# Archer Australian Incident Management

Archer Australian Incident Management Accelerator provides case management and incident response for reporting and categorizing cyber and physical incidents and determining the appropriate response procedures.

Archer Australian Incident Management Accelerator provides a streamlined version of the Archer Incident Management use case that supports specific requirements for managing incidents in Australia, such as ASIC’s RG78, OAIC, and Corporations Act s912D Checklists.

It provides a metrics dashboard for tracking and reporting the status of all incidents, their costs, related incidents, losses and recovery.

On this page

* [Release history](#Releasehistory)
* [Overview](#Overview)
  + [Key features and benefits](#Keyfeaturesandbenefits)
  + [Prerequisites (System requirements)](#PrerequisitesSystemrequirements)
  + [Compatible use cases and applications](#Compatibleusecasesandapplications)
    - [Related applications](#Relatedapplications)
* [Archer Australian Incident Management Accelerator components](#X05b53857c6408a0ae8a0c36d7f0940dd87810dd)
  + [Architecture diagram](#Architecturediagram)
  + [Process diagrams](#Processdiagrams)
    - [Incidents](#Incidents)
    - [Investigations](#Investigations)
  + [Applications](#Applications)
  + [Personas and access roles](#Personasandaccessroles)
    - [Permissions chart](#Permissionschart)
* [Installing Archer Australian Incident Management Accelerator](#X3b7f1d032c89087b2d4b5f5b58387af362433b4)
  + [Installation overview](#Installationoverview)
    - [Task 1: Prepare for the installation](#Task1Preparefortheinstallation)
    - [Task 2: Install the package](#Task2Installthepackage)
    - [Task 3: Set up data feeds (optional)](#Task3Setupdatafeedsoptional)
    - [Task 4: Test the installation](#Task4Testtheinstallation)
  + [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)
    - [Task 6: Activate advanced workflow](#Task6Activateadvancedworkflow)
  + [Setting up data feeds (optional)](#Settingupdatafeedsoptional)
    - [Task 1: Configure the ‘Create Regulatory Correspondence from Investigations’ data feed](#X236b6458e1565f2d85f62581f049ffd18621528)
    - [Task 2: Schedule a data feed](#Task2Scheduleadatafeed)
* [Using Archer Australian Incident Management Accelerator](#Xb7e66a259a249d267aa97922fb2e852d61e7067)
  + [Task 1: Create incidents](#Task1Createincidents)
  + [Task 2: Incidents – compliance review](#Task2Incidentscompliancereview)
  + [Task 3: Create investigations](#Task3Createinvestigations)
  + [Task 4: Investigation closure](#Task4Investigationclosure)
  + [Task 5: Incidents – incident owner review](#Task5Incidentsincidentownerreview)
  + [Task 6: Incidents – closure sign-off](#Task6Incidentsclosuresignoff)
* [Certification environment](#Certificationenvironment)

## Release history

Last updated: August 2023

## Overview

### Key features and benefits

The Archer Australian Incident Management Accelerator offering enables organizations to:

* Supports the documentation, triage and remediation of compliance and risk incidents.
* Includes a simplified workflow allowing the creation, compliance review, ownership and closure of incidents.
* Helps track due dates in line with regulatory reporting timeframes.
* Ability to track correspondence sent to and received from regulators.
* Supports the process to investigate into serious or likely breach.
* In-built checklists prompt the assessment of whether an incident could be:
  + Breach per Corporations Act 2001 s912D.
  + Reportable situation per Regulatory Guide 78 Breach reporting by AFS licensees and credit licensees (RG 78); or
  + Notifiable data breach per Office of the Australian Information Commissions (OAIC)

### Prerequisites (System requirements)

| Components | Prerequisites |
| --- | --- |
| Archer Solution Area(s) | Archer Business Resiliency |
| Archer Use Case(s) | Archer Incident Management |
| Archer Applications | * Incidents * Investigations * FAR Regulatory Correspondence (Optional) |
| Uses Custom Application | No |
| Requires On-Demand License | No. The offering requires Individual Accountability Management FAR Add-on license if you need to install FAR Regulatory Correspondence application. |
| Archer Requirements | Archer 6.13 and later |
| Prerequisite Requirements | Requirements for the installation and operation of Archer Australian Incident Management Accelerator includes the following use cases:   * Remediation Plans – (Archer Issues Management) |

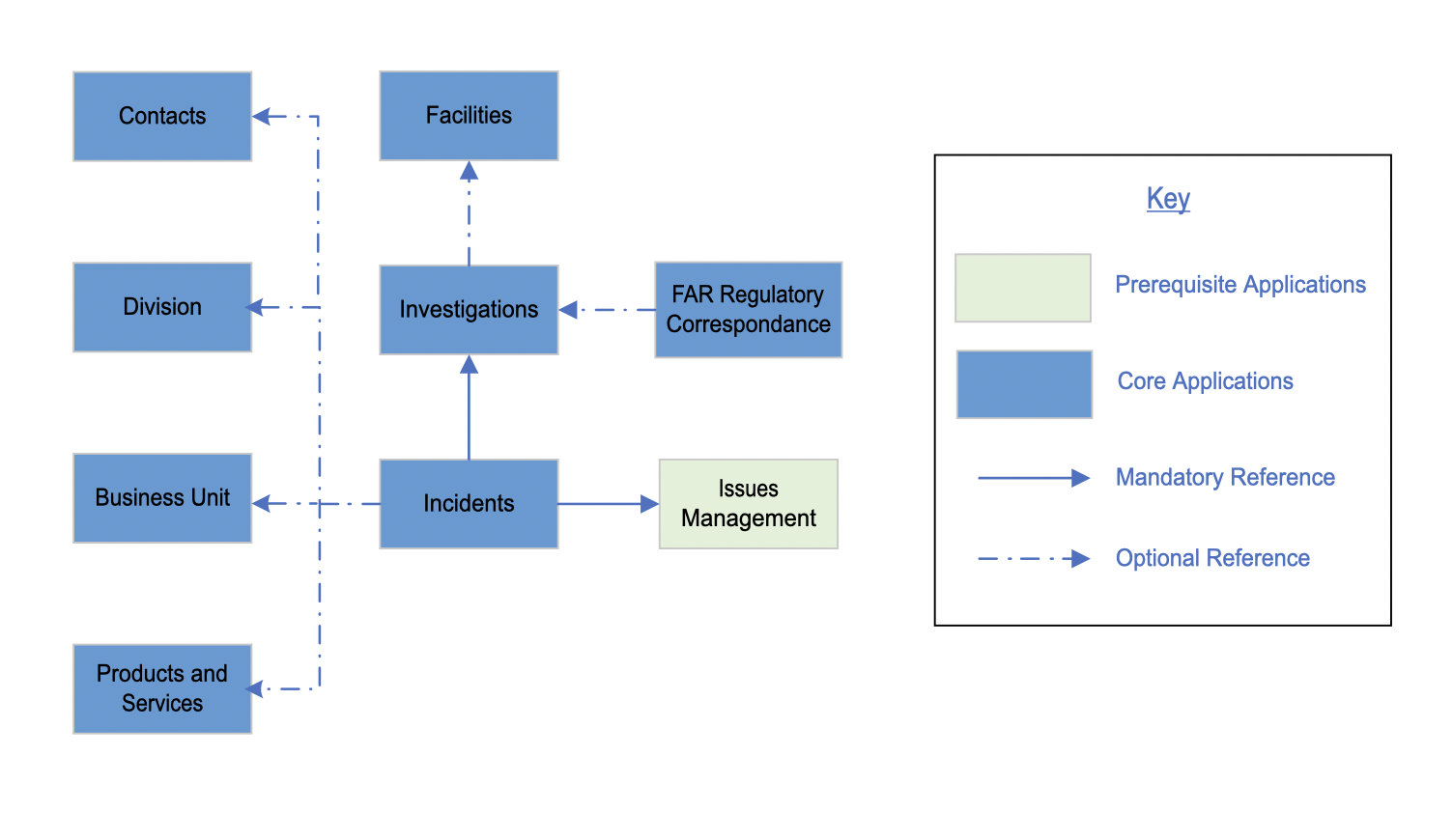
### Compatible use cases and applications

#### Related applications

| Application | Use Case | Primary Purpose(s) of the Relationship |
| --- | --- | --- |
| FAR Regulatory Correspondence | Individual Accountability Management | * You can tie your regulatory correspondence to the investigations. |
| Contacts | Business Asset Catalog | * To identify the Representative on the Incident |
| Business Unit | Business Asset Catalog | * To relate Business Units to the Incident for the Business Unit Impacted and/or the Business Unit where the Incident Occurred. |
| Division | Business Asset Catalog | * To relate Division to the Incident for the Division Impacted and/or the Division where the Incident Occurred. |
| Products and Services | Business Asset Catalog | * To relate Products and Services that are impacted by the Incident. |
| Facilities | Business Asset Catalog | * To relate Facilities that are related to the Investigations. |

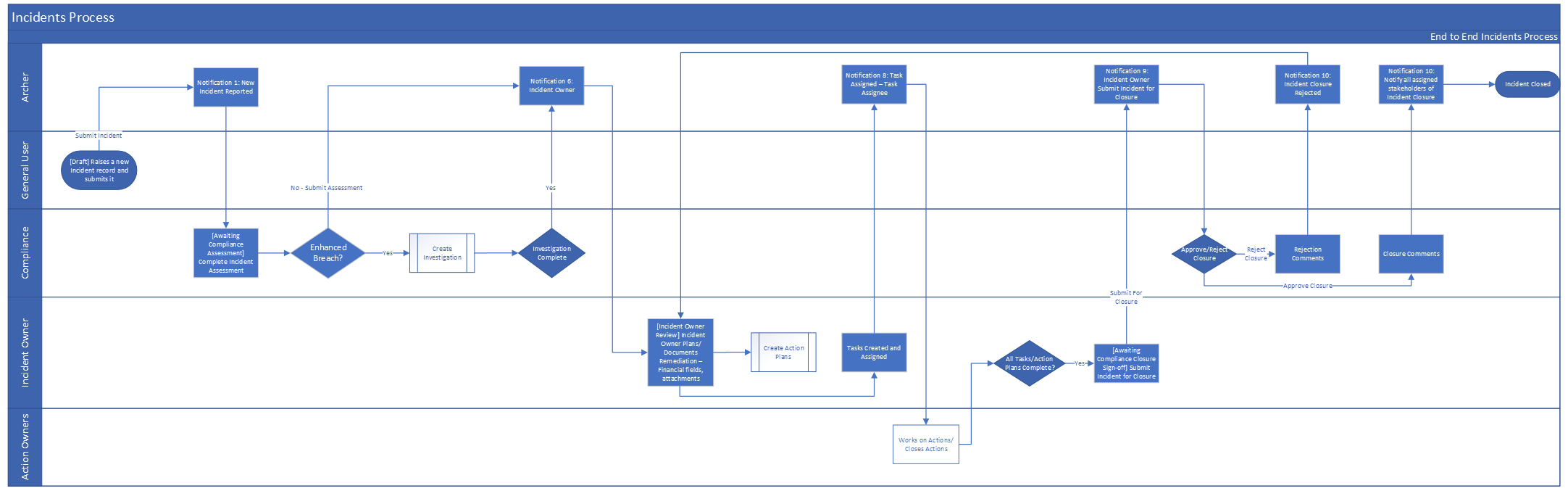
## Archer Australian Incident Management Accelerator components

### Architecture diagram

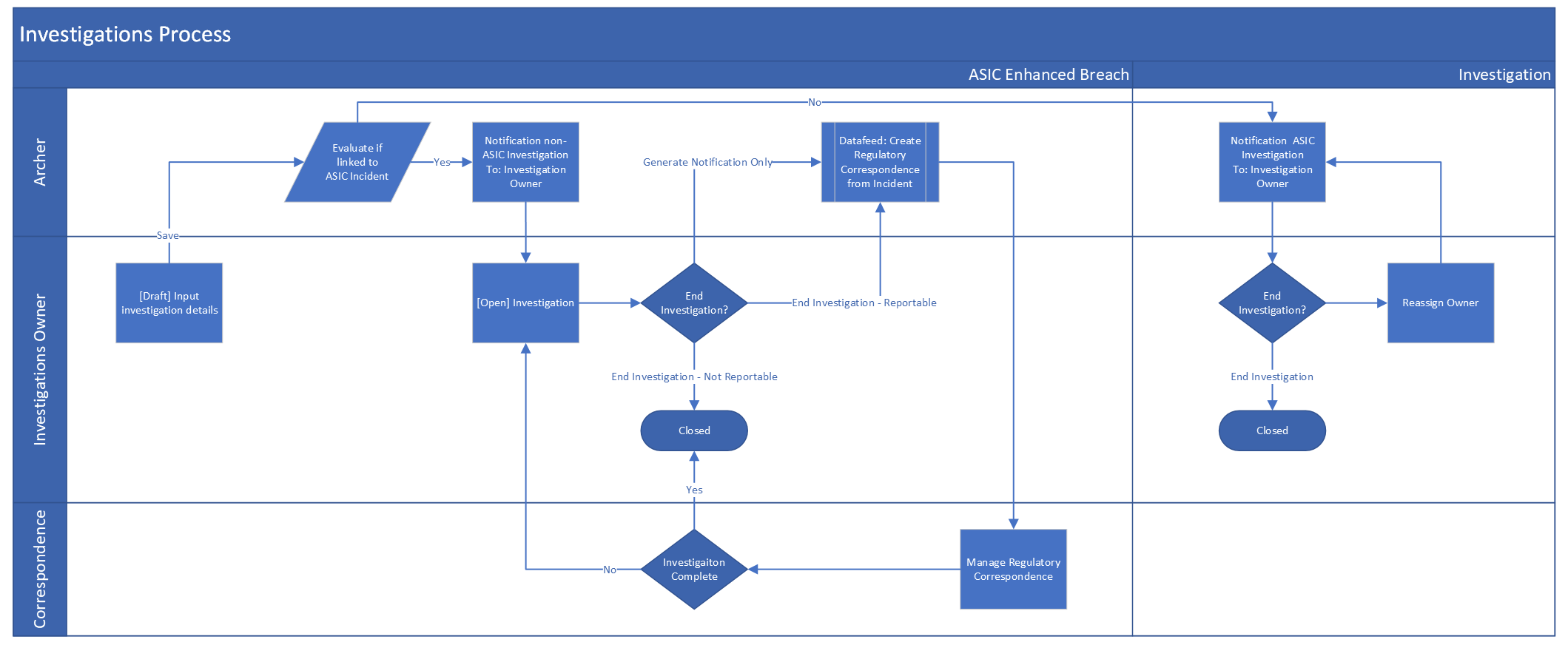


### Process diagrams

#### Incidents



#### Investigations



### Applications

| Application | Description |
| --- | --- |
| Incidents | The Incidents application provides a central repository for reporting incidents and managing the incident lifecycle. Through the Incidents application |
| Investigations | The Investigations application allows you to report and manage investigations for one or more incidents. |
| FAR Regulatory Correspondence | The FAR Regulatory Correspondence application provides the ability to track regulatory communication and track submission of such to the Regulator. |

### 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 |
| --- | --- |
| Compliance Manager | The Compliance Manager is the initial point of contact for intaking and triaging Incidents. The Compliance Manager is responsible for conducting the Impact Assessments, any Breach evaluations and assigning the Incident Owner. Furthermore, the Compliance Manager reviews the Incident once it’s been submitted by the Incident Owner for closure. |
| Incident Owner | The Incident Owner is the individual within the Business who owns the overarching Remediation of the Incident. The Incident Owner is also able to track details around Financial Loss. |
| Incidents Legal Team | The Incident Legal Team is a Group which can be leveraged to notify the Legal department where there might be a breach that requires Legal oversight. The Legal Team isn’t a formal part of the workflow, however they are notified when required as a result of Breach determination by the Compliance Manager. |

#### Permissions chart

| Applications | IM: Admin | IM: Owner | CM: Manager | RM: Manager | Incidents: Legal | Incidents: General User |
| --- | --- | --- | --- | --- | --- | --- |
| Incidents | CRUD | CRU | CRU | CRU | R | CRU |
| Investigations | CRUD | CRU | CRU | CRU | R |  |
| FAR Regulatory Correspondence | CRUD | CRU | CRU | CRU | R |  |
| Remediation Plans | CRU | CRU | CRU | R | R |  |
| Business Unit | RU | RU | RU | R | R |  |
| Division | RU | RU | RU | R | R |  |
| Contacts | RU | RU | RU | R | R |  |
| Products and Services | RU | RU | RU | R | R |  |
| Facilities | RU | RU | RU | R | R |  |

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

**Note:** For detailed, page-level access rights and record level permissions, see the Data Dictionary.

## Installing Archer Australian Incident Management Accelerator

### Installation overview

Complete the following tasks to install the offering.

#### Task 1: Prepare for the installation

1. Ensure that your Archer system meets the following requirements:
   * Archer Platform version 6.13
2. Obtain the Data Dictionary for the app-pack by contacting your Archer Account Representative. The Data Dictionary contains the configuration information for the use case.
3. Read and understand the "Packaging Data" section of Archer Help.

#### Task 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.

#### Task 3: Set up data feeds (optional)

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

#### Task 4: 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 a package installation. Packaging is a powerful feature that can make significant changes to an instance. Archer strongly recommends backing up the instance database before installing a package. This process enables a full restoration if necessary.

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

#### Task 2: Import the package

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

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

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

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

1. In the Available Packages section, select the package you want to map.
2. In the Actions column, click  for that package.

The analyzer runs and examines the information in the package. The analyzer automatically matches the system IDs of the objects in the package with the objects in the target instances and identifies objects from the package that are successfully mapped to objects in the target instance, objects that are new or exist but are not mapped, and objects that do not exist (the object is in the target but not in the source).

**Note:** This process can take several minutes or more, especially if the package is large, and may time out after 60 minutes. This time-out setting temporarily overrides any IIS time-out settings set to less than 60 minutes.

When the analyzer is complete, the Advanced Package Mapping page lists the objects in the package file and corresponding objects in the target instance. The objects are divided into tabs, depending on whether they are found within Applications, Solutions, Access Roles, Groups, Sub- forms, or Questionnaires.

1. 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 | 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 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. Nothing more needs to be done 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 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 Archer 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:
   1. In the toolbar, click Auto Map.
   2. 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. |

* 1. 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.
  1. 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 Checkmark icon is displayed in the tab title. The Missing objects icon is displayed next to the object to indicate that the object will not be mapped.

1. Verify that all other objects are mapped correctly.
2. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in Archer Help.
3. Once you have reviewed and mapped all objects, click .
4. Select I understand the implications of performing this operation and click OK.

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

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

#### Task 4: Install the package

All objects from the source instance are installed in the target instance unless the object can not 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.
   1. From the menu bar, click Admin menu.
   2. Under Application Builder, click Install Packages.
2. In the Available Packages section, locate the package file that you want to install, and click Install.
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. In the Configuration section, under Install Method, 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. In the Configuration section, under Install Option, select an option for each selected component. To use the same Install Option for all selected components, select an option from the top-level drop-down list.

* **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.

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 clean up post-install.
2. Click Install.
3. Click OK.

#### Task 5: Review the package installation log

1. Go to the Package Installation Log tab of the Install Packages page.
   1. From the menu bar, click Admin menu.
   2. Under Application Builder, click Install Packages.
   3. 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.

#### Task 6: Activate advanced workflow

1. Go to the Applications page.
   1. From the menu bar, click Admin menu.
   2. Under Application Builder, click Applications.
2. In the Applications section, select the Incidents Application.
3. On the Advanced Workflow Tab, click ‘Activate’ in the top right corner of the page.
4. Then click ‘Save Workflow’ in the top left corner of the page.
5. Repeat Step 1 above. In the Applications section, select the Investigations Application.
6. On the Advanced Workflow Tab, click ‘Activate’ in the top right corner of the page.
7. Then click ‘Save Workflow’ in the top left corner of the page.

### Setting up data feeds (optional)

If you are using or installed the FAR Regulatory Correspondence application, then configure the below data feed.

#### Task 1: Configure the ‘Create Regulatory Correspondence from Investigations’ data feed

1. Go to the Manage Data Feeds page.
   1. From the menu bar, click Admin menu.
   2. Under Integration, click Data Feeds.
2. In the Manage Data Feeds section, locate and select the ‘Create Regulatory Correspondence from Investigations’ data feed.
3. From the General tab in the General Information section, in the Status field, select Active.
4. Click the Transport tab. Complete the fields in the Transport Configuration section as follows: In the URL field, type: YourServerName/VirtualDirectoryName/ws/search.asmx
5. In the User Name 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).
6. 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).
7. Verify the settings on the Source Definition tab. This will be pre-configured to identify the necessary fields.

* **Note:** The Type and Clear Notification Helper Field on the Source Definition tab will be automatically populated when you install the data feed. Repopulating the fields by clicking on “Load Fields” will lead to removal of these pre-populated fields from the list. Hence, follow the below steps to add the two fields in Source definition tab:
* Add a new field by clicking on “Add New” and rename as “Type” and select field type “Static Text” with appropriate value “Breach” in the Text editor.
* Add a new field by clicking on “Add New” and rename as “Clear Notification Helper” and select field type “Static Text” with appropriate value “Created” in the Text editor. Also, be sure that the data mappings are configured correctly after the load fields.

1. Verify that except for the Regulatory Correspondence, key field values are not missing from the data feed setup window.
2. Click Save.

#### Task 2: Schedule a data feed

**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 is displayed. 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.
   1. From the menu bar, click Admin menu.
   2. Under Integration, click Data Feeds.
   3. Select the data feed.
   4. Click the Schedule tab.
2. Go to the Recurrences section and complete frequency, start and stop times, and time zone.
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.

## Using Archer Australian Incident Management Accelerator

### Task 1: Create incidents

User: General User

1. Create Incidents record.
   1. From the menu bar, click on the dropdown beside Incident Management Accelerator Workspace.
   2. Under Individual Incident Management > Incidents, click on New Record.
2. Fill in the following information in Event Information section:
   1. Enter Incident Name.
   2. Enter the Incident Description.
   3. Enter the details about How did the Incident Happen.
   4. Enter the details about Initial Actions Taken.
   5. Select Incident Cause by clicking Ellipsis  and making your selection.
   6. Select Interaction Point Affected by clicking Ellipsis  and making your selection.
   7. Select the Date Discovered, Date Occurred, and Date Reported by clicking the calendar icon next to the field
   8. Complete the remaining fields in the Event Information section.
3. (Optional) Add attachments/documentation to the record by clicking the | Add New | button in the Supporting Documentation field.
4. Once the record is complete, click Save in the Record Toolbar to save in record.
5. Click Submit Incident at the top left of the screen.

### Task 2: Incidents – compliance review

Users: Compliance Manager

1. Select the Incidents record you want to provide response by clicking the Incident Name under the Tasks section on your Task landing screen.
2. Click Edit in the top of the record.
3. Select user from the list in the Incident Owner field by clicking Ellipsis from the Incident Stakeholders section.
4. In the Intake Assessment section:
   1. Select Impact Assessment by clicking the down arrow next to the field and making your selection.
   2. Select Regulator by clicking Ellipsis and making your selection.
   3. If Impact Assessment is Critical OR Remediation Plan is Required for the Incident. Enter details in the Compliance Remediation Recommendations.
   4. Complete the remaining fields in the section.
5. In the Breach Assessment section:
   1. Select PotentialBreach? by clicking the down arrow next to the field and making your selection.
   2. If Potential Breach = Yes, select user from the list in the Applicable Legal Team field by clicking Ellipsis.
   3. If s912D Checklist Required? = Yes, complete the s912D Assessment section.
      1. If s912D Checklist Q5 = Yes, complete the Reportable Situation section.
      2. In the Reportable Situation section: if RG78 Checklist Q3 = Yes, then create Investigations by clicking the | Add New | button in the Investigations field. Refer below Tasks 3 and 4 for more details.
   4. If OAIC Assessment Required? = Yes, complete the OAIC Assessment section.
6. (Optional)Add Comments to the record by clicking the | Add New | button in the Comments section.
7. Click Save in the Record Toolbar.
8. Click Submit Assessment from the Actions dropdown at the top left of the screen.

### Task 3: Create investigations

User: Compliance Manager

1. Create Investigations record.
   1. From the menu bar, click on the dropdown beside Incident Management Accelerator Workspace.
   2. Under Individual Incident Management > Investigations, click on New Record.
2. Fill in the following information in General Information section:
   1. Enter Investigation Request Name.
   2. Select Related Incidents by clicking Ellipsis in the Target field.
3. In the Investigator Assignments section:
   1. Select user from the list in the Investigation Owner field by clicking Ellipsis.
   2. Select user from the list in the Investigation Manager field by clicking Ellipsis.
4. In the Investigation Request Information section:
   1. Select Request Type and Urgency by clicking the down arrow next to the field and making your selection.
   2. Select Investigation Location by clicking Ellipsis and making your selection.
   3. Enter Request Description.
5. Once the record is complete, click Save in the Record Toolbar to save in record.

### Task 4: Investigation closure

Users: Compliance Manager

1. Select the Incidents record you want to provide response by clicking the Incident Name under the Tasks section on your Task landing screen.
2. Click Edit in the top of the record.
3. Navigate to Investigation Outcome section.
4. Not a Reportable Situation
   1. Select ‘Not a Reportable Situation’ value in the Reportable Situation Resolution field.
   2. Click on End Investigation – Not Reportable from the Actions dropdown at the top left of the screen.
5. Reportable Situation
   1. Select relevant value in the Reportable Situation Resolution field.
   2. Enter details in the Investigation Outcome field.
6. Click on End Investigation – Reportable from the Actions dropdown at the top left of the screen.

### Task 5: Incidents – incident owner review

Users: Incident Owner

1. Select the Incidents record you want to provide response by clicking the Incident Name under the Tasks section on your Task landing screen.
2. Click Edit in the top of the record.
3. Navigate to the Resolution tab.
4. In the Financial Analysis section:
   1. Enter Financial Loss Amount, Recovered Amount and Amount Gained.
   2. Enter details in Cost Calculation field.
5. Create Remediation Plans by clicking the | Add New | button in the Remediation Plans section.
6. (Optional) Add Comments to the record by clicking the | Add New | button in the Comments section.
7. Click Save in the Record Toolbar.
8. Click Submit for Closure from the Actions dropdown at the top left of the screen.

### Task 6: Incidents – closure sign-off

Users: Compliance Manager

1. Select the Incidents record you want to provide response by clicking the Incident Name under the Tasks section on your Task landing screen.
2. Click Edit in the top of the record.
3. To Approve the incident closure
   1. Review the information in the Incidents Record.
   2. Enter comments in the Compliance Closure Comments field.
   3. Click on Approve Closure from the Actions dropdown at the top left of the screen.
4. To Reject the response:
   1. Click on Reject Closure from the Actions dropdown at the top left of the screen.
   2. Document the reason for rejecting the response in the Compliance Closure Rejection Comments field.
   3. Click on Submit from the Actions dropdown at the top left of the screen.
5. (Optional) Add Comments to the record by clicking the | Add New | button in the Comments section.
6. Click Save in the Record Toolbar.

## Certification environment

Date tested: August 2023

| Product Name | Version Information | Operating System |
| --- | --- | --- |
| Archer | 6.13 | Virtual Appliance |