Archer® Exchange

Archer® Suite

Version 6.7

Implementation Guide

December 2021

Third Party Security Risk Monitoring

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.

August 2021

Revised: December 2021

Table of Contents

Release Notes

What's New

The following table describes enhancements.

Date	Component	Description
December 2021	JavaScript	Re-Signed JavaScript file.
September 2021	Data Feeds	The RiskRecon JavaScript file was updated to add asset criticality and issue priority filtering capabilities. Corresponding updates were made to the TPSRM: Issues and TPSRM: Vendors data feeds that allow the last run time to be passed as a parameter. For more information, see Import the TPSRM: Vendors – JST Data Feed and Import the TPSRM: Issues – JST Data Feed.
August 2020	Data Feeds	The RiskRecon JavaScript file was updated for improved performance, severity filtering capability, and error handling for data feeds. For more information, see Import the TPSRM: Vendors – JST Data Feed and Import the TPSRM: Issues – JST Data Feed.
August 2020	Package Version	The Third Party Security Risk Monitoring package has been updated to 6.7.

Fixed Issues

The following table describes fixed issues.

Date	Component	Description
September 2020	Data Feeds	For customers who have Archer configured to use HTTPS and have a self-signed SSL certificate or another form of non-perfected SSL certificate from a top tier Certificate Authority, data feeds were failing due to validation errors. To resolve this issue, the verifyCerts optional parameter was added to the TPSRM: Vendors – JST data feed and TPSRM: Issues – JST data feed. This parameter is set to 'true' by default, and you must set it to 'false' if you have Archer configured to use HTTPS and have a non-perfected SSL certificate in place.

March 2020	Data Feeds	In Data Feed Manager, if ownEnterprise is set to 'yes' in the Custom Parameters section, the GUIDs for archerReportGUID and archerKeyFieldGUID are hardcoded in the JavaScript file. When you manually create a report in 6.4.1.1, the hardcoded GUID does not match the report GUID. To resolve this issue, the following parameters were added to the TPSRM: Vendors – JST data feed and the TPSRM: Issues – JST data feed: • ownEnterprise = false • archerReportGUIDTP = GUID of the 'TPSRM – Vendors to track' report in Third Party Profile. This value has been pre-populated. • archerKeyFieldGUIDTP = GUID of the 'Security Risk Monitoring ID' field in Third Party Profile. This value has been pre-populated. RSA recommends using the data feeds and JavaScript file added in the package.

Solution Summary

The Archer Third Party Security Risk Monitoring use case, powered by RiskRecon, delivers transparent security measurements, analytics, and analyst-level insight to dramatically improve your third-party risk management program. It provides organizations with visibility, insight and actionable intelligence into their third- and fourth-party IT risk environments. With Third Party Security Risk Monitoring, you can quickly assess the effectiveness of security controls for third parties, without relyingon manual spreadsheet assessments and long emails with no audit trails.

The Archer Third Party Security Risk Monitoring use case discovers and analyzes each third party's IT footprint using artificial intelligence (AI) to automatically measure the value of each asset. This enables analysts to quickly identify each third party's specific systems that pose the greatest risk, based on vulnerability severity and asset criticality. Organizations can leverage the Third Party Security Risk Monitoring use case both as a stand-alone solution for monitoring third-party risk or as the basis for implementing a broader IT and third-party risk management program when deployed with complementary Archer use cases.

Key Features

- Receive an actionable view of security issues for each third party
- Pinpoint potential exposures and root causes for 50+ security criteria
- Obtain on-demand assessments of any organization's security practices
- Demonstrate risk control quality to regulators and standards bodies
- Proactively identify common exposures throughout your third-party portfolio

Key Benefits

- Gain objective insight into your third-party security performance and IT landscape
- Continuously monitor third party security performance
- Optimize use of analysts' time and outside auditor resources
- Allocate risk resources to where they are needed most, to focus on high-value, low-performing third parties
- Engage third parties with accurate, actionable security performance insights and corrective actions

> **!** Important: This document refers to Archer Third Party Security Risk Monitoring, powered by RiskRecon. If you have previously obtained a RiskRecon product license and would like to take advantage of the functionality offered by this integration, you do not need to license Archer Third Party Security Risk Monitoring. You can use your RiskRecon license and complete the instructions in thisguide to enable communication between Archer and your RiskRecon product.
> However, you must have licenses for each of the pre-requisite Archer use cases listed in this guide to make use of the functionality provided by this integration.

Partner Integration Overview	
Archer Solution	Third Party Governance
Archer Use Cases	Third Party Catalog, Third Party Engagement, Issues Management
Archer Applications	Third Party Profile, 4th Parties, Exception Requests
Uses On-Demand Applications	Yes (3)
Requires On-Demand License	Yes

Use Case Components

This section contains high-level use case design information.

Applications

The following table describes the use case applications.

Application	Description
Third Party Profile	The Third Party Profile application is used to store information about each third party included in your business activities. Here, you can assign relationship managers, review associated contracts, and document meetings and activities associated with the relationship. Through the Third Party Profile application, you can: • Understand who your third parties are, what they do for you and who is responsible for the relationship. • Perform business impact analyses, the results of which are used to auto-calculate a third party tier. • Automatically determines which assessments are appropriate for the third party relationship.
Domain Ratings	The Domain Ratings on-demand application collects and tracks individual security domain ratings of third parties. The application integrates with Third Party Security Risk Monitoring to pull in individual scoring metrics across each of their security domains. Through the Domain Ratings application, you can: • Analyze the most recent domain score of the related third party. • Evaluate the domain score over a period of time. • See a heat map of all related issues contributing to the current score (if ingesting issues from Third Party Security Risk Monitoring).
Third Party Scan Results	The Third Party Scan Results on-demand application collects consistent vulnerability scan results delivered by data feed or manual creation. The application natively integrates with Third Party Security Risk Monitoring using data feeds, with the potential for additional integrations. Through the Third Party Scan Results application, you can:

	• Consolidate scan issues across multiple third parties and identify specific security domains and criteria based on scan results. • Auto-notify appropriate personnel when new vulnerability results are identified based on severity. • Follow technical recommendations for each scan result to assist with remediation.
Third Party Tickets	The Third Party Tickets on-demand application provides a method of creating and assigning tickets to specific third party scan results. Third party tickets can consolidate similar scan results based on defined filters such as severity or security domain. The application allows tickets to be assigned to a specific owner, who has one of two ways for addressing a ticket: • Create an Exception Request • Create a Remediation Each ticket includes information from third party scan results as well as roll-up data from any associated Exception Requests or remediation plans.
4th Parties	The 4th Parties application allows you to organize and manage information related to your third party suppliers and subcontractors. It serves as a repository for contact information, and its analytic capability gives you the ability to easily spot and mitigate potential risks.
Exception Requests	The Exception Requests application allows you to manage the process of granting, denying, and expiring exceptions to the remediation required in a third party ticket. Through built-in workflow, the application ensures that all exceptions are properly reviewed. The tool can also report on exceptions across the enterprise, monitoring them by control, department, or severity. Through the Exception Requests application, you can: • Enable employees to submit exception requests through an easy-to-use web interface. • Allow designated individuals to evaluate exception requests and approve or deny the requests based on risk posed to the business.

- Grant exceptions for a specific period of time and notify proper personnel as expiration dates approach.
- Enable management to track granted exceptions, facilitating periodic reviews of exceptions and the exceptions' impact.
- Allow employees to track the status of their own policy exception requests through My Requests reports.
- Understand the policies or standards with the most approved exceptions and use the information to support training and awareness programs.

Note: The Task Management application is not included in the Third Party Security Risk Monitoring package, however, you must configure Task Management settings for task creation and assignment. For more information, see Configure Task Management.

Access Roles and Record Permissions

The following table describes the use case access roles.

Access Roles	Permissions
Third Party: 1st Line of Defense	This role provides CRU access to Third Party Tickets, Third Party Scan Results, and Task Management, and read-only access to Third Party Profile and Domain Ratings for the first line of defense. The first line of defense typically includes Business Unit Owners, Business Unit Managers, and Relationship Managers. In this use case, this role is responsible for submitting third party tickets for exception requests and remediation plans.
Third Party: 2nd Line of Defense	This role provides CRU access to Third Party Tickets, Third Party Scan Results, and Task Management, and read-only access to Third Party Profile and Domain Ratings for the second line of defense. The second line of defense typically includes Business Unit Risk Owners. In this use case, this role is responsible for reviewing third party tickets submitted for remediation plans.
Third Party: Read Only	This role provides read-only access to Third Party Profile, Third Party Tickets, Third Party Scan Results, and Domain Ratings, and CRU access to Task Management.

Dashboards

The following table describes the use case dashboards.

Dashboard	Description
Third Party Security Risk Monitoring Overview	The Third Party Security Risk Monitoring Overview dashboard provides a high-level overview of Security Risk Monitoring ratings for each third party. You can compare overall third party risk ratings or view individual domain ratings. You can also view security findings, ticket status, and commonly used fourth parties to evaluate for risk exposure.
Third Party Security Risk Monitoring Tickets	The Third Party Security Risk Monitoring Tickets dashboard provides ticket owners and ticket reviewers with information about third party tickets. This dashboard includes ticket age, ticket assignments, and ticket status.

Data Feeds

The following table describes the use case data feeds.

Data Feed	Description
TPSRM: Vendors – JST	The TPSRM: Vendors – JST data feed is a JavaScript Transporter feed that imports third and fourth party data. The data feed is preconfigured to create new records when no match is found against the preconfigured data feed key, and to update records when Third Party Security Risk Monitoring performs new scans. If you want to change the preconfigured data feed key, you may do so in the provided XSLT.
TPSRM: Issues – JST	The TPSRM: Issues – JST data feed is a JavaScript Transporter feed that imports issues to the Third Party Profile, Domain Ratings, and Third Party Scan Results applications. The data feed is preconfigured to create new records when no match is found against the preconfigured data feed key, and to update records when Third Party Security Risk Monitoring creates, closes, or updates any issues. If you want to change the preconfigured data feed key, you may do so in the provided XSLT.
TPSRM: Create Task	The optional TPSRM: Create Task data feed is an Archer-to-Archer data feed that creates Task Management records on your company instance when a Ticket Owner creates a remediation for a ticket in the Third Party Tickets application. Source report: Tickets Pending Third Party Task Generation.

TPSRM: Sync Company Tasks to Third Party Instance	The optional TPSRM: Sync Company Tasks to Third Party Instance data feed is an Archer-to-Archer data feed that creates and syncs Task Management records from your company instance to align with the internal version created by the Security Risk Monitoring – Create Task data feed. Source report: A2A: Sync Company Tasks to Third Party Instance. **Note:** This data feed is imported on your third party (external) instance.
TPSRM: Sync Completed Third Party Tasks to Company Instance	The optional TPSRM: Sync Completed Third Party Tasks to Company Instance data feed is an Archer-to-Archer data feed that imports completed third party tasks back to your company instance. Source report: A2A: Sync Completed Third Party Tasks to Company Instance.

Configuring Archer Third Party Security Risk Monitoring

Before You Begin

This section provides instructions for configuring the Archer Third Party Security Risk Monitoringuse case, powered by RiskRecon, 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 in order to install the required components.

> **!** 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.

Obtain the Security Risk Monitoring IDs from Third Party Security Risk Monitoring

You must obtain the Security Risk Monitoring ID for each third party from Third Party Security Risk Monitoring prior to importing and running the data feeds. To obtain the Security Risk Monitoring ID, perform the following steps:

1. Log in to Third Party Security Risk Monitoring.
2. In the search bar at the top of the screen, enter the name of the third party for which you want to obtain the Security Risk Monitoring ID.
3. Go to the Company Profile tab.
4. In the Assessment Configuration section, locate and copy the TOE ID value.
5. Save the TOE ID for later use.
6. Repeat steps 2-5 for each third party you have.
   The Security Risk Monitoring ID (TOE ID) is inserted in the third party profile of each third party you have in Archer. See step 5 of *Insert the Security Risk Monitoring ID (TOE ID) from Third Party Security Risk Monitoring*.

Obtain the API Key from Archer Third Party Security Risk Monitoring

You must obtain an API key from Third Party Security Risk Monitoring prior to configuring the data feeds. To obtain a key, perform the following steps:

1. Log in to Third Party Security Risk Monitoring.
2. Go to My Account ➔ System Administration.
3. Locate the account for which you want to obtain an API key, then click Manage.
4. Select the API Keys tab under the System Administration section.
5. Click New Api Key.
6. Enter a description for the API key.
7. Select a key expiration date.
8. Click Create API Key.
9. Click the clipboard located on the left side of the user account to copy the key to your clipboard, and then save it for later use.
   This API key is used when defining customer parameters for the TPSRM: Vendors – JST and the TPSRM: Issues – JST data feeds. For example, see step 9 of *Import the TPSRM: Vendors – JST Data Feed**.*

Configuring Archer

Before you install the Third Party Security Risk Monitoring package in Archer, you must install all prerequisite use cases and download the following configuration files from the Archer Exchange onRSA Link:

- Archer 6.7 Third Party Security Risk Monitoring Install Package.zip
- TPSRM: Vendors 6.6 – JST.dfx5
- TPSRM: Issues 6.6 – JST.dfx5
- (Optional) TPSRM: Create Task.dfx5
- (Optional) TPSRM: Sync Company Tasks to Third Party Instance.dfx5
- (Optional) TPSRM: Sync Completed Third Party Tasks to Company Instance.dfx5

Note: The TPSRM: Create Task.dfx5, TPSRM: Sync Company Tasks to Third Party Instance.dfx5, and TPSRM: Sync Completed Third Party Tasks to Company Instance.dfx5 data feed files are optional. You only need to import these files if you plan to assign tasks to third party contacts through a secondary external third party instance.

For more information on installing the prerequisite use cases, see “Installing Issues Management,” “Installing Third Party Catalog,” and “Installing Third Party Engagement” in the Archer Online Documentation.

Install the Package

The following tasks detail how to import and install the Third Party Security Risk Monitoring 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. It is strongly recommended to back 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.
4. Locate and select the package that you want to import.
5. Click OK.
   The package file is displayed in the Available Packages section and is ready for installation.

Task 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.

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 map all objects in a tab automatically 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 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 then 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 that 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.
   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 on to 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 Install Packages page.
2. Click the Package Installation Log tab.
3. Click the package that you want to view.
4. 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.

Insert the Security Risk Monitoring ID (TOE ID) from Third Party Security Risk Monitoring

Once you have obtained the Security Risk Monitoring ID (TOE ID) for each third party from Third Party Security Risk Monitoring, you must insert it in each third party profile before you import and run data feeds. To insert the Security Risk Monitoring ID (TOE ID) in Archer, perform the following steps:

1. Open Archer.
2. Go to the Third Party Profile page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Profile.
3. Select the third party for which you obtained the Security Risk Monitoring ID.
4. Click Edit.
5. In the Details tab, insert the Security Risk Monitoring ID (TOE ID) in the Security Risk Monitoring ID field that you saved in step 5 of Obtain the Security Risk Monitoring IDs from Third Party Security Risk Monitoring.
6. In the Track Third Party Rating and Issues? field, do one of the following:
    - Select Yes if you want to track the third party using the Third Party Security Risk Monitoring use case.
    - Select No if you do not want to track the third party.
7. Click Save and Close.
8. Repeat steps 2-7 for each third party.

Configure the JavaScript Transporter Settings

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

1. Open the Archer Control Panel.
2. Go to Instance Management and select All Instances.
3. Select the instance.
4. On the General tab, go to the JavaScript Transporter section.
5. In the Max Memory Limit field, set the value to 2048 MB (2 GB).
6. In the Script Timeout field, set the value to 120 minutes (2 hours).
7. Require Signature is enabled by default on install. Signed Certificate Thumbprints are required for all Hosted clients.
    a. In the Signing Certificate Thumbprints section, add a thumbprint for each digitally signed JavaScript file.
        i. Double-click an empty cell in the Signing Certificate Thumbprints section.
        ii. Enter the digital thumbprint of the trusted certificate used to sign the JavaScript file.
        Note: For more information on how to obtain digital thumbprints, see Digital Thumbprints.

Important: If you enable Require Signature and do not specify thumbprints, JavaScript files will not be accepted by the system.

8. On the toolbar, click Save.

Digital Thumbprints

When running JavaScript data feeds, you can set the system 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.

Obtain a Certificate Thumbprint

1. On the Web Server and Services Server machines, open the Manage Computer Certificates program.
    a. Launch "certmgr" from the Start menu.
    b. Navigate to Certificates – Local Computer > Trusted Root Certification Authorities > Certificates.
2. Verify that the certificate is trusted.
    a. Double-click the Archer Technologies LLC certificate.
    b. In the Certificate window, click the Certification Path tab.

c. 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.

3. Obtain the trusted certificate thumbprint.
   a. In the Certificate window, click the Details tab.
   b. Scroll to and select the Thumbprint field.
   The certificate's digital thumbprint appears in the window.
   c. Copy the thumbprint.
   Note: For information on adding digital thumbprints, see Step 7a of Configure the JavaScript Transporter Settings regarding where thumbprint is relevant.

Configure Task Management

If you want to leverage the Task Management-based integration between your company and third party instances, you must configure settings to function with the Archer Third Party Security Risk Monitoring use case. Task Management is used when you choose to send remediation tasks to third party contacts in your third party instance for response. You only need to configure Task Management ifyou plan to use the following optional data feeds:

- TPSRM: Create Task
- TPSRM: Sync Company Tasks to Third Party Instance
- TPSRM: Sync Completed Third Party Tasks to Company Instance

Note: If you do not want to leverage Task Management to send remediation tasks to your third parties, continue to the data feeds section to set up the required data feeds. For more information, see Set Up Third Party Security Risk Monitoring Data Feeds.

Create Type Values

To leverage Task Management, you must create a Third Party Remediation type value on the company and third party instances.

Create a Third Party Remediation Type Value in the Task Management Application (Company Instance)

1. Log in to your company instance.
2. Go to the Manage Applications page.
   a. From the menu bar, click  .
   b. Under Application Builder, click Applications.
3. Select Task Management.
4. On the Fields tab, select the Type values list field.
5. Click the Values tab.
6. Create a Third Party Remediation value.
   a. Click Add New.

b. In the Text Value field, enter Third Party Remediation.
c. Click Save.

7. Click Save.

Create a Third Party Remediation Type Value in the Task Management Application (Third Party Instance)

1. Log in to your third party instance.
2. Go to the Manage Applications page.
    a. From the menu bar, click  .
    b. Under Application Builder, click Applications.
3. Select Task Management.
4. On the Fields tab, select the Type values list field.
5. Click the Values tab.
6. Create a Third Party Remediation value.
    d. Click Add New.
    e. In the Text Value field, enter Third Party Remediation.
    f. Click Save.
7. Click Save.

Configure Record Permissions

RSA recommends that you create an automatic record permission for Task Management to provide read-only access to members of the Third Party: Read Only group.

1. Log in to your third party instance.
2. Go to the Applications page:
    a. From the menu bar, click  .
    b. Under Application Builder, click Applications.
3. Locate and select Task Management.
4. Click the Fields tab.
5. Click Add New.
6. In the Field Types section, do the following:
    a. Expand the Advanced menu.
    b. Select Record Permissions.
    c. Click OK.
7. In the Name field, enter Read Only Access.
8. Click the Options tab and do the following:
9. In the Permissions section, select Automatic.
10. In the Rules section, click Add New.

11. In the Manage Automatic Selection Rule window, do the following:
    a. In the Rule Name field, enter Type Contains Third Party Remediation.
    b. In the Conditions section, enter the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Type	Contains	Third Party Remediation	N/A

    c. In the Users/Group Permission section, click Lookup.
12. Expand the Groups list, and do the following:
    a. Navigate to Third Party Management.
    b. Expand the Third Party Management list.
    c. Select Third Party: Read Only.
    d. Click OK.
    The Third Party: Read Only group is added to the rule with the Read check box selected.
13. Click Apply.
14. In the Default Users/Groups section, click Lookup.
15. Select Record Creator from the list of Available Users/Groups.
16. Click OK.
17. Click Save.

Add a Third Party Contact to the Third Party: Read Only Group

Once you configure record permissions for the Third Party: Read Only group, you can assign third party contacts to that group when remediating tasks in your third party instance.

1. Log in to your third party instance.
2. Go to the Users page:
    a. From the menu bar, click  .
    b. Under Access Control, click Users.
3. Select the user account you want to add to the Third Party: Read Only group.
4. Click the Groups tab.
5. Click Lookup.
6. Expand the Groups list, and do the following:
    a. Navigate to Third Party Management.
    b. Expand the Third Party Management list.
    c. Select Third Party: Read Only.
    d. Click OK.
7. Click Save.

Create Notifications

RSA recommends creating notifications to alert key stakeholders when tasks have been created and completed.

Create Third Party Remediation Task Creation Notifications

1. Log in to your third party instance.
2. Go to the Applications page:
    a. From the menu bar, click  .
    b. Under Application Builder, click Applications.
3. Locate and select Task Management.
4. Click the Layout tab.
5. Click the Rules tab.
6. Click Add New.
7. Select Create a New Rule from Scratch.
8. In the Name field, enter Notification: Third Party Remediation Task Creation.
9. In the Criteria section, enter the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Record Status	Equals	New	And
Type	Equals	Third Party Remediation	N/A

10. In the Linked Actions section, click Add New.
11. In the Available Action Types section, select Generate Notification.
12. Click OK.
13. In the General Information section, do the following:
    a. In the Name field, enter Notification: Third Party Remediation Task Creation.
    b. Set the Status to Active.
14. In the Template Design section, in the Letterhead field, select Archer Default - Creation.
15. Click the Content tab, and do the following:
    a. In the Subject field, enter "New Third Party Remediation Task:"
    b. In the Toolbar field, select Task ID.
    [Field: Task ID] is added to the subject line.
    c. In the Subject field, after [Field: Task ID], enter "Has Been Assigned"
    d. In the Body field, select the following fields:
        - Task ID
        - Type
        - Due Date
        - Assigned To
        - Description
        - Created by
16. Click the Delivery tab, and do the following:
    a. In the From Address field, enter the email that you want to appear as the notification sender.
    b. In the Frequency field, select Instantly.
    c. In the Email Recipient Options section, select Separate Emails.
    d. In the Recipients section, in the To field, select Assigned To.
    e. Click Save.

17. Click Save.

Create Third Party Remediation Task Reminder Notifications

1. Log in to your third party instance.
2. Go to the Applications page:
    a. From the menu bar, click  .
    b. Under Application Builder, click Applications.
3. Locate and select Task Management.
4. Click the Layout tab.
5. Click the Rules tab.
6. Click Add New.
7. Select Create a New Rule from Scratch.
8. In the Name field, enter Notification: Third Party Remediation Task Reminder.
9. In the Criteria section, enter the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Status	Does Not Equal	Complete	And
Type	Equals	Third Party Remediation	N/A

10. In the Linked Actions section, click Add New.
11. In the Available Action Types section, select Generate Notification.
12. Click OK.
13. In the General Information section, do the following:
    a. In the Name field, enter Notification: Third Party Remediation Task Reminder.
    b. Set the Status to Active.
14. In the Template Design section, in the Letterhead field, select Archer Default - Creation.
15. Click the Content tab, and do the following:
    a. In the Subject field, enter "Third Party Remediation Task Requires Action by"
    b. In the Toolbar field, select Due Date.

    [Field: Due Date] is added to the subject line.

c. In the Body field, select the following fields:

- Task ID
- Type
- Due Date
- Assigned To
- Description
- Created by

16. Click the Delivery tab, and do the following:

a. In the From Address field, enter the email that you want to appear as the notification sender.

b. In the Frequency field, select Reminder.

c. In the Criteria section, RSA recommends entering the following values:

Field	Operator	Days	Target	Occurrence
Due Date	Equals	0	After Today	Once
Due Date	Equals	5	After Today	Once

d. In the Email Recipient Options section, select Separate Emails.

e. In the Recipients section, in the To field, select Assigned To.

f. Click Save.

17. Click Save.

Create Third Party Remediation Task Complete Notifications

1. Log in to your company instance.
2. Go to the Applications page:

a. From the menu bar, click  .

b. Under Application Builder, click Applications.

3. Locate and select Task Management.
4. Click the Layout tab.
5. Click the Rules tab.
6. Click Add New.

7. Select Create a New Rule from Scratch.
8. In the Name field, enter Notification: Third Party Remediation Task Complete.
9. In the Criteria section, enter the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Status	Changed To	Complete	And
Type	Contains	Third Party Remediation	N/A

10. In the Linked Actions section, click Add New.
11. In the Available Action Types section, select Generate Notification.
12. Click OK.
13. In the General Information section, do the following:
    a. In the Name field, enter Notification: Third Party Remediation Task Complete.
    b. Set the Status to Active.
14. In the Template Design section, in the Letterhead field, select Archer Default - Complete.
15. Click the Content tab, and do the following:
    a. In the Subject field, enter “Third Party Remediation Task:”
    b. In the Toolbar field, select Task ID.

       [Field: Task ID] is added to the subject line.

    c. In the Subject field, after [Field: Task ID], enter “has been Completed”
    d. In the Body field, select the following fields:
       - Task ID
       - Type
       - Due Date
       - Assigned To
       - Description
       - Resolution
       - Created by

16. Click the Delivery tab, and do the following:
    a. In the From Address field, enter the email that you want to appear as the notification sender.
    b. In the Frequency field, select Instantly.
    c. In the Email Recipient Options section, select Separate Emails.
    d. In the Recipients section, in the To field, select Created by.
    e. Click Save.
17. Click Save.

Create Reports

You must configure the base reports for the optional TPSRM: Sync Company Tasks to Third Party Instance and TPSRM: Sync Completed Third Party Tasks to Company Instance data feeds.

Create the A2A: Sync Company Tasks to Third Party Instance Report

This report displays all remediation tasks that are created in the company instance and assigned to third party contacts. You must create this report on the company instance.

1. Log in to your company instance.
2. Go to the Task Management workspace.
    a. Click the drop-down arrow next to your username in the top-right corner of the screen.
    b. Click Workspaces Display.
    c. Select the check box next to Task Management.
    d. Click Save.
    e. From the menu bar, select Task Management.
    f. Click  next to Task Management.
3. Click New to create a new report.
4. In the Fields to Display section, add the following fields from Task Management in the Available window to the Selected window:
    - Tracking ID
    - Description
    - Attachments
    - Assigned To
    - Due Date
    - Status
    - Type
5. In the Filters section, enter the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Type	Contains	Third Party Remediation	And
Status	Does Not Equal	Complete	N/A

6. (Optional) In the Sorting section, enter the following values:

Field to Evaluate	Order	Grouping	Relationships
Task ID	Ascending	Disabled	N/A

7. Click Search.
8. Click Save.
9. In the Report Information section, in the Name field, enter A2A: Sync Company Tasks to Third Party Instance.
10. In the Report Type section, in the Permissions field, select Global Report.
11. Click Save.
12. From the search results page, in the Save drop-down menu, click Save Report Changes.
13. In the Report Information section, copy the numeric value from the ID field and save it for use when importing the TPSRM: Sync Company Tasks to Third Party Instance data feed.
    Note: Do not include the braces {} in the copied text.
    This numeric ID is used in the Report field when importing the optional TPSRM: Sync Company Tasks to Third Party Instance Report data feed. See step 9b of [(Optional) Import the TPSRM: Sync Company Tasks to Third Party Instance Data Feed](#).

Create the A2A: Sync Completed Third Party Tasks to Company Instance Report

This report displays all remediation tasks that have been completed by the third party contact. You must create this report on the third party instance.

1. Log in to your third party instance.
2. Go to the Task Management workspace.
   a. From the menu bar, select Task Management.
   b. Click  next to Task Management.
3. Click New to create a new report.
4. In the Fields to Display section, add the following fields from Task Management in the Available window to the Selected window:
   - Subject
   - Status
   - Resolution
   - Completion Date
5. In the Filters section, enter the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Status	Equals	Complete	And
Completion Date	Current	Day	And
Completion Date	Last	3 Days	And
Type	Equals	Third Party Remediation	N/A

6. In the Advanced Operator Logic field, enter 1 AND (2 or 3) AND 4.

7. (Optional) In the Sorting section, enter the following values:

Field to Evaluate	Order	Grouping	Relationships
Task ID	Ascending	Disabled	N/A

8. Click Search.
9. Click Save.
10. In the Report Information section, in the Name field, enter A2A: Sync Completed Third Party Tasks to Company Instance.
11. In the Report Type section, in the Permissions field, select Global Report.
12. Click Save.
13. From the search results page, in the Save drop-down menu, click Save Report Changes.
14. In the Report Information section, copy the numeric value from the ID field and save it for use when importing the TPSRM: Sync Completed Third Party Tasks to Company Instance data feed.
    Note: Do not include the braces {} in the copied text.
    This numeric ID is used in the Report field when importing the optional TPSRM: Sync Completed Third Party Tasks to Company Instance data feed. See step 9b of [(Optional) Import the TPSRM: Sync Completed Third Party Tasks to Company Instance Data Feed](#).

Set Up Third Party Security Risk Monitoring Data Feeds

The Third Party Security Risk Monitoring use case includes five data feeds:

- TPSRM: Vendors 6.6 – JST
- TPSRM: Issues 6.6 – JST
- (Optional) TPSRM: Create Task
- (Optional) TPSRM: Sync Company Tasks to Third Party Instance
- (Optional) TPSRM: Sync Completed Third Party Tasks to Company Instance

Import the TPSRM: Vendors – JST Data Feed

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.

Note: The TPSRM: Vendors – JST Data Feed is scheduled to run daily by default. See Schedule Data Feeds for information about modifying the schedule.

1. Log in to your company instance.
2. Go to the Manage Data Feeds page:
   a. From the menu bar, click  .
   b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM: Vendors 6.6 – JST.dfx5 data feed file.
5. Verify settings in the General tab.

a. In the General Information section, set the Status field to Active.
b. In the Feed Information section, confirm that the Target field is set to Domain Ratings.

6. Click the Transport tab.
7. In the Transport section, in the Transport Method field, select JavaScript Transporter.
8. In the Transport Configuration section, click Upload.
    a. Locate and select the TPSRM_6.6_v1.js JavaScript file.

9. In the Custom Parameters section, enter the following key values:

Key	Value
apiKey	[insert API Key from Third Party Security Risk Monitoring]
archerUrl	[insert the URL of your Archer instance]
archerInstance	[insert the name of your Archer instance]
archerUser	[insert user account name that has read access to all Third Party Profile records] **Note:** You can add this user to the Third Party: Read Only group for access.
archerPass	[insert password for the archerUser account name]
ownEnterprise	[should be set to false for TPSRM]
archerReportGUIDTP	[GUID of the 'TPSRM – Vendors to track' report in Third Party Profile. This value is pre-populated.]
archerKeyFieldGUIDTP	[GUID of the 'Security Risk Monitoring ID' field in Third Party Profile. This value is pre-populated.]
vendorEndpoints	Enter one or more of the following endpoints: • hostEndpoint • descEndpoint • industryEndpoint • subEndpoint By default, this value is set to descEndpoint, industryEndpoint, subEndpoint.

10. The following additional parameters are valid options for the Custom Parameters section:

Key	Type	Value
proxy	Protected	[insert the URL of the proxy server] **Note:** This key should only be entered if you use a proxy server. If you are an Archer Hosted (SaaS) customer,this key is required, and you must contact your Professional Services representative to configure this parameter.
LastRunTime	N/A	[last_retrieved=YYYY-MM-DD] Passed into the vendors feed to retrieve only ratings that have been updated since the last feed execution. Filters results published or updated after the provided date string in format YYYY-MM-DD. Example: To retrieve results updated on or after 2020-11-20, use the following value: last_retrieved=2020-11-20
requestsPerMin	N/A	[Upper threshold of outgoing requests per minute. This value is pre-populated.]
concurrencyLimit	N/A	[Max number of in-flight requests at any given time. This value is pre-populated.]
maxRetry	N/A	[Max number of retries per individual requests. This value is pre-populated.
archerReportLimit	N/A	[Max number of vendors for which you want to retrieve data. This value is pre-populated and set to 1000 by default.]
verifyCerts	N/A	[true] or [false] By default, this value is set to true. If you have configured Archer to use HTTPS, and the SSL certificate is self-signed or is another form of non-perfected SSL certificate from a top tier Certificate Authority, you must set this value to false.

11. Click Save.

> **!** Important: You must run the TPSRM: Vendors – JST data feed before running the TPSRM: Issues – JST data feed.

Import the TPSRM: Issues – JST Data Feed

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.

Note: The TPSRM: Issues – JST Data Feed is scheduled to run daily by default. See Schedule Data Feeds for information about modifying the schedule.

1. Log in to your company instance.
2. Go to the Manage Data Feeds page.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM: Issues 6.6 – JST.dfx5 data feed file.
5. Verify settings in the General tab.
    a. In the General Information section, set the Status to Active.
    b. In the Feed Information section, confirm that the Target field is set to Third Party Scan Results.
6. Click the Transport tab.
7. In the Transport section, in the Transport Method field, select JavaScript Transporter.
8. In the Transport Configuration section, click Upload.
    a. Locate and select the TPSRM_6.6_v1.js JavaScript file.
9. In the Custom Parameters section, enter the following key values:

Key	Value
apiKey	[insert API Key from Third Party Security Risk Monitoring]
minimumSeverity	[severity[]=severitylevel] You must specify each severity level that you want to filter. The following severity levels are available: • Info • Low • Medium • High • Critical Examples: • If you want to retrieve critical and high issues, enter the following value: severity[]=critical&severity[]=high

	• If you only want to retrieve medium issues, enter the following value: severity[]=medium • If you want to retrieve all severity issues, enter the following value: severity[]=info&severity[]=low&severity[]=medium&severity[]=high&severity[]=critical
archerUrl	[insert the URL of your Archer instance]
archerInstance	[insert the name of your Archer instance]
archerUser	[insert user account name that has read access to all Third Party Profile records] **Note:** You can add this user to the Third Party: Read Only group for access.
archerPass	[insert password for the archerUser account name]
ownEnterprise	[should be set to false for TPSRM]
archerReportGUIDTP	[GUID of the 'TPSRM – Vendors to track' report in Third Party Profile. This value is pre-populated.]
archerKeyFieldGUIDTP	[GUID of the 'Security Risk Monitoring ID' field in Third Party Profile. This value is pre-populated.]

10. The following additional parameters are valid options for the Custom Parameters section:

Key	Type	Value
proxy	Protected	[insert the URL of the proxy server] **Note:** This key should only be entered if you use a proxy server. If you are an Archer Hosted (SaaS) customer, thiskey is required, and you must contact your Professional Services representative to configure this parameter.
requestsPerMin	N/A	[Upper threshold of outgoing requests per minute. This value is pre-populated.]
concurrencyLimit	N/A	[Max number of in-flight requests at any given time. This value is pre-populated.]
maxRetry	N/A	[Max number of retries per individual requests. This value is pre-populated.]
archerReportLimit	N/A	[Max number of vendors for which you want to retrieve data. This value is pre-populated and set to 1000 by default.]

Key	Type	Value
verifyCerts	N/A	[true] or [false] By default, this value is set to true. If you have configured Archer to use HTTPS, and the SSL certificate is self-signed or is another form of non-perfected SSL certificate from a top tier Certificate Authority, you must set this value to false.
asset_value	N/A	[asset_value[]=assetlevel] You must specify each severity level that you want to filter. The following severity levels are available: • High • Low • Medium Filters results by asset_value that gets passed into the findings API endpoint. Examples: • If you want to retrieve only high asset values, enter the following value: asset_value[]=high • If you want to retrieve only low asset values, enter the following value: asset_value[]=low • If you want to retrieve only medium asset values, end the following value: asset_value[]=medium

Key	Type	Value
issuePriority	N/A	[priority[]=prioritylevel] You must specify each severity level that you want to filter. The following severity levels are available: • 1 • 2 • 3 Filters results by priority that gets passed into the findings API endpoint. Examples: • If you want to retrieve only an issue of priority 1, enter the following value: priority[] = 1 • If you want to retrieve only an issue of priority of 2, enter the following value: priority[]=2 • If you want to retrieve only an issue of priority 3, enter the following value: priority[]=3

11. Click Save.

(Optional) Import the TPSRM: Create Task Data Feed

This is an optional Archer-to-Archer data feed on your company instance.

1. Log in to your company instance.
2. Go to the Manage Data Feeds page:
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM: Create Task.dfx5 data feed file.
5. Verify settings in the General tab.
    a. In the General Information section, set the Status field to Active.
    b. In the Feed Information section, confirm that the Target field is set to Third Party Tickets.
6. Click the Transport tab.
7. In the Transport section, confirm that the Transport Method field is set to Archer Web Services Transporter.
8. In the Security section, in the URL field, insert the URL to your company instance.
9. In the Transport Configuration section, do the following:
    a. In the Search Type field, confirm that Report ID is selected.

b. In the User Name field, enter the username of a user that has read access to all Third Party Tickets.
Note: You can add this user to the Third Party: Read Only group for access.
c. In the Instance field, enter the name of your company instance.
d. In the Password field, enter the password of the username you provided in the User Name field.

10. If you are an Archer Hosted (SaaS) customer, in the Proxy section, set the Proxy Optionsfield to Use System Proxy.
11. Click Save.

(Optional) Import the TPSRM: Sync Company Tasks to Third Party Instance Data Feed

This is an optional Archer-to-Archer data feed on your third party instance that runs when you choose to assign a task to a third party contact. This data feed creates and syncs Task Management records on your third party instance to match the version on your company instance.

> Important: You must create the A2A: Sync Company Tasks to Third Party Instance report on your company instance before you import this data feed. For more information, see **Create the A2A: Sync Company Tasks to Third Party Instance Report**.

1. Log in to your third party instance.
2. Go to the Manage Data Feeds page:
   a. From the menu bar, click  .
   b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM: Sync Company Tasks to Third Party Instance.dfx5 data feed file.
5. Verify settings in the General tab.
   a. In the General Information section, set the Status field to Active.
   b. In the Feed Information section, confirm that the Target field is set to Task Management.
6. Click the Transport tab.
7. In the Transport section, confirm that the Transport Method field is set to Archer Web Services Transporter.
8. In the Security section, in the URL field, insert the URL to your company instance.
9. In the Transport Configuration section, do the following:
   a. In the Search Type field, confirm that Report ID selected.
   b. In the Report field, insert the report ID that you obtained in step 13 of Create the A2A: Sync Company Tasks to Third Party Instance Report.
   c. In the User Name field, enter a user name of a user who has read-only access to Third Party Remediations.

Note: You can add this user to the Third Party: Read Only group for access. For more information, see Configure Record Permissions.

d. In the Instance field, enter the name of your company instance.
e. In the Password field, enter the password of the username you provided in the User Name field.

10. If you are an Archer Hosted (SaaS) customer, in the Proxy section, set the Proxy Optionsfield to Use System Proxy.
11. Click Save.

(Optional) Import the TPSRM: Sync Completed Third Party Tasks to Company Instance Data Feed

This is an optional Archer-to-Archer data feed on the company instance that syncs completed third party tasks. This data feed pulls information from the third party instance back to the company instance.

> Important: You must create the A2A: Sync Completed Third Party Tasks to Company Instance report on your third party instance before you import this data feed. For more information, see **Create the A2A: Sync Completed Third Party Tasks to Company Instance Report**.

1. Log in to your company instance.
2. Go to the Manage Data Feeds page:
   a. From the menu bar, click  .
   b. Under Integration, click Data Feeds.
3. In the Manage Data Feeds section, click Import.
4. Locate and select the TPSRM: Sync Completed Third Party Tasks to Company Instance.dfx5 data feed file.
5. Verify settings in the General tab.
   a. In the General Information section, set the Status field to Active.
   b. In the Feed Information section, confirm that the Target field is set to Task Management.
6. Click the Transport tab.
7. In the Transport section, confirm that the Transport Method field is set to Archer Web Services Transporter.
8. In the Security section, in the URL field, insert the URL to your third party instance.
9. In the Transport Configuration section, do the following:
   a. In the Search Type field, confirm that Report ID is selected.
   b. In the Report field, insert the report ID that you obtained in step 14 of Create the A2A: Sync Completed Third Party Tasks to Company Instance Report.
   c. In the User Name field, enter a user name of a user who has read-only access to Third Party Remediations.

Note: You can add this user to the Third Party: Read Only group for access. See Configure Record Permissions for more information.

d. In the Instance field, enter the name of your third party instance.
e. In the Password field, enter the password of the username you provided in the User Name field.

10. If you are an Archer Hosted (SaaS) customer, in the Proxy section, set the Proxy Optionsfield to Use System Proxy.
11. Click Save.

Schedule Data Feeds

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

As you schedule your data feed, the Data Feed Manager validates the information. If any information is invalid, an error message displays. You can save the data feed and correct the errors later; but the data feed does not process until you make corrections.

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.
   d. Click the Schedule tab.
2. Go to the Recurrences section and complete frequency, start and stop times, and time zone. The following table describes the fields in the Recurrences section.

Field	Description
Frequency	Specifies the interval in which the data feed runs, for example, Minutely, Hourly, Daily, Weekly, Monthly, or Reference. • Minutely. Runs the data feed by the interval set. For example, if you specify 45 in the Every list, the data feed executes every 45 minutes. • Hourly. Runs the data feed by the interval set, for example, every hour (1), every other hour (2) and so forth. • Daily. Runs the data feed by the interval 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.

	• Recurrence. 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. For example, you can select to have a Threats data feed run immediately after your Assets data feed finishes. 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 Run 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 starts 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.

3. (Optional) To override the data feed schedule and immediately run your data feed, in the Run Data Feed Now section, click Start.
4. Click Save.

Edit the XSLT

XSLT is a language used for transforming the structure or format of XML documents. XSLT is used to manipulate XML documents into a format that can be properly ingested into Archer. When the Third Party Security Risk Monitoring use case, powered by RiskRecon, adds new security domains to monitor, you must modify the XSLT contained in the TPSRM: Vendors – JST and TPSRM: Issues – JST datafeeds to account for the changes.

Modify the XSLT in the TPSRM: Vendors – JST Data Feed

The XSLT contained in the TPSRM: Vendors – JST data feed is used to split records in the XML into individual records for each Security Domain. These individual records are populated in the Domain Ratings application and linked back to the master record contained in the Third Party Profile application.

> **!** Important: RSA recommends using an API development environment to make an API call to RiskRecon to determine the naming convention used for the new security domain and how it is referenced in the Rating and Web Directory nodes.

1. Log in to your company instance.
2. Go to the Manage Data Feeds page.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
3. Locate and select the TPSRM: Vendors – JST.dfx5 data feed file.
4. Click the Navigation tab.
5. Go to the Xml File Definition section and do the following:
    a. Press CTRL+A to select all the text in the XSLT.
    b. Press CTRL+C to copy all the text in the XSLT.
6. Open an external text editor.
7. Paste the text in the external text editor.
8. Save the file with a new file name to prevent overwriting the original XSLT.
9. To add a new security domain, copy the text beginning with <!--CREATE RECORD FOR WEB ENCRYPTION DOMAIN--> and ending with the </Record> tag before <!--CREATE RECORD FOR WEB APPLICATIONS DOMAIN-->. Using the out-of-the-box XSLT, this represents lines 8-87.
10. Paste the text you copied in step 9 to just after the closing </Record> tag on line 807.
    Note: The </xsl:for-each> command on line 808 should remain on the line directly after the text that you just pasted.
11. Change the newly pasted text that says <!--CREATE RECORD FOR WEB ENCRYPTION DOMAIN--> to <!--CREATE RECORD FOR *INSERT NEW DOMAIN TITLE HERE* DOMAIN-->.
    - For example, if the new security domain was titled Network Filtering, make the following revision:

      <!--CREATE RECORD FOR NETWORK FILTERING DOMAIN-->

12. Change the text between the <Risk_Recon_Domain> and </Risk_Recon_Domain> tags to the title of the new security domain.
    - For example, if the new security domain was titled Network Filtering, make the following revision:

      <Risk_Recon_Domain>Network Filtering</Risk_Recon_Domain>

13. Change the text between the <Rating> and </Rating> tags to incorporate the title of the new security domain. You must use all lowercase letters with an underscore (_) between words.
    - For example, if the new security domain was titled Network Filtering, make the following revision:

      <Rating>
      <xsl:value-of: select="network_filtering_rating"/>
      </Rating>

14. Change the text between the <Web_Directory> and </Web_Directory> tags to incorporate the title of the new security domain. You must use all lowercase letters with an underscore (_) between words.
    - For example, if the new security domain was titled Network Filtering, make the following revision:

      <Web_Directory>
      network_filtering
      </Web_Directory>

15. Save the file in the external text editor.
16. Press CTRL+A to select all the text.
17. Press CTRL+C to copy all the text.
18. Reopen the Archer window that you had open in step 5.
19. In the Xml File Definition section, press CTRL+A to select the original XSLT.
20. To overwrite the original XSLT, press CTRL+V to paste the modified XSLT.
21. Click Save.

Modify the XSLT in the TPSRM: Issues – JST Data Feed

The XSLT contained in the TPSRM: Issues – JST data feed is used to modify the format of the XML that contains the issues linked to each Security Criteria and Security Domain. It also converts the data contained in the securityDomain node into a name appropriate for Archer.

> **!** Important: RSA recommends using an API development environment to make an API call to RiskRecon to determine the naming convention used for the new security domain and how it is referenced in the Rating and Web Directory nodes.

1. Log in to your company instance.
2. Go to the Manage Data Feeds page.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
3. Locate and select the TPSRM: Issues – JST.dfx5 data feed file.
4. Click the Navigation tab.
5. Go to the Xml File Definition section and do the following:
    a. Press CTRL+A to select all the text in the XSLT.
    b. Press CTRL+C to copy all the text in the XSLT.
6. Open an external text editor.
7. Paste the text in an external text editor.
8. Save the file with a new file name to prevent overwriting the original XSLT.

9. Navigate to the beginning of the <xsl:choose> loop contained on line 255 of the out-of-the-box XSLT.
   Note: Within this loop, Archer tests the value returned in the securityDomain node. Depending on that value, Archer assigns specific text to the RiskReconDomain variable.
10. Copy the following three lines of code that begin on line 256 and end on line 258:

```
<xsl:when test="$securityDomain='software_patching'">
        <xsl:value-of select="'Software Patching'"/>
</xsl:when>
```

11. Paste the three lines of code from step 10 after the </xsl:when> tag on line 294 and before the </xsl:choose> tag on line 295.
12. In the lines of code you pasted in step 11, change the text after "$securityDomain= to incorporate the new security domain. You must use all lowercase letters with an underscore (_) between words.
    - For example, if the new security domain was titled Network Filtering, make the following revision:

```
<xsl:when test="$securityDomain='network_filtering'">
```

13. Change the text after the <xsl:value-of select="' text to incorporate the new security domain.
    - For example, if the new security domain was titled Network Filtering, make the following revision:

```
<xsl:value-of select="'Network Filtering'"/>
```

14. After making these changes, the new lines of text should look like the following text:

```
<xsl:when test="$securityDomain='network_filtering'">
        <xsl:value-of select="'Network Filtering'"/>
</xsl:when>
```

15. Save the file in the external text editor.
16. Press CTRL+A to select all the text.
17. Press CTRL+C to copy all the text.
18. Reopen the Archer window that you had open in step 5.
19. In the Xml File Definition section, press CTRL+A to select the original XSLT.
20. To overwrite the original XSLT, press CTRL+V to paste the modified XSLT.
21. Click Save.

Using Third Party Security Risk Monitoring

You can use the Archer Third Party Security Risk Monitoring use case to track the risk ratings foryour third parties and manage third party scan results.

Review Risk Ratings

You can review an up-to-date security risk overview of any third party to inform decisions about whether your company should initiate or continue your business relationship with that third party. Ratings are based on a scale from 0-10, with 0 being the worst and 10 being the best. The rating information is updated nightly through the TPSRM: Vendors - JST data feed. Third Party Security Risk Monitoring runs updated scans approximately every 2-4 weeks for each third party.

1. Go to the Third Party Profile page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Profile.
2. Select the third party that you want to review.
3. Go to the Risk Ratings tab.
4. In the Security Risk Monitoring Rating Details tab, review the following third party details:
    - Company Description
    - Industry
    - Industry Average
    - Percentile Rank
    - Overall Security Risk Monitoring Rating
5. Select the Overall Security Risk Monitoring Rating to open the third party profile in Third Party Security Risk Monitoring, where you can review the risk rating in more detail.
6. In the Security Risk Monitoring Trend & Heat Map section, review the following third party details:
    a. Overall Rating Trend. A visual representation of a third party's overall Third Party Security Risk Monitoring risk rating over time. The scoring trends allow you to view periods of inclining or declining ratings and address them with your third parties as needed.
    b. Third Party Scan Results heat map. A visual representation of the severity and criticality of all open issues for a third party. To open the Third Party Scan Results Heat Map report, do the following:
        i. Click Display Report.
        ii. Select a number on the heat map to display the third party scan results matching that asset value and severity level.
7. In the Domain Ratings section, review the individual security domain ratings for the security areas.

8. To review more detailed information about an individual domain rating, click the link under the Domain Rating ID column. This opens the individual domain rating in the Domain Ratings application.

> **!** Important: When new security domains are added by Third Party Security Risk Monitoring, you must modify the XSLT contained in the TPSRM: Vendors – JST and TPSRM: Issues – JST data feeds to account for the changes. For more information, see **Edit the XSLT**.

9. In the Additional Information tab, review the following third party details:
    a. Security Risk Monitoring Subsidiaries
    b. Hosting locations
10. Go to the 4th Parties tab to view the fourth parties that provide hosting services to the third party you are reviewing.
11. To review more detailed information about an individual fourth party, click the link under the 4th Party Name column. This opens the individual fourth party record in the 4th Parties application.

Manage Third Party Scan Results

Third Party Security Risk Monitoring identifies third party vulnerability issues and ingests that data into Third Party Scan Results through a nightly data feed. You can view the scan results repository to triage issues for response from your third parties. Additionally, you can link third party scan results to tickets and enter the tickets into the Third Party Tickets advanced workflow.

Note: Archer automatically sets the overall status of a Third Party Scan Result vulnerability issue to 'Verified' if the Last Seen date is older than 60 days.

Create Tickets

There are multiple options for creating and linking tickets to third party scan results:

- Bulk Action
    - Scheduled bulk create references (recommended method)
    - On-demand bulk action
    - On-demand bulk update
- Inline Edit
- Manual Ticket Creation

Create Tickets Using Bulk Action

Bulk actions enable you to take an action on multiple records in a single application simultaneously.

Create a Scheduled Bulk Create Reference (recommended method)

RSA recommends scheduling bulk create references to automatically link third party scan results to tickets. The bulk create reference evaluates all third party scan results that meet your defined filter criteria, and then it groups the scan results into tickets on a scheduled basis. You can create multiple bulk create references for different filter criteria.

Complete the following steps to schedule a bulk create reference:

1. Go to the Third Party Scan Results page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Scan Results.
2. Click  , and click Schedules.
3. Click Add New to add a new bulk action schedule.
4. Complete the General Information section.
5. (Optional) In the Notifications section, choose when you want the system to send notifications.
6. In the Recurrences section, schedule the frequency and time you want to run the bulk create reference.

> **!** Important: This schedule correlates with the TPSRM: Issues – JST data feed. Archer recommends that you set the Frequency to the same as or less than the frequency of the TPSRM: Issues – JST data feed and set the Start Time to a later start time than the data feed.

7. In the Filters section, RSA recommends entering the following values:

Field to Evaluate	Operator	Value(s)	Relationships
Severity	Contains	High, Critical	And
Vendor	Does Not Equal	No Selection	And
New Ticket Required?	Contains	Yes	N/A

> **!** Important: The values you enter in the Severity field correlate to the custom parameters you entered when you imported the TPSRM: Issues – JST data feed. For example, if you entered "severity[]=Medium&severity[]=High&severity[]=Critical" as the key value for minimumSeverity in the data feed, and enter "High, Critical" as the values for Severity in the bulk create reference, then the data feed will ingest medium, high, and critical issues, but the bulk action will filter out the medium issues and only create tickets for high and critical issues.

8. Click Save.
9. In the Bulk Actions section, click Add New.
10. In the General Information section, do the following:
    a. Enter a name for the bulk action.
    b. Enter an alias.
    c. Set the Status to Active.
    d. (Optional) Enter a description for the bulk action.
11. In the Group By field of the Bulk Create Configuration section, RSA recommends that you select the following fields: Security Criteria, Vendor, and Security Domain.

12. In the Field Value Expression section, RSA recommends entering the following values:

Field	Operator	Value(s)
Security Criteria	Mapped	Security Criteria
Security Domain	Mapped	Security Domain
Ticket Owner	Static	[user]
Vendor	Mapped	Vendor

13. Click Save.
14. Click  to close out of Manage Bulk Action and return to Manage Bulk Schedule screen.
15. When you are finished making changes to the scheduled bulk action, click Save and then click  .

    The bulk action automatically runs on a scheduled basis by grouping third party scan results into new tickets based on the filters you set.

Create an On-Demand Bulk Action

Similar to a scheduled bulk create reference, an on-demand bulk action is a bulk action that allows you to select a batch of third party scan results to triage into tickets. Instead of running on a schedule, an on-demand bulk action allows you to create one-time bulk actions as needed.

Complete the following steps to create an on-demand bulk action:

1. Go to the Third Party Security Risk Monitoring Tickets dashboard.
    a. From the menu bar, click Third Party Governance.
    b. Under Dashboards, select Third Party Security Risk Monitoring Tickets.
2. In the Unassigned Third Party Scan Results iView, click the vertical bar that represents the third party for which you want to link unassigned scan results to tickets.
3. Select the records for which you want to perform an on-demand bulk create.
4. In the Options drop-down menu, select Enable Bulk Create.
   Note: A warning message appears if you select a record that exceeds the limit of 1000 for selecting individual records. You can only apply bulk actions to all search results if the search results exceed 1000. You can lower the number by clicking Modify in the report to modify your search criteria.
5. Select the third party scan results that you want to evaluate and group together.
6. Click Create New Reference.
7. In Reference Field, select Third Party Tickets.
8. Specify the grouping criteria to evaluate the third party scan results and logically group them. For example, you could group third party scan results by Vendor, Security Domain, and Security Criteria.
9. Enter a value for the Ticket Owner.
10. Click Submit.

The system creates the tickets and enrolls them into the Third Party Tickets advanced workflow. The tickets are assigned to the ticket owner specified in step 9.

Perform an On-Demand Bulk Update

On-demand bulk update allows you to update a large selection of existing records.

Complete the following steps to perform an on-demand bulk update:

1. Go to the Third Party Security Risk Monitoring Tickets dashboard.
    a. From the menu bar, click Third Party Governance.
    b. Under Dashboards, select Third Party Security Risk Monitoring Tickets.
2. In the Unassigned Third Party Scan Results iView, click the vertical bar that represents the third party for which you want to link unassigned scan results to tickets.
3. Select the records for which you want to perform an on-demand bulk update.
4. In the Options drop-down menu, select Enable Bulk Update.
   Note: A warning message appears if you select a record that exceeds the limit of 1000 for selecting individual records. You can only apply bulk actions to all search results if the search results exceed 1000. You can lower the number by clicking Modify in the report to modify your search criteria.
5. Update existing records as needed.
6. Click Save Changes.

Update Tickets Using Inline Edit

Inline edit allows you to link third party scan results to existing tickets in a line-by-line process. Inline editing is useful when you only want to update a small number of tickets. If you want to create or update tickets on a larger scale, RSA recommends using bulk action.

Complete the following steps to perform an inline edit:

1. Go to the Third Party Security Risk Monitoring Tickets dashboard.
    a. From the menu bar, click Third Party Governance.
    b. Under Dashboards, select Third Party Security Risk Monitoring Tickets.
2. In the Unassigned Third Party Scan Results iView, click the vertical bar that represents the third party for which you want to link unassigned scan results to tickets.
3. Select the records for which you want to perform an inline edit.
4. In the Options drop-down menu, select Enable Inline Edit.
5. Update individual third party scan results as needed.
6. Click Save.

Create Tickets Manually

If you want to create a ticket for a third party scan result, you can do it manually through the Third Party Scan Results application. This option only allows you to link one third party scan result to one new ticket. Manual ticket creation is not recommended if you have several third party scan results that you want triaged through ticketing.

Complete the following steps to manually create a ticket for a third party scan result:

1. Go to the Third Party Scan Results page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Scan Results.
2. Locate and select the scan result that you want to add a ticket to.
3. In the Third Party Tickets section, click Add New.
4. Complete the General Information section.
5. In the Stakeholders section, assign a Ticket Owner and Ticket Reviewer.
6. (Optional) In the Comments section, add any comments that are applicable to the ticket.
7. Click Save.
   The saved ticket is enrolled in the Third Party Tickets advanced workflow and is assigned to the Ticket Owner as specified in the Stakeholders section.

Manage Third Party Tickets

Once a ticket is created and saved, it enters the Third Party Tickets advanced workflow where you can manage your tickets to completion.

Review Third Party Tickets

User: Ticket Owner

When a third party ticket is created, you must decide whether to accept it, reject it, or reassign the ticket to another Ticket Owner.

1. Go to the Third Party Tickets page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Tickets.
2. Select the ticket you want to review.
3. Review all the sections of the ticket.
4. Do one of the following:
    - Accept the ticket. Click Accept.
      The ticket is accepted and can then be routed through the appropriate remediation path.

- Reject the ticket. Click Reject.
  The ticket is sent to the Ticket Reviewer to confirm the cancelation or re-insert into the workflow by submitting changes.

- Reassign the ticket. Click Reassign.
  The ticket opens in Edit mode and you can assign a new Ticket Owner. Once complete, click Assign Ticket, and the system notifies the new Ticket Owner.

Resolve Accepted Tickets

User: Ticket Owner

Once a ticket has been accepted, you must decide how to resolve it.

1. Go to the Third Party Tickets page.
   a. From the menu bar, click Third Party Governance.
   b. Click Third Party Catalog.
   c. Click Third Party Tickets.
2. Select the ticket you want to resolve.
3. Click Edit.
4. Review the ticket details.
5. Do one of the following:
   - Click Create Exception Request to create an exception request for the ticket.
     A new Exception Requests section is added to the bottom of the ticket. In the Exception Requests section, you can link an existing exception request to the ticket or create a new one. Once the exception has been submitted, the exception request is sent to the Ticket Reviewer for evaluation.

     For more information, see "Managing Exception Requests" in the Archer Issues Management use case documentation.

   - Click Reassign Ticket to reassign the ticket.
     The ticket opens in Edit mode, and you can assign a new Ticket Owner. Once complete, click Assign Ticket, and the system notifies the new Ticket Owner.

   - Click Reject to reject the ticket.
     The ticket is sent to the Ticket Reviewer to confirm the cancelation or re-insert into the workflow by submitting changes.

   - Click Create Remediation Plan to complete a remediation for the ticket.
     A new Remediation Details section is added to the bottom of the ticket. See Manage Remediations for more information.

Manage Remediations

When a Ticket Owner chooses to resolve a ticket through remediation, a new Remediation Details section is added to the ticket to provide information about the remediation. A ticket can be remediated internally on your company instance or externally on your third party instance by a third party contact.

Create an Internal Remediation on the Company Instance

User: Ticket Owner

To create a remediation on your company instance, do the following:

1. Log in to your company instance.
2. Go to the Third Party Tickets page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Tickets.
3. Select the ticket for which you want to create an internal remediation.
4. Click Edit.
5. Go to the Remediation Details section.
6. Enter any relevant information.
7. Confirm that the Send Task to Third Party? field is set to No.
8. Do one of the following:
    - If you are prepared to submit the remediation for review, click Submit for Review.
    - If you want to commit your changes but not send the remediation for review, click Save or Save and Close.

Create an External Remediation for the Third Party Instance

User: Ticket Owner

If you want a third party contact to remediate a ticket, you can send a remediation task to them from your company instance to your third party instance. The TPSRM: Create Task data feed creates tasks for third party contacts. Then the TPSRM: Sync Company Tasks to Third Party Instance data feed pulls task information to the third party instance. When the task is complete, the TPSRM: Sync Completed Third Party Tasks to Company Instance data feed pulls the task information back to the company instance.

> **!** Important: To send a remediation task to a third party contact, you must have a third party instance set up with user accounts for your third party contacts. The TPSRM: Create Task and the TPSRM: Sync Completed Third Party Tasks to Company Instance data feeds must be imported on your company instance, and the TPSRM: Sync Company Tasks to Third Party Instance data feed must be imported on your third party instance.

1. Log in to your company instance.
2. Go to the Third Party Tickets page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.

c. Click Third Party Tickets.

3. Select the ticket for which you want to create an external remediation.
4. Click Edit.
5. In the Remediation Details section, do the following:
    a. In the Expected Remediation Date field, enter a date for which you expect the ticket to be remediated.
    b. In the Requested Remediation Details field, enter information that you want the third party contact to review.
    c. In the Send Task to Third Party? field, select Yes.
    d. In the Third Party Contact(s) field, select the third party contact for which you want to assign the remediation task.
    Note: The third party contact must have a user account created on both the company and third party instances. The usernames must match.
6. (Optional) In the Third Party Attachments section, create and attach a detailed report to the ticket.
    Note: RSA recommends that you create and attach a report that includes all relevant details for each issue to ensure that the third party contact understands each item they need to resolve.
    a. In the Third Party Scan Results section, click Display Report to view a report that details the third party scan results attached to the ticket.
    b. Click Export.
    c. Select the file format for which you want to export the report.
    d. Once the export is complete, select Click Here.
    e. In the window at the bottom of the screen, click Save As.
        i. Enter a file name and select the location to store the file.
        ii. Click Save.
    f. In the Third Party Attachments section, click Add New.
    g. Locate and select the file you want to attach.
    h. Click Open.
    i. Click OK.
6. Do one of the following:
    - Click Submit for Review. For more information, see Submit a Ticket for Approval.
    - Click Save or Save and Close.
    If you have set up notifications for Task Management in Create Notifications, the system sends an email notification to the third party contact about the creation of a remediation task. The task is assigned to the third party contact in the third party instance through the TPSRM: Sync Company Tasks to Third Party Instance data feed. The system also sends email notifications to the third party contact as the task approaches the due date. When the third party contact completes the task, the system notifies the Ticket Owner and it gets sent back to the company instance through the TPSRM: Sync Completed Third Party Tasks to Company Instance data feed.

Submit a Ticket for Approval

User: Ticket Owner

You can submit a ticket to a Ticket Reviewer for approval before or after all tasks are complete.

If you click Submit for Review on a ticket before all tasks are complete, the ticket remains in a hold status until all tasks are completed. You will not have to Submit for Review again. Instead, the system automatically removes the ticket from a holding state and sends the ticket to the Ticket Reviewer once all tasks are complete.

If you want to wait until all tasks are complete, submit a ticket by opening it in Edit mode and verify that all tasks are closed. Make changes as needed, and then click Submit for Review.

The ticket is sent to the Ticket Reviewer for approval.

Review a Remediated Ticket

User: Ticket Reviewer

When a remediation is created for a ticket, the Ticket Reviewer must decide whether to approve it, reject it, make an update, or reassign the ticket to another Ticket Owner.

1. Go to the Third Party Tickets page.
    a. From the menu bar, click Third Party Governance.
    b. Click Third Party Catalog.
    c. Click Third Party Tickets.
2. Select the ticket you want to review.
3. Click Edit.
4. Review the Remediation Details section.
5. Do one of the following:
    - Click Approve to approve the remediation.
      The remediation is approved. Once the remediation is verified, the ticket is closed.

    - Click Reject Plan to reject the remediation.
      The ticket is sent back to the Ticket Owner for them to decide whether to create an exception request, reassign the ticket, reject the ticket, or create a new remediation plan.

    - Click Update Remediation Plan to ask for more details about the remediation.
      The ticket is sent back to the Ticket Owner to provide additional details about the remediation plan.

- Click Reassign to reassign the ticket.
  The ticket opens in Edit mode, and you can then choose a new Ticket Owner. Once complete, click Assign Ticket, and the system notifies the new Ticket Owner.

Certification Environment for Archer

Date Tested: August 2021

Certification Environment		
Product Name	**Version Information**	**Operating System**
Archer GRC	6.7	Virtual Appliance
RiskRecon	August 2021	SaaS