Archer® Exchange

Archer® Suite

Version 6.8

Implementation Guide

December 2021

LexisNexis Regulatory Compliance - Enhanced Content

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.archerirm.com/company/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.

December 2021

Revised: December 2021

Table of Contents

Release Notes

New and Changed Features

The following table describes enhancements.

Release Version	Published Date	Notes
Archer 6.8	December 2020	Initial Release
Archer 6.8	December 2021	Re-Signed JavaScript file.

Chapter 1: Overview

About LexisNexis Regulatory Compliance - Enhanced Content

The Archer LexisNexis Regulatory Compliance Enhanced Content integration allows you to automatically import regulatory data directly into the Archer Policy Program Management use case. The enhancements made to the solutions allows users view the regulation (mandate) and the designated regulator linked back to the regulatory obligations. Archer produces real-time reports and user-specific dashboards to view the mandates tied to specific regulations and the compliance of those mandates as tested through the Controls Assurance solution. This integration builds on the LexisNexis Regulatory Compliance integration which pulls in the Obligation/Sub Obligation, Tools, and Regulatory Alerts.

Key Features and Benefits

LexisNexis Regulatory Compliance Enhanced Content integration with Archer enables organizations to:

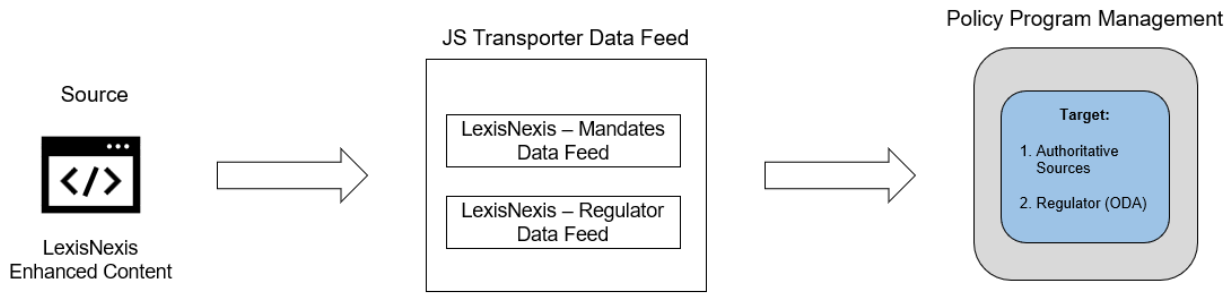
- Consolidate information from multiple regulatory bodies.
- Centrally manage Regulations, Laws and Requirements and map them to Regulators, Obligations and Policies.
- Report on overall compliance of the Regulation within the organization.

Requirements

Components	Requirement
Archer Solution	Regulatory & Corporate Compliance Management
Archer Use Case(s)	The following use cases take advantage of the information provided by the LexisNexis Regulatory Compliance Enhanced Content integration: • Archer Policy Program Management
Archer Applications	Leverages the following applications: • Authoritative Sources
Uses Custom Application	One On-Demand Application is required. • Regulators
Requires On-Demand License	Yes
Archer Requirements	Archer release 6.8 or later
LexisNexis Requirements	Valid LexisNexis Enhanced Content license is required.
Supported Platform Version	This offering has been developed for and validated on Archer Platform Release 6.8

Integration Diagram

The following diagram provides an overview of interaction between LexisNexis Regulatory Compliance Enhanced Content and Archer.



The integration process follows the following flow:

1. The Archer data feed for the LexisNexis Regulatory Compliance Enhanced Content Integration pulls the data from the source: LexisNexis Regulatory Compliance Enhanced Content API URL and imports the data into Target: Authoritative Sources application and Regulators ODA.
2. When the user logins into the LexisNexis Regulatory Compliance Enhanced Content URL, a list of all the Mandates and Regulators available are visible.

Chapter 2: Configuring LexisNexis Regulatory Compliance Enhanced Content Integration

Before You Begin

This section provides instructions for configuring the LexisNexis Regulatory Compliance Enhanced Content offering with the Archer Platform. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products to install the required components.

All LexisNexis Regulatory Compliance Enhanced Content links must be working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The integration described in this guide is being provided as a reference implementation for evaluation and testing purposes. It may or may not meet the needs and use cases for your organization. If additional customizations or enhancements are needed, it is recommended that customers contact RSA Professional Services for assistance.

Configuring Archer

Before you import the LexisNexis Regulatory Compliance Enhanced Content data feeds, complete the following tasks. First, install Archer LexisNexis Regulators 6.8 Install Package.zip in your Archer environment, Version 6.8 or above. Then configure Authoritative Sources application for the LexisNexis Regulatory Compliance Enhanced Content Integration.

Installing the Package

The following tasks detail how to import and install the Archer LexisNexis Regulators 6.8 Install Package.zip.

Step 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. RSA 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.

Step 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.

Step 3: Map Objects in the Package

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.

The following table describes the icons.

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 " Parent and Child Object Mapping " 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.

The following table describes the options.

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.

Step 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.

Step 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.

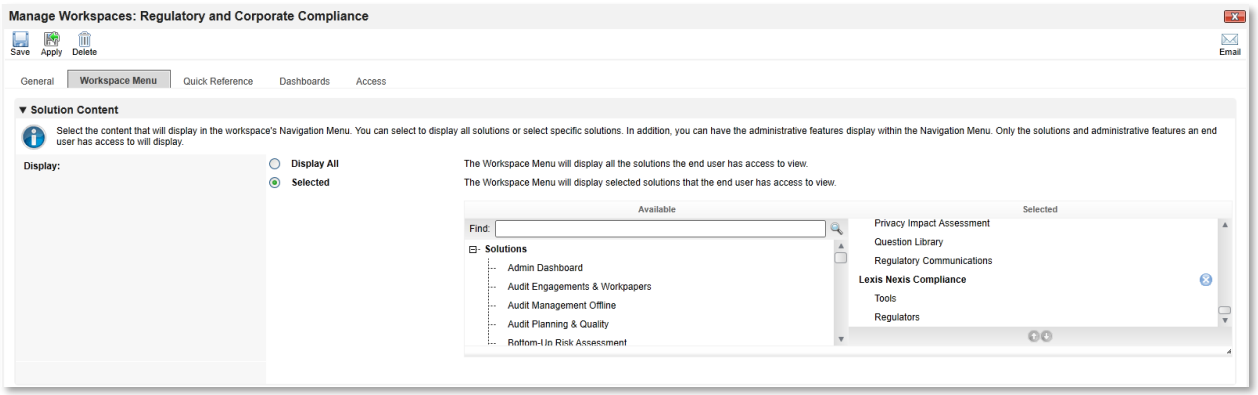
2. Click the package that you want to view.
3. In the Package Installation Log page, in the Object Details section, click View All Errors.
   For a list of packaging installation log messages and remediation information for common messages, see “Package Installation Log Messages” in the Archer Online Documentation.

Step 6: Adding Regulators ODA to Regulatory and Corporate Compliance workspace

1. Go to the Workspaces page.

   a. From the menu bar, click  .
   b. Under Workspaces and Dashboards, click Workspaces.

2. Select Regulatory and Corporate Compliance.
3. Go to Workspaces Menu tab.
4. Search Lexis Nexis Compliance and add to the list as shown below:



5. Click Save.

Configuring Authoritative Sources Application

Task 1: Add Fields to the Authoritative Sources Application

1. Click  and navigate to Applications. Under the **Application Builder** dropdown, select **Applications**.
2. Select the **Authoritative Sources** application and navigate to the **Fields** tab.

Level: **Source**

3. Edit the **Content Source** Values List field and Add a new value “LexisNexis”.
4. In the **Fields** tab. Add the following fields:
   a. Country
      i. Type: Value List (Field Specific)
      ii. Display Options: Values Popup
      iii. Configuration: Maximum Selection=No Maximum
   b. Date Archived
      i. Type: Date
      ii. Display Options: Date/Time
   c. Date Changed
      i. Type: Date
      ii. Display Options: Date/Time
   d. LN Date Created
      i. Type: Date
      ii. Display Options: Date/Time
   e. Is Archived?
      i. Type: Values List (Field Specific)
      ii. Display Option: Drop Down
   f. Is Government?
      i. Type: Values List (Field Specific)
      ii. Display Option: Drop Down
   g. Level
      i. Type: Values List (Field Specific)
      ii. Display Options: Values Popup

iii. Configuration: Maximum Selection=No Maximum

h. Source ID
   i. Type: Text

i. State
   i. Type: Values List (Field Specific)
   ii. Display Options: Values Popup
   iii. Configuration: Maximum Selection=No Maximum

j. URL
   i. Type: External Link

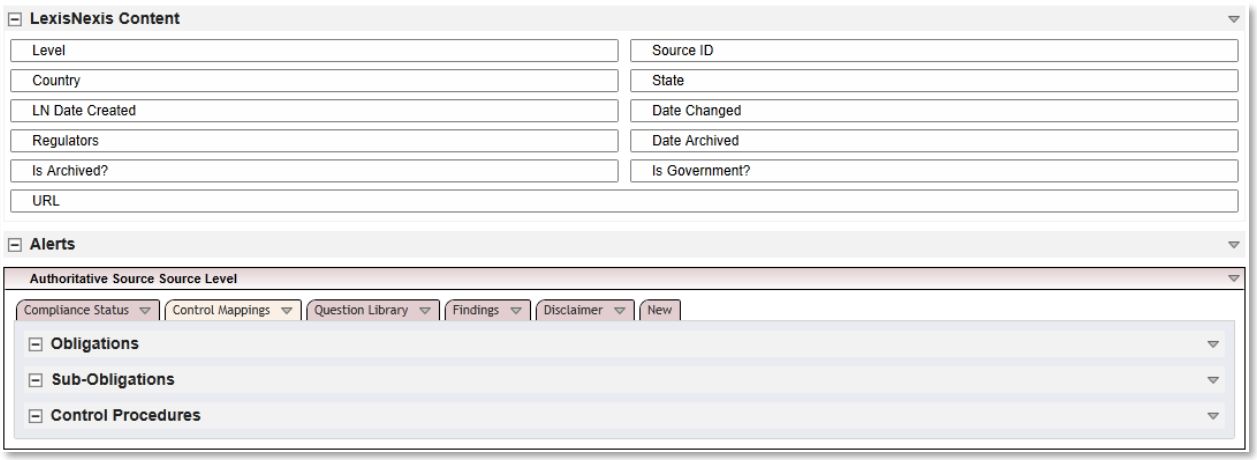
k. Rename the field Regulator (Authoritative Sources) to “Regulators”
   i. Type: Related Records
   ii. Display Control: Single Column

l. Create New / Rename existing Control Standards field to “Obligations”
   i. Type: Cross-Reference/ Related Records
   ii. Available Reference: Control Standards
   iii. Display Control: Grid
   iv. Record Lookup Configuration/Grid Display Properties Display Fields: Standard ID, Standard Name, Statement.

m. Sub-Obligations
   i. Type: Cross-Reference/ Related Records
   ii. Available Reference: Control Standards
   iii. Display Control: Grid
   iv. Record Lookup Configuration/Grid Display Properties Display Fields: Standard ID, Standard Name, Statement.

n. Alerts
   i. Type: Cross-Reference/ Related Records
   ii. Available Reference: Regulatory Intelligence Items
   iii. Display Control: Grid
   iv. Record Lookup Configuration/Grid Display Properties Display Fields: Tracking ID, Title, Abstract

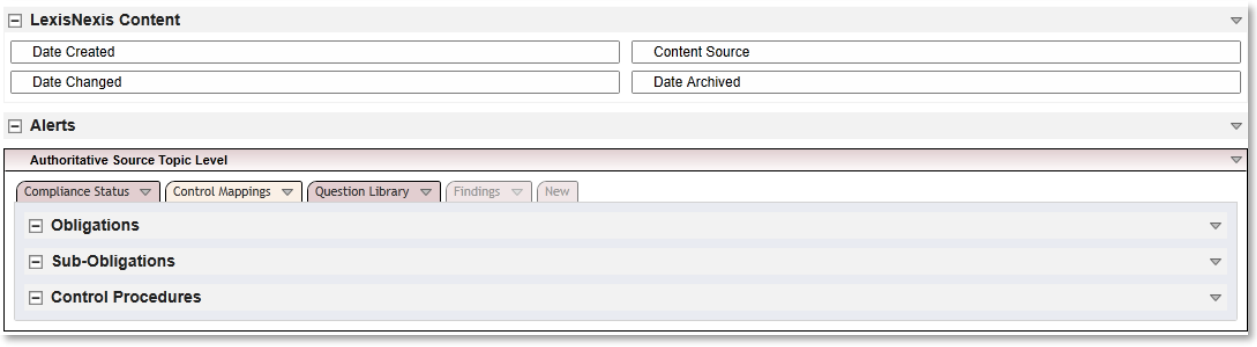
5. Navigate to **Layout -> Designer** tab **->** Add New Layout Object
6. **Add Section** named “LexisNexis Content” under “Authoritative Source” section.
7. Place all the above created fields as shown in the screenshot below



8. Click **Apply**.

Level: **Topic**

9. In the **Fields** tab. Add the following fields:
    a. Date Archived
        i. Type: Date
        ii. Display Options: Date/Time
    b. Date Changed
        i. Type: Date
        ii. Display Options: Date/Time
    c. Date Created
        i. Type: Date
        ii. Display Options: Date/Time
    d. Create New / Rename existing Control Standards field to “Obligations”
        i. Type: Cross-Reference/Related Records
        ii. Available Reference: Control Standards
        iii. Display Control: Grid
        iv. Record Lookup Configuration/Grid Display Properties Display Fields: Standard ID, Standard Name, Statement.
    e. Sub-Obligations
        i. Type: Cross-Reference/ Related Records
        ii. Available Reference: Control Standards
        iii. Display Control: Grid
        iv. Record Lookup Configuration/Grid Display Properties Display Fields: Standard ID, Standard Name, Statement.
    f. Alerts
        i. Type: Cross-Reference/ Related Records
        ii. Available Reference: Regulatory Intelligence Items
        iii. Display Control: Grid
        iv. Record Lookup Configuration/Grid Display Properties Display Fields: Tracking ID, Title, Abstract
10. **Add Section** named “LexisNexis Content” under “Topic” section.
11. Place all the above created fields as shown in the screenshot below



12. Click **Apply**.

Level: **Section**

13. Repeat Steps 9 to 13.

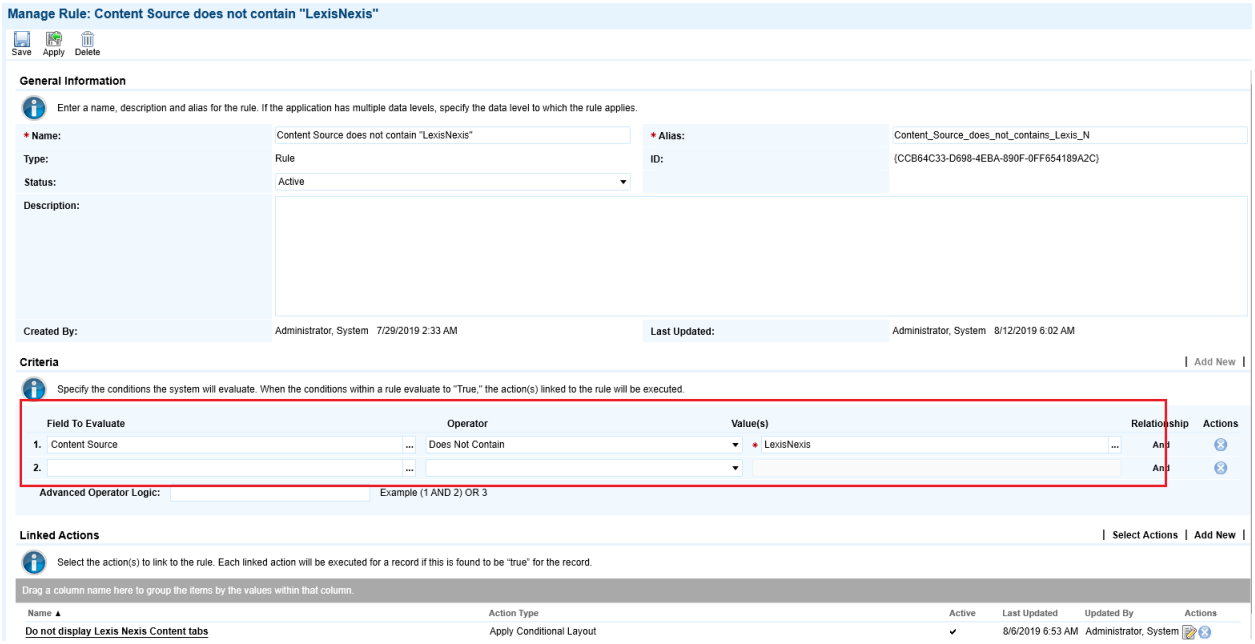
Level: **Sub-Section**

14. Repeat Steps 9 to 13.

Task 2: Add DDEs to Account for New Layout Changes

Rule 1: Hide LexisNexis Content Tabs

1. Repeat below steps 2 to 6 at all levels (Source, Topic, Section and Sub Section) in Authoritative Sources application.
2. Navigate to the **Layout -> Rules tab** for the following steps.
3. Create New Rule from scratch:
    a. Name: Content Source Does Not Contain LexisNexis
    b. Criteria:
        i. Content Source **Does Not Contain** LexisNexis
4. Click **|Add New|** in the **Linked Actions** section.
5. Select Apply Conditional Layout and click OK.
    a. Name: Hide LexisNexis Content tabs.
    b. Hide all sections related to LexisNexis Content. Below is the list of sections:
        i. LexisNexis Content section: **Do Not Display**
        ii. Alerts section: **Do Not Display**
        iii. Control Mappings tab -> Obligations and Sub-Obligations sections: **Do Not Display**
    c. Set Qualified Users/Groups to Everyone.
    d. Save Action.
6. **Save** rule.



Configuring the Data Feed

The following data feeds are used as part of the LexisNexis Regulatory Compliance Enhanced Content Integration process:

LexisNexis Regulatory Compliance Enhanced Content data feeds are JavaScript transporter data feeds that retrieves data (Mandates and Regulators related data) from the LexisNexis Regulatory Compliance Enhanced Content API URL and creates and updates the records in the Archer Authoritative Sources and Regulators application.

All data feeds must be configured. After setting up the data feeds, you can schedule them to run **as needed per your organization's requirements**. For more information on Scheduling data feeds, see the Scheduling Data Feeds section.

Configuring the JavaScript Transporter Settings

Before you upload a JavaScript file, you must configure JavaScript Transporter settings in the Archer Control Panel.

1. On the General tab, go to the **JavaScript Transporter** section.
   a. Open the **Archer Control Panel**.
   b. Go to **Instance Management** and select **All Instances**.
   c. Select the instance you want to use.
   d. On the **General** tab, go to the **JavaScript Transporter** section.
2. In the **Max Memory Limit** field, set the value to 2048 MB (2 GB).
3. In the **Script Timeout** field, set the value to 120 minutes (2 hours).
4. (Optional) If you want to allow only digitally signed JavaScript files in the data feed, enable **Require Signature**.
   a. In the JavaScript Transporter Settings section, select the checkbox **Require Signature**. A new empty cell appears in the **Signing Certificate Thumbprints** section
   b. In the **Signing Certificate Thumbprints** section, double-click an empty cell.
   c. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.

      Note: For information on how to obtain digital thumbprints, see Obtaining Digital Thumbprints.

      Important: If you enable Require Signature and specify no thumbprints, no JavaScript files will be accepted by the system.

   d. (Optional) If you want to add additional thumbprint sources, repeat steps b-c for each thumbprint.
5. On the toolbar, click **Save**.

Obtaining Digital Thumbprints

When running JavaScript data feeds, you can set the Archer instance to only allow digitally signed JavaScript files from trusted sources for security considerations.

For a certificate to be trusted, all the certificates in the chain, including the Root CA Certificate and Intermediate CA certificates, must be trusted on both the Web Server and Services Server machines.

Archer Technologies LLC cert in the Trusted Root CA Store

Archer Technologies LLC certificate is not present on every machine's root by default.

1. On the JavaScript file, right-click and select Properties.
    a. Click the Digital Signatures tab.
    b. From the Signature List window, select Archer Technologies LLC.
    c. Click the Details button.
    d. Click View Certificate.
    e. Click Install Certificate.
    f. Select Local Machine.
    g. Click Next.
    h. Select Place all certificates in the following store and click Browse.
        i. Select Trusted Root Certification Authorities and click OK.
        ii. Click Next.
        iii. Click Finish.
2. Upon successful import, click OK.

Obtaining a Certificate Thumbprint

1. In the Archer Control Panel environment, open the Manage Computer Certificates program.
    a. Click Start.
    b. Type: certificate
    c. From the search results, click **Manage Computer Certificates**.
2. Ensure that your trusted source certificates are in the **Certificates** sub-folder of the **Trust Root Certification Authorities** folder.
3. In the **Certificates** sub-folder, double-click the Archer Technologies LLC certificate that contains the thumbprint you want to obtain.
4. Verify that the certificate is trusted.
    a. In the Certificate window, click the Certification Path tab.
    b. Ensure that the Certificate Status windows displays the following message:
    This certificate is OK
    Note: If the Certificate Status windows displays something different, follow the on-screen instructions.
5. Obtain the trusted certificate thumbprint.
    a. In the Certificate window, click the Details tab.
    b. Select the Thumbprint field.
    The certificate's digital thumbprint appears in the window.

c. Copy the thumbprint.

Setting up the LexisNexis Regulatory Compliance Enhanced Content Data Feeds

Important: Before you upload a JavaScript file, configure JavaScript Transporter settings in the Archer Control Panel. For more information, see Configure the JavaScript Transporter Settings.

There are two new data feeds created for this integration that must run in the following order:

1. LexisNexis - Mandates: 01_LexisNexis _-_ Mandates.dfx5
2. LexisNexis – Regulators: 02_LexisNexis _-_ Regulators.dfx5

The following steps set up the feeds:

LexisNexis - Mandates

1. Go to the **Manage Data Feeds** page.
   a. From the menu bar, click  .
   b. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click **Import**.
3. Locate and select the: **01_LexisNexis _-_ Mandates.dfx5** file.
4. Click Open.
5. In the **General Information** tab.
   a. In the **General Information** section, in the **Status** field, select **Active**.
   b. In the **Feed Information** section, verify the Target is **Authoritative Sources -> Source** application.
6. Click the **Transport** tab.
7. In the **Transport Configuration** section, do the following:
   a. Click Upload.
   b. From the Upload JavaScript File dialog, click **Add New**.
   c. Locate and select the **LexisNexisAPI.js** file.
   d. Click Open.
   e. From the **Upload JavaScript File** dialog, click **OK**.
8. In the Custom Parameters section, enter key values. The following table describes the value for each key in Custom Parameters.

Key	Value
url	LexisNexis URL (Required) Ex: https://compliance.store.lexisnexis.com.au
Username	[Valid value]

	Default = [empty] (Required)
Password	[Valid value] Default = [empty] (Required)
ignoreLastRunTime	[Valid value of true/false] Default = true (Optional) Set the value to false if you wish to obtain the response from a specific date. The specific date being the LastRunTime of the data feed.
dataSource	[Valid value] Default = mandates (Required) Note: Do not modify the value. It is being used in the script to identify the Enhanced content.
pageSize	[Valid value] Default = 2000 (Optional) Description: Used to return the count of data from the API. Default value is 100. Maximum value is 2000.

9. The following additional parameter provides valid options for the Custom Parameters section for the current JavaScript file.

Key	Value
proxy	[Valid value] Default = [empty] (Optional)
verifyCerts	[Valid value of true/false] Default = [empty] (Optional)
country	[Valid value] Default = [empty] (Optional) Description: mandate country of origin Ex: Australia, International
level	[Valid value] Default = [empty] (Optional) Ex: Federal, Local, State, Territory or Blank

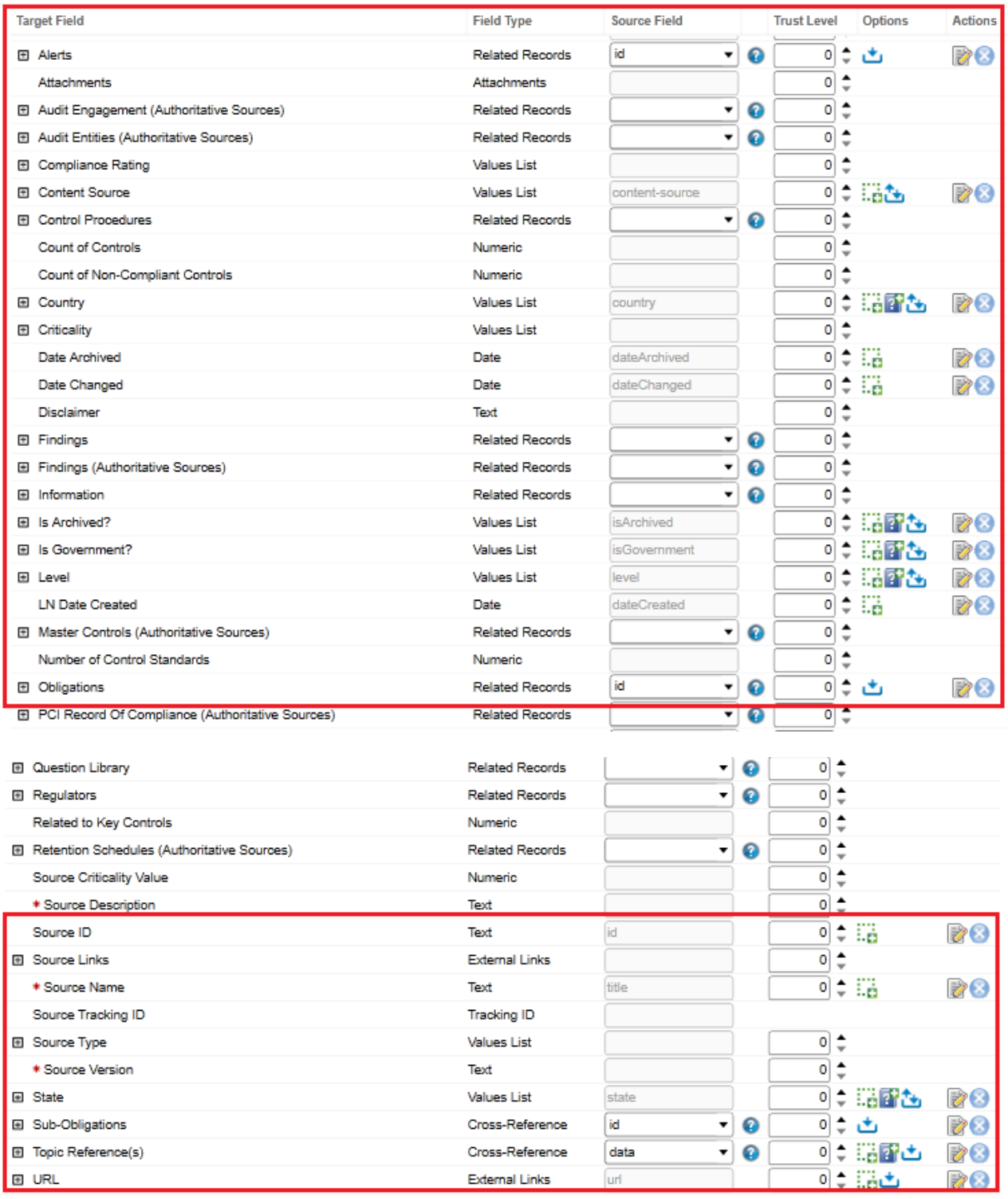
For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log. In the Data Feed Setup window, verify that the key fields are present.

10. Click **Save**.
11. Click the **Data Map** tab.
12. In the **Field Map** sub tab, configure all the source fields (new and modified) to the target Authoritative Sources fields.

Level 1: **Source**

Source Field (Level 1)	Target Field (Source)
content-source	Content Source
country	Country
dateArchived	Date Archived
dateChanged	DateChanged
dateCreated	LN Date Created
isArchived	Is Archived?
isGovernment	Is Government?
level	Level
id	Source ID
title	Source Name
state	State
url	URL
relationships->obligations->data->id	Obligations->Standard ID
relationships->subobligations->data->id	Sub-Obligations->Standard ID
relationships->alerts->data->id	Alerts->LN ID

The screen shows below provide examples of these field mappings.

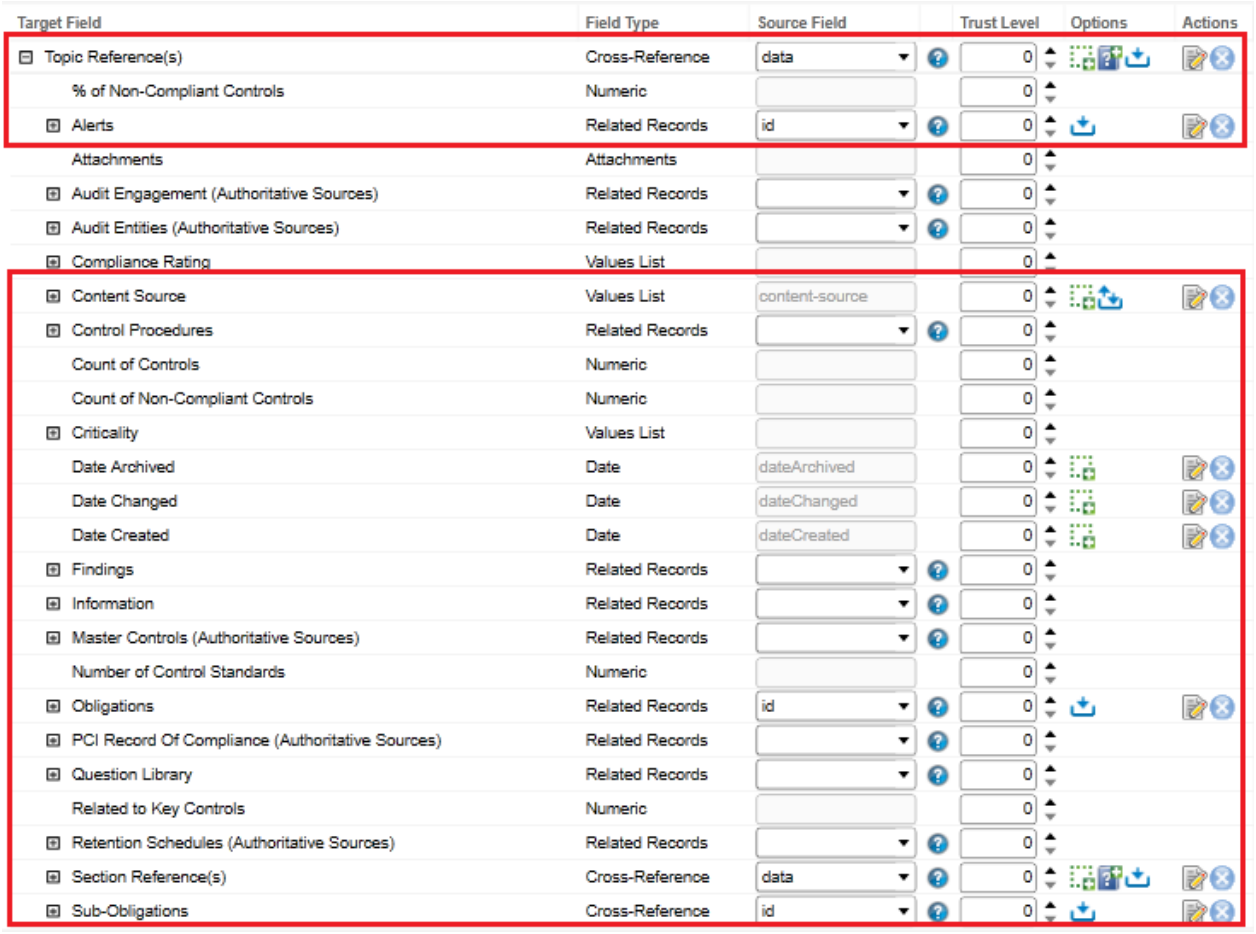


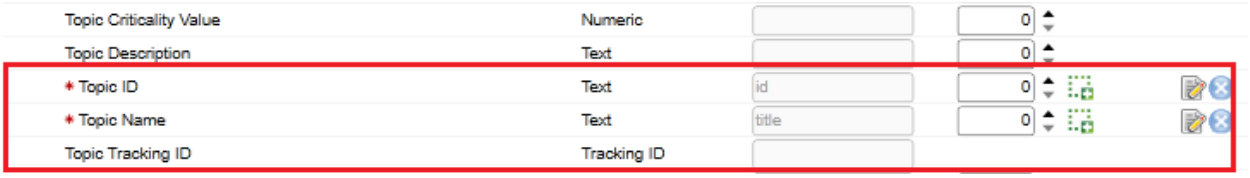
Target Field	Field Type	Source Field	Trust Level	Options	Actions
Alerts	Related Records	id	0		
Attachments	Attachments		0		
Audit Engagement (Authoritative Sources)	Related Records		0		
Audit Entities (Authoritative Sources)	Related Records		0		
Compliance Rating	Values List		0		
Content Source	Values List	content-source	0		
Control Procedures	Related Records		0		
Count of Controls	Numeric		0		
Count of Non-Compliant Controls	Numeric		0		
Country	Values List	country	0		
Criticality	Values List		0		
Date Archived	Date	dateArchived	0		
Date Changed	Date	dateChanged	0		
Disclaimer	Text		0		
Findings	Related Records		0		
Findings (Authoritative Sources)	Related Records		0		
Information	Related Records		0		
Is Archived?	Values List	isArchived	0		
Is Government?	Values List	isGovernment	0		
Level	Values List	level	0		
LN Date Created	Date	dateCreated	0		
Master Controls (Authoritative Sources)	Related Records		0		
Number of Control Standards	Numeric		0		
Obligations	Related Records	id	0		
PCI Record Of Compliance (Authoritative Sources)	Related Records		0		
Question Library	Related Records		0		
Regulators	Related Records		0		
Related to Key Controls	Numeric		0		
Retention Schedules (Authoritative Sources)	Related Records		0		
Source Criticality Value	Numeric		0		
* Source Description	Text		0		
Source ID	Text	id	0		
Source Links	External Links		0		
* Source Name	Text	title	0		
Source Tracking ID	Tracking ID				
Source Type	Values List		0		
* Source Version	Text		0		
State	Values List	state	0		
Sub-Obligations	Cross-Reference	id	0		
Topic Reference(s)	Cross-Reference	data	0		
URL	External Links	url	0		

Level 2: **Topic**

Source Field (Level 2)	Target Field (Topic References)
content-source	Content Source
dateArchived	Date Archived
dateChanged	DateChanged
dateCreated	LN Date Created
id	Topic ID
title	Topic Name
relationships->obligations->data->id	Obligations->Standard ID
relationships->subobligations->data->id	Sub-Obligations->Standard ID
relationships->alerts->data->id	Alerts->LN ID

The screen shows below provide examples of these field mappings.

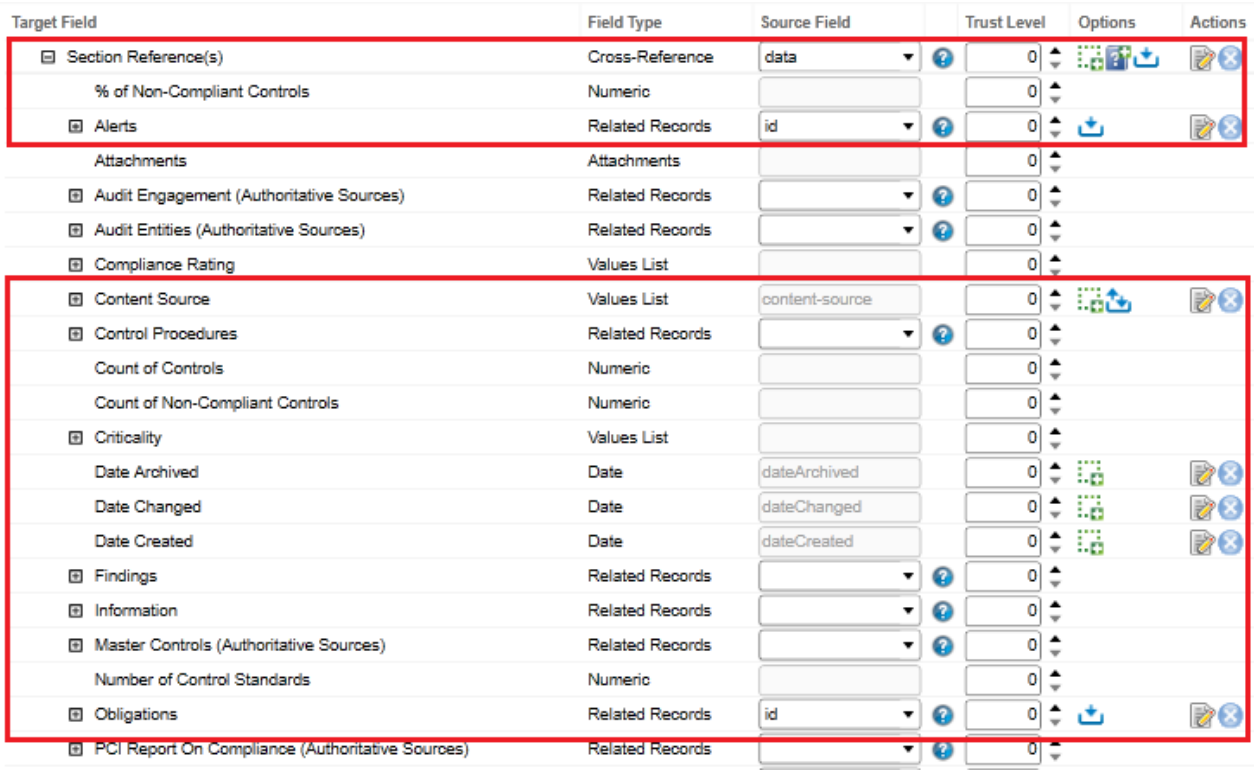


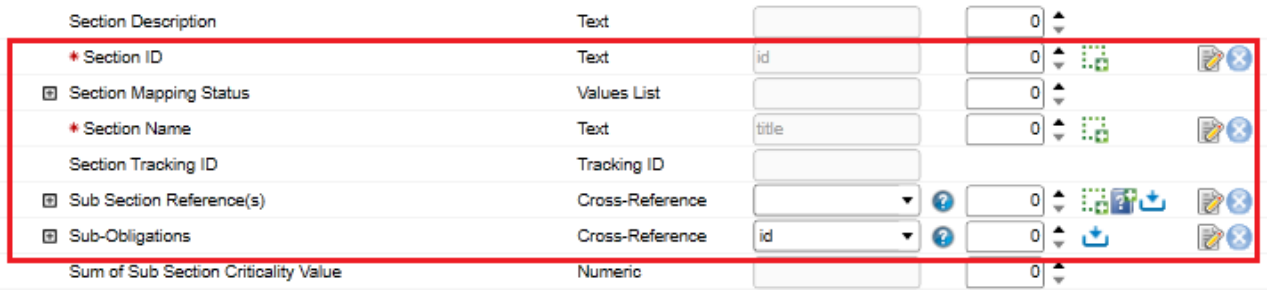


Level 3: **Section**

Source Field (Level 3)	Target Field (Section References)
content-source	Content Source
dateArchived	Date Archived
dateChanged	DateChanged
dateCreated	LN Date Created
id	Section ID
title	Section Name
relationships->obligations->data->id	Obligations->Standard ID
relationships->subobligations->data->id	Sub-Obligations->Standard ID
relationships->alerts->data->id	Alerts->LN ID

The screen shows below provide examples of these field mappings.

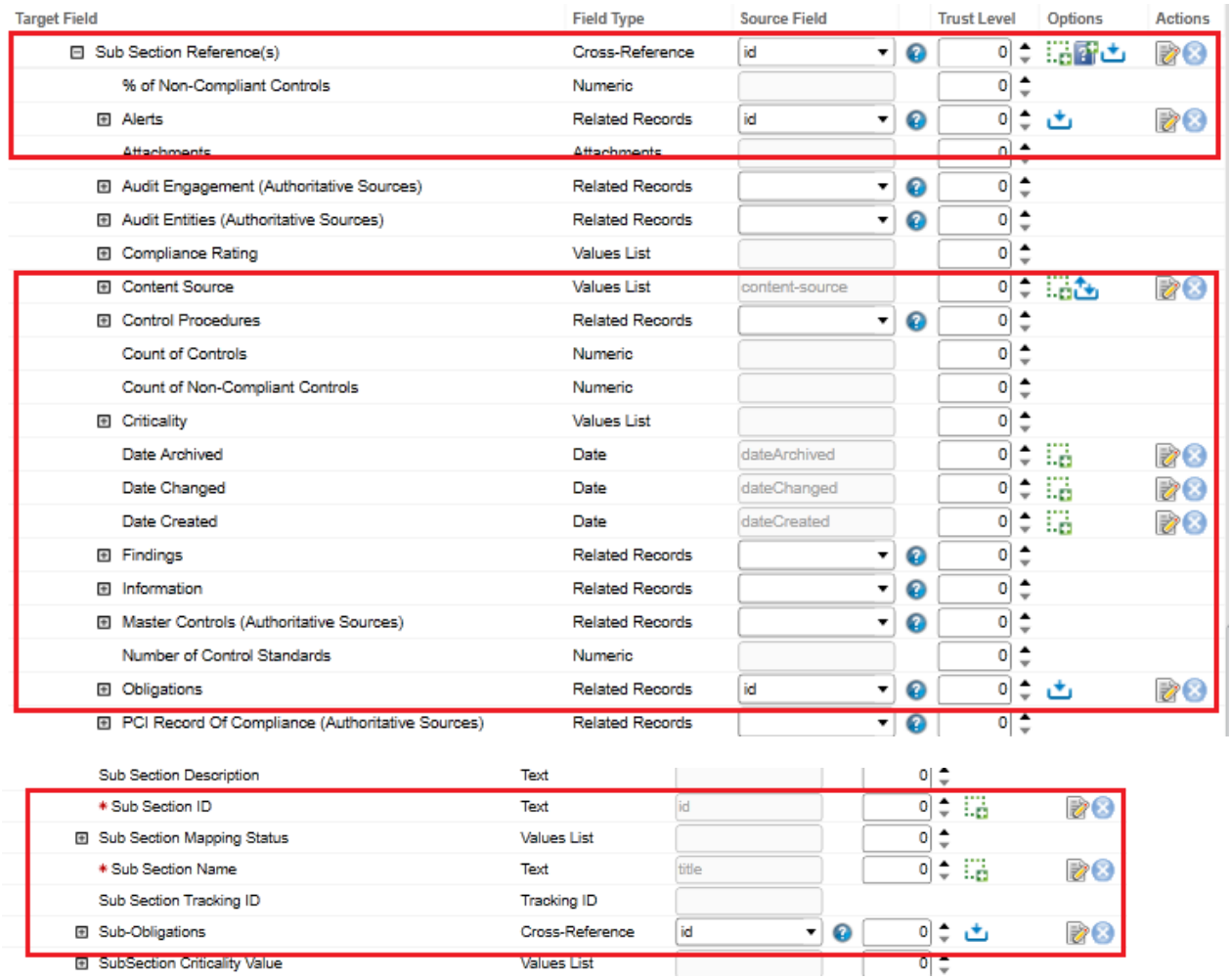




Level 4: **Sub Section**

Source Field (Level 4)	Target Field (Sub Section References)
content-source	Content Source
dateArchived	Date Archived
dateChanged	DateChanged
dateCreated	LN Date Created
id	Sub Section ID
title	Sub Section Name
relationships->obligations->data->id	Obligations->Standard ID
relationships->subobligations->data->id	Sub-Obligations->Standard ID
relationships->alerts->data->id	Alerts->LN ID

The screen shows below provide examples of these field mappings.



13. In the Key Field Definitions Sub tab, add the following as key field for Authoritative Sources application.
    a. Source: Source ID
    b. Topic References(s): Topic ID
    c. Section References(s): Section ID
    d. Sub Section References(s): Sub Section ID

    Reference Fields:
    e. Alerts: LN ID
    f. Obligations: Standard ID
    g. Sub-Obligations: Standard ID

LexisNexis - Regulators

1. Go to the **Manage Data Feeds** page.
    a. From the menu bar, click .
    b. Under Integration, click Data Feeds.

2. In the Manage Data Feeds section, click **Import**.
3. Locate and select the **02_LexisNexis _-_Regulators.dfx5** file.
4. Click Open.
5. In the **General Information** tab.
   a. In the **General Information** section, in the **Status** field, select **Active**.
   b. In the **Feed Information** section, verify the Target is **Regulators** application.

6. Click the **Transport** tab.
7. In the **Transport Configuration** section, do the following:
   a. Click Upload
   b. From the Upload JavaScript File dialog, click **Add New**.
   c. Locate and select the **LexisNexisAPI.js** file.
   d. Click Open.
   e. From the **Upload JavaScript File** dialog, click **OK**.
8. In the Custom Parameters section, enter key values. The following table describes the value for each key in Custom Parameters.

Key	Value
url	LexisNexis URL (Required) Ex: https://compliance.store.lexisnexis.com.au
Username	[Valid value] Default = [empty] (Required)
Password	[Valid value] Default = [empty] (Required)
ignoreLastRunTime	[Valid value of true/false] Default = true (Optional) Set the value to false if you wish to obtain the response from a specific date. The specific date being the LastRunTime of the data feed.
dataSource	[Valid value] Default = regulators (Required) Note: Do not modify the value. It is being used in the script to identify the Enhanced content.
pageSize	[Valid value] Default = 2000 (Optional)

	Description: Used to return the count of data from the API. Default value is 100. Maximum value is 2000.

9. The below additional parameter provides valid options for the Custom Parameters section for the current JavaScript file.

Key	Value
proxy	[Valid value] Default = [empty] (Optional)
verifyCerts	[Valid value of true/false] Default = [empty] (Optional)
country	[Valid value] Default = [empty] (Optional) Description: mandate country of origin Ex: Australia, International
level	[Valid value] Default = [empty] (Optional) Ex: Federal, Local, State, Territory or Blank

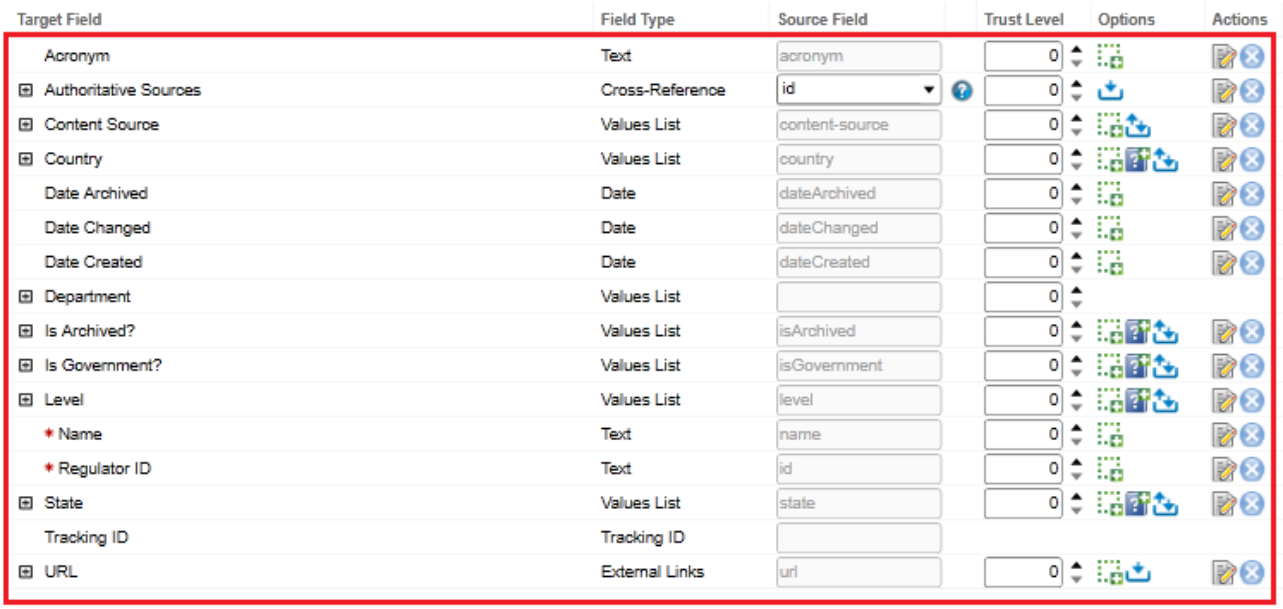
For each key type, determine whether you want it to be Protected or Plain Text. Selecting Protected encrypts the key value for the specified key in the log. In the Data Feed Setup window, verify that the key fields are present.

10. Click **Save**.
11. Click the **Data Map** tab.
12. In the **Field Map** sub tab, configure all the source fields (new and modified) to the target Tools fields.

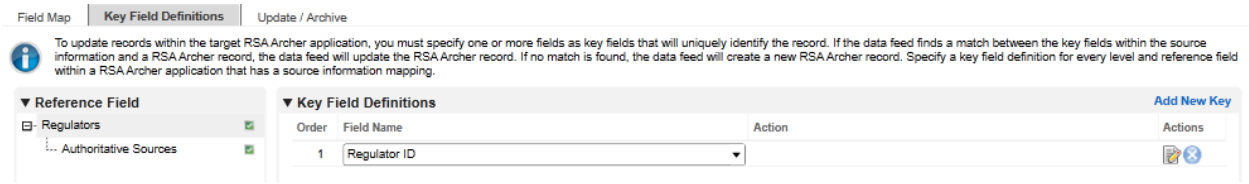
Source Field (Level 1)	Target Field (Source)
acronym	Acronym
content-source	Content Source
country	Country
dateArchived	Date Archived
dateChanged	DateChanged
dateCreated	Date Created

isArchived	Is Archived?
isGovernment	Is Government?
level	Level
id	Regulator ID
name	Name
state	State
url	URL
relationships->mandates->ArcherRecord->id	Authoritative Sources->Source ID

The screen shows below provide examples of these field mappings.



13. In the Key Field Definitions Sub tab, add the “Regulator ID” as key field for Regulators, “Source ID” for Authoritative Sources.



14. Schedule tab: This data feed is a Reference feed configured to run after 01 LexisNexis – Mandates data feed.

Scheduling Data Feeds

When you schedule a data feed, the Data Feed Manager validates the information. If any information is invalid, an error message will display. You can save the data feed and correct the errors later, but that data feed is not processed until the errors are rectified.

Important: A data feed must be active and valid to successfully run.

1. Go to the **Schedule** tab of the data feed that you want to modify.
   a. From the menu bar, click  .
   b. Under **Integration**, click Data Feeds.
   c. Select the data feed you want to modify.
   d. Click the **Schedule** tab.
2. In the **Recurrences** section, enter the frequency, start and stop times, and time zone for the data feed.
3. (Optional) In the Run Data Feed Now section, click Start to override the data feed schedule and run the data feed immediately.
4. Click **Save**.

The following table describes the fields in the **Recurrences** section.

Field	Description
Frequency	Specifies the interval in which the data feed runs. • **By minute:** Runs the data feed by the minute interval set. For example, if you specify 45 in every list, the data feed executes every 45 minutes. • **Hourly:** Runs the data feed by the hourly interval set. For example, every hour (1), every other hour (2), and so forth. • **Daily:** Runs the data feed by the daily internal set. For example, every day (1), every other day (2), and so forth. • **Weekly:** Runs the data feed based on a specified day of the week. For example, every Monday of the first week (1), every other Monday (2), and so forth. • **Monthly:** Runs the data feed based on a specified week of the month. For example, 1st, 2nd, 3rd, 4th, or Last. • **Reference:** Runs a specified data feed as runs before the current one. This option indicates to the Data Feed Service that this data feed starts as soon as the referenced data feed completes successfully. From the Reference Feed list, select after which existing data feed the current data feed starts. A reference data feed will not run when immediately running a data feed. The Data Feed Now option only runs the current data feed.
Every	Specifies the interval of the frequency in which the data feed runs.
Start Time	Specifies the time the data feed begins running.
Start Date	Specifies the date on which the data feed schedule begins.
Time Zone	Specifies the time zone in of the server that runs the data feed.

5. Test the data feed to ensure that all obligation, alerts and tools details from LexisNexis were imported into the Control Standard, Regulatory Intelligence Items and tools application. If testing fails, try verifying the data feed and re-run. If you experience multiple failures, please contact your RSA Partner.

Troubleshooting Guidelines

1. The LexisNexis authentication API does not support concurrent calls. Please ensure when the data feed is configured and executing, no other instances (example: data feeds) is calling the LexisNexis API with the same credentials at the same time.

Appendix A: Certification Environment

Date Tested: December 2020

Product Name	Version Information	Operating System
Archer Suite	6.8	Virtual Appliance
LexisNexis	API v2.0	NA