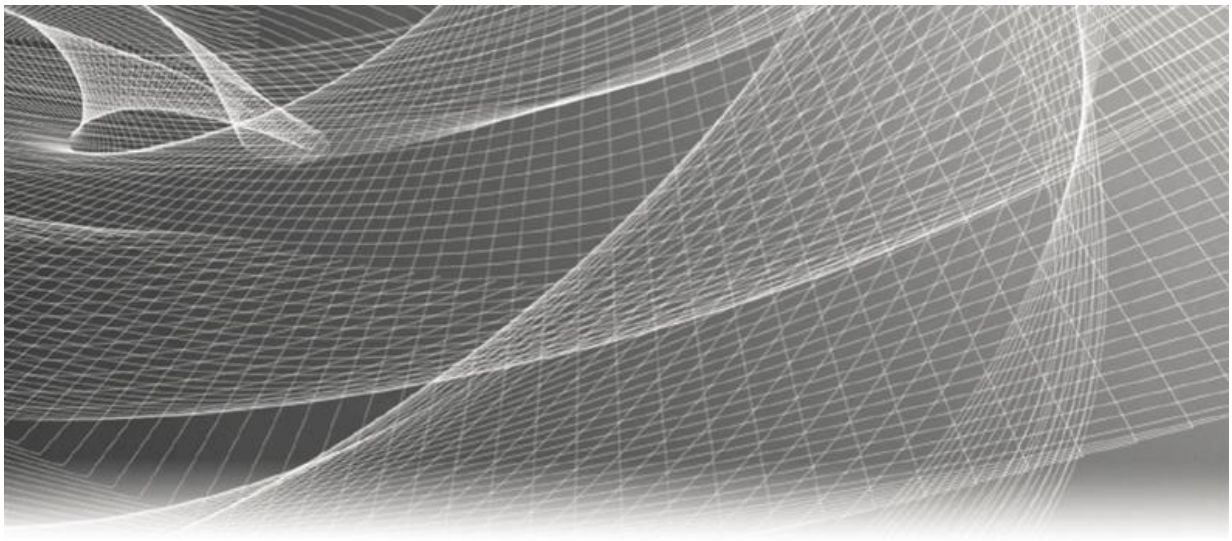


RSA® Archer
NIST-Aligned Privacy Framework
App-Pack

6.8 & Later

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: https://community.rsa.com/community/rsa-customer-support.

Trademarks

License agreement

Third-party licenses

This product may include software developed by parties other than RSA.

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.

Note on Section 508 Compliance

The RSA Archer GRC is built on web technologies which can be used with assistive technologies, such as screen readers, magnifiers, and contrast tools. While these tools are not yet fully supported, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer GRC.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC 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." EMC CORPORATION 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.

August 2020

Table of Contents

Chapter 1: Overview

About RSA® Archer NIST-Aligned Privacy Framework Assessment

The National Institute of Standards and Technology (NIST) published a privacy framework, in collaboration with private and public sector stakeholders, to help organizations better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.

While good cybersecurity practices help manage privacy risk by protecting people's information, privacy risks also may arise from how organizations collect, store, use, and share this information to meet their missions or business objectives, as well as how individuals interact with products and services. NIST believes that organizations that design, operate, or use these products and services better address the full scope of privacy risk with more tools to support better implementation of privacy protections.

The NIST Privacy Framework is composed of three parts:

- Core
- Profiles
- Implementation Tiers

Each component reinforces how organizations manage privacy risk through the connection between business or mission drivers, organizational roles and responsibilities, and privacy protection activities. The Core provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk. The Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk. Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile. The Privacy Framework approach to privacy risk is to consider Privacy Events as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete lifecycle from data collection through disposal.

Note: The structure of the NIST Privacy Framework is similar to the NIST Cybersecurity Framework. There are overlaps in some; however, for this offering, privacy management will only be addressed. This offering allows you to conduct assessments against the NIST Cybersecurity Framework.

Key Features and Benefits

The RSA Archer NIST-Aligned Privacy Framework Assessment app-pack enables an organization to:

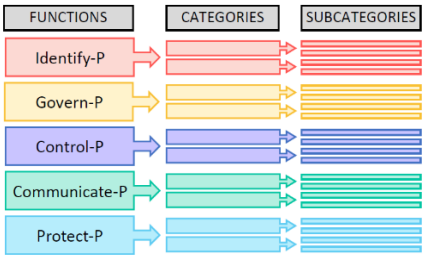
- Create a Current Profile indicating which privacy implementation tier is being achieved.
- Identify a Target Profile that describes the organization's desired privacy implementation tier.
- Conduct a Privacy Risk Assessment against Core activities from NIST's Privacy Framework.
- Analyze the Current Profile against the Target Profile to determine gaps.
- Implement an Action Plan to address privacy gaps.
- Conduct an assessment against the NIST Cybersecurity and Privacy Framework.

Benefits include:

- Building a better privacy foundation by bringing privacy risk into parity with broader enterprise risk portfolio.
- Improve protection of individual privacy and resiliency of critical infrastructure.
- Reinforce privacy risk management through a common language and consistent process for communicating requirements and progress.
- Maintain compliance with regulatory requirements.

Key Terminology

Core: The Core is a set of privacy protection activities and outcomes that allows for communicating prioritized privacy protection activities and outcomes across an organization from the executive level to the implementation/operations level. The Core is further divided into key Categories and Subcategories—which are discrete outcomes—for each Function.



Implementation Tiers: Implementation Tiers ("Tiers") provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed. When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices, the degree of integration of privacy risk into its enterprise risk management portfolio, its data processing ecosystem relationships, and its workforce composition and training program.

Profile: A Profile represents an organization's current privacy activities or desired outcomes. To develop a Profile, an organization can review all of the outcomes and activities in the Core to determine which are most important to focus on based on business or mission drivers, data processing ecosystem role(s), types of data processing, and individuals' privacy needs. An organization can create or add Functions, Categories, and Subcategories as needed. Profiles can be used to identify opportunities for improving privacy posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). Profiles can be used to conduct self-assessments and to communicate within an organization or between organizations about how privacy risks are being managed.

Prerequisites (ODA and system requirements)

Components	Recommended Software
Operating System	Windows Server 2012 R2
Database Server	Microsoft SQL Server 2014 (64-bit)
Services Server	Java Runtime Environment (JRE) 8 (64-bit)
RSA Archer	RSA Archer 6.8 & later
On-Demand Licenses	The RSA Archer NIST-Aligned Privacy Framework App-Pack requires three (3) On-Demand Applications (ODA) licenses. If you have previously installed the RSA Archer Cybersecurity Framework App-Pack, only one (1) ODA is required for this offering.

Compatible Use Cases and Applications

RSA Archer NIST-Aligned Privacy Framework includes the following optional applications:

Application	Use Case	Primary Purpose(s) of the Relationship
Business Unit	RSA Archer Issues Management, RSA Archer Business Impact Analysis, RSA Archer Third Party Catalog, RSA Archer Policy Program Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Key Indicator Management, RSA Archer IT Asset Catalog , RSA Archer Business Asset Catalog , RSA Archer Federal Assessments & Authorizations, RSA Archer Federal Continuous Monitoring	To relate Business Units in scope to the NIST Profile.
Business Processes	RSA Archer Business Impact Analysis, RSA Archer Third Party Engagement, RSA Archer Policy Program Management, RSA Archer IT Controls Assurance, RSA Archer IT Risk Management, RSA Archer Policy Program Management, RSA Archer Controls Assurance Program Management, RSA Archer Data Governance, RSA Archer Business Asset Catalog, RSA Archer Top-Down Assessment, RSA Archer Bottom-Up Risk Assessment, RSA Archer Federal Assessments & Authorization	To relate Business Processes in scope to the NIST Profile.
Applications	RSA Archer Audit Engagements & Workpapers, RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party	To relate Applications in scope to the NIST Profile.

	Governance, RSA Archer IT Asset Catalog, RSA Archer IT Controls Assurance, RSA Archer Information Security Management System, RSA Archer PCI Management, RSA Archer IT Security Vulnerabilities Program, RSA Archer IT Risk Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Data Governance, RSA Archer Operational Risk Management, RSA Archer Federal Continuous Monitoring	
Devices	RSA Archer Audit Engagements & Workpapers, RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party Governance, RSA Archer IT Asset Catalog, RSA Archer IT Controls Assurance, RSA Archer Information Security Management System, RSA Archer PCI Management, RSA Archer IT Security Vulnerabilities Program, RSA Archer IT Risk Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Data Governance, RSA Archer Federal Continuous Monitoring	To relate Devices in scope to the NIST Profile.
Products and Services	RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party Risk Management, RSA Archer Third Party Engagement, RSA Archer Cyber Incident & Breach Response, RSA Archer Business Asset Catalog, RSA Archer Bottom-Up Risk Assessment	To relate Products and Services in scope to the NIST Profile.
Facilities	RSA Archer Audit Engagements & Workpapers, RSA Archer Incident Management, RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party Catalog, RSA Archer IT Controls Assurance, RSA Archer Information Security Management System, RSA Archer PCI Management, RSA Archer IT Risk Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Controls Assurance Program Management, RSA Archer Business Asset Catalog, RSA Archer Bottom-Up Risk Assessment, RSA Archer Federal Assessments & Authorization, RSA Archer Federal Continuous Monitoring	To relate Facilities in scope to the NIST Profile.

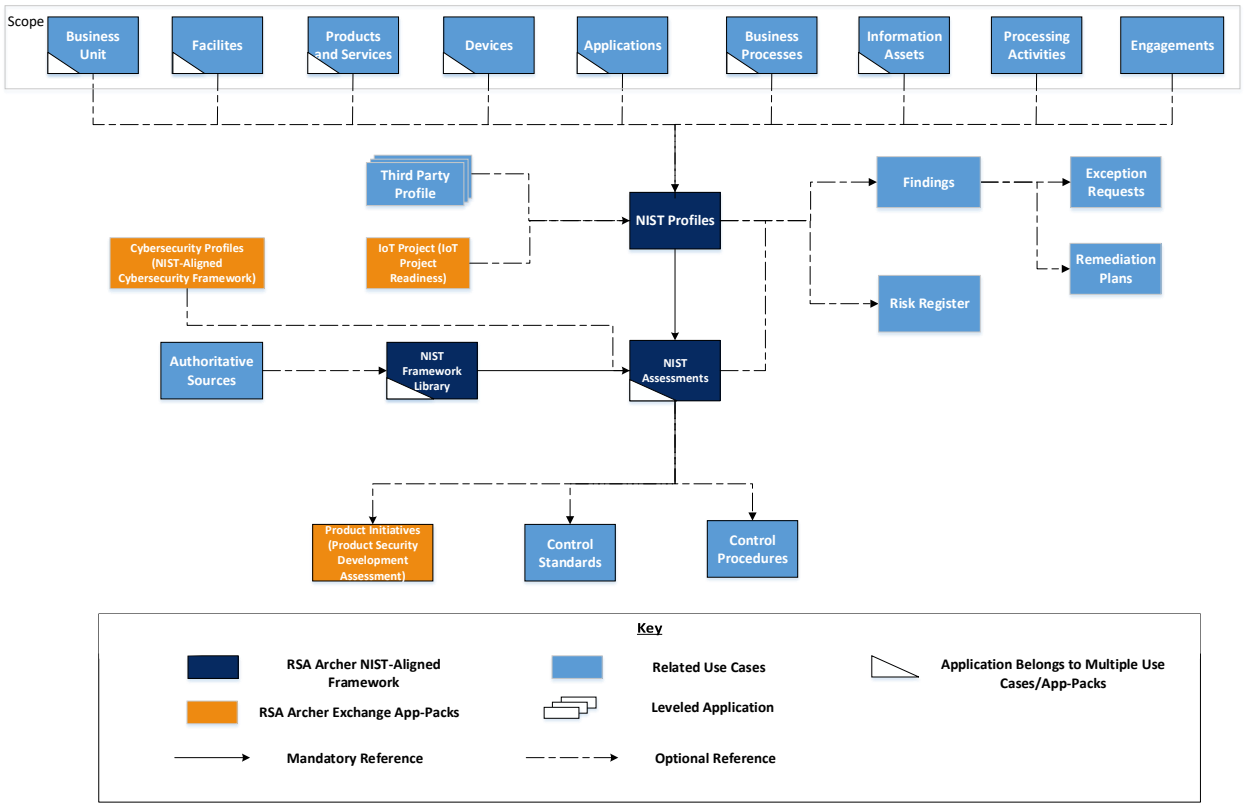
Information Assets	RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer IT Controls Assurance, RSA Archer Information Security Management System, RSA Archer PCI Management, RSA Archer IT Risk Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Controls Assurance Program Management, RSA Archer Data Governance, RSA Archer Business Asset Catalog, RSA Archer Federal Assessments & Authorization	To relate Information Assets in scope to the NIST Profile.
Processing Activities	RSA Archer Data Governance	To relate Processing Activities in scope to the NIST Profile.
Third Party Profile	RSA Archer Third Party Catalog, RSA Archer Third Party Risk Management, RSA Archer Third Party Engagement	To relate Third Parties to the NIST Profile.
Engagements	RSA Archer Third Party Catalog, RSA Archer Third Party Risk Management, RSA Archer Third Party Engagement	To relate Engagements to the NIST Profile.
Findings	RSA Archer Issues Management, RSA Archer Federal Assessments & Authorization	To capture findings to the gaps NIST Profile/NIST Assessments.
Remediation Plans	RSA Archer Issues Management	To relate remediations to the NIST Profile /NIST Assessments.
Exception Requests	RSA Archer Issues Management	To related exceptions to the gaps in NIST Profile /NIST Assessments.
Risk Register	RSA Archer Information Security Management System, RSA Archer IT Risk Management, RSA Archer Risk Catalog, RSA Archer Top-Down Assessment, RSA Archer Information Security Management System	To relate risks to the gaps NIST Profile/NIST Assessments.
Control Standards	RSA Archer Policy Program Management, RSA Archer Federal Assessments & Authorization	To relate impacted/in place Control Standards to NIST Profile/NIST Assessments.
Control Procedures	RSA Archer IT Controls Assurance, RSA Archer Information Security Management System, RSA Archer PCI Management, RSA Archer IT	To relate impacted/in place Control Procedures.

	Risk Management, RSA Archer Controls Assurance Program Management, RSA Archer Data Governance, RSA Archer Top-Down Assessment, RSA Archer Federal Assessments & Authorization	to NIST Profile/NIST Assessments.
Authoritative Sources	RSA Archer Policy Program Management, RSA Archer Controls Monitoring Program Management	To relate impacted Authoritative Sources to NIST Framework Library.
IoT Profiles	RSA Archer IoT Project Readiness (RSA Exchange)	To relate IoT Projects in scope to the NIST Profile.
Product Initiatives	RSA Archer Product Security Development Assessment (RSA Exchange)	To relate Product Initiatives to NIST Profile/Assessments.

Chapter 2: NIST-Aligned Privacy Framework Components

Architecture Diagram

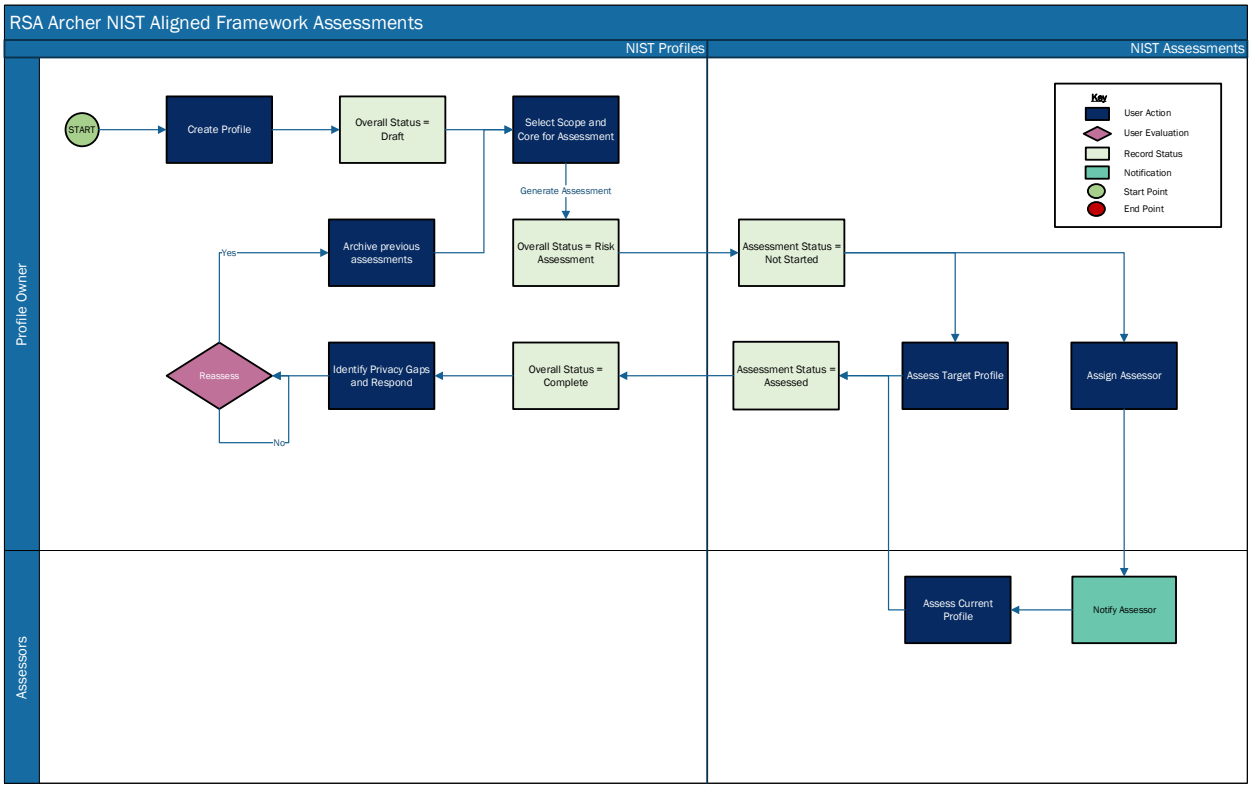
The following diagram shows the relationship between the applications in RSA Archer NIST-Aligned Framework app-pack.



Note: CSF Framework Library and CSF Assessments are a part of RSA Archer Cybersecurity Framework 6.4 SP1 package and will need to be updated if upgrading. Please see the RSA Archer Cybersecurity Framework release 6.8 implementation guide for upgrade details.

Swim Lane Diagram

The following diagram shows the general workflow of the use case.



Applications

The following table describes the applications in RSA Archer NIST-Aligned Privacy Framework App-Pack.

Application	Description
NIST Profiles	The NIST Profiles application documents the scope and framework for the assessment, stakeholders, current and target profile, and any associated action plans.
NIST Framework Library	The NIST Framework Library application contains the NIST Privacy and Cybersecurity Frameworks. It contains the Functions, Categories, Subcategories, and Informative References and Authoritative Sources.
NIST Assessments	The NIST Assessments application contains the assessments to determine the current and target profile. It also documents any supporting evidence during the assessment process.

Personas and Access Roles

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

Function	Description	How many?	Optional/Required
Profile Owner	Responsible for creating Profiles, defining context for privacy risk assessment, determining target profile, and communicating the results of the privacy risk assessment to the organization. Can be someone who owns a business process, product, or service.	Many	Required
Assessor	Responsible for conducting privacy risk assessments to establish current profile and implementing action plans to address gaps with target profile. Responsible for the evaluation of the privacy profile. This role could include someone from internal audit, internal compliance, legal, etc.	Many	Required

The following table describes the Access Roles:

Applications	NIST Framework: Profile Owners	NIST Framework: Assessors	NIST Framework: Read-Only
NIST Framework Library	CRU	R	R
NIST Profiles	CRU	R	R
NIST Assessments	CRU	RU	R
Remediation Plans	CRU	CRU	R
Exceptions Requests	CRU	CRU	R
Findings	CRU	CRU	R
Business Units	R	R	R
Business Processes	R	R	R
Applications	R	R	R

Devices	R	R	R
Products and Services	R	R	R
Facilities	R	R	R
Information Assets	R	R	R
Processing Activities	R	R	R
Third Party Profile	R	R	R
Engagements	R	R	R
Risk Register	R	R	R
Controls Standards	R	R	R
Control Procedures	R	R	R
Authoritative Sources	R	R	R
IoT Project	R	R	R
Product Initiatives	R	R	R

C = Create, R = Read, U = Update, D = Delete

Note: Members of the groups NIST Framework: Owners, NIST Framework: Assessors, NIST Framework: Read-Only, at minimum, need read access at record level for the applications related to the NIST Profile, NIST Assessments, and NIST Framework applications to view or select related records.

Chapter 3: Installing RSA Archer NIST-Aligned Privacy Framework

Complete the following tasks to install the application.

Step 1: Prepare for the Installation

1. Ensure that your RSA Archer system meets the following requirements:
    - RSA Archer Platform version 6.8
2. Download the ODA install package from the RSA Archer Exchange on RSA Link: https://community.rsa.com/community/products/archer-grc/exchange/documentation-downloads.
3. Read and understand the "Packaging Data" section of the RSA Archer Online Documentation.

Step 2: Install the Package

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

Step 3: Test the Installation

Test the RSA Archer NIST-Aligned Privacy Framework according to your company standards and procedures, to ensure that it works with your existing processes.

Step 4: Import the Content into NIST Framework Library

Import the content files into the NIST Framework Library.

Note: Users having CSF content in the NIST Framework Library application **must** update the value of “Framework Source” field to “NIST CSF” at all levels. Next, complete the steps below:

1. Import the Function file
    - Choose Import type as “Create New Records”.
    - Make sure the key fields in the files match the key fields in the applications.
    - After the **completion** of the import, Navigate to Application Builder -> Applications -> NIST Framework Library.
    - Navigate to options tab of the field **Function (Version)** and select the option to make it as a key field.
2. Import the Category file
    - Choose Import type as “Create New Records”.
    - Make sure the key fields in the files match the key fields in the applications.
    - After the **completion** of the import, Navigate to Application Builder -> Applications -> NIST Framework Library.
    - Revert the changes at the Function Level: Navigate to options tab of the field **Function** and select the option to make it as a key field.

- Navigate to options tab of the field **Category (Version)** and select the option to make it as a key field.

3. Import the subcategories file
    - Choose Import type as “Create New Records”.
    - Make sure the key fields in the files match the key fields in the applications.
    - After the **completion** of the import, Navigate to Application Builder -> Applications -> NIST Framework Library.
    - Revert the changes at the Category Level: Navigate to options tab of the field **Category** and select the option to make it as a key field.
    - Navigate to options tab of the field **Sub-Category (Version)** and select the option to make it as a key field.
4. Import the Informative Reference files:
    - Choose Import type as “Create New Records”.
    - Make sure the key fields in the files match the key fields in the applications.
      Note: For auto-mapping of Authoritative source field during import - Make sure the key fields in the Authoritative source application at each level (for example, Source, Topic, Section and Sub-Section) match the field header value for each file.
    - After the **completion** of import of all the informative references files, Navigate to Application Builder -> Applications -> NIST Framework Library.
    - Revert the changes at the Sub-Category Level: Navigate to options tab of the field **Sub-Category** and select the option to make it as a key field.

    Note: The Informative references file provides the relation between NIST Privacy content and NIST Cybersecurity content. Import NIST cybersecurity content to your Authoritative Sources application if not available.

Step 5: Configure the Data Feeds

Configure and test the following data feeds:

1. **Generate NIST Assessments**: This is an Archer to Archer data feed configured to automatically generate NIST Assessments for the Core. Below are the steps to configure the feed after package install:
    a. Go to Administration -> Integration -> Data Feeds and click on the Generate NIST Assessments feed.
    b. In General tab change status to “Active”.
    c. In Transport tab
        i. Provide the Archer URL in Security Section.
        ii. Provide Username, Instance and Password in Transport Configuration section.
    d. Verify Data Mapping in Data Map tab.
    e. Schedule the data feed to run as-per your requirement in Schedule.

2. **Archive NIST Assessments:** This is an Archer to Archer data feed configured to automatically generate NIST Assessments for the Core. Below are the steps to configure the feed after package install:
    a. Go to Administration -> Integration -> Data Feeds and click on the Archive NIST Assessments feed.
    b. In General tab change status to "Active".
    c. In Transport tab
        i. Provide the Archer URL in Security Section.
        ii. Provide Username, Instance and Password in Transport Configuration section.
    d. Verify Data Mapping in Data Map tab.
    e. Schedule the data feed to run as-per your requirement in Schedule tab.

Installing the RSA Archer NIST-Aligned Framework Package

Step 1: Back Up Your Database

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

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

Step 2: Import the Package

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

Step 3: Map Objects in the Package

1. In the Available Packages section, select the package you want to map.
2. In the Actions column, click  for that package.
   The analyzer runs and examines the information in the package. The analyzer automatically matches the system IDs of the objects in the package with the objects in the target instances and identifies objects from the package that are successfully mapped to objects in the target instance, objects that are new or exist but are not mapped, and objects that do not exist (the object is in the target but not in the source).

Note: This process can take several minutes or more, especially if the package is large, and may time out after 60 minutes. This time-out setting temporarily overrides any IIS time-out settings set to less than 60 minutes.
When the analyzer is complete, the Advanced Package Mapping page lists the objects in the package file and corresponding objects in the target instance. The objects are divided into tabs, depending on whether they are found within Applications, Solutions, Access Roles, Groups, Sub-forms, or Questionnaires.

3. On each tab of the Advanced Mapping Page, review the icons that are displayed next to each object name to determine which objects require you to map them manually.

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

4. For each object that requires remediation, do one of the following:
    - To map each item individually, on the Target column, select the object in the target instance to which you want to map the source object. If an object is new or if you do not want to map an object, select Do Not Map from the drop-down list.
      Important: Ensure that you map all objects to their lowest level. When objects have child or related objects, a drill-down link is provided on the parent object. Child objects must be mapped before parent objects are mapped. For more details, see "Mapping Parent/Child Objects" in the RSA Archer Online Documentation.

- To automatically map all objects in a tab that have different system IDs but the same object name as an object in the target instance, do the following:
    a. In the toolbar, click Auto Map.
    b. Select an option for mapping objects by name.

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

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

When all objects are mapped, the icon is displayed in the tab title. The icon is displayed next to the object to indicate that the object will not be mapped.

5. Verify that all other objects are mapped correctly.
6. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the RSA Archer Online Documentation.
7. Once you have reviewed and mapped all objects, click .
8. Select I understand the implications of performing this operation and click OK.
   The Advanced Package Mapping process updates the system IDs of the objects in the target instance as defined on the Advanced Package Mapping page. When the mapping is complete, the Import and Install Packages page is displayed.
   Important: Advanced Package Mapping modifies the system IDs in the target instance. Any Data Feeds and Web Service APIs that use these objects will need to be updated with the new system IDs.

Step 4: Install the Package

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

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

    Note: Items in the package that do not match an existing item in the target instance are selected by default.
4. Click Lookup.
5. For each component section, do the following:
    Note: To move onto another component section, click Continue or select a component section in the Jump To drop-down menu.
    a. In the Install Method drop-down menu, select an install method for each selected component.
    Note: If you have any existing components that you do not want to modify, select Create New Only. You may have to modify those components after installing the package to use the changes made by the package.
    b. In the Install Option drop-down menu, select an install option for each selected component.
    Note: If you have any custom fields or formatting in a component that you do not want to lose, select Do Not Override Layout. You may have to modify the layout after installing the package to use the changes made by the package.
6. Click OK.
7. To deactivate target fields and data-driven events that are not in the package, in the Post-Install Actions section, select the Deactivate target fields and data-driven events that are not in the package checkbox. To rename the deactivated target fields and data-driven events with a user-defined prefix, select the Apply a prefix to all deactivated objects checkbox, and enter a prefix. This can help you identify any fields or data-driven events that you may want to review for cleanup post-install.
8. Click Install.

9. Click OK.

Step 5: Review the Package Installation Log

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

Chapter 4: Using RSA Archer Privacy Framework

Task 1: Create a Privacy Profile

Users: Profile Owner

1. Go to the NIST Profile record.
    a. From the menu bar, click NIST Aligned Framework.
    b. Under Solutions, click NIST-Aligned Framework.
    c. Under Applications, click NIST Profile.
    d. In the NIST Profile record browser, click New Record.
2. Enter a Profile Name, Profile Description in the General Information section.
3. Select value NIST Privacy in Framework Assessed field in Details section.
4. Enter Assessment Start Date and other assessment details for the NIST Profile in the Details section.
5. Select Assessor(s), Profile Owner(s) and other stakeholders in the Stakeholders section.
6. Select the scope that are part of the boundary for the NIST Profile. Use the ellipses button to find existing records or provide the details in the text box in the Scope section.
7. Attach any necessary documentation in the Documentation Section.
8. Click Save in the Record Toolbar.

Task 2: Generate Privacy Assessments

Users: Profile Owner

1. Navigate to the Assessments tab of the NIST Profile.
2. Click on the Framework Library cross-reference field to look up.
    a. Select the Functions or Categories or Sub-Categories that need to be assessed
    b. Click Ok.
3. Once the desired Functions or Categories or Sub-Categories are selected, select “Yes” in Generate Assessments flag in the Assessment Generation section.
4. Click Save or Save and Close.
5. Wait for the Privacy Assessments to be generated.

    Note: Assessments are generated for each Sub-Category selected. For selection made at Function or Category level, the Assessments will be generated for all the associated Sub-Categories in NIST Assessments application.

Task 3: Assess Target Profile and Assign Assessor

Users: Profile Owner

1. Navigate to the Assessments tab of the NIST Profile.

2. Navigate to the NIST Assessments cross-reference field to see the Privacy Assessments that were generated in the previous step.
3. Click on “Enable Inline Edit” for the NIST Assessments section.
4. Select the assessor in the Assessor field.
5. Select the Target Tier.
6. Click Save Changes or Save.

Task 4: Assess Current Profile

Users: Assessor

1. Navigate to the Assessments tab of the NIST Profile.
2. Navigate to the NIST Assessments cross-reference field to see the Privacy Assessments that were generated in the previous step.
3. Click into a NIST Assessment Record by clicking on Tracking ID.
4. Use the Lookup button to select the Informative Reference for the particular sub-category.
    a. Select an Informative Reference.
    b. Click Ok to return finish making the selection.
5. Select the assessor in the Assessor field to reassign Assessor.
6. Select the Current Tier.
7. Enter Implementation Details of the how the Sub-Category was implemented and assessed.
8. Click Save in the Record Toolbar.
9. If Current Tier does not equal the Target Tier, then there is a capability gap and a Finding record can be created to track the capability gap.
10. Repeat steps 3 through 9 for each of the Privacy Assessments.

Task 5: Review Privacy Profile

Users: Profile Owner

1. Navigate to NIST Profile.
2. Review the Assessment Summary section.
3. Provide Response in the NIST Profile and/or NIST Assessments.
4. Select value Review Complete in Profile Owner Review Status field in Details tab -> Review Section.

Task 6: Archive and Reassess

Users: Profile Owner

1. Navigate to NIST Profile.
2. Select value Yes for Archive Assessments field in Assessments Helper Section.

3. Click Save or Save and Close.
4. Repeat tasks 2 through 5 once existing assessments are archived.