# Archer IIC-Aligned IoT Security Maturity Assessment

With the increase of usage for Internet of Things (IoT) devices, organizations need to understand where to focus attention when implementing IoT devices in regard to security to minimize the risks and threats to the organization. They need to ensure that the appropriate security controls are in place. Without properly identifying the security gaps, organizations may be investing in unnecessary security measures. Deciding where to focus limited security resources is a challenge for most organizations given the complexity of a constantly changing security landscape.

The Security Maturity Model (SMM) was developed by the Industrial Internet Consortium (IIC) to provide a framework for IoT.  This framework helps organizations to understand where they are as far as security is concerned and identify the gaps from where they would like to be.  It describes security domains and various techniques available and guidance as to which mechanisms can be used to achieve the desired security maturity level.

The Archer IIC-Aligned IoT Security Maturity Assessment solution allows customers to create an IoT Security Risk Profile to capture the risk assessments and their results. In addition, it tracks the current security maturity level and the progress to achieving the target security maturity level.

On this page

* [Release notes](#Releasenotes)
* [Overview of Archer IIC-Aligned IoT Security Maturity Assessment](#X029f89e3035b900a8517e9bb390f5f806d158ea)
  + [Key features and benefits](#Keyfeaturesandbenefits)
  + [Prerequisites (ODA and system requirements)](#PrerequisitesODAandsystemrequirements)
  + [Compatible use cases and applications](#Compatibleusecasesandapplications)
    - [Related applications](#Relatedapplications)
* [Archer IIC-Aligned IoT Security Maturity Assessment components](#Xe34f4cb1265146d601d8b56234039eeffb7bff5)
  + [Architecture diagram](#Architecturediagram)
  + [Swim lane diagram](#Swimlanediagram)
  + [Applications](#Applications)
  + [Personas and access roles](#Personasandaccessroles)
* [Installing Archer IIC-Aligned IoT Security Maturity Assessment](#X425b1ca48bb4a2224750e1951ce387ddee5791d)
  + [Installation overview](#Installationoverview)
    - [Task 1: Prepare for the installation](#Task1Preparefortheinstallation)
    - [Task 2: Install the package](#Task2Installthepackage)
    - [Task 3: Set up data feeds](#Task3Setupdatafeeds)
    - [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](#Settingupdatafeeds)
* [Using Archer IIC-Aligned IoT Security Maturity Assessment](#Xef0f8bf7e38ad737e5880d82a4e7f14fc970630)
  + [Task 1: Create a new IoT security profile](#Task1CreateanewIoTsecurityprofile)
  + [Task 2: Generate IoT Security Maturity Assessments](#X1a4dacf5f39e8626a253235186b13c771add1b2)
  + [Task 3: Complete IoT Security Maturity Assessments](#Xbd7bd75071e8f2384fa3e65edb1a97b7a6c1451)
  + [Task 4: Archive and reassess](#Task4Archiveandreassess)
* [Certification environment](#Certificationenvironment)

## Release notes

| Archer Version | Published Date | Notes |
| --- | --- | --- |
| 6.7 | May 2020 | Initial Release |
| 6.12 | May 2023 | Recertification |

## Overview of Archer IIC-Aligned IoT Security Maturity Assessment

### Key features and benefits

The Archer IIC-Aligned IoT Security Maturity Assessment offering enables organizations to:

* Create an IoT Security Risk Profile to capture maturity assessment and results
* Identify the scope of the security maturity assessment
* Determine current security posture and desired security maturity level
* Develop remediation plans to address gaps in security posture and maturity

Benefits include:

* Understand security posture for IoT implementations
* Minimize impacts to the organization through proper mitigation of security risks
* Prioritize security resources for IoT implementations
* Compliance with standards and regulations through implementing appropriate security measures

### Prerequisites (ODA and system requirements)

| Components | Prerequisites |
| --- | --- |
| Archer Requirements | Archer 6.12 and later |
| Requires On-Demand License | Yes. The Archer IIC-Aligned IoT Security Maturity Assessment App-Pack requires two (2) On-Demand Applications license. |
| Archer Applications | * IoT Security Profiles * IoT Security Maturity Assessment |
| Pre-requisite Applications | Requirements for the installation and operation of Archer IIC-Aligned IoT Security Maturity Assessment includes the following applications:   * Exception Requests– Archer Issues Management * Remediation Plans – Archer Issues Management |

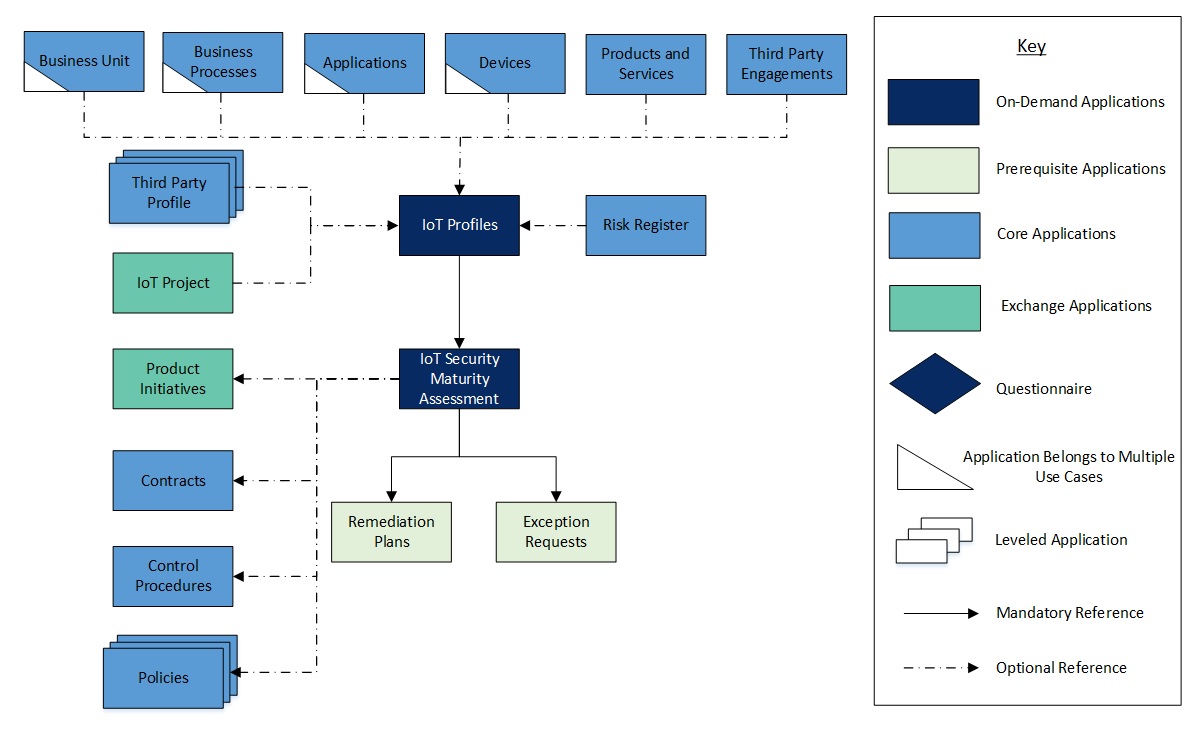
### Compatible use cases and applications

#### Related applications

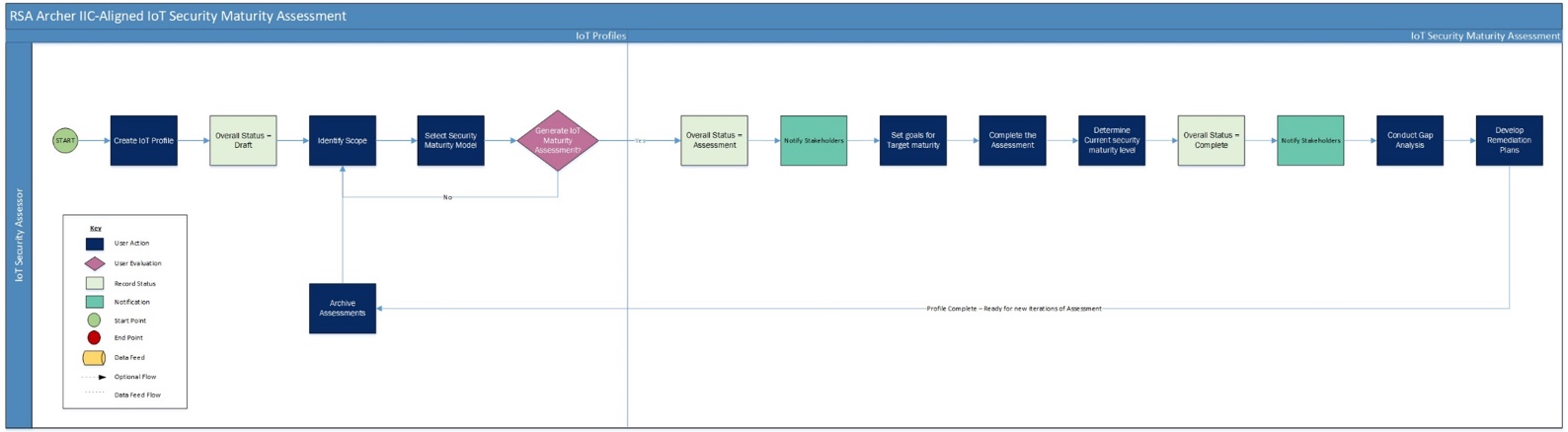
| Application | Use Case | Primary Purpose(s) of the Relationship |
| --- | --- | --- |
| Business Unit | Archer Issues Management, Archer Business Impact Analysis, Archer Third Party Catalog, Archer Policy Program Management, Archer Cyber Incident & Breach Response, Archer Key Indicator Management, Archer IT Asset Catalog, Archer Business Asset Catalog, Archer Federal Assessments & Authorizations, Archer Federal Continuous Monitoring | * To relate Business Units that are impacted by the IoT Profiles |
| Business Processes | Archer Audit Engagements & Workpapers, Archer Business Impact Analysis, Archer IT Risk Management, Archer Controls Assurance Program Management, Archer Data Governance, Archer Top-Down Assessment, Archer Policy Program Management, Archer IT Controls Assurance, Archer Business Asset Catalog, Archer Bottom-Up Risk Assessment, Archer Federal Assessments & Authorizations, Archer Federal Continuous Monitoring. | * To relate Business Processes that are impacted by the IoT Profiles |
| Applications | Archer Audit Engagements and Workpapers, Archer Business Continuity and IT Disaster Recovery Planning, Archer Third Party Governance, Archer IT Asset Catalog, Archer IT Controls Assurance, Archer IT Security Vulnerabilities Program, Archer IT Risk Management, Archer Cyber Incident & Breach Response, Archer Data Governance, Archer PCI Management, Archer Information Security Management System, Archer Operational Risk Management, Archer Federal Continuous Monitoring | * To relate Applications that are impacted by the IoT Profiles |
| Devices | Archer Audit Engagements and Workpapers, Archer Business Continuity and IT Disaster Recovery Planning, Archer Third Party Governance, Archer IT Asset Catalog, Archer IT Controls Assurance, Archer IT Security Vulnerabilities Program, Archer IT Risk Management, Archer Cyber Incident & Breach Response, Archer PCI Management, Archer Information Security Management System, Archer Data Governance, Archer Federal Continuous Monitoring | * To relate Devices that are impacted by the IoT Profiles |
| Products and Services | Archer Business Continuity and IT Disaster Recovery Planning, Archer Third Party Risk Management, Archer Cyber Incident and Breach Response, Archer Controls Monitoring Program Management, Archer Business Asset Catalog, Archer Controls Monitoring Program Management, Archer Bottom-Up Risk Assessment | * To relate Products and Services that are impacted by the IoT Profiles |
| Third Party Profile | Archer Business Continuity and IT Disaster Recovery Planning, Archer Information Security Management System, Archer IT Risk Management, Archer Top-Down Assessment | To identify, track and provide visibility for Initiatives that pose a risk to theorganization |
| Third Party Engagements | Archer Third Party Catalog, Archer Third Party Risk Management, Archer Third Party Engagement | * To relate Engagements to the IoT Profiles |
| Contracts | Archer Third Party Catalog | * To relate Contracts to the IoT Profiles |
| Control Procedures | Archer IT Controls Assurance, Archer Information Security Management System, Archer PCI Management, Archer IT Risk Management, Archer Controls Assurance Program Management, Archer Data Governance, Archer Top-Down Assessment, Archer Federal Assessments & Authorization | * To relate impacted/in place Control Procedures to IoT Profiles |
| Policies | Archer Policy Program Management | * To relate Policies to the IoT Profiles |
| Product Initiatives | Archer Product Security Development Assessment | * To relate Product Initiatives to the IoT Profiles |
| IoT Project | Archer IoT Project Readiness | * To relate IoT Projects to the IoT Profiles |
| Risk Register | IT Risk Management, Top-Down Risk Assessment, Risk Catalog, Information Security Management System | * Risks can be documented and tracked |

## Archer IIC-Aligned IoT Security Maturity Assessment components

### Architecture diagram



### Swim lane diagram



### Applications

| Application | Description |
| --- | --- |
| IoT Profiles | The IoT Profiles application captures the scope of the assessment, target security goals, target, and current security maturity levels. It also tracks the remediation plans to address the gaps in the current and target maturity levels. |
| IoT Security Maturity Assessment | The IoT Security Maturity Assessment application captures the results to determine the current security maturity level.  It also documents the evidence for assessment. |

### 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 (per Information System)? | Optional / Required |
| --- | --- | --- | --- |
| IoT Security Assessor | Responsible for defining the scope of the assessment, conducting the security maturity assessment, and managing the action plans for mitigation of risks.  This person may be someone from the IT Security department or someone who is responsible for the implementation of the IoT project. | Many | Required |

| Applications | IoT Security Assessor |
| --- | --- |
| IoT Profiles | CRU\* |
| IoT Security Maturity Assessment | RU |
| Remediation Plans | CRU |
| Exceptions Requests | CRU |
| Business Units | R |
| Business Processes | R |
| Applications | R |
| Devices | R |
| Products and Services | R |
| Third Party Profile | R |
| Third Party Engagements | R |
| Contracts | R |
| Control Procedures | R |
| Policies | R |
| Risk Register | R |
| Product Initiatives | R |
| IoT Project | R |

C = Create, R = Read, U = Update, D = Delete, \* Indicates Record Permissions

**Note:** Members of the IoT Security Assessor should also be assigned to the EM: Read Only and TM: Read Only groups under Enterprise Management and Third Party Risk Management to allow selection of Business Unit, Business Processes, Applications, Devices, Third Party Profiles, Products and Services, etc.

## Installing Archer IIC-Aligned IoT Security Maturity Assessment

### 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 6.12
2. Download the ODA install package from: <https://www.archerirm.community/t5/exchange-downloads/archer-iic-aligned-iot-security-maturity-assessment-app-pack-6-7/ta-p/564214>
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](#InstallAppPackage) for complete information.

#### Task 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](#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 ID sin 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.

1. 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 check box. 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 IoT Profiles 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.

### Setting up data feeds

Two Data Feeds are included in the Archer IIC-Aligned IoT Security Maturity Assessment app-pack package:

* Generate IoT Security Maturity Assessments: This Data Feed is used to create new IoT Security Maturity Assessment records.  The report returns data from the selection of Domain or Sub-Domain or Practice from value list field within IoT profiles application and is triggered by workflow initiated by the user in IoT Profiles application.
* Archive IoT Security Maturity Assessments: This Data Feed copies data from cross-reference IoT Security Maturity Assessments (Practice) in IoT Profiles application to Archived IoT Security Maturity Assessment and is triggered by workflow initiated by the user in IoT Profiles application.

Repeat the following steps for each Data Feed:

1. Go to Manage Data Feeds page:
   1. From the menu bar, click Admin menu.
   2. Under Integration, click Data Feeds.
2. Locate and select the Data Feed.
3. Verify settings in the General tab.
   1. In the General Information section, set the Status field to Active.
   2. In the Feed Information section, confirm that the Target field is set to IoT Profiles.
4. Click the Transport tab.
   1. In the Transport section, confirm that the Transport Method field is set to Archer Web Services Transporter.
   2. In the Security section, in the URL field, insert the URL to your instance.
   3. In the Transport Configuration section, do the following:
      1. In the User Name and Password fields, type the username and password of a Platform user.
      2. In the Instance field, enter the name of your instance.
5. Verify the settings on the Source Definition tab. This will be pre-configured.
6. Verify the settings and mappings on the Data Map tab. This will be pre-configured.
7. The Key Definition fields should be pre-populated based on the information from the imported Data Feed.
8. The final configuration step is to schedule the data feed. Click the Schedule tab and configure the frequency and start time of the Data Feed.
9. Click Save to apply your configuration to the data feed.
10. (Optional) To override the data feed schedule and immediately run your data feed, in the Run Data Feed Now section, click Start.
11. Click the Run Detail link for additional information on the status of the feed or to troubleshoot any feed errors.

## Using Archer IIC-Aligned IoT Security Maturity Assessment

### Task 1: Create a new IoT security profile

Users: IoT Security Assessor

1. Go to the IoT Profiles record.
   1. From the menu bar, click IoT Security Risk Assessment.
   2. Under Applications, click IoT Profiles.
   3. click New.
2. Fill in the following information in General Information section:
   1. Enter Profile Name.
   2. Select Assessment Type and Assessment Frequency for the profile by clicking the down arrow next to the field and making your selection.
   3. If Assessment Type is Third Party Profile, Enter the Third Party Name related to IoT Profile OR select the associated Third Party Profile by clicking Ellipsis  and selecting respective record.
   4. Select Assessment Methods for the profile.
   5. Select the Assessment Start Date by clicking the calendar icon next to the field.
   6. Enter the Description for the profile.
3. Select user from the list in the IoT Security Assessor field by clicking Ellipsis from the Stakeholders section.
4. (Optional) Select user from the list in the Profile Reviewer and Watchers field by clicking Ellipsis from the Stakeholders section.
5. (Optional) Scope must be defined by selecting the associated Business Units, Business Processes, Applications, Devices, Product and Services or Third Party Engagements by clicking Ellipsis  and selecting respective record in the Scope tab.
6. (Optional) Add Comments to the profile by clicking the | Add New | button in the Comments section.
7. (Optional) Add attachments/documentation to the record by clicking the | Add New | button in the Supporting Documentation field.
8. Once the record is complete, click Save in the Record Toolbar to save in record. After saving the IoT Profile, the record will be enrolled into advanced workflow.

### Task 2: Generate IoT Security Maturity Assessments

Users: IoT Security Assessor

1. Select the IoT Profile record you want to generate assessments.
2. Click the Edit button in the top of the record.
3. Navigate to the Assessments tab.
4. Select the applicable Domains or SubDomains or Practice from Generate IoT Security Maturity Assessments field by clicking on lookup in IoT Security Maturity Model section.
5. Click on Generate Assessments from the Actions dropdown at the top left of the screen.
6. Wait for the IoT Security Maturity Assessments to be generated and the system will return the user to the record upon refresh or recalculate.

* **Note:** Assessments are generated for each Practice selected. For selection made at Domain or SubDomain level, the Assessments will be generated for all the associated Practices in IoT Security Maturity Assessments application.

1. Click Save in the Record Toolbar.

### Task 3: Complete IoT Security Maturity Assessments

Users: IoT Security Assessor

1. Select the IoT Profile record you want to complete assessments.
2. Click the EDIT button in the top of the record.
3. Navigate to the Assessments tab.
4. Select the Target goals (Comprehensiveness) and Scope Levels in the IoT Security Maturity Target (Domain) section.
5. Select the Target goals (Comprehensiveness) and Scope Levels in the IoT Security Maturity Target (Sub Domain) section.
6. Fill in the following information in the IoT Security Maturity Assessments (Practice) section:
   1. Enable Inline Edit
   2. Select values in the Target Comprehensiveness Level and Target Scope Level of each Practice.
   3. Select values in the Current Comprehensiveness Level and Current Scope Level of each Practice.
   4. Click on Save Changes button at the top of the page or Save button at the end of the row in IoT Security Maturity Assessment (Practice) section.
   * OR
   1. Select a record from the IoT Security Maturity Assessments (Practice) section.
   2. Click the Edit button in the top of the record.
   3. View the Comprehensiveness Level and Scope Level Definition at the top of the application layout by expanding the section.
   4. Select Target Comprehensiveness Level and Target Scope Level by clicking the down arrow next to the field and making your selection.
   5. View the Practice table by expanding the section.
   6. Select Current Comprehensiveness Level and Current Scope Level by clicking the down arrow next to the field and making your selection.
   7. (Optional) Identify relevant Policies, Controls, or Contracts for the Practice by selecting the associated Policies, Controls Procedures, or Contracts record by clicking the | Add New | or | Lookup | button.
   8. (Optional) Identify relevant product initiatives for the Practice record by selecting the associated Product Initiatives record by clicking the | Add New | or | Lookup | button.
   9. click Save in the Record Toolbar.
   10. Repeat the above steps for each of the practice in the IoT Security Maturity Assessments (Practice) section.
7. Once the assessment is complete, Click on Assessments Complete from the Actions dropdown at the top left of the screen.

### Task 4: Archive and reassess

Users: IoT Security Assessor

1. Select the IoT Profile record you want to Archive assessments and Perform Reassessment.
2. Click the Edit button in the top of the record.
3. Click on Archive & Reassess button at the top left of the screen.
4. Existing IoT Security Maturity Assessments will be copied to the Archived IoT Security Assessments section.
5. The Current Comprehensiveness Level and Current Scope Level of IoT Security Maturity Assessments (Practice) will be set to blank.
6. Navigate to the Assessments tab.
7. (Optional) Select the Target goals (Comprehensiveness) and Scope Levels in the IoT Security Maturity Target (Domain) section.
8. (Optional) Select the Target goals (Comprehensiveness) and Scope Levels in the IoT Security Maturity Target (Sub Domain) section.
9. Fill in the following information in the IoT Security Maturity Assessments (Practice) section:
   1. Enable Inline Edit
   2. (Optional) Select values in the Target Comprehensiveness Level and Target Scope Level of each Practice.
   3. Select values in the Current Comprehensiveness Level and Current Scope Level of each Practice.
   4. Click on Save Changes button at the top of the page or Save button at the end of the row in IoT Security Maturity Assessment (Practice) section.
   * OR
   1. Select a record from the IoT Security Maturity Assessments (Practice) section.
   2. Click the Edit button in the top of the record.
   3. (Optional)View the Comprehensiveness Level and Scope Level Definition at the top of the application layout by expanding the section.
   4. (Optional) Select Target Comprehensiveness Level and Target Scope Level by clicking the down arrow next to the field and making your selection.
   5. View the Practice table by expanding the section.
   6. Select Current Comprehensiveness Level and Current Scope Level by clicking the down arrow next to the field and making your selection.
   7. (Optional) Identify relevant Policies, Controls, or Contracts for the Practice by selecting the associated Policies, Controls Procedures, or Contracts record by clicking the | Add New | or | Lookup | button.
   8. (Optional) Identify relevant test procedures and results for the Practice record by selecting the associated Product Initiatives record  by clicking the | Add New | or | Lookup | button.
   9. click Save in the Record Toolbar.
   10. Repeat the above steps for each of the practice in the IoT Security Maturity Assessments (Practice) section.
   11. Once the assessment is complete, Click on Assessments Complete from the Actions dropdown at the top left of the screen.

## Certification environment

Date tested: May 2023

| Product Name | Version Information | Operating System |
| --- | --- | --- |
| Archer | 6.12 | Windows Server 2012 |