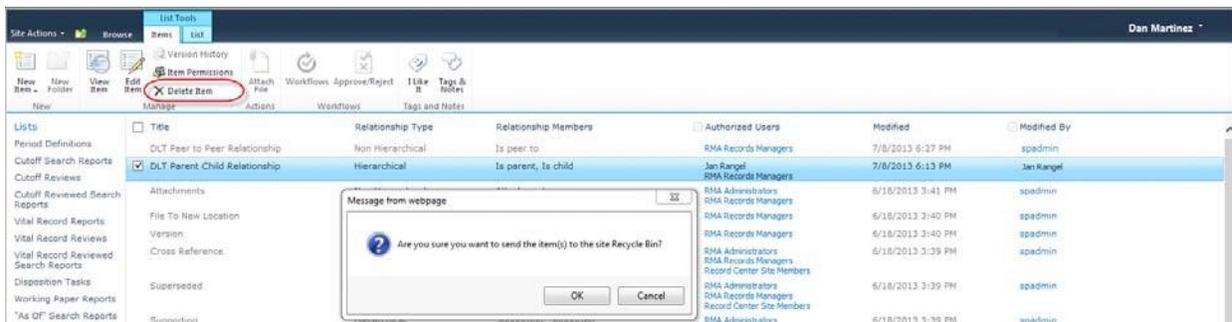2. Select **Items** to display the ribbon.

Figure 4-6 Relationship Types - Delete Item

3. Select **Delete Item** on the header ribbon. A prompt opens asking *Are you sure you want to send the item(s) to the site Recycle Bin?*

4. Click **OK** and the Relationship Type is deleted and removed from the **Relationship Type View** list or click **Cancel** to return to the **Relationship Type View** list without deleting the selected Relationship Type.

    If the Relationship Type is currently used by one or more records, an error displays.

4.1.4 Viewing a Relationship Type

To view the details of an existing Relationship Type, you must view the Relationship Type item.

Select

1. From the **Relationship Type View**, select the Relationship Type you want to view. Only one Relationship Type can be selected at a time.
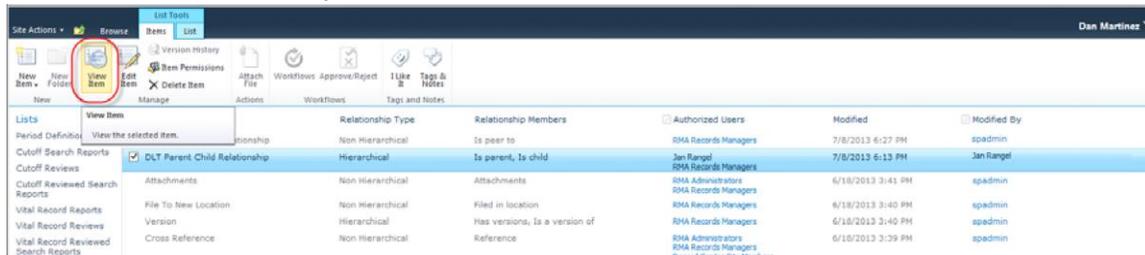
2. **Items** to display the ribbon.

Figure 4-7 Relationship Types - View Item

3. Click the **View Item** button on the header ribbon. The **Relationship Type View** dialog box opens displaying the Relationship Type details in read only mode. If the selected Relationship Type is based on Hierarchical Relationship Form Type, the dialog box updates as shown in the following figure.
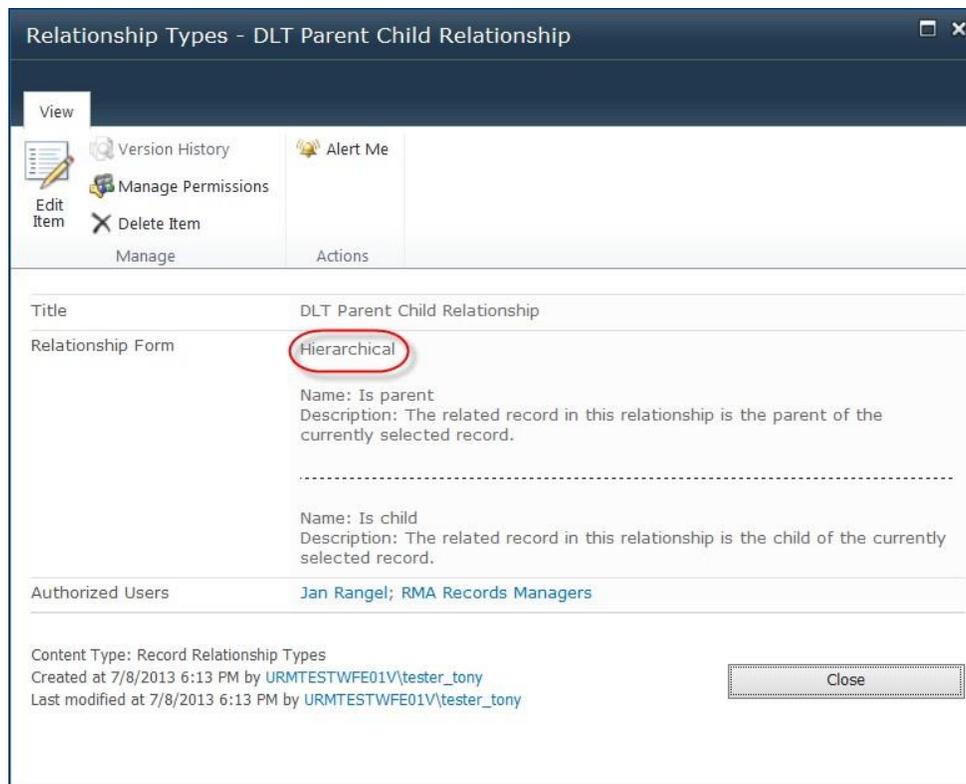

Figure 4-8 Relationship Types - View Item Dialog Box

If the selected Relationship Type is based on a Non Hierarchical **Relationship Form Type**, the dialog box updates with the following fields:
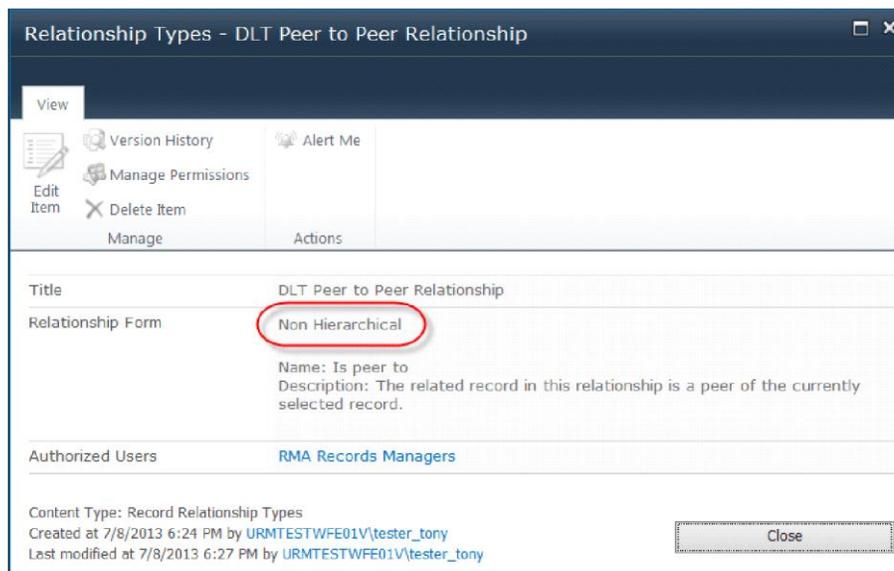
Figure 4-9 Relationship Types - View Item Non-Hierarchical

4.   From the **Relationship Type View**, you can edit, delete, or manage permissions of the selected Relationship Type.

5.   Click **Close** to return to the **Relationship Type View** list.

4.2 Record Relationship Administration

Record Relationship Administration supports creating, viewing, and managing record relationships directly from a selected record in the Record Library. The Record Relationship Administration is broken into two sections:

1. **Define a New Relationship**: Provides the ability to directly create a new record relationship for the selected record

2. **Relationships**: Provides the ability to view and manage existing relationships for the selected record

Intended User: End User, Records Manager

To access the Record Relationship Administration:

1.   Open a **SharePoint Records Center**. The Records Center home page opens.

2.   Select **Libraries** to display all libraries and then select the desired library. A list of all record folders and/or record items contained in the selected library displays.

3.   Navigate to your record in the library.

4.   **Record Relationship Administration** from the action menu for the record.
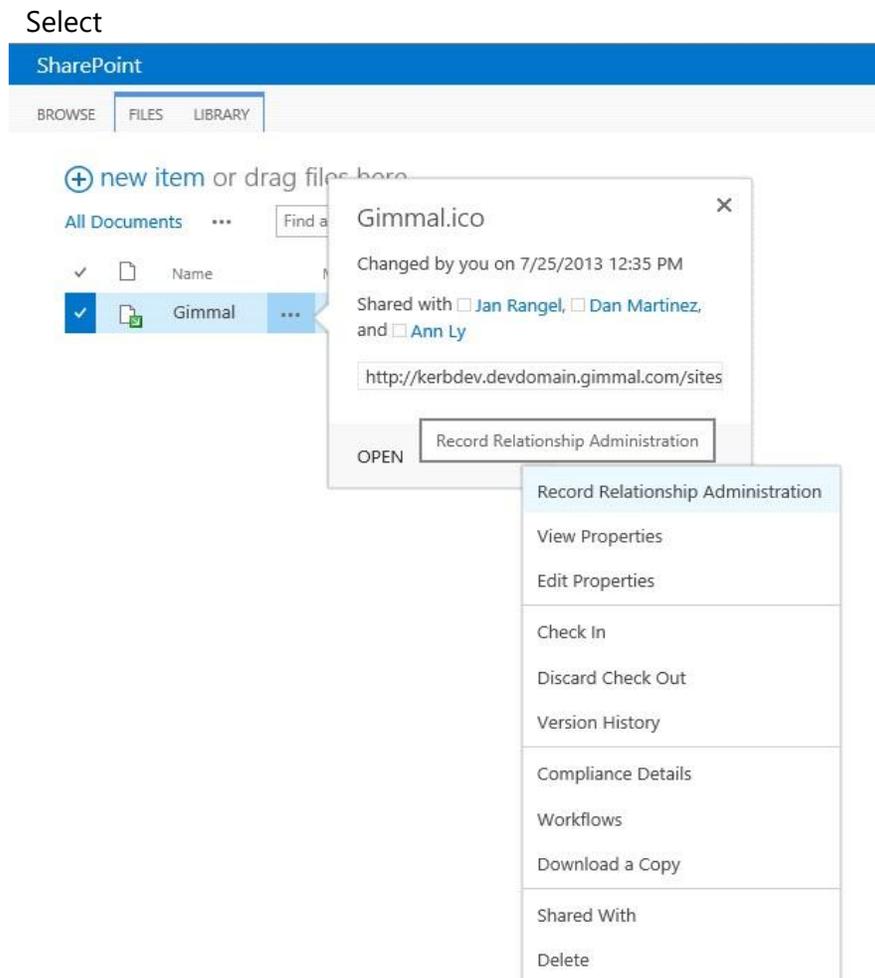
Select

Figure 4-10 Record Relationship Action Menu

4.2.1 Define a New Relationship

The **Define a New Relationship** list is the top section of the **Record Relationship Administration** page. Define a New Relationship supports creation of a new relationship between the currently selected record and one or more other records in the system.

The displayed list of Relationship Types is ordered by **Creation Date** and based on the Relationship Types that you have access to as defined in the **Authorized User** list. The Relationship Types are listed as *Create a **Relationship Type Member Name** relationship* with the **Relationship Type Member Name** defined by:

- If a Relationship Type is Hierarchical, it has two entries:
  - Relationship Type Parent Member Name
  - Relationship Type Child Member Name
- If a Relationship Type is Non Hierarchical, it has one entry:
  - Relationship Type Member Name

Creating a Record Relationship

To create a new Record Relationship:

1. From the **Relationship Administration: Define a New Relationship**, select a Relationship Type from the displayed list.

   A **Related Records - New Item** dialog box opens with fields for creating a new Record Relationship.

Figure 4-11 Related Records - New Item Dialog Box

2. (**Required**) Enter the **Title**. The **Title** should be a user friendly identifier of the new Record Relationship.

3. (**Required**) **Relationship Title** is defaulted based on the selected Relationship Type. You can change the **Relationship Title** using the menu based on the Relationship Types where you are defined as an **Authorized User**. The **Relationship Title** defines the **Related Records** displayed fields.

4. If the selected **Relationship Title** is based on a Hierarchical relationship type, the dialog box updates with the following fields:

Figure 4-12 Related Records - New Item Hierarchical Dialog Box

5. (**Required**) Select the **New Parent Record**. If the Relationship Type selected was a Parent

   Relationship Type, the **New Parent Record** defaults to the currently selected record's **Record Identifier** and cannot be updated. Otherwise, the browse feature uses the standard SharePoint record selector to navigate to a parent record.

6. (**Required**) Select the **Child Record(s)**. If the Relationship Type selected was a Child Relationship Type, the **Child Record(s)** defaults to the currently selected record's **Record Identifier**. The browse feature uses the standard SharePoint record selector to navigate to a new child record.

   - **Add** button. After you browse and select the child record, click Add to update the list with the selected child record.

   - **Delete** button. To remove a child record from the list, highlight the listed child record and click **Delete**.

   - You must add at least one **Child Record**.

   - For multiple **Child Records**, repeat *this step* for each **Child Record**.

7. If the selected **Relationship Title** is based on a Non Hierarchical relationship type, the dialog box updates with the following fields:

Figure 4-13 Related Records - New Item Non Hierarchical

8. (**Required**) Select the **Related Record(s)**. The **Related Record(s)** default to the currently selected record's **Record Identifier**. The browse feature uses the standard SharePoint record selector to navigate to a new related record.

- **Add** button. After you browse and select a related record, click Add to update the list with the selected related record.

- **Delete** button. To remove a related record from the list, highlight the listed related record and Click **Delete**.

- You must add at least two **Related Records**.

- For multiple **Related Records**, repeat this step for each **Related Record**.

9. Click **Save** and the new Record Relationship is created and displayed in the **Relationship Administration Management: Relationships** list. Click **Cancel** to return to the **Relationship Administration Management** page without creating a new Record Relationship.

10. After the new Record Relationship is saved, the new relationship displays on each record's **Record Relationship Administration: Relationships** page, as well as in the **Related Records View**.

4.2.2 Relationships List

The **Relationships** list is the bottom section of the **Record Relationship Administration** page. It lists all existing Record Relationships for the currently selected record. In addition it provides an access point to the **Edit Related Records** and **Delete Related Records** dialog boxes.

The following table describes the Relationships list with a description of each heading.

Table 4-2 Relationships List

List Heading	Description
Relationship Type	The **Description** of the Relationship Type for the Record Relationship instance.
	Parent Member: If the currently selected record is the Parent in a Hierarchical relationship, the Parent Member Description will be displayed.
	Child Member: If the currently selected record is the Child in a Hierarchical relationship, the **Child Member Description** will be displayed. *Non Hierarchical Member*: If the currently selected record, is a Non Hierarchical relationship the **Member Description** will be displayed.
Related Records	**Record Identifiers** for each record related to the currently selected record. **Each Record Identifier** is listed on a single line and grouped by Relationship Type.
Containing Folder	Folder path for the related record. Selecting this link will open up the SharePoint folder that contains the related record.
Document	File name for the related record. Selecting this link opens an option to view or download the related record file.
Edit	Action link that opens the **Related Records Edit** dialog box. From this dialog box you can update the selected Record Relationship. Any updates to the Record Relationship will refresh the **Relationships** list and the **Related Records View**.
	Only Authorized Users as defined in the Relationship Type for the Record Relationship can edit.
Delete	Action link that opens a prompt dialog box asking '*Do you want to delete this relationship?*' Any deletion will update the *Relationships* list and the *Related Records View*. Only **Authorized Users** as defined in the Relationship Type for the Record Relationship can delete.

Editing a Record Relationship

To change a listed Record Relationship, you must edit the Record Relationship item. The **Relationship Administration Management: Relationships** list provides a point of access to edit a relationship item.

1. From the **Relationship Administration Management: Relationships** list, click **Edit** on the Record Relationship you would like to update.

- If the selected Record Relationship is based on a Relationship Title that is a Hierarchical relationship type, the dialog box updates with the following fields:
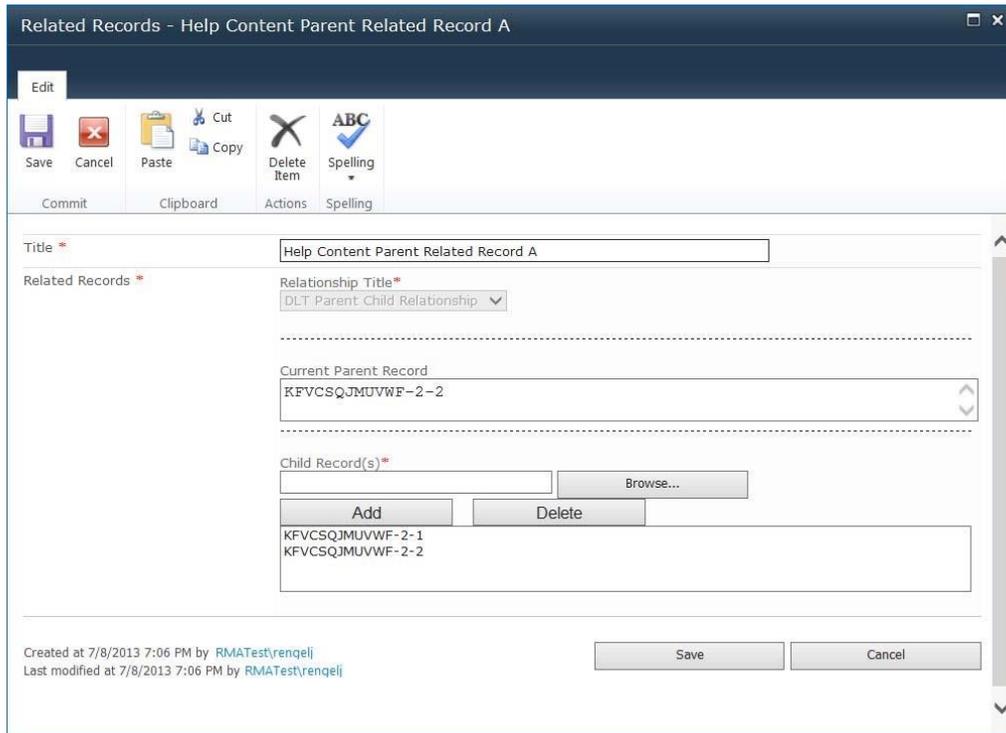

Figure 4-14 Related Records - Edit Item Hierarchical Dialog Box

- If the selected Record Relationship is based on a Relationship Title that is a Non-Hierarchical relationship type, the dialog box updates with the following fields:
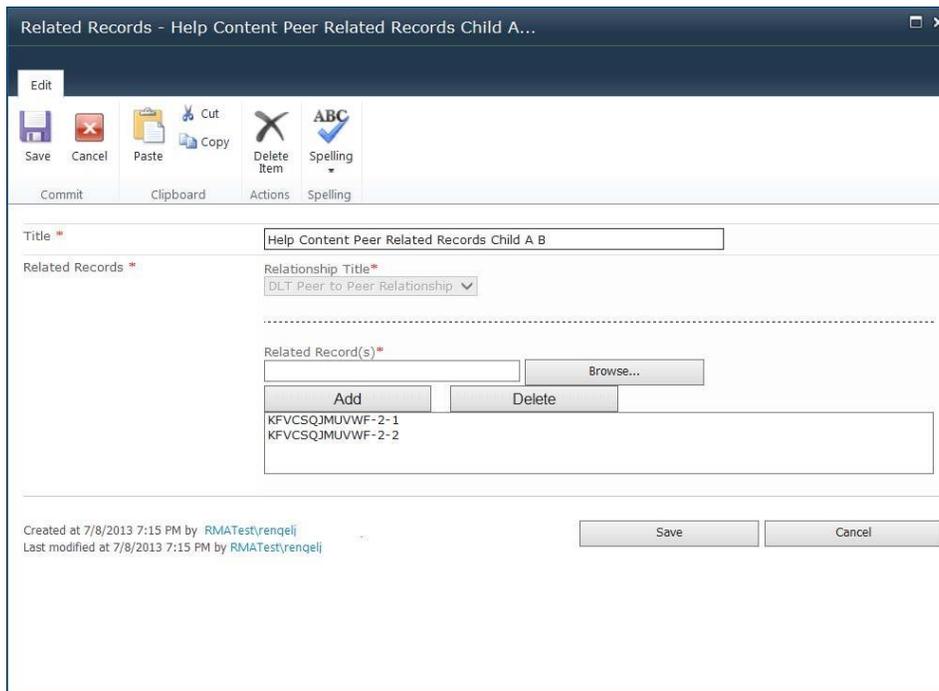

Figure 4-15 Related Records - Edit Item Non- Hierarchical Dialog Box

2. Update the information in the fields you want to change.

3. **Relationship Title** is not editable. A new Record Relationship must be created to change this value. If Hierarchical, **Parent Record** is not editable. A new Record Relationship must be created to change this value.

4. (**Required**) **Related Record(s) or Child Record(s)**. The browse feature uses the standard SharePoint record selector to navigate to a record.

   - **Add** button. After you browse and select a related record, click **Add** to update the list with the selected record.

   - **Delete** button. To remove a record from the list, highlight the listed record and click **Delete**.

   - If the **Parent Record** is currently part of disposition or cutoff processing, the list of **Child Record(s)** cannot be changed. An error displays on **Save**.

   - You must have at least two **Related Record(s)** or one **Child Record(s)**.

   - For multiple **Related** or **Child Records**, repeat *Step 4* for each **Related** or **Child Record**.

5. Click **Save** and the Record Relationship is updated and displayed in the **Relationship Administration Management -Relationships** list. Click **Cancel** to return to the **Relationship Administration Management** list without updating the selected relationship.

6. After the Record Relationship update is saved, the updated relationship displays on each record's **Record Relationship Administration: Relationships** list, as well as the **Related Records View**.

Deleting a Record Relationship

To remove a listed Record Relationship from your site, you must delete the Record Relationship item. The **Relationship Administration Management: Relationships** list provides a point of access for deleting a relationship item. You must be an RMA Manager, RMA Administrator, or Site Administrator to delete a record relationship.

1. From the **Relationship Administration Management: Relationships** list, click **Delete** on the Record Relationship you would like to remove. A prompt opens asking *Do you want to delete this relationship*?

2. Click **OK** and the Record Relationship is deleted and removed from the **Record Relationship Administration: Relationships** list, or click **Cancel** to return to the **Record Relationship Administration: Relationships** list without deleting the selected Record Relationship.

   - If the Record Relationship is currently assigned to one or more records that are a part of disposition or cutoff processing, you cannot delete the relationship.

3. After the Record Relationship is deleted, the relationship is removed from each record's **Record Relationship Administration: Relationships** list, as well as the **Related Records View**.

4.3 Record Relationships (Related Records)

Record Relationships are instances of Relationship Types that have been applied to records. The Record Relationship provides the actual linkage between the records in a relationship. Record Relationships is also referred to as Related Records, the terminology is used interchangeably throughout Compliance Suite.

Compliance Suite provides the ability to create, edit, view, or delete Record Relationships using a SharePoint list.

Intended User: End User, Records Manager

To access the **Related Records View** list:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.
2. Select **Libraries** from the Quick Launch to display all lists, libraries, and other apps in your **SharePoint Records Center**.
3. Select the **Related Records** list to display a list view of all Record Relationships in your Site Collection.

The following table describes the **Related Records View** list with a description of each heading.

Table 4-3 Related Records View

Title	User friendly name that differentiates the Record Relationship item from other Record Relationships.
	Example: Rendition Relationship for Project A
Relationship Title	Relationship Type that is the base for each Record Relationship item. These values are based on the Title of the Relationship Type items.
	Example: Supporting/Supported Document
Related Records	**Record Identifiers** for all parent, child, or related records in the Record Relationship item. They are listed in a semi-colon separated list.
Modified	When the relationship was last modified.
Modified By	Compliance Suite username of the user who last modified the relationship.

4.3.1 Creating a Record Relationship

To define a relationship between two or more records, a Record Relationship must be created. The **Related Records View** provides a point of access to create this new Record Relationship item. An additional point of access to this view is provided on the **Record Relationship Administration: Relationships** page.

1. From the **Related Records View**, there are two ways to initiate the record relationship creation process.

   - Click **+Add new item** link from the bottom of the list.

   - Select **List Tools → Items** tab. In the header ribbon, Select **New Item → Record Relationships**.

Figure 4-16 Related Records View New Item

2. A **Related Records - New Item** dialog box opens with fields for creating a new Record Relationship.

Figure 4-17 Related Records View New Item Dialog Box

3. (**Required**) Enter the **Title**. The **Title** should be a user-friendly identifier of the new Record Relationship.

4. (**Required**) Select the **Relationship Title** for the Record Relationship. The **Relationship Title** is a menu based on the Relationship Types where you are defined as an **Authorized User**. The selection of the **Relationship Title** defines the fields displayed.

---

5. If the selected **Relationship Title** is based on a Hierarchical relationship type, the dialog box updates with the following fields:
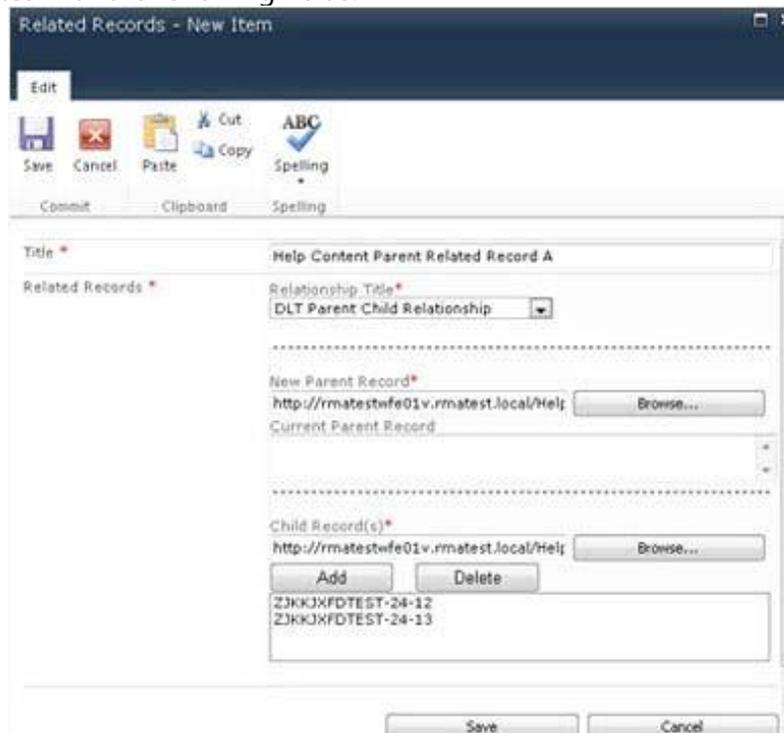

Figure 4-18 Related Records View New Item Hierarchical Dialog Box

6. (**Required**) Select the **New Parent Record**. The browse feature uses the standard SharePoint record selector to navigate to a parent record.

7. (**Required**) Select the **Child Record(s)**. The browse feature uses the standard SharePoint record selector to navigate to a child record.

   ● **Add** button. After you have browsed and selected a child record, Click **Add** to update the list with the selected child record.

   ● **Delete** button. To remove a child record from the list, highlight the listed child record and Click **Delete**.

   ● You must add at least one **Child Record**.

   ● For multiple **Child Records**, repeat *Step 7* for each **Child Record**.

8. If the selected **Relationship Title** is based on a Non Hierarchical relationship type, the dialog box updates with the following fields:
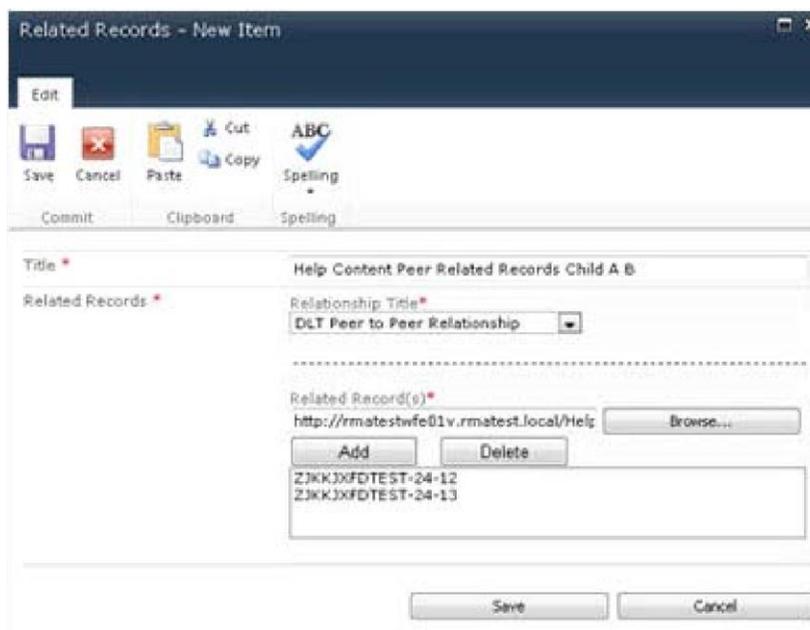
Figure 4-19 Related Records View New Item Non Hierarchical Dialog Box

9. (**Required**) Select the **Related Record(s)**. The browse feature uses the standard SharePoint record selector to navigate to a related record.

   - **Add** button. After you have browsed and selected a related record, Click **Add** to update the list with the selected related record.

   - **Delete** button. To remove a related record from the list, highlight the listed related record and click **Delete**.

   - You must add at least two **Related Records**.

   - For multiple **Related Records**, repeat this step for each **Related Record.**

10. Click **Save** and the new Record Relationship is created and displayed in the **Related Records View** list. Click **Cancel** to return to the **Related Records View** list without creating a new Record Relationship.

11. After the new Record Relationship is saved, the new relationship displays on each record's **Record Relationship Administration: Relationships** page.

4.3.2 Editing a Record Relationship

To change an existing Record Relationship, you must edit the Record Relationship item. The **Related Records View** provides a point of access to edit this relationship item. An additional point of access to this view is provided on the **Record Relationship Administration: Relationships** page.

1. From the **Related Records View** list, select the Record Relationship you want to edit. Only one Record Relationship can be selected at a time.

2. Click **Items** to display the header ribbon.

Figure 4-20 Related Records Edit Item

3. Select **Edit Item** button on the header ribbon. The **Related Records Edit** dialog box opens displaying the Record Relationship details.

- If the selected Record Relationship is based on a Relationship Title that is a Hierarchical relationship type, the dialog box updates with the following fields:
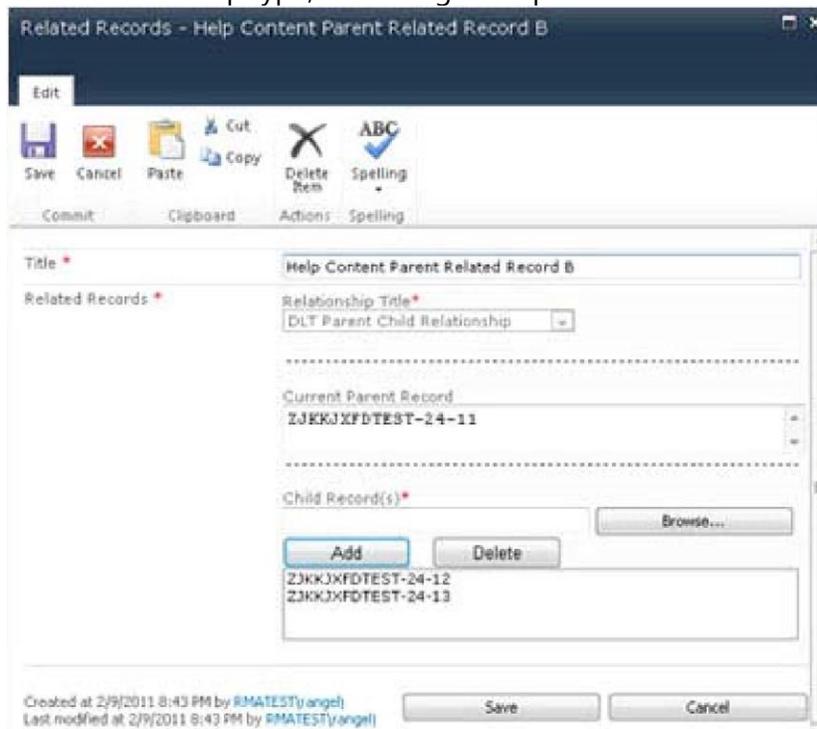

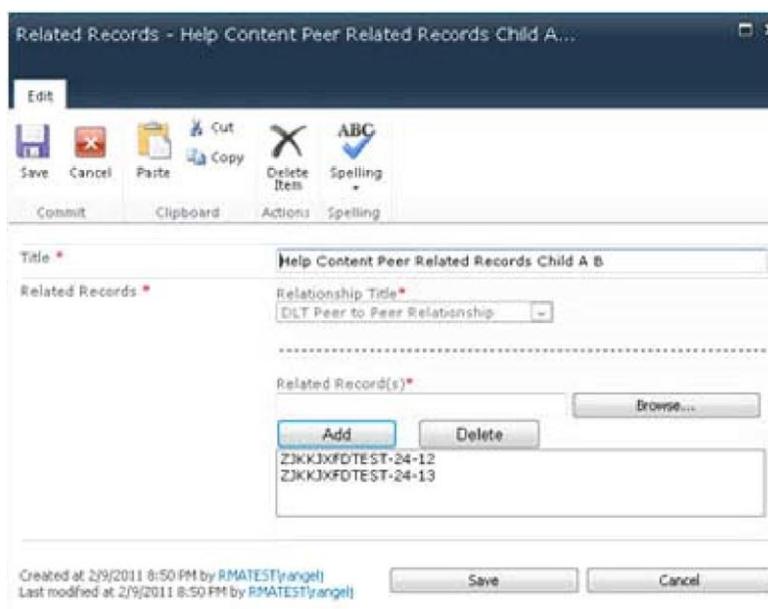*Figure 4-21 Related Records Edit Item Hierarchical Dialog Box*

- If the selected Record Relationship is based on a **Relationship Title** that is a Non Hierarchical relationship type, the dialog box updates with the following fields:

Figure 4-22 Related Records Edit Item Non-Hierarchical Dialog Box

4. Update the information in the fields you want to change.

5. **Relationship Title** is not editable. A new Record Relationship must be created to change this value.

    ●   If Hierarchical, **Parent Record** is not editable. A new Record Relationship must be created to change this value.

6. (**Required**) **Related Record(s) or Child Record(s)**. The browse feature uses the standard SharePoint record selector to navigate to a record.

    ●   **Add** button. After you browse and select a related record, click **Add** to update the list with the selected record.

    ●   **Delete** button. To remove a record from the list, highlight the listed record and click **Delete**.

    ●   If the **Parent Record** is currently part of disposition or cutoff processing, the list of **Child Record(s)** cannot be changed. An error will be displayed on **Save**.

    ●   You must have at least two **Related Record(s)** or one **Child Record(s)**.

    ●   For multiple **Related** or **Child Records**, repeat *Step 5* for each **Related** or **Child Record**.

7. Click **Save** to update the Record Relationship. The changes are displayed in the **Related Records View** list. Click **Cancel** to return to the **Related Records View** list without updating the selected Record Relationship.

8. After the Record Relationship update is saved, the updated relationship displays on each record's **Record Relationship Administration: Relationships** page.

4.3.3 Deleting a Record Relationship

To remove an existing Record Relationship item from your site, you must delete the Record Relationship item. The **Related Records View** provides a point of access to delete a relationship item. An additional point of access to this feature is provided on the **Record Relationship Administration: Relationships** page.

1. From the **Related Records View** list, select the Record Relationship you want to delete. Only one Record Relationship can be selected at a time.

2. Click **Items** to display the header ribbon.

Figure 4-23 Related Records Delete Item

3. Select **Delete Item** on the header ribbon. A prompt opens asking *Are you sure you want to send the item(s) to the site Recycle Bin?*

4. Click **OK** and the Record Relationship is deleted and removed from the **Related Records View** list or click **Cancel** to return to the **Related Records View** list without deleting the selected Record Relationship.

   ● If the Record Relationship is currently assigned to one or more records that are a part of disposition or cutoff processing, you will not be able to delete the relationship.

5. After the Record Relationship is deleted, the relationship will be removed from each record's **Record Relationship Administration: Relationships** page.

4.3.4 Viewing a Record Relationship

To view the details of an existing Record Relationship, you must view the Record Relationship item. The Related Records View provides a point of access to view a relationship item.

1. From the **Related Records View**, select the Record Relationship you want to view. Only one Record Relationship can be selected at a time.

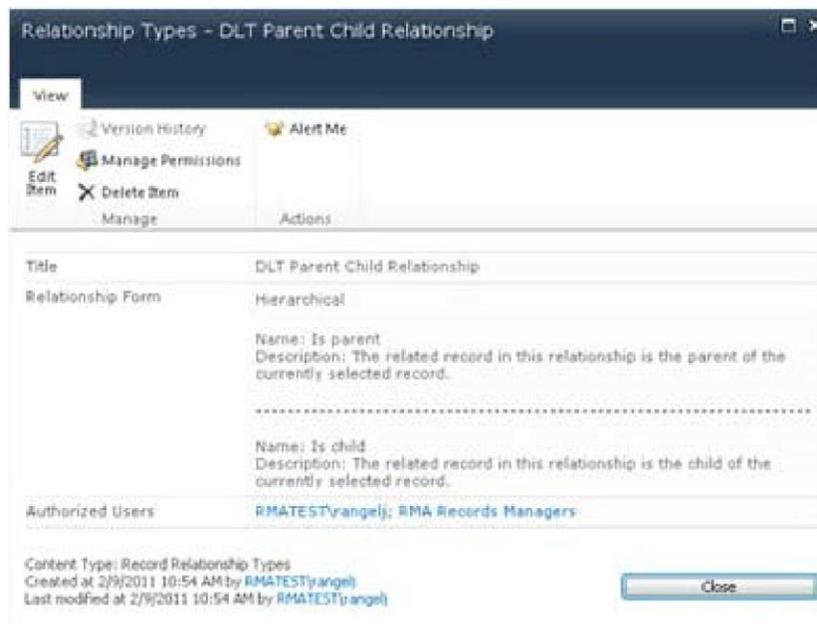   ● Click **Items** to display the header ribbon.

Figure 4-24 Related Records View Item

2. Select **View Item** on the header ribbon. The **Related Records View** dialog box opens displaying the Record Relationship details in read only mode. This dialog box is the same for Hierarchical and Non Hierarchical relationship types.
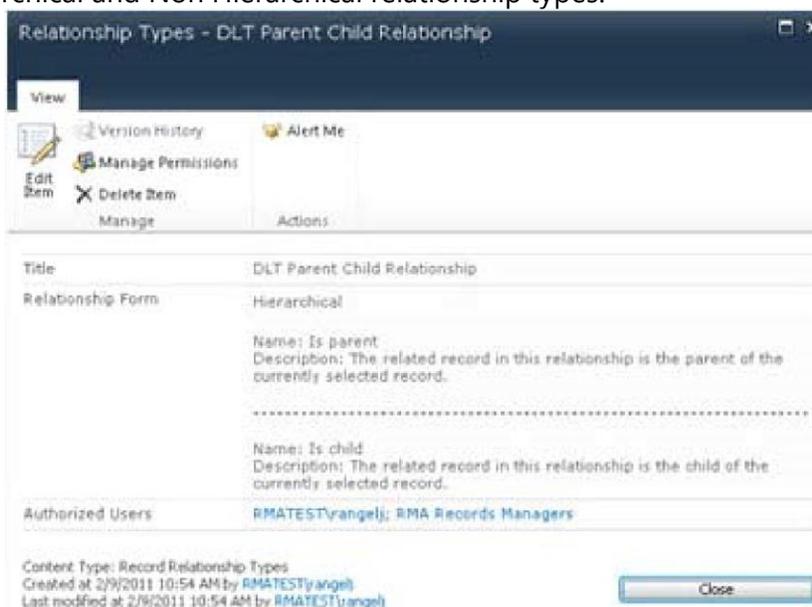

Figure 4-25 Viewing a Relationship Type Dialog Box

3. Click **Close** to return to the **Related Records View** list.

5 Period Definitions

Period Definition functionality is available in a SharePoint Records Center with Compliance Suite enabled. To use the Period Definition features, Compliance Suite must be installed and the Gimmal RMA Period Definition Content Type, Gimmal RMA Period Definitions List, and Gimmal RMA Period Management Site Column features must be active.

Compliance Suite supports user defined Period Definitions. A Period Definition is a unit of time or frequency that defines recurring records management processes and actions. Period Definitions support the management of records based on your organization's record management policies. Features of Period Definitions support are:

- Cutoff Processing
- Vital Records Review

Compliance Suite provides the ability to create, edit, view, or delete Period Definitions using a SharePoint list. By default, this list is created in your records center. If you are using multiple record centers with the Period Feature enabled, each site has a period definition list. You can use period management settings, which enable your record's center to point to another site's period default list.

In addition to the **Period Definitions View** list, Period Definitions (also known as Periods) can be managed using the **File Plan Builder: Periods** in your SharePoint Records Center.

In the site setting compliance section, there is a **Period Management Settings** page, as shown in the following figure. There are two text boxes for inheritances, including one that allows you to specify a definition list included on the screen.
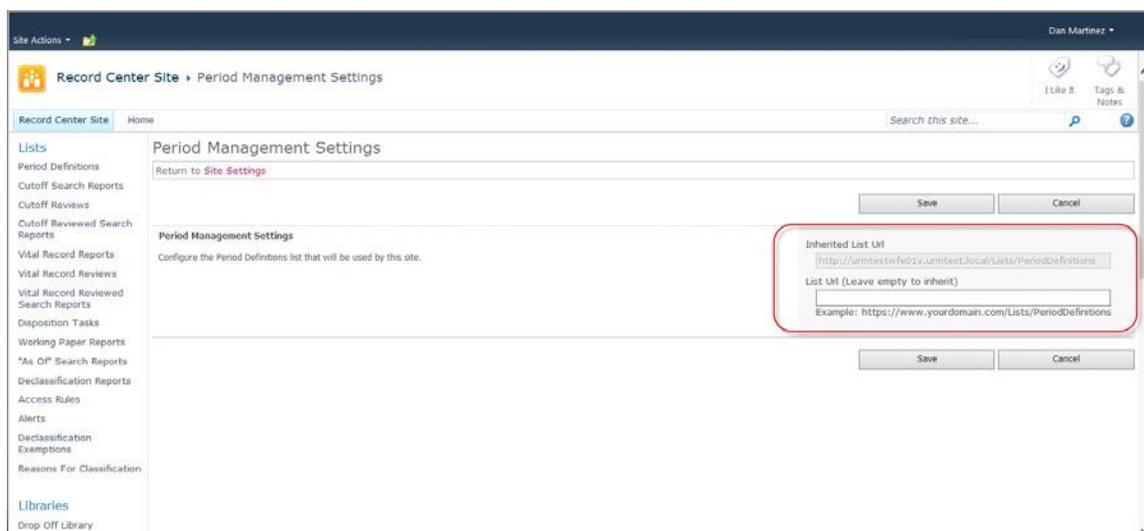

Figure 5-1 Period Definitions Period Management Settings

Intended User: Records Manager

To access the Period Definitions View list:

1. Open a SharePoint Records Center. The Records Center Home Page opens.

2. Select **Libraries** and then **Period Definitions**.

   A list view of all Period Definitions defined in your Site Collection displays.

   The following table describes the **Period Definitions View** list.

Table 5-1 Period Definitions View

LIst View Heading	Description
Period Name	Unique name that differentiates the Period Definition from other Period Definitions.
	The **Period Name** is used on the **Record Container** dialog boxes as the selection list for **Vital Record Review Indicator: Review Period Cycle** and **Cutoff Criteria: Enable Periods → Period Type** menu. The **Period Name** is also used on the **Record Item** dialog boxes as the selection list for **Cutoff Criteria: Enable Periods → Period Type** dropdown.
	Example: Calendar Year
Period Description	Descriptive statement used to further differentiate the Period Definition from other Period Definitions.
Modified	When the access rule was last modified.
Modified By	Compliance Suite username of the user who last modified the rule.

5.1 Creating a Period Definition

Before a period can be used for Vital Records or Cutoff Processing, you must create a Period Definition.

1. From the **Period Definitions View**, there are two ways to initiate the period definition creation process.

   - Click **Add new item** or **+ new item** from the bottom of the list.

   - Select the **Items** tab. In the header ribbon, select **New Item** and then select **Period Definition**.

Figure 5-2 Period Definitions Create New Period Definition

- A **Period Definitions - New Item** dialog box opens with fields for creating a new Period Definition.

Figure 5-3 Period Definitions Create New Period Definition

2. (**Required**) Enter the **Period Name**. The **Period Name** is a unique identifier for the new Period Definition. It populates the **Vital Records Review Indicator: Review Period Cycle** and **Cutoff Criteria: Enable Periods** menu in **Record Container** and **Record Item** dialog boxes.

3. Enter a **Period Description**. The **Period Description** is a descriptive statement that defines the purpose of this Period Definition.

4. (**Required**) Enter the **Period Start Date**. The **Period Start Date** defines the first calendar date (MM/DD/YYYY) of the first period to be calculated. To select a date from a calendar, click the Date Selector button in this field. The calendar feature uses the standard SharePoint calendar to select a date.

Note:

The Period Start Date defaults to the date the period was created, so you must enter the correct date.

5. (**Required**) Select the **Period Duration**. The **Period Duration** defines the frequency for processing Record Container(s) or Record Item(s) assigned this Period Definition. The options are **Daily**, **Weekly**, **Monthly**, and **Yearly**.

6. If the selected **Period Duration** is **Daily**, the dialog box updates with the following fields:

Figure 5-4 Period Definitions Create New Period Definition Daily

Enter **Every** [number] **Days**. Example: *Every 1 day(s)*.

7. If the selected **Period Duration** is **Weekly**, the dialog box updates with the following fields:

Figure 5-5 Period Definitions Create New Period Definition Weekly

Enter **Every** [number] **week(s)** on [Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday] Example: Every 2 weeks on Wednesday

8. If the selected **Period Duration** is **Monthly**, the dialog box updates with the following fields:

Figure 5-6 Period Definitions Create New Period Definition Monthly Dialog Box

Select one of the following options:

- Enter the **Day** [numerical day of month] **of every** [number] **month(s)**. Example: Day 30 of every 2 month(s).

- Enter **The** [first, second, third, fourth, or last] [day, weekday, weekend day, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday] **of every** [number of months] **month(s)**. Example: The first Friday of every 3 months.

9. If the selected **Period Duration** is **Yearly**, the dialog box updates with the following fields:
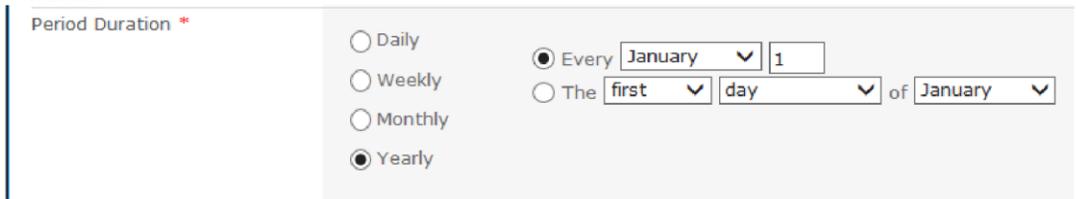
Figure 5-7 Period Definitions Create New Period Definition Yearly Dialog Box

Select one of the following options:

- Enter **Every** [name of month] [date in month]. Example: Every January 1.

- Enter **The** [first, second, third, fourth, or last], [day, weekday, weekend day, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday] **of** [name of month]. Example: The first Monday of January.

10. Click **Save** to create the new Period Definition. The changes are displayed in the **Period Definitions View** list. Click **Cancel** to return to the **Period Definitions View** list without creating a new Period Definition.

11. After the new Period Definition is saved, the new Period Definition is displayed as a selection in the Vital Records Review Indicator: Review Period Cycle and Cutoff Criteria: Enable Periods menu in the Record Container and Record Item dialog boxes.

Note:

Period Definitions created through this **Period Definitions View** list do not display in the **File Plan Builder: Periods** list.

5.2 Editing a Period Definition

To change an existing Period Definition, you must edit the Period Definition item.

1. From the **Period Definitions View**, select the Period Definition you want to edit. Only one Period Definition can be selected at a time.

2. Select the **Items** tab to display the header ribbon.
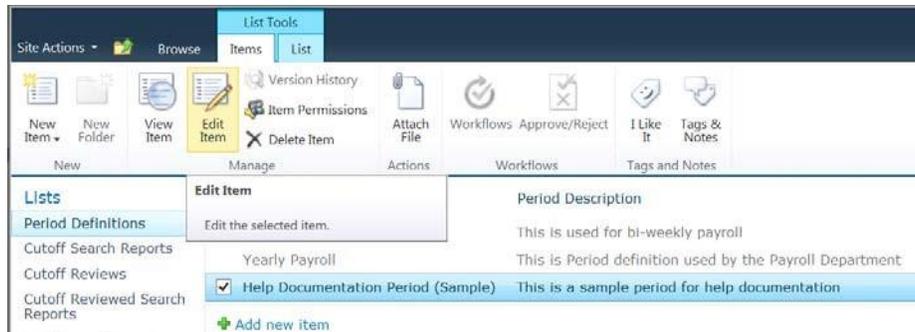
Figure 5-8 Period Definitions Edit Period Definition

3. Select **Edit Item** on the header ribbon. The **Period Definitions Edit** dialog box opens displaying the selected Period Definition details.
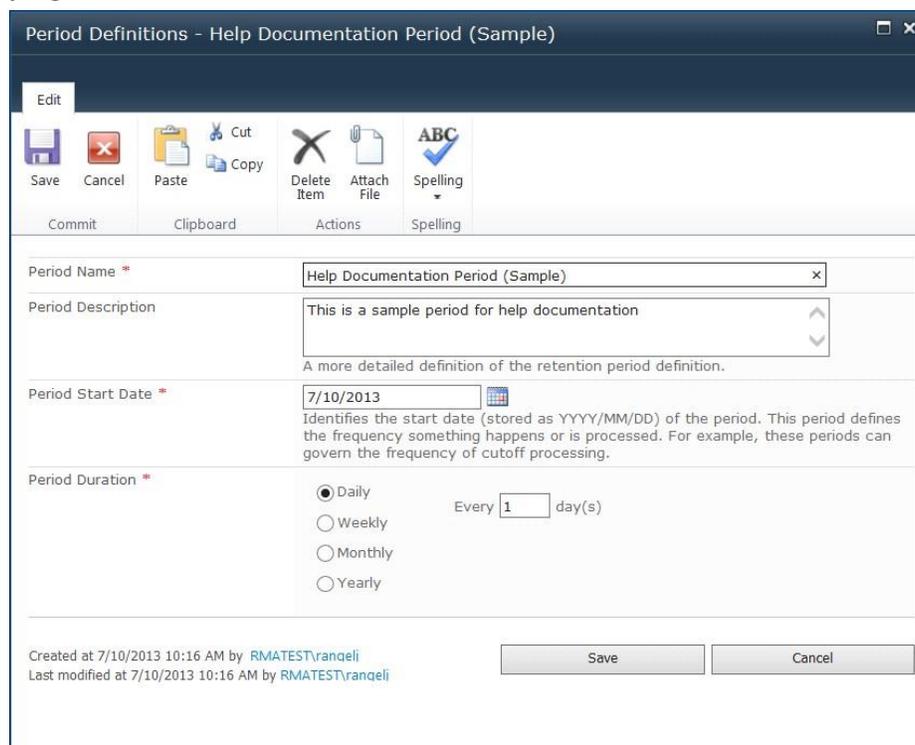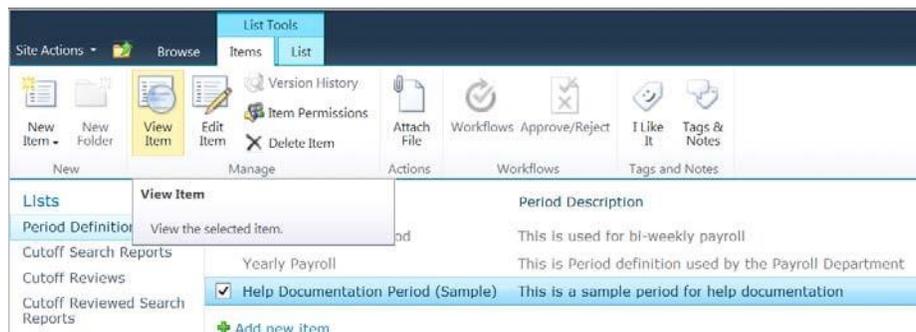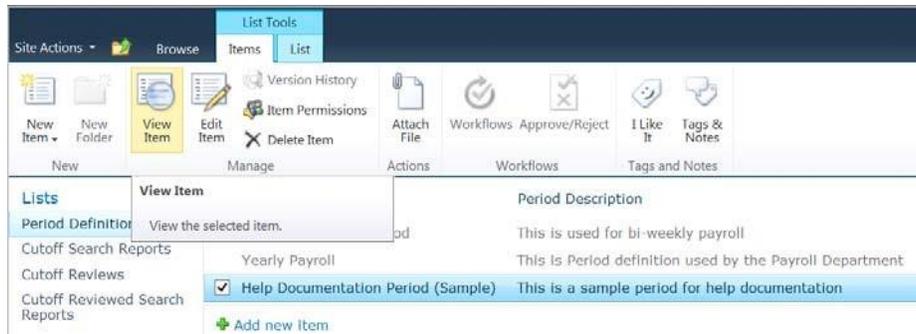

Figure 5-9 Period Definitions Edit Period Definition

4. Update the information in the fields you want to change.

● (**Required**) **Period Name** must be unique across all Period Definitions.

● (**Required**) **Period Start Date** updates affect existing Record Container(s) and Record Item(s) that use this Period Definition hence forth.

● (**Required**) **Period Duration** updates affect existing Record Container(s) and Record Item(s) that use this Period Definition hence forth. See Creating a Period Definition help for details on setting the **Period Duration.**

5. Click **Save** to update the Period Definition. You can see the changes in the **Period Definitions View** list. Click **Cancel** to return to the **Period Definitions View** list without updating the selected Period Definition.

6. After the Period Definition change is saved,

   ● Any existing Record Container(s) and Record Item(s) that use this Period have the updates applied hence forth.

   ● The updated Period Definition is displayed as a selection in the **Vital Records Review** I**ndicator: Review Period Cycle** and **Cutoff Criteria: Enable Periods** menu in the **Record Container** and **Record Item** dialog boxes.

Note:

Period Definitions updated through this **Period Definitions View** list are not updated in the **File Plan Builder: Periods** list.

5.3 Viewing a Period Definition

To view the details of an existing Period Definition, you must view the Period Definition item.

1. From the **Period Definitions View**, select the Period Definition you want to view. Only one Period Definition can be selected at a time. When a Period Definition is selected the **List Tools → Items** header ribbon opens.

Figure 5-10 Period Definitions View Period Definition

2. Select **View Item** on the header ribbon. The **Period Definitions View** dialog box opens displaying the Period Definition details in read-only mode.

Figure 5-11 Period Definitions View Period Definition Detail Dialog Box

3. From the **Period Definitions View**, you can Edit, Delete, or Manage Permissions of the selected Period Definition.

4. Click **Close** to return to the **Period Definitions View** list.

5.4 Deleting a Period Definition

To remove an existing Period Definition from your site, you must delete the Period Definition item.

1. From the **Period Definitions View**, select the Period Definition(s) you want to delete.

   If the selected Period Definition(s) is currently used by one or more Record Container(s) and/or Record Item(s), the affected items are updated with a new Period Definition, which currently defaults to the first Period Definition in the selection list. Delete with caution and ensure that the Period Definition(s) you are removing is not in use.

2. Select the **Items** tab to display the header ribbon.

3. Select **Delete Item** on the header ribbon. A prompt opens asking *Are you sure you want to send the item(s) to the site Recycle Bin?*
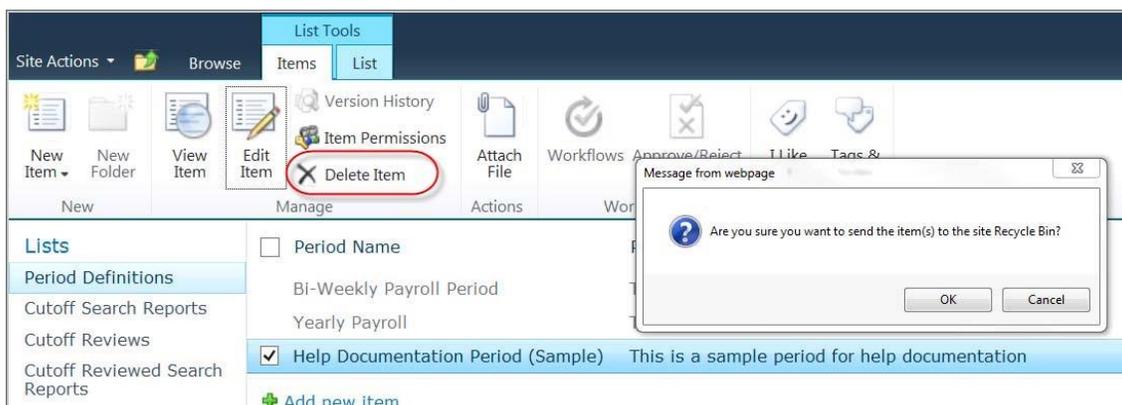
Figure 5-12 Period Definitions Delete Period Definition

4. Click **OK** and the Period Definition(s) is deleted and removed from the Period Definitions View list or click **Cancel** to return to the **Period Definitions View** list without deleting the selected Period Definition(s).

6 Event Management

Event Management functionality is available in a SharePoint Records Center with Compliance Suite enabled. To use the Event Management features, Compliance Suite Event Management must be installed and the following Event Management farm features must be active:

- GimmalSoft Compliance Suite - Event Management Service Installer
- GimmalSoft Compliance Suite - Event Management Action

The GimmalSoft Compliance Suite - Event Management Service is created and started in Central Administration.

Compliance Suite supports user defined Event Types and Event Instances. An Event Type is the definition of a happening that triggers records management processes and actions for a given record or Record Container. An Event Instance is the actual occurrence of the defined Event Type. In Compliance Suite, Event Management supports Cutoff Processing and Closing of Record Folders based on happenings that will take place at some unspecified/unknown time in the future. A few examples of Event Types include:

- Employee John Doe Termination
- Property ABC Sale
- Contract XYZ Expiration
- Project 123 Complete

There are two list views that support Event Management:

1. Manage Events List
   - **SharePoint Records Center → Compliance Suite → Event Management**
   - **SharePoint Records Center → Site Actions → Site Settings → Compliance Suite → Event Management**
2. Manage Event Instances
   - Right-click on a selected Event
   - Select View Instances of this Event

6.1 Event Types

Event Types define a happening that triggers records management processes and actions for a given record or Case Based Container. Event Types are used in Cutoff Processing as defined in the Cutoff Criteria: Enable Events for a Record Container(s) and/or Record Item(s).

Compliance Suite provides the ability to Create, Edit, View, Delete, or Manage Permissions for Event Types using a SharePoint list. In addition to the Manage Events list, Event Types can be

---

managed through the File Plan Builder: Events in your SharePoint Records Center. However, Event Types managed through the Manage Events SharePoint list cannot be managed in File Plan Builder: Events list.

Intended User: Records Manager

To access the **Manage Events** list:

1. Open a SharePoint Records Center. The Records Center Home Page opens.

2. You can access the **Manage Events** list by the following:

   - Select **Event Management** from the Compliance Suite header ribbon.

   - Select **Site Actions** and then select **Site Settings** from the header navigation.

   - Select **Event Management** under the **Compliance Suite** section.

The following table describes the **Manage Events** list with a description of each heading.

Table 6-1 Manage Events List

List View Heading	Description
Name	Unique name that differentiates the Event Type from other Event Types. The Name is used on the Record Container and Record Item dialog boxes as the selection list for **Cutoff Criteria: Enable Events** and then **Select Events**. Example: Project 123 Complete
Description	Descriptive statement used to further differentiate the Event Type from other Event Types.

6.1.1 Creating an Event Type

Before an event can be used for **Cutoff Processing**, an Event Type must be created.

1. From the **Manage Events** list, there are two ways to initiate the event type creation process.

   - Click **+Add New Event** link from the bottom of the list.

   - Select **Items** tab. In the header ribbon, select **New Event**.
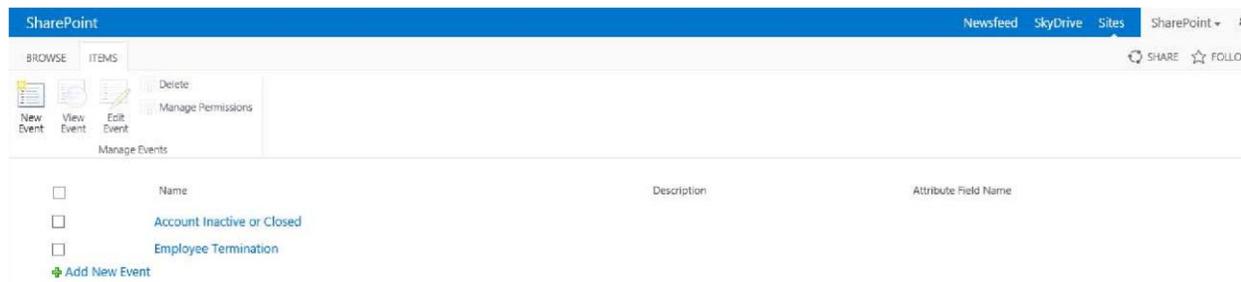
Figure 6-1 Event Management Create Event Type

2. The **Gimmal Compliance Suite - Event Management Service Application** dialog box opens with fields for creating a new Event Type.

Figure 6-2 Event Management Create Event Type Dialog Box

3. (**Required**) Enter the **Name**. The **Name** is a unique identifier for the new Event Type. It is used to populate the **Cutoff Criteria: Enable Events** selection in **Record Container** and **Record Item** dialog boxes.

4. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this Event Type.

5. Click **Save** to create the new Event Type. It displays in the **Manage Events** list. Click **Cancel** to return to the **Manage Events** list without creating a new Event Type.

6. After the new Event Type is saved, the new Event Type displays as a selection in the **Cutoff Criteria: Enable Events** in the **Record Container and/or Record Item** dialog boxes.

Note:

Event Types created through this Manage Events list do not appear in the File Plan Builder: Events list.

6.1.2 Editing an Event Type

To change an existing Event Type, you must edit the Event Type item. to edit an Event Type, you must have Update Event Item permission on the selected Event Type.

1. From the **Manage Events** list, select the Event Type you want to edit. Only one Event Type can be selected at a time. There are two ways to initiate editing an event type.

    ●   Select **Items** tab. In the header ribbon, Select **Edit Event.**

    ●   Select **Edit Event** from the action menu for the selected Event Type.
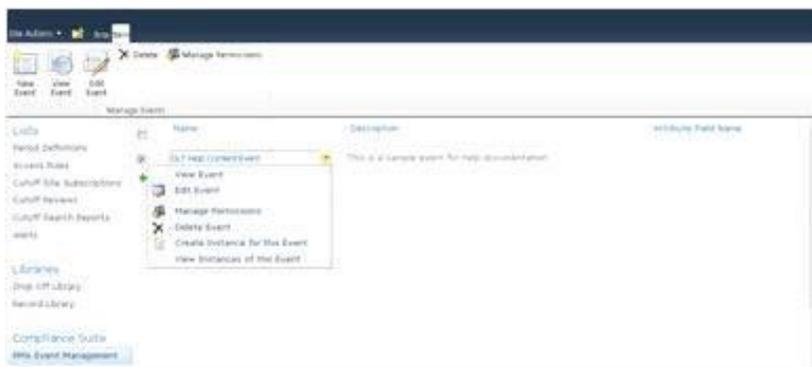
Figure 6-3 Event Management Edit Event Type

2. An **Update Event** dialog box opens displaying the selected Event Type details.

Figure 6-4 Event Management Edit Event Type Dialog Box

3. Update the information in the fields you want to change.

    ●   (**Required**) Name must be unique across all Event Types.

4. Click **Save** to update the Event Type. The changes are displayed in the **Manage Events** list. Click **Cancel** to return to the **Manage Events** list without updating the selected Event Type.

5. After the Event Type change is saved, the updated Event Type is displayed as a selection in the Cutoff Criteria: Enable Events in the Record Container and Record Item dialog boxes.

Note:

Event Types updated through this Manage Events list will not be updated in the File Plan Builder: Events list.

6.1.3 Viewing an Event Type

To view the details of an existing Event Type, you must view the Event Type item. to view an Event Type, you must have Read Event Item permission on the selected Event Type.

1. From the **Manage Events** list, select the Event Type you wish to view. Only one Event Type can be selected at a time. There are two ways to initiate viewing an event type.

   - Select **Items** tab. In the header ribbon, Select **View Event.**

   - Select **View Event** from the action menu for the selected Event Type.
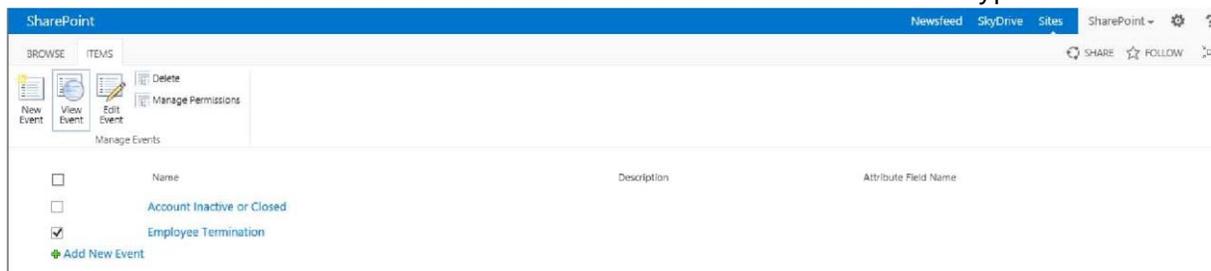
Figure 6-5 Event Management View Event Type

2. A **View Event** dialog box opens displaying the selected Event Type details in read only mode.
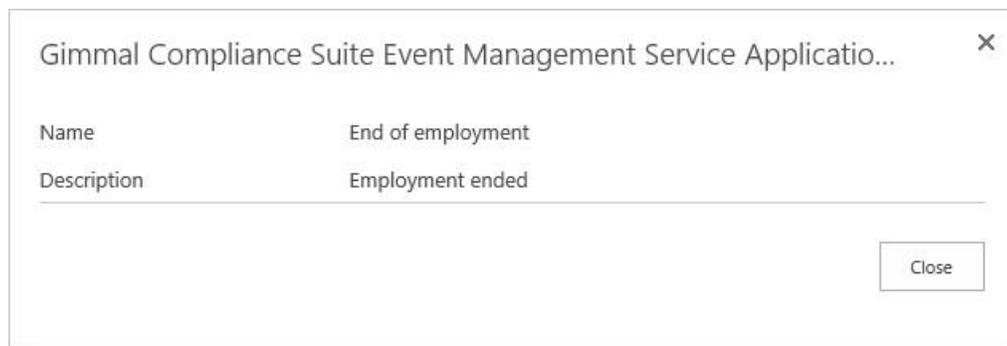
Figure 6-6 Event Management View Event Type Detail Dialog Box

3. From **View Event**, you can edit, delete, or manage permissions of the selected Event Type if you have the appropriate permission.

4. Click **Close** to return to the **Manage Events** list.

6.1.4 Managing Permissions for an Event Type

Compliance Suite events managed through the **Manage Events** list have a default security applied based on SharePoint groups and roles. For Event Types created through the **Manage Events** list, you should modify the permissions for Event Types and its' Event Instances through the **Manage Permissions** dialog box.

The following table describes the default groups and permissions for access and management of events in **SharePoint Records Center Manage Events** list.

Table 6-2 Manage Events Groups and Permissions

Group/Role	Permission
Compliance Suite Event Management - Service Application Administrator	Enables initial access to management of events.
	to manage events, a user must first be configured either directly or as a member of a group assigned to this role in the Compliance Suite Event Management - Service Application Administrator.
	To fully access Event Management features in SharePoint Records Center, a user must also be assigned a Compliance Suite Event Management Service Application group as described below.
	Once assigned a Compliance Suite group, any users in this role can create, update, view, delete, and manage permissions, and instantiate Event Instances for Event Types through the Manage Events list. These users do not need to be assigned permission through Manage Permission for an Event Type as described in the table below.
Manage Claims Admins	Any user added in this group will have the same access as user in Compliance Suite - Event Management Suite Event Management Service Application Administrator. This functionality is part of an environment where you cannot directly add users directly to the service application.
RMA Records Managers	Enables access to management of events through the Manage Events list in a SharePoint Records Center.
	To fully access Event Management features, a user in the RMA Records Managers group must also be assigned permission through Manage Permission for an Event Type. See the table below for permission assignment details.
RMA Local Records Officers	Same permission as RMA Records Managers.
RMA Administrators	Same permission as RMA Records Managers.

Site Owners	Same permission as RMA Records Managers.

Table 6-2 Manage Events Groups and Permissions

Group/Role	Permission
Site Members	No default permission. Site Members are typical end users. A user in this group must be assigned permission through Manage Permission for an Event Type to have access to view an Event Type. See the next table for permission assignment details.

A user with the appropriate group assignment as described in the previous table can modify the permissions for a specific Event Type and its Event Instances through the **Manage Permissions** dialog box.

The following table describes the **Manage Permission** dialog box with a description of each permission field.

Table 6-3 Manage Permission Dialog Box Fields

Field	Description
Read Event Item Users	Enables access to View Event and View Event Instance to selected users and groups. Enables access to select the Event Type in the Cutoff Criteria: Enable Events field in Record Container and Record Item dialog boxes. By default the creator of the Event Type will have access to view the Event Type and Event Instance(s).
Update Event	Enables access to Edit Event and Edit Event Instance to selected users and groups.
Item Users	By default the creator of the Event Type will have access to edit the Event Type and Event Instance(s). By default the creator of the Event Instance will have access to edit the Event Instance. If a user is granted Update Event Item Users permission, the user also has Read Event Item Users permission.

Table 6-3 Manage Permission Dialog Box Fields

Field	Description

Delete Event Item Users	Enables access to Delete for the Event Type and Event Instances to selected users and groups.
	By default the creator of the Event Type will have access to delete the Event Type and Event Instance(s).
	By default the creator of the Event Instance will have access to delete the Event Instance.
	If a user is granted **Delete Event Item Users** permission, the user also has **Read Event Item Users** and **Update Event Item Users** permissions.
Trigger Event Item Users	Enables access to *Create Event Instance* to selected users and groups.
	By default the creator of the Event Type will have access to create Event Instances.
	If a user is granted Trigger Event Item Users permission, the user also has Read Event Item Users permission.
Manage Permissions Users	Enables access to Manage Permissions for the Event Type to selected users and groups.
	By default the creator of the Event Type will have access to Manage Permissions.
	If a user is granted Manage Permissions Users permission, the user also has Read Event Item Users, Update Event Item Users, Delete Event Item Users, and Trigger Event Item Users permission.

By default, a Records Manager assigns a user to have Read Access to Events in the site. To define the Access Control List (ACL) for each event you should check the **User Defined ACL** check box, and then each event will have access based on what is defined in ACL.

For each permission field described, it is recommended to add user groups such as Human Resources instead of individual user names. There are two ways to add **Users/Groups**:

- Semicolon-separated list

- Standard SharePoint address book lookup To manage permissions for an Event Type:

- From the **Manage Events** list, select the Event Type you want to manage permissions. Only one Event Type can be selected at a time. There are two ways to initiate manage permissions for an event type.
  - Select **Items** tab. In the header ribbon, select **Manage Permissions**.
  - Select **Manage Permissions** from the action menu for the selected Event Type.
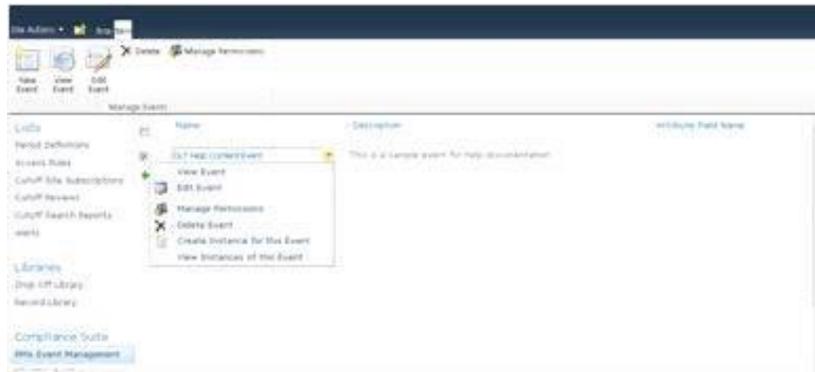
Figure 6-7 Event Management Mange Event Type Permissions

- A **Manage Permissions** dialog box opens displaying the selected Event Type permission details.
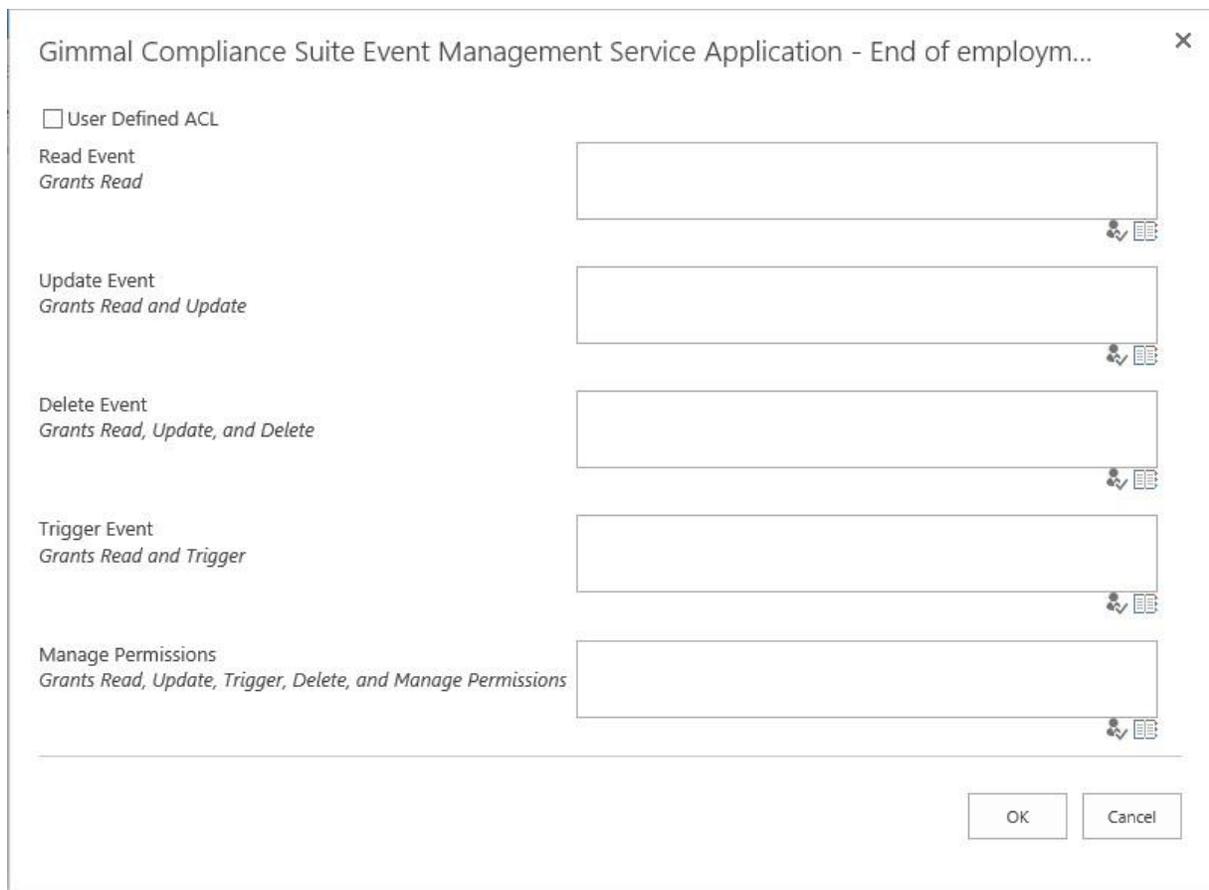
Figure 6-8 Manage Permissions Dialog box

- Enter the **Read Event** users/groups.
- Enter the **Update Event** users/groups.
- Enter the **Delete Event** users/groups.

- Enter the **Trigger Event** users/groups.

- Enter the **Manage Permissions** users/groups.

- Click **OK** and the Event Type permissions are updated or click **Cancel** to return to the **Manage Events** list without updating the selected Event Type permissions.

- After the Event Type permission changes are saved, the selected users/groups will have the updated permissions for this Event Type and any Event Instances based on this Event Type.

Note:

Event Type permissions managed through this Manage Events list will not affect permission in the **File Plan Builder: Events** list.

6.1.5 Deleting an Event Type

To remove an existing Event Type from your site, you must delete the Event Type item. to delete an Event Type, you must have Delete Event Item permission on the selected Event Type.

1. From the **Manage Events** list, select the Event Type(s) you want to delete. There are two ways to initiate deleting an event type.

   - Select **Items** tab. In the header ribbon, Select **Delete**.

   - Select **Delete Event** from the action menu for the selected Event Type(s).

   - A prompt opens asking 'Are you sure you want to delete the event(s)?'

2. Click **OK** and the Event Type(s) is deleted and removed from the **Manage Events** list or click **Cancel** to return to the **Manage Events** list without deleting the selected Event Type(s).

   - If the selected Event Type(s) is currently used by one or more Record Container(s) and/ or Record Item(s), the affected items will remain unchanged. Please delete with caution and ensure the Event Type you are removing is not in use.

   - All Event Instances associated with the selected Event Type(s) will be deleted along with the Event Type.

Note:

Event Types deleted through this **Manage Events** list will not be removed in the File Plan Builder: Events list.

6.2 Event Instances

Event Instances define the actual occurrence of an Event Type. For example, if the Event is Project 123 Complete an instance of the Event Type would be the completion of the project on 04/01/2011.

Compliance Suite provides the ability to Create, Edit, View, or delete Event Instances using a SharePoint list. Events Instances are always managed in context with a selected Event Type.

Intended User: Records Manager

To access the **Manage Event Instances** list for a selected Event Type:

1. From the **Manage Events** list, select the Event Type you wish to manage instances.

2. Select **View Instances of this Event** from the action menu of the selected Event Type.
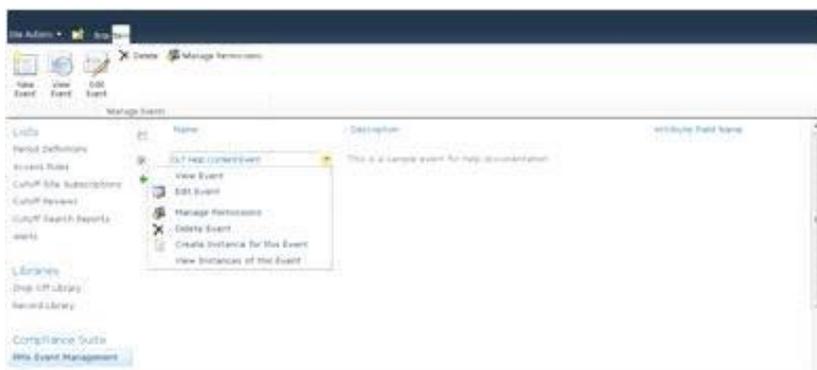
Figure 6-9 Event Management View Instances of Event

3. To return to the **Manage Events** list, Select **Back to List Events** from the **Manage Event Instances** header.

Figure 6-10 Event Management Back to List Events

The following table describes the Manage Event Instances list with a description of each heading.

Table 6-4 Manage Event Instances

List View Heading	Description
Event Instance Id	Automatically generated identification number. Provides a unique identifier for each Event Instance based on the selected Event Type. Example: 1
Attribute Field Name	This field is not currently used by the Compliance Suite application.
Date	Calendar date the event instance occurred. Example: For event type Project 123 Complete, if Product 123 completed on 04/01/2011, this field value would be 04/01/2011.

6.2.1 Creating an Event Instance

In Compliance Suite to actively use an Event Type for **Cutoff Processing** an Event Instance must be created for the Event Type. Anytime an Event Type occurs in the application, an Event Instance should be created. to create an Event Instance, you must have Trigger Event Item permission on the selected Event Type.

1. From the **Manage Event Instance** list, there are two ways to initiate the event instance creation process.

   - Click **+Add New Event Instance** link from the bottom of the list.

   - Select **Items** tab. In the header ribbon, Select **New Event Instance**.

Figure 6-11 Event Management Create Event Instance

2. From the **Manage Event** list, you can also initiate the event instance creation process. Select **Create Instance for this Event** from the action menu for the selected Event Type. A **Create Event Instance** dialog box opens with fields for creating a new Event Instance.

Figure 6-12 Event Management Create Event Instance Dialog Box

---

Note:

While you can schedule more than one instance for a single event, Cs only uses the first instance's Date. For a more extensible mechanism for event instances and for selective grouping of records affected by an event instance Gimmal's Enterprise Events can be used as an alternative.

---

3. **Event Name** is a read only field that displays the name of the Event Type for this Event Instance.

4. (**Required**) Enter a **Date**. The **Date** defines the calendar date the event instance occurred. The date you enter is set as the cutoff date, which allows the ability to back date records for retention purposes. To select a date from a calendar, click the Date Selector button in this field. The calendar feature uses the standard SharePoint calendar to select a date.

5. **Attribute Field Name** is currently not used by the Compliance Suite application.

6. Click **Save** to crate the new Event. It is displayed in the **Manage Event Instances** list. Click **Cancel** to return to the Manage Event Instances list without creating a new Event Instance.

6.2.2 Editing an Event Instance

To change an existing Event Instance, you must edit the Event Instance item. To edit an Event Instance, you must have Trigger Event Item permission on the selected Event Type.

1. From the **Manage Event Instance**s list, select the Event Instance you want to edit. Only one Event Instance can be selected at a time. There are two ways to initiate editing an event instance.

   ● Select **Items** tab. In the header ribbon, Select **Edit Event Instance**.

- Select

    Edit Event Instance from the action menu for the selected Event Instance.

Figure 6-13 Event Management Edit Event Instance

2. An **Update Event Instance** dialog box opens displaying the selected Event Instance details.
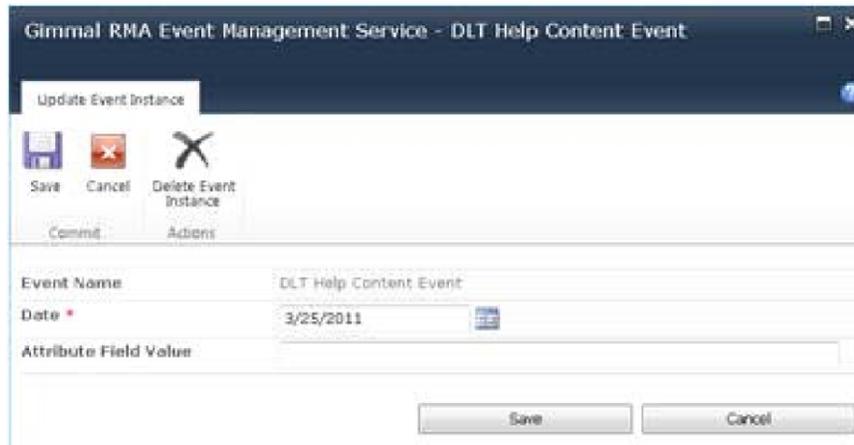
Figure 6-14 Event Management Update Event Instance Dialog Box

3. Update the information in the fields you want to change.

    - Event Name is read only.

4. From the **Update Event Instance** dialog box, you can delete the selected Event Instance if you have the appropriate permission.

5. Click **Save** to update the Event Instance. The changes are displayed in the **Manage Event Instances** list. Click **Cancel** to return to the **Manage Event Instances** list without updating the selected Event Instance.

6.2.3 Viewing an Event Instance

To view the details of an existing Event Instance, you must view the Event Instance item. To view an Event Instance, you must have Read Event Item permission on the selected Event Type.

- Select

1. From the **Manage Event Instances** list, select the Event Instance you want to view. Only one Event Instance can be selected at a time. There are two ways to initiate viewing an event instance.

   Items tab. In the header ribbon, select **View Event Instance**.

- Select **View Event Instance** from the action menu for the selected Event Instance.
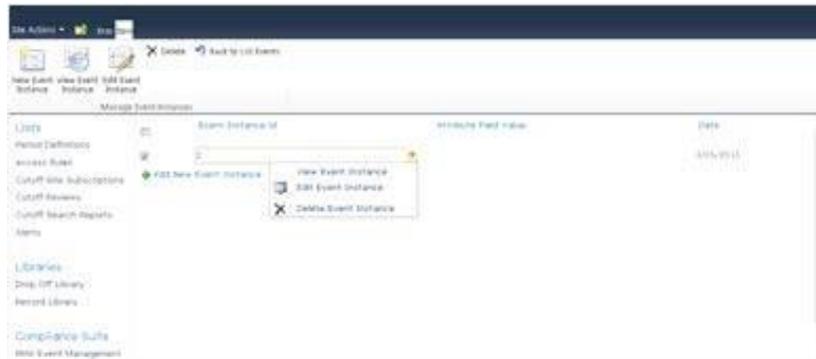
Figure 6-15 Event Management View Event Instance

2. A **View Event Instance** dialog box opens displaying the selected Event Instance details in read-only mode.

Figure 6-16 Event Management View Event Instance Detail Dialog Box

3. From the **View Event Instance** dialog box, you can edit or delete the selected Event Instance if you have the appropriate permission.

4. Click **Close** to return to the **Manage Event Instances** list.

6.2.4 Deleting an Event Instance

To remove an existing Event Instance from your site, you must delete the Event Instance item. To delete an Event Instance, you must have Trigger Event Item permission on the selected Event Type.

- Select

1. From the **Manage Event Instances** list, select the Event Instance(s) you want to delete. There are two ways to initiate deleting an event instance.

   - Select **Items** tab. In the header ribbon, select **Delete**.

     Delete Event Instance from the action menu for the selected Event Instance.

Figure 6-17 Event Management Delete Event Instance

2. A prompt opens with the message *Are you sure you want to delete the event instance(s)?*

3. Click **OK** and the Event Instance is deleted and removed from the **Manage Event Instances** list or click **Cancel** to return to the **Manage Event Instances** list without deleting the selected Event Instance.

7 Vital Records

A vital record is any record in an organization that would be required to reconstitute the organization's normal business functions after a major disaster. This is referred to as Continuity of Operations (COP). Records managers are responsible for identifying an organization's vital records and ensuring those records are maintained in a manner pursuant to internal policy and external regulations.

Many vital records require periodic review and updating. A good example of this is an organization's Emergency Notification List. This record is a list of the first people (and organizations) to call in the event of a major disaster. Because people change jobs and companies can go out of business, it is important that someone at every organization periodically review the Emergency Notification List to ensure that all the information is current and accurate.

The Compliance Suite vital records review process consists of the following steps:

1. Records Manager marks the record containers as vital by setting the Vital Record Review Indicator site column of the record container.

2. Records Manager searches for vital record containers that need review by clicking the Due for Vital Review link on left pane of the Records Center Administration site.

3. Records Manager views past search reports for the vital record libraries and record containers that need review by visiting the Vital Records Reports list on the Records Center Administration site.

4. Records Manager launches Vital Records Review workflows on the selected vital record containers that need review by viewing past search reports from the Vital Records Reports list.

5. An email notification is sent to the Vital Records Reviewers.

6. Local Records Officer (LRO) (assigned reviewer for the workflow task) reviews the Vital Records Review workflow task by clicking the task link in the email received or by going to the Workflow Task list.

7. Records Manager views the workflow and task history by viewing the workflow history from the Vital Records Reviews list or the workflow task history from the Workflow Task list.

Intended User: Compliance Suite Administrator, Records Manager, Local Records Officer

The following table describes the Vital Records lists and the functions associated with each list.

Table 7-1 Vital Records Functions

List Heading	Description and Function
Vital Record Reports	Custom list that store reports for the vital record containers due for review and initiate vital records review workflows on them.

Vital Record Reviews	Custom list that store information about the vital record containers on which the Vital Record Workflow has been started.

7.1 Indicating Vital Records

Indicating vital records functionality is available in a SharePoint Records Center with Compliance Suite and Vital Records enabled.

Compliance Suite Records Manager can indicate record containers that are considered vital. Compliance Suite enables records managers to indicate vital records in a child container of a parent record container. Compliance Suite also enables records managers to edit existing vital records properties in a container.

7.1.1 Indicating Vital Records in a New Container

To indicate vital records in a record container, you must create the container.

1. From the header ribbon, click **New Container**.
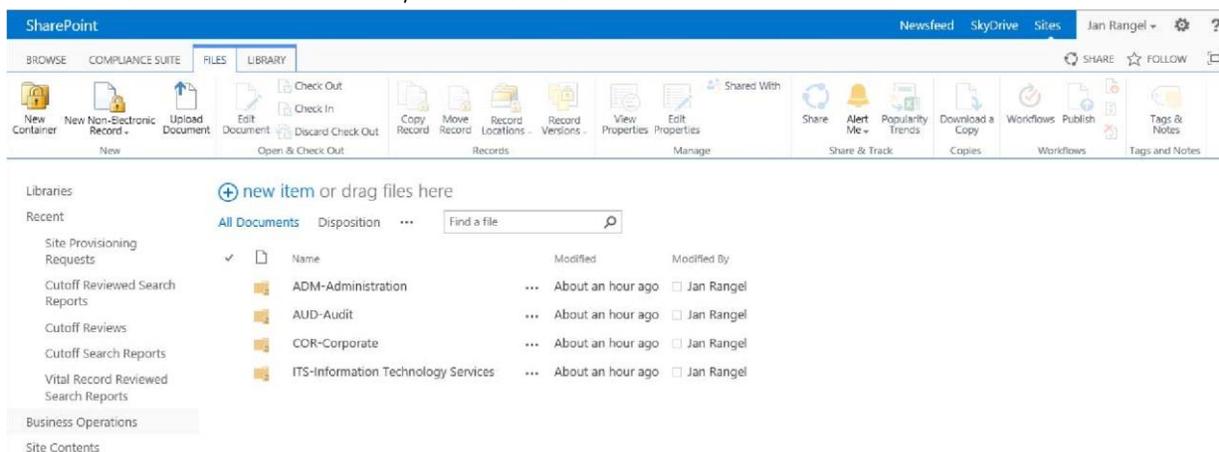
Figure 7-1 Vital Records Indicating Vital Records New Container

A **New Folder** dialog box opens with fields for creating a new container.
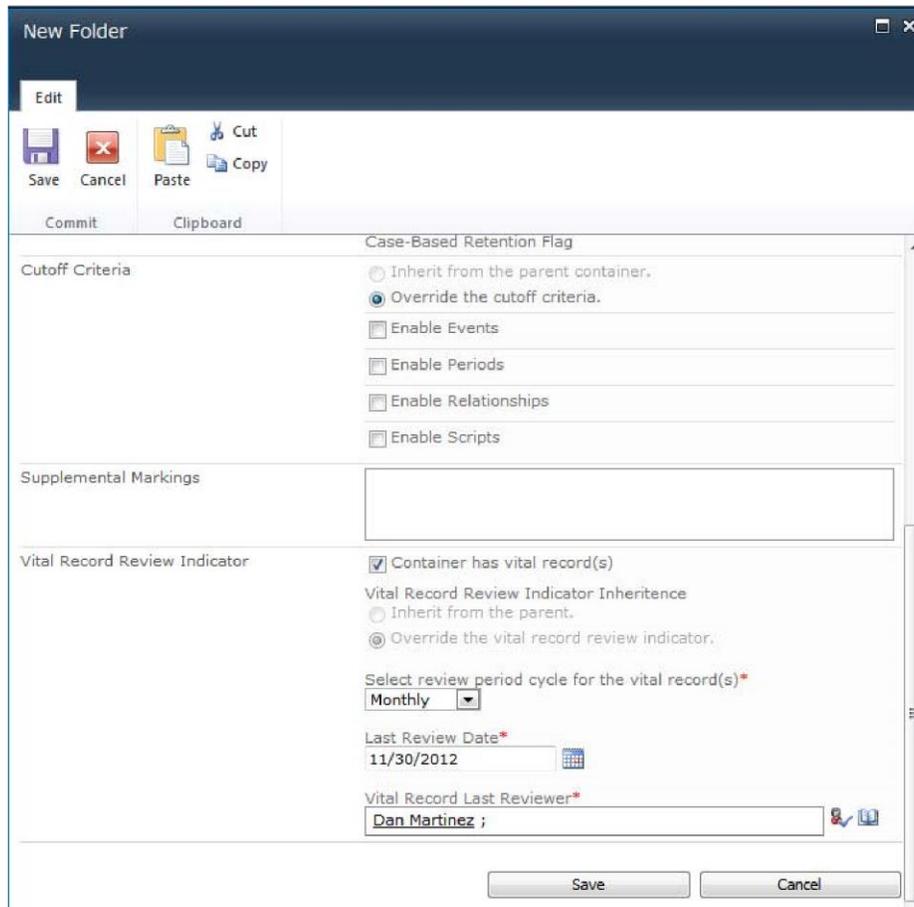
Figure 7-2 Vital Records Indicating Vital Records New Folder Dialog Box

2. Complete all the fields that are marked with a red asterisk.

3. Scroll down to the **Vital Record Review Indicator** section. Select the **Container has vital record(s)** check box to indicate that the container contains vital records.

4. (**Required**) Select the review period cycle in the **Select review period cycle for the vital records** field. Refer to Chapter 5 Period Definitions for additional information.

5. (**Required**) Enter the last review date in the **Last Review Date** field. The **Last Review Date** is the date the records in the new container were last reviewed and the date from which the new review date will be calculated. (The initial **Last Review Date** can be set to any date.)

6. (**Required**) Type the name of the last reviewer in the **Vital Reviewer** field. This is the person or group that last reviewed the record and is used as the default when successive reviews are performed.

7. Click **Save** to create the new container. It displays in the record container list. Click **Cancel** to return to the record container list without creating a new container.

7.1.2 Editing Vital Records Properties in a Container

To change existing vital records properties in a record container, you must edit the container.

1. From the container list screen, there are two ways to edit vital records properties.

   ● Select the library list and click on the **Edit Properties** menu.
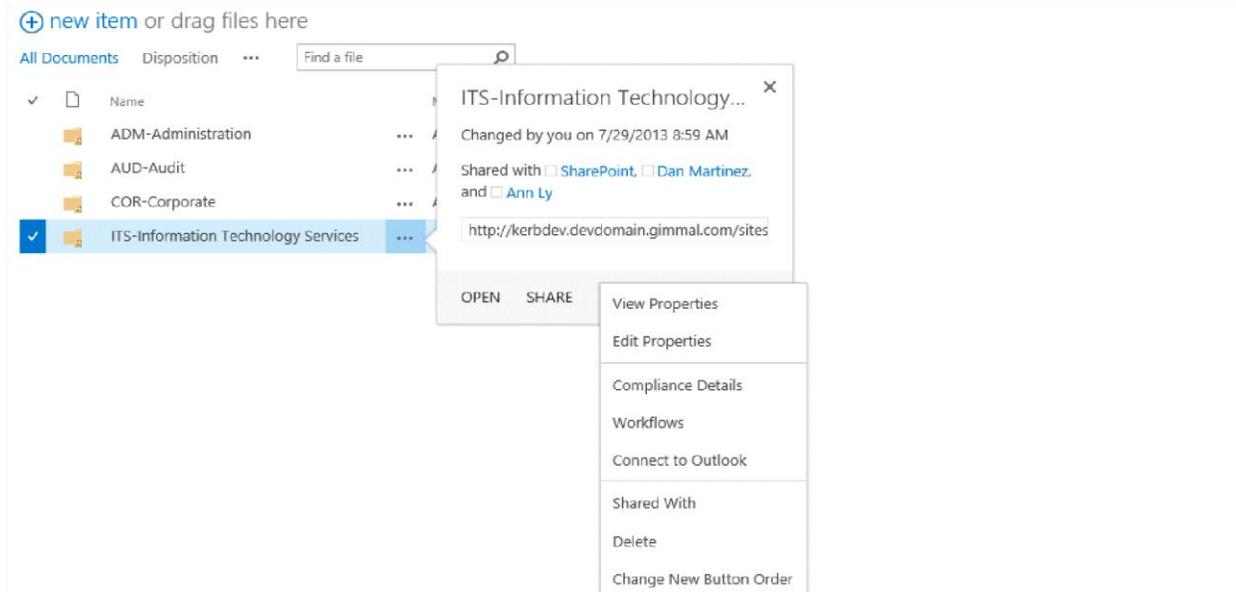
Figure 7-3 Vital Records Edit Properties

   ● You can also select L**ibrary Tools,** click the **Documents** tab. In the header ribbon, select **Edit Properties**.

2. The **Edit Container** dialog box opens with fields for editing the container.

3. Scroll down to the **Vital Record Review Indicator** fields and update the necessary fields.

Figure 7-4 Vital Records Indicating Vital Records Review Indicator

4. Click **Save** to update the container. Click **Cancel** to return to the container list screen without editing the container.

7.1.3 Indicating Vital Records in a Child Container

To indicate that a child container of a parent record container contains vital records, perform the following steps.

1. From the parent record container, select the **Files** tab.

2. In the header ribbon, click **New Container**.

3. A New Folder dialog box opens with fields for creating a new container.

4. Scroll down to the Vital Record Review Indicator field. Select the **Container has vital record(s)** check box. The **Select review period cycle for the vital record(s)**, L**ast Review Date**, and **Vital Record Last Reviewer** fields default to the settings of the parent container.

Note:

When creating a child folder where the parent is under a vital record review, you can inherit the vital settings from the parent, add your own settings, or choose to not make it vital at all.

---

5. Click **Save** to create the new container. It displays in the parent record container list. Click **Cancel** to return to the parent record container list without creating a new container.

7.1.4 Removing a Vital Record on a Record Container

To remove a vital record indicator on a record container, you must edit the container.

1. Select the container twice to display the action menu and click **Edit Properties**.
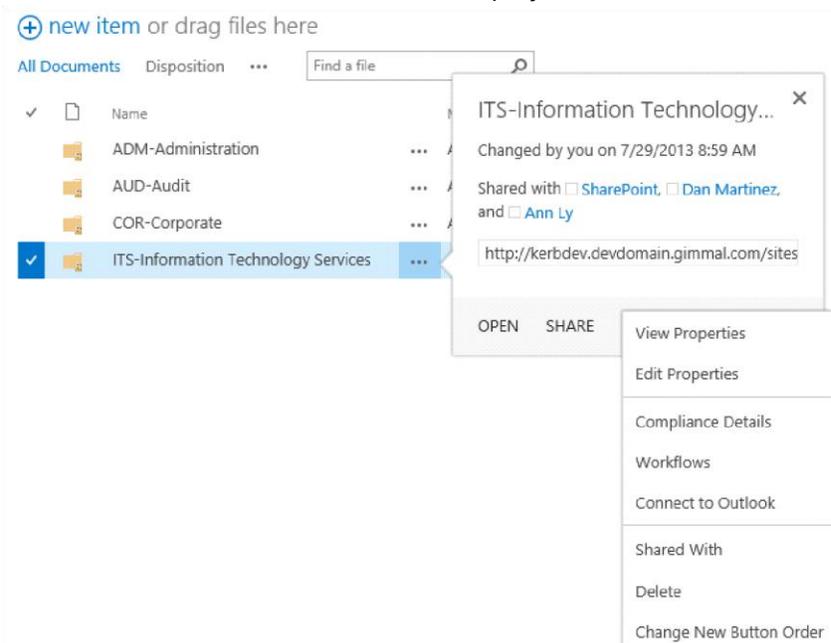
Figure 7-5 Vital Records Edit Properties

An *Edit Container* dialog box opens with fields for editing the container.

Figure 7-6 Vital Records Edit Container Dialog Box

2. Scroll down to the **Vital Record Review Indicator** field and deselect the **Container has vital record(s)** check box. The **Select review period cycle for the vital records, Last Review Date**, and **Last Reviewer** fields are removed from the **Vital Record Review Indicator** field.

Figure 7-7 Vital Records Container Edit Container, Has Vital Records Check box

3. Click **Save** to save changes to the record container. Click **Cancel** to return to the record library list without creating a new container.

Note:

If you later indicate that the container contains vital records, you must reset values in the Select review period cycle for the vital records, Last Review Date, and Vital Record Last Reviewer fields.

7.2 Searching Vital Records

Searching vital records functionality is available in a SharePoint Records Center with Compliance Suite and Vital Records enabled.

Compliance Suite Records Managers can search for vital record containers in two ways:

1. Search vital records that need review by utilizing the **Vital Records Due for Review** screen.

2. Search vital records that have already been reviewed by utilizing the **Reviewed Vital Records** screen.

7.2.1 Searching Vital Records Due for Vital Review

To search for Vital Records Due for Vital Review:

1. Select **Due for Vital Review** in the **Vital Records** section of the Compliance Suite header ribbon. The **Due for Vital Review** screen displays.

2. You must specify the search criteria for vital records due for vital review. Enter the title, select a review eligibility date and select the search sites. The following is an example of the search criteria.

Figure 7-8 Vital Records Due for Vital Review Screen

3. (**Required**) In the **Review eligibility date** field, enter today's date or a future date that vital records are eligible for review.

4. To select site(s) containing vital records, click on the site and click **Submit**. At least one site must be selected.

5. Click **Submit** to begin the search. A message similar to the following displays:

Figure 7-9 Vital Records Search Report Submitted Message

If you need to exit this screen while waiting for the submitted report to complete, you can click the **Vital Record Reports** under the *Lists* section in the Quick Launch.

6. Click the link and once the search is complete, the following screen displays.

Figure 7-10 Vital Records Search Report List

7. The **Vital Record Search Report** dialog box displays the search results. Click the report name to view the search results for that report.

Figure 7-11 Vital Record Search Report Dialog Box

7.2.2 Processing Vital Record Reviews

Refer to section 6.3, "Vital Records Review Workflows" for this procedure.

7.2.3 Searching Reviewed Vital Records

To search for Reviewed Vital Records:

1. Select **Due for Vital Review** in the **Vital Records** section of the Compliance Suite header ribbon. The *Reviewed Vital Records* screen opens with fields for searching reviewed vital records.

Figure 7-12 Vital Records Reviewed Vital Records Screen Search Fields

2. Enter a unique title for the search in the **Vital Report Title** field.

3. (**Required**) In the **Review Date Range** section, enter review dates in the **Start Date** and **End Date** fields.

4. Click the box next to the site(s) you want to search. An example completed search entry follows.

Figure 7-13 Vital Records, Reviewed Vital Records Screen, Completed Search Entry

5. Click **Submit** to begin the search or **Clear** to clear the entire page. A message similar to the following displays when you click **Submit**.

Figure 7-14 Vital Records, Reviewed Vital Records, Report Submitted Message

If you need to exit this screen while waiting for the submitted report to complete, you can click the **Vital Record Reviewed Search Reports** under the *Lists* section in the Quick Launch.

6. Click on the **Vital Record Reviewed Search Reports** link to see the search results generated with data specified, as follows:

Figure 7-15 Vital Record Reviewed Search Reports

7. Click the link of the title from the search report that was just created.

Figure 7-16 Vital Record Reviewed Search Report Details

7.3 Vital Records Review Workflows

Compliance Suite Records Managers can use workflows to assist in the process of reviewing vital records. Compliance Suite Records Managers can start workflows and view workflow task history by the following methods:

- Starting workflows from the Vital Record Report dialog box
- Viewing workflow task history from the workflow task list

7.3.1 Starting Vital Records Review Workflows

Compliance Suite Records Managers can start Vital Record Review workflows on vital record containers that need review.

Note:

The Complete Task button is not present in the Vital Record Review Workflow Task dialog box.

Follow these steps:

1. Select **Due for Vital Review** in the **Vital Records** section of the Compliance Suite header ribbon. The *Due for Vital Review* screen displays.

Figure 7-17 Due for Vital Review

---

2. (**Required**) In the **Review eligibility date** field, enter today's date or a future date that vital records will be eligible for review.

3. (**Required**) Click to select the sites that contain the vital records.

4. Click **Submit**. The report submitted message displays.

Note:

There is a delay before the results are available.

Report Submitted
Your report has been scheduled and will complete when the timer job completes. To view the status of your report, please visit the Vital Record Reports list.

Figure 7-18 Report Submitted Message

If you need to exit this screen while waiting for the submitted report to complete, you can click the **Vital Record Reports** under the *Lists* section in the Quick Launch.

5. Click the Vital Record Reports link to see the Search Reports listing, as follows:

Figure 7-19 Vital Records Review Search Reports Listing

6. Click the name of the Vital Record Report link you created to view the container.

Figure 7-20 Vital Records Review, Click on Vital Record Report Link

7. Click the **Workflow** box and click the check mark to the right of the Reviewers name to verify the name. Click **Start** to begin the workflow on the Vital Record. The names that are displayed are the last reviewers, but you can change these names. When a group name is entered as a reviewer, any member of the group can modify the workflow task.

Figure 7-21 Vital Records Review, Start Workflow

8. Click **Start**. The following message displays when the workflow task begins. A workflow task assignment email is sent to the assigned reviewer and an entry is created in the workflow task list.
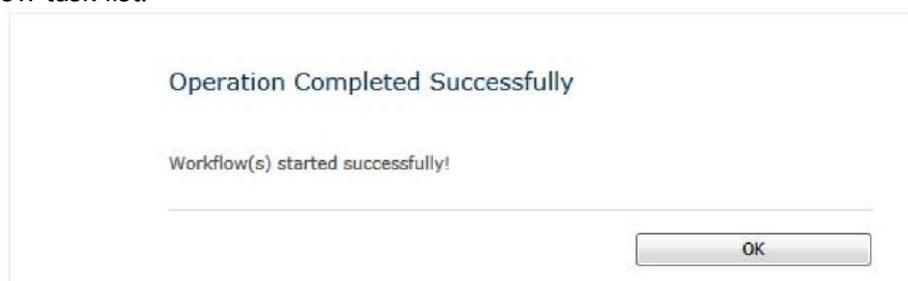

Figure 7-22 Workflow Started Successfully Message

9. Click **OK** to return to the Vital Records Review screen.

7.3.2 Reviewing Workflow Tasks

The assigned reviewer for the workflow task reviews the Vital Records Review Workflow task by clicking the task link in the email received or by accessing the Workflow Task list.

You can review a workflow task via email notification or by accessing the workflow task list. To review a workflow task via email notification, follow these steps. You can also review the items from email.

1. Click the **Vital Records Reviews** link. The **Workflow** status column tells you the status of the workflow.

2. When a user starts a Vital Record Review workflow and the review period on the container is started, a records review Workflow Task is created.

3. The reviewer receives an email notification when the Workflow Task is created.

4. Open the email client to receive the email notification stating the container is due for vital records review. Click the task link to open the task. The Vital Records Review Workflow Task screen displays.
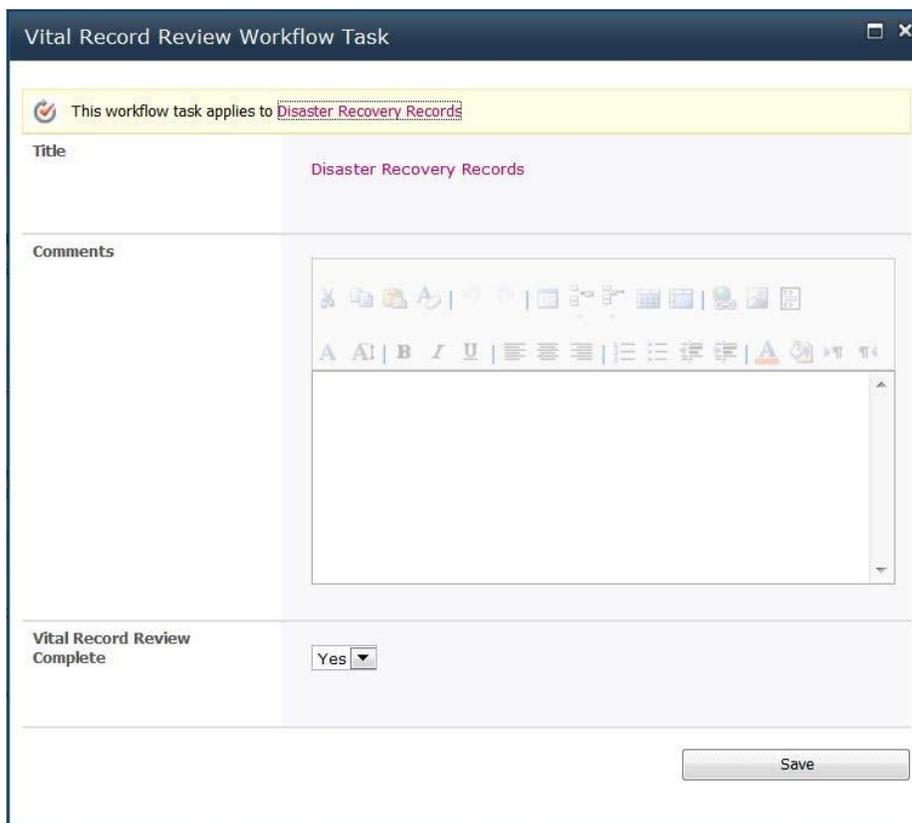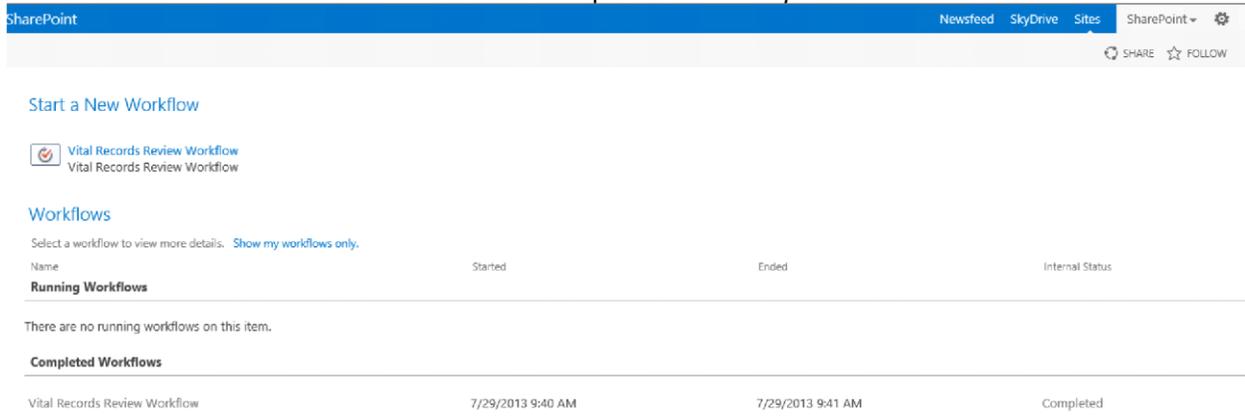
Figure 7-23 Workflow Task Screen

5. To review the records, click the link in the **Title** field.

6. Enter optional comments in the **Comments** field. Click **Save** to save changes.

7. After completing the vital records review, click **Yes** in the **Vital Record Review Complete** field.

8. Click **Complete Task** to complete the task. Click **Save** to exit the **Vital Records Review Workflow Task** screen and return to the **Records Center** home screen.

9. Complete the comment field, change the **Vital Record Review Complete** status to Yes, and click **Save**. The window displays the Task Completed Successfully message, as follows:

Figure 7-24 Table Task Completed Successfully Message

10. Once a workflow completes, the **Vital Records Review Workflow** status column in the **Vital Record Review View** screen is updated to *Completed*.

Figure 7-25 Workflow Status Column

8 Holds

A legal hold is a result of current or anticipated litigation, audit, or government investigation where there is a need to preserve content to avoid spoliation of evidence. The legal hold is typically initiated by a notice or communication from legal counsel that suspends the normal disposition or processing of records. Upon receipt, an organization takes action on records and record collections to ensure that they are not removed as part of their normal retention schedule process.

In addition to the hold abilities provided by SharePoint, Compliance Suite provides additional holds functionality, such as folder holds and Global Holds for record centers. Compliance Suite functionality enables administrators, records managers, and local records officers to add holds to entire record containers. Once a hold is placed on a record container, existing records, as well as records that are subsequently added, will automatically be placed under hold. Records that are placed under hold cannot be destroyed. Compliance Suite administrators, records managers, and local records officers can release holds on record containers as well as records. Once all holds are released on a record container, existing records, as well as records that are subsequently added, can be destroyed.

Intended User: Records Manager, Local Records Officer, Compliance Suite Administrator, Compliance Officer

---

Note:

The intended users will not have initial access to Central Administration. The Add and Run Global Holds function does not need to have access to Central Administration.

The following table describes the **Holds** → **All Items** list with a description of each heading.

Table 8-1

List View Heading	Description
Title	Unique identifier that differentiates the Holds from other Holds.
Description	Descriptive statement that defines the purpose of the Hold.
Managed By	Name(s) or group(s) responsible for managing the Hold.
Hold Status	Current status of the hold.

8.1 Using Global Holds Functionality

Global Holds enable a compliance officer to place holds on items from multiple site collections based on a search query. This functionality also allows you to save queries and apply holds to matching items on a recurring basis. For every Site that is to be considered for crawling for the

Global Hold, the Site Feature "GimmalSoft Compliance Suite - Holds Management" must be activated.

Global Holds extends SharePoint's default Holds functionality. SharePoint supports placing holds in only a single site.

Note:

Global Holds functionality is available only to Site Collection Administrators and others in the *Gimmal Holds Add* or *Gimmal Holds Remove* group. Those in the *Gimmal Holds Add* group are allowed to place Global Holds, create recurring Global Holds, and edit recurring Global Holds. Those in the *Gimmal Holds Remove* group are allowed to remove recurring Global Holds.

You can add, run, and manage Global Holds from the Compliance Suite header ribbon.

1. Click **Add/Run Global Hold** from the header ribbon to access the **Global Holds** page.
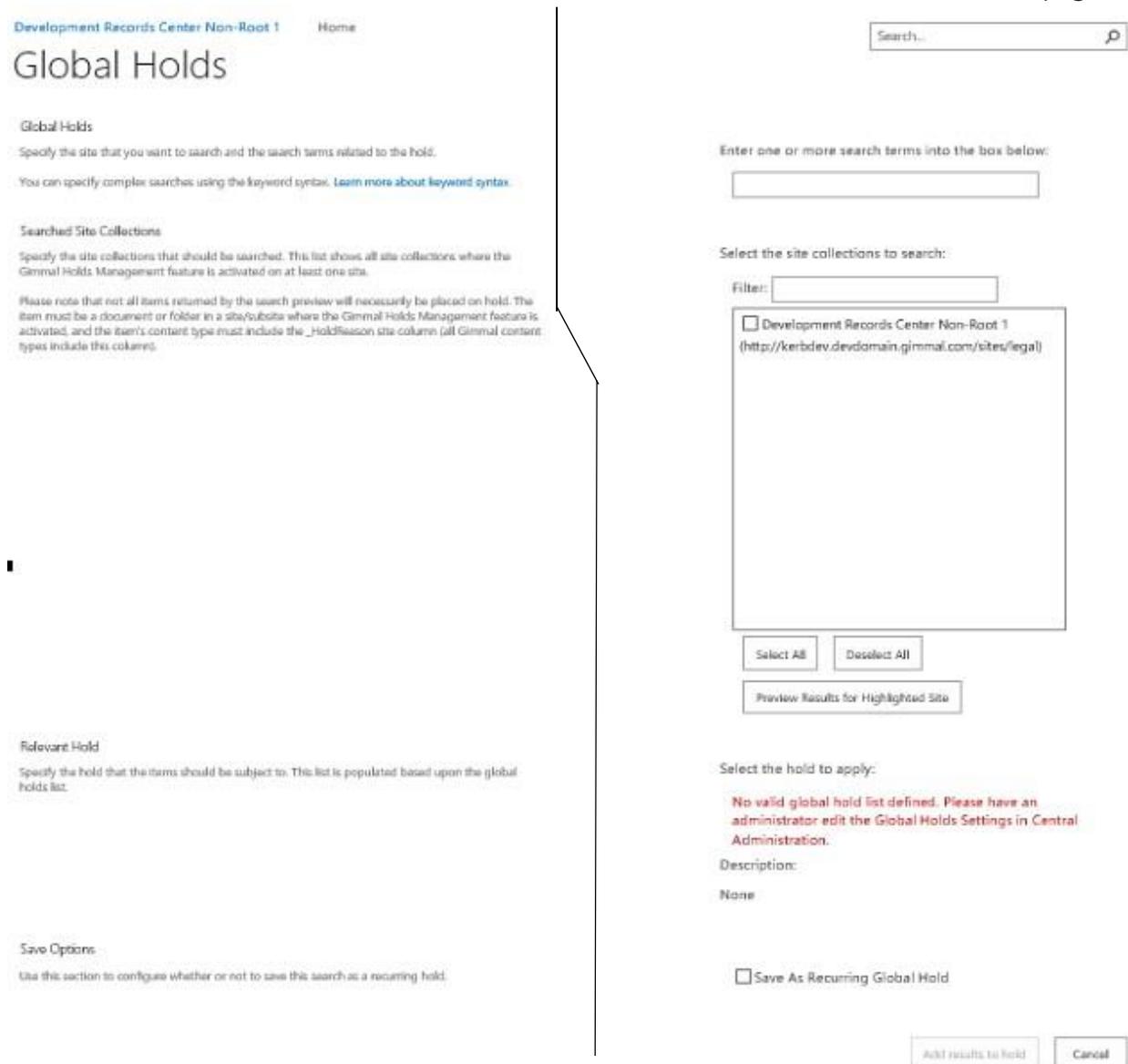
Figure 8-1 Global Holds

On the right side of the Global Holds screen, you can specify a search query, select site collections where the Global Hold is to be applied, select which Global Hold to apply, and choose whether or not the Global Hold should be recurring. Holds listed in this page are pulled from the holds list specified as the Global Holds list. A hold placed on a container puts all items in the container on hold regardless of whether it is Case Based Retention (CBR) or not.

When you click **Add Results to Hold**, the search is processed and run by SharePoint's Search and
Process timer job. This is similar to the way the default Holds functionality works. Because SharePoint restricts holds to a single site, Gimmal actually creates a local copy of the Global Hold in each site where the hold is applied. The local copy is synced to and controlled by the Global

Hold. It is updated each time the Global Hold is updated, and is released when the Global Hold is released. If any searches are saved as recurring Global Holds, these searches are run and applied, by default on a weekly basis. This can be scheduled at any time by changing the recurring schedule for the Gimmal Compliance Suite - Global Holds Timer Job in Central Administration. Local holds can also be created per site collection.

Note:

If the site already has a hold defined with the same name as the one created, the hold functionality will still work.

To manage recurring Global Holds, follow these directions.

- Select **Manage Recurring Global Holds** from the header ribbon.

    The page is a simple grid of the saved queries and the holds they apply. They can be deleted or edited from this page.

8.2 Creating a Hold

Before a hold or global hold can be placed on a container or record, it must be created.

To create a hold, use the following procedure:

1. Select **Settings** and then **Site Settings**.
2. The **Site Settings** screen opens. Select **Holds** under the **Hold** section.
3. The **Holds** → **All Items** screen opens. You can add a hold by the following;
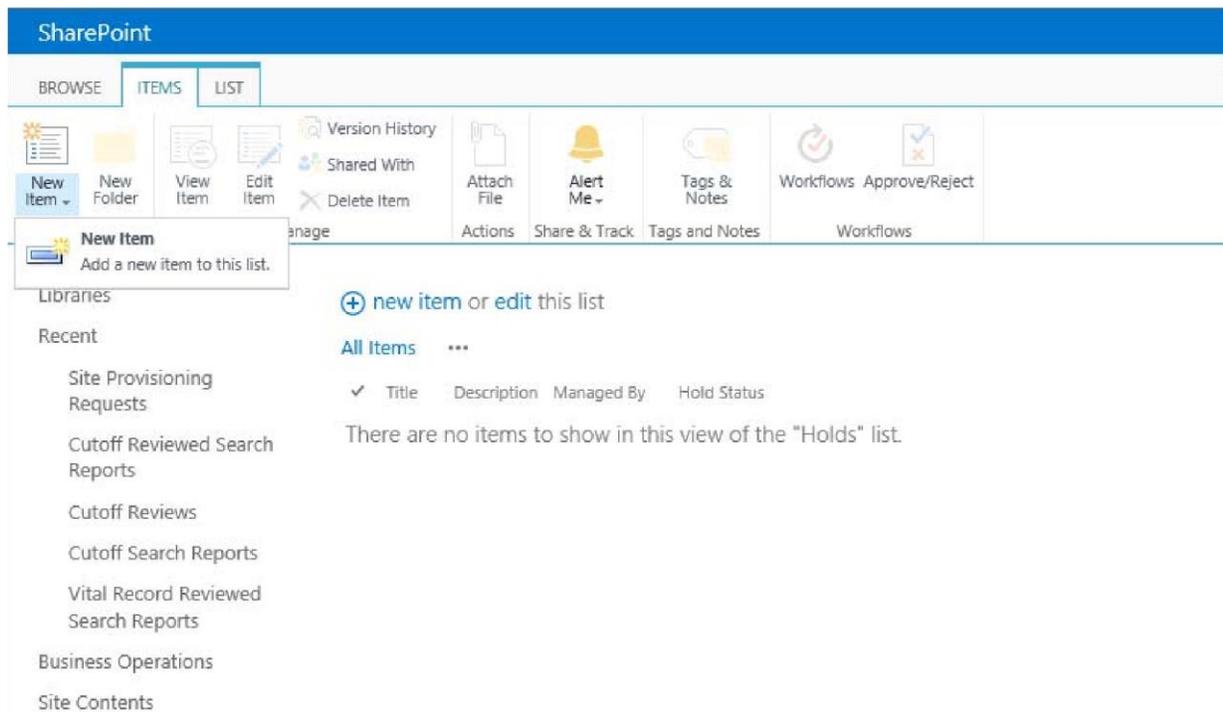   a. Click **+ new item**.
    b. Click the **Items** tab.

Figure 8-2 Adding a New Hold Item

c. In the header ribbon, select **New Item** and then **New Item**.

A **Holds - New Item** dialog box opens with fields for creating a new hold.

Figure 8-3 New Holds Item Dialog Box

4. Enter the **Title**. The **Title** is a unique identifier for the new hold. (**Required**)

5. Enter a **Description**. The **Description** should be a descriptive statement that defines the purpose of this hold.

6. In the **Managed By** field, enter name(s) or group(s) managing the hold by adding name(s) or group(s) via the People Picker.

7. Click **Save** to create the new hold. It is displayed in the **Holds → All Items** list. Click **Cancel** to return to the **Holds → All Items** list without creating a new hold.

8.3 Adding a Hold to a Record Container

Compliance Suite enables administrators and records managers to add holds to record containers. Once a hold is placed on a record container, existing records, as well as records that are subsequently added, will automatically be placed under hold. Records that are placed on hold cannot be destroyed.

To add a hold to a record container, perform the following steps:

1. From the target container screen, click to the right of the container on which you want to place a hold. Click again and select **Compliance Details** from the action menu.

Figure 8-4 Container Holds: Compliance Details

2. The **Compliance Details** dialog box opens. In the **Hold Status** field, click the **Add/ Remove** from hold link.
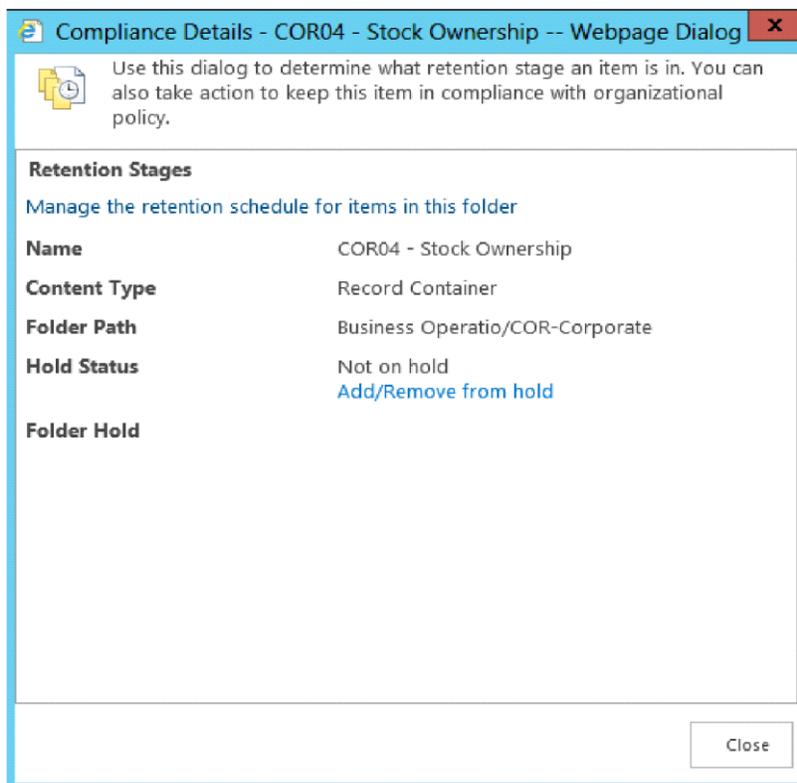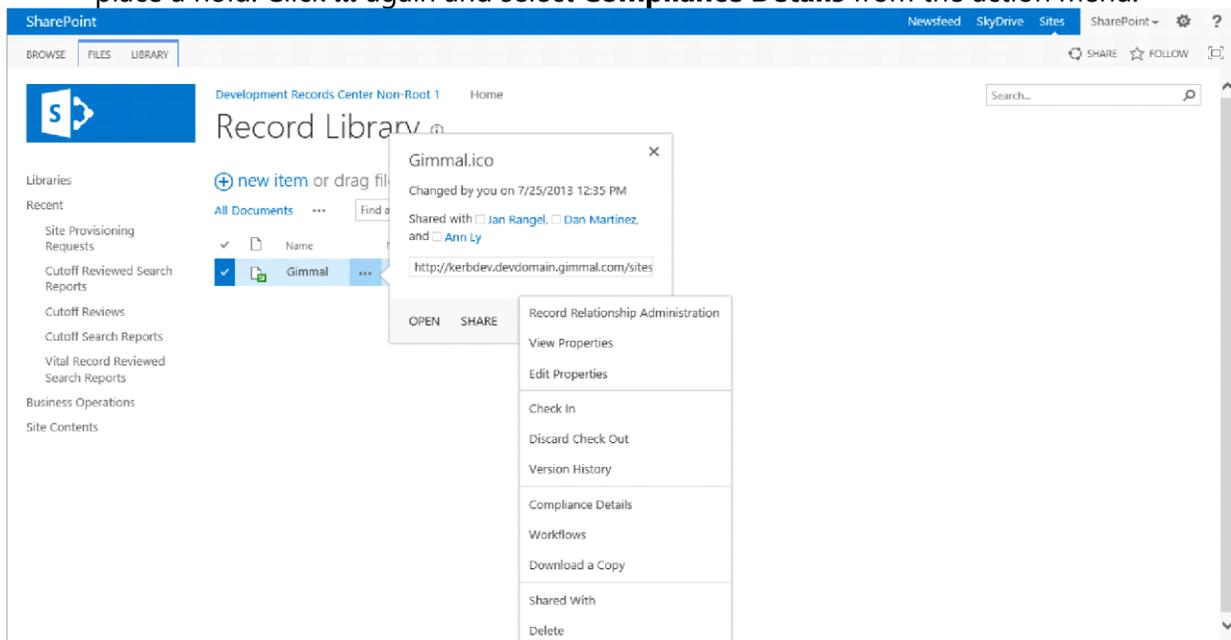
15 January 2019

Figure 8-5 Add/Remove from Hold Link

3. The **Item Holds Status** screen opens with options to add or remove an item from hold. Click the **Add to a hold:** radio button and select a hold from the **Select a hold** menu.

Figure 8-6 Adding a Container Hold

Note:

Items with any hold(s) already placed on them display the hold(s) below the *This item is under the following hold(s)* message at the top left corner of the **Item Hold Status** screen.

---

4. Click **Save** to add the hold to the record container. Click **Cancel** to cancel and return to the target container screen without adding a hold to the record container.

8.4 Adding a Hold to a Record

To add a hold to a record, perform the following steps:

1. From the target container screen, click **...** to the right of the record on which you want to place a hold. Click **...** again and select **Compliance Details** from the action menu.

Figure 8-7 Record Holds: Action Menu

---

2. The **Compliance Details** dialog box opens. In the Hold Status field, click the **Add/ Remove from hold** link.
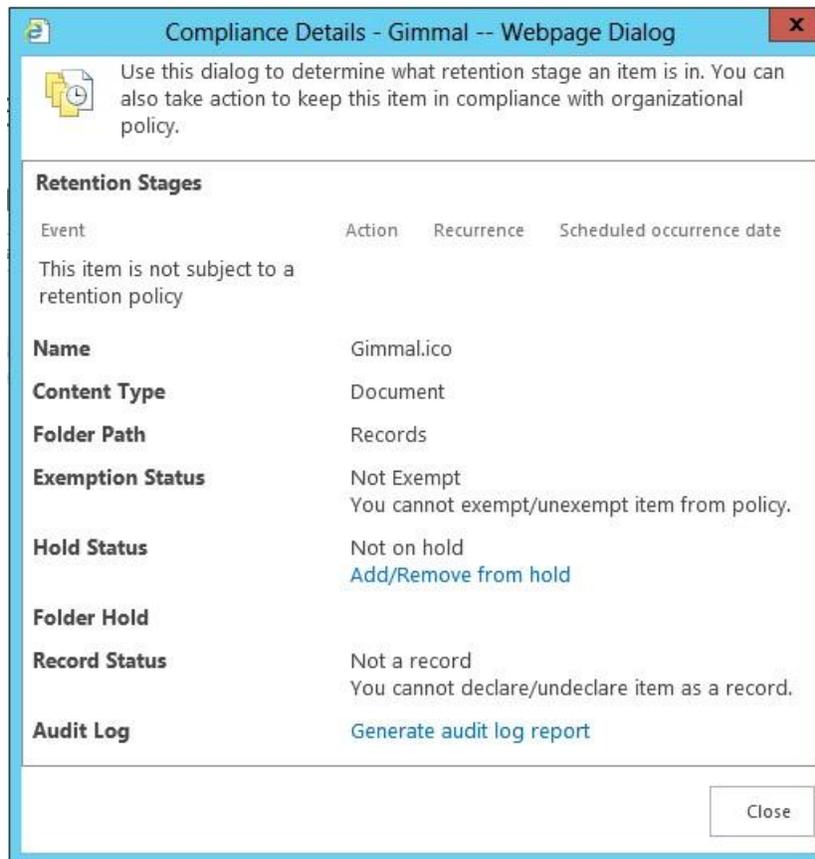

Figure 8-8 Record Holds: Compliance Details

3. The **Item Holds Status** screen opens with options to add or remove an item from hold. Select the **Add to a hold** radio button and select a hold from the **Select a hold** menu.
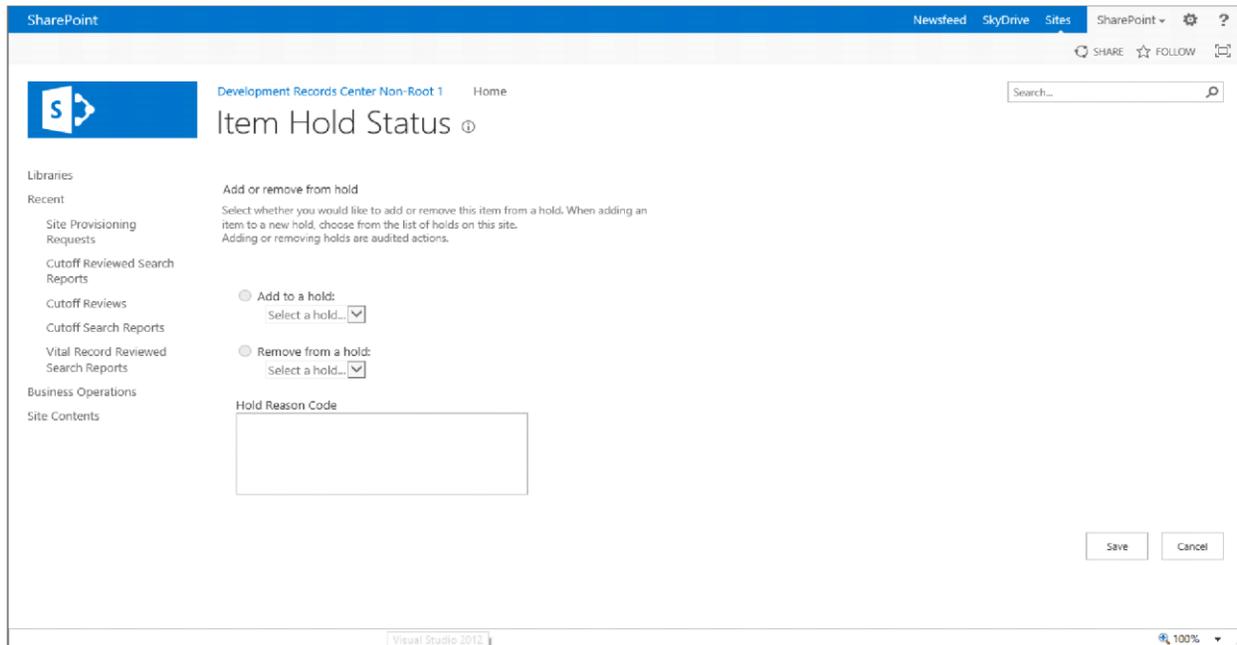
Figure 8-9 Record Holds: Adding a Hold

4. Click **Save** to add the hold. Click **Cancel** to cancel and return to the record screen without adding a hold to a record.

8.5 Removing a Hold from a Record Container

Compliance Suite enables administrators and records managers to remove holds that have been previously placed on record containers. Once a hold is removed from a record container, existing records in the record container, as well as records subsequently added to the record container, can be destroyed.

To remove a hold from a record container, perform the following steps:

1. From the target container screen, click **...** to the right of the container on which you want to remove a hold. Click **...** again and select **Compliance Details** from the action menu.
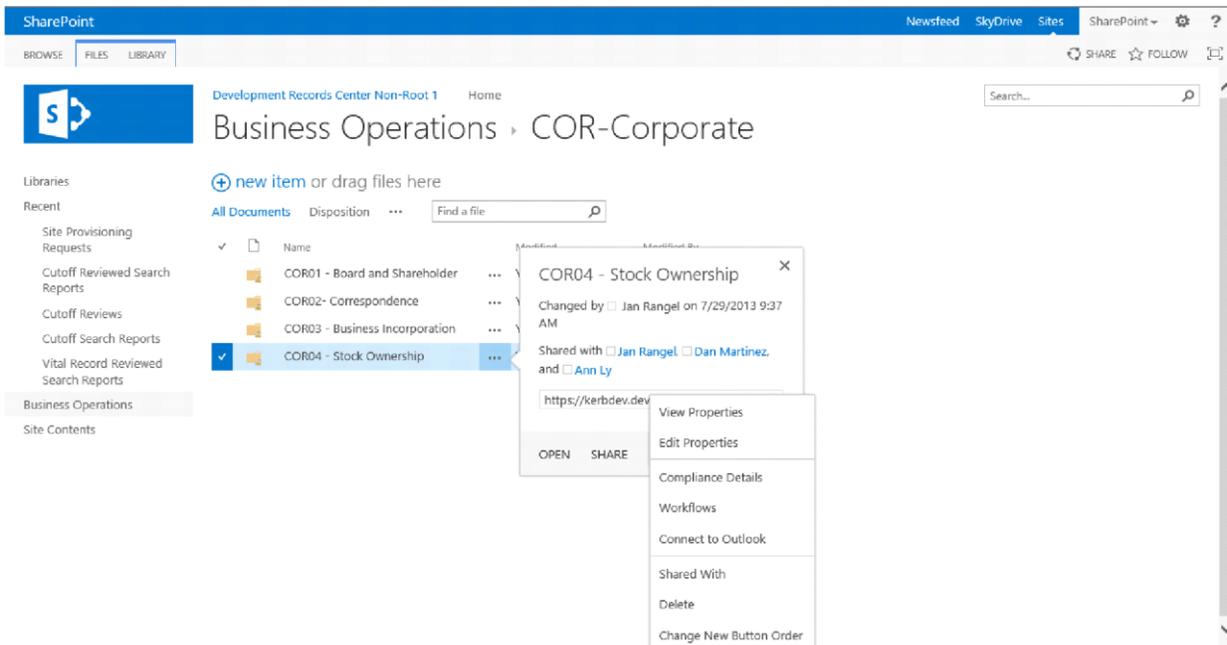
Figure 8-10 Container Holds: Compliance Details

2. The **Compliance Details** dialog box opens. In the **Hold Status** field, click the **Add/ Remove from hold** link.

3. The **Item Holds Status** screen opens with options to add or remove an item from hold. Items with any additional hold(s) placed on them display the hold(s) below the *This item is under the following hold(s)* message at the top left corner of the **Item Hold Status** screen.

4. Click the **Remove from a hold** radio button and select a hold from the **Select a hold** menu.

Item Hold Status ⓘ

Add or remove from hold

Select whether you would like to add or remove this item from a hold. When adding an item to a new hold, choose from the list of holds on this site.
Adding or removing holds are audited actions.

○ Add to a hold:
   Select a hold... ▾

○ Remove from a hold:
   Select a hold... ▾

Hold Reason Code

Figure 8-11 Removing a Hold

5. Enter a Hold Reason Code in the **Hold Reason Code** field.

6. Click **Save** to remove the hold from the record container. Click **Cancel** to cancel and return to the target container screen without removing a hold from the record container.

8.6 Removing a Hold from a Record

Removing holds has a couple of important notes associated with the functionality:

- You cannot release a hold that is part of a recurring global hold except from the global hold list. If it is released from the global hold list the recurring global holds are updated automatically to remove any items with this hold.

- There is no difference between global holds and global recurring holds. You can tell whether a hold is part of a global hold by adding the Global property to your view in the Holds list.

To remove a hold from a record, perform the following steps:

1. From the target container screen, click the **...** to the right of the container from which you want to remove a hold and select **Compliance Details** from the menu.
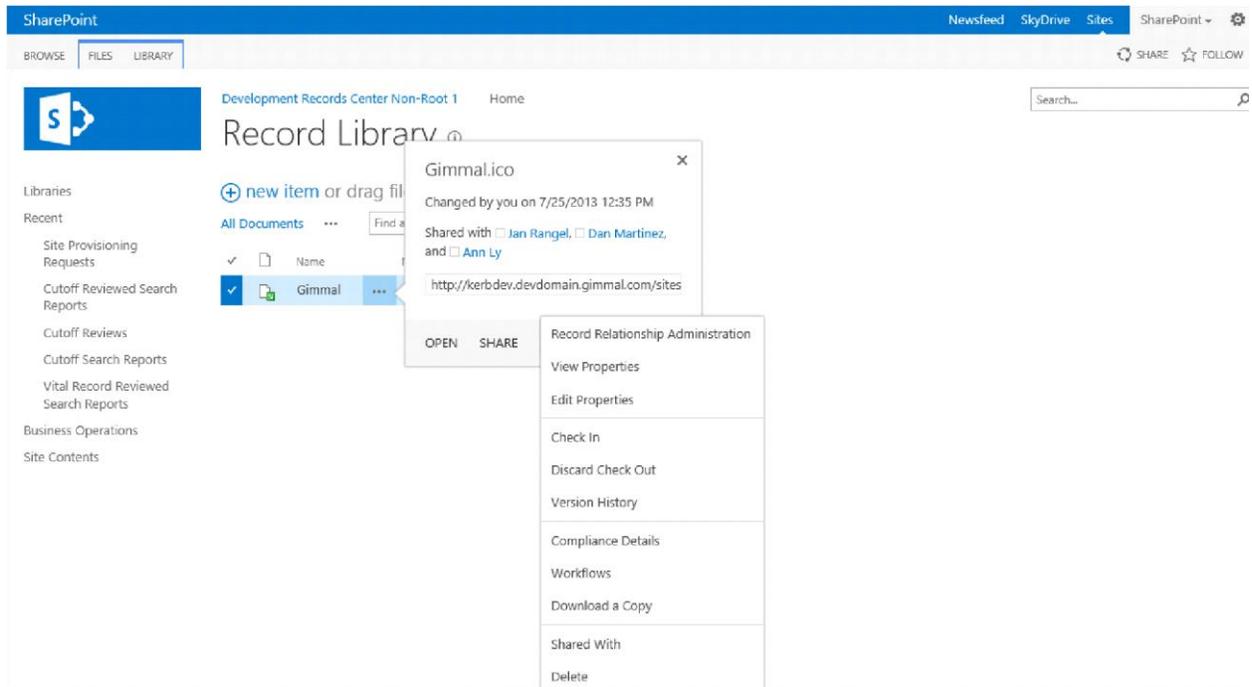
Figure 8-12 Selecting Compliance Details

2. The **Compliance Details** dialog box opens. In the **Hold Status** field, click the **Add/ Remove from hold** link.
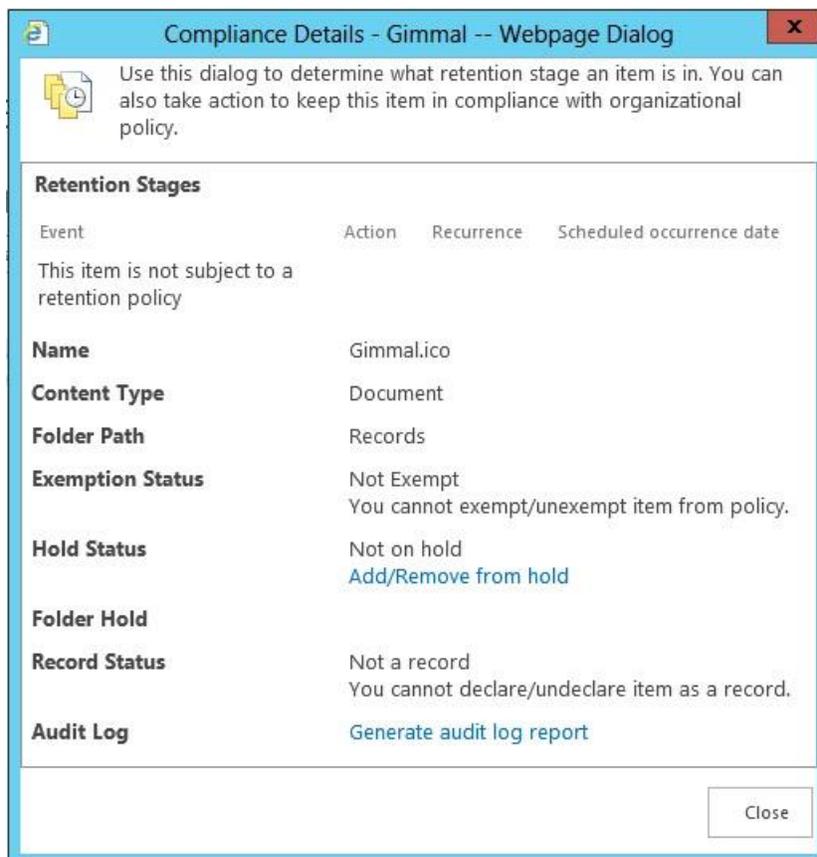

Figure 8-13 Add/Remove Hold Link

3. The **Item Holds Status** screen opens with options to add or remove an item from hold. Items with any additional hold(s) placed on them have the hold(s) displayed below the *This item is under the following hold(s)* message at the top left corner of the **Item Hold Status** screen. Select the **Remove from a hold** radio button and select a hold from the **Select a hold** menu.

Figure 8-14 Removing a Hold

4. Enter a Hold Reason Code in the **Hold Reason Code** field.

5. Click **Save** to remove the hold from the record. Click **Cancel** to cancel and return to the target container screen without removing the hold from the record.

8.7 Releasing a Hold

Compliance Suite enables administrators and records managers to release holds once a discovery is resolved.

To release a hold, perform the following steps:

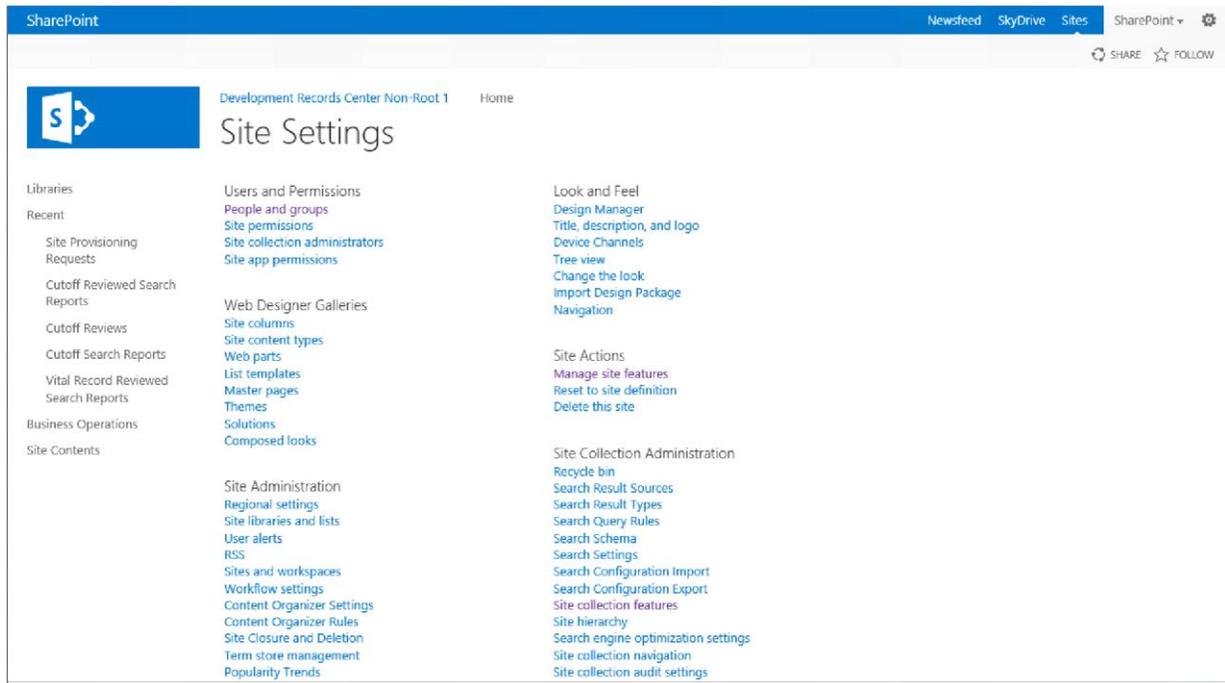1. Select **Settings** and then **Site Settings** from the header navigation. The **Site Settings** screen opens.

Figure 8-15 Site Settings

2. Select **Holds** under the **Hold** section or **Holds** in the header ribbon. The Holds → All Items screen opens.

3. To release a hold, you must first view the hold. Select to the right of the hold you want to release and click **View Item**.
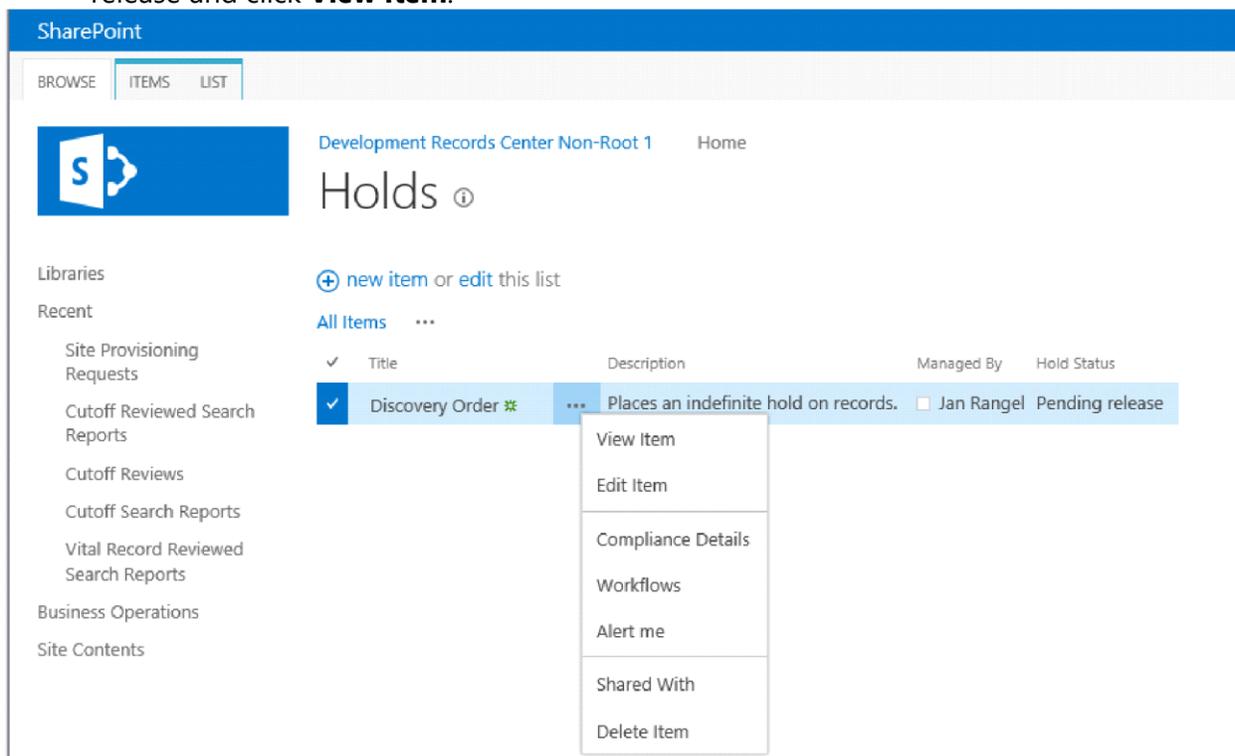
Figure 8-16 Holds Open Menu

4. Select the hold you want to view and then select the **Items** tab. In the header ribbon, select **View Item**.
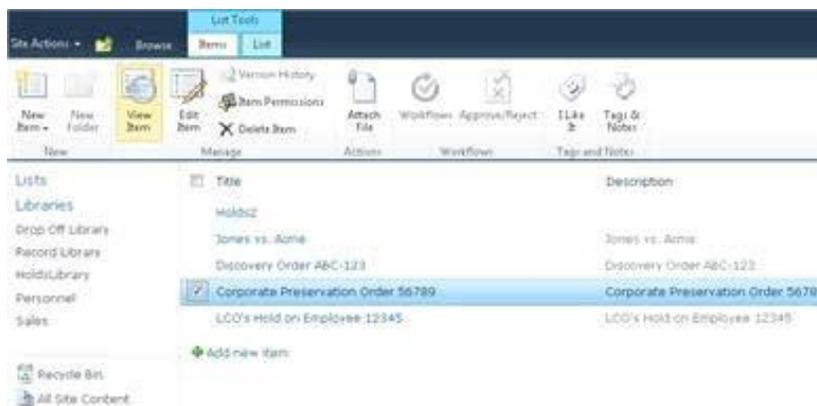

Figure 8-17 Holds - View Item

5. The **Holds - View Item** dialog box opens. In the **Holds Status** field, click the **Release hold** link.
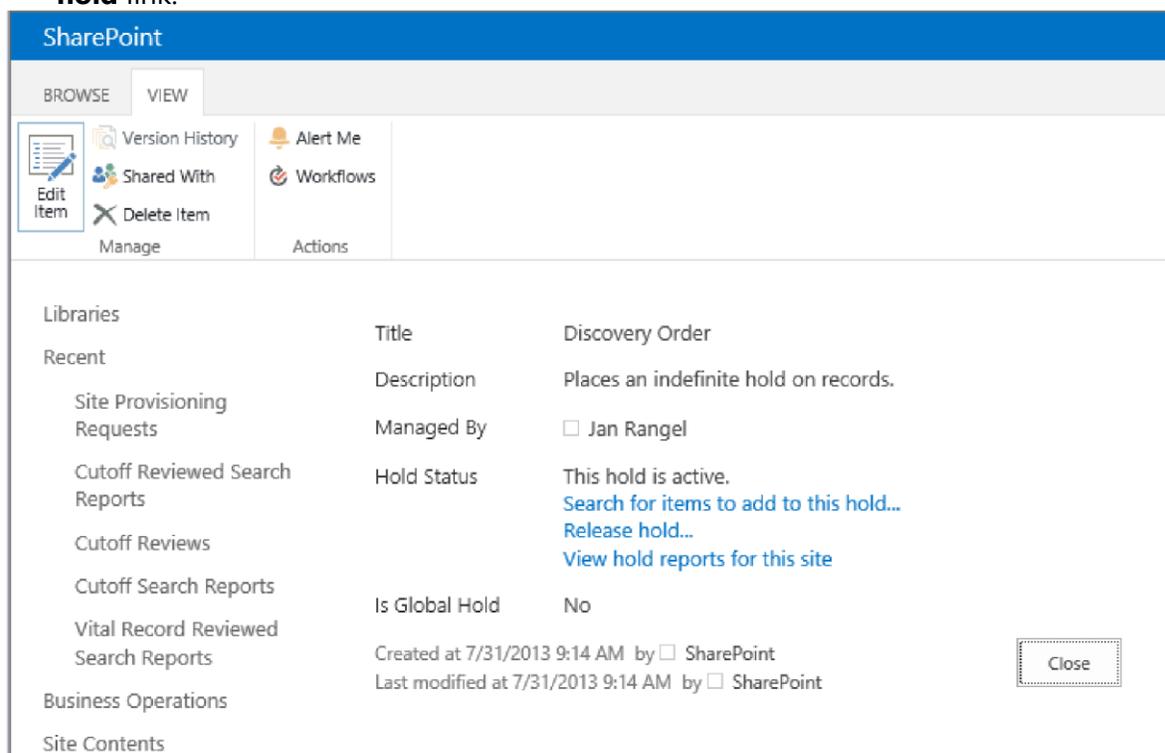

Figure 8-18 Holds - View Item Dialog Box

6. The **Release Hold** screen opens. Enter optional comments in the **Comments** field, then click **Release Hold** to release the hold or **Cancel** to cancel the operation.
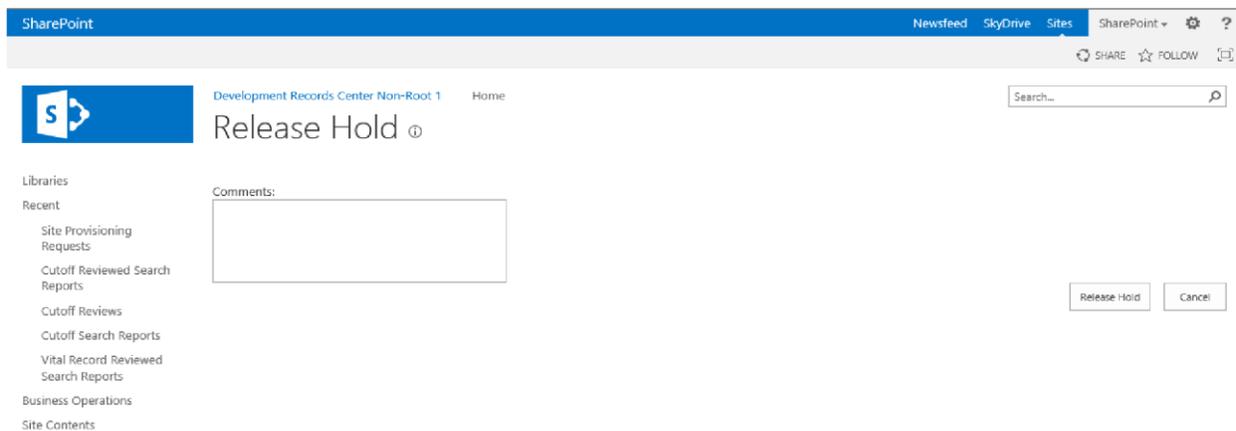
Figure 8-19 Release Hold

7. The updated **Holds → All Items** screen opens. A *Pending release* status message displays in the **Hold Status** column. Once the hold is released, it no longer displays in the **Holds → All Items** list.
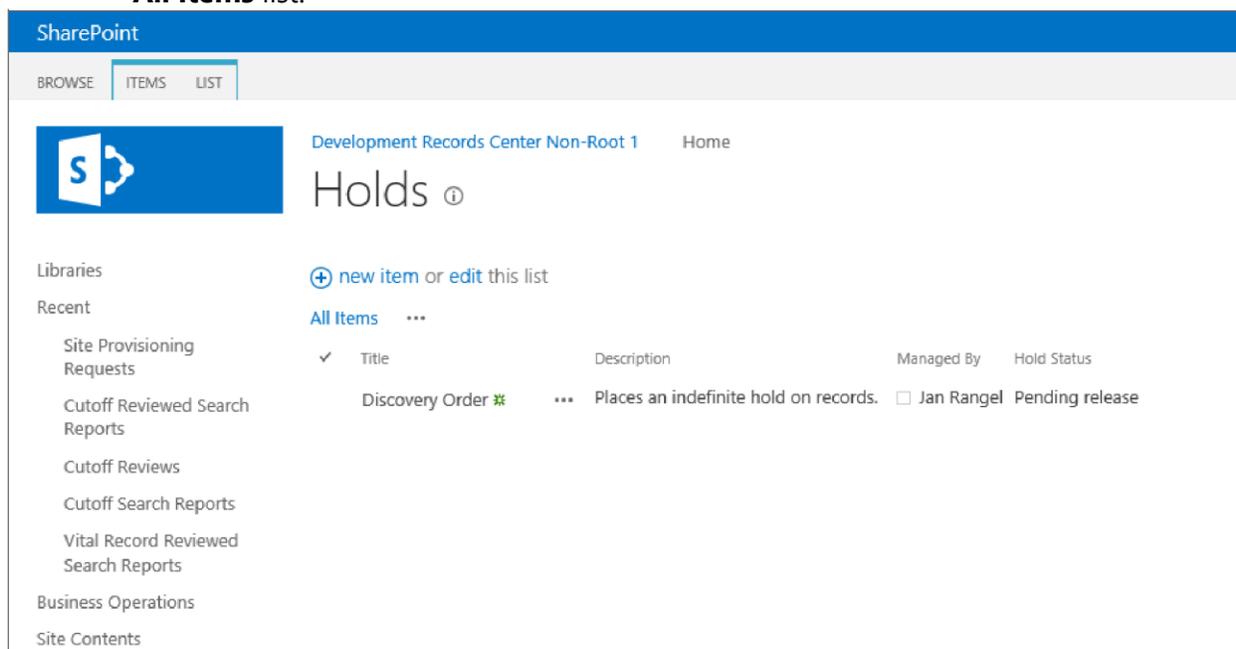

Figure 8-20 Holds - Pending Release Status

8.8 Editing a Hold

To change an existing hold, you must edit the hold item:

1. From the **Holds → All Items** screen, select the hold you want to edit. You can only edit one hold at a time.

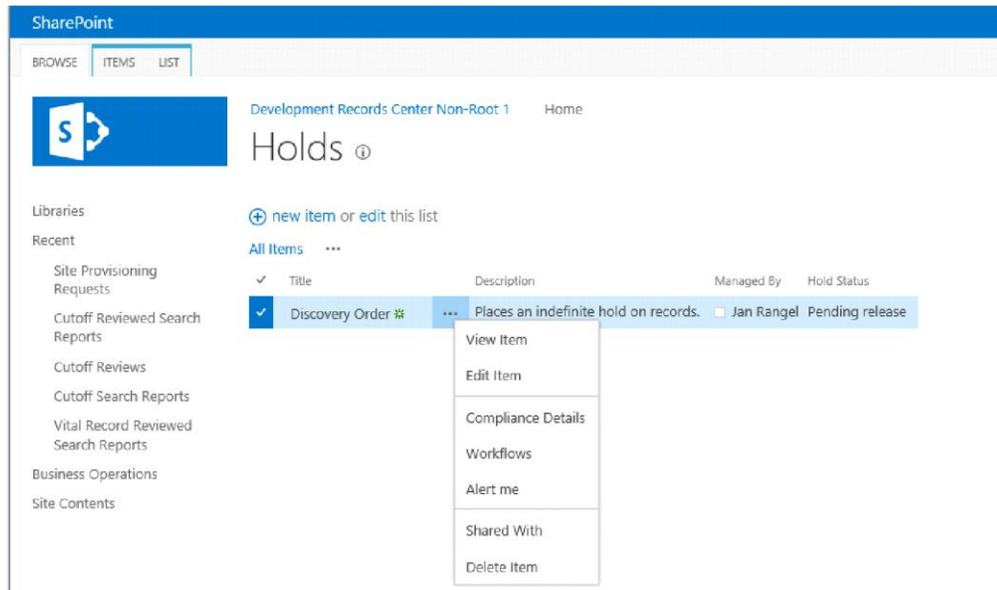   ● Click **...** to the right of the hold you want to edit and click **Edit Item**.

Figure 8-21 Holds - Edit Item Selection

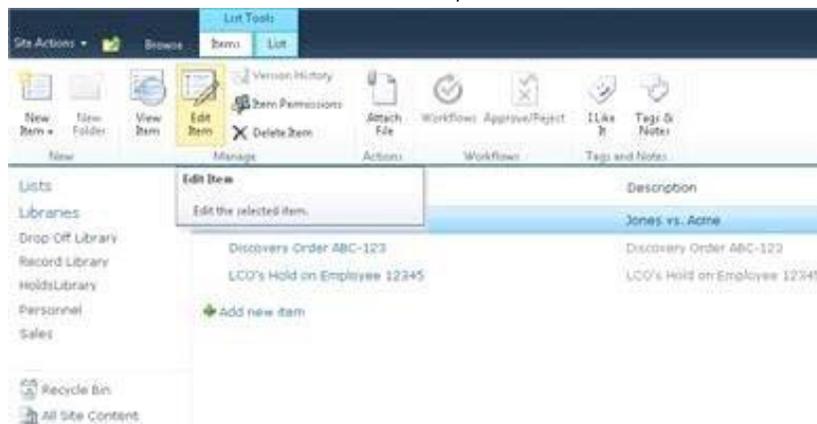- Click the **Items** tab. In the header ribbon, select **Edit Item**.

Figure 8-22 Holds - Edit Item

2. The **Holds Edit** dialog box opens, displaying the selected Holds details.
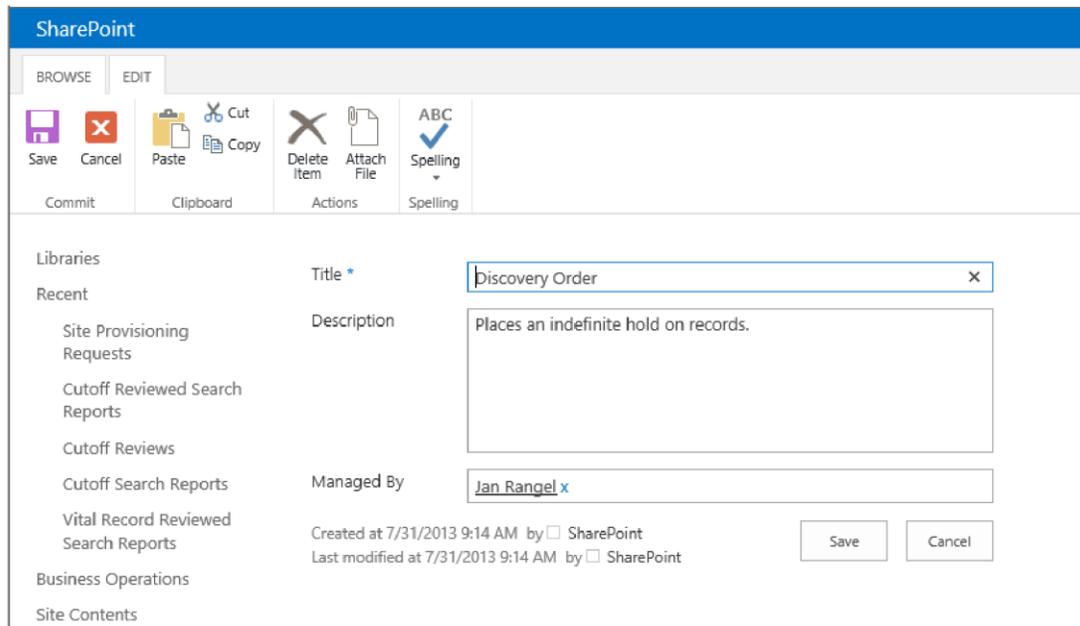
Figure 8-23 Holds: Edit Item

3. Update the information in the fields you want to change.

4. Click **Save** to update the changes. They are displayed in the **Holds → All Items** list. Click **Cancel** to return to the **Holds → All Items** list without updating the selected hold.

8.9 Viewing a Hold

To view the details of an existing hold, you must view the hold item:

1. From the **Holds → All Items** screen, select **...** to the right of the hold you want to view and click **View Item**. You can only view one hold at a time.

Figure 8-24 Holds Open Menu

- Select the **Items** tab. In the header ribbon, select **Edit Item**.

Figure 8-25 Edit Item in Header ribbon

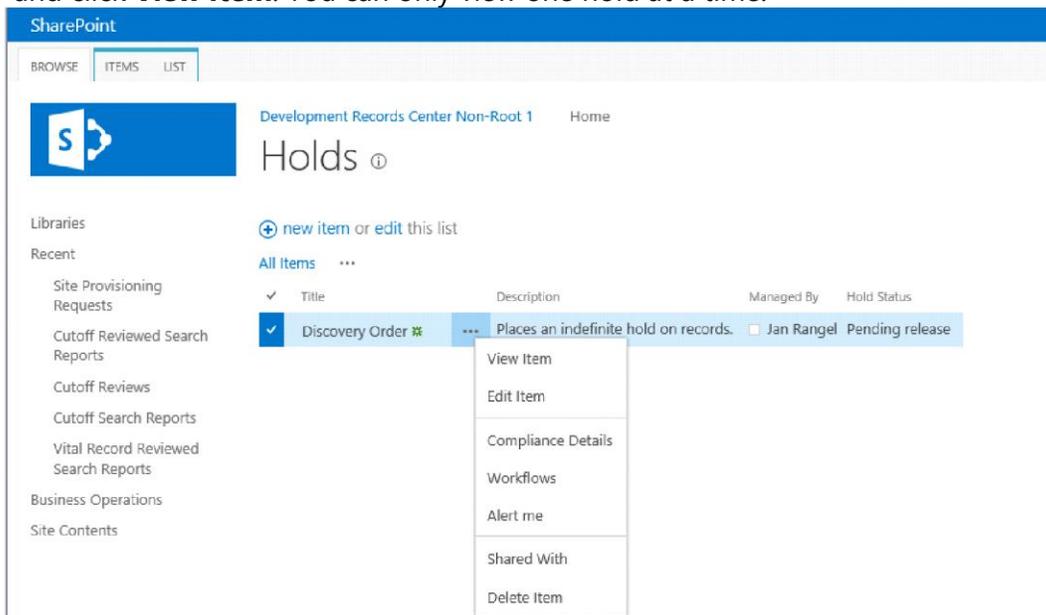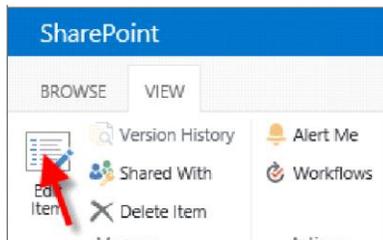2. The **Holds View** dialog box opens, displaying the selected hold details.
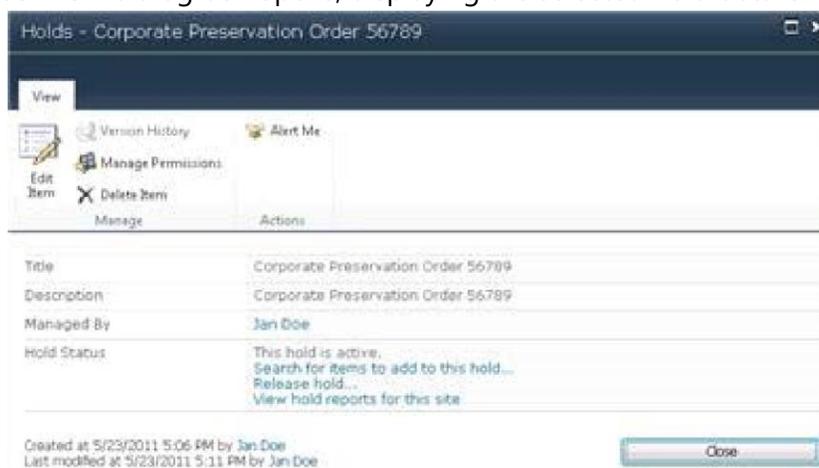
Figure 8-26 Holds View Dialog Box

3. From the **Holds View**, you can edit, delete, or manage permissions of the selected hold.

4. To make changes to the hold status, go to the **Hold Status** field. The **Hold Status** field contains the active Hold Status and three links. Click the **Search for items to add to this hold...** link to open the Search and Add Hold screen, where you can search and add hold contents. Click the **Release hold...** link to open the Release Hold screen, where you can release the hold. Click the **View hold reports for this site** link to open the Hold Reports screen, where you can view, edit, and print hold reports.

5. Click **Close** to return to the **Holds → All Items** dialog box.

9 Cutoff and Closing Folder Processing

This chapter explains and provides instructions for cutting off records. The process of cutting off records starts the aging process which can ultimately lead to a disposition decision. The disposition process can include transfer steps and ultimately the disposal of the records.

Final retention does not begin until you have cutoff the records. For instance, if you have invoice records with a monthly cutoff and a three-year disposition, records will be eligible for cutoff monthly and disposition will follow three years after the approved cutoff.

Cutoff and Closing Folder Processing functionality is available in a SharePoint Records Center with Compliance Suite enabled.

Compliance Suite Cutoff and Closing Folder Processing consist of the following procedures:

1. Configuring cutoff type
2. Searching Records Due for Cutoff
3. Cutoff Review
4. Cutoff Search Reports
5. Cutoff Review Workflows
6. Compliance Suite Reverse Cutoff

Intended User: Compliance Suite Administrator, Records Manager

9.1 Configuring the Cutoff Type

Compliance Suite enables administrators to configure Cutoffs in a number of ways. The following table lists each Cutoff type and a description of the Cutoff.

Table 9-1 Cutoff Types

Cutoff Type	Description and Function
Event Based Cutoff	Event Types define a specific trigger that must occur before records management processes and actions for a given record or set of records is enacted upon. Event Types are used in Cutoff Processing as defined in the Cutoff Criteria: Enable Event for a Record Container(s) and/or Record Item(s). Examples of Event based retention are Employee Terminates, Contract Ends, Asset Sold, Project Ends, Legal Matter completes etc. Events typically are used with Case Based Retention Record Categories.

Table 9-1 Cutoff Types

Cutoff Type	Description and Function
Period Based Cutoff	A Period Definition is a unit of time or frequency that defines records management processes and actions. Periods are used in Cutoff Processing as defined in the Cutoff Criteria: Enable Periods for a Record Container(s) and/or Record Item(s). For more information on Periods, see the Period Definitions help section.
Record Relationship Based Cutoff	A Record Relationship is an association that links two or more records. Record Relationships are used in *Cutoff Processing* as defined in the **Cutoff Criteria: Enable Relationships** for a *Record Container(s)* and/or *Record Item(s)*. An example of Relationship based cutoff is when records are superseded. For example, you have an Employee Manual for 2013 and come out with a new one for 2014. When a supersede relationship is created between these records, the 2013 record is then eligible for cutoff.
Custom Script Based Cutoff	Compliance Suite has the ability to leverage custom script files to resolve unique cutoff requirements. The user can enter command line syntax for execution in a text box. Custom scripts are used in Cutoff Processing as defined in the Cutoff Criteria: Enable Scripts for a Record Container(s) and/or Record Item(s).
Combination of Cutoffs	Compliance Suite has the ability to combine cutoff types. The cutoff can be based on the combination of cutoff options (e.g., a combination of Event Based Cutoff and Period Based Cutoff.

9.2 Assigning Cutoff Criteria to a Record Container

The cutoff is set when you assign the cutoff criteria in File Plan Builder and instantiate into a record center. You can modify an existing container's cutoff criteria. With the proper security permissions, you can establish new containers that inherit the cutoff criteria from its parent container.
You can also override the Cutoff Criteria (see Step 3).

1. From the target record container, select the Files tab. In the header ribbon, select **New Container**.
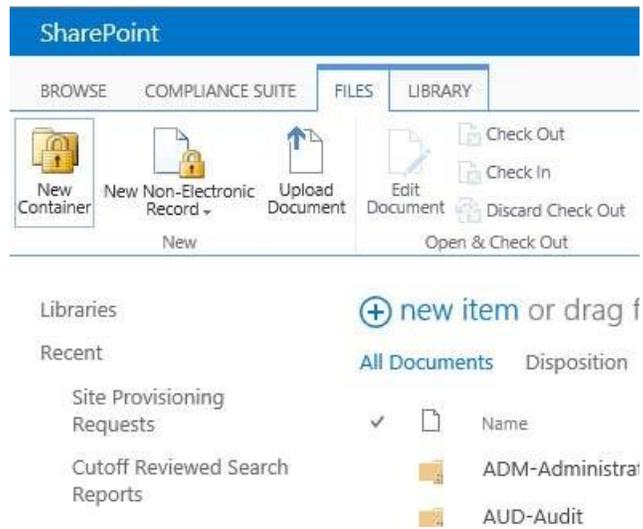
Figure 9-1 New Container Option

Optionally, you can assign cutoff in the File Plan Builder (FPB) or modify the cutoff for an existing container using File Plan Builder.

2. A **New Folder** dialog box opens with fields for creating a new container.

Figure 9-2 Create a New Container

3. Scroll down to the **Cutoff Criteria** field. By default, the child container displays the I**nherit the Cutoff Criteria** from the parent container.

Figure 9-3 Cutoff Criteria

4. To enable event based cutoffs, check the **Enable Event** check box. The **Select event type(s): and Selected event types**: fields are displayed. Select the event type(s) and click the right arrow button (>). The event(s) is displayed in the **Selected event types:** box.

These following options only display if more than one event is selected:

- Click the radio button beside **The first event will trigger the cutoff** to indicate that the first event will trigger the cutoff. The first event fulfilled is the only one acted on, all other events are ignored.

- Click th**e All events must occur for cutoff** radio button to indicate that all events must occur to trigger the cutoff.
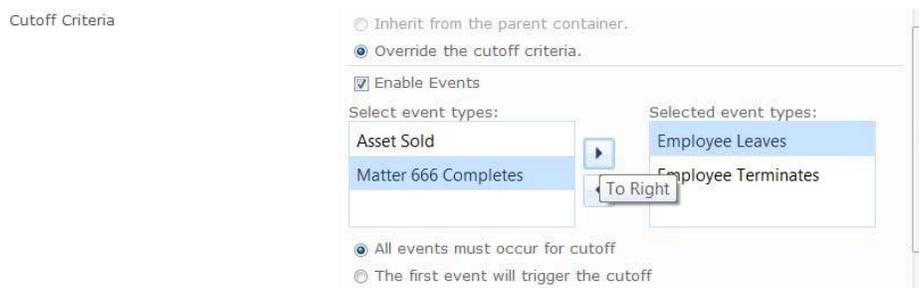

Figure 9-4 Enable Events

5. To enable period-based cutoffs, check the **Enable Periods** check box. The **Select the period type:** menu box is displayed. Click the period type for the cutoff. Options are based on the period definitions that have been created (for example, Monthly, Daily, and Yearly).
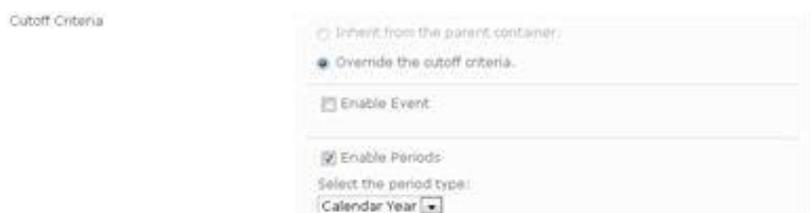

Figure 9-5 Enable Periods

6. To enable relationship based cutoffs, select the **Enable Relationships** check box. The **Select the relationship role:** menu is displayed. Click the relationship type for the cutoff. Options of cutoff relationship types are Superseded or Version. For example, you can have version 1.0 of a record and a version 1.1 is added. Version 1.0 is now eligible for cutoff.

Note:

Version 1.1 is only related if a Version Relationship is created. It does not happen automatically. Compliance Suite does not handle versions automatically.
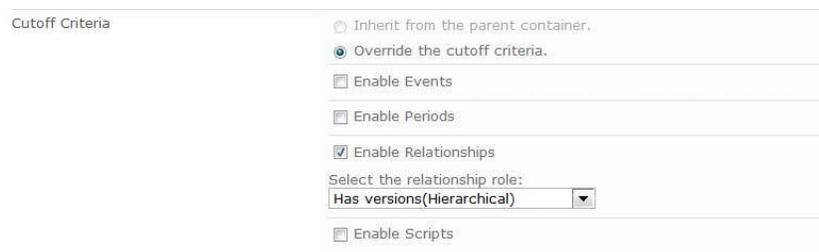

Figure 9-6 Enable Relationships

7. To enable script based cutoffs, check the **Enable Scripts** check box. The **Enter the pathname of the script:** text box is displayed. Enter the pathname of the script (pathname is a Uniform Naming Convention (UNC) path to a .bat or .ps1 file). To view more details on this feature click on **Advanced Help**.
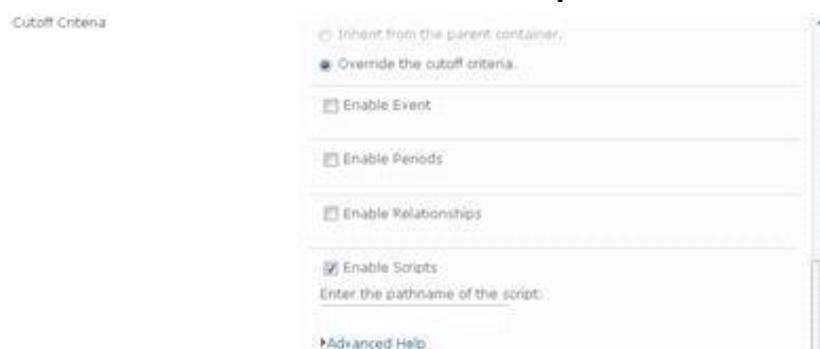

Figure 9-7 Enable Scripts

8. Click **Save** to create the new container. It is displayed in the record library container list. Click **Cancel** to return to the record library container list without creating a new container.

9.3 Searching Records Due for Cutoff

Searching records due for cutoff functionality is available in a SharePoint Records Center with Compliance Suite enabled.

Records Managers can search for cutoff records in two ways:

1. Search records that need cutoff review by utilizing the Due for Cutoff Review screen. You can only search for records due for cutoff using this method.

2. Search records that have already been cut off by utilizing the Reviewed Cutoff Records report. You can search for records that have been cutoff using this method.

9.3.1 Searching Records Due for Cutoff Review

To search for records Due for Cutoff Review, use the following procedure.

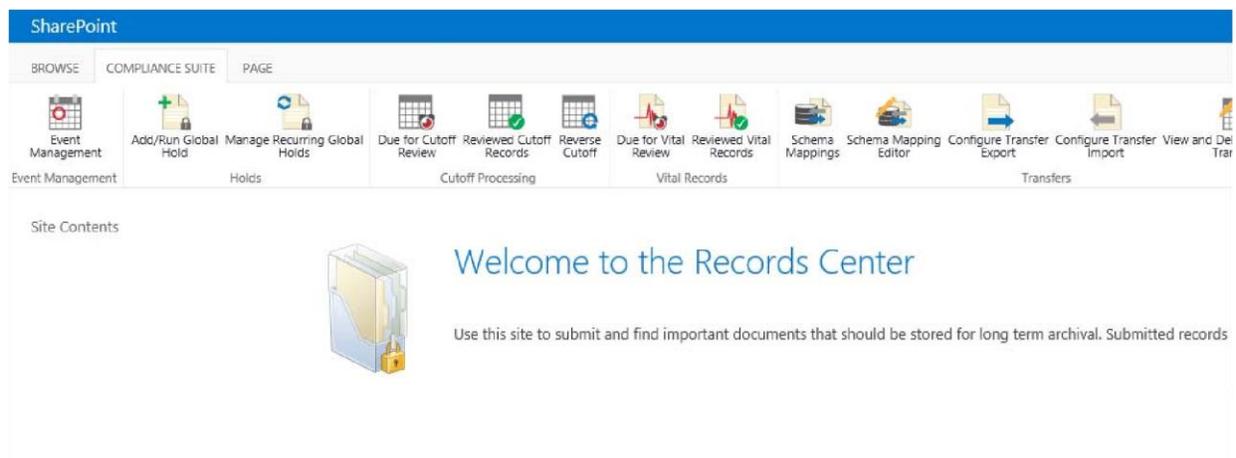1. select the Due for Cutoff Review icon in the header ribbon.

Figure 9-8 Due for Cutoff Review Option

2. The **Due for Cutoff Review** screen enables users to specify the title for the report, which will be listed as an entry in the Cutoff Search Reports, the eligibility date, and the names of the sites to query for Records that are to be cut off.

Figure 9-9 Due for Cutoff Review

3. In the **Cutoff Eligibility Date** field, enter today's date or a future date that records will be eligible for cutoff review.

4. (**Required**) In the **Sites** field, select the site or sites that you want to query for records that can contain records due for cutoff.

5. Click **Submit**. The following message displays in the center pane. You can click the **Cutoff Search Reports** link to view the report.

Figure 9-10 Report Submitted Message

Note:

A Timer Job is run to complete the report; otherwise, the status is pending. To see when your status has changed from *In Progress* to *Complete*, refresh the window from the Cutoff Search Reports list.

9.3.2 Start the Cutoff Process

After the **Due for Cutoff Review** runs and records are found, you can start the Cutoff Process.

1. Click the **Cutoff Search Reports** link.

Figure 9-11 Cutoff Search Reports

Note:

You must refresh the screen to know when the Pending Status changes to Complete.

2. Click on the list entry that represents the report that was just run. The list of records that are eligible for cutoff based on the search criteria displays.

3. Click the link for at least one item and click **Start**. The full path of the record is displayed when you hover and look at the browser status bar. Clicking the link opens the record (that is, the .docx, .txt, or CBR container).

Figure 9-12 Starting a Review

4. Enter the name of a reviewer to approve the cutoff process. To verify the Reviewer is valid, you must click the green check mark to the right of the viewer's name. Once you click **Start**, the cutoff workflow task starts and an email notification is sent to the reviewer telling them they have to process the cutoff approval.

5. The following message displays in a popup window: *Operation Completed Successfully*.

Click **OK** and you are taken to the Cutoff Reviews list.

9.4 Cutoff Reviews

Compliance Suite supports **Cutoff Reviews**. The tasks are created on the site from which the search was created or executed. The report and all tasks are only created in the site where the report was initiated. The users who have permission to complete this task include the Site Collection Admin, RMA Records Manager, RMA Administrators, the user Assigned To, and the Current User who is in the Assigned To Group. These users can review, approve, or delete the Cutoff Review workflow task by clicking the task link in the email received or by going to the Workflow Task list.

Intended User: Users, Records Manager, Local Records Officer (LROs), Records Administrator

To view a list of all Cutoff Review Tasks:

1. Open a **SharePoint Records Center** with Compliance Suite enabled. The **Welcome to the Records Center** view opens.

2. From the **Record Center Lists**, select **Cutoff Reviews**. You will see a list view of all Cutoff Review Tasks defined in the current site.

The following table describes the Cutoff Reviews list and the functions associated with each heading.

Table 9-2 Cutoff Reviews

List View Heading	Description and Function
Title	The name of the record or folder.
Cutoff Item URL	URL of the cutoff item.
Cutoff Date	Date the record was cutoff and closed.
Review Date	The date the cutoff review was performed.
Reviewer	Name of the person who performed the cutoff review.
Review Status	Status of cutoff review process for the record.
Modified	Date of the most recent modifications.
Cutoff Review Workflow	Workflow status of the review.

9.4.1 Approving or Rejecting Cutoff Reviews

To approve or reject the workflow tasks for any item in the list. Use the following procedure to approve or reject the details of an existing Cutoff Review Task item.

1. From the **Cutoff Reviews** list, click the **In Progress** link in the Cutoff Review Workflow field of the Cutoff Review Task you want to approve or reject. Only one Cutoff Review Task can be selected at a time.

Figure 9-13 Cutoff Review Task

2. Click the **In Progress** link to go to the Cutoff Review Workflow screen.

Figure 9-14 Cutoff Review Workflow Screen

3. Click the title of a Task. In this example, click on the Cutoff Review record Cutoff Review record Sample 1.docx report.

Figure 9-15 Selecting a Workflow Task

4. The last step is to set the **Cutoff Review Complete** menu on the bottom of the screen to **Yes** and to click on the **Complete Task** button. The record has now been approved for cutoff and this sets the trigger date for aging once the timer jobs have been run.
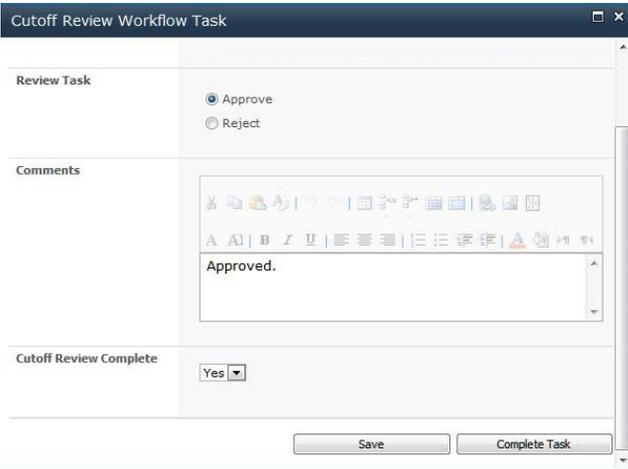
Figure 9-16 Completing the Cutoff Review

9.5 Cutoff Search Reports

Compliance Suite supports Cutoff Search Reports. You can use the Search report to see what has been processed for cutoff and what still needs to be processed by visiting the Cutoff Search Reports list in the Record Center Administration site.

Compliance Suite provides the ability to Edit, View, or Delete existing Cutoff Search Reports. The report is only created in the site where the report was initiated.

Intended User: Compliance Suite Administrators

To view a list of all Cutoff Search Reports:

1. Open a **SharePoint Records Center** with Compliance Suite enabled. The *Welcome to the Records Center* view opens.

2. Select **Cutoff Processing → Due for Cutoff Review** from the header ribbon. A list view of all Cutoff Search Reports defined in your site displays.

    The following table describes the **Cutoff Search Reports** list and the functions associated with each heading.

Table 9-3 Cutoff Search Reports

List View Heading	Description and Function
Cutoff Report Title	The name that was given for the report.
Cutoff Eligibility Date	This is the date that was used as the cutoff date when the report was generated (for example, the items in the report will fall in this date range for cutoff).

Table 9-3 Cutoff Search Reports

List View Heading	Description and Function
Sites	Sites containing the cutoff records to review.

9.5.1 Viewing a Cutoff Search Report

When a user performs a cutoff search using the **Due for Cutoff Review** function, a Cutoff Search Report list item is created in the **Cutoff Search Reports** list. To view an existing Cutoff Search Report, you must view the Cutoff Search Report item.

1. From the **Cutoff Search Report View**, select the **Cutoff Search Report** you want to view. Only one **Cutoff Search Report** can be selected at a time. When a Cutoff Search Report is selected, the **List Tools → Items** opens in the header ribbon.
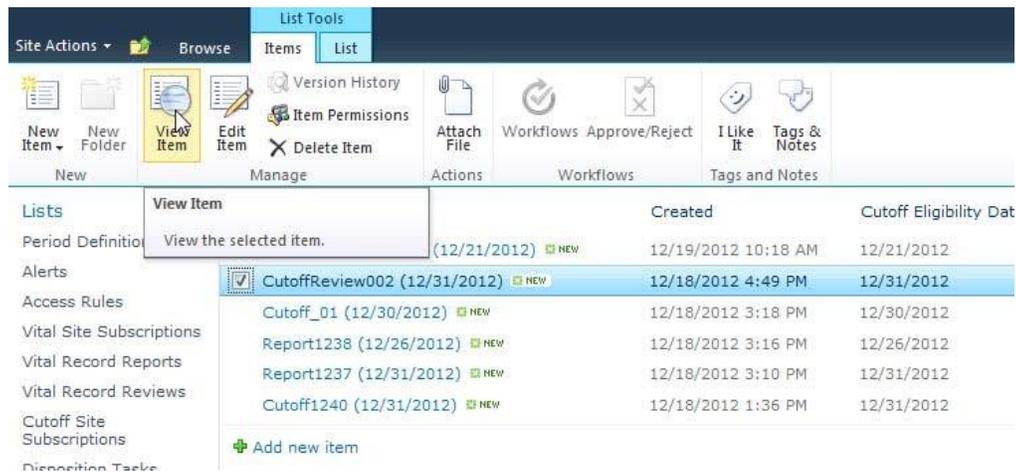
Figure 9-17 Cutoffs - View Item Selection

2. Select **View Item** button on the header ribbon. The **Cutoff Report Search Results** dialog box opens, displaying the selected Cutoff Search Report details.
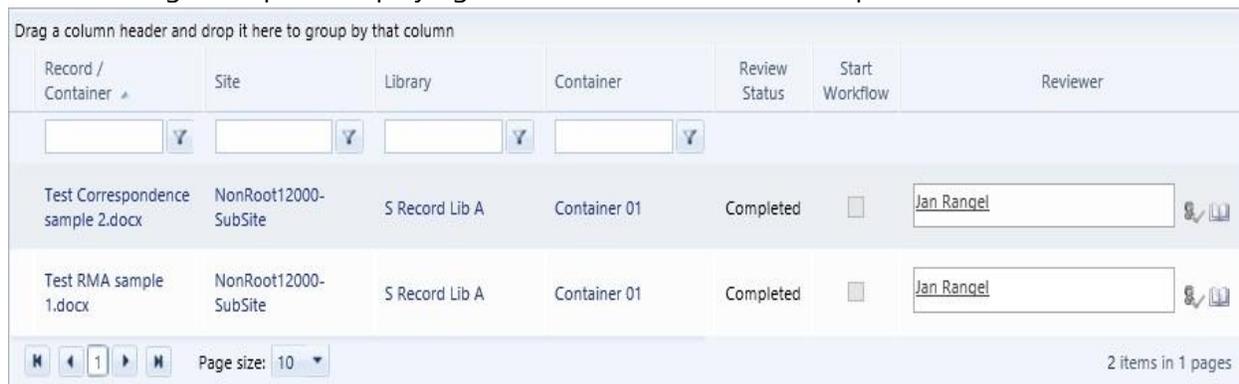
Figure 9-18 Viewing the Cutoff Search Report Details Dialog Box

9.5.2 Deleting a Cutoff Search Report

To remove an existing Cutoff Search Reports from your site, you must delete the Cutoff Search Reports item.

1. From the **Cutoff Search Reports List** screen, select the Cutoff Search Report that you want to delete. When a report is selected, the **List Tools → Items** opens in the header ribbon.
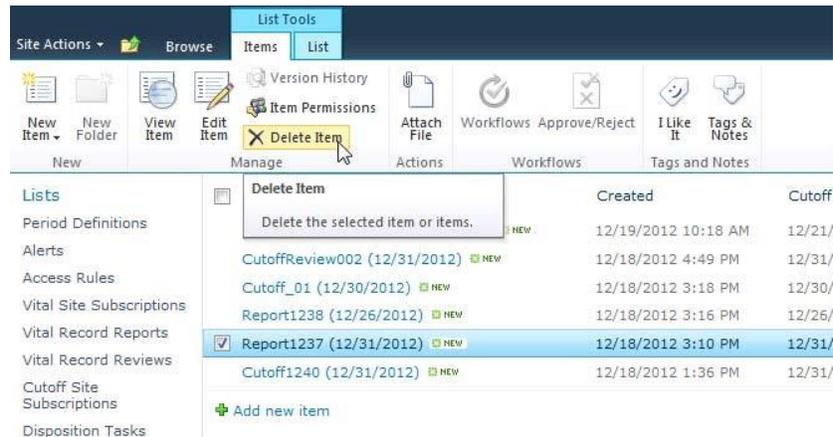
Figure 9-19 Cutoffs: Delete Item Selection

2. Click the **Delete Item** button on the header ribbon. A prompt opens asking *Are you sure you want to send the item(s) to the site Recycle Bin?*

3. Click **OK** and the Cutoff Search Report(s) is deleted and removed from the **Cutoff Search Reports** list or click **Cancel** to return to the **Cutoff Search Reports** list screen without deleting the selected Cutoff Search Report(s).

9.6 Cutoff Review Workflows

Compliance Suite Records Managers can use a cutoff workflow to assist in the process of reviewing cutoff records. Compliance Suite Records Managers can start workflows and view workflow task history by the following methods:

- Starting workflows from the dialog box
- Viewing workflow task history from the workflow task list

9.6.1 Running a Cutoff Review Workflow

Compliance Suite Records Managers can run Cutoff Review Workflows on the selected cutoff record containers and records that need review by viewing past search reports from the **Cutoff Search Reports** list.

To start a Cutoff Review workflow:

1. Select **Site Contents** and then **Cutoff Search Reports**.
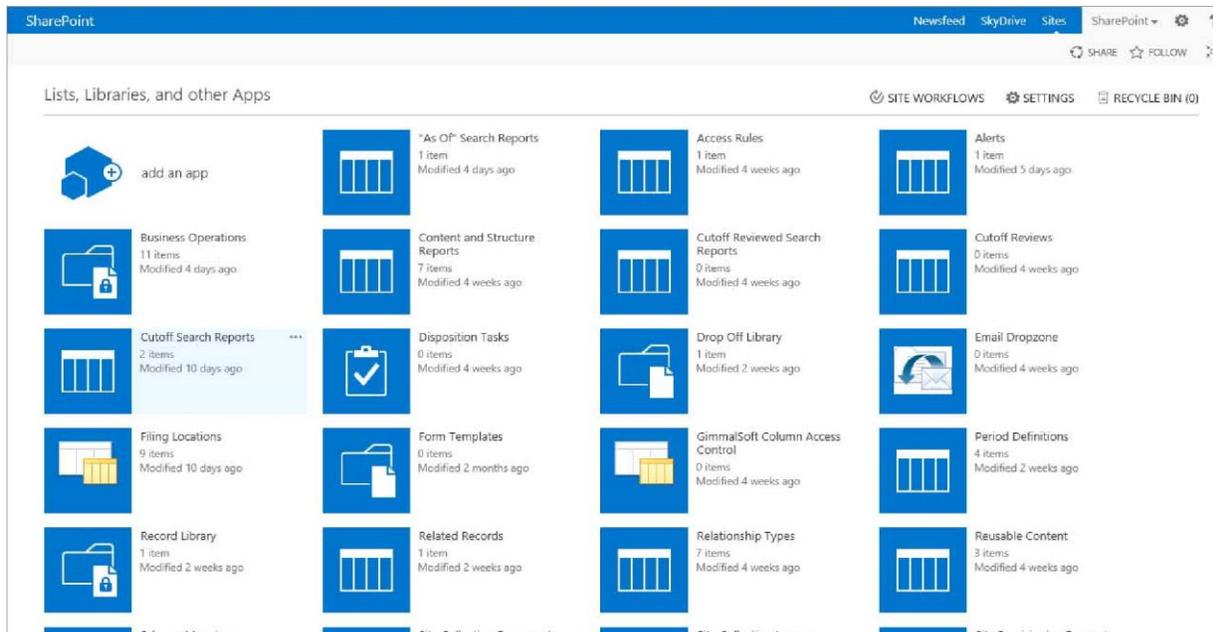
Figure 9-20 Selecting Cutoff Search Reports

2. Click **Cutoff Search Reports** to see reports, as follows:

Figure 9-21 Cutoff Search Reports

3. After clicking an entry in the **Cutoff Search Reports** link, the following screen displays.

Figure 9-22 Cutoff Search Report Details

4. Check the **Start Workflow** check box on each cutoff record to review, enter the name of the reviewer, and check the reviewer's name by clicking the check mark beside the name.

5. Click **Start** to start the workflow.

6. When the window with the following message displays, click **OK**.
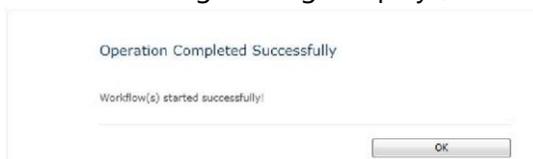
Figure 9-23 Successful Operation Message

The Search Reports screen displays.

9.6.2 Reviewing Cutoff Workflow Tasks

After the record or container Cutoff Process has started, a cutoff records workflow starts. The assigned reviewer for the workflow task can review the Cutoff Review Workflow task by accessing the Workflow Task list.

To review a workflow task via the Workflow Task list, follow these steps.

1. Select **Cutoff Processing** and then **Due for Cutoff Review** from the header ribbon.

2. Select an entry in the list and click on the workflow task. Scroll down and click on the **Cutoff Reviews List** link.

Figure 9-24 Cutoff Workflows

3. The **Workflow Task** dialog box displays. In the **Review Task** field, click **Approve** to approve the workflow or **Reject** to reject the workflow. Enter optional comments in the **Comments** field.
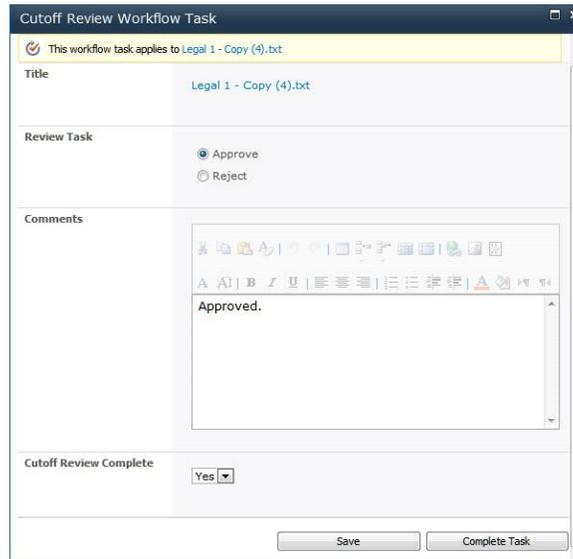
Figure 9-25 Cutoff Review Workflow Task

4. To indicate that the cutoff review is complete, select the item and choose **Edit**. Click **Complete Task** and select **Yes**. A *Task saved successfully...* message displays.
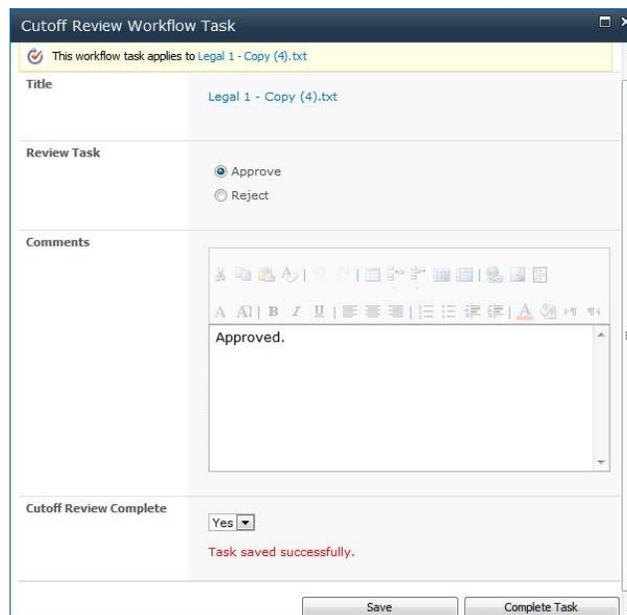
Figure 9-26 Completing a Workflow Task

To save the Workflow task without completing the cutoff review, click **No** in the **Cutoff review complete** field.

5. Click the **X** in the upper right corner of the title bar to close the task.

---

6. Once a workflow is completed, the **Cutoff Review Workflow** status column in the **Due for Cutoff Review View** screen is updated to Completed.

Figure 9-27 Workflow Completed Status

9.7 Compliance Suite Reverse Cutoff

Compliance Suite **Reverse Cutoff** functionality allows users to clear the cutoff date of a record or a Case Based Retention record container allowing them to appear in **Due for Cutoff Review** searches again.

To perform or start and not implement Compliance Suite Reverse Cutoff:

1. Select **Cutoff Processing** and then **Reverse Cutoff** from the header ribbon.
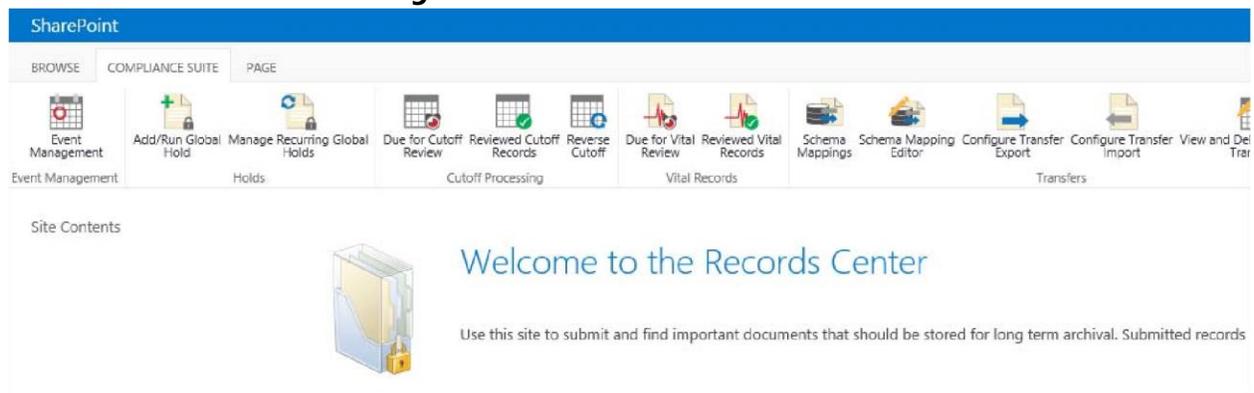
Figure 9-28 Selecting Reverse Cutoff

2. The **Compliance Suite Reverse Cutoff** screen displays. Click the **Select Record or Container** button.

Figure 9-29 Select Record or Container

3. When the **Select an Asset** dialog box displays, select the record or Case Based Retention record container you want to reverse cutoff.

4. Click **OK** or click **Cancel** to cancel the operation and return to the Compliance Suite Reverse Cutoff screen.
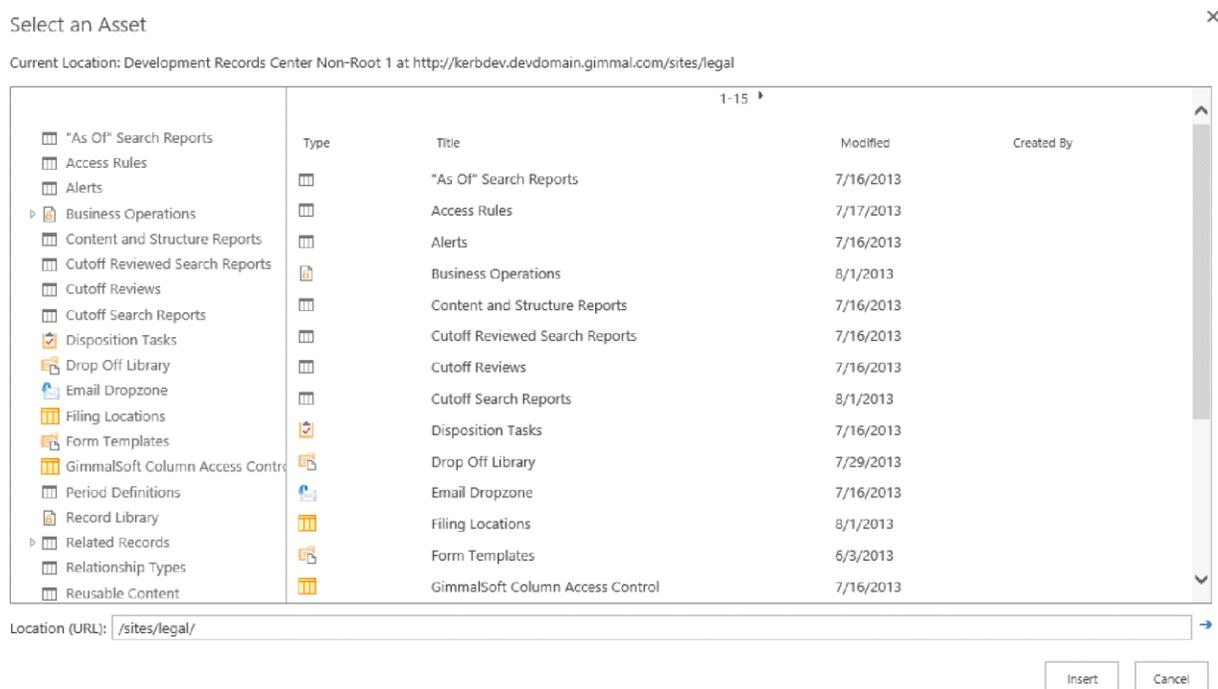
Figure 9-30 Select an Asset

5. The **Compliance Suite Reverse Cutoff** screen displays, showing the URL of the record or Case Based Retention (CBR) record container under the **Select Record or Container** button. If the CBR Container is closed, you are prompted to reopen the container.
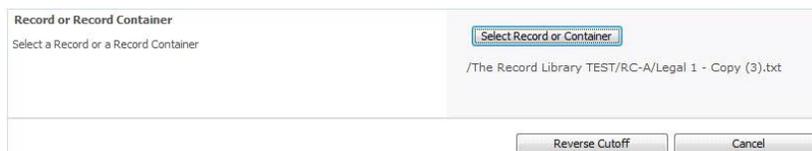
Figure 9-31 Reversed Container

> **Note:**
>
> If you select a container that does not contain records or CBR containers, the message that is displayed in the **Select a Record or a Record Container** field says: *The selection is invalid. Only CBR-Categories, or records in non-CBR Categories, can be selected.* Click the **Reverse Cutoff** button to reverse cutoff on the record or Case Based Retention record container or **Cancel** to cancel the operation and return to the Records Center home screen.

6. Click the **Reverse Cutoff** button to reverse cutoff on the record or Case Based Retention record container or **Cancel** to cancel the operation and return to the Records Center home screen.

Figure 9-32 Successful Reversed Cutoff Message

7. To implement reverse cutoff on more than a single item click on the **Select Record or Container** button to repeat the reverse cutoff process, or click **Cancel** to cancel the operation and return to the **Records Center** home screen. If you do a cutoff on a CBR container you can optionally open the container.

10 Disposition Processing

Disposition is the last stage in the record life cycle where records are disposed. There are two ways to dispose of records: transfer and destruction. A records disposition program provides for the effective and efficient management of records no longer needed in office space to conduct current business. It has three main objectives:

1. The prompt disposal of temporary records whose authorized retention periods have expired

2. The timely and systematic transfer to economical storage of records no longer needed in office space but not yet eligible for final disposition

3. The identification and transfer of permanent records to offsite storage

Compliance Suite enables disposition processing through its File Plan Builder tool. File Plan Builder is a tool to create and manage a file plan that supports your organization's records management policies. Compliance Suite allows administrators and records managers to create and modify retention schedule policies for record containers by setting Disposition Instructions in File Plan Builder. A retention schedule specifies how long a record stays (is retained) in a phase and when the record transitions to the next phase. Disposition Instructions are instructions that define what to do with records at certain points in their lifecycle. Disposition Instructions consist of lifecycle stages that define duration specifications (for example, 2 Months) and disposition actions (e.g., Delete Record) to be performed when the duration specification is met. For more information on File Plan Builder, see the latest version of the *File Plan Builder Administration Guide*.

Compliance Suite Disposition Processing consists of the following steps:

1. Compliance Suite records manager creates a Disposition Action. A Disposition Action defines the technical parameters of the action to be taken as part of the disposition process.

2. Compliance Suite records manager creates Disposition Instructions.

3. Compliance Suite records manager applies Disposition Instructions to a file plan container.

4. Disposition Instructions are translated into a SharePoint information management policy for expiration.

5. Retention stages are defined as part of Disposition Instructions and are applied to the file plan container.

6. Compliance Suite records manager sets a Cutoff Date. Compliance Suite uses the Cutoff Date as the default date for Disposition Processing, but Compliance Suite administrators and records managers can set different dates at their discretion.

7. A GimmalSoft Compliance Suite Disposition Metadata Timer Job updates the disposition metadata from the disposition objects onto the SharePoint folders and records.

8. An Information Management Policy Timer Job processes records periodically/nightly, and those records that become eligible enter into the first Disposition Stage. For Compliance Suite, all disposition actions are workflows.

9. A Compliance Suite Disposition Task Workflow creates a task that links to its corresponding record or record folder.

Intended User: Compliance Suite Administrator, Records Manager

10.1 Compliance Suite Disposition Workflows

Compliance Suite enables Compliance Suite records managers to add and customize disposition workflows.

Note

Before a Disposition Workflow is selected, it must be associated with the library.

The following tables describe the Compliance Suite Disposition Workflows and Advanced Disposition Workflows.

Table 10-1 Disposition Workflows

Disposition Workflow Name	Description
Delete Record and Metadata	Removes all document versions and metadata. Deletes a record upon confirmation.
Delete Record, Retain Metadata	Deletes record but retains the record's metadata. Deletes record upon confirmation.
Transfer Record	Transfers record out of SharePoint to the UNC destination location that is specified in the transfer location of the Workflow Settings. For more information on transferring records, see the Transfers help section.
Transfer Record, Delete Record and Metadata	Transfers record to a NARA-approved format, then deletes record and metadata. Deletes record upon confirmation.
Transfer Record, Delete Record and Retain Metadata	Transfers record to a NARA-approved format, then deletes record and retains record's metadata. Deletes record upon confirmation.

Table 10-2 Advanced Disposition Workflows

Advanced Disposition Workflow Name	Description
Advanced Delete Record and Metadata	Removes all document versions and metadata. Provides advanced options to either confirm the deletion or to suppress it allowing for automatic disposition.
Advanced Delete Record, Retain Metadata	Deletes record but retains the record's metadata. Provides advanced options to either confirm the deletion or to suppress it allowing for automatic disposition.
Advanced Transfer Record	Transfers record out of SharePoint to the UNC destination location that is specified in the transfer location of the Workflow Settings. For more information on transferring records, see the Transfers help section.
Advanced Transfer Record, Delete Record and Metadata	Transfers record to a NARA-approved format, then deletes record and metadata. Provides advanced options to either confirm the deletion or to suppress it allowing for automatic disposition.
Advanced Transfer Record, Delete Record and Retain Metadata	Transfers record to a NARA-approved format, then deletes record and retains record's metadata. Provides advanced options to either confirm the deletion or to suppress it allowing for automatic disposition.

Note:

The advanced workflows are available only if activated. Please see the latest version of the *Compliance Suite Installation Guide* for more information.

10.1.1 Adding and Customizing Delete Record Disposition Workflows

To add a Compliance Suite Delete Record Disposition Workflow, perform the following steps:

1. Add a workflow: From the target record container, click the **Library** tab in the header ribbon; then select **Workflow Settings** and **Add a Workflow**.
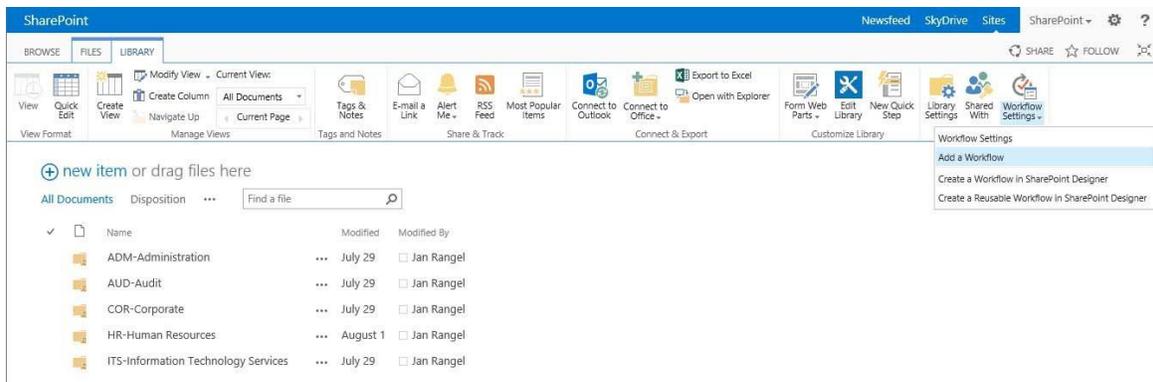
Figure 10-1 Add a Workflow

The **Add a Workflow** dialog box displays with fields for adding a new workflow.

Figure 10-2 Add a Workflow dialog box

2. In the **Content Type** field, select **All** in the **Run on items of this type:** menu box.

3. In the **Workflow** field, select the workflow that you want to use. The Advanced workflow options only display if they have been activated.

4. (**Required**) In the **Type a unique name for this workflow** field, type a unique name for the workflow.

5. In the **Task List** field, select **Disposition Tasks**.

6. In the **History List** field, select **Workflow History**.

7. In the **Start Options** field, click:

   - **Allow this workflow to be manually started by an authenticated user with Edit item permissions** if you want to allow the workflow to be manually started by an authenticated user with Edit permissions

   - **Require Manage List Permissions** to start the workflow if you want to require the Manage List Permissions to start the workflow

   - **Start this workflow when a new item is created** if you want to start the workflow when a new item is created

   - **Start this workflow when this item is changed** if you want to start the workflow when the item is changed.

8. Click **Next** to add the workflow.

9. The **Customize the GimmalSoft Compliance Suite Advanced Delete Record And Metadata Workflow** or **Customize the Compliance Suite Delete Record - Retain Metadata Workflow** screen, depending on which workflow you added, is displayed with fields for customizing the workflow.

10. In the **Specify a Task List** field, select the Disposition Task Last in the **Disposition Task List** menu box. Selections include: *Disposition Tasks* and *Workflow Tasks*.

11. In the **Specify a Destruction Certificate Container** field, click **Create a Destruction Certificate** if you want to create a Destruction Certificate for the record container. Ensure you have previously created a Destruction Certificates container in a Destruction Certificates record library that will store Destruction Certificates. Click **Browse** and select the location for the Destruction Certificate record container in the **Destruction Certificate Record Container** field. The **Select an Asset** dialog box opens. Select the container in which you want to store the destruction certificates in the **Destruction Certificates Library** and click **OK**. The location of the Destruction Certificate container is displayed in the **Destruction Certificate Record Container** field.

Note:

Be sure that you do not select a closed record container as the target for the disposition certificates.

12. In the **Require a Delete Confirmation Page** field:

    a. Select **Delete Confirmation Required** if you want to require a Delete Confirmation Page.

    b. If you selected an Advanced workflow, select **Remove All Confirmations** if you want all confirmations removed.

13. Click **Associate Workflow** to create the workflow or click **Cancel** to cancel the operation without adding a new workflow.

10.1.2 Adding and Customizing Transfer Record Disposition Workflow

To add a Compliance Suite Transfer Record Disposition Workflow, perform the following steps:

1. Add a workflow: From the target record container, select the **Library** tab in the header ribbon; then select **Workflow Settings** and **Add a Workflow**.

    The **Document Library Settings → Add a Workflow** screen is displayed with fields for adding a new workflow.

2. In the **Content Type** field, select **All in the Run** for **Items of this type**.

3. In the **Workflow** field, select **Compliance Suite Transfer Record** or **Advanced Compliance Suite Transfer Record**. The Advanced workflow options only appear if they have been activated.

4. (**Required**) In the **Type a unique name for this workflow** field, type a unique name for the workflow.

Note:

If you are using File Plan Builder to associate the Disposition Instruction, the name employed here must match the Disposition Action in File Plan Builder.

5. In the **Task List** field, select **Disposition Tasks** in the **Select a task list** field.

6. In the **History List** field, select **Workflow History** in the **Select a history list** field.

7. In the **Start Options** field, click:

    *   **Allow this workflow to be manually started by an authenticated user with Edit item permissions** if you want to allow the workflow to be manually started by an authenticated user with Edit permissions

    *   **Require Manage List Permissions to start the workflow** if you want to require the Manage List Permissions to start the workflow

    *   **Start this workflow when a new item is created** if you want to start the workflow when a new item is created

- **Start this workflow when this item is changed** if you want to start the workflow when the item is changed

8. Click **Next** to add the workflow.

9. The **Customize the Compliance Suite Transfer Record Workflow** screen displays with fields for customizing the Compliance Suite Transfer Record Disposition Task workflow.

10. In the **Specify a Task List** field, select a **Transfer Task List**. The options are *Disposition Tasks* and *Workflow Tasks*.

11. In the **Specify a Confirmation Receipt List** field, select a list where confirmation receipt details can be entered. The options are *Disposition Tasks* and *Workflow Tasks*.

12. In the **Select Schema Mappings File** field, select a Schema Mappings File. Compliance Suite options are Date Received, NARA, Basic Export Schema and Transfer Record.

13. (**Required**) In the **Specify a Transfer Location** field, enter a network drive to serve as an output destination for transferred records.

    The **Transfer Location** is the network file location where the records and their metadata will be exported. The **Transfer Location Network Path** details should be provided by your Compliance Suite Administrator.

14. Click **Associate Workflow** to create the workflow or click **Cancel** to cancel the operation without adding a new workflow.

10.1.3 Adding and Customizing Record, Delete Record and Metadata Workflow

To add a Compliance Suite Transfer Record, Delete Record and Metadata Disposition Workflow, perform the following steps:

1. Add a workflow: From the target record container, select the **Library** tab in the header ribbon. Select **Workflow Settings** and then **Add a Workflow**.

2. The **Document Library Settings** → **Add a Workflow** dialog box is displayed with fields for adding a new workflow.

3. In the **Content Type** field, select **All** from the **Run on items of this type** menu. This is the default selection.

4. In the **Workflow** field, select **Compliance Suite Transfer Record, Delete Record and Metadata** or **Advanced Compliance Suite Transfer Record, Delete Record and Metadata**. The Advanced workflow options only appear if they have been activated.

5. (**Required**) In the **Type a unique name for this workflow** field, type a unique name for the workflow.

 Note:

If you are using File Plan Builder to associate the Disposition Instruction, the name employed here must match the Disposition Action in File Plan Builder.

---

6. In the **Task List** field, select Disposition Tasks in the **Select a task list:** field.

7. In the **History List** field, select Workflow History in the **Select a history list:** field.

8. In the **Start Options** field, click:

   - **Allow this workflow to be manually started by an authenticated user with Edit item permissions** if you want to allow the workflow to be manually started by an authenticated user with Edit permissions

   - **Require Manage List Permissions to start the workflow** if you want to require the Manage List Permissions to start the workflow

   - **Start this workflow when a new item is created** if you want to start the workflow when a new item is created

   - **Start this workflow when this item is changed** if you want to start the workflow when the item is changed

9. Click **Next** to add the workflow.

10. The workflow screen displays with fields for customizing the workflow.

11. In the **Specify a Transfer Confirmation Task List** field, select a **Transfer Confirmation Task List**. This is the list where transfer tasks are created. The options are Disposition Tasks and Workflow Tasks.

12. In the **Specify a Confirmation Receipt List** field, select a list where confirmation receipt details can be entered. The options are Disposition Tasks and Workflow Tasks.

13. In the **Specify a Task List** field, select a Transfer Task List. The options are Disposition Tasks and Workflow Tasks.

14. In the **Select Schema Mappings File** field, select a Schema Mappings File. The options are Date Received, NARA, Basic Export Schema, and Transfer Record.

15. (**Required**) In the **Specify a Transfer Location** field, enter a network drive to serve as an output destination for transferred records.

    The **Transfer Location** is the network file location where the records and their metadata will be exported. The Transfer Location Network Path details should be provided by your Compliance Suite Administrator.

16. In the **Specify a Destruction Certificate Container** field, click **Create a Destruction Certificate** if you want to create a Destruction Certificate for the record container.

    Ensure that you have previously created a Destruction Certificates container in a Destruction Certificates record library that will store Destruction Certificates.

17. Click **Browse** and select the location for the Destruction Certificate record container in the Destruction Certificate Record Container field. The **Select an Asset** dialog box opens.

18. Select the container in which you want to store the destruction certificates in the Destruction Certificates Library and click **OK**. The location of the Destruction Certificate container is displayed in the **Destruction Certificate Record Container** field.

19. In the **Require a Delete Confirmation Page** field:

    a. Select **Delete Confirmation Required** if you want to require a Delete Confirmation Page.

    b. If you selected an advanced workflow, select **Remove All Confirmations** if you want all confirmations removed.

20. Click **Associate Workflow** to create the workflow or click **Cancel** to cancel the operation without adding a new workflow.

10.1.4 Adding and Customizing Transfer Record, Delete Record and Retain Metadata Workflow

To add a Compliance Suite Transfer Record, Delete Record and Retain Metadata Disposition Workflow, perform the following steps:

1. Add a workflow: From the target record container, select the **Library** tab in the header ribbon; then select **Workflow Settings** and **Add a Workflow**.

    The **Document Library Settings → Add a Workflow** screen is displayed with fields for adding a new workflow.

2. In the **Content Type** field, select **All** in the **Run on items of this type** menu.

3. In the **Workflow** field, select **Compliance Suite Transfer Record, Delete Record and Retain Metadata** or **Advanced Compliance Suite Transfer Record, Delete Record and Retain Metadata**. The Advanced workflows only appear if they have been activated.

4. (**Required**) In the **Type a unique name for this workflow** field, type a unique name for the workflow.

Note:

If you are using File Plan Builder to associate the Disposition Instruction, the name employed here must match the Disposition Action in File Plan Builder.

---

5. In the **Task List** field, select **Disposition Tasks**.

6. In the **History List** field, select **Workflow History**.

7. In the **Start Options** field, click:

    - **Allow this workflow to be manually started by an authenticated user with Edit item permissions** if you want to allow the workflow to be manually started by an authenticated user with Edit permissions

- **Require Manage List Permissions to start the workflow** if you want to require the Manage List Permissions to start the workflow

- **Start this workflow when a new item is created** if you want to start the workflow when a new item is created

- **Start this workflow when this item is changed** if you want to start the workflow when the item is changed

8. Click **Next** to add the workflow.

9. The workflow displays with fields for customizing it.

Figure 10-3 Customize Screen

10. In the **Specify a Task List** field, select a **Transfer Task List**. The options are Disposition Tasks and Workflow Tasks.

11. In the **Specify a Confirmation Receipt List** field, select a list where confirmation receipt details can be entered. The options are Disposition Tasks and Workflow Tasks.

12. In the **Select Schema Mappings File** field, select a Schema Mappings File. The options are Date Received, NARA, Basic Export Schema and Transfer Record.

13. (**Required**) In the **Specify a Transfer Location** field, enter a network drive to serve as an output destination for transferred records. The Transfer Location is the network file location where the records and their metadata will be exported. The Transfer Location Network Path details should be provided by your Compliance Suite Administrator.

14. In the **Specify a Destruction Certificate Container** field, click **Create a Destruction Certificate** if you want to create a Destruction Certificate for the record container.

   Ensure you have previously created a Destruction Certificates container in a Destruction Certificates record library that will store Destruction Certificates.

15. Click **Browse** and select the location for the Destruction Certificate record container in the **Destruction Certificate Record Container** field. The **Select an Asset** dialog box opens.

16. Select the container in which you want to store the destruction certificates in the Destruction Certificates Library and click **OK**. The location of the Destruction Certificate container is displayed in the **Destruction Certificate Record Container** field.

17. In the **Require a Delete Confirmation Page** field:

    a. Select **Delete Confirmation Required** if you want to require a Delete Confirmation Page.

    b. If you selected an advanced workflow, select **Remove All Confirmations** if you want all confirmations removed.

18. Click **Associate Workflow** to create the workflow or click **Cancel** to cancel the operation without adding a new workflow.

10.1.5 Removing a Compliance Suite Disposition Workflow

To remove a Compliance Suite Disposition Workflow, perform the following steps:

1. From the target record container, click the **Library** tab in the header ribbon. Select **Workflow Settings** and then select **Workflow Settings**. The **Document Library Settings → Workflow Settings** screen displays.

2. Select **Remove**, **Block**, or **Restore a Workflow**.

3. The **Workflows** screen displays. Locate the workflow(s) you want to remove and click the **Remove** radio button(s).

Figure 10-4 Workflows Screen

4. Click **OK** to remove the workflow(s) or **Cancel** to cancel the operation without removing the workflow(s).

10.2 Disposition Workflow Tasks

Compliance Suite enables Compliance Suite records managers to add, edit, view, and delete disposition workflow tasks. All of the tasks involved with a Disposition Workflow Task are recorded in the Disposition Tasks list that is associated with the workflow. The Disposition Workflow Tasks list is designated when the workflow is added to a list, library, or content type. The following table describes the Disposition Tasks list and a description of each heading.

Note

Disposition workflows must be run in English as an English user.

Table 10-3 Disposition Tasks

List View Heading	Description
Content Type	Type of Disposition Task. The options are Disposition Task, Transfer Task, and Confirmation Task.
Title	Unique identifier used to further differentiate the Disposition Task from other Disposition Tasks.
Status	Status of the Disposition Task. The options are Not Started, In Progress, Completed, Deferred, and Waiting on someone else.
Priority	Priority of the task. The options are (1) High, (2) Normal and (3) Low.
% Complete	Completion percentage of the Disposition Task.

10.2.1 Processing a Disposition Workflow Task

To process an existing Disposition Workflow Task, perform the following steps.

1. From the **Disposition Tasks → All Tasks** screen, select the Disposition Workflow Task you want to process.

2. You can only process one Disposition Workflow Task at a time. There are two ways to process a Disposition Workflow Task.

   - Click **...** twice to display the menu and click **Edit Item**.

   - Select **List Tools → Items** tab. Select the item and select the **Items** tab. In the header ribbon, select **Edit Item**. The **Workflow Task** dialog box displays.

3. In the **Disposition** field, click **Delete this record or container** to delete the record or container or click **Do not delete this record or container** if you do not want to delete the record or container. Enter optional comments in the **Comments** field.

4. Click **OK** to process the Disposition Workflow Task or **Cancel** to return to the **Disposition Tasks → All Tasks** list without processing the selected Disposition Workflow Task.

10.2.2 Viewing a Disposition Workflow Task

To view the details of an existing Disposition Workflow Task, you must view the Disposition Workflow Task item.

1. From the **Disposition Tasks → All Tasks** screen, select the **Disposition Workflow Task** that you want to view. You can only view one Disposition Workflow Task at a time. There are two ways to view a Disposition Workflow Task.

   - Click **...** to display the open menu and click **View Item**.

   - Select the item to view and click the **Items** tab. In the header ribbon, select **View Item**. The **Disposition Tasks View** dialog box displays.
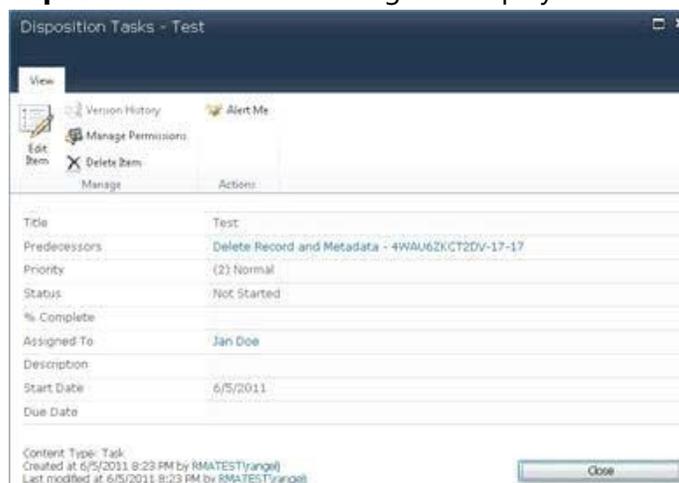
Figure 10-5 Disposition Tasks

2. From the **Disposition Task View**, you can edit, delete, or manage permissions of the selected Disposition Workflow Task.

3. Click **Close** to return to the **Disposition Tasks → All Tasks** screen.

10.3 Retention Schedule Policy

Retention schedule, also known as retention rules, specifies how long a record stays (is retained) in a phase and when the record transitions to the next phase. A retention schedule can be driven by time, event, or event time. Event time means that when a specified time has taken place after a particular event has happened; a record has to move out of the current phase and into the next phase. The time does not start calculating until the particular event has taken place (e.g., the closing of a case or project or the termination of a task or employee).

Compliance Suite allows administrators and records managers to create and modify retention schedule policies for record containers by setting Disposition Instructions in "Disposition Processing" on page 156. Disposition Instructions consist of lifecycle stages that define duration specifications (e.g., 2 Months) and actions (e.g., Delete Record) to be performed when the duration specification is met. For more information refer to the chapter "Disposition Processing" on page 156.

11 Bulk Task Processing

Compliance Suite's Bulk Task Processing feature allows you to process Cutoff Review tasks in the Workflow Tasks list or Disposition/Transfer tasks in the Disposition Tasks list in bulk. Bulk Task Processing differs from Bulk Processing in that Bulk Processing focuses on metadata, while Bulk Task Processing focuses on not only metadata changes related to the tasks but task completion as well. It provides a context-aware interface that allows for bulk metadata updates and completion of tasks in bulk that are for tasks that are going through a cutoff review or disposition process.

Because there can be numerous tasks to process in Bulk Task Processing, it is done asynchronously and a saved report named as you desire contains all of the results.

Intended User: Records Manager, Compliance Suite Administrator

11.1 Configuring Custom Columns for Bulk Task Processing

If you have added custom columns to the Workflow task list and/or the Disposition task list and want them to appear in the Bulk Task Processing component, follow the steps below.

1. Navigate to **Central Administration > Compliance Suite > Bulk Task Processing Settings**. The Bulk Task Processing Settings page displays.
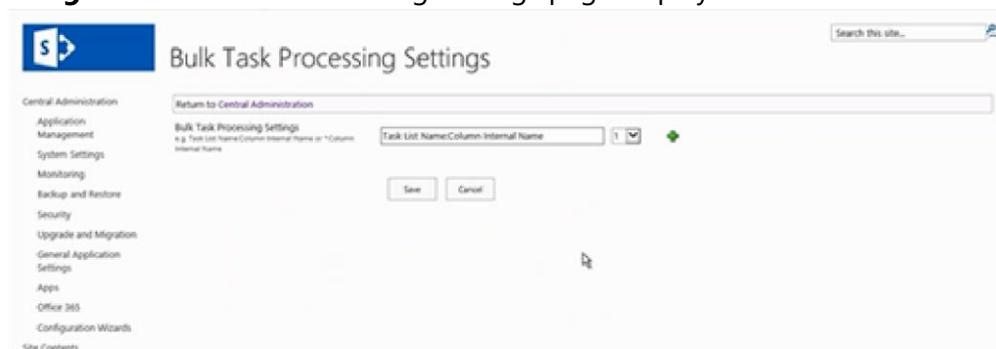
Figure 11-1 Bulk Task Processing Settings Page

Note:

If the **Bulk Task Processing Settings** link does not appear, activate the **Gimmal Compliance Suite - Bulk Task Processing** farm feature. Refer to the *Compliance Suite Installation Guide* for information to perform this task.

---

2. Enter the desired **Task List Name** and **Column Internal Name** in the **Bulk Task Processing Settings** field. For example, if you added a column to the Disposition Tasks list named *Deferred*, the format to enter would be *Disposition Tasks: Deferred*.

You can enter up to three column names at a time. Click + next to the field name to display additional fields to enter additional column names.

3. If you want to apply these column names to multiple task lists, simply replace the task list name with an asterisk.

Figure 11-2 Applying Columns to Multiple Task Lists

4. Click **Save**.

5. Navigate to **Site Contents > Disposition Tasks** to verify that the configured column displays display in the column lists.

   You can also access B**ulk Task Processing** to ensure that the columns display in the desired task tabs.

Figure 11-3 Verifying Configured Columns in Bulk Task Processing Tabs

11.2 Cutoff Review Tasks

Follow these steps to process cutoff review tasks in bulk from the Workflow Tasks list:

1. Select **Site Contents > Workflow Tasks**. The current **Workflow Tasks** screen displays.

Figure 11-4 Workflow Tasks

2. Select **Bulk Task Processing** from the Compliance Suite ribbon bar.

Figure 11-5 Selecting Bulk Task Processing from the Compliance Suite Ribbon Bar

The Bulk Task Processing page displays the **Cutoff Review Task** tab.

Figure 11-6 Bulk Task Processing - Cutoff Review Task Tab

3. (**Required**) Enter a title to help you identify this batch of bulk task processing in the **Bulk Task Report Title** field.

4. Select the **Review Task** that you want to perform in bulk on these items. In the previous figure, **Approve** is selected.

5. Enter any **Comment** about this batch of bulk task processing, which is applied to each item you select for processing.

6. Review this task's items available for processing in the lower part of the page. You can also click on the **Library** or **Container** links to review an item. You can also filter the items in the fields across the top of the item list.

7. Click the check box in the upper left of the items to select all items for processing or individually select them. The select all check box selects all items across all pages for a specific tab and not just the visible items on the page. If you select multiple items on different pages, the selection is preserved when submitting items for bulk processing. For example, your page size is 10 and you have three pages. If you select one item on page1 and then two items on page 3, all three items are processed.

Note:

If you select all items and there are more than 1000, a message displays asking if you want to select all tasks.

---

8. Click **Bulk Task Processing** at the bottom or top of the page. The items are queued to be processed by the Bulk Task Processing Timer job.The following message displays:

GimmalSoft Compliance Suite - Bulk Task Processing Timer Job started Successfully

Click here to view the Bulk Task Processing List. It will show the status of Bulk Task Processing Report.

Figure 11-7 Successful Bulk Task Processing Message

9. Click the link to display the Bulk Task Processing Report page and view the status. You can also go to **Site Contents > Bulk Task Processing Report** to view the status at any time.

Bulk Task Processing Report ⓘ

⊕ new item

Bulk Task Processing Report   All Items   •••   Find an item   🔎

✓	Title	Status	Items To Process
	Delete Records 9/10/15 (9/10/2015)	Completed	0
	Transfer Record (9/21/2015)	Completed	0
	Cutoff Review (9/29/2015) ❈	Pending	1
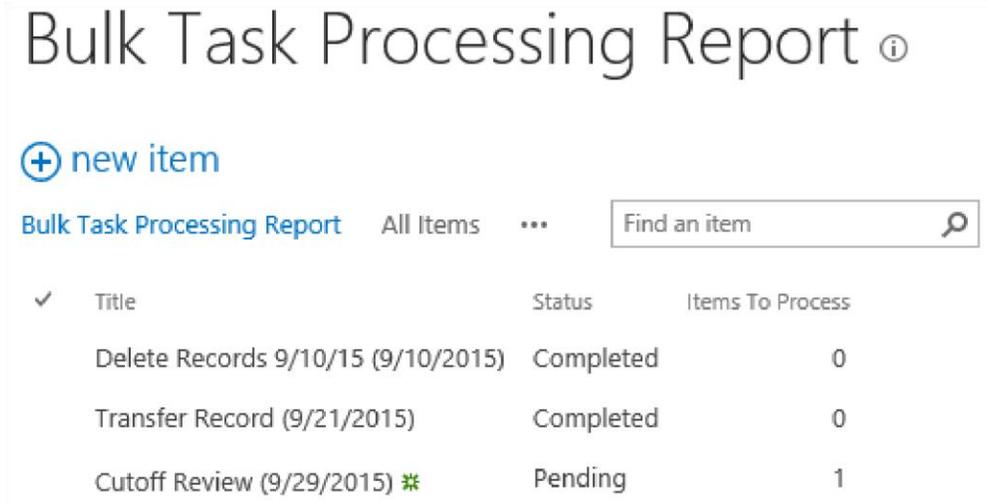
Figure 11-8 Bulk Task Processing Report Page and Status

10. Click the **Cutoff Review** report to view the items that were processed.

Bulk Task Processing Report - [Cutoff Review (9/29/2015)]

Record / Container	Site	Library	Container	Task Type	Workflow Name	Workflow Type	Reviewer	Review Status	Bulk Processing Status
Record 1.docx	Record Center	Bulk Test Library	Cutoff Folder	Cutoff Review Task	Cutoff Review Workflow	Cutoff Review Workflow	Test User	Completed	Successful

⏮ ◀ 1 ▶ ⏭   Page size 10 ▾   1 items in 1 pages

Cancel

Figure 11-9 Bulk Task Processing Report - Cutoff Review

11.3 Disposition Tasks

Disposition tasks indicate the action to take on a record at the end of its lifecycle. Compliance Suite offers the following disposition tasks:

- Delete Record and Metadata
- Delete Record, Retain Metadata
- Transfer Record - Transfer Task
- Transfer Record, Delete Record and Metadata
- Transfer Record, Delete Record, Retain Metadata

Important!

You must navigate to a Disposition Task List before selecting **Bulk Task Processing** in the Compliance Suite ribbon bar. You receive an error message if you have not selected a list.

The task types display on the Disposition Task, Transfer Task, or Transfer Confirmation tabs in Bulk Task Processing. Each tab displays the items related to that tab type, along with the specific metadata that can be entered.

Note:

The **Disposition Task**, **Transfer Task** and **Transfer Confirmation** tabs only display if there are transfer tasks that are **Not Started** in the Disposition Task list.
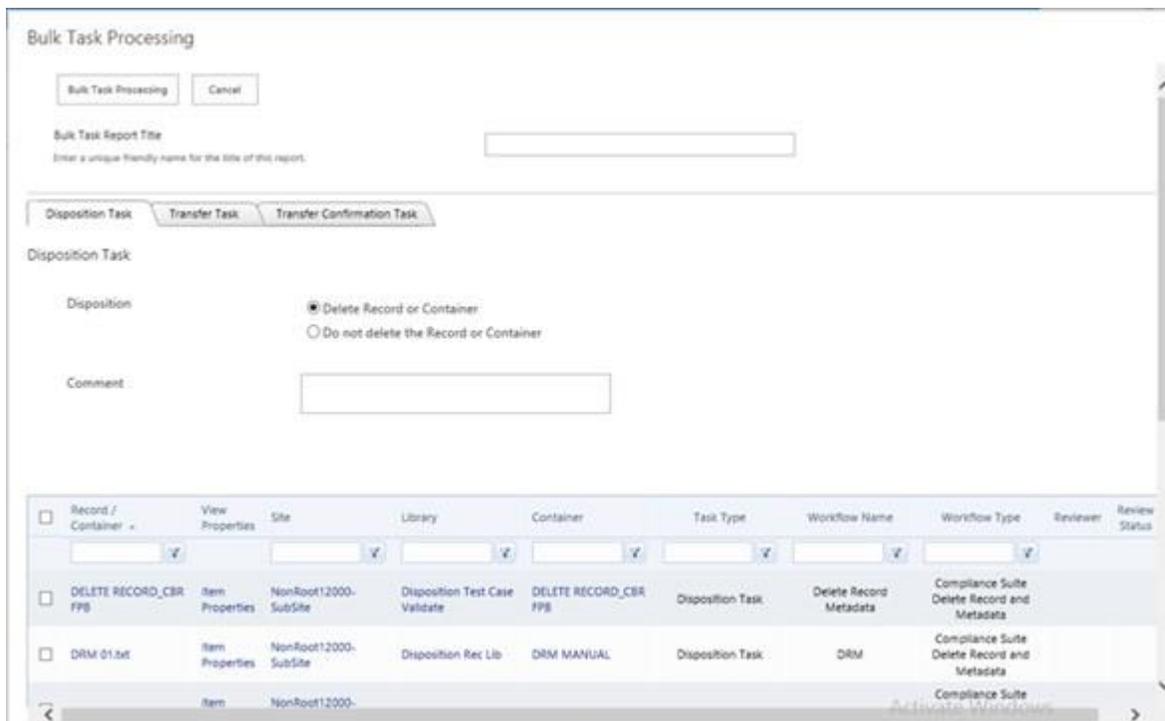
Figure 11-10 Disposition Task Tab
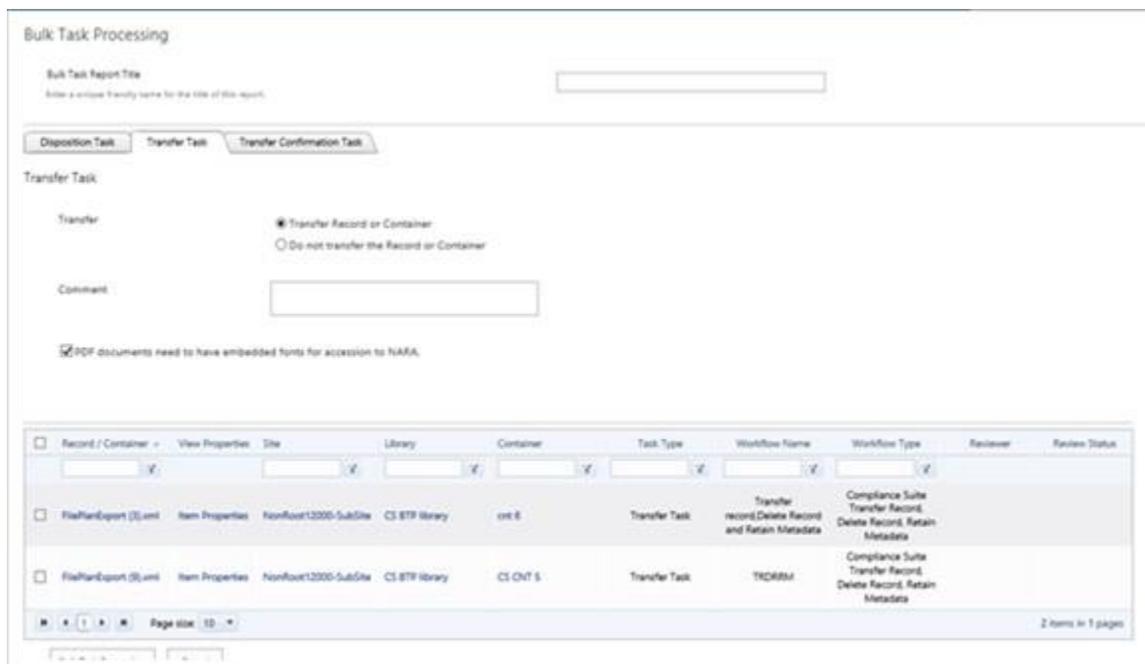
Figure 11-11 Transfer Task Tab
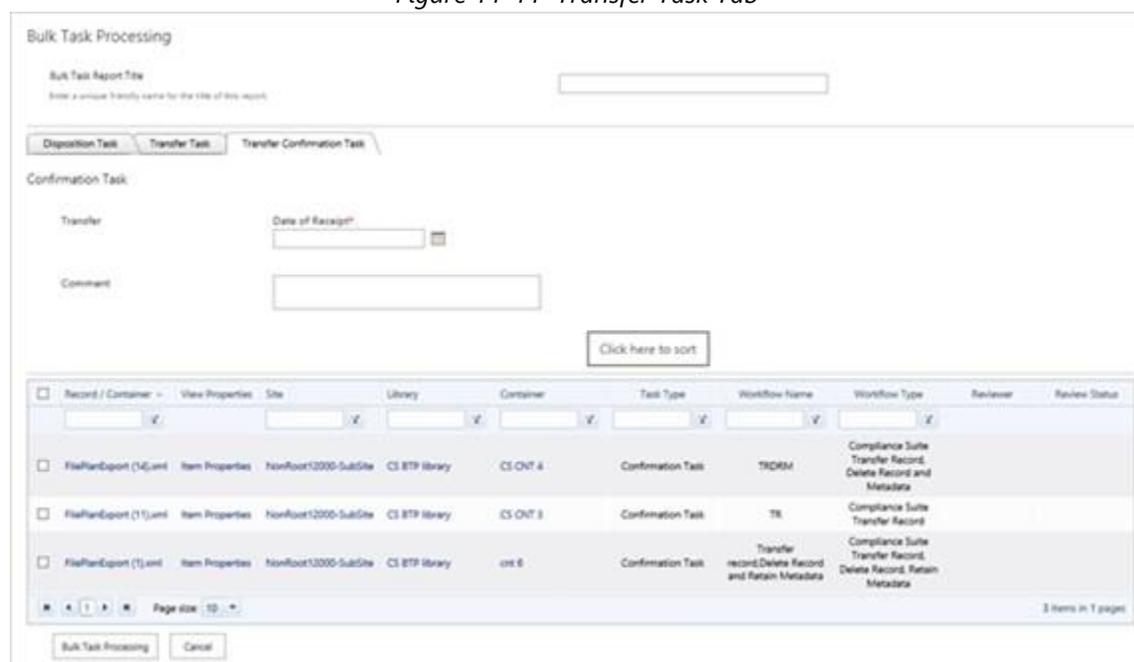
Figure 11-12 Transfer Confirmation Tab

11.4 Accessing Disposition Lists

You can navigate to the **Disposition Tasks List** by one of the following ways:

- Click **Lists** to the far right of the Compliance Suite tool bar and selecting **Disposition Tasks**
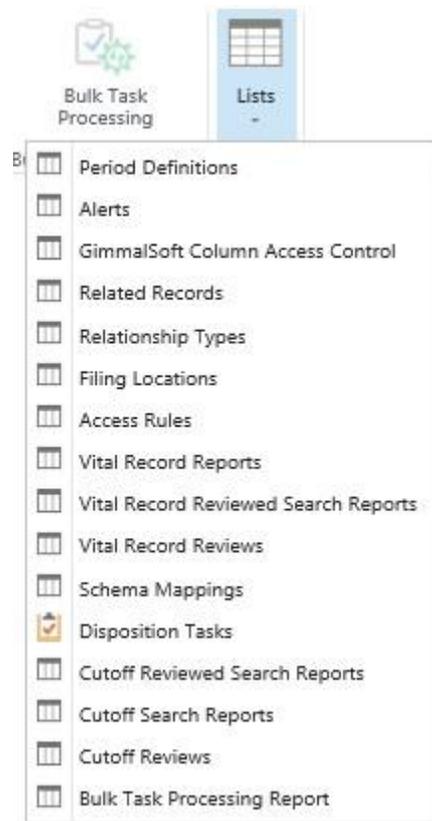
Figure 11-13 Compliance Suite Lists

- Select **Site Contents > Disposition Tasks.** The **Disposition Tasks** page displays the records queued for disposition processes.

Figure 11-14 Sample Disposition Tasks List

- Click **Bulk Task Processing** from the Compliance Suite ribbon bar.

Figure 11-15 Selecting Bulk Task Processing from the Compliance Suite Ribbon Bar

The Bulk Task Processing page displays with a tab for each task type from the **Disposition Task List**.

Figure 11-16 Bulk Task Processing Page

11.4.1 Processing Disposition Tasks

Disposition tasks allow you to delete the record and metadata or delete the record and retain the metadata. Follow these steps to process disposition tasks in bulk:

1. If not already selected, select the **Disposition Task** tab.

2. (**Required**) Enter a title to help you identify this batch of bulk task processing in the **Bulk Task Report Title** field.

3. Select the option that you want to perform in bulk on these items, which is applied to each item you select for processing. In the previous figure, **Delete Record or Container** is selected for **Disposition**.

4. Enter any **Comment** about this batch of bulk task processing, which is applied to each item you select for processing.

5. Review this task type's items available for processing in the lower part of the page. You can click on the **Library** or **Container** links to review an item to ensure an item is ready for disposition. You can also filter the items in the fields across the top of the item list.

Important!

Be sure you are ready to delete items in the Disposition Task list! The only way to retrieve them is to restore your system.

---

6. Click the check box in the upper left of the items to select all items for processing or individually select them. The select all check box selects all items across all pages for a specific tab and not just the visible items on the page.

   If you select multiple items on different pages, the selection is preserved when submitting items for bulk processing. For example, your page size is 10 and you have three pages. If you select one item on page 1 and then two items on page 3, all three items are processed.

Figure 11-17 Selecting Items for Processing

Note:

If you select all items and there are more than 1000, a message displays asking if you want to select all tasks.

---

7. Click **Bulk Task Processing** at the bottom or top of the page.

Figure 11-18 Bulk Task Processing Button

8. The items are queued to be processed by the Bulk Task Processing Timer job. The following message displays:

GimmalSoft Compliance Suite - Bulk Task Processing Timer Job started Successfully

Click here to view the Bulk Task Processing List. It will show the status of Bulk Task Processing Report.

Figure 11-19 Successful Bulk Task Processing Message

9. Click the link to display the Bulk Task Processing Report page and view the status.

Bulk Task Processing Report ⓘ

⊕ new item

Bulk Task Processing Report   All Items   •••   Find an item   🔍

✓	Title	Status	Items To Process
	Delete Records 9/10/15 (9/10/2015) ※	Running	2
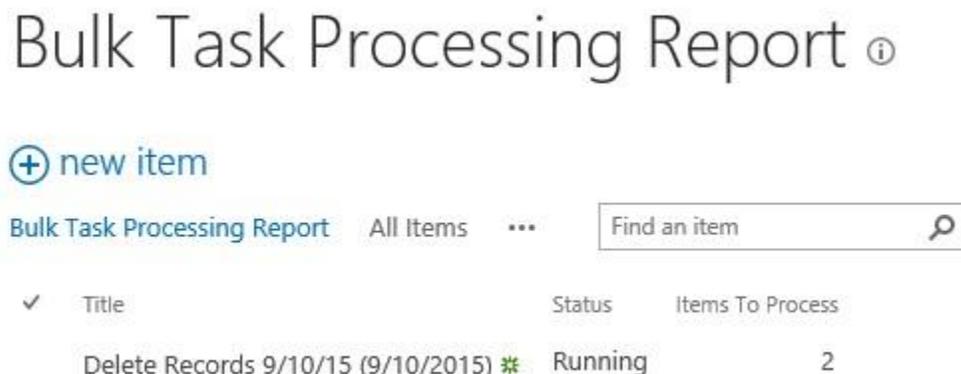
Figure 11-20 Bulk Task Processing Report Page and Status

10. Navigate to the Bulk Task Processing Reports page and select the report you created once it completes to observe that the disposition task was successful.

Bulk Task Processing Report - [Delete Records 9/10/15 (9/10/2015)]

Record / Container ▲	Site	Library	Container	Task Type	Workflow Name	Workflow Type	Reviewer	Review Status	Bulk Processing Status
☑	☑	☑	☑	☑	☑	☑			
Record 1.docx	Record Center	Bulk Test Library	Root Folder	Disposition Task	Compliance Suite Delete Record and Metadata	Compliance Suite Delete Record and Metadata			Successful
Record 2.aspx	Record Center	Bulk Test Library	Root Folder	Disposition Task	Compliance Suite Delete Record, Retain Metadata	Compliance Suite Delete Record, Retain Metadata			Successful

| ⏮ ◀ 1 ▶ ⏭   Page size: 10 ▼ | | 2 items in 1 pages |

Cancel

Figure 11-21 bulk Task Processing Report - Delete Records

11.4.2 Processing Transfer Tasks

Transfer tasks allow you to perform the following transfer tasks in bulk:

● Transfer Record - Transfer Task

● Transfer Record, Delete Record and Metadata

● Transfer Record, Delete Record, Retain Metadata

From the **Disposition Tasks** page, follow these steps to process transfer tasks in bulk:

1. Select **Bulk Task Processing** from the Compliance Suite header ribbon.

2. Navigate to the **Transfer Task** tab in **Bulk Task Processing**.

Figure 11-22 Transfer Task Tab

3. (**Required**) Enter a title to help you identify this batch of bulk task processing in the **Bulk Task Report Title** field.

4. Select transfer tasks enabled with the desired **Workflow Name**. You can select Compliance Suite Transfer Record, Transfer Record, Delete Record and Metadata, or Transfer Record, Delete Record, Retain Metadata.

5. Click the check box in the upper left of the items to select all items for processing or individually select them. The **Select all** check box selects all items across all pages for a specific tab and not just the visible items on the page.

   If you select multiple items on different pages, the selection is preserved when submitting items for bulk processing. For example, your page size is 10 and you have three pages. If you select one item on page 1 and then two items on page 3, all three items are processed.

Note:

If you select all items and there are more than 1000, a message displays asking if you want to select all tasks.

6. Click **Bulk Task Processing** at the bottom of the page.

Figure 11-23 Bulk Task Processing Button

The items are queued to be processed by the Bulk Task Processing Timer job. The following message displays.

GimmalSoft Compliance Suite - Bulk Task Processing Timer Job started Successfully

Click here to view the Bulk Task Processing List. It will show the status of Bulk Task Processing Report.

Figure 11-24 Successful Bulk Task Processing Timer Job Message

7. Navigate to the Bulk Task Processing Reports page and select the report once its status is complete. You can also go to **Site Contents > Bulk Task Processing Report** to view the status at any time.

8. Return to the Disposition Task List and observe that the confirmation task(s) now displays.

9. Select Bulk Task Processing from the Compliance Suite header ribbon.

10. Select the **Transfer Confirmation** task tab. The items that you previously processed for transfer now display in the list.

Figure 11-25 Transfer Confirmation Task Tab

11. Enter a descriptive name for the report in **Bulk Task Report Title**, select the **Date of Receipt** for the **Transfer**, and enter any **Comments**.

12. Click **Bulk Task Processing** at the bottom of the page.

13. Navigate to the Bulk Task Processing Reports page and select the report you created once it completes to observe that the transfer confirmation task was successful.

Figure 11-26 Bulk Task Process Report - Transfer

12 Email Management

Email Management functionality is available within a **SharePoint Records Center** with Compliance Suite enabled. To use Email Management features, Compliance Suite must be installed and the *Compliance Suite Email Management*, *Compliance Suite Email Management Service Application Installer*, and *Compliance Suite Email Management Service Application Installer* features must be active.

Email is the *de facto* standard for business communication and as such, email messages and attachments must adhere to your organization's records management policies. Compliance Suite Email Management enables users to upload and file email messages and attachments as records within your organization's file plan in a SharePoint Records Center. Users can file an email message with attachment(s) as a single record or opt to file the email message and attachment(s) separately as unique records.

Compliance Suite uses the following content types, libraries, and service application administration features for the implementation of Email Management:

1. Record Content Types

   - *Email Upload*: Content type used by Email Management to upload email messages into the **Email DropZone** library. Email Upload uses **Email Header Mappings** to automatically assign values to select site columns based on the email header information. **Email Header Mappings** is configured by the Compliance Suite Administrator.

   - *Email Record*: Content type used to file email messages in a SharePoint Records Center. Email Record does not use the **Email Header Mappings** to automatically assign values to select site columns based on the email header information. After an Email Upload item is filed into a Filing Location (Record Container) within a SharePoint Records Center, the Email Upload item content type should be changed to Email Record to enable records management capabilities.

   - See Compliance Suite Record Content Types help for more details.

2. Administration Configuration

   - *Email Header Mappings*: For **Email Upload** content types, maps the information contained in an uploaded email's header to an **Email Upload** site column. When a user uploads a new email into the **Email DropZone** library, the mapped site column values are automatically populated based on the email header definition. By default upon installation, **To**, **CC**, **BCC**, **Subject**, **DateSent**, and **DateReceived** are mapped.

   - *Manage Email Distribution Lists*: For **Email Upload** content types, defines the SharePoint users included in an email distribution list. If the email message contains an email distribution list in the **To**, **CC**, or **BCC** site columns, when a user uploads a new email into the **Email DropZone** library the corresponding **Expanded To**, **Expanded CC**, and **Expanded Bcc** fields will be updated to include all SharePoint users defined in the **Email Distribution List - Distribution List Members** configuration.

3. Email DropZone Document Library

- SharePoint Document Library used to upload email messages (with or without attachments) for filing into a SharePoint Records Center.

Email Management supports two methods for initiating the upload of email messages with or without attachments into the **Email DropZone** library:

1. User initiated upload of an email message (.msg) manually from the file system into the **Email DropZone** library.

2. Third party tool to upload an email from your email management system (e.g. Microsoft Outlook) directly into the **Email DropZone** library. **Intended User**: End User; Records Manager

12.1 Uploading and Filing an Email Message as a Record

Prior to filing an email message as a record in your file plan, the email message must be uploaded to a library by an end user either manually from the file system or directly from your email management system (e.g. Microsoft Outlook) through the use of a third party tool. Email DropZone is provided to distribute emails to additional lists.

12.1.1 Uploading an Email Message

To manually upload an email message (.msg) into the Email DropZone library:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.

2. Select the **Email Dropzone** library from the Quick Launch.

3. From the **Email Dropzone** library, there are two ways to initiate uploading a new email message.

- Select **New Item** at the top of the list.

- Click **Library** on the header ribbon; then select **Upload Document**.

4. Browse your local or network drive to select the saved email message (.msg) you want to upload. Click **OK**.

- The selected email message (.msg) is uploaded into the **Email Dropzone** library and checked out to the user.

5. An **Email Dropzone - Email Upload Edit Properties** dialog box opens with fields for updating the new Email Upload item.
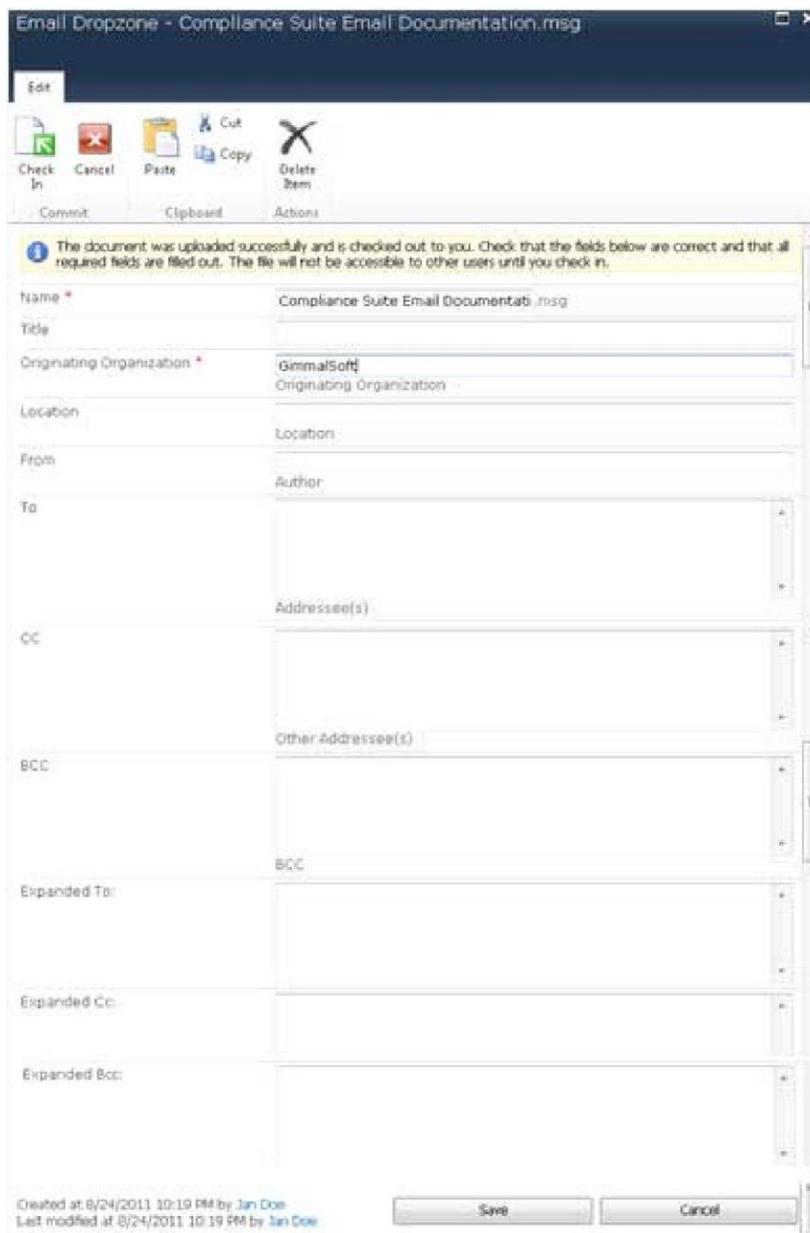
Figure 12-1 Email DropZone Message

6.   Enter values for all required fields. Optional fields can be assigned values as needed.

- (**Required**) **Name** is automatically entered based on the uploaded email message file name.

- (**Required**) Enter Originating Organization.

See Compliance Suite Record Content Types for more details on *Email Upload* fields (site columns).

7.   Click **Check In** or **Save** and the Email Upload item is updated and checked in.

8. Click **Cancel** to return to the **Email Dropzone** library without updating or checking in the Email Upload item.

9. After the new Email Upload item is saved and checked in:

    ●   The **Email Header Mappings** configurations are applied.

    ●   Any **Email Distribution Lists** assigned to the **To**, **CC**, and/or **BCC** fields are expanded to the assigned distribution list members (SharePoint users) in the corresponding **Expanded To**, **Expanded CC**, and **Expanded Bcc** fields.

    ●   The Email Upload item is now ready to be filed into a Filing Location (file plan).

12.1.2 Filing and Email Message as a Record

After the email message has been uploaded as an **Email Upload** content type to the Email Dropzone library by an end user either manually from the file system or through the use of a third party tool, the email message is ready to be filed into a Filing Location (file plan).

If the uploaded email message has attachments that you want to file separately, the attachments should be filed as individual records before you file the email message. See Filing an Email Attachment Separately help for more details.

To file the email message from the **Email Dropzone** library:

1. From the **Email Dropzone** library, select the Email Upload item you would like to file as a record. Only one Email Upload item can be selected at a time.

2. Select the **Move Record** link from the action menu for the Email Upload item.

3. The **Move Selected Record** dialog box is displayed.

Figure 12-2 Move Selected Record

- Select a **Filing Location** to file the email message

- Click **Submit** to file the email message to the selected filing location. The email message will be removed from the **Email Dropzone** library. The email message will be displayed in the selected Filing Location's corresponding Record Container.

- Click **Cancel** to close the dialog box and return to the **Email Dropzone** library without filing the email message.

4. If you selected **Submit** in step 3,

- Select the **Library** that corresponds to the selected **Filing Location** for the Email Upload item.

- Navigate to and select the Email Upload item you filed in Step 3. In SharePoint 2013, you must select the item and click the **Documents** tab.

- Select **Edit Properties** on the header ribbon or from the action menu for the Email Upload item. The **Record - Edit Properties** dialog box will open.

- (**Required**) Change the **Content Type** from *Email Upload* to *Email Record*. This is required to enable records management capabilities for the email message record.

- Click **Save** to save the **Content Type** change.

- Click **Cancel** to close the dialog box without saving the **Content Type** change. If you cancel without changing the **Content Type**, the email message record will not be enabled to work with all records management capabilities.

12.2 Filing an Email Attachment as a Record

If an uploaded email message contains one or more attachments, each attachment can be filed separately as an individual record.

To individually file an attachment contained within an email message from the **Email Dropzone** library:

1. From the **Email Dropzone** library, select the Email Upload item that contains one or more attachment(s) you would like to file as records. Only one Email Upload item can be selected at a time.

2. Select **File Attachment Separately...** link from the action menu for the Email Upload item.
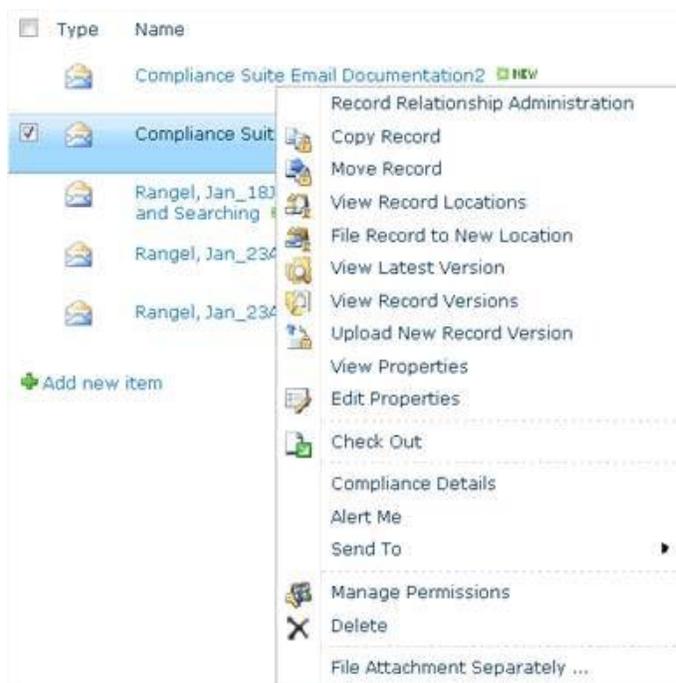
Figure 12-3 Record Relationship Administration Menu

The Filing Attachment Separately dialog box displays.
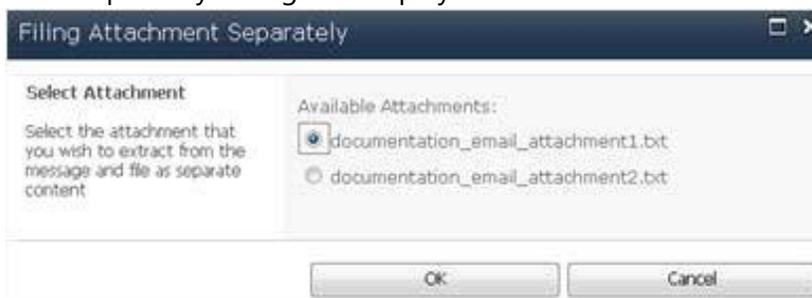
Figure 12-4 Filing Attachment Separately Dialog Box

- Select the **Available Attachments** you want to file as a record. The **Available Attachments** options are based on all attachments contained within the selected Email Upload content. Only one **Available Attachments** option can be selected.

- Click **OK** to continue filing the selected email attachment.

- Click **Cancel** to close the dialog box and return to the **Email Dropzone** library without filing the email attachment.

3. If you selected **Ok** in step 3,

- A Record Relationship with the Relationship Type of *Attachments* will be created between the Email Upload item (email message) and the new Record item (email attachment).

- The **Record - Edit Properties** dialog box will open. Enter the record metadata for the email attachment you are filing. See Working with Records help for more details on record metadata (site columns).

- Click **OK** to file the email attachment and close the **Record - Edit Properties** dialog box.

- Click **Cancel** to close the dialog box and return to the **Email Dropzone** library without filing the email attachment. The email attachment will be temporarily filed in the **Drop Off Library** for further editing and record declaration.

4. If you selected **Ok** in step 4,

    - The email attachment will be filed as a record into the selected **Filing Location**.

    - The email attachment will be removed as an attachment within the Email Upload item (email message).

5. Repeat Steps 2 - 5 for each email attachment you want to file separately.

13 Transfers

Transfers functionality is available within a **SharePoint Records Center** with Compliance Suite enabled. To use the Transfer features, Compliance Suite must be installed and the Compliance Suite Transfer Base feature must be active. In addition, by default you must be a member of the RMA Records Managers SharePoint group. However, the default group permission can be changed by your Compliance Suite Administrator to meet your organization's records management policies.

Transfers provide the functionality to import and export record content and metadata into and out of SharePoint Record Centers. Transferring out of your SharePoint Records Center enables the archiving of records to a Network File share, where they can then be sent for long-term storage based on your organization's records management policies. In addition, transferring into your SharePoint Records Center enables migration from legacy record repositories.

Transfers are used to support:

- *Disposition Stage/Actions*: A record's disposition processing can include a disposition action that executes a transfer workflow to exports records from a SharePoint Records Center. See Disposition Processing help documentation for further details.

- *User Initiated Export of Records*: A records manager can configure and execute a onetime export of records based on a Record Library, Record Container, and/or Record Item.

- *User Initiated Import of Records*: A records manager can configure and execute a onetime import of records.

- *History of Transfers*: A records manager can view past and upcoming scheduled transfers.

Compliance Suite uses the following pages and lists for the implementation of Transfers:

- **Schema Mappings**: Creating a new Schema Mapping that is used for Transfer Exports.

- **Schema Mapping Editor**: Updating and viewing of existing Schema Mappings.

- **Schema Mappings List**: Creating, updating, viewing, and deleting Schema Mappings. However, it is not recommended to use this list for creating or updating a Schema
  Mapping. The preferred method for creating a new Schema Mapping is the **Schema Mappings** page. The preferred method for updating an existing Schema Mapping is the **Schema Mapping Editor** page.

- **Configure Transfer Export**: Configuring a one-time only export of records from a SharePoint Records Center to a network file share.

- **Configure Transfer Import**: Configuring a one-time only import of records into a SharePoint Records Center from a network file share.

- **View and Delete Scheduled Transfers**: Displaying all scheduled transfer activities and their status. This view includes one-time transfer exports, one-time transfer imports, and transfer exports launched from a disposition processing task.

Before the Records Manager configuring and scheduling a transfer export or import, the Compliance Suite Administrator must configure a shared network file location. Please contact your Compliance Suite Administrator for details on your organization's network file location(s).

Intended User: Records Manager

13.1 Schema Mappings

Compliance Suite supports user defined Schema Mappings for transferring records from a SharePoint Records Center. Schema Mappings are the SharePoint items that define the site column
(metadata) configuration and .xml format when exporting records either to National Archives and Records Administration (NARA) or to another records management archival system based on your organization's records management policies or for an ad-hoc export of records. Schema Mappings use a combination of **Transfer Export Type** (Transfer for Export or Transfer to NARA) and **GimmalSoft Content Type** to define the metadata that will be exported.

Compliance Suite provides the ability to create, edit, view, or delete Schema Mappings.

Intended User: Records Manager

To access the Schema Mapping views:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.

2. To access the **Schema Mappings** list view:

   - Select **Libraries** from the Quick Launch to display a list of all Site Contents.

   - Select the **Schema Mappings** list. You see a list view of all Schema Mappings defined within your Site Collection.

3. There are two ways to access **Schema Mappings** view:

   - Select the **Schema Mappings** list from the **Site Contents** page.

   - Select **Settings** and then select **Site Settings**. Select **Schema Mappings** under the **Compliance Suite** section.

4. To access **Schema Mapping Editor** view, select **Settings** and then select **Site Settings**.

5. Select **Schema Mapping Editor** under the **Compliance Suite** section.

The default **Schema Mappings List** view displays a list of all Schema Mappings defined within your Site Collection. The following table describes the **Schema Mappings List** view with a description of each heading that is displayed when the view opens.

Table 13-1 Schema Mappings List

List View Heading	Description
Title	Descriptive name that differentiates the Schema Mapping from other Schema Mappings in the *Schema Mappings List*.

Table 13-1 Schema Mappings List

List View Heading	Description
Configuration Type	Defines the type of export for the Schema Mapping. On the *Schema Mappings* and *Schema Mapping Editor* pages the **Configuration Type** is labeled **Select Transfer Export Type**. The **Configuration Type** determines the *Required* metadata fields that will be included in the export for each *GimmalSoft Content Types* or any content type that inherits from the RMA Record. Any metadata field that is not *Required* is considered *Optional* and can be configured for inclusion in the export by the user. Values: Transfer for Export; Transfer to NARA

13.1.1 Schema Mapping Configuration Type and GimmalSoft Content Type Mapping

Compliance Suite Transfers is configured with a predefined mapping of **Configuration Type** also referred to as **Transfer Export Type** to **GimmalSoft Content Type Required** metadata fields. This predefined mapping defines the **GimmalSoft Content Type** site column (metadata) fields that will always be exported based on a Schema Mapping item's selected **Configuration Type/ Transfer Export Type**. The predefined mapping cannot be altered. The GimmalSoft Content Types include RMA Record and any content types that inherit from RMA Record.

The **GimmalSoft Content Type Optional** metadata fields included in each export are configured by a records manager based on your organization's records management policies. The **Optional** metadata fields are based on the available metadata fields that have not been defined as *required* for each GimmalSoft Content Type. All Organizational Defined Content Types that inherit from RMA Record will have their unique metadata listed as *Optional* metadata fields. In addition, all organizational defined fields added to standard GimmalSoft Content Types will be listed as **Optional** metadata fields. See 13.1.2 Creating a Schema Mapping for details on configuring **Optional** metadata fields.

The following table describes the predefined mapping of Configuration Type/Transfer Export Type options (*Transfer to Export* and *Transfer to NARA*) to **GimmalSoft Content Type Required** metadata fields.

Table 13-2 Configuration/Transfer Export Types

Content Type	Transfer to Export	Transfer to NARA

RMA Record	• Document ID; XML Element Name: @RecordIdentifier	• Document ID; XML Element Name: @RecordIdentifier
	• Subject; XML Element Name: @Title	• Subject; XML Element Name: @Title
	• Author; XML Element Name: @Creator	• Author; XML Element Name: @Creator
	• Media Type; XML Element Name: @Media	• Media Type; XML Element Name: @Media
	• Format Type; XML Element Name: @Format	• Format Type; XML Element Name: @Format
	• Publication Date; XML Element Name: @DatePublished	• Publication Date; XML Element Name: @DatePublished
	• Date Filed; XML Element Name: @DateFiled	
	• Originating Organization; XML Element Name: @OriginatingOrganization	
	• Supplemental Markings; XML Element Name: @SupplementalMarkingList	
Correspondence Record	No Required Fields	No Required Fields
Digital Photo Correspondence Record	No Required Fields	No Required Fields

Table 13-2 Configuration/Transfer Export Types

Content Type	Transfer to Export	Transfer to NARA
Digital Photo Record	• Document ID; XML Element Name: @RecordIdentifier	• Document ID; XML Element Name: @RecordIdentifier
	• Caption; XML Element Name: @Caption	• Caption; XML Element Name: @Caption
	• Photographer; XML Element Name: @Photographer	• Photographer; XML Element Name: @Photographer
	• Copyright; XML Element Name: @CopyRight	• Copyright; XML Element Name: @CopyRight
	• Bit Depth; XML Element Name: @BitDepth	• Bit Depth; XML Element Name: @BitDepth
	• Image Size; XML Element Name: @ImageSize	• Image Size; XML Element Name: @ImageSize
	• Image Source; XML Element Name: @ImageSource	• Image Source; XML Element Name: @ImageSource
	• Compression; XML Element Name: @Compression	• Compression; XML Element Name: @Compression
	• International Color Consortium/Image Color Management (ICC/ICM) Profile; XML Element Name: @ICCMProfile	• International Color Consortium/Image Color Management (ICC/ICM) Profile; XML Element Name: @ICCMProfile
	• Exchangeable Image File Formal (EXIF) Information; XML Element Name: @EXIFInformation	• Exchangeable Image File Formal (EXIF) Information; XML Element Name: @EXIFInformation

Content Type	Transfer to Export	Transfer to NARA

Table 13-2 Configuration/Transfer Export Types

Email Record	• Document ID; XML Element Name: @RecordIdentifier • From; XML Element Name: @Sender • To; XML Element Name: @PrimaryAddress • CC; XML Element Name: @SecondaryAddress • BCC; XML Element Name: @HiddenAddress • Subject; XML Element Name: @Subject • Date Sent; XML Element Name: @SentTimeStamp • Date Received; XML Element Name: @ReceivedTimeStamp	• Document ID; XML Element Name: @RecordIdentifier • From; XML Element Name: @Sender • To; XML Element Name: @PrimaryAddress • CC; XML Element Name: @SecondaryAddress • BCC; XML Element Name: @HiddenAddress • Subject; XML Element Name: @Subject • Date Sent; XML Element Name: @SentTimeStamp • Date Received; XML Element Name: @ReceivedTimeStamp
Email Upload	• Document ID; XML Element Name: @RecordIdentifier • From; XML Element Name: @Sender • To; XML Element Name: @PrimaryAddress • CC; XML Element Name: @SecondaryAddress • BCC; XML Element Name: @HiddenAddress • Subject; XML Element Name: @Subject • Date Sent; XML Element Name: @SentTimeStamp • Date Received; XML Element Name: @ReceivedTimeStamp	• Document ID; XML Element Name: @RecordIdentifier • From; XML Element Name: @Sender • To; XML Element Name: @PrimaryAddress • CC; XML Element Name: @SecondaryAddress • BCC; XML Element Name: @HiddenAddress • Subject; XML Element Name: @Subject • Date Sent; XML Element Name: @SentTimeStamp • Date Received; XML Element Name: @ReceivedTimeStamp

Table 13-2 Configuration/Transfer Export Types

Non-Electronic Correspondence DoD Record	No Required Fields	No Required Fields

Content Type	Transfer to Export	Transfer to NARA
Non-Electronic DoD Record	No Required Fields	No Required Fields
PDF Correspondence Record	No Required Fields	No Required Fields
PDF Record	• Document ID; XML Element Name: @RecordIdentifier • Producing Application; XML Element Name: @ProducingApplication • Producing Application Version; XML Element Name: @ProducingApplicationVersion • PDF Version; XML Element Name: @PDFVersion • Creating Application; XML Element Name: @CreatingApplication • Document Security Settings; XML Element Name: @DocumentSecuritySetting	• Document ID; XML Element Name: @RecordIdentifier • Producing Application; XML Element Name: @ProducingApplication • Producing Application Version; XML Element Name: @ProducingApplicationVersion • PDF Version; XML Element Name: @PDFVersion • Creating Application; XML Element Name: @CreatingApplication • Document Security Settings; XML Element Name: @DocumentSecuritySetting
Scanned Correspondence Record	No Required Fields	No Required Fields

Table 13-2 Configuration/Transfer Export Types

Scanned Record	• Document ID; XML Element Name: @RecordIdentifier • Scanned Image Format and Version; XML Element Name: @ScannedImageFormatAndVersion • Image Bit Depth; XML Element Name: @ImageBitDepth • Image Resolution; XML Element Name: @ImageResolution	• Document ID; XML Element Name: @RecordIdentifier • Scanned Image Format and Version; XML Element Name: @ScannedImageFormatAndVersion • Image Bit Depth; XML Element Name: @ImageBitDepth • Image Resolution; XML Element Name: @ImageResolution
Web Correspondence Record	No Required Fields	No Required Fields
Content Type	**Transfer to Export**	**Transfer to NARA**
Web Record	• Document ID; XML Element Name: @RecordIdentifier • Web File Name; XML Element Name: @FileName • Web Platform; XML Element Name: @WebPlatform • Web Site Name; XML Element Name: @WebSiteName • Web Site Uniform Resource Locator (URL); XML Element Name: @WebSiteURL • Capture Method; Element Name: @CaptureMethod • Capture Date; XML Element Name: @CaptureDate • Content Management System; XML Element Name: @ContentManagementSystem • Contact; XML Element Name: @Contact	• Document ID; XML Element Name: @RecordIdentifier • Web File Name; XML Element Name: @FileName • Web Platform; XML Element Name: @WebPlatform • Web Site Name; XML Element Name: @WebSiteName • Web Site Uniform Resource Locator (URL); XML Element Name: @WebSiteURL • Capture Method; Element Name: @CaptureMethod • Capture Date; XML Element Name: @CaptureDate • Content Management System; XML Element Name: @ContentManagementSystem • Contact; XML Element Name: @Contact

Table 13-2 Configuration/Transfer Export Types

13.1.2 Creating a Schema Mapping

Before records can be exported using the Transfers feature, a Schema Mapping must be created. The Schema Mapping is required for the **Configure Transfer Export** page and to configure any of the Transfer workflows launched during Disposition Processing.

1. Open the **Schema Mappings** page. The dialog box opens with fields for creating a new Schema Mapping.

Figure 13-1 Schema Mappings Page

2. (**Required**) Enter the **Title**. The **Title** is a descriptive identifier for the new Schema Mapping. The **Title** is displayed on the **Schema Mappings List** and in the **Schema Mapping** menu on the **Schema Mapping Editor** page as well as in the **Select Schema Mappings File** menu on the **Configure Transfer Export** page.

3. (**Required**) Select the Select Transfer Export Type.

   - This field defines the type of export for this Schema Mapping

   - The available options are *Transfer for Export* and *Transfer to NARA*. The default selected option is *Transfer for Export*.

   - The selected option determines the **Required** metadata fields that will be included in the export. Any metadata field that is not listed as **Required** will be displayed as an **Optional** metadata field that can be configured for inclusion in the export for each GimmalSoft Content Type or any content type that inherits from RMA Record.

   - The selected option in combination with the **Select Gimmal Content Type** field defines the *Required* and *Optional* metadata displayed on the page. Refer to 13.1.1 Schema Mapping Configuration Type and GimmalSoft Content Type Mapping for more details.

4. (**Required**) Select the Select Gimmal Content Type.

   - This field is a menu-based content types within your Site Collection that inherit from RMA Record content type. The default selected option is *RMA Record*.

   - In combination with the selected **Select Transfer Export Type**, this field updates the *Required* and *Optional* metadata displayed on the page.

Figure 13-2 Gimmal Content Type

5. View the **Required** metadata fields. The **Required** metadata fields will be automatically included in any export based on this Schema Mapping. The displayed **Required** metadata fields for each **Select Gimmal Content Type** option are based on the selected **Select Transfer Export Type** and cannot be changed. Refer to the Schema Mapping Configuration Type and GimmalSoft Content Type Mapping help documentation for more details.

6. Select the **Optional** metadata fields to include in any export based on this Schema Mapping. The displayed **Optional** metadata fields for each selected **Select Gimmal Content Type** option are the available metadata fields that are not listed as **Required**. To select any of the **Optional** metadata fields:

   ● (**Required**) Select the **Include** check box to the right of the **Optional** metadata field name.

   ● (**Required**) Enter the **Element Name** in the text box to the right of the Include check box. The E**lement Name** will be the name displayed for this metadata field in any export based on this Schema Mapping. The **Element Name** must begin with an underscore (_) or a letter in the alphabet. After the first character, all others must be an underscore (_) or any alphanumeric character.

7. Repeat Steps 4 - 6 for each **Select Gimmal Content Type** option you are configuring for this Schema Mapping.

   ● You can select one or more content types for each Schema Mapping. However, only one content type will be displayed on the page at a time. To select more than one content type, select the first content type and set all desired **Optional** metadata fields as defined above then select each additional content types individually and set the desired **Optional** metadata fields as applicable.

8. Click **Create** to create the new Schema Mapping. It is displayed on the **Schema Mappings List** and in the **Schema Mapping** menu on the **Schema Mapping Editor** page. The **Schema Mappings** page closes and the **Records Center Home Page** is displayed.

9. Click **Cancel** to return to the **Records Center Home Page** without creating a new Schema Mapping.

10. After the new Schema Mapping is created,

   ● The new Schema Mapping is displayed as a selection in the **Select Schema Mappings File** menu on the **Configure Transfer Export** dialog box.

   ● The new Schema Mapping will be available for use by configuration of any Transfers workflow used in Disposition Processing. For more details on Transfers through Disposition Processing see the Disposition Processing help documentation.

13.1.3 Editing a Schema Mapping

To change an existing Schema Mapping, you must update the Schema Mapping item.

1. Open the **Schema Mapping Editor** page and select the **Schema Mapping** you want to edit. Only one Schema Mapping can be selected at a time. The dialog box updates displaying the selected **Schema Mapping** details.

Figure 13-3 Editing a Schema Mapping Dialog Box

2. Update the information in the fields you want to change.

    ●   (**Required**) **Title**.

    ●   **Select Transfer Export Type** updates will change the required metadata that will be exported when this updated Schema Mapping is used for any transfer export hence forth. See 13.1.2 Creating a Schema Mapping and 13.1.1 Schema Mapping Configuration Type and GimmalSoft Content Type Mapping for more details.

    ●   **Select Gimmal Content Type** *Optional* metadata updates will be applied to any transfer export that uses this Schema Mapping hence forth. See 13.1.2 Creating a Schema Mapping and 13.1.1 Schema Mapping Configuration Type and GimmalSoft Content Type Mapping for more details.

3. Click **Save** to update the Schema Mapping. The changes are displayed in the **Schema Mappings List** and in the **Schema Mapping** menu on the **Schema Mapping Editor** page. The **Schema Mapping Editor** page closes and the **Records Center** home page is displayed.

4. Click **Cancel** to return to the **Records Center Home Page** without updating the selected Schema Mapping.

5. After the Schema Mapping change is saved, the following are implemented:

    ●   The updated Schema Mapping is displayed as a selection in the **Select Schema Mappings File** menu on the **Configure Transfer Export** dialog box.

    ●   The updated Schema Mapping is available for use by any Transfers workflows used in Disposition Processing. For more details on Transfers through Disposition Processing see 10 Disposition Processing.

13.1.4 Viewing a Schema Mapping

To view the details of an existing Schema Mapping, you must view the Schema Mapping item.

1. Click the **All Site Content** link at the bottom of the Quick Launch list.

2. Click the **Schema Mappings** link in the Lists section of the All Site Content display.

3. From the **Schema Mappings View**, select the Schema Mapping you want to view. Only one Schema Mapping can be selected at a time. Select the Schema Mapping and click the **Items** tab.
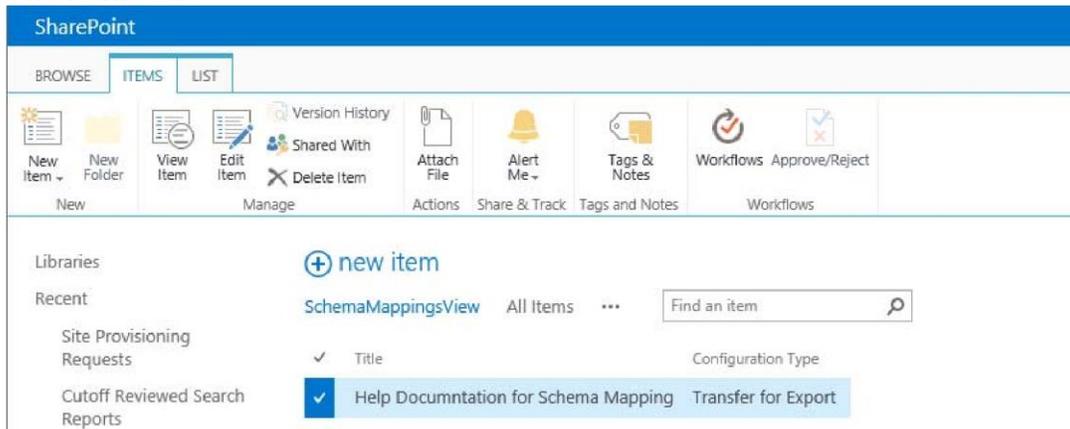
Figure 13-4 Items Tab header ribbon

4. Select **View Item** button on the header ribbon. The **Schema Mappings View** dialog box opens displaying the Schema Mapping details in read-only mode.
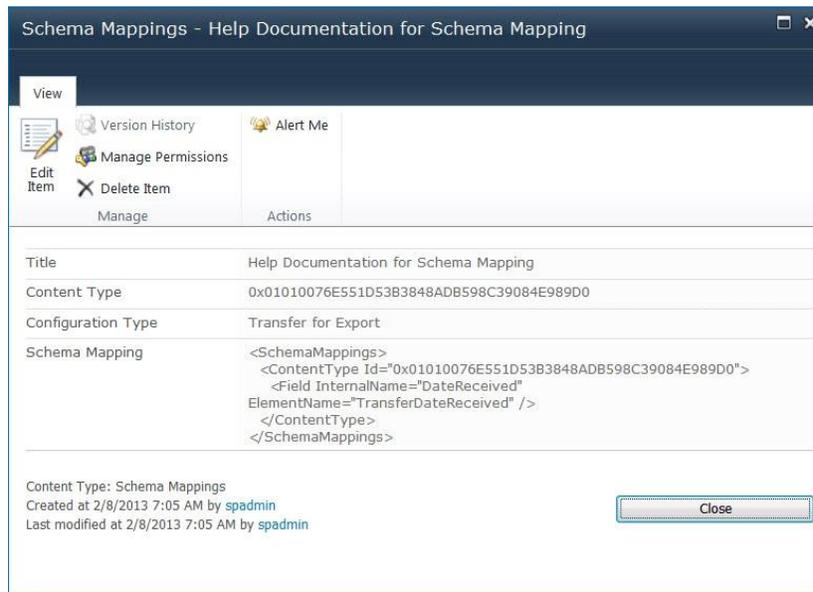
Figure 13-5 Schema Mappings View Dialog Box

5. From the **Schema Mappings View** dialog box, you can delete the selected Schema Mapping. To edit the selected Schema Mapping, refer to 13.1.3 Editing a Schema Mapping on page 200 .

6. Click **Close** to return to the **Schema Mappings List**.

13.1.5 Deleting a Schema Mapping

To remove an existing Schema Mapping from your site, you must delete the Schema Mapping item.

1. From the **Schema Mappings View**, select the Schema Mapping(s) that you want to delete. When a Schema Mapping is selected the **List Tools → Items** header ribbon opens.

2. Click the **Items** tab.
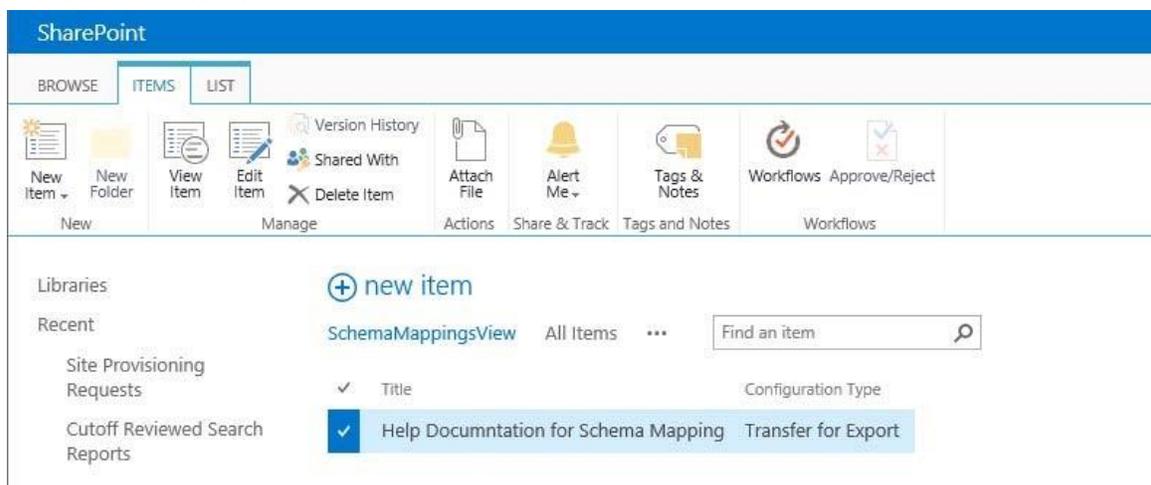
Figure 13-6 Items Tab Header Ribbon

3. Select **Delete Item** button on the header ribbon. A prompt opens asking *Are you sure you want to send the item(s) to the site Recycle Bin?*

4. Click **OK** and the Schema Mapping(s) is deleted and removed from the **Schema Mappings List** and the **Schema Mapping** menu on the **Schema Mapping Editor** page. The dialog box closes and the **Schema Mappings List** is displayed.

5. Click **Cancel** to return to the **Schema Mappings List** without deleting the selected Schema Mapping(s).

6. After the Schema Mapping is deleted, the deleted Schema Mapping(s) no longer appears as a selection in the **Select Schema Mappings File** menu on the **Configure Transfer Export** dialog box.

Caution!

If the deleted Schema Mapping is currently used by one or more Transfers workflows used in Disposition Processing, the Transfers workflow will no longer work. Please delete with caution.

13.2 Exporting Records and Metadata

Compliance Suite supports the exporting of records and their metadata from your SharePoint Records Center to a network file location. Using the Transfers functionality, there are two ways to initiate exporting records and metadata:

1. *Configure Transfer Export*: A records manager can configure and execute a one-time only export of records based on a Record Library, Record Container, and/or Record Item.

2. *Disposition Workflow*: A record's disposition processing can include a disposition action that executes a transfer's workflow to exports records from your SharePoint Records Center. See 10 Disposition Processing for further details.

Before exporting records and metadata through Transfers, a Schema Mapping(s) must be created. In addition, a network file location for storing exported records and metadata must be configured by your Compliance Suite Administrator.

Intended User: Records Manager

13.2.1 Exporting Records through Configure Transfer Export

One-time exporting of records and metadata from your SharePoint Records Center is supported through the **Configure Transfer Export** page. Configure Transfer Export provides the ability to configure a one-time only export of records and metadata from your SharePoint Records Center.

To access Configure Transfer Export:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.

2. Click **Settings** and then **Site Settings** from the header navigation. On **Site Settings**, select **Configure Transfer Export** under the **Compliance Suite** section. The dialog box opens with fields for configuring a one-time only Transfer Export.

Figure 13-7 Configure Transfer Export

3. (**Required**) Enter the **Title**. The **Title** is a descriptive identifier for the Transfer Export configuration. The **Title** displays on the **View** and **Delete Scheduled Transfers** list.

4. (**Required**) Select the **Select Transfer Export Type**. The **Select Transfer Export Type** is used to limit the list of **Select Schema Mappings File** options to only Schema Mappings that match the selected **Select Transfer Export Type**. The available options are *Transfer for Export* and *Transfer to NARA*. The default selected option is *Transfer for Export*.

---

5. (**Required**) Select the **Select Schema Mappings File**. The **Select Schema Mappings File** defines the Schema Mapping item to use for this export. The selection options are based on existing Schema Mapping items that have a **Configuration Type** equal to the **Select Transfer Export Type** selected previously.

6. (**Required**) Enter the **Select Destination Network Path**. The **Select Destination Network Path** is the network file location where the records and their metadata will be exported. The **Select Destination Network Path** details should be provided by your Compliance Suite Administrator.

7. Select the **Select records by Library**, **Category**, or **Record Individually** to be included in this export. To select a Library, Category (Record Container), or Record within your Site Collection:

   - Click **Browse** to open the SharePoint Asset Selector.

   - Using the SharePoint Asset Selector, select the Library, Category (Record Container), or Record that you would like to include. Your selection displays in the **Location (URL)** field at the bottom of the Asset Selector.

   - Click **OK** to save the selection and close the Asset Selector, or click **Cancel** to close the Asset Selector without saving the selection.

8. Click **Add selected record(s) under selected site/library/category** to add the records selected in Step 7 to the transfer export configuration.

   - If a Library or Category (Record Container) was selected, all records contained within the Library or Category (Record Container) will be added.

   - The added record(s) will be listed above the Select records by Site, Library, Category, or Record Individually field.

9. Once the selected record(s) have been added, the following properties display:

   - Table of all selected records displays Document ID, Name, Subject, Date Filed, Publication Date, Created By, and Originating Organization.

   - Check box to the left of the Document ID to include or exclude the record from the export. By default all selected records are checked.

   - Clicking the **Clear all records** button to the bottom right of the table removes all records selected for export.

10. Click **Create** and the new Transfer Export Configuration is created and displayed on the **View and Delete Scheduled Transfers List**. The **Configure Transfer Export** page closes and the **Records Center Home Page** is displayed.

11. Click **Cancel** to return to the **Records Center** home page without creating a new Transfer Export Configuration.

After the new Transfer Export Configuration is created, and when the GimmalSoft Compliance Suite Transfer Timer Job is executed, the new Transfer Export Configuration will be processed and all affected records and their metadata will be exported to the selected network file location.

13.2.2 Exporting Records through Disposition Processing

Records and their metadata can be exported from your SharePoint Records Center as a part of Disposition Processing. Disposition Actions can be configured to execute a Transfers workflow to export the files based on your organization's records management policies.

Refer to chapter 10 Disposition Processing for more details.

13.2.3 Exported Record and Metadata Network File Structure

When an export is executed through either the Configure Transfer Export page or Disposition Processing, the applicable records and their metadata are exported to the assigned network file location. The following folder structure and files will be created as a part of the export:

- *Files*: Folder where all of the records that are included in the transfer will be exported. The record file name will be the unique **ID** of the record that is exported.

- *metadata.xml*: The .xml file that contains the metadata and network file path for all records included in the transfer export.

To access exported records and metadata:

1. Browse to the **Destination Network Path** as defined in your transfer export configuration or workflow.

2. View the metadata.xml file.

3. Browse to the **Files** folder within the **Destination Network Path** as defined in your transfer export configuration or workflow. The **Files** folder contains the record content included in the export. Each record's file system name is defined as a *ComputerFile* element within the metadata.xml file.

13.3 Importing Records and Metadata

Importing records and metadata is supported through the **Configure Transfer Import** page. This page provides the ability to configure a one-time only import of records and metadata into your SharePoint Records Center.

Before importing records and metadata through Configure Transfer Import, a valid metadata.xml file along with record content must exist in an accessible network file location. The network file location for accessing records and metadata for import should be configured by your Compliance Suite Administrator.

Note

When records are exported from your SharePoint Records Center using a Schema Mapping with a **Configuration Type** of *Transfer for Export*, the system generated *metadata.xml* file can be used to import the records back into a SharePoint Records Center. However, if the records were exported using a Schema Mapping with a **Configuration Type** of *Transfer for*

NARA; the system generated files cannot be used to import the records back into a SharePoint Records Center.

Intended User: Records Manager

To import records using **Configure Transfer Import**:

1. Open a **SharePoint Records Center**. The **Records Center** home page opens.
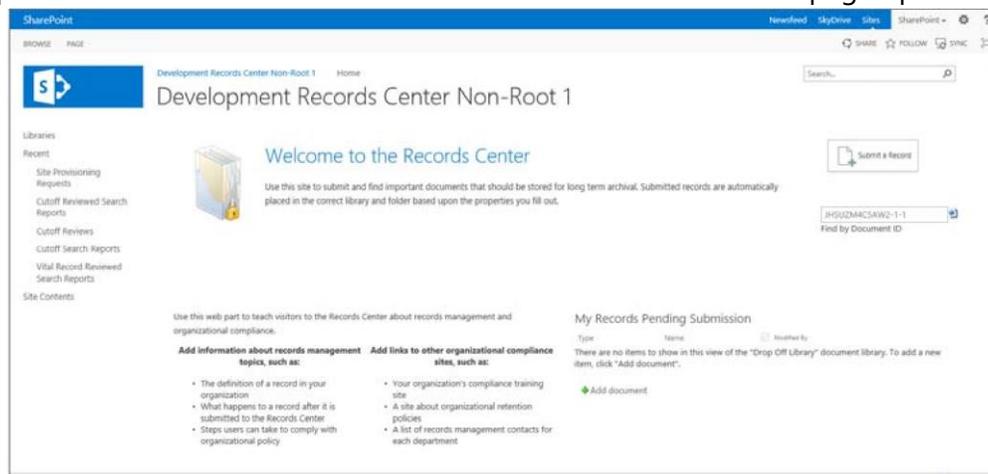
Figure 13-8 Records Center Home Page

2. To access **Configure Transfer Import**, click **Settings** and then select **Site Settings** from the header navigation. On **Site Settings**, select **Configure Transfer Import** under the **Compliance Suite** section. The dialog box opens.

Figure 13-9 Configure Transfer Import

3. (**Required**) Enter the **Title**. The **Title** is a descriptive identifier for the Transfer Import configuration. The **Title** displays on the **View and Delete Scheduled Transfers** list.

4. (**Required**) Select the **Select a Gimmal Compliance Suite Transfer metadata.xml file**. This is the network file location of the *metadata.xml* used to import records into your SharePoint Records Center. The **Select a Gimmal Compliance Suite Transfer metadata.xml file** network location should be provided by your Compliance Suite Administrator.

5. Click **Next** and the dialog box opens with fields for mapping each *Record Folder* defined in the *metadata.xml* to **Folders (Record Containers)** within your SharePoint Records Center. This mapping defines the **Record Container** where the records will be imported in your SharePoint Records Center.
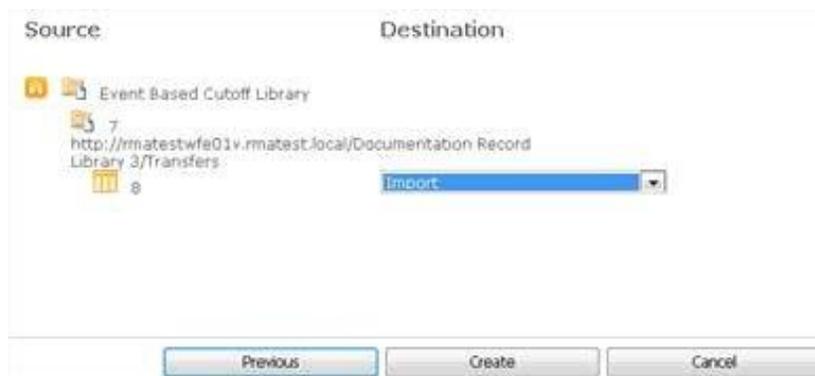
Figure 13-10 Mapping Record Folders

6. Select a Folder from the menu displayed to the right of each Record Folder. The Folder options include all Record Containers that are contained within the Category (Record Container).

7. Repeat for each Record Folder displayed on the Step 5 - Folder Mapping page.

8. Click **Create.** The new Transfer Import Configuration is created and displayed on the View and Delete Scheduled Transfers list. The **Configure Transfer Import** page closes and the **Records Center** home page displays.

Note

At any point in the previous steps, you can click **Cancel** to return to the **Records Center Home Page** without creating a new Transfer Import Configuration.

At any point in the previous steps, click **Previous** to return to the previous dialog box.

---

9. After the new Transfer Import Configuration is created, when the GimmalSoft Compliance Suite Transfer Timer Job is executed, the new Transfer Import Configuration will be processed and all affected records and their metadata will be imported to the selected Record Container(s).

13.4 Viewing and Deleting Scheduled Transfers

The viewing and auditing of transfer activities is supported through the View and Delete Scheduled Transfers list. This list provides the ability to view all scheduled transfer activities along with their status. When a Transfer activity is initiated either one-time or through a disposition processing transfers workflow, a transfer task is added to the **View and Delete Scheduled Transfers** list. From this **View and Delete Scheduled Transfers** list, a user can:

- Delete a transfer task
- View **Parameters** of a transfer task
- View **Status** of a transfer task

- View the **Results**
- View **Result Exceptions** of a transfer task

Intended User: Records Manager

To access the **View and Delete Scheduled Transfers** list:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.

2. Click **Settings** and then select **Site Settings** from the header navigation. On **Site Settings**, select **View and Delete Scheduled Transfers** under the **Compliance Suite** section.

3. The screen opens with a list of all transfer tasks scheduled within your Site Collection. This includes one-time transfers and those initiated through disposition processing. Clicking the **Reset** button resets the pending transfer to a pending state.
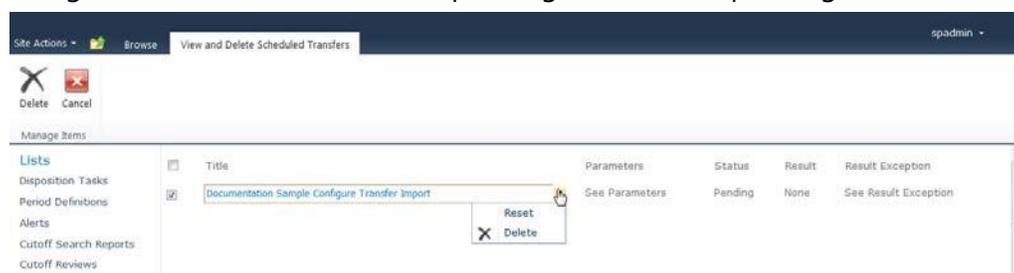
Figure 13-11 Reset Pending Transfer

4. The **View and Delete Scheduled Transfers** list displays the following information for each transfer task:

- **Title**: Title of the transfer task as set in the **Title** field on the **Configure Transfer Export** or **Configure Transfer Import** page. If the transfer task is initiated from a disposition processing working, the **Title** will be *Export Configuration created by [name of workflow]*.

- **Parameters**: Link that opens a dialog box with configuration parameters for the transfer task. These parameters are saved and displayed in an .xml structure.

- **Status**: Status of the transfer task. Valid options are *Pending*, *Running*, or *Completed*. The status of the transfer task is dependent on the execution of the GimmalSoft Compliance Suite Transfer Timer Job.

- **Result**: Results for the transfer task after the execution of the GimmalSoft Compliance Suite Transfer Timer Job. Valid options are *None*, *Fail*, or *Success*. If the **Result** is set to *None* then the GimmalSoft Compliance Suite Transfer Timer Job has not been run.

- **Result Exception**: Link that opens a dialog box with the results, including any exceptions, for the transfer task after the execution of the GimmalSoft Compliance Suite Transfer Timer Job. If the GimmalSoft Compliance Suite Transfer Timer Job has not run, the link still displays but contains no information.

5. To view the transfer task parameters, click **See Parameters** link for the transfer task item. A dialog box opens displaying the transfer task parameters.

Figure 13-12 Transfer Task Parameters

6. If a transfer task fails, to view the transfer task result exception, click the **See Result Exception** link for the transfer task item. A dialog box displays the transfer task result exceptions.

7. To remove a transfer task, click on the transfer task item **Title** and select **Delete** from the action menu for the transfer task. Clicking **Reset** to reset the configured transfer to a pending state.

Figure 13-13 Reset a Transfer

- A prompt opens asking *Are you sure you want to delete item(s)?*

- Click **OK** and the transfer task is deleted and removed from **View and Delete Scheduled Transfers**.

- Click **Cancel** to return to the **View and Delete Scheduled Transfers** list without deleting the selected transfer task.

14 Alerts

Alerts is a SharePoint e-mail notification service that informs users when documents in libraries or items in a list have been created, modified, or deleted.

Alerts functionality is available within a **SharePoint Records Center** with Compliance Suite enabled. To use the Alerts features, **Compliance Suite** must be installed and the *Alerts* feature must be active.

Compliance Suite Alerts functionality offers notification capability that can be configured to meet specific and very granular requirements. Alerts functionality is available to **SharePoint Records Center** libraries and lists and is very useful when managing Records Centers. Alerts can be triggered when a record is inserted, updated, or deleted and meets a specific qualification.

Records become candidates for an alert if one or more of its properties, *Site Columns*, that provide metadata about the record, are selected in the **Alerts Qualification** field.

Intended User: Records Manager, Compliance Suite Administrator, Power User

Defining and implementing an alert are two distinct processes. A **Compliance Suite** administrator, records manager, or local records officer can define the qualifications and criteria that will trigger the alert. Implementing an alert requires a power user familiar with CAML queries and PowerShell scripts.

Alerts provide a scripting capability to allow only authorized individuals to attach process actions to any or all metadata fields or to restrict record access based on the content of fields. The process actions can vary from a simple CAML query to a complex PowerShell script. In addition to its name and description, an alert is made up of the following components:

- Alert Qualification
- Alert Criteria
- Alert Recipient
- Email Notification
- Alert Script Command

Alerts can be created, viewed, updated, and deleted using a SharePoint list. To view a list of all Alerts:

1. Open a **SharePoint Records Center**. The **Records Center Home** Page opens.
2. Select **Libraries** in the Quick Launch section to display your Site Contents. Select **Alerts** to display a list view of all Alerts defined within your Site Collection. The following table describes the Alerts View list with a description of each heading.

Table 14-1 Alerts View

List View Heading	Description
Title	Unique name that differentiates the Alert from other Alerts.
Alert Description	Descriptive statement used to further differentiate the Alert from other Alerts.
Alert Type	The Alert Type. The options are Insert, Update, and Delete.
Alert Qualifications	List of alert qualifications.
Alert Criteria	Alert criteria (either a CAML query or a script command) that Advanced Users can manually enter.
Email Recipients	Names of email recipients of the Alert.

14.1 Creating an Alert

Before an alert can be sent to a user, an Alert must be created.

1. From the Alerts View screen, there are two ways to instantiate the alert creation process.

    ●   Select **New Item** at the top of the list.

    ●   Select the **Items** tab. In the header ribbon, Select **New Item** and then **Alerts**.
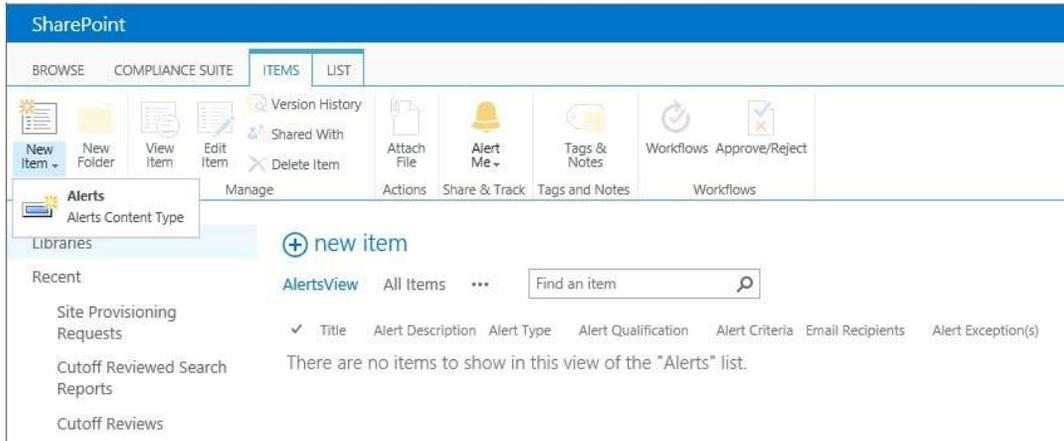

Figure 14-1 New Alert Item

An **Alerts - New Item** dialog box displays with fields for creating a new Alert.
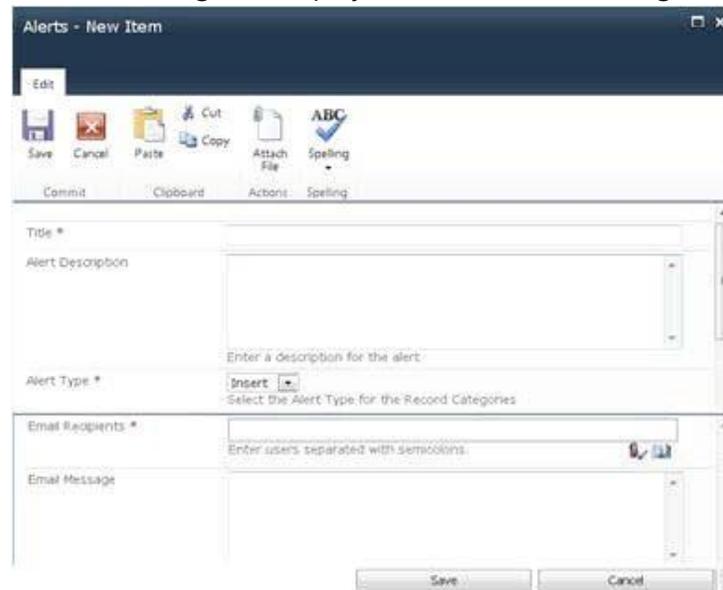

Figure 14-2 Creating a New Alert

2. (**Required**) Enter the **Title**. The **Title** is a unique identifier for the new Alert.

3. Enter an **Alert Description**. The **Alert Description** should be a descriptive statement that defines the purpose of this Alert.

4. (**Required**) Select the **Alert Type** for the Record Categories. The options are:

    - *Insert*: The alert is evaluated when a record is added to the record repository.

    - *Update:* The alert is evaluated when a `record`'s metadata is updated.

    - *Delete:* The alert is evaluated when a record is deleted.

5. (**Required**) Select the **Alert Qualification(s)**. Select the appropriate site column(s) for the Alert in the menu. The selected site column(s) must exist in the Record in order for the Alert to be executed. For the Update Alert Type, the selected site column(s) value(s) must be modified as well.

6. Enter Alert criteria in either the CAML Query or Script **Alert Criteria** fields. Entering alert criteria is optional and is only recommended for users who possess advanced programming capabilities.
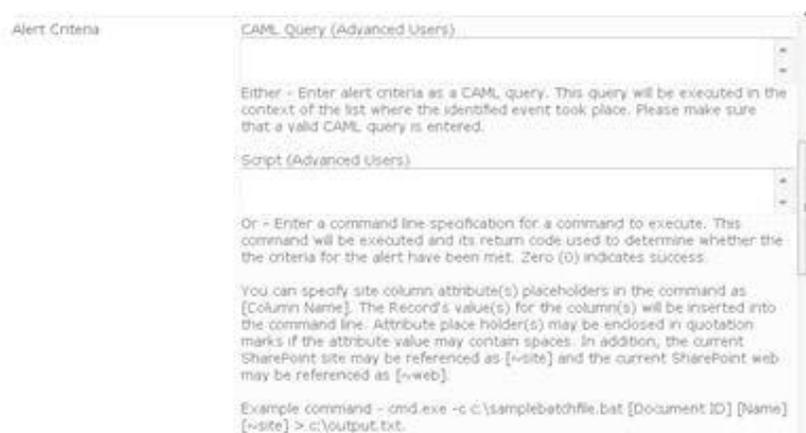
Figure 14-3 Alert Criteria

For a CAML query:

- A query is executed in the context of the list where the identified event took place.

- The CAML query must be valid and return at least one value so that the alert can be executed.

- Processed `item's` metadata values can be substituted within a CAML query by wrapping the property name with brackets (`'['`, `']'`). For example, to use the name value, [Name] would be included where the actual value is expected.

- The following is an example of a CAML query that would trigger a notification when the value of the subject is set to `'update'`:

```
<Where><And><Eq><FieldRef Name='_dlc_DocId' /><Value
Type='Text'>[Document ID
Value]</Value></Eq><Contains><FieldRef
Name='DoDRecordSubject' /><Value
Type='Text'>update</Value></Contains></And></Where>
```

For a Script query:

- A Command line specification must be entered for a command to execute. An example command to execute SendUpdateEmail.ps1 script located in c:_AlertsTest folder that passes a documentID and a subject value would be as follows:
  powershell.exe   -noprofile   C:_AlertsTest\SendUpdateEmail.ps1 "'[Document ID Value]'" "'[DoDRecordSubject]'"

- The following is an example of a script file called SendUpdateEmail.ps1 that is located in c:_AlertsTest used to trigger a notification when the value of the subject is set to 'update'.

The content of the script is as follows:

```
#
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
#
# Parameters:
# [0]: record document id
#; [1]: DoD Subject Field Value
#
#
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++


#[string] $execOn = Get-Date
[string] $location = Get-Location
[string] $outputOld = "$location\SendUpdateEmail.ps1.out.txt"
[string] $output = "C:\_AlertsTest\SendUpdateEmail.ps1.out.txt"
[int] $returnValue = 0


# ensure that the arguments are as we expect if
($args.Length -eq 2)
{
[string] $recordDocumentId = $args[0]
[string] $dodSubjectValue = $args[1]


# write out parameters
Out-File -encoding ASCII -force $output -append -input ""
Out-File -encoding ASCII -force $output -append -input "--------------------
-parameters-------------------------------------------"
```

```
Out-File    -encoding    ASCII    -force    $output    -append    -input
"executed:.............$execOn"

Out-File -encoding ASCII -force $output -append -input "record document
id:...$recordDocumentId"

Out-File  -encoding  ASCII  -force  $output  -append  -input  "dod  subject
value:....$dodSubjectValue


if ($returnValue -eq 0)

{

Out-File -encoding ASCII -force $output -append -input "-→ does the subject
value    that    is    passed    for    the    item    equal    'update'"    if
($dodSubjectValue.ToLower().Equals ("update"))

{

Out-File -encoding ASCII -force $output -append -input "-→ subject value is
equal 'update'"

$relationshipRetVal = 0

}

else

{

Out-File -encoding ASCII -force $output -append -input "-→ subject value is
NOT equal 'update'"

$relationshipRetVal = 1

}

$returnValue = $returnValue + $relationshipRetVal

}


Out-File  -encoding  ASCII  -force  $output  -append  -input  "-→  return value =
$returnValue"

Out-File -encoding ASCII -force $output -append -input ""

# return the return value

exit $returnValue }


#catch    all    return

exit 1

#
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

- This command will be executed and its return code used to determine whether the criteria for the Alert have been met.

- Processed `item's` metadata values can be passed as parameters to the script by wrapping the property name with brackets (`'[',  ']'`). For example, to use the name value, `"'[Name]'"` would be included where the actual value is expected.

- Zero (0) indicates success.

7. (**Required**) Enter names of email recipients of the Alert in the **Email Recipients** field.

8. In the **Email Message** field, enter a message that will be sent to the selected email recipients when the message is received.

9. In the **Alert Script Command** field, enter the command for executing the Alert script. The script file must exist on the SharePoint server.

10. Click **Save** to create the new alert. It is displayed in the Alerts View list. Click **Cancel** to return to the **Alerts View** list without creating a new Alert.

14.2 Editing an Alert

To change an existing Alert, you must edit the Alert item.

1. From the **Alerts View** screen, select the Alert you want to edit. Only one Alert can be selected at a time.
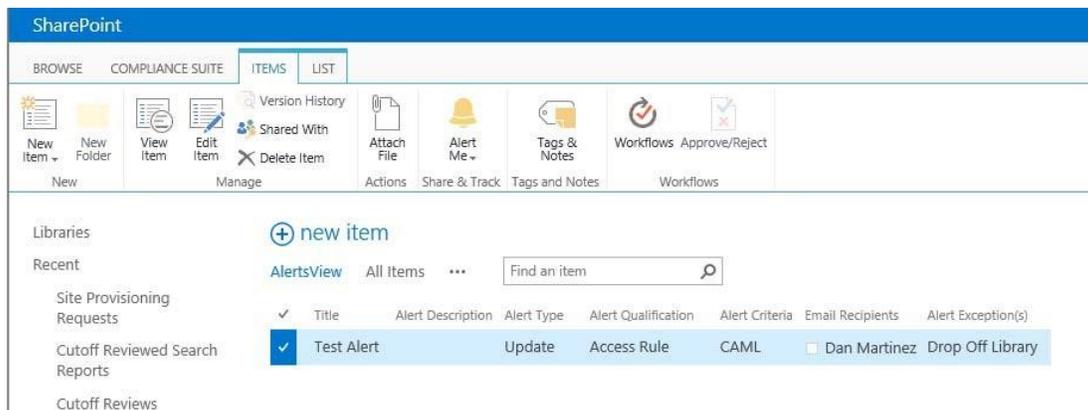
2. Click the **Items** tab.

Figure 14-4 Edit Alert Item

3. Select **Edit Item** button on the header ribbon. The **Alerts Edit** dialog box opens, displaying the selected Alerts details.
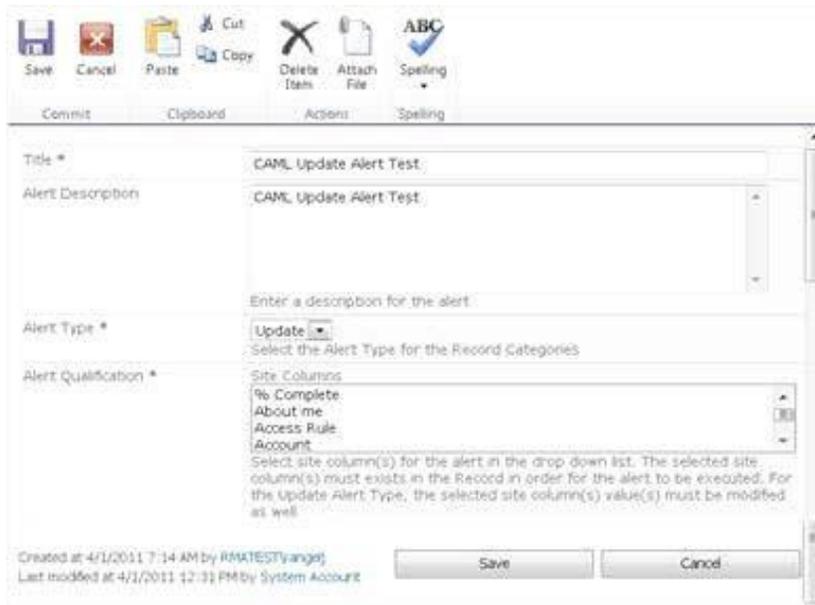
Figure 14-5 Alerts Dialog Box

4. Update the information in the fields you want to change.

5. Click **Save** to update the Alert. The changes are displayed in the **Alerts View** list. Click **Cancel** to return to the **Alerts View** list without updating the selected Alert.

14.3 Viewing an Alert

To view the details of an existing Alert, you must view the Alert item.

1. From the **Alerts View** screen, select the Alert you want to view. Only one Alert can be selected at a time.

2. Click the **Items** tab to open the header ribbon.

3. Select the **View Item** button on the header ribbon. The **Alerts View** dialog box opens displaying the Alert details in read-only mode.
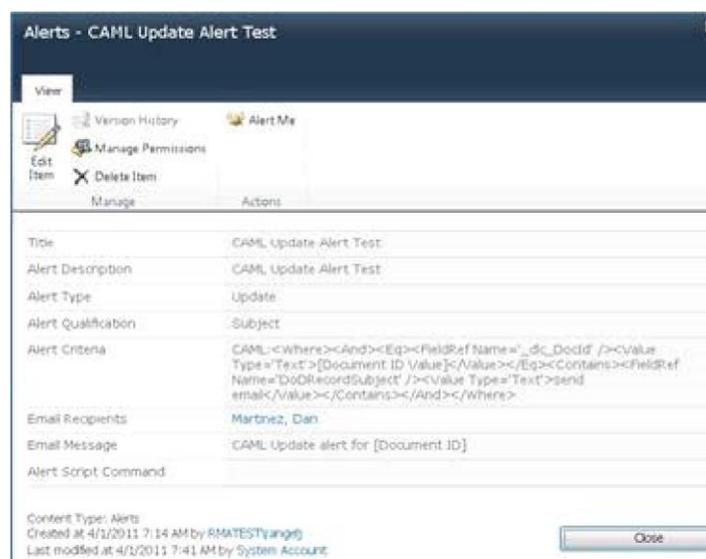
Figure 14-6 View Alert

4. From the **Alerts View**, you can edit, delete, or manage permissions of the selected Alert.

5. Click **Close** to return to the **Alerts View List**.

14.4 Deleting an Alert

To remove an existing Alert from your site, you must delete the Alert item.

1. From the **Alerts View** screen, select the Alert(s) you want to delete.

2. Click the Items tab to open the header ribbon.

3. Click the **Delete** Item on the header ribbon. A prompt opens asking *Are you sure you want to send the item(s) to the site Recycle Bin?*

4. Click **OK** and the Alert(s) is deleted and removed from the **Alerts View** list or click **Cancel** to return to the **Alerts View** list without deleting the selected Alert(s).

15 Reports

Reports functionality is available within a **SharePoint Records Center** with Compliance Suite enabled. To use the Reports features, Compliance Suite must be installed and the Gimmal Compliance Suite As of Reports and User Permissions Reports features must be active. Reports include:

15.1 User Permission Reports

Compliance Suite supports user defined reporting on User Permission settings across your SharePoint Site Collection. User Permission is the authorization given to users that enables them to perform specific functions on specific items within your Site Collection. User Permission

Reports can be performed against any type of item that is contained within a SharePoint List or Library in your Site Collection. This includes the following Compliance Suite items:

- Record Libraries, Containers, and Items
- Access Rules
- Events
- Period Definitions
- Record Relationships and Relationship Types
- Vital Record Reports and Reviews

Note

Only documents with unique permissions display in the tree view.

The User Permission Report allows you to easily view the user permission settings across your Site Collection(s) in two ways:

- By site: In a site, you can view a report on user permission settings for an individual SharePoint Library contained in the selected site.
- By event

Intended User: Records Manager

To access the User Permission Reports:

1. Open a **SharePoint Records Center**. The **Records Center** home page opens.
2. Select **Settings** and then **Site Settings** from the header navigation. On **Site Settings**, select **User permission reports** under the **Compliance Suite** section.

   The **User Permission Reports** screen opens with options for running the User Permission Report. The following table describes the default **User Permission Reports** view.

Table 15-1 User Permission Reports

Feature/Title	Description

Sites Tab	Configuration options for running the User Permission Report based on SharePoint Sites. Start from: allows the user to select *This Site* or *Site Collection* as the basis for the report. Levels: allows the user to select *Single Site*, *Site Collection*, or *Entire Site Structure* as the basis for the report. If you select *Entire Site Structure* the Start from: options become disabled. *Site Item(s) List*: The list of site items will be refreshed based on the Start from: and Levels: options selected. A user can select a specific site item to appear in the report by checking the item in the list. **Note:** If a site item has the icon on it, then the item is not inheriting permissions, resulting in the possibility of unique permission settings.
Events Tab	Configuration options for running the User Permission Report based on Compliance Suite Events. Search text box allows you to filter the Event List. The search filter will find all events containing the search string anywhere within the Event Name. For example, *XYZ* would return *Contract Expiration for XYZ* and *XYZ Project Complete*. *Event List* will dynamically update based on the search filter. By default, the **Event List** will display all Events in your Site Collection. A user can select a specific event to appear in the report by checking the event item in the list.
Select a User	SharePoint User that is base for the user permission report. The report supports only one user at a time. Example: DOMAIN\JaneSmyth
View Permissions	Action button that runs the report based on the configuration options selected.

Table 15-1 User Permission Reports (Continued)

Feature/Title	Description

Export Current Report	Action button that exports the report to a comma delimited (.csv) file.
	The **Export Current Report** button is deactivated until a report is run and the report results are displayed.
Change Report Settings	Action button that opens a window to configure the display of Record Containers on screen and in the export file.
	The default configuration setting is to **Not Show Containers**.
Report Detail Table	Report results are displayed in a table structure on screen.
	The report results vary based on report type and are discussed in detail in the following sections.

15.1.1 View User Permissions by Sites

The User Permission Report can be generated on either *All* or *Selected SharePoint Site(s)*. You can also further refine the report by selecting specific items in a SharePoint site.

To run the User Permission Report by a site(s):

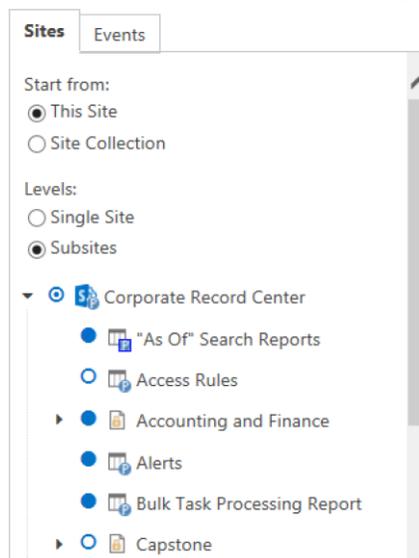1. Select the **Sites** tab on the **User Permission Report** page.

Figure 15-1 Sites Tab

The **Sites** tab is divided into two sections. The top section displays site selection options. The bottom section displays items contained within the selected site(s).

2. Select **Start from**.

- **This Site**: Display only the current Site

- **(Default) Site Collection**: Display all Sites within the current Site Collection
3. Select **Levels** option.
    - **Single Site**: Display only the selected Site(s). Subsites do not display.
    - **Subsites**: Display the primary Site(s) and Subsites. **(Default)**
    - **Entire Site Structure**: Display the entire site structure. If you select this option, the Start from: options become disabled.
4. Select the check boxes for all **Site Items** to include in the User Permission Report.

Note:

If a site item has the icon on it, the item is not inheriting permissions. Unique permission settings are possible in this situation.
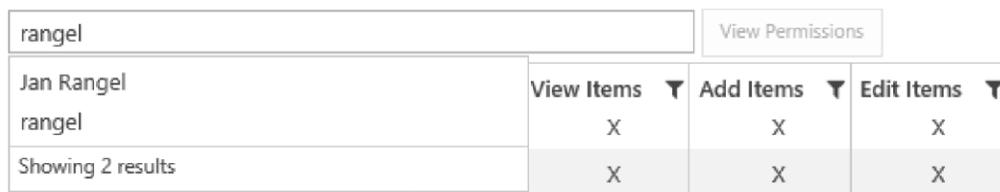
5. Start entering a user's account name, user name, or email address in **Enter names or email addresses** at the top of the User Permission Reports area.

Figure 15-2 Selecting a User

The names matching the letters you have entered display.

Figure 15-3 Searching Users Results Example

6. Select the name that you want.
7. Click **View Permissions** to run the User Permission Report based on the selected criteria.
    - The report process can take a few minutes depending on the number of items included in the criteria.
    - While the report is processing the following message displays: *Analyzing site permissions. Please wait.*
    - The report results display in a table under the **Select a User** options. The table headings are described in Table 15-2.
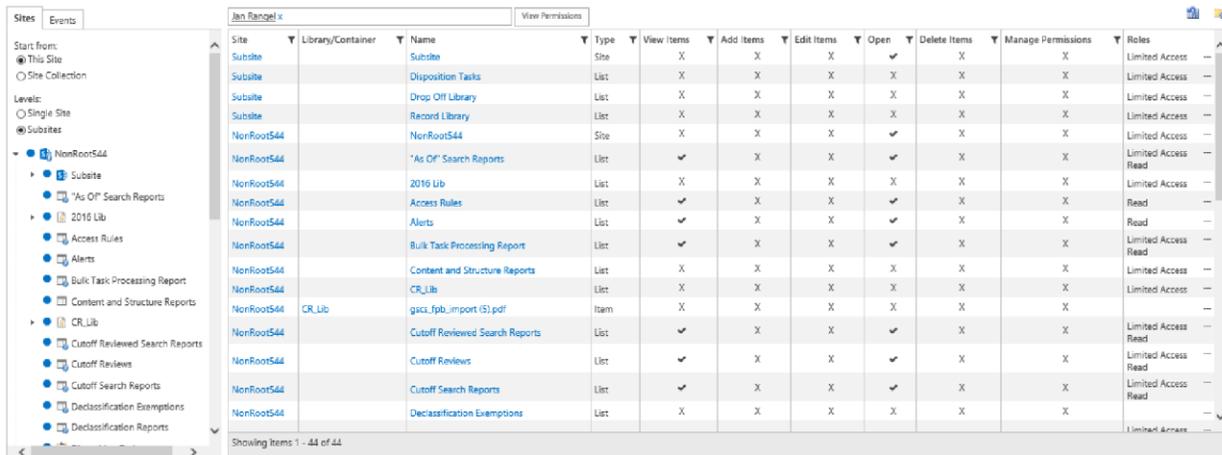
Figure 15-4 View User Permissions by Sites

Table 15-2 View Users Permissions by Sites

Report Heading	Description
Icon	Iconography depicting the content type for the line item. **Note:** If an item has the icon on it, the item is not inheriting permissions. Unique permission settings could be present and display in the line item Roles column.
Site	SharePoint Site Name that contains the line item. This column is useful if the report contains information from multiple sites.
Container	Parent Record Container for the line item.
Title	The Title of the line item. This is the Title field from the item.
Type	Type of the line item. The values for Type include site, list, item, or folder.
View Items	A check mark indicates the user has permission to view the line item or items within the line item type. If a dash symbol displays, it is Not Applicable for the line item.

Table 15-2 View Users Permissions by Sites

Report Heading	Description
Add Items	A check mark indicates the user has permission to create items within the line item type. This is only applicable to lists, folders, and containers. An X indicates that it is Not Applicable for the line item.
Edit Items	A check mark indicates the user has permission to edit the line item or items within the line item type. An X indicates that it is Not Applicable for the line item.
Open	A check mark indicates the user has permission to open the line item or items within the line item type. An X indicates that it is Not Applicable for the line item.
Delete Items	A check mark indicates the user has permission to delete the line item or items within the line item type. An X indicates that it is Not Applicable for the line item.
Manage Permissions	A check mark indicates the user has permission to manage permissions for the line item or items within the line item type. An X indicates that it is Not Applicable for the line item.
Roles	Specific permissions settings assigned to the user for the line item. Placing focus on a Role for a line item cell opens a window that displays the exact permission inheritance for the user.

The View User Permissions by Sites report results table uses the standard filter and sort capabilities.

15.1.2 View User Permissions by Events

The User Permission Report allows the report to be run based on All or Selected Compliance Suite Event(s).

To run the User Permission Report by Event(s):

1. Select the **Events** tab on the **User Permission Report** page.

2. The **Events** tab is divided into two sections. The top section displays a search field. The bottom section displays events contained within your Site Collection.
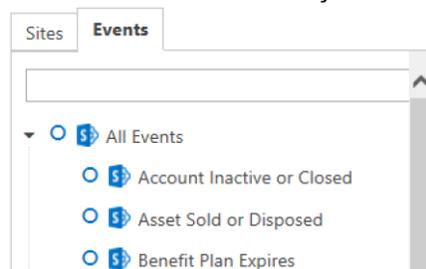
Figure 15-5 Events Tab

3. Enter an event name or a partial event name in the **Search** text box.

   ● The **Event Items** list dynamically updates based on the search filter.

   ● The search filter finds all events containing the search string anywhere within the **Event Name**.

4. Select the options for all **Event Items** to include in the User Permission Report.

5. Start entering a user's account name, user name, or email address in **Enter names or email addresses** at the top of the User Permission Reports area.

Figure 15-6 Selecting a User

The names matching the letters you have entered display.

Figure 15-7 Searching Users Results Example

6. Select the name that you want.

7. Click **View Permissions** to run the User Permission Report based on the selected criteria.

   ● The report process can take a few minutes depending on the number of items included in the criteria.

   ● While the report is processing, the following message displays: *Analyzing events. Please wait.*

   ● The report results display in a table under the **Select a User** options. The table headings are described in Table 15-3.

Figure 15-8 View User Permissions by Events

Table 15-3 View Users Permissions by Events

Report Heading	Description
Icon	Iconography depicting the content type for the line item. For the report by event(s), all icons are the event content type icon.
Event	The Event Name.
Read Event	A check mark indicates the user has permission to read the event. An X indicates that the user does not have permission to read the event.
Update Event	A mark indicates the user has permission to edit the event. An X indicates the user does not have permission to edit the event.
Delete Event	A check mark indicates the user has permission to delete the event. An X indicates the user does not have permission to delete the event.
Trigger Event	A check mark indicates the user has permission to create event instances based on this event. An X indicates the user does not have permission to create event instances based on this event.
Manage Permissions	A check mark indicates the user has permission to manage permissions for the event. An X indicates the user does not have permission to manage permissions for the event.

The View User Permissions By Events report results table uses the standard filter and sort capabilities.

15.1.3 User Permission Report Settings

The User Permission Report supports configuration of the report display and export settings based on Record Container permissions. The report settings are only applicable to the User Permission Report by Sites.

To configure the User Permission Report settings:

1. Click the **Change Report Settings** button. The button displays as a folder icon to the right of the **Export Current Report** button.

    A **Change Report Settings** dialog box opens with options for configuring the display of Record Containers within the onscreen report results table and export file.

Figure 15-9 Change Report Settings

2. Select **Show Containers** option. By default, it is unchecked. If **Show Containers** is checked, the following options are enabled:

   - **all**: Displays all Record Containers regardless of permission

   - **(Default) with unique permissions**: Displays only Record Containers that have nondefault permission

3. To close the report settings, click the **X** in the upper right hand corner of the dialog box. All changes are automatically applied to the report results table and subsequent exported reports.

Note

Report settings revert to default options when the User Permission Report is closed.

15.1.4 Exporting User Permission Report

The User Permission Report allows exporting the report results to a comma delimited (.csv) file.

To export the User Permission Report:

1. After the report results display, click the **Export Current Report** button. The button displays as a table icon to the right of the **View Permissions** button. A **Save As** dialog box opens with options for saving the export file.

2. Browse your local or network machine to select a location and enter a **File name** to save the report results.

3. Click **Save** to save the exported report to your local or network machine. Click **Cancel** to return to the User Permission Reports without exporting the report results.

15.2 "As Of" Reporting

"As Of" Reporting functionality is available within a **SharePoint Records Center** with Compliance Suite enabled and the *Gimmal RMA "As Of" Reporting* feature, which must be active.

Compliance Suite "As Of" Reporting supports user-defined reporting on records pending disposition actions (tasks) across your SharePoint Site Collection(s). "As Of" Reporting is a planning tool for records managers, allowing them to gain insight into upcoming disposition

actions for records across your organization. The Gimmal Compliance Suite - Disposition Metadata Timer Job must be run before running "As Of" Reporting, to set the disposition stage dates for all records that have a calculated expiration date.

"As Of" reporting is performed against any records or case-based record containers within a Record, Document, Email Library, or List in your Site Collection(s) that is not hidden and contains an Action Date. You can select a single or multiple Sites within your Site Collection(s). In a Site, you can report on pending disposition actions for an individual SharePoint Library contained in the selected Site.

Intended User: Records Manager

To access "As Of" Reporting:

1. Open a SharePoint Records Center.

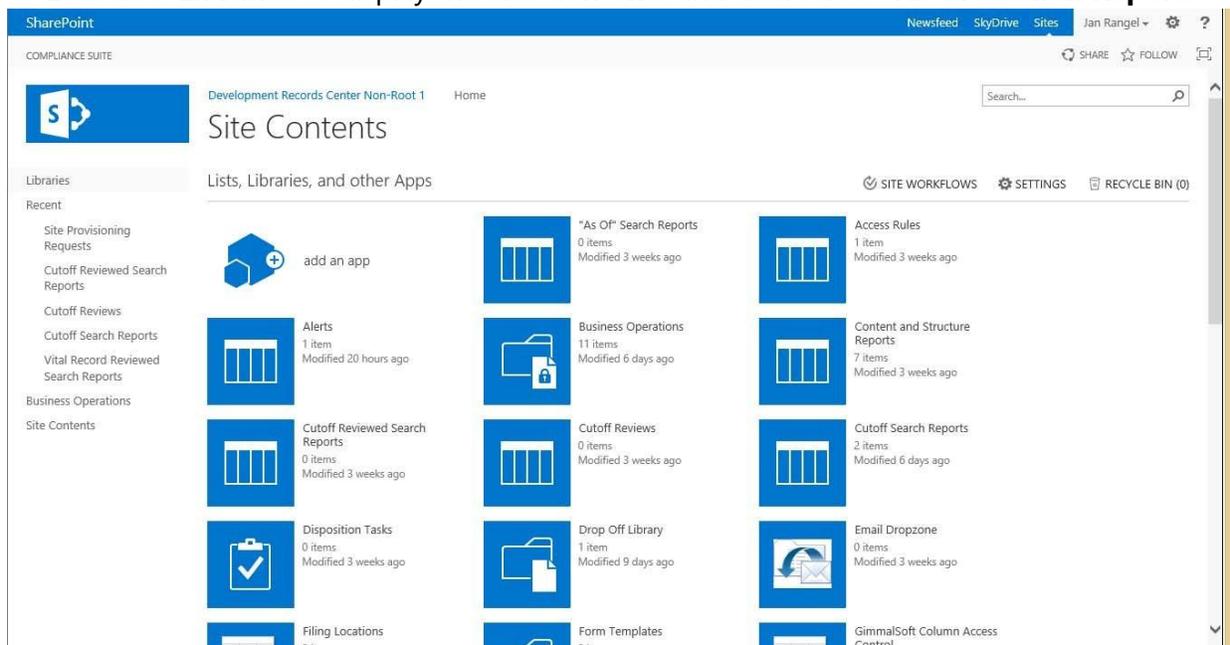2. Select **Libraries** to display the **Site Contents** and then select **"As Of" Search Reports**.

Figure 15-10 Selecting "As Of" Search Reports

The *"As Of" Reports* dialog box opens with options for running "As Of" Reporting.

3. Click **New Item** at the top of the list. The "As Of" Reporting page displays.

Figure 15-11 New "As Of" Report

The following table describes the default "*As Of*" *Reports* page.

Table 15-4 "As Of" Reports Page

Report Heading	Description
"As Of" Report Title	A unique (friendly) name for the title of the report.
Disposition Action	Disposition Action (SharePoint Policy Action) that is the base for the report. The report supports only one selected disposition action at a time. You can search on Any Action to show all actions in the report. Example: Permanently Delete

Table 15-4 "As Of" Reports Page

Report Heading	Description
Effective Date	Disposition Action (Task) effective date for records and record containers that is the base for the report. The report supports two options for selecting an effective date: In the next: Allows the user to select upcoming time frame as the basis for the report. The user can enter the number of days, months or years from today's date to include in the report. The default is *30 day(s)*. Between: Allows the user to select a start and end date as the basis for the report. The user can select the Start Date and End Date from the standard calendar.
Sites	Configuration options for running the "As Of" Report based on SharePoint Sites. Start from: Allows the user to select *This Site* or *Site Collection* as the basis for the report. Levels: Allows the user to select *Single Site*, *Site Collection*, or *Entire Site Structure* as the basis for the report. If you select *Entire Site Structure* the Start from: options become disabled. *Library List*: The list of site document, email, or record libraries will be refreshed based on the Start from: and Levels: options selected. Any site library or list that can contain records or record containers with disposition actions will be displayed. A user can select a specific site library to appear in the report by checking the item in the list.
Custom Fields	This option enables you to add up to three custom fields to your "As Of" Report. These fields display as column headings in your final report, once your report renders.

15.2.1 Viewing "As Of" Reporting by Sites

To run the "As Of" Report:

1. Select **Libraries** to display the **Site Contents** and then select "**As Of" Search Reports**.
2. Select **New Item** at the top of the list. The "As Of" Reporting dialog box displays.

Figure 15-12 "As Of" Reporting Dialog Box

3. Enter a unique name for the report title.

4. Select an **Action** from the menu, such as *Any Action* or *Permanently Delete*.
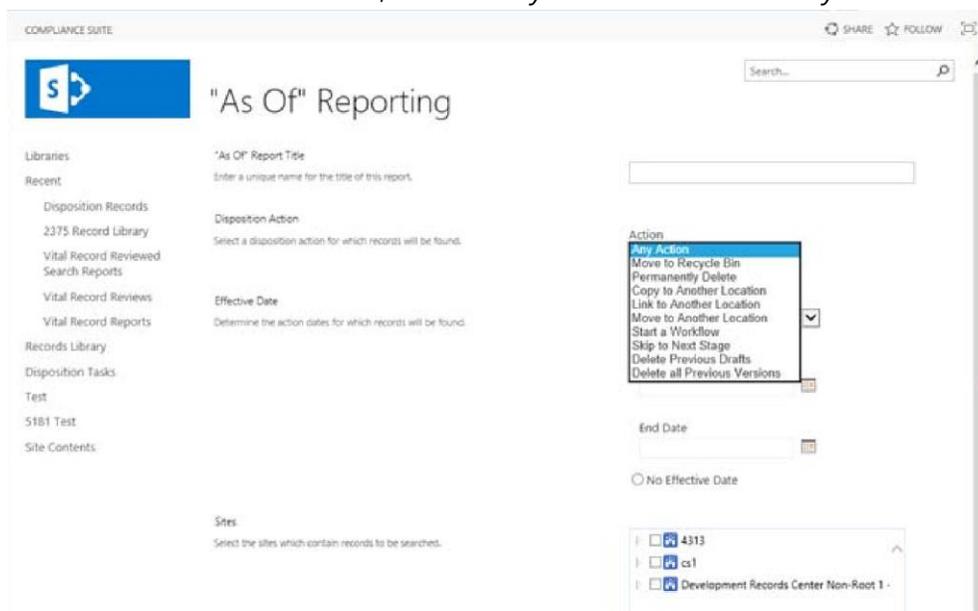

Figure 15-13 Selecting an Action

5. Specify either a time period or a date range in **Effective Date**.

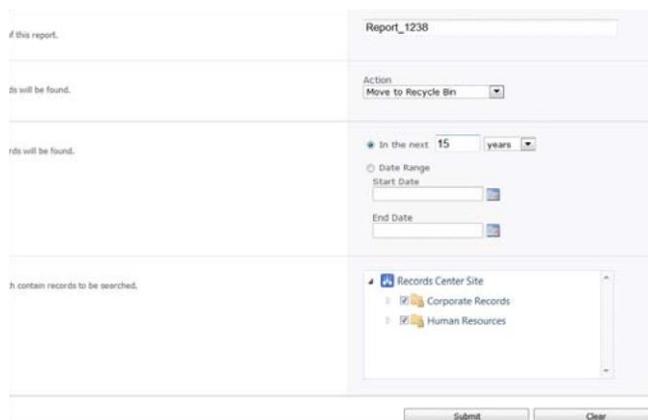6. Select the containers to search in **Libraries / Containers**.

Figure 15-14 New "As Of" Report

7. After clicking **Submit**, a message displays in the center pane. Click **"As Of" Search Reports** to view the report.

Note

A Timer job runs to complete the report; otherwise, the status is pending. To see when status has changed from *Pending* to *Complete*, refresh the window.

8. When the job completes, the status in the Search Reports changes from *Pending* to *Complete*.

Figure 15-15 Search Reports Status

9. To view the "As Of" Search Report, click the report title you assigned.

Figure 15-16 Viewing the As Of Search Report

15.2.2 Exporting As Of Report Results

As Of Reporting supports the exporting of the report results to Excel.

To export the As Of Report results:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.
2. Select Libraries to display the Site Contents and then "As Of" Search Reports.
3. When the Library reports display, click the title of the report you want to inspect.

Figure 15-17 "As Of" Search Results

4. From the "As Of" Search Report, click **Export**.
5. Click **Open** to view the information in Microsoft Excel.

Figure 15-18 Opening an "As Of" Report in Excel

6. Click **Save** and select **Save As** to save the information to a Microsoft Excel comma-separated values (.csv) file.

15.3 Report Exclusion Settings

Using Report Exclusions Settings, you can create a rule that excludes sites and libraries from reports. For example, you can set exclusions for Vital Record lists, Cutoff lists, Period lists, Drop Off library, Email DropZone, and "As Of" Reporting, or add any site and library to exclude them. Once set, Compliance Suite ignores those records according to the pattern that you set so that they are not contained in reports (for example, Email DropZone).

Follow these steps to set report exclusions:

1. Under the Compliance Suite area of SharePoint, select **Report Exclusions Settings**.

Figure 15-19 Selecting Report Exclusions Settings

The Report Exclusions Settings screen displays.
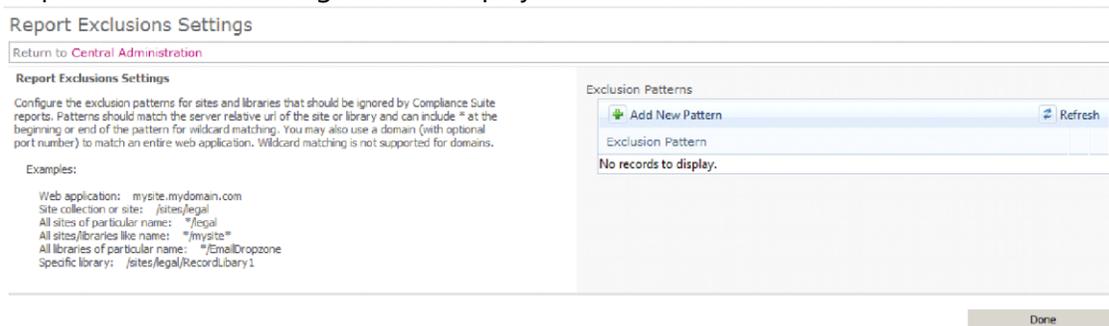

Figure 15-20 Report Exclusions Settings

2. Select **Add New Pattern**. The **Exclusion Pattern** field displays.
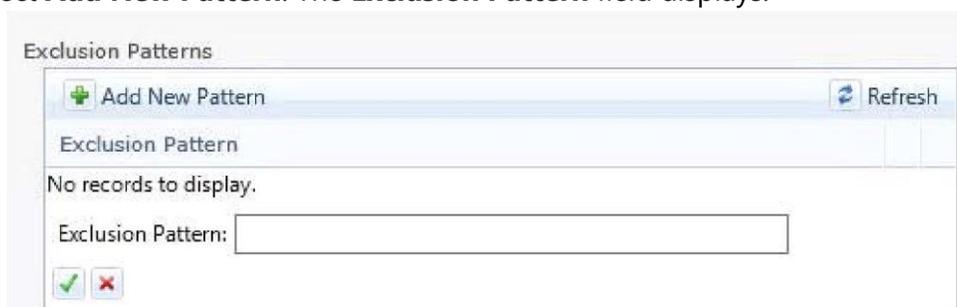

Figure 15-21 Exclusion Patterns Field

3. Enter the exclusion pattern for the records you do not want included in reports and click the **Go** button. The new exclusion pattern displays.

Figure 15-22 New Exclusion Pattern

4. If you want to edit the pattern, click the **Edit** button. The Exclusion Pattern field displays where you can enter changes.
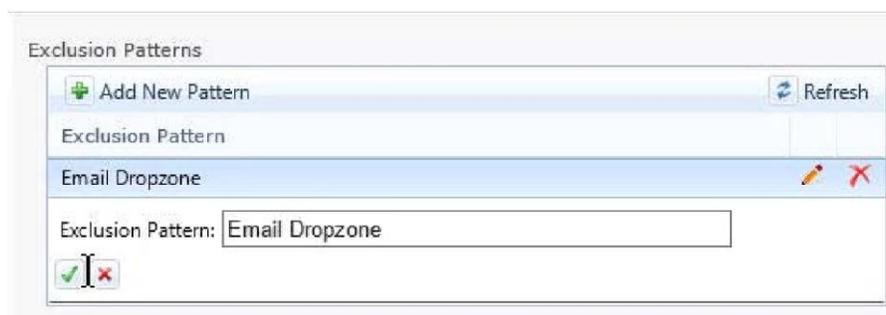
Figure 15-23 Edit Exclusion Pattern

5.   Click the **Go** button. The record you entered is excluded from reports.

16 Bulk Processing

Bulk Processing functionality is available within a **SharePoint Records Center** with Compliance Suite enabled. To use Bulk Processing, Compliance Suite must be installed and the site feature *Gimmal Compliance Suite Bulk Processing* and the site collection feature *Gimmal Compliance Suite Bulk Processing* Site Columns must be active.

Compliance Suite Bulk Processing enables the processing of one or more records in a single action. Standard SharePoint functionality supports the processing of only one item at a time which can become cumbersome when managing large volumes of records.

Bulk Processing supports site column (field) updates across multiple records in a single action. For example, if a storage location change affects multiple records, Bulk Processing can be used to update the **Location** site column for all affected records. This only happens for a record library where bulk metadata changes have been configured.

Compliance Suite uses the following for the implementation of Bulk Processing:

1. **Bulk Processing Administration** page: Configuration of Bulk Processing definitions. The Bulk Processing definitions define the Bulk Processing options that are available to end users within select SharePoint Records Center Lists and Libraries. By default, no Bulk Processing definitions are configured. To access this page you must be a member of the *RMA Bulk Processing Administrators SharePoint* group.

2. **Bulk Processing Header/Record Action**: Initiation of Bulk Processing from configured SharePoint Records Center Lists and Libraries. The **Bulk Processing** action button displays on the List or Library header ribbon under the **Manage** features. To enable the **Bulk Processing** action button, a user must select one or more items from the configured List or Library and should at least have edit permission on item.

Intended User: End User, Records Manager, Compliance Suite Administrator, RMA Bulk Processing Administrators

16.1 Bulk Processing Administration

Before initiating Bulk Processing for records, Compliance Suite Bulk Processing must be configured through the **Bulk Processing Administration** page to meet your organization's records management policies. To access the **Bulk Processing Administration** page, a user must be a member of the RMA Bulk Processing Administrators SharePoint group.

Bulk Processing Administration defines the Bulk Processing definitions available for selected SharePoint Lists and Libraries. These definitions define the Bulk Processing options that are enabled for end users within your SharePoint Records Center. The definition types supported by Bulk Processing include:

1. Field Update Definition

- Defines Content Type and their Site Columns that can be updated using Bulk Processing

- Supported through the Manage Field Definition task

2. List Workflow Definition

- Defines List Workflows where task metadata can be updated using Bulk Processing

- A List Workflow is a Compliance Suite Bulk Processing Compliant workflow that has been configured for association with a selected List or Library. Examples of List Workflows include Disposition Processing, Cutoff Review, and Vital Record Review workflows.

Note:

Bulk Processing Administration can only update a task's metadata. It cannot complete the task. To bulk complete certain tasks, use the Gimmal Bulk Task Processing.

- Task updates include the approval and/or entering of task information, such as comments for multiple tasks at the same time

In addition to the configuration of Bulk Processing definitions, Bulk Processing Administration provides the ability to configure the default settings for Bulk Processing. These settings define the options listed previously that display on the **Bulk Processing Administration** page, as well as the length of time Bulk Processing audit (history) information is saved.

Intended User: Bulk Processing Administrators

To access the Bulk Processing Administration page:

1. Open a SharePoint Records Center. The Records Center Home Page opens.

2. You can access Bulk Processing Administration in either of these two ways:

   a. Select **Bulk Processing Administration** from the Compliance Suite header ribbon.

   b. Select **Settings** and then **Site Settings** from the header navigation. On **Site Settings**, select **Bulk Processing Administration** in the **Compliance Suite** section.

3. The **Bulk Processing Administration** screen opens with options for configuring Bulk Processing definitions.
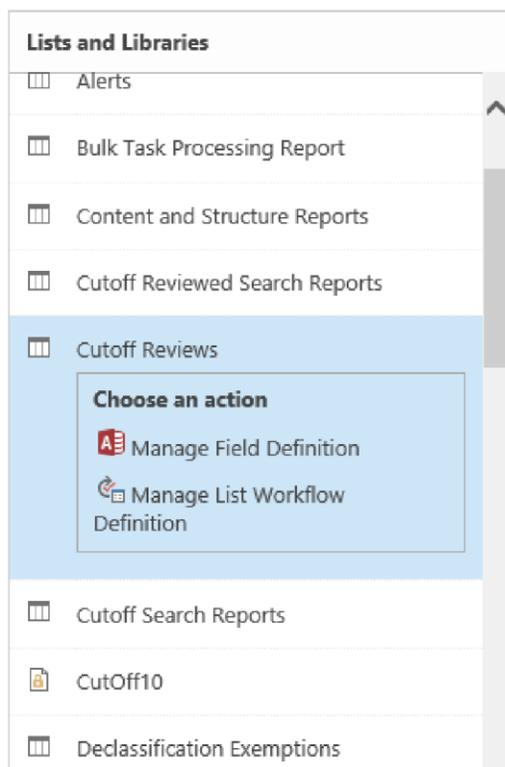
Figure 16-1 Bulk Processing Administration Page

The following table describes the **Bulk Processing Administration** screen.

Table 16-1 Bulk Processing Administration Screen

Feature/Title	Description
Bulk Processing Administration Settings	Action button that opens a window to configure the settings for Bulk Processing. The action button is displayed on the top right, under the page description.
List or Library Selection	List of SharePoint List and Libraries that can be configured for Bulk Processing. A user can select a List or Library to configure for Bulk Processing by selecting the item in the displayed list. Only one List or Library can be selected at a time. Example: Cutoff Review

Table 16-1 Bulk Processing Administration Screen

Feature/Title	Description

Task Selection	List of available definition types along with an option to *Manage Current Definitions*.
	When a user selects a List or Library, the valid Tasks become enabled.
	Manage Field Definition is enabled if the selected List or Library has associated content types.
	Manage List Workflow Definition is enabled if the selected List or Library has an associated Compliance Suite Bulk Processing Compliant List Workflow.

16.1.1 Bulk Processing Administration Settings

Bulk Processing Administration provides the ability to configure which definition tasks display on the **Bulk Processing Administration** page, as well as the length of time Bulk Processing audit (history) information is saved in the system.

To configure the Bulk Processing Administration settings:

1. Click the **Action** button on the top right of the page under the page description.

2. A **Settings** dialog box opens with options for selecting the available definition tasks and number of days to retain bulk processing audit history.

Figure 16-2 Bulk Processing Settings

3. Select the **Allow** option(s). By default, all options are selected.

   - **Field-Based Processing**: Display **Manage Field Update Definition** task.

   - **List Workflow Processing**: Display **Manage List Workflow Definition** task.

4. (**Required**) Enter/Select the **Clear processing history after [XX] days**. The default setting is *7*.

5. To close the settings, click the **X** in the upper right hand corner of the dialog box. All changes are applied to the **Bulk Processing Administration** page.

   - Previously configured definitions will not be affected by any changes to the settings.

16.1.2 How to Manage a Field Definition

To enable site column (field) updates across multiple items within a SharePoint List or Library, **Manage Field Update Definition** must be configured for the List or Library.

To configure **Manage a Field Update Definition** for a List or Library:

1. On the **Bulk Processing Administration** page, click on the desired List or Library.
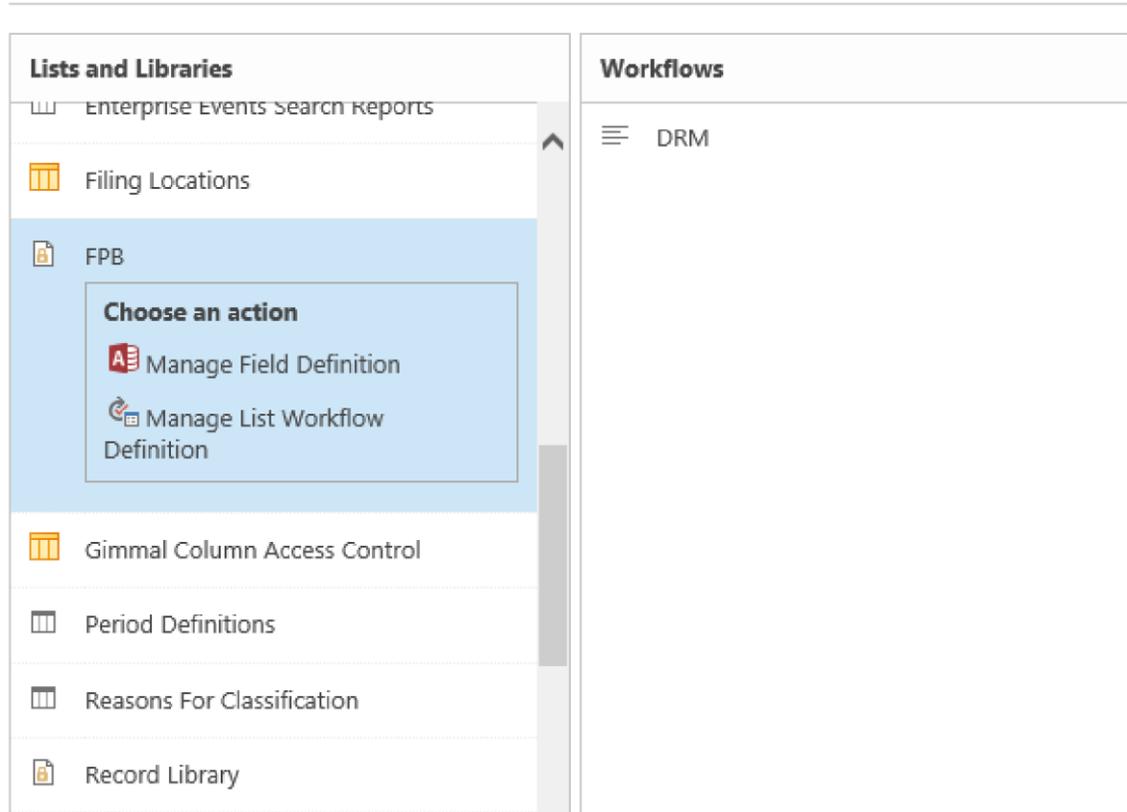

Figure 16-3 Bulk Processing: Selecting a Library

2. If the List or Library has no current definitions configured and it has associated Content Types, the **Select a Task** option **Manage Field Definition** is enabled.

Note:

If the option is disabled, the selected List or Library either has an existing definition; does not have a valid content type(s) associated; or **Manage a Field Update Definition** has been disabled in the **Bulk Administration Settings**.

---

3. **Select a content type** from the list of displayed content types.

- The content types are SharePoint Content Types that have been associated to the selected List or Library.

- The selected Content Type updates the Available Fields displayed on the page.

Figure 16-4 Field Update Definition

4. Select **Available Fields** and indicate if the selected field is **required?**

- The fields are the site columns associated with the selected **Content Type**. These fields include site columns that are inherited. For example, Title or Subject.

- All selected **Fields** are included on the **Process Bulk Selections** dialog box when a user initiates bulk processing for the selected **Content Type** within the selected List or Library in your SharePoint Records Center.

- All selected **Fields** that are marked **required?** are required on the **Process Bulk Selections** dialog box.

5. Enter **Display Name**. The **Display Name** is the user-friendly name that will be displayed on the **Process Bulk Selections** dialog box when a user initiates bulk processing for the selected **Content Type** within the selected List or Library in your SharePoint Records Center. If no **Display Name** is entered, the **Content Type's** name will be used.

6. Select **Enabled**. Selecting **Enabled** allows the bulk processing definition to be used by an end user in your SharePoint Records Center. By default, this is unchecked.

7. Select **Only update when**. Selecting **Only update when** enables options for setting up bulk processing to only execute when records meet selected criteria.

- Select a **Site Column Name**.

- Select a **Site Column Operator**.

- Enter a **Site Column Value**. The **Site Column Value** input type displayed is based on the selected **Site Column Name** type. For **Text** the input type is a *text box*. For **Date**,

a calendar lookup displays. For **Managed Metadata**, a lookup to Managed Metadata terms is displayed. For **Boolean**, radio options for *Yes* and *No* are displayed.

8. Click **Add**.

9. If the selected **Content Type** has inherited (child) Content Types, the A**pply Definition Inheritance** dialog box displays.
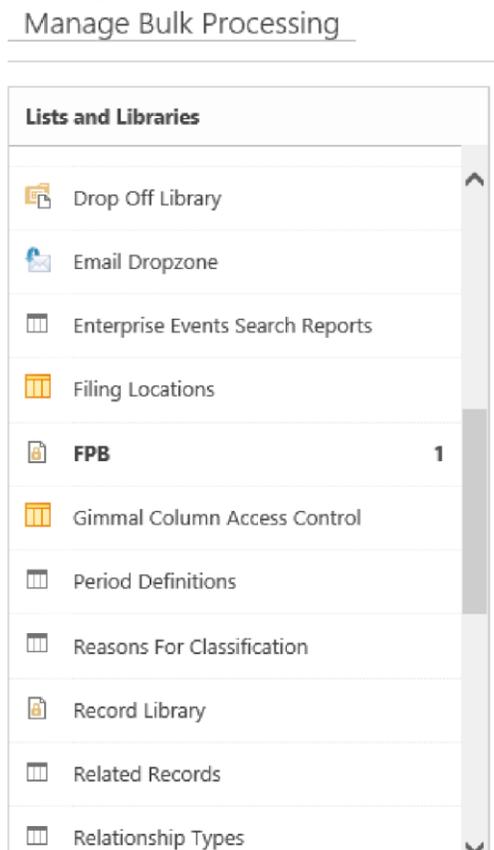

Figure 16-5 Apply Definition Inheritance Dialog Box

- Select the inherited **Content Types** you want to include as a part of this definition.

- By default no inherited **Content Types** are selected.

- Select the arrow to expand any displayed inherited **Content Type** to see additional inherited **Content Types** as applicable.

After selecting the inherited **Content Type(s)**, click **Continue** to save your selection or select **Cancel** to close the **Apply Definition Inheritance** dialog box without saving.

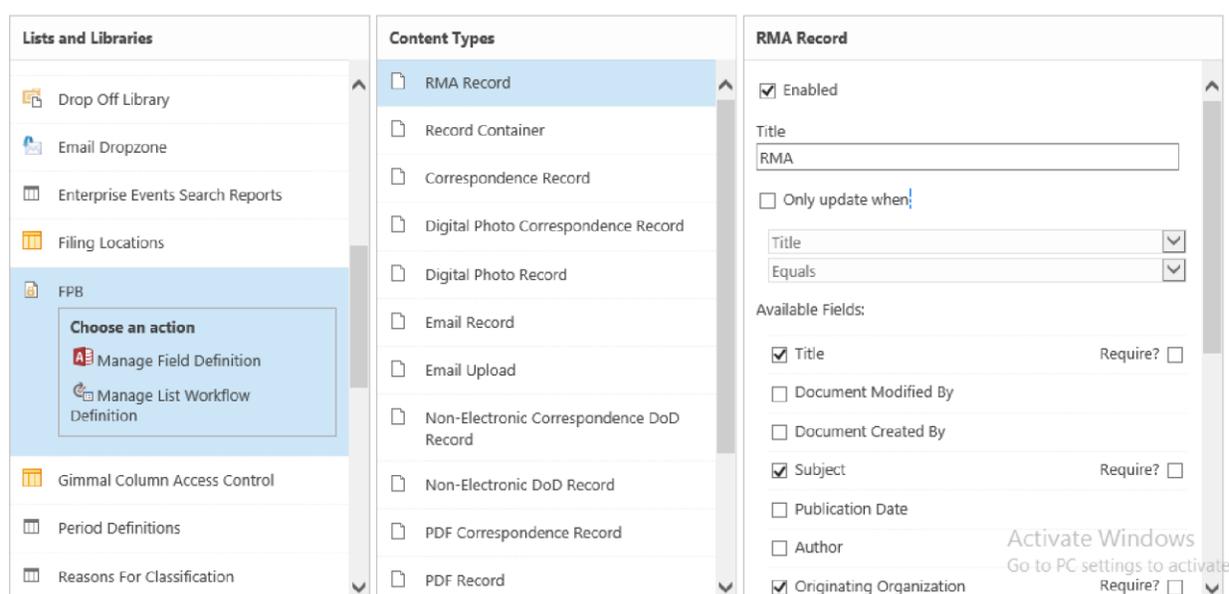10. After adding the definition, you are returned to the Field Update Definition screen.

Figure 16-6 Updated Field Update Definition Window

- The selected Content Type displays with a number **1** in the lower right corner.
- Any selected **Inherited Content Type(s)** are disabled and displayed with a lock icon. Definitions for **Inherited Content Type(s)** cannot be changed.
- Bulk Processing is enabled on the header ribbon of the selected List or Library in your SharePoint Records Center.

11. To close the dialog box, click the X in the upper right hand corner.

16.1.3 How to Manage a List Workflow Definition

To enable bulk processing to update metadata in a workflow task within a SharePoint List or Library, the **Manage List Workflow Definition** must be configured. The selected definition task depends on the type of workflow associated with the selected List or Library.

To manage the List Workflow Definition for a List or Library:

1. On the **Bulk Processing Administration** page, select the desired List or Library.
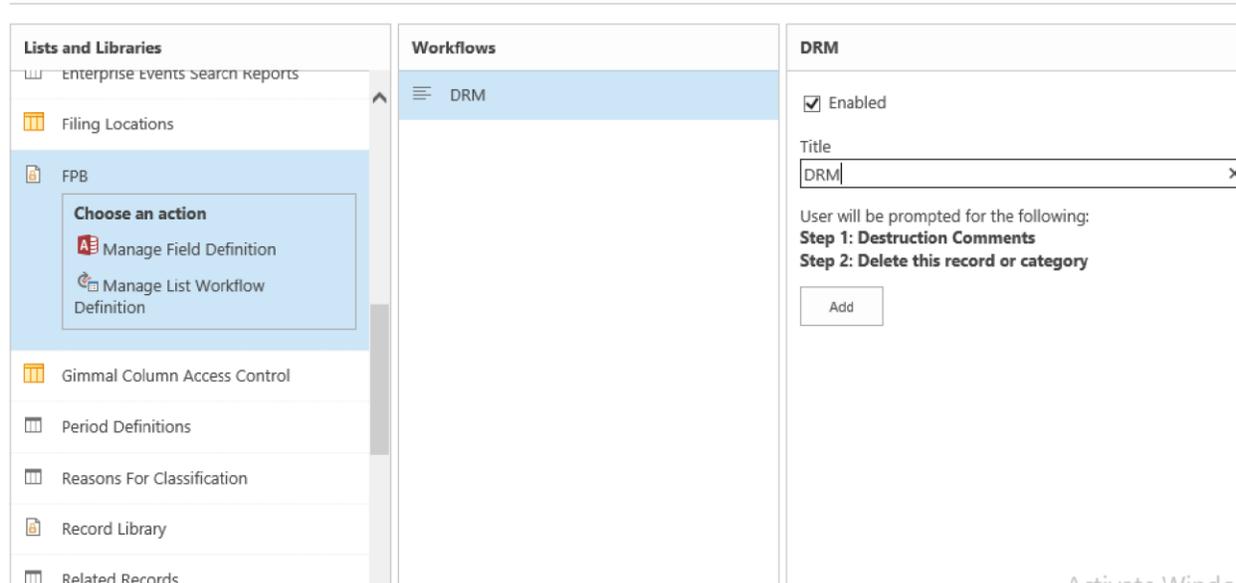
Figure 16-7 Selecting a List/Library for Workflow

2. If the List or Library has no current definitions configured and it has one or more associated Compliance Suite Bulk Processing Compliant List workflow(s), the **Select a Task** option **Manage List Workflow Definition** is enabled.

- If the option is disabled, the selected List or Library either has an existing definition; does not have a valid Compliance Suite Bulk Processing Compliant List workflow associated; or **Manage List Workflow Definition** has been disabled in the **Bulk Administration Settings**.

- By default, **Disposition Processing**, **Cutoff Review**, and **Vital Record Review** workflows are *Compliance Suite Bulk Processing Compliant*.

3. Click the **Manage List Workflow Definition** link. The **List Workflow Definition** screen opens with options for selecting list workflows for Bulk Processing.
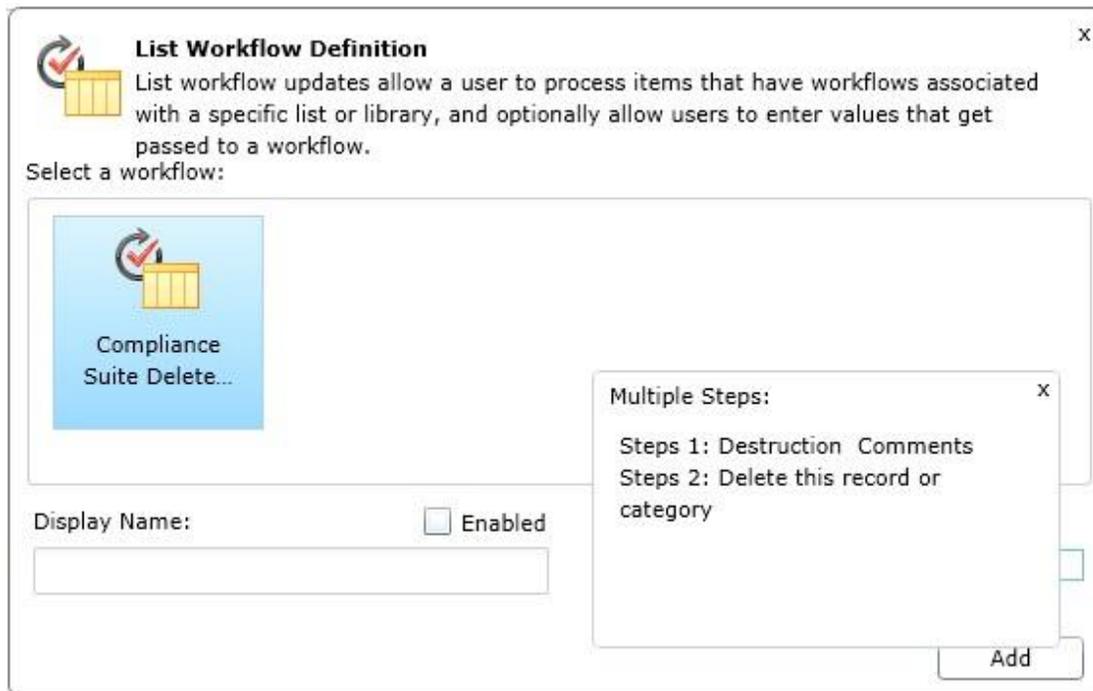
Figure 16-8 List Workflow Definition

4. **Select a workflow** from the list of displayed workflows.

   - The list of workflows are all Compliance Suite Bulk Processing Compliant **List** workflows that have been associated to the selected List or Library.

   - The selected **Workflow** updates the **User will be prompted for the following** displayed on the page.

5. Enter **Display Name**. The **Display Name** is the user friendly name that displays on the **Process Bulk Selections** dialog box when a user initiates bulk processing for workflow tasks based on the selected **Workflow** within the selected List or Library in your SharePoint Records Center.

6. Select **Enabled**. Selecting **Enabled** allows the bulk processing definition to be used by an end user in your SharePoint Records Center. By default, this is unchecked.

7. View **User will be prompted for the following**. This displays all workflow tasks for the selected **Workflow** that are configured for Bulk Processing input. If more than one workflow task has been configured, a **multiple steps** link will be displayed. Clicking **on multiple steps** opens a dialog box displaying all of the configured workflow task inputs.
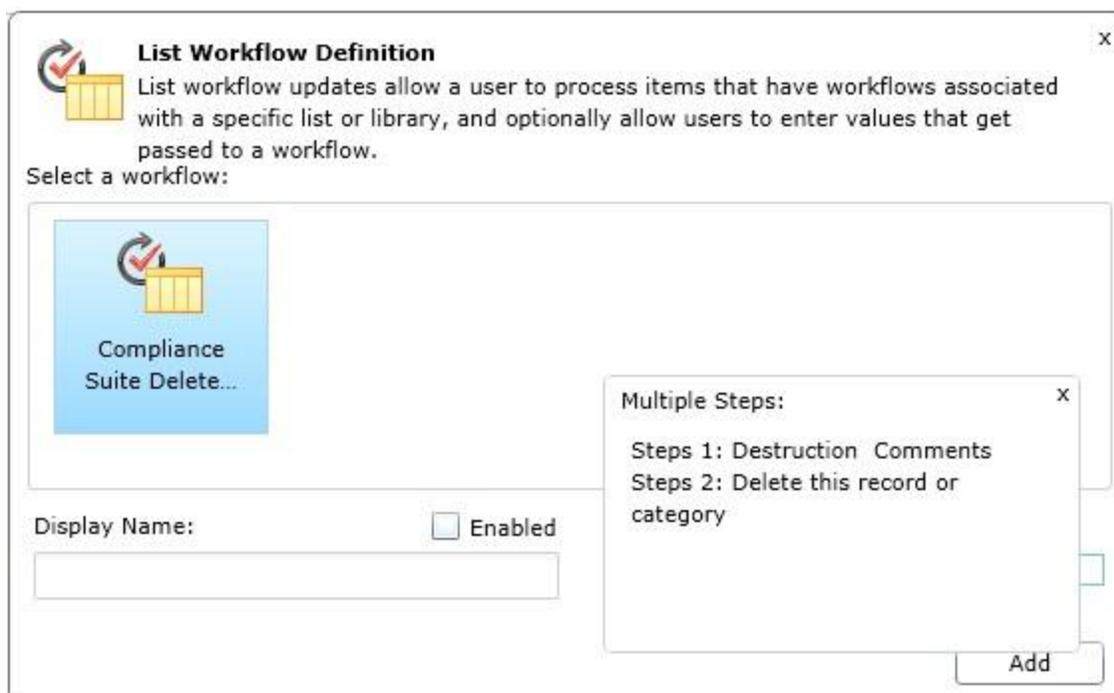
Figure 16-9 Multiple Workflow Steps

8. Click **Add**. The selected Workflow displays with a number 1 in the lower right corner.

9. Click **Save**. Bulk Processing is enabled on the header ribbon of the selected List or Library in your SharePoint Records Center.

10. To **Manage List Workflow Definition** for another workflow, repeat Steps 4 - 9.

11. To update an existing **Manage List Workflow Definitions**, select the **Workflow** that is associated with the definition, make changes, and click **Save**. See Manage Current Definitions help for more details.

12. To remove an existing **Manage List Workflow Definition**, select the Workflow that is associated with the definition and click **Remove**.

13. To close the **Manage List Workflow Definition** dialog box, click the **X** in the upper right hand corner of the dialog box.

    If one or more definitions were added, the number of definitions added is displayed next to the selected List or Library. For example, if you add a definition for *Delete Record and Metadata* and Transfer Record a 2 will be displayed next to the selected List or Library.

16.1.4 Managing Current Definitions

To update an existing Bulk Processing definition associated with a List or Library, you can manage field or workflow definitions.

To access **Manage Field** or **Workflow Definitions** for a List or Library:

1. On the **Bulk Processing Administration** page, select the List or Library that contains the definition you want to update.

2. If the List or Library has existing definitions configured, the **Select a Task** options **Manage Field Definitions** and **Manage List Workflow Definitions** are enabled.

   - If the options are disabled, the selected List or Library has no existing definition(s). You must add a definition. See ""How to Manage a Field Definition" on page 241 or "How to Manage a List Workflow Definition" on page 244 for more details.

3. Select the **Manage Field Definition** or **Manage List Workflow Definition** link. The **Field Update Definition** or **List Workflow Definition** dialog box opens, depending on your selection.

4. Make the desired changes and click Save.

Note:

Updates immediately take affect for the selected List or Library.

5. To remove an existing definition, click **Remove**.

6. To close the dialog box, click the **X** in the upper right hand corner of the window.

16.2 Initiating Bulk Processing for Site Column (Field) Updates

After one or more Bulk Processing Field Update Definition(s) have been configured through the Bulk Processing Administration page, you can initiate Bulk Processing for records within configured SharePoint List or Libraries. Initiating Bulk Processing for site column (field) updates allows the user to set the same site column values for multiple records at the same time.

Intended User: End User; Records Manager

To initiate Bulk Processing for selected records within a List or Library:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.

2. Navigate to and select one or more items you want to include in Bulk Processing. In the **Manage** group, click the **Bulk Processing** button.
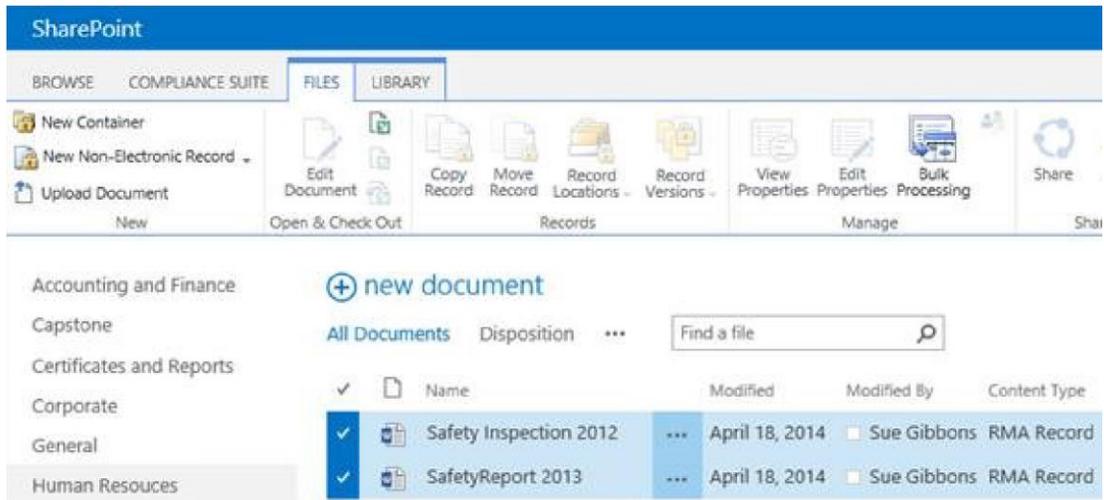
Figure 16-10 Selecting Items for Bulk Processing

3. Click the **Files** tab on the header ribbon.

4. Select **Bulk Processing** in the **Manage** subsection on the header ribbon. Bulk Processing Ribbon Button will only be enabled if user have edit permission on all selected items.

5. If the Content Type(s) of the selected items do not have a configured **Field Update Definition** or configured **Field Update Definition** was not enabled or if there is an existing Bulk Processing request, the following message displays:
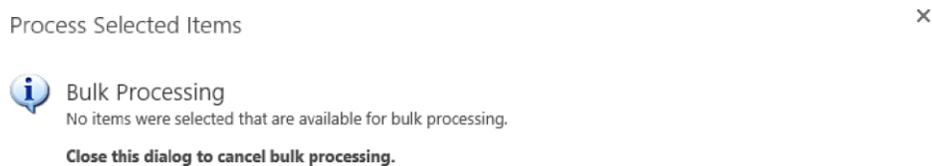

Figure 16-11 No Items for Bulk Processing Message

6. If the Content Type(s) of the selected items have one or more configured **Field Update Definition(s)**, the **Process Bulk Selections** dialog box opens displaying the configured site column/field options.

Figure 16-12 Process Bulk Selections

Note:

Fields that SharePoint requires display with a red asterisk (*). You must enter a value in these fields.

7. Enter the **Site Column/Field** value(s). The **Site Column(s)/Field(s)** displayed are based on the **Field Update Definition** associated with the current List or Library and the selected items' content type(s).

8. If the selected items include multiple content types with unique **Field Update Definitions**, each **Field Update Definition** displays as a tab on the **Process Bulk Selections** dialog box. The tab name is the **Display Name** set on the associated **Field Update Definition**.

   ● Click on the **Tab Name** or select **Next** → or **-< Previous** to navigate the displayed tabs.

   ● Repeat Step 7 for each displayed tab.

9. To close **Process Bulk Selections** without saving or submitting, click the **X** in the upper right hand corner of the **Process Bulk Selections** dialog box.

10. To submit **Process Bulk Selections**, click **Submit**. The **Process Bulk Selections** for the selected items are queued for processing by the RMA Bulk Record Processing Job. When the processing is successfully completed, a confirmation message displays.

    ● The selected item(s) **Has Bulk Updates Pending** field is set to *Yes*.

    ● If a selected item does not meet the Only update when criteria as defined in the associated Field Update Definition, the item is skipped and is not updated.

    ● If a selected item is under an existing Hold or Record Retention Schedule, the item is skipped and is not updated.

11. After the RMA Bulk Record Processing Job is successfully executed for valid selected items,

    ● The processed items Has Bulk Updates Pending field is set to No.

    ● The processed items will have site column(s)/field(s) updated based on the values set on the Process Bulk Selections dialog box.

16.3 Initiating Bulk Processing for Workflow Tasks

After one or more Bulk Processing for Workflow Definitions have been configured through the Bulk Processing Administration page, you can initiate Bulk Processing to update metadata for workflow tasks within configured SharePoint List or Libraries. Initiating Bulk Processing for workflow tasks allows the user to set task information (such as comments) for multiple workflow tasks at a time.

Note:

Bulk Processing Administration can only update a task's metadata. It cannot complete the task. To bulk complete certain tasks, use the Gimmal Bulk Task Processing.

The bulk processing initiation steps for workflow tasks based on List or Content Type Workflow Definitions is the same. The steps in this document refer to both as Workflow Definitions.

Intended User: End User; Records Manager

To initiate Bulk Processing for selected workflow tasks within a List or Library:

1. Open a **SharePoint Records Center**. The **Records Center Home Page** opens.

2. Select **Libraries** to see all lists, libraries, and other apps in the Site Contents.

3. Navigate to and select one or more items you want to include in Bulk Processing. Click the **Items** tab to open the header ribbon.

Figure 16-13 Selecting Items for Bulk Processing

4. Select **Bulk Processing** button under the **Manage** features on the header ribbon.

5. If the selected item(s) does not have an associated **Workflow Definition** or if the definition is not enabled or if there is an existing Bulk Processing request, a message displays that there were no items for bulk processing.

6. If the selected items have one or more associated **Workflow Definitions**, the **Process Bulk Selections** dialog box opens displaying the task field configurations for the definitions associated with the current List or Library and the selected items' associated workflow.

Figure 16-14 Process Bulk Selections

7. Enter the **Task** field value(s). The **Task** fields displayed are based task inputs enabled for Bulk Processing in the Workflow template. These are the task inputs that are displayed as read-only on the **Bulk Processing Administration - Workflow Definition** page.

Note:

Required fields display with a red asterisk.

8. If the selected items include multiple workflows with unique **Workflow Definitions**, each **Workflow Definition** displays as a tab on the **Process Bulk Selections** dialog box. The tab name is the **Display Name** set on the associated **Workflow Definition**.

   - Click on the **Tab Name** or select **Next** → or -< **Previous** to navigate the displayed tabs.

   - Repeat Step 7 for each displayed tab.

9. To close **Process Bulk Selections** without saving or submitting, click the **X** in the upper right hand corner of the **Process Bulk Selections** dialog box.

10. To submit **Process Bulk Selections**, click **Submit** button. The **Process Bulk Selections** for the selected items will be queued for processing by the RMA Bulk Record Processing Job. A message displays that the bulk processing was successful. The selected item(s) **Has Bulk Updates Pending** field is set to *Yes*.

11. After the RMA Bulk Record Processing Job is successfully executed for valid selected items,

    - The processed items **Has Bulk Updates Pending** field is set to *No*.

    - The processed items (tasks) are updated based on the values set on the **Process Bulk Selections** dialog box.