# Archer Product Security Development Assessment

Companies see value in transitioning to a DevOps process model, which allows faster turnaround and less waste in the development process; however, this new model opens companies up to new security risks that need to be monitored as the development teams iterate. Third party libraries significantly increase the vulnerability of software and need to continually be monitored for risk. To reduce risk and vulnerabilities, security should be an ongoing integrated part of the DevOps process by performing continual software security tests. Product Security teams should be able to view and understand the risks that new products impart on the company and provide insight into the paths to approve or mitigate risk before deployment. With faster cycle times and a desire to quickly deploy new products, a consistent and repeatable process is essential to ensure all risks are understood at all levels.

* Inefficient approval processes and oversight can slow down development
* Product management needs to understand all the product features that are being worked on
* Third party libraries massively increase the vulnerability of a software and must be continually monitored for risk (future tracking of libraries)
* Development teams need to perform continual security tests on software to reduce vulnerabilities
* A consistent and repeatable process is necessary to manage access and edits to product elements

The Archer Product Security Development Assessment offering helps organizations to track threat models, approvals for product initiatives, and mitigation plans to address findings as a result of the threat model risk assessment.

On this page

* [Release notes](#Releasenotes)
  + [Release 6.12](#Release612)
* [Overview of Archer Product Security Development Assessment](#Xd290d59ba24f8f535fbc94c76dc44e582bdb24a)
  + [Key features and benefits](#Keyfeaturesandbenefits)
  + [Prerequisites (ODA and system requirements)](#PrerequisitesODAandsystemrequirements)
  + [Compatible use cases and applications](#Compatibleusecasesandapplications)
    - [Related applications](#Relatedapplications)
* [Archer Product Security Development Assessment components](#X48a821c38a23df54f82c9f22b3b1439a587d5b3)
  + [Architecture diagram](#Architecturediagram)
  + [Swim lane diagram](#Swimlanediagram)
  + [Applications](#Applications)
  + [Personas and access roles](#Personasandaccessroles)
* [Installing Archer Product Security Development Assessment](#Xf9ac0a1e42564c143b7053fada12c1cd333505e)
  + [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: Configure the data feed](#Task1Configurethedatafeed)
    - [Task 2: Schedule a data feed](#Task2Scheduleadatafeed)
* [Using Archer Product Security Development Assessment](#X4c6374a3d0317e0d76172c0421cc219785c81da)
  + [Task 1: Create a new initiative](#Task1Createanewinitiative)
  + [Task 2: Document threat model](#Task2Documentthreatmodel)
  + [Task 3: Risk identification and mitigation](#Task3Riskidentificationandmitigation)
  + [Task 4: Reviewing risk mitigation](#Task4Reviewingriskmitigation)
  + [Task 5: Initiative development](#Task5Initiativedevelopment)
  + [Task 6: Reviewing initiative (Security Manager)](#Task6ReviewinginitiativeSecurityManager)
  + [Task 7: Reviewing initiative (Product Manager)](#Task7ReviewinginitiativeProductManager)
  + [Task 8: Resubmitting an initiative](#Task8Resubmittinganinitiative)
  + [Task 9: Deploy initiative](#Task9Deployinitiative)
  + [Task 10: Create a countermeasure plan](#Task10Createacountermeasureplan)
  + [Task 11: Reviewing countermeasure plan](#Task11Reviewingcountermeasureplan)
* [Certification environment](#Certificationenvironment)

## Release notes

### Release 6.12

| Document Version | Published Date | Notes |
| --- | --- | --- |
| 1.0 | February 2020 | Initial release on Archer Exchange |
| 1.1 | May 2023 | Recertification and minor updates:   1. Countermeasures: Updated Related Initiatives cross reference calculation as it was displaying all project initiatives with no initiative risk assessment, if countermeasure is not assigned to any initiative risk assessment. 2. Data feed Generate Initiative Risk Assessments: When multiple records are in queue for assessment generation, records for all potential threats from the source report were being created for initiatives irrespective of the threats selected within them. Update made to the source transform to fix the issue. |

## Overview of Archer Product Security Development Assessment

### Key features and benefits

The Archer Product Security Development Assessment offering enables organizations to:

* Document product initiatives for the organization.
* Manage and track threat model information.
* Identify risks and mitigation strategies associated with threat modeling.

Track results and approvals for Security Testing and Third-Party Library.

Benefits include:

* Consistent and repeatable process for managing initiatives and risks
* Faster cycle times by addressing security threats earlier in the development cycle
* Understand and minimize impacts to the organization through mitigating risks
* Ensure accountability for security during the development cycle

### Prerequisites (ODA and system requirements)

| Components | Prerequisites |
| --- | --- |
| Archer Solution Area(s) | IT & Security Risk Management |
| Archer Use Case(s) | Issues Management |
| Archer Applications | Requirements for the installation and operation of ArcherProduct Security Development Assessment includes the following applications:   * Exception Requests– Archer Issues Management * Remediation Plans – Archer Issues Management |
| Uses Custom Application | Yes |
| Requires On-Demand License | Yes. The Archer Product Security Development Assessment App-Pack requires four (4) On-Demand Application licenses. |
| Archer Requirements | Archer 6.12 and later |

### Compatible use cases and applications

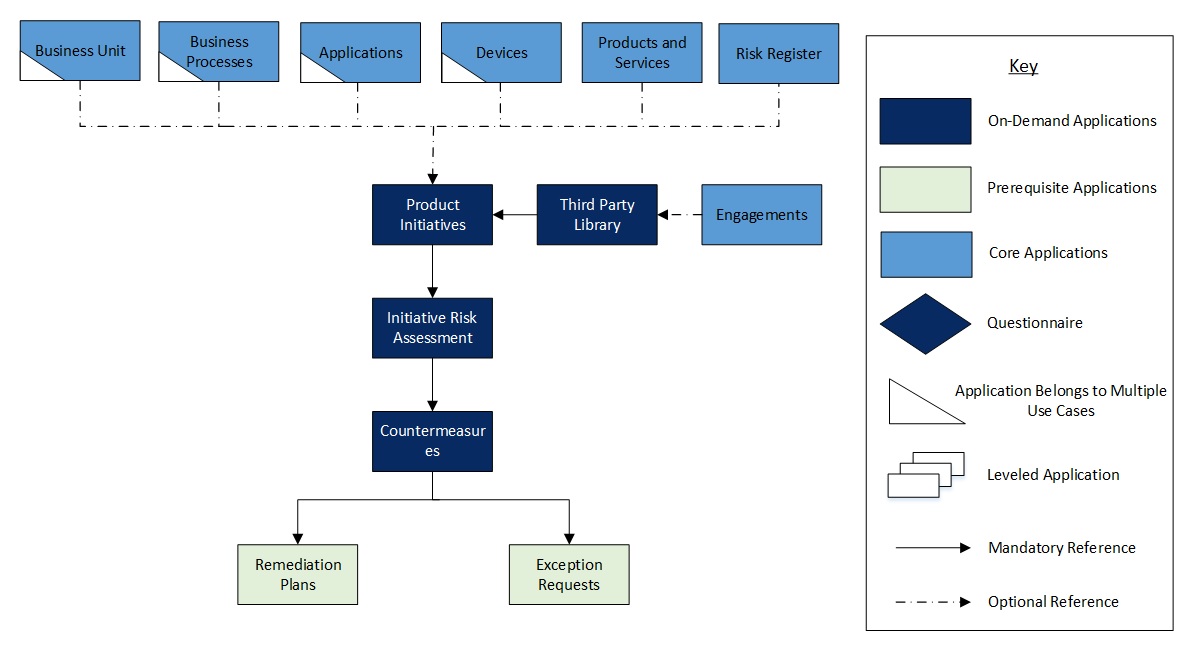
#### Related applications

| Application | Use Case | Primary Purpose(s) of the Relationship |
| --- | --- | --- |
| Business Unit | Business Asset Catalog | To relate Business Units that are impacted by the Product Initiatives |
| Business Processes | Business Asset Catalog | To relate Business Processes that are impacted by the Product Initiatives |
| Applications | IT Asset Catalog | To relate Applications that are impacted by the Product Initiatives |
| Devices | IT Asset Catalog | To relate Devices that are impacted by the Product Initiatives |
| Products and Services | Business Asset Catalog | To relate Products and Services that are impacted by the Product Initiatives |
| Risk Register | Risk Catalog; Top-Down Assessment(Operational Risk Management)  or  IT Risk Management; Information Security Management System(IT Security Risk Management)  or  Operational Scenario Analysis (Operational Scenario Analysis) | To identify, track and provide visibility for Initiatives that pose a risk to the organization. |
| Control Procedures | Controls Assurance Program Management; Data Governance (Regulatory and Corporate Compliance)  or  Top-Down Assessment(Enterprise & Operational Risk Management)  or  IT Controls Assurance; IT Risk Management; Information Security Management System; PCI Management(IT Security Risk Management) | You can tie your procedures to the control procedures that they are meant to evaluate.  When you scope an entity, the system can also pull in related control procedures. |

## Archer Product Security Development Assessment components

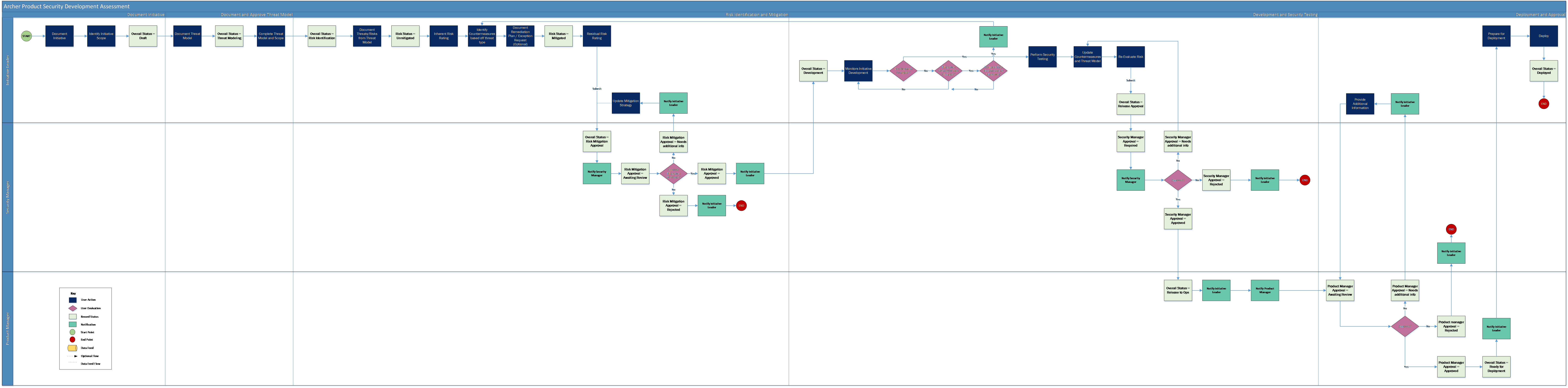
### Architecture diagram

The following diagram shows the relationship between the applications in Archer Product Security Development Assessment.

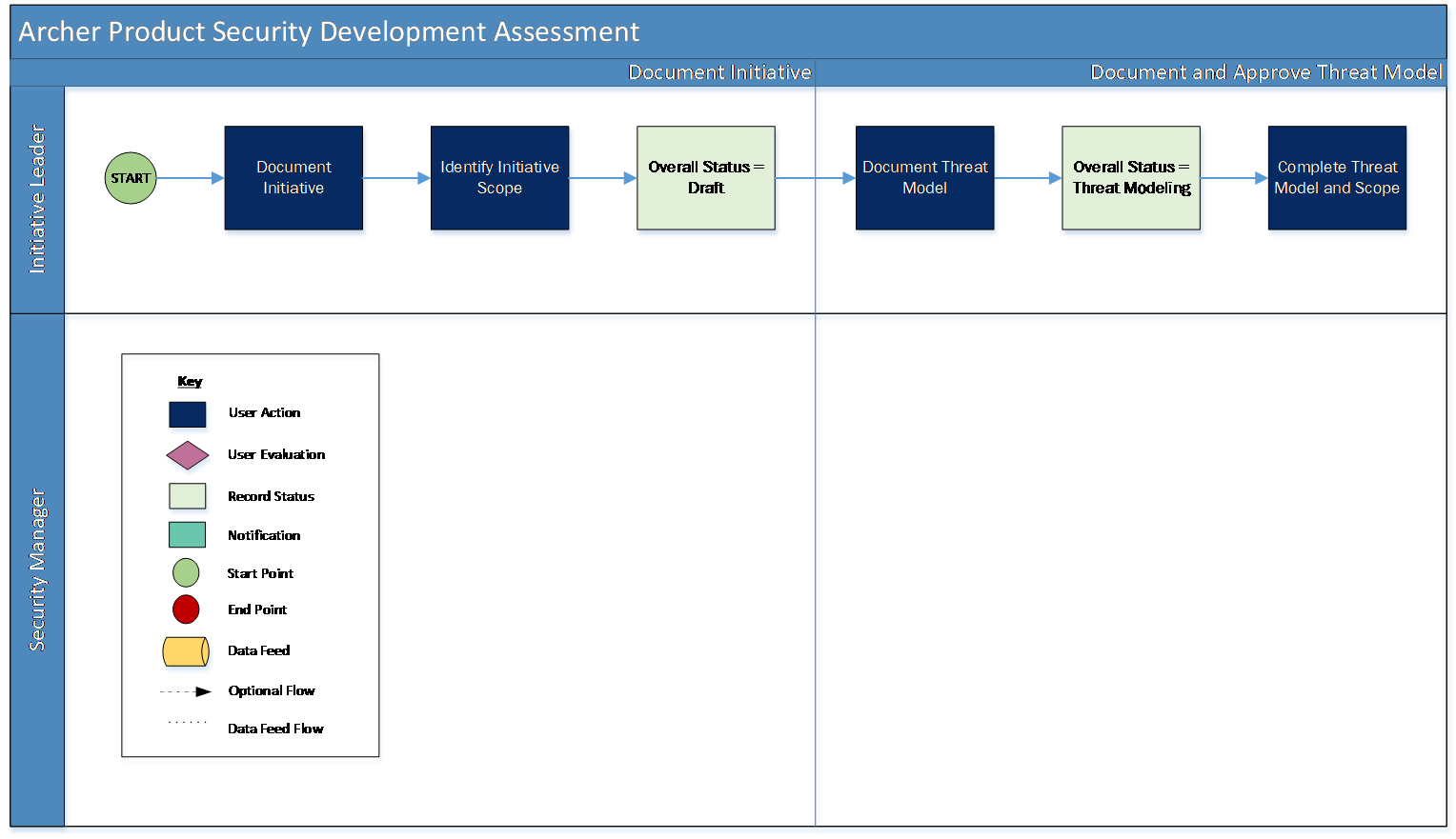


### Swim lane diagram

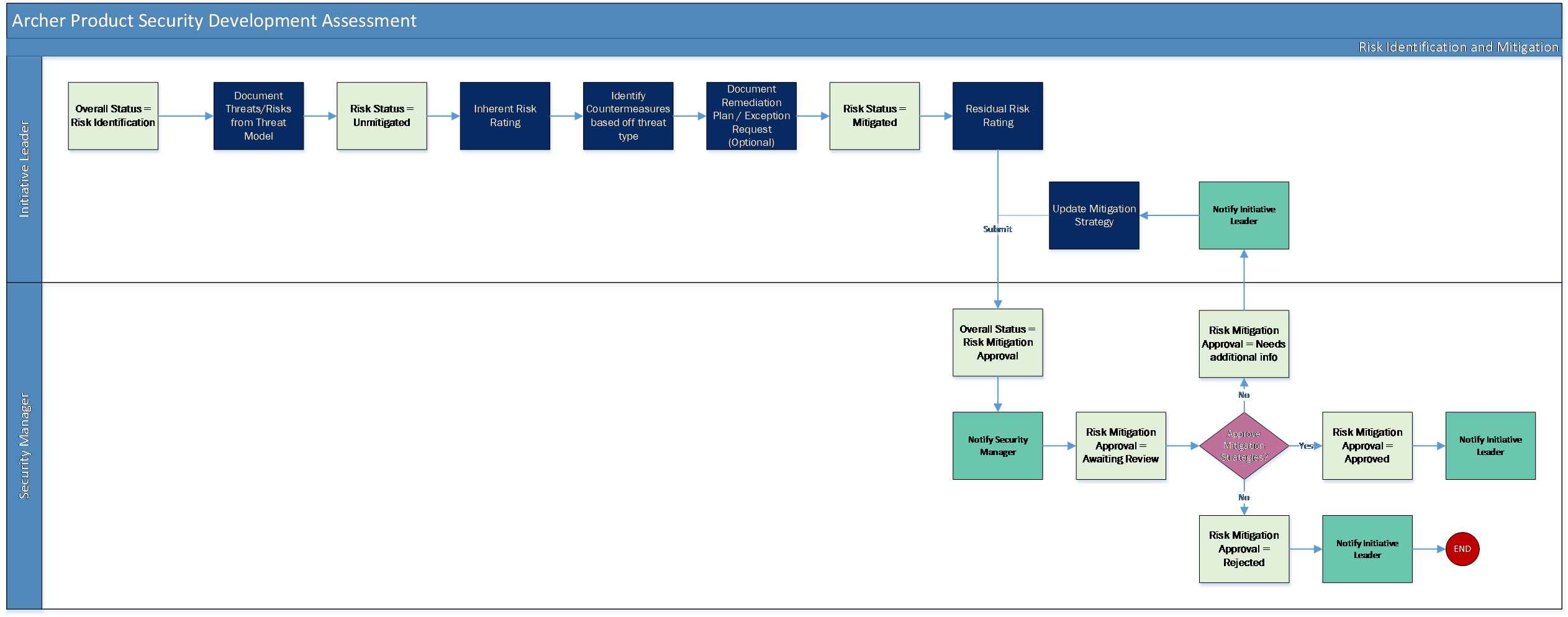
The flow is as follows: First a Product initiative is documented and its scope and threat model is documented. Any associated risk related to the product are identified and mitigated. Then the product development and testing is performed. Once all approvals are obtained the all security testing is cleared the product is deployed. Each stage is discussed below.



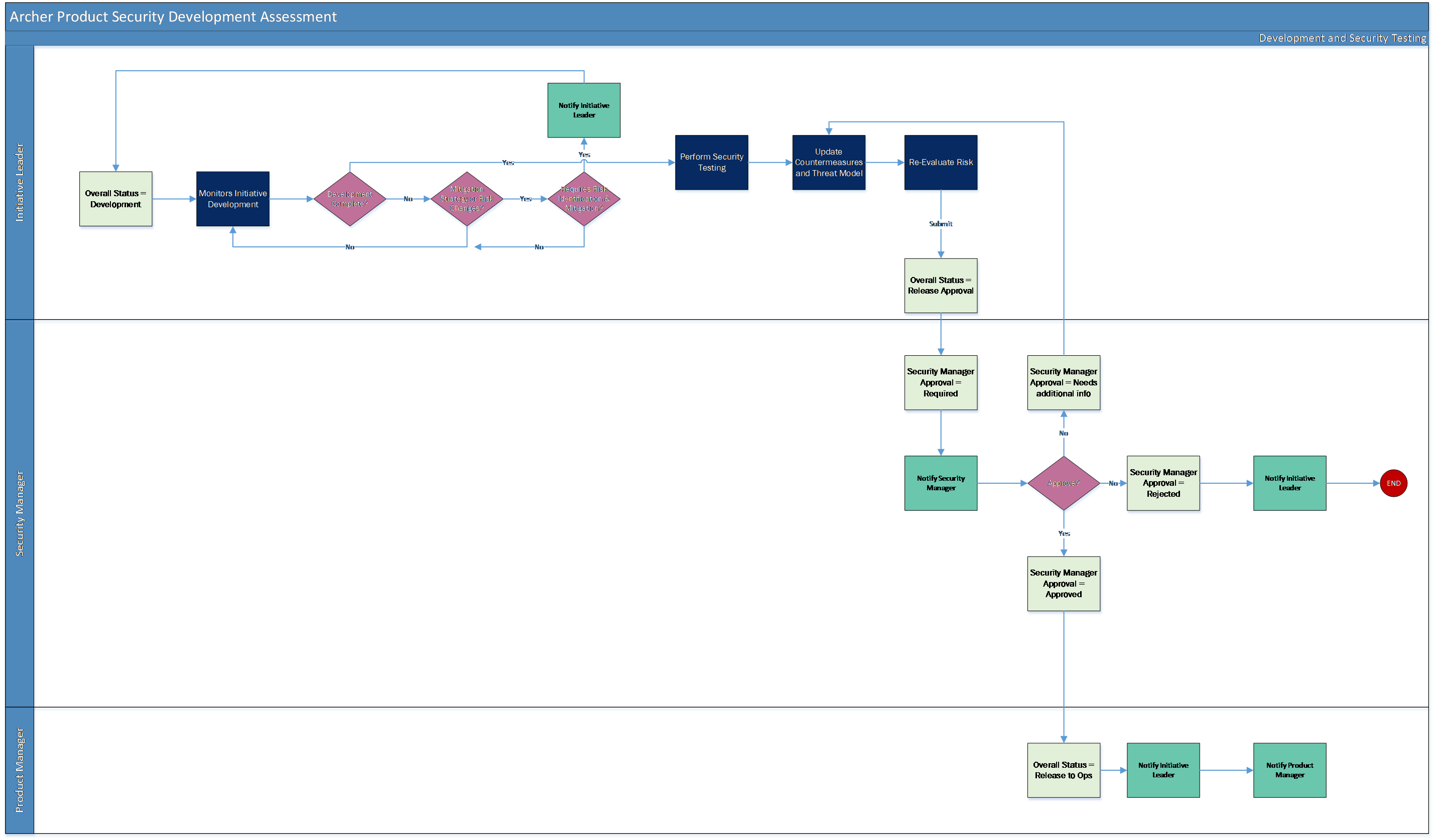
Scoping and Threat Model:



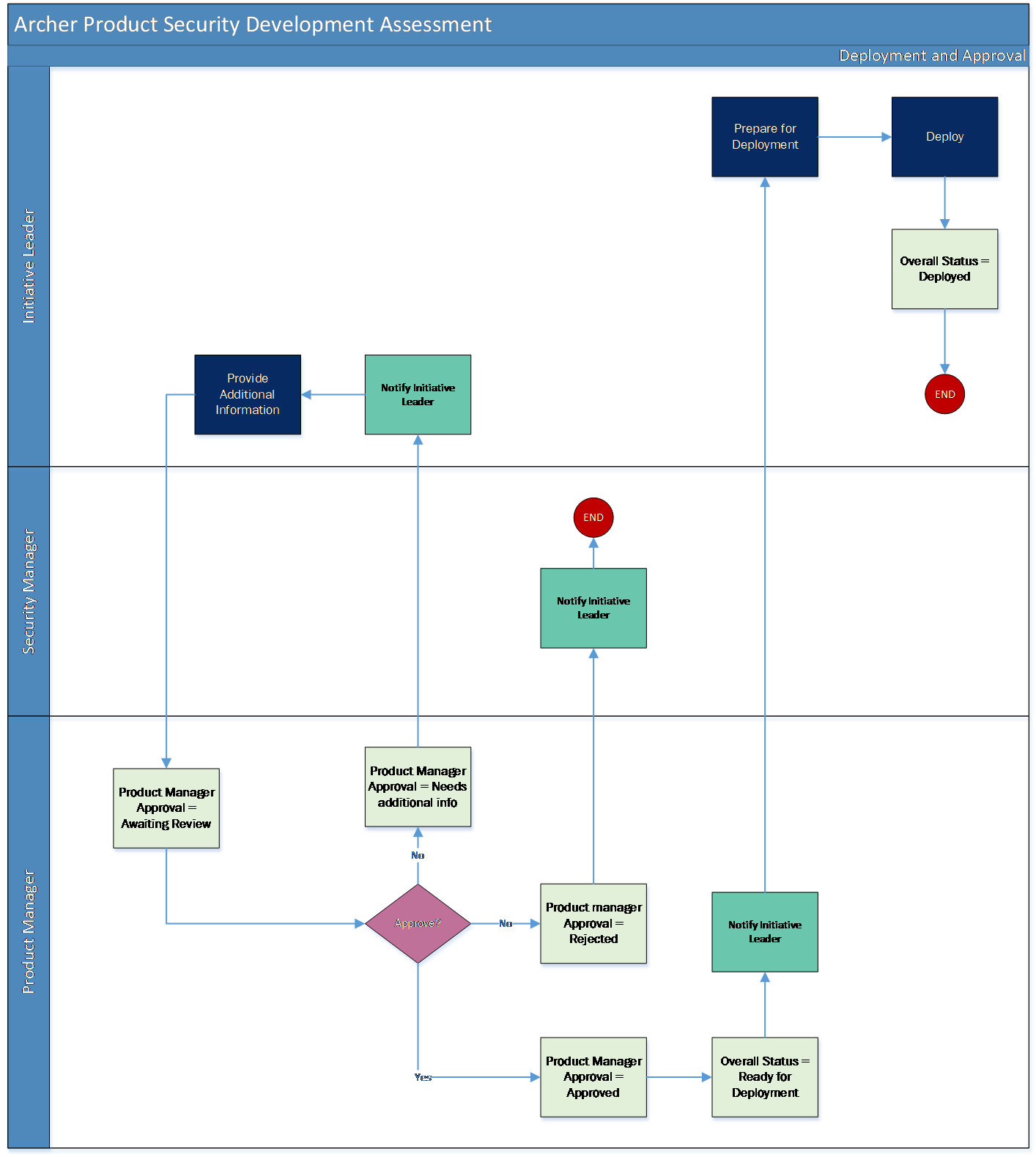
Risk Identification and Mitigation:



Development and Security Testing:



Deployment:



### Applications

| Application | Description |
| --- | --- |
| Product Initiatives | The Product Initiatives application documents all the information regarding the initiative. It contains the scope of the initiative, threat models, and risk assessments. |
| Third Party Library | The Third Party Library application documents the third party libraries used in the initiatives and associates them to the Third Party Engagements. |
| Initiative Risk Assessment | The Initiative Risk Assessment application captures the results from the risk assessment, findings, countermeasures, and mitigation plans or exception requests. |
| Countermeasures | The Countermeasures application captures the controls to reduce the risk against threats identified during the risk 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 |
| --- | --- |
| Initiative Leader | This person is responsible for the development of the initiative and for implementing the indicated countermeasures. This person may be a Product Owner or someone on the Product Security Team. |
| Security Manager | Responsible for the monitoring of third party application usage and initiative risk. This person in in charge of validating risk mitigation and risk assessment changes submitted by Initiative Leaders. This person might be a manager in the Product Security Team. |
| Product Manager | Responsible for reviewing and approving initiative features. They are responsible for aligning features with overall product mission and business rational. This person may be a Product Owner or someone in the Product Management department. |
| Risk Officer | Monitor and review initiative risk above set risk tolerances. They may also be the one who sets appropriate risk levels for different teams. This person might be someone in the Risk department or someone with authority in the Engineering department. |

| Applications | Initiative Leader | Security Manager | Product Manager | Risk Officer |
| --- | --- | --- | --- | --- |
| Product Initiatives | CRU\* | CRU\* | RU | R |
| Third Party Library | CRU\* | CRU\* | RU | R |
| Initiative Risk Assessment | CRU | CRU | RU | R |
| Countermeasures | CRU | CRU | RU | R |
| Remediation Plans | CRU | CRU | R | R |
| Exceptions Requests | CRU | CRU | R | R |
| Business Units | R | R | R | R |
| Business Processes | R | R | R | R |
| Applications | R | R | R | R |
| Devices | R | R | R | R |
| Products and Services | R | R | R | R |
| Risk Register | R | R | R | R |

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

**Note:** Members of the Initiative Leader, Security Manager, Product Manager, and Risk Officer should also be assigned to the EM: Read Only groups under Enterprise Management and Third Party Risk Management to allow selection of Business Unit, Business Processes, Applications, Devices, Products and Services.

## Installing Archer Product Security Development Assessment

### 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 6.12
2. Obtain the Data Dictionary for the ODA 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.

#### Step 2: Install the package

Installing a package requires that you import the package file, map the objects in the package to objects in the target instance, and then install the package. See [Installing the Application Package](#InstallAppPackage) for complete information.

#### 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](#SettingUpDataFeeds) 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 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

1. From the menu bar, click Admin menu > Application Builder > Install Packages.
2. In the Available Packages section, locate the package you want to map.
3. In the Actions column, click Map package for that package.

* The analyzer 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 instance 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).
* When the analyzer is complete, the Advanced Package Mapping page lists the objects in the package file and corresponding objects in the target instance.

1. On the Advanced Mapping page, click to open each category and review the icons next to each object to determine which objects you must map manually.

The following table describes the icons.

| Icon | Name | Description |
| --- | --- | --- |
| Awaiting mapping review | Awaiting Mapping Review | Indicates that the system could not automatically match the object or one of its children to a corresponding object in the target instance.  Objects marked with this icon must be mapped manually.  New objects should not be mapped. Select Do Not Map from the drop-down menu to clear this icon for an individual object, or click Do Not Map to clear the icon for all unmapped objects. |
| Mapping completed | Mapping Completed | Indicates that the object and all children are mapped to objects in the target instance, or that they have been marked as Do Not Map. Nothing more needs to be done with these objects in Advanced Package Mapping. |

* **Note:** You can run the mapping process without mapping all objects. The Awaiting mapping review icon is for informational purposes only.

1. For objects awaiting mapping review, do one of the following:
   * To map each object individually, use the drop-down menu in the Target column to select the object in the target instance to which you want to map the source object. To leave an object unmapped, select Do Not Map in the Target column.
   * To automatically map all objects in a category that have different system IDs but the same object name as an object in the target instance, click Auto Map. Select whether to ignore case and spaces when matching object names. Click OK.
   * To mark all unmapped objects as Do Not Map, click Do Not Map.
2. (Optional) Click Filter to enable filter fields that you can use to find specific objects in each mapping category. To undo your mapping selections, click Undo, then select whether to undo all mappings in the category or only the mappings on a single page. If you choose to undo all mappings, you will be returned to the categories list.
3. (Optional) To save your mapping selections and return to the categories list without committing changes to the target instance, click RSA.
4. After you review and map all objects, click Execute.
5. Select I understand the implications of performing this operation. Click OK.

* When the mapping is complete, the Import and Install Packages page displays.
* **Important:** Advanced Package Mapping modifies the system IDs in the target instance. You must 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 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 check box, 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.

### Setting up data feeds

#### Task 1: Configure the 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 Generate Initiative Risk Assessmentsdata 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. 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 Product Security Development Assessment

### Task 1: Create a new initiative

Users: Initiative Leader

1. Go to the Product Initiatives record.
   1. From the menu bar, click Product Security Development Assessment.
   2. Under Solutions, click Product Security Development Assessment.
   3. Under Applications, click Product Initiatives.
   4. click New.
2. Enter Initiative Name in the General Information section.
3. Select the Initiative Type and Risk Tolerance values by clicking the down arrow next to the field and making your selection.
4. Select the Estimated Start Date and Estimated End Date by clicking the calendar icon next to the field.
5. Enter Estimated Cost in the General Information section.
6. Enter the Description for the Initiative.
7. Select user from the list in the Security Manager, Product Manager and Risk Officer field by clicking  from the Roles and Responsibilities section.
8. (Optional) Select any Watchers you would like to add to the Initiative by clicking  and selecting their user name.
9. Once the record is complete, click Save in the Record Toolbar to save in record. After saving the Initiative, the record will be enrolled into workflow.
10. Scope must be defined by selecting the associated Business Units, Business Processes, Applications, Devices or Product and Services by clicking   and selecting respective record.
11. Add or Lookup a Third Party Library record by clicking the | Add New | or | Lookup | button in the Third Party Library section.
12. (Optional) Add Comments to the request by clicking the | Add New | button in the Comments section.
13. (Optional) Add attachments/documentation to the record by clicking the | Add New | button in the Supporting Documentation field.
14. Click Save in the Record Toolbar to save in Product Initiative record.
15. Click on Document Threat Model button at the top left of the screen.

### Task 2: Document threat model

Users: Initiative Leader

1. Select the Initiative you want to document threat model by clicking the Initiative Name under the Tasks section on your Task landing screen.
2. Click the Edit button in the top of the record.
3. Enter Threat Model Name in the Threat Modeling Information section.
4. Enter the Threat Model Location.
5. Select user from the list in the Threat Modeling Team field by clicking  from the Threat Modeling Information section.
6. Add Threat Model to the record by clicking the | Add New | button in the Threat Modeling Documents field.
7. Click on Threat Model Complete button at the top left of the screen.

### Task 3: Risk identification and mitigation

Users: Initiative Leader

1. Select the Initiative that you want to perform Risk Identification and Mitigation by clicking the Initiative Name under the Tasks section on your Task landing screen.
2. Click the Edit button in the top of the record.
3. Select Potential Threat values by clicking Ellipsis from the Threat Information section in Risk Identification and Mitigation tab.
4. Click on Generate Assessment button at the top left of the screen. Wait for Initiative Risk Assessment records to be generated. After the generation of the Assessment, follow the steps below:
5. In Edit mode, navigate to Initiative Risk Assessment section in Risk Identification and Mitigation tab and Enable Inline edit.
6. Inline Edit: Select Inherent Impact and Inherent Likelihood field values by clicking the down arrow next to the field and making your selection in Initiative Risk Assessment section.
7. Inline Edit: Select Countermeasure from the Lookup by clicking Ellipsis in the Initiative Risk Assessment section.
8. Inline Edit: Select Residual Impact and Residual Likelihood field values by clicking the down arrow next to the field and making your selection in Initiative Risk Assessment section.
9. Click on Save Changes button at the top of the page or Save button at the end of the row in Initiative Risk Assessment section.
10. Click Save in the Record Toolbar to save in Product Initiative record. ​The Inherent Risk and Residual Risk values will be populated in Assessment Summary section.
11. Make sure all Assessment Status is Complete. Click on Submit for Review button in the top left of the screen.

### Task 4: Reviewing risk mitigation

Users: Security Manager

1. Select the Product Initiative you want to review by clicking the Initiative Name under the Taskssection on your Task landing screen.
2. Click the Edit button in the top of the record.
3. To Approve the request
   1. Inline Edit: Select ‘Approved’ from Risk Mitigation Approval field value by clicking the down arrow next to the field and making your selection in Initiative Risk Assessment section.
   2. Click on Save Changes button at the top of the page or Save button at the end of the row in Initiative Risk Assessment Section.
   3. Make sure the Risk Mitigation Approval field contains Approved in all the Initiative Risk Assessment records.
   4. Click on Approve button in the top left of the screen.
4. To request additional information from the Initiative Leader:
   1. Inline Edit: Select ‘Needs Additional Information’ from Risk Mitigation Approval field value by clicking the down arrow next to the field and making your selection in Initiative Risk Assessment Section.
   2. Click on Save Changes button at the top of the page or Save button at the end of the row in Initiative Risk Assessment Section.
   3. Document the additional information requested in the Risk Mitigation Review Comments field.
   4. Click on Request Additional Information button at the top left of the screen.
5. To Reject the Initiative:
   1. Inline Edit: Select ‘Rejected’ from Risk Mitigation Approval field value by clicking the down arrow next to the field and making your selection in Initiative Risk Assessment Section.
   2. Click on Save Changes button at the top of the page or Save button at the end of the row in Initiative Risk Assessment Section.
   3. Document the reason for rejecting the request in the Risk Mitigation Review Comments field.
   4. Click on Reject button at the top left of the screen.

### Task 5: Initiative development

Users: Initiative Leader

1. Go to the Product Initiatives record.
   1. From the menu bar, click Product Security Development Assessment.
   2. Under Solutions, click Product Security Development Assessment.
   3. Under Applications, click Product Initiatives.
2. Select the initiative record in ‘Development’ Status.
3. Click the Edit button in the top of the record.
4. Update countermeasures selected in the Initiative Risk Assessment section for identified risks if there were changes.
5. Upload threat model if there were changes by clicking the | Add New | button in the Threat Modeling Documents field.
6. Indicate justification for any threats with Unmitigated status in the Comments field by clicking the | Add New | button in the Comments section.
7. Reevaluate residual risk if required.
8. Once the record is Complete. Click on Development Complete button in the top left of the screen.

### Task 6: Reviewing initiative (Security Manager)

Users: Security Manager

1. Select the Product Initiative you want to review by clicking the Initiative Name under the Tasks section on your Task landing screen.

* OR
* Go to the Product Initiatives record.
  1. From the menu bar, click Product Security Development Assessment.
  2. Under Solutions, click Product Security Development Assessment.
  3. Under Applications, click Product Initiatives.
* Select the initiative record in ‘Release Approval’ Status.

1. Click the Edit button in the top of the record.
2. To Approve the request
   1. Click on Approve button in the top left of the screen. The user has a secure way to approve the record with electronic signatures.
   2. User enters their Archer password for completing the Approve action.
   3. Electronic signature is tracked through entries in a History Log field and by having a system generated snapshot automatically attached to an attachment field.
3. To request additional information from the Initiative Leader:
   1. Document the additional information requested in the Comments field.
   2. Click on Request Additional Information button at the top left of the screen.
4. To Reject the Initiative:
   1. Document the reason for rejecting the request in the Comments field.
   2. Click on Reject button at the top left of the screen.

### Task 7: Reviewing initiative (Product Manager)

Users: Product Manager

1. Select the Product Initiative you want to review by clicking the Initiative Name under the Tasks section on your Task landing screen.

* OR
* Go to the Product Initiatives record.
  1. From the menu bar, click Product Security Development Assessment.
  2. Under Solutions, click Product Security Development Assessment.
  3. Under Applications, click Product Initiatives.
* Select the initiative record in ‘Release to Ops’ Status.

1. Click the Edit button in the top of the record.
2. To Approve the request
   1. Click on Approve button in the top left of the screen. The user has a secure way to approve the record with electronic signatures.
   2. User enters their Archer password for completing the Approve action.
   3. Electronic signature is tracked through entries in a History Log field and by having a system generated snapshot automatically attached to an attachment field.
3. To request additional information from the Initiative Leader:
   1. Document the additional information requested in the Comments field.
   2. Click on Request Additional Information button at the top left of the screen.
4. To Reject the Initiative:
   1. Document the reason for rejecting the request in the Comments field.
   2. Click on Reject button at the top left of the screen.

### Task 8: Resubmitting an initiative

Users: Initiative Leader

1. Select the initiative you want to revise by clicking the Initiative Name under the Tasks section onyour Task landing screen.
2. Click the Edit button in the top of the record.
3. Make the revisions requested by Security Manager or Product Manager.
4. (Optional) Add attachments to the record by clicking the | Add New | button in the Supporting Documentation field.
5. (Optional) Add additional comments to the record by clicking the | Add New | button in the Comments section.
6. Click on Resubmit for Review button in the top left of the screen.

### Task 9: Deploy initiative

Users: Initiative Leader

1. Go to the Product Initiatives record.
   1. From the menu bar, click Product Security Development Assessment.
   2. Under Solutions, click Product Security Development Assessment.
   3. Under Applications, click Product Initiatives.
2. Select the initiative record in ‘Ready for Deployment’ Status.
3. Click the Edit button in the top of the record.
4. Select the Deployment Date by clicking the calendar icon next to the field in the General Information section.
5. Click on Deploy button at the top left of the screen.

### Task 10: Create a countermeasure plan

Users: Initiative Leader

1. Go to the Countermeasures record.
   1. From the menu bar, click Product Security Development Assessment.
   2. Under Solutions, click Product Security Development Assessment.
   3. Under Applications, click Countermeasures.
   4. click New.
2. Enter Countermeasure Name in the General Information section.
3. Select the Threat Type by clicking Ellipsis next to the field and making your selection.
4. Select user from the list in the Countermeasure Approver field by clicking Ellipsis from the General Information section.
5. Enter Countermeasure Cost and Countermeasure Description in the General Information section.
6. Scope must be defined by selecting the related Applications, Devices or Product and Services by clicking Ellipsisand selecting respective record.
7. Select the Approach type field value by clicking the down arrow next to the field and making your selection in the Countermeasure Plan section.
8. Select the Expiration Date by clicking the calendar icon next to the field in the Countermeasure Plan section.
9. Enter Countermeasure Implementation in the Countermeasure Plan section.
10. Document the Code and Scan Parameters in the Countermeasure Plan section.
11. Add Testing Plan details to the Countermeasure by clicking the | Add New | button in the Testing Plan section.
12. (Optional)Add Comments to the Countermeasure by clicking the | Add New | button in the Comments section.
13. (Optional) Add attachments/documentation to the record by clicking the | Add New | button in the Related Documents field.
14. Once the Countermeasure is complete, select ‘Yes’ in the ‘Ready for Review?’ field value to submit the countermeasure for review.
15. Click Save in the Record Toolbar to save in Countermeasure record.

### Task 11: Reviewing countermeasure plan

Users: Security Manager

1. Go to the Countermeasures record.
   1. From the menu bar, click Product Security Development Assessment.
   2. Under Solutions, click Product Security Development Assessment.
   3. Under Applications, click Countermeasures.
2. Select the Countermeasure record in ‘Submitted’ Status.
3. Click the Edit button in the top of the record.
4. To Approve the request
   1. Select ‘Approve’ from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   2. Click Save in the Record Toolbar to save in Countermeasure record.
5. To request additional information from the Initiative Leader:
   1. Select ‘Needs Additional Information’ from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   2. Document the additional information requested in the Comments field.
   3. Click Save in the Record Toolbar to save in Countermeasure record.
6. To Reject the Countermeasure:
   1. Select ‘Reject’ from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   2. Document the reason for rejecting the request in the Comments field.
   3. Click Save in the Record Toolbar to save in Countermeasure record.
7. To Decommission the Countermeasure:
   1. Select ‘Decommission’ from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   2. Document the reason for Decommissioning the request in the Comments field.
   3. Click Save in the Record Toolbar to save in Countermeasure record.

## Certification environment

Date tested: May 2023

| Product Name | Version Information |
| --- | --- |
| Archer | 6.12 |