# Archer NIST-Aligned Framework App-Pack

The Archer NIST-Aligned Framework app-pack contains 3 frameworks:

* Cybersecurity
* AI Risk Management
* Privacy

On this page

* [Release notes](#Releasenotes)
  + [Known issues](#Knownissues)
* [Overview](#Overview)
  + [About Archer NIST Aligned Framework App-Packs](#AboutArcherNISTAlignedFrameworkAppPacks)
  + [Key features and benefits](#Keyfeaturesandbenefits)
  + [Key terminology](#Keyterminology)
  + [Prerequisites (ODA and system requirements)](#PrerequisitesODAandsystemrequirements)
  + [Compatible use cases and applications](#Compatibleusecasesandapplications)
    - [Related applications](#Relatedapplications)
  + [Additional resources](#Additionalresources)
* [Components](#Components)
  + [Architecture diagram](#Architecturediagram)
  + [Swim lane diagram](#Swimlanediagram)
  + [Applications](#Applications)
  + [Personas and Access Roles](#PersonasandAccessRoles)
* [Installing Archer NIST Aligned Framework App-Packs](#X6e5c7b99f54b62c7b39cc0e15ea92c13eeeb257)
  + [Security considerations](#Securityconsiderations)
  + [Installation overview](#Installationoverview)
    - [Step 1: Prepare for the Installation](#Step1PreparefortheInstallation)
    - [Step 2: Install the package](#Step2Installthepackage)
    - [Step 3: Import the Content files into NIST Framework Library](#X6b71193ed4d8481dd2a6e07fc1e5621a48e1b38)
    - [Viewing ISO Content](#ViewingISOContent)
    - [Step 4: Set up data feeds](#Step4Setupdatafeeds)
    - [Step 5: Test the installation](#Step5Testtheinstallation)
  + [Installing the package](#Installingthepackage)
    - [Task 1: Back up your database](#Task1Backupyourdatabase)
    - [Task 2: Import the package](#Task2Importthepackage)
    - [Task 3: Map objects in the package](#Task3Mapobjectsinthepackage)
    - [Task 4: Install the package](#Task4Installthepackage)
    - [Task 5: Review the package Installation Log](#Task5ReviewthepackageInstallationLog)
  + [Setting up data feeds](#Settingupdatafeeds)
    - [Task 1: Import a data feed](#Task1Importadatafeed)
    - [Task 2: Schedule a data feed](#Task2Scheduleadatafeed)
    - [Validating a data feed](#Validatingadatafeed)
    - [Running a data feed](#Runningadatafeed)
    - [Setting up a reference data feed](#Settingupareferencedatafeed)
* [Using the Archer NIST Aligned Framework App-Packs](#X62fe63f2631bbcd8420289663374c0002d7f722)
  + [Task 1: Create a Profile](#Task1CreateaProfile)
  + [Task 2: Complete Profile Scope](#Task2CompleteProfileScope)
  + [Task 3: Generate Framework Assessments](#Task3GenerateFrameworkAssessments)
  + [Task 4: Determine Target Profile and Assign Assessors](#X72f56e11a588618d8259746a6d15608282ba8f9)
  + [Task 5: Complete Profile Assessment](#Task5CompleteProfileAssessment)
  + [Task 6: Review Profile](#Task6ReviewProfile)
  + [Task 7: Archive and Reassess](#Task7ArchiveandReassess)
* [Upgrading the Archer NIST-Aligned Framework App-Packs](#X290cc140961864720357f5e0e5ae8d76ec358c0)
  + [Adding informative reference for NIST-Aligned Framework 2024.03](#X52598a011a89d9b4f6f3e1123e71d4fe5691f4a)
  + [Change log for NIST-Aligned Framework 2024.03 users.](#X7ff831cd4b7257e8c8365caa9f0e67346dc3470)
* [Certification environment](#Certificationenvironment)

## Release notes

| Date | Version | Changes |
| --- | --- | --- |
| December 2024 | Archer 2024.03 | * The NIST CSF 1.1 Authoritative Source must be imported before importing Informative References for NIST CSF 2.0 due to mappings between NIST CSF 2.0 and NIST CSF 1.1. The documentation and package have been updated to include the requirement for NIST CSF 1.1 Authoritative Source. |
| May 2024 | Archer 2024.03 | * The package has been updated with NIST Profiles content import CSV files. |
| March 2024 | Archer 2024.03 | * Added the ability to conduct assessment against NIST CSF 2.0. * New fields added for Implementation Examples at subcategory level. * New import files for NIST CSF 2.0 content. * New Report object field in NIST profile to compare NIST 1.1 to NIST 2.0 assessments. * New DDEs to show/hide comparison report object based on Assessment versions. |
| September 2023 | Archer 6.13 | * Added the ability to conduct assessments against NIST AI Risk Management Framework. * Added a new Archer Web Services Transporter Data Feed to perform auto-scoping based on selected business processes. * Added new mail merge templates for framework score cards. * Added new fields and reports to support the new features. * Removed the History Log field from NIST Profiles and NIST Assessments applications. |
| August 2020 | Archer 6.8 | * Combined the package for CSF and Privacy framework. * Changed the Cybersecurity Framework Library name to NIST Framework Library. * Changed the Cybersecurity Assessments name to NIST Assessments. * Added new ODA NIST Profiles application. * Added new fields, dashboards, and a workspace. * Added the ability to conduct assessments against the NIST Privacy Framework. * Streamlined the workflow for Profile assessment and review. |

### Known issues

| Component | Issue ID | Description |
| --- | --- | --- |
| Package Import | CE-121096 | Groups:   * “app-grm-admin-enhanced-tester” * ‘Products and Services (Customer Offered) – R”   May appear during package installation. But can be ignored. |

## Overview

### About Archer NIST Aligned Framework App-Packs

The National Institute of Standards and Technology (NIST) has worked with various stakeholders to develop frameworks for cybersecurity, privacy, and artificial intelligence (AI) risk management. The frameworks are based on existing standards, guidelines, and practices to help organizations better manage risks to individuals, organizations, and society associated as they relate to cybersecurity, privacy, and AI.

* The NIST Cybersecurity Framework was created through collaboration between industry and government stakeholders.  This framework provides a consistent set of standards and guidelines for organizations to follow.  In doing so, this framework promotes protection of an organization's critical infrastructure and the ability to manage cybersecurity-related risk.
* The NIST Privacy Framework was created to improve privacy through enterprise risk management. This framework helps organizations manage privacy risks by taking privacy into account as they design and deploy systems, products, and services that affect individuals. It also helps organizations communicate their privacy practices and encourage cross-organizational workforce collaboration.
* The NIST AI Risk Management Framework is a collaboration between private and public sectors to develop a framework to help organizations better manage risks to individuals, organizations, and society associated with artificial intelligence.  This framework intends to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.

The NIST Frameworks all have a similar structure consisting of the following components:

* The Core is a set of high-level functions that are broken down into categories and subcategories that make up the framework activities and outcomes.
* A Profile represents an organization’s current activities and desired outcomes.  Profiles are created by selecting activities and outcomes from the Core based on mission drivers, data process ecosystem role(s), types of data processing, individual and organizational needs, etc.  Profiles can be used to conduct self-assessments and identify opportunities to improve the current state of the organization.
* The Implementation Tiers provide context on how an organization views their cybersecurity, privacy, or AI implementation and the processes in place to manage those risks.  Tiers describe the degree to which an organization’s risk management practices exhibit the characteristics defined in the framework.

### Key features and benefits

The Archer NIST Aligned Framework app-packs enable organizations to:

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

Benefits include:

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

### Key terminology

**Core:** Core is a set of activities and outcomes that allows for communicating prioritized 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 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.

**Note:** NIST has not currently recommended any implementation tiers for the AI Risk Management Framework. Organizations can define them as per their requirements. NIST does not currently provide out-of-the-box definitions used in the Archer NIST Assessments application.

**Profile:** A Profile represents an organization’s current activities or desired outcomes. To develop a Profile, an organization can review all the outcomes and activities in the Core to determine which are most important to focus on based on business or mission drivers, etc. An organization can create or add Functions, Categories, and Subcategories as needed. Profiles can be used to:

* Identify opportunities for improving cybersecurity/privacy/ai risk posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state).
* Conduct self-assessments and communicate within an organization or between organizations about how risks are being managed.

### Prerequisites (ODA and system requirements)

| Components | Prerequisites |
| --- | --- |
| Archer Solution Area(s) | * Archer Regulatory & Corporate Compliance Management * Archer IT & Security Risk Management |
| Archer Use Case(s) | N/A |
| Archer Applications | N/A |
| Uses Custom Application | No |
| Requires On-Demand License | Yes. Three (3) On-Demand Licenses are required. |
| Archer Requirements | Archer 2024.03 and later |
| Partner/Vendor Requirements | N/A |

### Compatible use cases and applications

#### Related applications

| Application | Use Case | Primary Purpose(s) of the Relationship |
| --- | --- | --- |
| Business Unit | Third Party Catalog, Issues Management, Business Impact Analysis, Key Indicator Management, IT Asset Catalog, Business Asset Catalog, ESG Management System | To relate Business Units in scope to the NIST Profile. |
| Business Processes | Top-Down Assessment, Risk Assessment Management, Business Impact Analysis, Audit Engagements & Workpapers, IT Controls Assurance, Third Party Engagement, Business Asset Catalog, Data Governance | To relate Business Processes in scope to the NIST Profile. |
| Applications | Third Party Governance, Audit Engagements & Workpapers, Self-Assessment Management, IT Asset Catalog, Data Governance | To relate Applications in scope to the NIST Profile. |
| Devices | Third Party Governance, Audit Engagements & Workpapers, IT Asset Catalog, Data Governance | To relate Devices in scope to the NIST Profile. |
| Products and Services | Risk Assessment Management, Third Party Risk Management, Third Party Engagement, Business Asset Catalog, Operational Scenario Analysis | To relate Products and Services in scope to the NIST Profile. |
| Facilities | Incident Management, Third Party Catalog, Risk Assessment Management, Audit Engagements & Workpapers, IT Risk Management, Business Asset Catalog, Data Governance, ESG Management System | To relate Facilities in scope to the NIST Profile. |
| Information Assets | Data Governance, Business Asset Catalog | To relate Information Assets in scope to the NIST Profile. |
| Processing Activities | Data Governance | To relate Processing Activities in scope to the NIST Profile. |
| Third Party Profile | Third Party Catalog, Operational Scenario Analysis | To relate Third Parties to the NIST Profile. |
| Engagements | Third Party Catalog, Third Party Risk Management, Third Party Engagement | To relate Engagements to the NIST Profile. |
| Findings | Issues Management | To capture findings to the gaps NIST Profile/NIST Assessments. |
| Remediation Plans | Issues Management | To relate remediations to the NIST Profile /NIST Assessments. |
| Exception Requests | Issues Management | To related exceptions to the gaps in NIST Profile /NIST Assessments. |
| Risk Register | Information Security Management System, IT Risk Management, Risk Catalog, Top-Down Assessment, Operational Scenario Analysis | To relate risks to the gaps NIST Profile/NIST Assessments. |
| Control Standards | Policy Program Management | To relate impacted/in place Control Standards to NIST Profile/NIST Assessments. |
| Control Procedures | IT Controls Assurance, Information Security Management System, PCI Management, IT Risk Management, Controls Assurance Program Management, Data Governance, Top-Down Assessment | To relate impacted/in place Control Procedures to NIST Profile/NIST Assessments. |
| Policies | Policy Program Management | To relate impacted/in place Policies to NIST Profile/NIST Assessments. |
| Authoritative Sources | Policy Program Management | To relate impacted Authoritative Sources to NIST Framework Library. |
| IoT Profiles | Archer IoT Project Readiness (Exchange) | To relate IoT Projects in scope to the NIST Profile. |
| Product Initiatives | Archer Product Security Development Assessment (Exchange) | To relate Product Initiatives to NIST Profile/Assessments. |

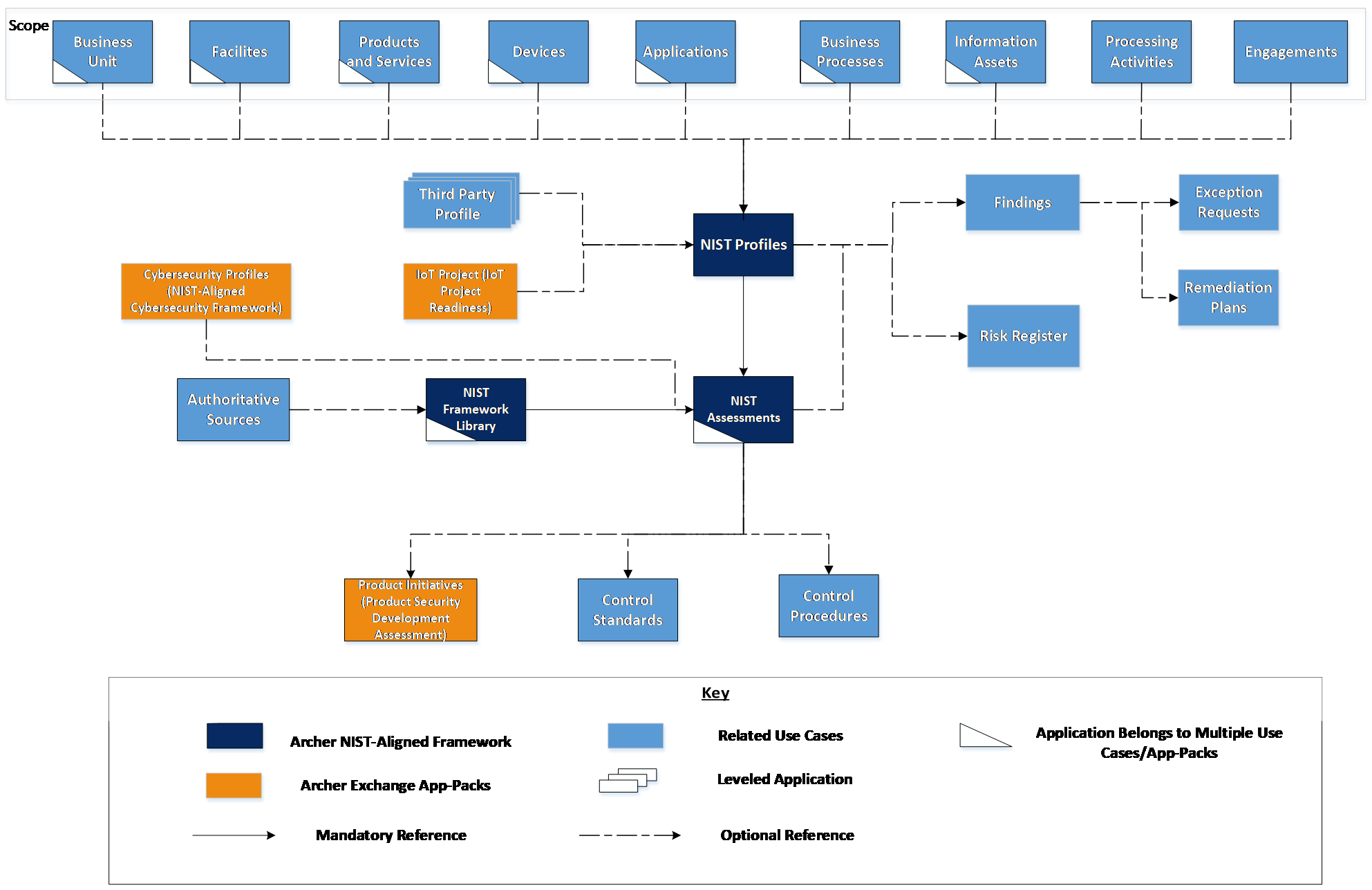
### Additional resources

The following additional resources are available for this offering:

* NIST CSF 2.0 - <https://doi.org/10.6028/NIST.CSWP.29>
* NIST CSF 2.0 QSG:<https://doi.org/10.6028/NIST.SP.1301>

## Components

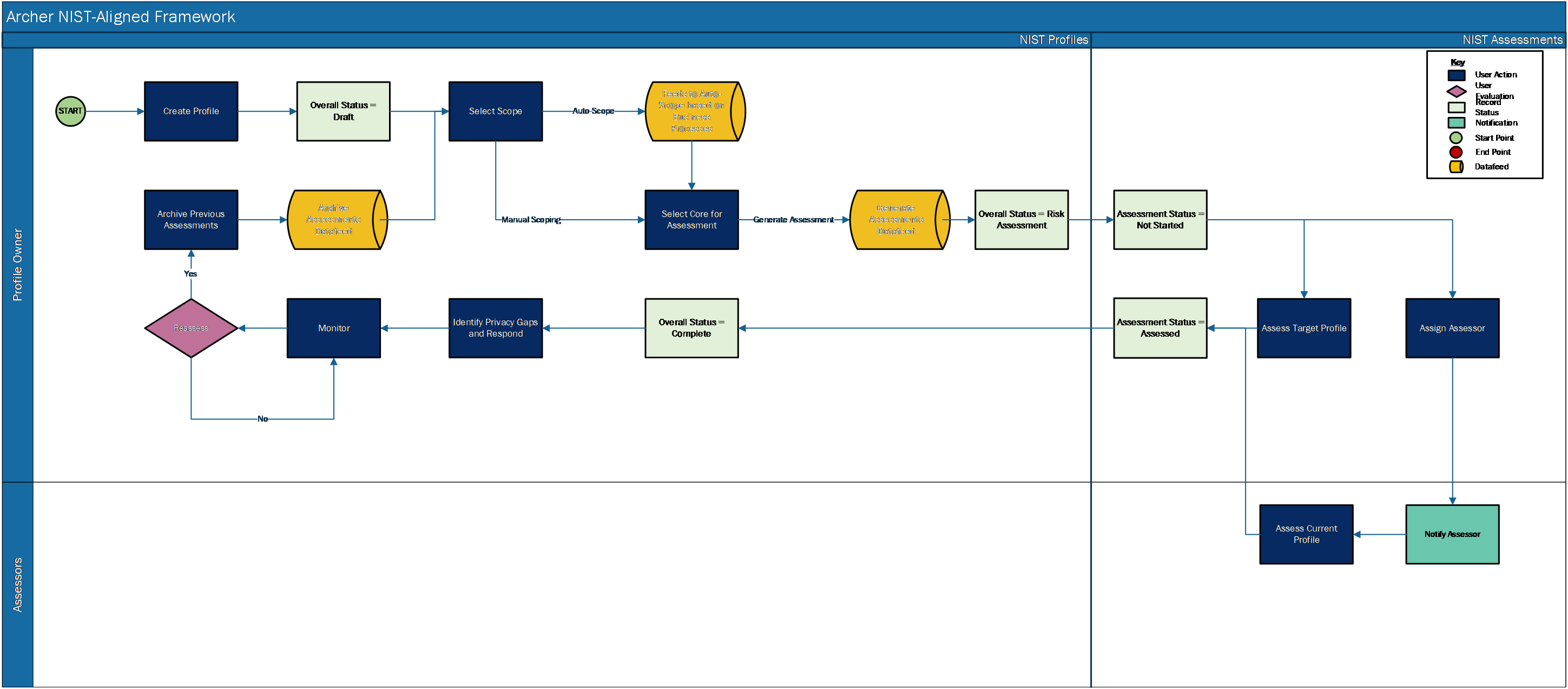
### Architecture diagram



**Important:** Cybersecurity Profiles is available to the users who are still using the initial Archer NIST-Aligned Cybersecurity Framework version 6.4 SP1 package.

### Swim lane diagram

The process starts with a Profile Owner creating a profile in the NIST Profiles application. The Profile Owner defines the profile scope and selects the desired framework applicable for the profile.  After selecting the Core activities, a data feed generates the assessments. The Profile Owner assigns the assessments to the Assessors and identifies the target tier in which they would like to achieve for the selected for the Core activities. Assessors identify the current tier of the assessments. Once all assessments are complete, the Profile Owner reviews the profile and provides additional information as needed. Stakeholders identify the risks and action items required to achieve the targets. After a pre-defined time frame, the profile is reassessed again to determine its current state.



### Applications

| 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, Cybersecurity, and AI Risk Management Frameworks.  It also 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 assessments, determining the target profile, and communicating the assessment results to the organization. This role could include a business process manager, business unit manager, or information system owner. The Profile Owner will likely own multiple business processes. | Many | Required |
| Assessor | Responsible for conducting assessments to establish current profile and implementing action plans to address gaps with the target profile. Responsible for evaluating the current profile. This role could include someone from internal audit, internal compliance, legal, etc.​ | Many | Required |

The following table describes the Access Roles. C = Create, R = Read, U = Update, D = Delete

| 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 |
| Policies | R | R | R |
| Authoritative Sources | R | R | R |
| IoT Project | R | R | R |
| Product Initiatives | R | R | R |

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

## Installing Archer NIST Aligned Framework App-Packs

### Security considerations

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ARCHER 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.  ARCHER RECOMMENDS CUSTOMERS PERFORM A FULL SECURITY EVALUATION PRIOR TO IMPLEMENTATION.

### Installation overview

Complete the following tasks to install the offering.

#### Step 1: Prepare for the Installation

1. Ensure that your Archer system meets the following requirements:
   * Archer Platform version 2024.03
2. Obtain the Data Dictionary for the ODA by contacting your Archer Account Representative or calling 1-888-539-EGRC. The Data Dictionary contains the configuration information for the use case.
3. Read and understand "Packaging Data" in the Archer Platform Help.

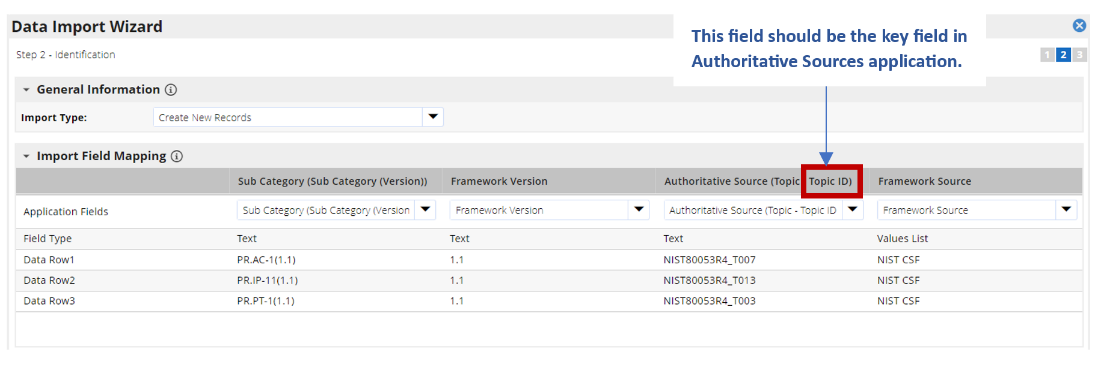
#### Step 2: Install the package

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. For more information, see [Installing the Packages](#InstallAppPackage).

#### Step 3: Import the Content files into NIST Framework Library

**Important:** Users having CSF content (v1.0 and/or v1.1) in the NIST Framework Library application must update the value of “Framework Source” field to “NIST CSF” at all levels. A new field, “Subcategory Name”, is added to Subcategory Level. Users can import this content from the updated Subcategory file in the package. For NIST AI content, additional fields are added to the Subcategory level to accommodate the data from the NIST AI RMF Playbook. Users must create these fields before importing the data. Depending upon the framework type, content files needed to be imported varies.

1. To import the necessary library content, do any of the following:
   * From the menu, click > Integration > Data Imports, and select the application, questionnaire, or sub-form to which you are importing data.
   * From a workspace menu, hover over the application that you want to import data into and click.  
     This option is only available if the application configuration owner has enabled data import from the navigation menu and you have access rights for importing.
   * From the search results page in an application, click and select Import.
2. Import Functions
   1. Load your data file and select import options. For more information on this step, see [Importing Data](https://help.archerirm.cloud/platform_613/en-us/content/platform/integration/int_dimp_importing.htm#Task2Loadyourdatafileandselectimportoptions) in the Archer Platform Help.
   2. On the Step 2 – Identification page, in the Import Type field, select Create New Records.
   3. Ensure that the key fields in the files match the key fields in the applications.
   4. After the import completes, Navigate to > Application Builder > Applications > NIST Framework Library.
   5. In the Designer tab > Layout tab > Objects panel, click the Function (Version)field.
   6. In the Properties panel> Options section of the field, select Make this the key field.
3. Import the Categories
   1. Load your data file and select import options. For more information on this step, "Importing Data" in the Archer Platform Help.
   2. On the Step 2 – Identification page, in the Import Type field, select Create New Records.
   3. Ensure that the key fields in the files match the key fields in the applications.
   4. After the import completes, Navigate to > Application Builder > Applications > NIST Framework Library.
   5. In the Designer tab > Layout tab > Objects panel, click the Function field.
   6. In the Properties panel> Options section of the field, select Make this the key field.
   7. In the Designer tab > Layout tab > Objects panel, click the Category (Version) field.
   8. In the Properties panel> Options section of the field, select Make this the key field.
4. Import the Subcategories
   1. Load your data file and select import options. For more information on this step, see "Importing Data" in the Archer Platform Help.
   * **Note:** For NIST AI RMF content, the source file includes HTML formatting. While importing the content, select Source File has HTML Formatting.
   1. On the Step 2 – Identification page, in the Import Type field, select Create New Records.
   2. Ensure that the key fields in the files match the key fields in the applications.
   3. After the import completes, Navigate to > Application Builder > Applications > NIST Framework Library.
   4. In the Designer tab > Layout tab > Objects panel, click the Category field.
   5. In the Properties panel> Options section of the field, select Make this the key field.
   6. In the Designer tab > Layout tab > Objects panel, click the Subcategory (Version) field.
   7. In the Properties panel> Options section of the field, select Make this the key field.
5. Import all the Informative References

* **Important:** Before importing the Informative References data, ensure that the NIST CSF v1.1 Authoritative Source Content is available in your Archer instance, as the Informative References for NIST CSF 2.0 are mapped to NIST CSF v1.1 Authoritative Source Content. If NIST CSF v1.1 Authoritative Source Content is not available in your Archer instance, then import the content data available in the '1.1\_NIST\_CSF\_AuthSrc' folder of the downloaded installation package.
  1. Load your data file and select import options. For more information on this step, see "Importing Data" in the Archer Platform Help.
  2. On the Step 2 – Identification page, in the Import Type field, select Create New Records.
  3. Ensure that the key fields in the files match the key fields in the applications.
  + **Note:** For auto-mapping of Authoritative source field during import –Ensure that 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. For example, see the screenshot below.
  + 
  1. After the import completes, Navigate to > Application Builder > Applications > NIST Framework Library.
  2. In the Designer tab > Layout tab > Objects panel, click the Subcategory field.
  3. In the Properties panel> Options section of the field, select Make this the key field.

**Note:** The Crosswalk Informative references file provides the relation between NIST Privacy content and NIST Cybersecurity content. If NIST Privacy and Cybersecurity authoritative source content is not already available in your Archer instance, import the content to your Authoritative Sources application. Content is available for download in Exchange Community. Currently, there is no Informative References file being provided for out-of-the-box NIST AI RMF content.

#### Viewing ISO Content

To receive the latest ISO content, customers must have an up-to-date licensing agreement with ANSI. ANSI must confirm the Licensing agreement before Archer Support can release the content to the person of record on file with ANSI.

Begin the process by contacting Archer Technical Support to request ISO content. Archer Technical Support will provide ANSI contact information to submit a request to confirm the ISO licensing agreement with Archer. Once the request has been submitted, ANSI will confirm the licensing agreement with Archer Technical Support and the ISO content will be distributed. If the licensing agreement does not exist or is no longer up-to-date, ANSI will provide instructions on how to obtain a new licensing agreement.

#### Step 4: Set up data feeds

You must import and schedule each use case data feed that you want to use. See [Setting Up Data Feeds](#SettingUpDataFeeds) for complete information.

#### Step 5: Test the installation

Test the application according to your company standards and procedures, to ensure that the use case works with your existing processes.

### Installing the package

#### Task 1: Back up your database

There is no undo function for package installation. Packaging is a powerful feature that can make significant changes to an instance. Archer strongly recommends that you 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. You must manually delete new objects created by the package installation.

#### Task 2: Import the package

1. From the menu bar, click Admin menu> Application Builder > Install Packages.
2. In the Available Packages section, click Import.
3. Click Add New, and then select the package file that you want to import.
4. Click OK.

The Available Packages section displays the package file and is ready for installation.

#### Task 3: Map objects in the package

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

1. From the menu bar, click > Application Builder > Install Packages.
2. In the Available Packages section, select the package you want to map.
3. In the Actions column, click Analyze 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.

1. 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.

On each tab of the Advanced Mapping Page, review the icons next to each object to determine which objects you must map manually.

| Icon | Name | Description |
| --- | --- | --- |
| Awaiting mapping review | 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 icon 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 run the mapping process without mapping all the objects. The Awaiting mapping review icon is for informational purposes only. |
| Checkmark | Mapping  Completed | Indicates that the object and all child objects are mapped to an object in the target instance. There are no further steps required with these objects in Advanced Package Mapping. |
| Missing objects | 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. |

1. 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 a child or related objects, the parent object provides a drill-down link. You must map child objects before parent objects. For more details, see "Mapping Parent/Child Objects" in the Archer Platform Help.
   * 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:
2. In the toolbar, click Auto Map.
3. 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 uncommitted 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, in the Actions column, click .

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

6. Verify that all other objects are mapped correctly.

7. (Optional)To save your mapping settings so that you can resume working later, see "Importing and Exporting Mapping Settings" in the Archer Platform Help.

8. Once you have reviewed and mapped all objects, click Execute.

9. 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. You will need to update any Data Feeds and Web Service APIs that use these objects, 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. The Log Messages section provides a list of conditions that may cause objects not to be installed. The Package Installation Log section displays a log entry.

1. From the menu bar, click  > Application Builder > Install Packages.
2. In the Available Packages section, locate the package file that you want to install, and click Install.
3. In the Selected Components section, click the Lookup button to open the Package Selector window.
   * 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.

1. Under the Install Method drop-down menu, select an option for each selected component. To use the same Install Method for all selected components, select a method from the top-level drop-down list.

**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.

1. 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.
2. Click Install.
3. Click OK.

#### Task 5: Review the package Installation Log

1. From the menu bar, click  > Application Builder > Install Packages.
2. In the Package Installation Log tab, click the package that you want to view.
3. In the Package Installation Log page, in the Object Details section, click View All Errors.

* **Note:** To view individual logs, in the Errors column of the log you want to view, click the Failures link or Warnings link. Clicking View All Errors, Failures, or Warnings opens the specific errors on a different page.

1. Click the Export icon to export the log file.
2. Click Close.

### Setting up data feeds

Configure the data feeds:

1. Auto Scope NIST Profile Business Processes: This Archer Web Services Transporter Data Feed is configured to automatically copy the following from business processes to profile: Applications, Devices, Business Units, Facilities, Products and Services, Information Assets, Devices related to the Applications, Applications related to Devices.
2. Generate NIST Assessments: This Archer Web Services Transporter Data Feed is configured to automatically generate NIST Assessments for the Core.
3. Archive NIST Assessments: This Archer Web Services Transporter Data Feed is configured to automatically archive NIST Assessments for the Profile.

#### Task 1: Import a data feed

1. Go to the Manage Data Feeds page.
   1. From the menu bar, click .
   2. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, click Import.
3. Locate and select the .dfx5 file for the data feed.
4. From the General tab in the General Information section, in the Status field, select Active.
5. Click the Transport tab. Complete the fields in the Transport Configuration section as follows: In the URL field, type: YourServerName/VirtualDirectoryName/ws/search.asmx
6. In the Username and Password fields, type the username and password of a Platform user that has API access and access to all the records on the Platform instance (from which the data feed is coming).
7. In the Instance field, type the name of the Platform instance from which the data feed is coming (this is the instance name as you enter it on the Login window).
8. Verify that key field values are not missing from the data feed setup window.
9. Click Save.

#### Task 2: Schedule a data feed

A data feed must be active and valid to successfully run. A successful data feed run processes all input data, completes all expected record updates, and does not report any failures in the Run Details Report.

#### Validating a data feed

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

#### Running a data feed

You can set up data feeds to run automatically at regular intervals. This reduces the time and effort required to import data from an external file.

You can initiate data feeds at various times and configure them to run in regular increments for an indefinite period of time.

You can run the data feed immediately.

To prevent excess server load, schedule data feeds on a staggered basis. You can schedule a maximum of 10 data feeds to run at a time. If more than 10 data feeds are scheduled, each remaining data feed runs as the previous one completes.

#### Setting up a reference data feed

A reference feed allows you to specify another feed. This indicates to the Data Feed Service that this feed will start running as soon as the referenced feed completes successfully.

1. Go to the Run Configuration tab > Schedule section.
2. Do one of the following to schedule your data feed.
   * Run on Schedule. You can configure your data feed to run on a defined schedule.
   * Run After. The Data Feed Services starts the current data feed after the referenced data feed completes successfully.
   * Run Now.
3. To save the data feed, click Save or Save and Close

## Using the Archer NIST Aligned Framework App-Packs

### Task 1: Create a Profile

User: Profile Owner

1. From the workspace menu, click > NIST-Aligned Framework > NIST-Aligned Framework > NIST Profiles.
2. On the NIST Profiles application, click to add a new record.
3. In the General Information section, enter a Profile Name and Profile Description.
4. In the Details section, do the following:
   1. In the Framework Assessed field, select one of the following values: NIST CSF/NIST Privacy/NIST AI.
   2. Enter the Assessment Start Date.
   3. Complete the remaining fields, as needed.
5. In the Stakeholders section, do the following:
   1. Select Profile Owner(s), Assessor(s).
   2. Complete the remaining fields, as needed.
6. In the Scope section, select the scope that is part of the boundary for the NIST Profile. Scoping can be done in two ways:
   1. Manually select and update the scope. In the fields, use to find existing records, or provide the scope details in the Scope field.
   2. To auto-scope, do the following:
      1. In the Business Processes field, click to look up and select records.
      2. In the Auto Scope with Business Processes field, select Yes.
7. In the Documentation section, attach any necessary documentation.
8. Click Save.

### Task 2: Complete Profile Scope

User: Profile Owner

**Important:** This step is only required if profile scoping is not completed during Task 1.

1. Navigate to the Details tab of the NIST Profile.
2. Profile Owner completes the profile scope (if not already done).
3. In the Scope section, select the scope that is part of the boundary for the NIST Profile. Scoping can be done in two ways:
   1. Manually select and update the scope. In the fields, use to find existing records, or provide the scope details in the Scope field.
   2. To auto-scope, do the following:
      1. In the Business Processes field, click to look up and select records.
      2. In the Auto Scope with Business Processes field, select Yes.

### Task 3: Generate Framework Assessments

User: Profile Owner

1. In the NIST Profiles record, navigate to the Assessments tab.
2. In the Assessment Generation section, do the following:
   1. In the Framework Library field, click Ellipsis to look up and select the Functions or Categories or Sub-Categories to assess, and click OK.
   2. In the Generate Assessments Flag field, select Yes.
3. Click Save or Save and Close.
4. Wait for the NIST Assessments to generate.

* **Note:** Assessments are generated for each Subcategory 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 4: Determine Target Profile and Assign Assessors

User: Profile Owner

1. In the NIST Profiles record, navigate to the Assessments tab.
2. Navigate to the NIST Assessments cross-reference field to see the Assessments that were generated.
3. In the NIST Assessments section, click Enable Inline Edit.
4. Select the Assessor.
5. Select the Target Tier.
6. Click Save.

### Task 5: Complete Profile Assessment

User: Assessor

1. In the NIST Profiles record, navigate to the Assessments tab.
2. Navigate to the NIST Assessments cross-reference field to see the Assessments that were generated in the previous step.
3. In the NIST Assessments section, to complete the assessments, do one of the following:
   1. Click the Tracking ID of a Framework Assessment Record.
   2. Click Enable Inline Edit.
4. In the Informative Reference column, clickEllipsisto look up and select the Informative Reference for the Subcategory, and click OK.
5. Select the Current Tier.
6. Enter the Implementation Details of how the Subcategory was implemented and assessed.
7. If you are using Inline Edit, click Save Changes. Otherwise, click Save.
8. If the Current Tier does not equal the Target Tier, this means that there is a capability gap, and a Finding record can be created to track the capability gap.
9. For each Framework Assessment, repeat Steps 3-8.

### Task 6: Review Profile

User: Profile Owner

1. In the NIST Profiles record, navigate to the Analysis tab.
2. Review the Assessment Summary section.
3. Provide a response using one of the following steps:
   1. In the NIST Profiles record, navigate to the Risk and Response tab > Risk Response section.
   2. In the NIST Assessments record, navigate to the Response tab > Response section.
4. In the NIST Profiles record, navigate to the Review section.
5. In the Profile Owner Review Status field, select Review Complete.

### Task 7: Archive and Reassess

User: Profile Owner

1. In the NIST Profiles record, navigate to the Assessments Helper section.
2. In the Archive Assessments field, select Yes.
3. Click Save or Save and Close.
4. Repeat tasks 2 through 4 once existing assessments are archived.

## Upgrading the Archer NIST-Aligned Framework App-Packs

### Adding informative reference for NIST-Aligned Framework 2024.03

**Note:** The current Archer content file has Informative Reference for NIST CSF. For other Informative Reference links to Authoritative sources please use the below steps to generate the content file.

* Create a new CSV file. Add data as per below columns.

The file for Informative reference should have the following rows:

| Subcategory (Subcategory(Version)): |
| --- |
| * Framework Version |
| * Authoritative Source (Section - Section ID)/Sub-Section –Sub-Section ID |
| * Framework Source |

Each type of Authoritative Source should have a separate file.

### Change log for NIST-Aligned Framework 2024.03 users.

The following components have been updated as part of the NIST-Aligned Framework 2024.03 release.

**Note:**

* Archer recommends performing an impact analysis of any changes before installing the packages.
* During package installation:
  + If the Upgrade and Create New option is selected, any changes made within applications are replaced by the package.
  + If Override Layout(s) is selected, any existing layouts are overridden.
* After package installation, iViews are not removed from Dashboards, and Reports are not removed from iViews. Removing iView and Dashboard content is a manual task.

The following table describes the changes:

| Component | Updates |
| --- | --- |
| Global Values Lists | Changed:   1. “NIST: Functions” - Added values Govern – AI, Manage – AI, Map – AI, Measure - AI. 2. “NIST: Framework Source” - Added new value NIST AI |
| NIST Framework Library | New Fields Sub Category Level:   1. Implementation Details. |
| NIST Profiles | Layout Objects:   1. Analysis Tab->Section: Current Profile Version Scorecard 2. Report Object: NIST 1.1 vs NIST 2.0   New Fields:   1. Profile Targets Multiple Version ? :   Calculation:IF(      AND(              OR(COUNTIF(REF([Archived NIST Assessments],[Framework Version]),"=2.0")>0,COUNTIF(REF([NIST Assessments],[Framework Version]),"=2.0")>0),              OR(COUNTIF(REF([Archived NIST Assessments],[Framework Version]),"=1.1")>0,COUNTIF(REF([NIST Assessments],[Framework Version]),"=1.1")>0)              ),      VALUEOF([Profile Targets Multiple Version ?],"Yes"), VALUEOF([Profile Targets Multiple Version ?],"No"))  New Data Driven Events:   1. Profile Targets Multiple Version = Yes 2. Filter: Profile Targets Multiple Version contains Yes    1. Action: Display Version Comparison Report Object       1. Apply Conditional Layout: Display Version Comparison Report Object   Updated Data Driven Events:   1. Action: Default Action – Show Capability Gap/Progress Trending – Functions, Hide: Current Profile Version Scorecard |
| NIST Assessments | New Fields:   1. NIST 1.1 Capability Gap 2. NIST 2.0 Capability Gap   Reports:   1. Comparison (Report Object) |

## Certification environment

Date Tested: March 2024

| Product Name | Version Information |
| --- | --- |
| Archer | 2024.03 |