# Archer OMB A-123-Aligned Accelerator

OMB A-123, or Office of Management and Budget Circular A-123, serves as a directive from the Office of Management and Budget (OMB) to federal agencies, offering guidance on internal controls and financial management. Its primary aim is to establish, assess, and maintain internal controls within agencies to ensure the efficient utilization of resources, reliable financial reporting, and compliance with relevant laws and regulations.

The Archer OMB A-123-Aligned Accelerator provides workflow and updates to existing use cases for Government entities to maintain compliance with the OMB A-123 regulation, which outlines the management of risk alongside internal controls, including the required processes and activities, such as testing internal controls.  Organizations can conduct an assessment on an internal control, identify the risks and control activities, communicate the results internally and externally, and continually monitor the controls for improvement.

On this page

* [Release history](#Releasehistory)
* [Overview of OMB A-123-Aligned Accelerator](#OverviewofOMBA123AlignedAccelerator)
  + [Key features and benefits](#Keyfeaturesandbenefits)
  + [Prerequisites (ODA and system requirements)](#PrerequisitesODAandsystemrequirements)
  + [Compatible use cases and applications](#Compatibleusecasesandapplications)
    - [Related applications](#Relatedapplications)
  + [Impacted use case(s)](#Impactedusecases)
* [Archer OMB A-123-Aligned Accelerator components](#Xd29a30679ee8846d6e37dc5f53aba807e3a9675)
  + [Architecture diagram](#Architecturediagram)
  + [Swim Lane diagram](#SwimLanediagram)
  + [Applications](#Applications)
  + [Personas and Access Roles](#PersonasandAccessRoles)
* [Installing Archer OMB A-123-Aligned Accelerator](#X5f6f3f8c9688a689eed12528525bc200e2e4d5e)
  + [Security considerations](#Securityconsiderations)
  + [Installation overview](#Installationoverview)
    - [Step 1: Prepare for the installation](#Step1Preparefortheinstallation)
    - [Step 2: Install the package](#Step2Installthepackage)
    - [Step 3: Set up data feeds](#Step3Setupdatafeeds)
    - [Step 4: Test the installation](#Step4Testtheinstallation)
  + [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 Archer OMB A-123-Aligned Accelerator](#UsingArcherOMBA123AlignedAccelerator)
  + [Task 1: Describe the task](#Task1Describethetask)
* [Certification environment](#Certificationenvironment)

## Release history

Last updated: May 2024

## Overview of OMB A-123-Aligned Accelerator

### Key features and benefits

With the offering, you will be able to:

* Document, test, and manage changes to key control flows and processes that affect reporting elements.
* Create projects to manage the compliance testing and determine what controls should be in scope for each test cycle.
* Catalog a consolidated view of risks and internal controls within the organization.
* Monitor risks against established tolerances and risk appetite.
* Manage risk alternatives on a consolidated basis.
* Ensure that all stakeholders are engaged in risk management commensurate with their scope of responsibility.
* Provide consistent risk and control reports from one consistent system of record.
* Establish an organized, managed process to escalate, approve, and remediate.

### Prerequisites (ODA and system requirements)

The following table lists the components and prerequisites for Archer OMB A-123-Aligned Accelerator.

| Components | Prerequisites |
| --- | --- |
| Archer Solution Area(s) | * Archer Regulatory & Corporate Compliance Management * Enterprise and Operational Risk Management |
| Archer Use Case(s) | * Top-Down Risk Assessment * Control Assurance Program Management * Financial Controls Monitoring * Key Indicator Management * Bottom-Up Risk Assessment * Issues Management |
| Uses Custom Application | No |
| Requires On-Demand License | Zero (0) Archer On-Demand Application (ODA) licenses are required for this offering. |
| Archer Requirements | Archer Platform Release 2024.03 and later |
| Partner/Vendor Requirements | N/A |
| Operating System | Windows Server 2022 R2 |
| Database Server | Microsoft SQL Server 2022 (64-bit) |
| Supported Archer Environments | * On-Premises * Archer SaaS |

### Compatible use cases and applications

#### Related applications

| Application | Use Case | Primary Purpose(s) of the Relationship |
| --- | --- | --- |
| Third Party Profile | Third Party Catalog | * If third parties are involved. The profiles can be linked in the Control Procedures Application. |
| Loss Events | Loss Event Management | * Can be linked to Risk Profiles for tracking losses. |
| BCDR Plan | Business Continuity & IT Disaster Recovery Planning | * Lists business continuity and/or disaster recovery plan related to risk |
| Authoritative Sources | Policy Program Management | * Define business context for the identified risk |
| Policies | Policy Program Management | * Define business context for the identified risk and root cause analysis |

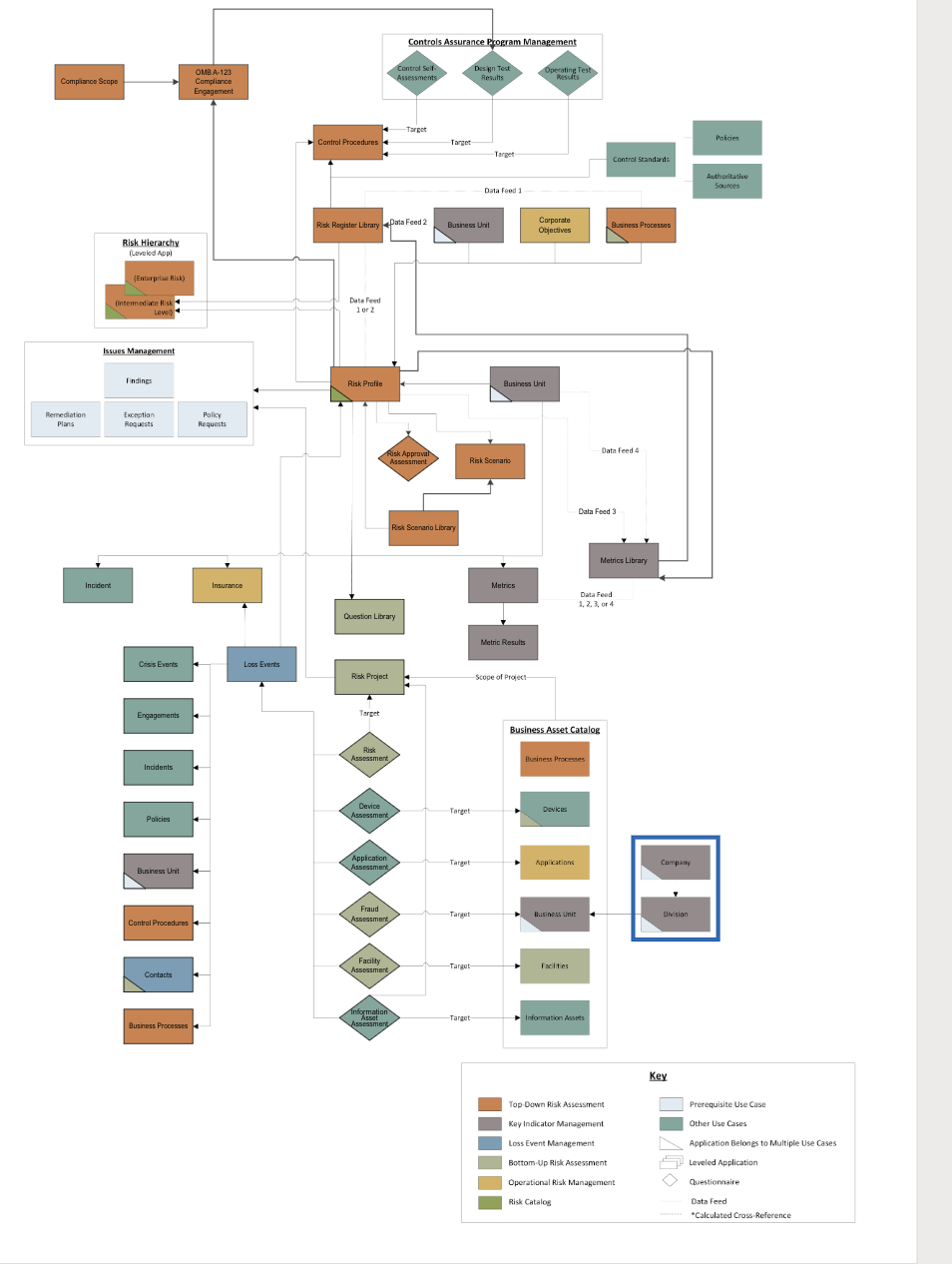
### Impacted use case(s)

| Archer Use Case(s) |
| --- |
| Top-Down Risk Assessment |

## Archer OMB A-123-Aligned Accelerator components

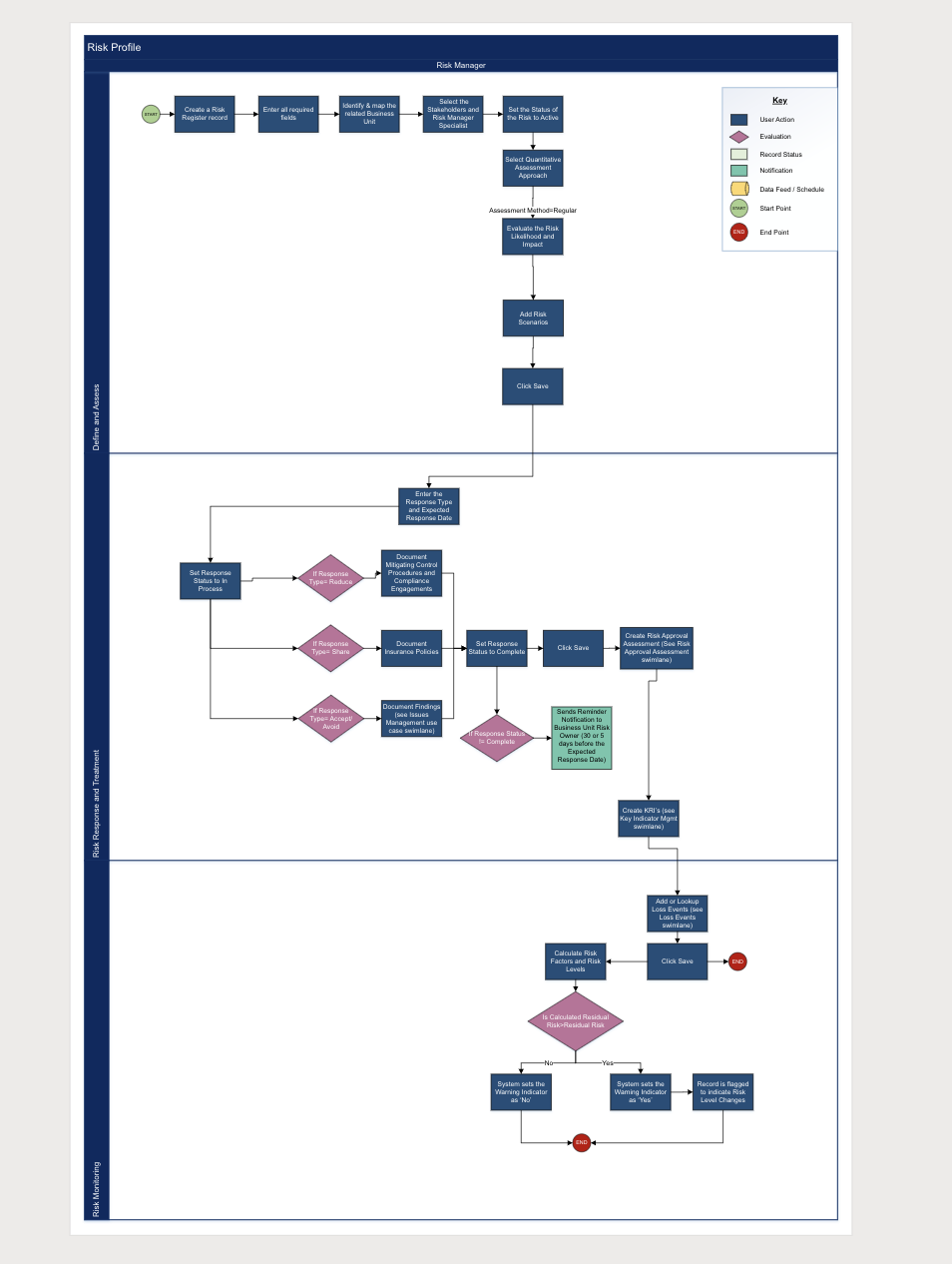
### Architecture diagram

The following diagram shows the relationships between the applications that make up Archer OMB A-123-Aligned Accelerator.



### Swim Lane diagram

The following diagram shows the general workflow of the application.



### Applications

The following table describes the OMB A-123 applications.

| Application | Description |
| --- | --- |
| Business Processes | The Business Processes application captures the base data for a given process. A process may be assigned to a particular business unit or shared across multiple business units. The application enables you to track the business processes personnel, business impact, and ITIL category, and associate it with other aspects of the enterprise infrastructure. |
| Contacts | The Contacts application serves as a central repository for contact information, is utilized across multiple areas of Archer, and contains information that is often leveraged by other use cases. Updates to a profile record within this application automatically propagate in any records where that contact information is displayed. |
| Business Unit | The Business Unit application provides the user with a detailed view of all activities related to the specific business unit. Utilizing this application, users can view related risks, control procedures, incidents, products and services and other enterprise-level information and see how changes to these related elements influence the overall business unit. In addition, users can determine whether an individual business unit falls into the "in scope" category for assessments and audits, as well as evaluate the business unit's overall risk and compliance. |
| Business Process | The Business Processes application captures the base data for a given process. A process may be assigned to a particular business unit or shared across multiple business units. Processes are related to products and services, applications, controls, scoping decisions and process walk-throughs. |
| Authoritative Sources | The Authoritative Sources application allows you to centrally manage standards, regulations, laws, and requirements and map them to the policies and control standards for rationalization purposes. The authoritative source repository provides you with a meaningful understanding of what guides and governs your business, and it allows you to formulate policies appropriately to aid in demonstrating regulatory compliance. |
| Risk Hierarchy | This Risk Hierarchy application coupled with the Risk Profile application creates a 3-level risk roll-up solution. This application enables an organization to roll-up their risks from the risk Profile to an intermediate summary level, and then to an enterprise summary level. |
| Risk Project | The purpose of the Risk Project application is to provide a repository for all risk-related projects. Project records follow a comprehensive, start-to-finish approach, and include sections for project staffing and scoping, risk identification, risk analysis and risk treatment. |
| Risk Scenario | The Risk Scenario application allows Risk Managers to break down a Risk Profile record into a smaller, more assessable unit by defining conditions and parameters that make the scenario unique.  Such parameters might include frequency, stakeholders, specific product lines and any other condition that would need a separate assessment. This now defined scenario can then be assessed to provide a more precise analysis of risk. Through the Risk Scenario application you can: - Define and Review the parameters of your scenarios as they relate to your risks - Analyze and Assess your risk scenarios |
| Risk Scenario Library | The Risk Scenario Library application serves as a catalog of Risk Scenario templates. Those templates can be used to generate new Risk Scenario records without having to create them from scratch. Those scenarios can then be linked to Risk Profile records for analysis purposes. |
| Control Procedures | The Control Procedures application supports the Archer Regulatory & Corporate Compliance Use Cases. It serves as a central repository for instances of control procedures, baselines and activities that are mapped to corporate Master Controls, establishing the foundation for enterprise-wide risk monitoring and compliance measurement. Control Procedures are categorized into two types: Technical and Process. Based on the selected type, different pieces of information are captured, and different testing options are made available. |
| OMB A-123 Compliance Engagement | The Compliance Engagement application enables the Compliance Team to create engagements targeting certain compliance scopes, control sets, or control instances, to kick off and manage the lifecycle of testing, and to report on the results of testing to executive management. |
| Metrics | The Metrics application allows you to establish periodic measurements for objectives, including key performance indicators (KPIs) and key risk indicators (KRIs). Each metric can be related to risks in the Risk Profile application and corporate objectives tracked in the Archer Policy Management solution. |
| Metrics Library | The Metrics Library application contains a master inventory of pre-approved metrics that can be drawn upon by practitioners as a template for metrics placed into production within an Operational Risk Management Program. Metrics placed in the Metrics Library will typically be approved by the risk management team and serve to speed up the process of developing a metrics program and ensuring consistency in metrics used across the organization. |
| Metrics Results | The Metrics Library application contains a master inventory of pre-approved metrics that can be drawn upon by practitioners as a template for metrics placed into production within an Operational Risk Management Program. Metrics placed in the Metrics Library will typically be approved by the risk management team and serve to speed up the process of developing a metrics program and ensuring consistency in metrics used across the organization. |

### 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 |
| --- | --- |
| OMB Admins | Improves program outcomes & develops proposals to comply with detected risks. |
| OMB Management | Designs internal control system. |
| OMB Contracting or Grants & Program Officers | Manages risk of fraud in Federal operations. |
| OMB Internal/External Auditors | Conducts independent and objective audits, evaluations, & investigations. Keeps management informed of risks detected. |
| OMB Executives | Oversees the establishment of the Agency’s risk profile, regular assessment of risk, and development of appropriate risk response |

## Installing Archer OMB A-123-Aligned Accelerator

### 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. Client is solely responsible for ensuring that the installation of the application is performed in a secure manner. Archer recommends clients 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.

#### Step 3: Set up data feeds

You must import and schedule each use case data feed that you want to use. See Setting Up Data Feeds for complete information.

#### Step 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 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, 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 Admin menu> 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 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:
     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, in the Actions column, click Undo.
  + 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 "Importing and Exporting Mapping Settings" in the Archer Platform Help.
3. Once you have reviewed and mapped all objects, click Execute.
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:** 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 Admin menu> 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. Items in the package that do not match an existing item in the target instance are selected by default.
4. 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 Admin menu> 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

Import the data feeds in the following order:

| Data Feed | Description |
| --- | --- |
| Generate Findings for Risk Profile | Generates finding automatically when residual Risk is greater than the average Risk appetite. |
| RCCM: Scope Compliance Engagement by Control Procedures/Control Set | Uses identified Control Set values within Control Procedures records to identify Control Procedures matching the selected criteria and associates any related data to the Compliance Engagement Record. Business Processes, Facilities, Primary Controls, and Applications are linked to Control Procedures. Information Assets, Storage Devices, and Devices are linked to Applications. The data feed creates a Scoping Unit record for each Control Procedure that is associated to the Compliance Engagement. |
| RCCM: Scope Compliance Engagement by Compliance Scope | Uses identified Compliance Scope records and associates any related data to the Compliance Engagement Record. Control Procedures, Primary Controls, Business Processes, Applications, Devices, Storage Devices, Facilities, and Information Assets that are related to the Compliance Scope record are linked to the Compliance Engagement record. The data feed creates a Scoping Unit record for each Control Procedure that is associated to the Compliance Engagement. |
| RCCM: Scope Compliance Engagement by Compliance Scope/Control Set | Uses identified Compliance Scope records and associates any related data to the Compliance Engagement Record. Control Procedures, Primary Controls, Business Processes, Applications, Devices, Storage Devices, Facilities, and Information Assets that are related to the Compliance Scope record are linked to the Compliance Engagement record. The data feed creates a Scoping Unit record for each Control Procedure that is associated to the Compliance Engagement. |
| Create Metrics from Metric Library Risks | Targets the Risk Generator application and allows users to create Risk Profile records based on their selections for Risk Statements and impacted targets (for example, business units or facilities). |

#### Task 1: Import a 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, 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 is completed successfully.
   * Run Now.
3. To save the data feed, click Save or Save and Close.

## Using Archer OMB A-123-Aligned Accelerator

### Task 1: Describe the task

Create and Manage Risk

User: OMB: Admins, OMB Executives

1. Login into Archer and expand the Operation Risk Management Workspace.
2. Go to Top-Down Risk Assessment Solution.
3. Create Risks Profile.
   1. In the Business Context Tab
      1. Populate Objective.
   2. In the Risk Alternatives Tab
      1. Inherent Likelihood.
      2. Residual Likelihood.
      3. Inherent Impact
      4. Residual Impact.
   3. In the Risk Analysis
      1. Avg Calculated Risk Appetite
      2. Average Risk Level Status
      3. Add Risk Scenario.
      4. Possible to add via Data feed.
4. In the Risk Response Section
   1. Add Risk Type
   2. Add Mitigating control procedures and follow the control Procedure workflow.
   3. Add OMB A-123 Compliance Engagement and follow the workflow. In the Engagement Record add
      1. Scope via Data feed for scope.
      2. Testing via Data feed for test.
   4. Finding to be created via Automatic Data feed.
5. Risk Monitoring Section
   1. Add KRI added and follow the KRI workflow.
   2. Metrics Records can be added via Datafeed.
6. Save.

**Note:** The Data feeds which are to be run can be found in the Data feed Section.

## Certification environment

Date Tested: May 2024

| Product Name | Version Information | Operating System |
| --- | --- | --- |
| Archer | 2024.03 | Windows |