Archer® Exchange

Archer® Suite

6.7 P6+

eDiscovery Management

Application Guide Version 1.0

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks
RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement
This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses
This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies
This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution
Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CUSTOMER IS SOLELY RESPONSIBLE FOR ENSURING THAT THE INSTALLATION OF THE APPLICATION IS PERFORMED IN A SECURE MANNER. RSA RECOMMENDS CUSTOMERS PERFORM A FULL SECURITY EVALUATION PRIOR TO IMPLEMENTATION.

© 2021 RSA Security LLC or its affiliates. All Rights Reserved.

April 2021

Table of Contents

Chapter 1: Overview of eDiscovery Management

About eDiscovery Management

The eDiscovery Management app-pack is an application designed to connect the X1 platform to the Archer IRM environment to allow Archer workflows to manage the discovery, remediation, mitigation and resolution of issues of PII, PCI, PHI, or any other metadata discovered by the eDiscovery platform from your targeted native endpoints.

The app-pack leverages a data import to bring in metadata information collected by the X1 platform on files, emails and other elements matching search criteria using the X1 platform interface.

Key Features and Benefits

With the application, you will be able to:

- Organize collections of imported eDiscovery Data attributes into eDiscovery Projects
- Examine metadata for imported eDiscovery Data records
- Perform assessments for eDiscovery Projects
- Generate metrics across Projects and Data records to present relevant information to leadership
- Manage and collate Findings for eDiscovery Projects.

Prerequisites (ODA and system requirements)

Components	Recommended Software
ODA License	eDiscovery Management requires 2 ODA licenses. In addition, one (1) questionnaire is required for this offering. This requires a licensed use case that enables questionnaires for this package to function properly.
Operating System	Windows Server 2012 R2
Database Server	Microsoft SQL Server 2014 (64-bit)
Services Server	Java Runtime Environment (JRE) 8 (64-bit)
Archer	Archer 6.7 P6 and later
Use Cases	Archer Issues Management

Compatible Use Cases and Applications

Related Applications

Application	Use Case	Primary Purpose(s) of the Relationship
Control Procedures	Archer Issues Management	• Allows for workflow management and collections of found issues inside eDiscovery.

	Archer IT Controls Assurance (IT Security Risk Management)	• Allows for discovered elements, gaps, and projects to be mapped to appropriate control procedures.
Control Standards	Archer Policy Program Management	• Allows for mapping to potentially impacted control standards.
Business Processes	Multiple Use Case Mappings	• Allows discovered elements to be mapped to business processes
Information Assets	Multiple Use Case Mappings	• Allows discovered elements to be mapped to a particular data structure inside the environment
Devices	Multiple Use Case Mappings	• Allows discovered elements to be mapped to a particular hardware platform inside the environment
Findings	Archer Issues Management	• Allows discovered elements to be mapped to Finding for issues resolution and remediation workflow

Additional Resources

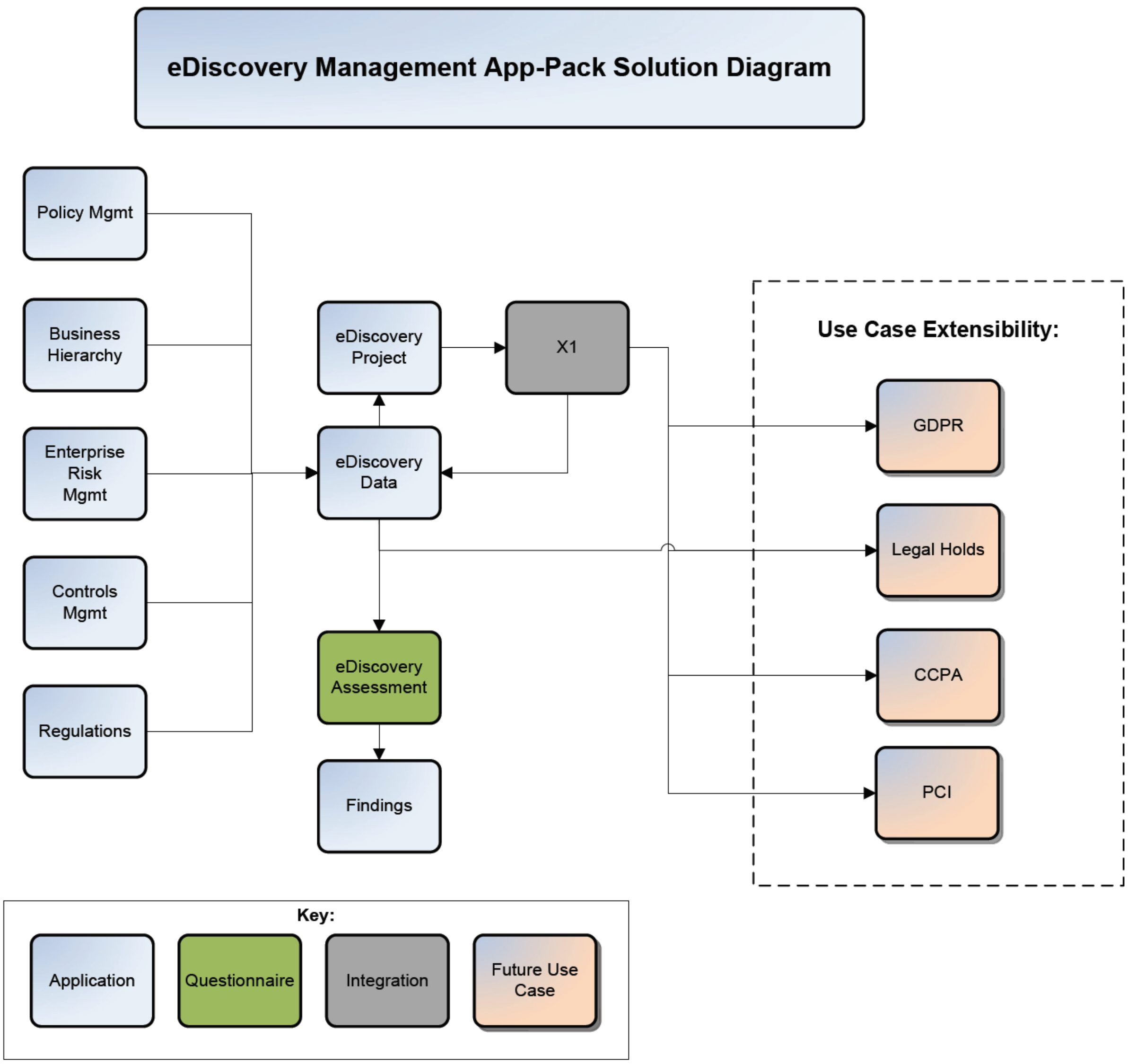
The following additional resources are available for this app-pack:

- Third-party website X1E Remote Collection On-Demand

Chapter 2: eDiscovery Management Components

Architecture Diagram

The following represents the core app-pack solution diagram as well as extensibility and cross-references.



Applications

Application	Description
eDiscovery Project	The eDiscovery Project captures the staff, scope, and metrics of all examined imported and worked eDiscovery Data records. Allows for management of large collections of records. This application is used as an aggregator for eDiscovery Data records. It captures the "why" of the overall effort, whether the effort is regulatory, audit, or compliance based.
eDiscovery Data	The eDiscovery Data record application stores metadata for each data record discovered and imported by the X1 platform. eDiscovery Data can be email, filetypes, or other regular expressions as represented in the native endpoints for the data source that is being mined. This application represents the "what" of the data being pulled.
eDiscovery Assessment	The eDiscovery Assessment provides questions around the location, security, and disposition of your data risk. Findings are auto generated based upon answers and allow you to treat the associated risk.

Personas and Access Roles

The following table describes the functions that make up the application's organization roles. Depending on the organization of your company, these functions and responsibilities may vary.

Function	Description
eDiscovery Manager	Reviews Owner work and approves or rejects reports. CRU access for all eDiscovery applications / questionnaires.
eDiscovery Administrator	Maintains the Application and Owners. Reports to Manager. CRUD access for all eDiscovery applications / questionnaires. All Admin options for eDiscovery applications / questionnaires. Note: This is the only role assigned Delete Permissions to records in eDiscovery applications.
eDiscovery Owner	Inputs data, runs searches, and generates reports for Manager. CRU access for all eDiscovery applications / questionnaires.
eDiscovery Read - Only	Read Access for eDiscovery data. Useful for executive / Compliance / Audit staff performing external review. R access for all eDiscovery applications / questionnaires

Chapter 3: Installing eDiscovery Management

Installation Overview

Complete the following tasks to install the application.

Step 1: Prepare for the Installation

1. Ensure that your Archer system meets the following requirements:
    - Archer Platform version 6.7 P6 or higher.
2. Download the ODA install package from the Archer Exchange on RSA Link: https://community.rsa.com/t5/archer-exchange/ct-p/archer-exchange
3. Read and understand the "Packaging Data" section of the Archer Online Documentation.

Step 2: Install the Package

Installing a package requires that you import the package file, map the objects in the package to objects in the target instance, and then install the package. See Installing the Application Package for complete information.

Step 3: Test the Installation

Test the application according to your company standards and procedures, to ensure that the app-pack works with your existing processes.

Installing the Package

Task 1: Back Up Your Database

There is no Undo function for a package installation. Packaging is a powerful feature that can make significant changes to an instance. Archer strongly recommends backing up the instance database before installing a package. This process enables a full restoration if necessary.

An alternate method for undoing a package installation is to create a package of the affected objects in the target instance before installing the new package. This package provides a snapshot of the instance before the new package is installed, which can be used to help undo the changes made by the package installation. New objects created by the package installation must be manually deleted.

Task 2: Import the Package

1. Go to the Install Packages page.
    a. From the menu bar, click  .
    b. Under Application Builder, click Install Packages.
2. In the Available Packages section, click Import.
3. Click Add New, then locate and select the package file that you want to import.
4. Click OK.
   The package file is displayed in the Available Packages section and is ready for installation.

Task 3: Map Objects in the Package

Important: This step is required only if you are upgrading to a later version of [ODA name].

1. In the Available Packages section, select the package you want to map.
2. In the Actions column, click for that package.
   The analyzer runs and examines the information in the package. The analyzer automatically matches the system IDs of the objects in the package with the objects in the target instances and identifies objects from the package that are successfully mapped to objects in the target instance, objects that are new or exist but are not mapped, and objects that do not exist (the object is in the target but not in the source).
   Note: This process can take several minutes or more, especially if the package is large, and may time out after 60 minutes. This time-out setting temporarily overrides any IIS time-out settings set to less than 60 minutes.
   When the analyzer is complete, the Advanced Package Mapping page lists the objects in the package file and corresponding objects in the target instance. The objects are divided into tabs, depending on whether they are found within Applications, Solutions, Access Roles, Groups, Sub-forms, or Questionnaires.
3. On each tab of the Advanced Mapping Page, review the icons that are displayed next to each object name to determine which objects require you to map them manually.

Icon	Name	Description
	Awaiting Mapping Review	Indicates that the system could not automatically match the object or children of the object to a corresponding object in the target instance. Objects marked with this symbol must be mapped manually through the mapping process. **Important:** New objects should not be mapped. This icon should remain visible. The mapping process can proceed without mapping all the objects. **Note:** You can execute the mapping process without mapping all the objects. The icon is for informational purposes only.
	Mapping Completed	Indicates that the object and all child objects are mapped to an object in the target instance. Nothing more needs to be done with these objects in Advanced Package Mapping.
	Do Not Map	Indicates that the object does not exist in the target instance or the object was not mapped through the Do Not Map option. These objects will not be mapped through Advanced Package Mapping and must be remedied manually.

	Undo	Indicates that a mapped object can be unmapped. This icon is displayed in the Actions column of a mapped object or object flagged as Do Not Map.

4. For each object that requires remediation, do one of the following:
    - To map each item individually, on the Target column, select the object in the target instance to which you want to map the source object. If an object is new or if you do not want to map an object, select Do Not Map from the drop-down list.
      Important: Ensure that you map all objects to their lowest level. When objects have child or related objects, a drill-down link is provided on the parent object. Child objects must be mapped before parent objects are mapped. For more details, see "Mapping Parent/Child Objects" in the Archer Online Documentation.
    - To automatically map all objects in a tab that have different system IDs but the same object name as an object in the target instance, do the following:
        a. In the toolbar, click Auto Map.
        b. Select an option for mapping objects by name.

Option	Description
Ignore case	Select this option to match objects with similar names regardless of the case of the characters in the object names.
Ignore spaces	Select this option to match objects with similar names regardless of whether spaces exist in the object names.

        c. Click OK.
        The Confirmation dialog box opens with the total number of mappings performed. These mappings have not been committed to the database yet and can be modified in the Advanced Package Mapping page.
        d. Click OK.
    - To set all objects in the tab to Do Not Map, in the toolbar, click Do Not Map.
      Note: To undo the mapping settings for any individual object, click in the Actions column.

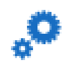
   When all objects are mapped, the icon is displayed in the tab title. The icon is displayed next to the object to indicate that the object will not be mapped.
5. Verify that all other objects are mapped correctly.
6. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the Archer Online Documentation.
7. Once you have reviewed and mapped all objects, click .
8. Select I understand the implications of performing this operation and click OK.

The Advanced Package Mapping process updates the system IDs of the objects in the target instance as defined on the Advanced Package Mapping page. When the mapping is complete, the Import and Install Packages page is displayed.

Important: Advanced Package Mapping modifies the system IDs in the target instance. Any Data Feeds and Web Service APIs that use these objects will need to be updated with the new system IDs.

Task 4: Install the Package

All objects from the source instance are installed in the target instance unless the object cannot be found or is flagged to not be installed in the target instance. A list of conditions that may cause objects not to be installed is provided in the Log Messages section. A log entry is displayed in the Package Installation Log section.

1. Go to the Install Packages page.
   a. From the menu bar, click  .
   b. Under Application Builder, click Install Packages.
2. In the Available Packages section, do the following:
   a. Locate the package file you want to install.
   b. In the Actions column, click  .
3. In the Selected Components section, select the components of the package that you want to install.
   - To select all components, select the top-level checkbox.
   - To install only specific global reports in an already installed application, select the checkbox associated with each report that you want to install.

   Note: Items in the package that do not match an existing item in the target instance are selected by default.
4. Click Lookup.
5. For each component section, do the following:

   Note: To move onto another component section, click Continue or select a component section in the Jump To drop-down menu.
   a. In the Install Method drop-down menu, select an install method for each selected component.

      Note: If you have any existing components that you do not want to modify, select Create New Only. You may have to modify those components after installing the package to use the changes made by the package.
   b. In the Install Option drop-down menu, select an install option for each selected component.

      Note: If you have any custom fields or formatting in a component that you do not want to lose, select Do Not Override Layout. You may have to modify the layout after installing the package to use the changes made by the package.
6. Click OK.

7. To deactivate target fields and data-driven events that are not in the package, in the Post-Install Actions section, select the Deactivate target fields and data-driven events that are not in the package checkbox. To rename the deactivated target fields and data-driven events with a user-defined prefix, select the Apply a prefix to all deactivated objects checkbox, and enter a prefix. This can help you identify any fields or data-driven events that you may want to review for cleanup post-install.
8. Click Install.
9. Click OK.

Task 5: Review the Package Installation Log

1. Go to the Package Installation Log tab of the Install Packages page.
    a. From the menu bar, click .
    b. Under Application Builder, click Install Packages.
    c. Click the Package Installation Log tab.
2. Click the package that you want to view.
3. In the Package Installation Log page, in the Object Details section, click View All Warnings.

Step 6: Activate Advanced Workflow

1. Go to the Applications page.
    a. From the menu bar, click .
    b. Under Application Builder, click Applications.
2. In the Applications section, select the **eDiscovery Data** Application.
3. On the Advanced Workflow Tab, click ‘Activate’ in the top right corner of the page.
4. Then click ‘Save Workflow’ in the top left corner of the page.

Chapter 4: Using eDiscovery Management

Task 1: Perform the Import

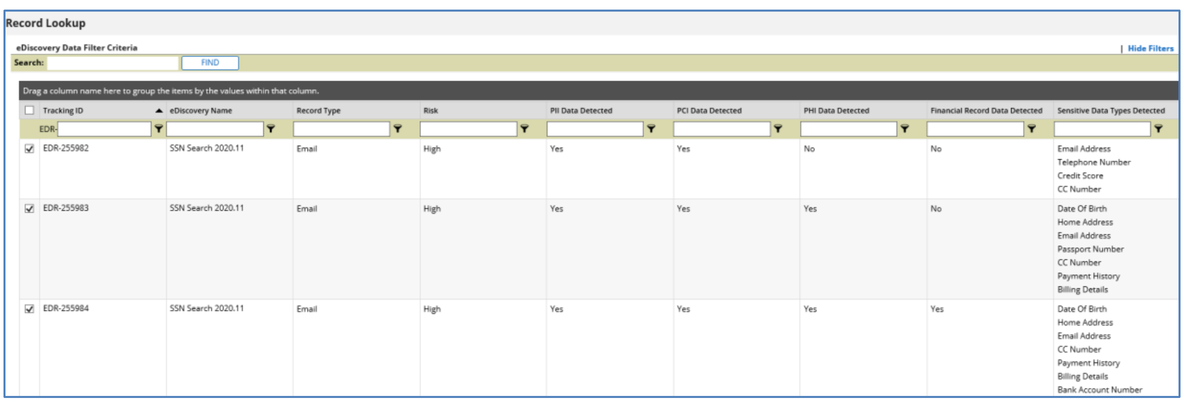
User: (typically eDiscovery – Owner persona)

1. Go to the Settings, Integration, Data Imports.
    a. From the menu bar, click  .
    b. Under Integration, Click Data Imports
2. Select eDiscovery Data
3. Execute Data Import with import files downloaded from X1.

Task 2: Setup the eDiscovery Project

User: (typically eDiscovery – Manager persona)

1. Go to eDiscovery Project
2. Select Add New Record
3. Complete Project Information
4. Assign Staff
5. Attach eDiscovery Data Records
    a. From the EDICOVERY DATA Cross Reference field, select Lookup
    b. Use Lookup filters and select appropriate records



Record Lookup

eDiscovery Data Filter Criteria | Hide Filters

Search: FIND

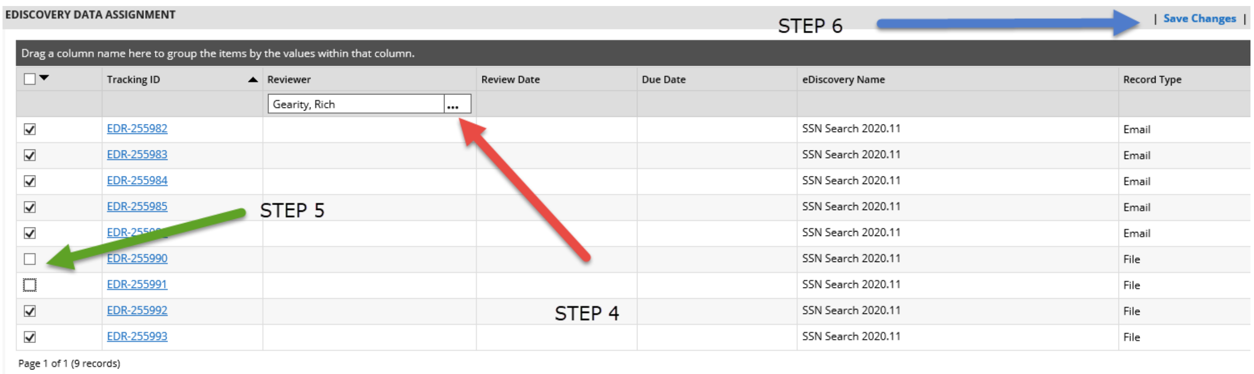
Drag a column name here to group the items by the values within that column.

Tracking ID	eDiscovery Name	Record Type	Risk	PII Data Detected	PCI Data Detected	PHI Data Detected	Financial Record Data Detected	Sensitive Data Types Detected
EDR-								
EDR-255982	SSN Search 2020.11	Email	High	Yes	Yes	No	No	Email Address Telephone Number Credit Score CC Number
EDR-255983	SSN Search 2020.11	Email	High	Yes	Yes	Yes	No	Date Of Birth Home Address Email Address Passport Number CC Number Payment History Billing Details
EDR-255984	SSN Search 2020.11	Email	High	Yes	Yes	Yes	Yes	Date Of Birth Home Address Email Address CC Number Payment History Billing Details Bank Account Number

Task 3: Assign Reviewer(s) to the eDiscovery Data records

User: (typically eDiscovery – Owner persona)

1. From the eDiscovery Application, open the Report titled eDiscovery Data Assignment.
2. Add any additional fields (if any) and filter for desired records.
3. Under Options, Select Enable Bulk Update
4. Assign Reviewer for records.
5. Select which records to apply the Reviewer to.



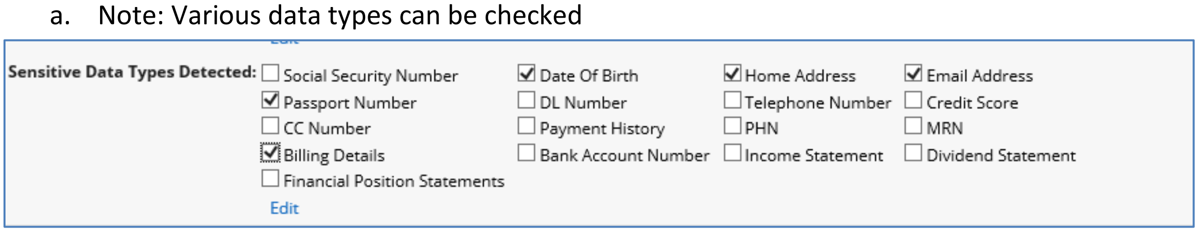
6. Select Save Changes

Task 4: Review the eDiscovery Data records

User: (typically eDiscovery – Owner persona)

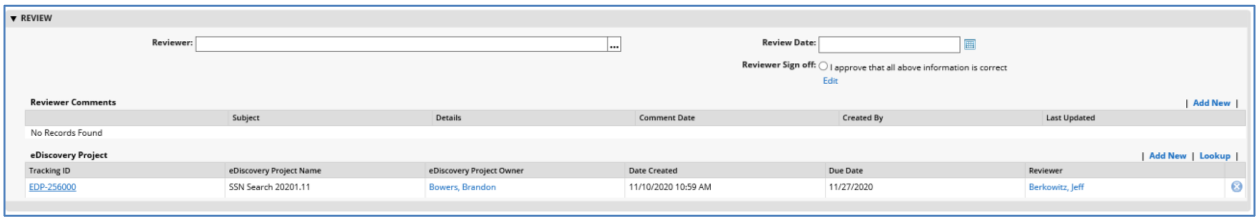
1. Examine the (Email / File) Metadata section and the link information provided
2. Map Controls impacted – reviewers can map to the following:
   a. Control Standards
   b. Control Procedures

3. Map Enterprise elements impacted – reviewers can map to the following:
   a. Business Unit
   b. Business Process
4. Complete the data types detected section.
   a. Note: Various data types can be checked

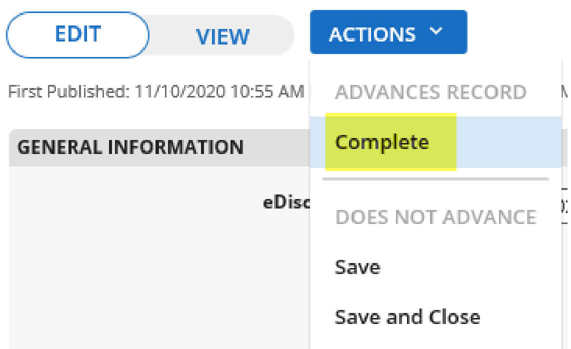


   b. These will determine the population of the Data Detected fields above the previous field. These XX Data Detected are populated by Data Driven Events.

5. Complete Review Section.
    a. Populate your userid
    b. Check Sign off when complete.



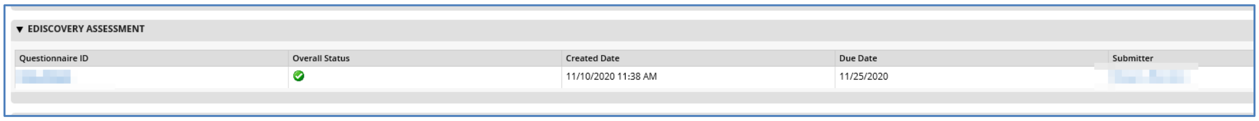
6. Add commentary as needed in the Reviewer Comments
7. When complete, Select Actions COMPLETE to finish the Advanced Workflow



Task 5: Complete the eDiscovery Assessment

User: (typically eDiscovery – Manager persona)

1. In the eDiscovery Project record, you will see the eDiscovery Assessment cross-reference field.
    a. This questionnaire will be auto generated after attaching eDiscovery Data records to the Project.



2. There is a total of 37 questions.
3. Workflow has been simplified as **Overall Status** will be marked complete when all questions are answered.
4. Complete / Add Comments as needed.