RSA Archer®
Product Security Development Assessment

6.6 & Later

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: https://community.rsa.com/community/rsa-customer-support.

Trademarks

RSA, the RSA Logo, RSA Archer, RSA Archer Logo, and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm.

License agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-party licenses

This product may include software developed by parties other than RSA.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Note on Section 508 Compliance

The RSA Archer GRC is built on web technologies which can be used with assistive technologies, such as screen readers, magnifiers, and contrast tools. While these tools are not yet fully supported, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer GRC.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION 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.

November 2019

Table of Contents

Chapter 1: Overview of RSA Archer Product Security Development Assessment

About RSA 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 RSA 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.

Key Features and Benefits

The RSA 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

Key Terminology

Application. Database that stores a specific type of data record such as policies, assessments, assets, threats, vulnerabilities, and controls.

Authorized User. A user who has logged into the system and has a right to perform some operation. The system knows the identity and permissions granted to this individual.

Cross-Reference. A field type that allows users to create associations between records in the same application (internal references) or records in two separate applications (external references). By adding a cross-reference to an application, the system automatically adds a Related Record field.

Dashboard. With reports defined and saved in the inventory of system reports, those identified as Global Reports can be added to dashboards. Each dashboard can include one of many reports in the format they were saved.

Notifications. Emails sent from RSA Archer to Users or Groups, based on a schedule or a change in the record status.

Record. A collection of field values, stored within applications, sub-forms, or questionnaires.

Report. Saved search criteria that can be run again later. In RSA Archer, the construct for reports is a combination of a query and its related output presentation options. The data returned is filtered by a user permission, allowing users to see only the data for which they have been granted access.

Sub-Form. For one application, administrators can develop multiple sub-forms to hold all related data. Sub-forms can be shared across applications; however, changing a sub-form affects all applications using that sub-form.

Task. Action items that have been assigned to a user in relation to the Support Request.

User. Any person who uses and is registered within the system. In this guide, the user is assumed to be an employee using RSA Archer Support Requests.

User Profile. Preferences of the registered user that are saved within the system.

Workspace. Display mechanism that provides the user with a way to access their data.

Prerequisites (ODA and system requirements)

Components	Recommended Software
Operating System	Windows Server 2012 R2 or 2016 Standard or Datacenter editions.
Database Server	Microsoft SQL Server 2016 SP 1 (64-bit) or 2016 Enterprise Edition (64-bit) or 2017 (64-bit) Note: SQL Express is not supported
Services Server	Java Runtime Environment (JRE) 8 (64-bit)
RSA Archer	RSA Archer 6.6 and later
On-Demand Licenses	The RSA Archer Product Security Development Assessment App-Pack requires four (4) On-Demand Applications license.
Pre-Requisite Applications	Requirements for the installation and operation of RSA Archer Product Security Development Assessment includes the following applications: • Exception Requests – RSA Archer Issues Management • Remediation Plans – RSA Archer Issues Management

Compatible Use Cases and Applications

Application	Use Case	Primary Purpose(s) of the Relationship
Business Unit	RSA Archer Issues Management, RSA Archer Business Impact Analysis, RSA Archer Third Party Catalog, RSA Archer Policy Program Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Key Indicator Management, RSA Archer IT Asset Catalog, RSA Archer Business Asset Catalog, RSA Archer Federal Assessments & Authorizations, RSA Archer Federal Continuous Monitoring	To relate Business Units that are impacted by the Product Initiatives
Business Processes	RSA Archer Audit Engagements & Workpapers, RSA Archer Business Impact Analysis, RSA Archer IT Risk Management, RSA Archer Controls Assurance Program Management, RSA	To relate Business Processes that are impacted by the Product Initiatives

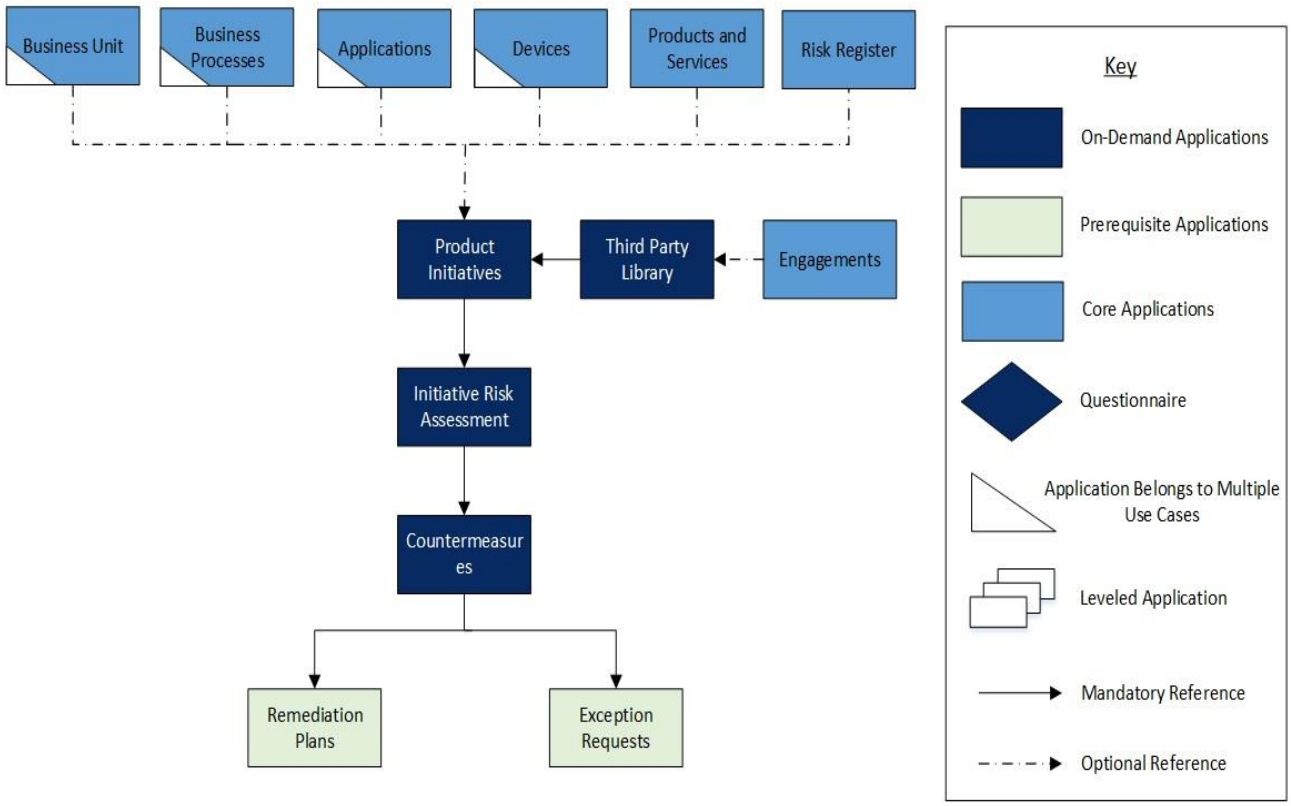
	Archer Data Governance, RSA Archer Top-Down Assessment, RSA Archer Policy Program Management, RSA Archer IT Controls Assurance, RSA Archer Business Asset Catalog, RSA Archer Bottom-Up Risk Assessment, RSA Archer Federal Assessments & Authorizations, RSA Archer Federal Continuous Monitoring).	
Applications	RSA Archer Audit Engagements and Workpapers, RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party Governance, RSA Archer IT Asset Catalog, RSA Archer IT Controls Assurance, RSA Archer IT Security Vulnerabilities Program, RSA Archer IT Risk Management, RSA Archer Cyber Incident & Breach Response, RSA Archer Data Governance, RSA Archer PCI Management, RSA Archer Information Security Management System, RSA Archer Operational Risk Management, RSA Archer Federal Continuous Monitoring	To relate Applications that are impacted by the Product Initiatives
Devices	RSA Archer Audit Engagements and Workpapers, RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party Governance, RSA Archer IT Asset Catalog, RSA Archer IT Controls Assurance, RSA Archer IT Security Vulnerabilities Program, RSA Archer IT Risk Management, RSA Archer Cyber Incident & Breach Response, RSA Archer PCI Management, RSA Archer Information Security Management System, RSA Archer Data Governance,	To relate Devices that are impacted by the Product Initiatives

	RSA Archer Federal Continuous Monitoring	
Products and Services	RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Third Party Risk Management, RSA Archer Cyber Incident and Breach Response, RSA Archer Controls Monitoring Program Management, RSA Archer Business Asset Catalog, RSA Archer Controls Monitoring Program Management, RSA Archer Bottom-Up Risk Assessment	To relate Products and Services that are impacted by the Product Initiatives
Risk Register	RSA Archer Business Continuity and IT Disaster Recovery Planning, RSA Archer Information Security Management System, RSA Archer IT Risk Management, RSA Archer Top-Down Assessment	To identify, track and provide visibility for Initiatives that pose a risk to the organization.

Chapter 2: RSA Archer Product Security Development Assessment Components

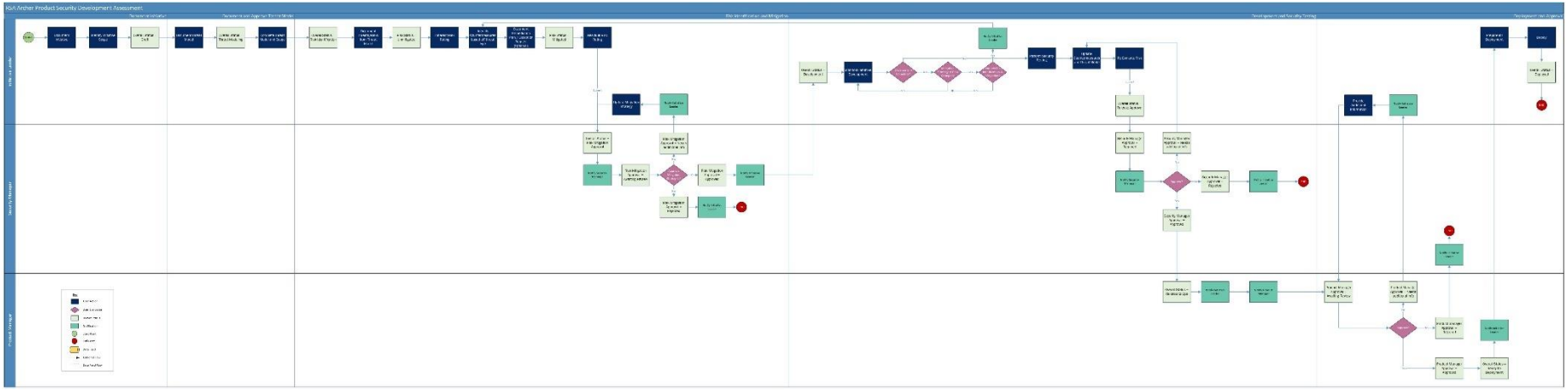
Architecture Diagram

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



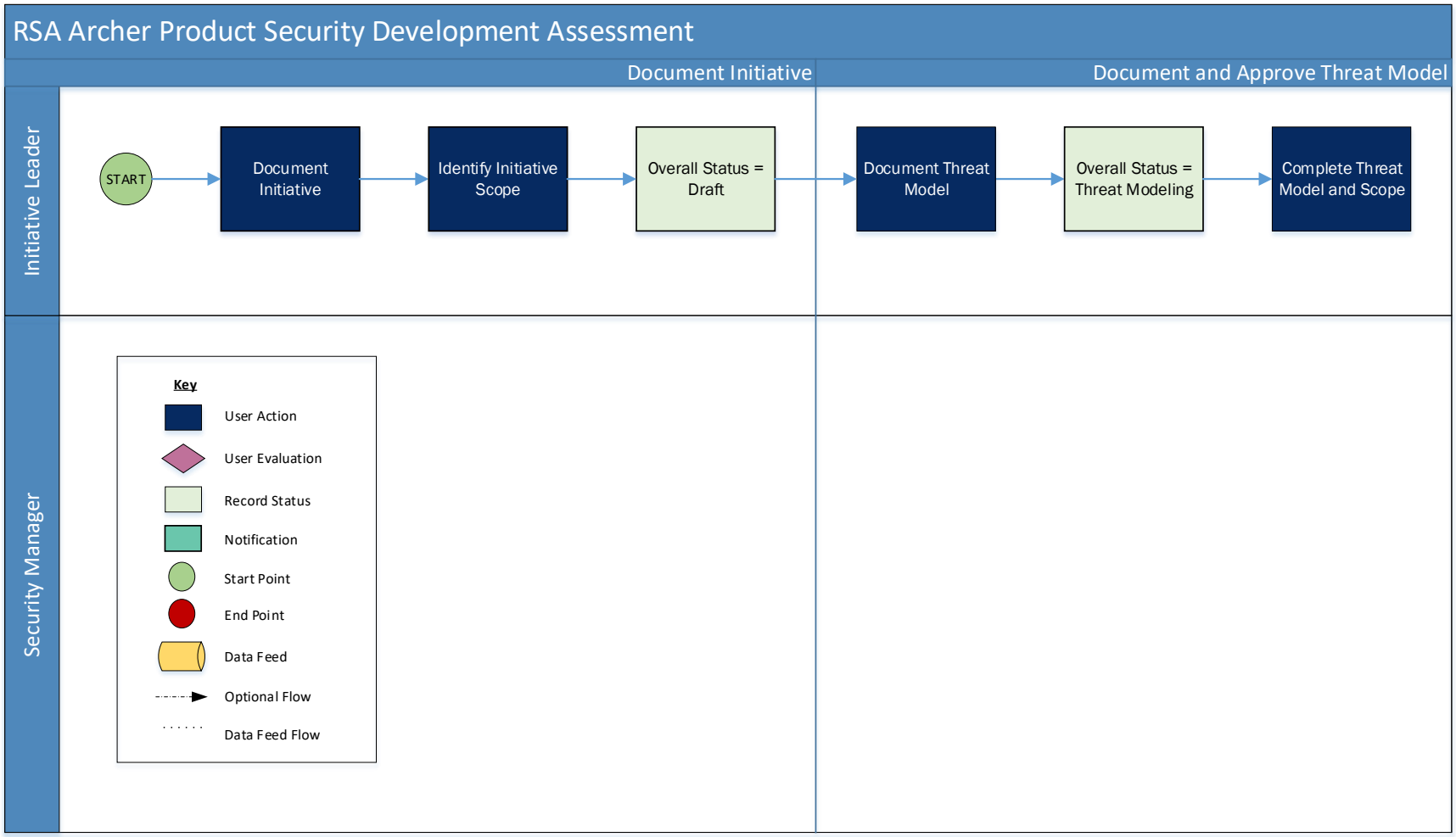
Swim Lane Diagram

The following diagram shows the general workflow of the use case.

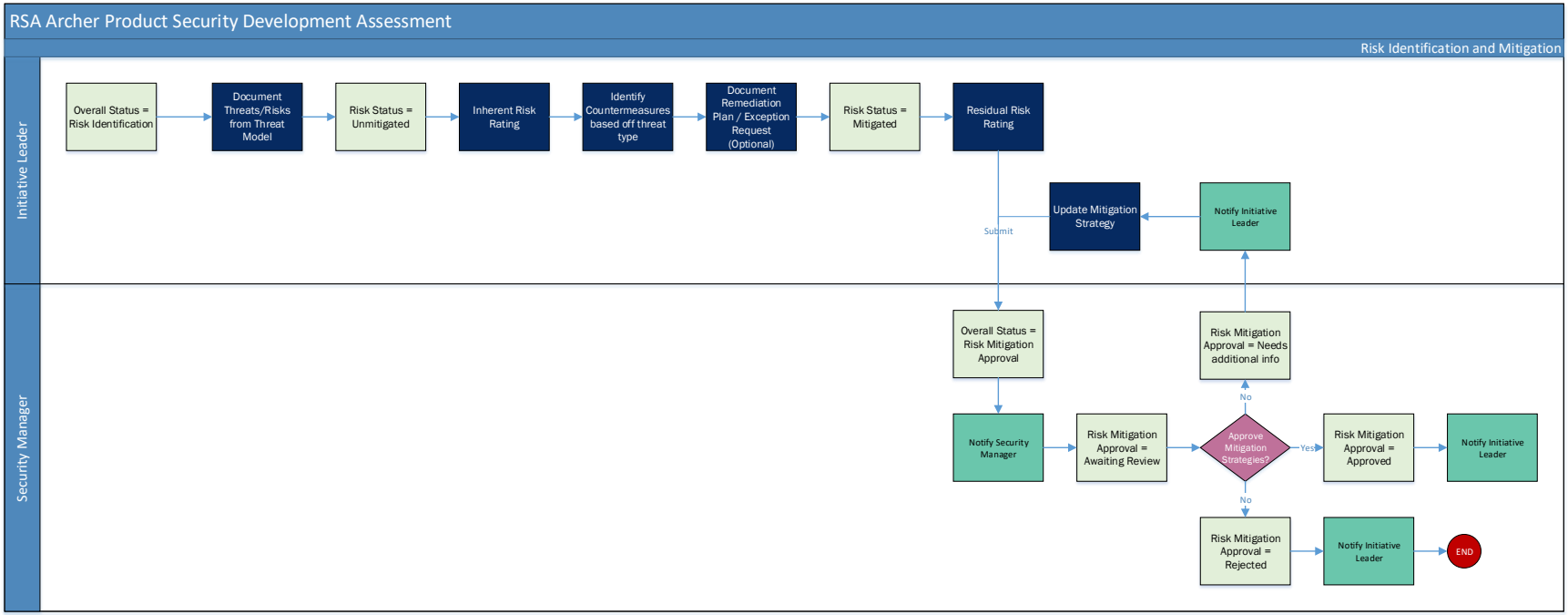


The swim lane diagram has been split by each phase as shown below:

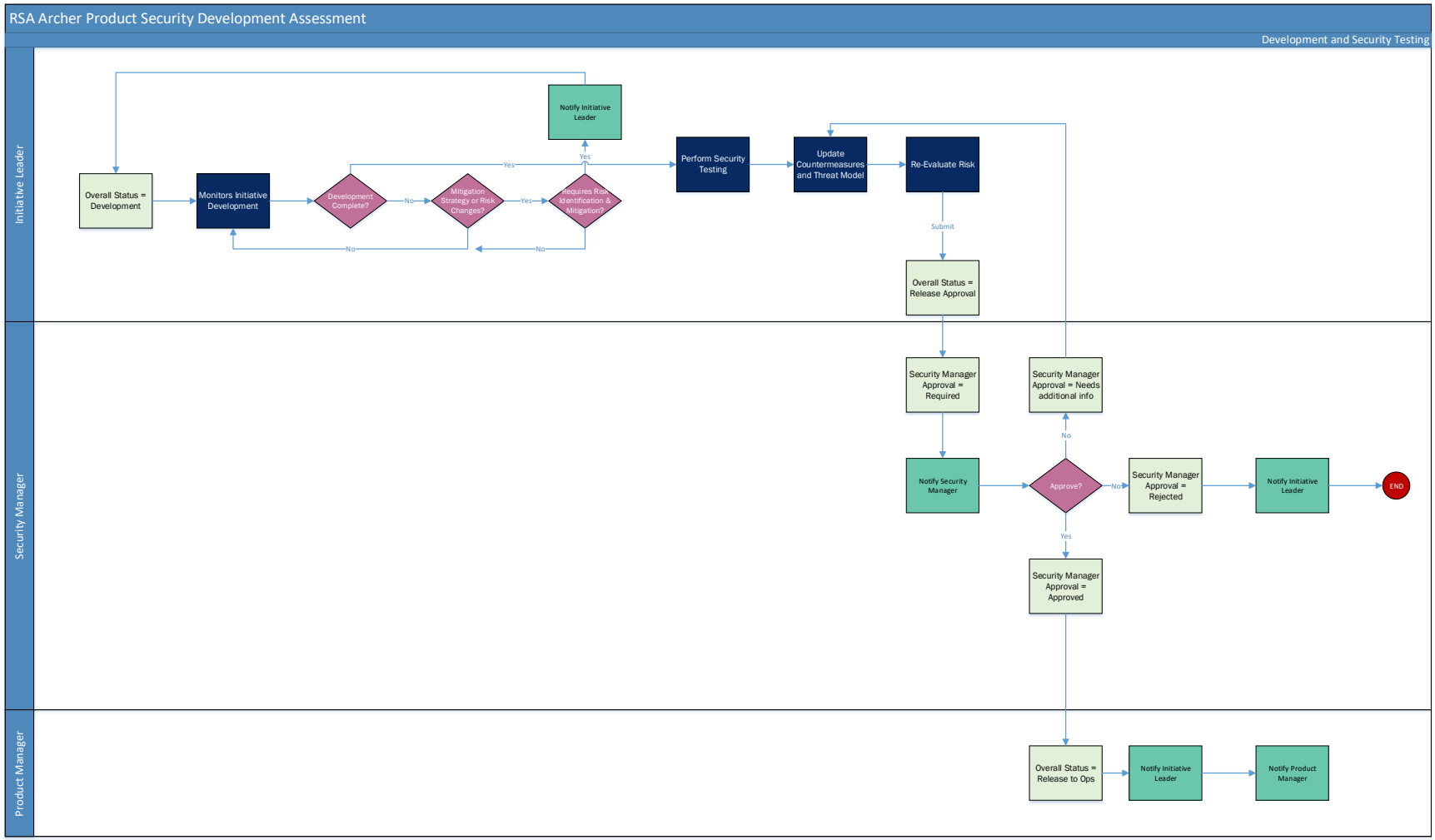
Scoping and Threat Model:



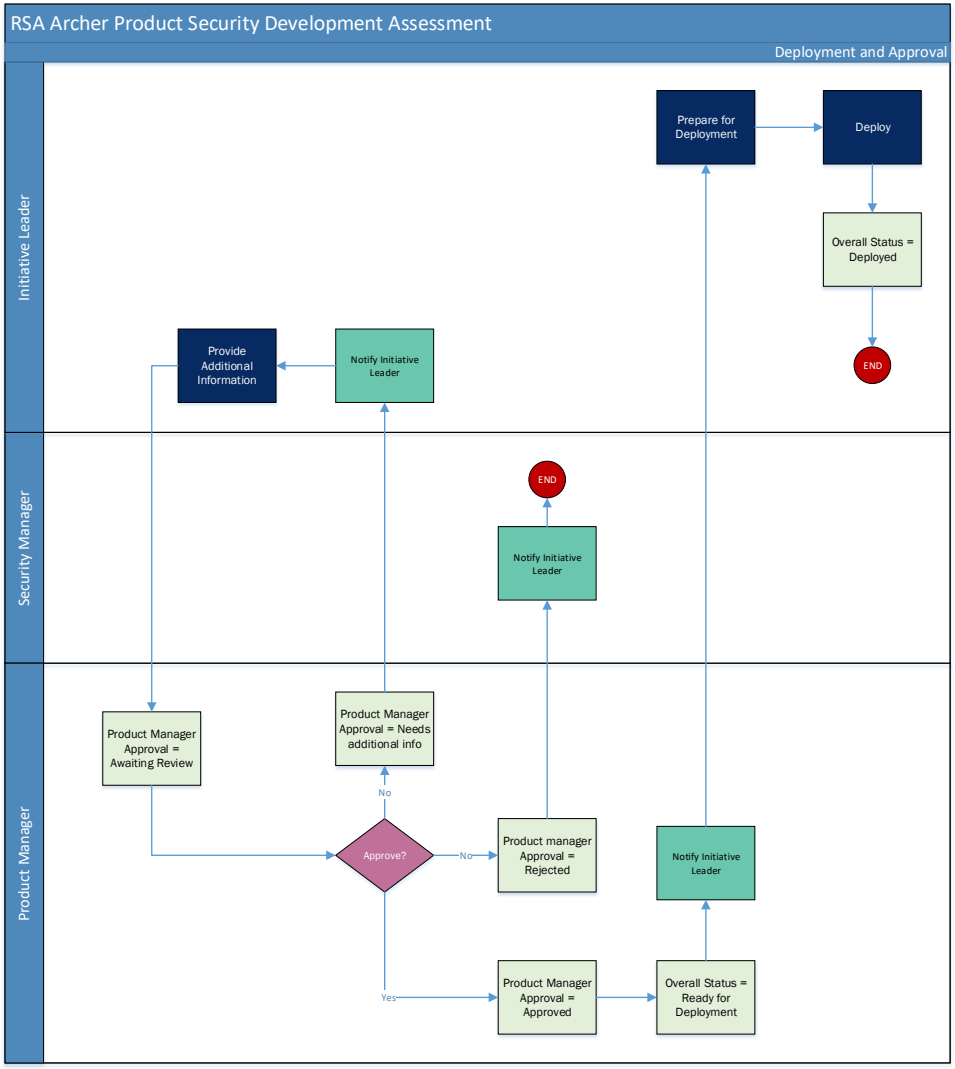
Risk Identification and Mitigation:



Development and Security Testing:



Deployment:



Applications

The following table describes the applications in RSA Archer Product Security Development Assessment.

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	How many (per Information System)?	Optional / Required
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.	Many	Required
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.	One or Two	Required
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	Many	Required

	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.	Many	Optional

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.

Chapter 3: Installing RSA Archer Product Security Development Assessment

Complete the following tasks to install the application.

Step 1: Prepare for the Installation

1. Ensure that your RSA Archer GRC system meets the following requirements:
    - RSA Archer GRC Platform version 6.6
2. Download the ODA install package from the RSA Archer Exchange on RSA Link: https://community.rsa.com/community/products/archer-grc/exchange/documentation-downloads.
3. Read and understand the "Packaging Data" section of the RSA Archer GRC Online Documentation.

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” for complete information.

Step 3: Test the Installation

Test the RSA Archer Product Security Development Assessment app-pack according to your company standards and procedures, to ensure that it works with your existing processes.

Installing the RSA Archer Product Security Development Assessment Package

Step 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. RSA 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.

Step 2: Import the Package

1. Go to the Install Packages page.
    a. From the menu bar, click  .
    b. 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.

Step 3: Map Objects in the Package

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.
3. 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.

The following table describes the icons.

Icon	Name	Description
	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  icon is for informational purposes only.
	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.

	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.

4. 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 " Parent and Child Object Mapping " in the RSA Archer Online Documentation.
   - 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:
     a. In the toolbar, click Auto Map.
     b. Select an option for mapping objects by name.

The following table describes the options.

Option	Description
Ignore case	Select this option to match objects with similar names regardless of the case of the characters in the object names.
Ignore spaces	Select this option to match objects with similar names regardless of whether spaces exist in the object names.

     c. Click OK.

     The Confirmation dialog box opens with the total number of mappings performed. These mappings have not been committed to the database yet and can be modified in the Advanced Package Mapping page.

     d. Click OK.
   - To set all objects in the tab to Do Not Map, in the toolbar, click Do Not Map.
     Note: To undo the mapping settings for any individual object, click in the Actions column.

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

5. Verify that all other objects are mapped correctly.
6. (Optional) To save your mapping settings so that you can resume working later, see "Exporting and Importing Mapping Settings" in the RSA Archer Online Documentation.
7. Once you have reviewed and mapped all objects, click  .
8. Select I understand the implications of performing this operation and click OK.

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

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

Step 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. 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.
   a. From the menu bar, click  .
   b. Under Application Builder, click Install Packages.
2. In the Available Packages section, do the following:
   a. Locate the package file you want to install.
   b. In the Actions column, click  .
3. In the Selected Components section, select the components of the package that you want to install.
   - To select all components, select the top-level checkbox.
   - To install only specific global reports in an already installed application, select the checkbox associated with each report that you want to install.

   Note: Items in the package that do not match an existing item in the target instance are selected by default.
4. Click Lookup.
5. For each component section, do the following:
   Note: To move onto another component section, click Continue or select a component section in the Jump To drop-down menu.
   a. In the Install Method drop-down menu, select an install method for each selected component.

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.

b. In the Install Option drop-down menu, select an install option for each selected component.

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.

6. Click OK.
7. 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.
8. Click Install.
9. Click OK.

Step 5: Review the Package Installation Log

1. Go to the Package Installation Log tab of the Install Packages page.
   a. From the menu bar, click  .
   b. Under Application Builder, click Install Packages.
   c. 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 Errors.

Setting up Data Feed

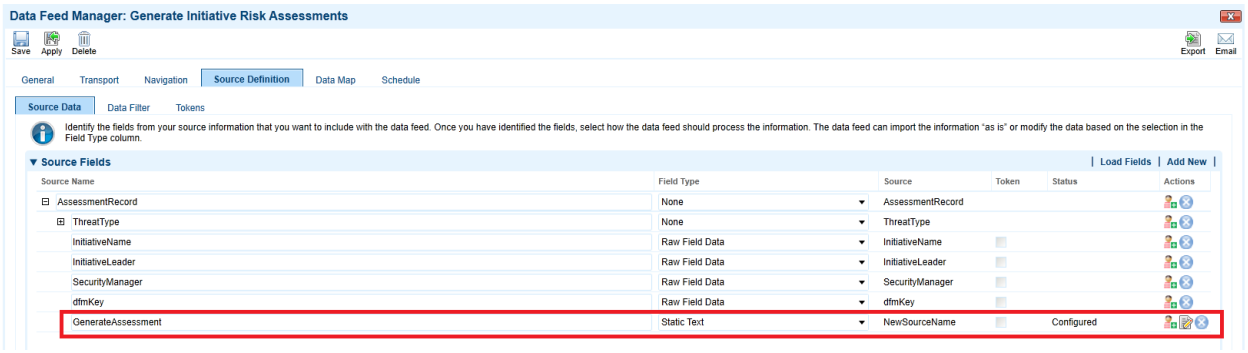
Data Feed **Generate Initiative Risk Assessments** is included in the RSA Archer Product Security Development Assessment app-pack package. This Data feed is used to create new Initiative Risk Assessment records during the phase of Risk Identification and Mitigation. Follow below steps to setup the Data Feed:

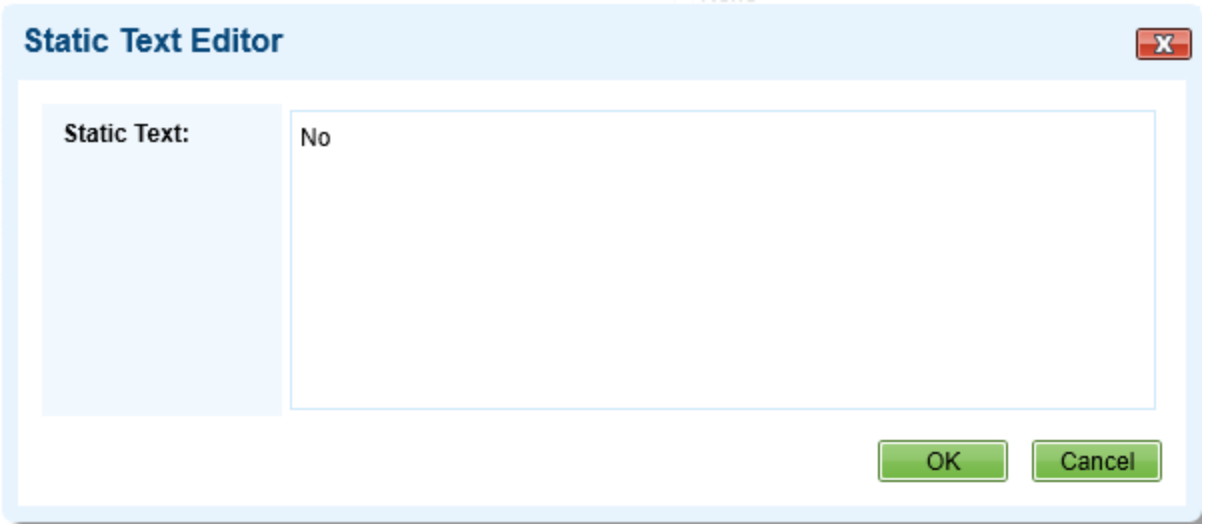
1. Go to Manage Data Feeds page:
   a. From the menu bar, 
   b. Under Integration, click Data Feeds.
2. Locate and select the data feed **Generate Initiative Risk Assessments**.
3. Verify settings in the General tab.
   a. In the General Information section, set the Status field to Active.
   b. In the Feed Information section, confirm that the Target field is set to Initiative Risk Assessment.
4. Click the Transport tab.

a. In the Transport section, confirm that the Transport Method field is set to Archer Web Services Transporter.
b. In the Security section, in the URL field, insert the URL to your instance.
c. In the Transport Configuration section, do the following:
    i. In the User Name and Password fields, type the username and password of a Platform user.
    ii. 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. Click the **Run Detail** link for additional information on the status of the feed or to troubleshoot any feed errors.

Note: All the Source Fields on the **Source Definition** tab will get automatically populated when you import the data feed. Repopulating the fields by clicking on “Load Fields” will lead to removal of one pre-populated field from the list i.e., **GenerateAssessment**. Hence, add a new field by clicking on “Add New” and rename as “GenerateAssessment” and select field type “Static Text” with value “No” in the Text editor (Pleased see screenshots below). Also, make sure that the data mappings are configured correctly after the load fields.





Please refer below table for Source and Target Fields mapping:

Source Fields	Target Fields
dfmKey	**DFM Key** [Field Type: Text]
InitiativeLeader	**Initiative Leader** [Field Type: Record Permissions]
SecurityManager	**Security Manager** [Field Type: Record Permissions]
ThreatType	**Threat Type** [Field Type: Values List]
InitiativeName	Product Initiatives -> **Initiative Name** [Field Type: Related Records -> Text]
GenerateAssessment	Product Initiatives -> **Generate Risk Assessment** [Field Type: Related Records -> Values List]

Chapter 4: Using RSA Archer Product Security Development Assessment

Task 1: Create a New Initiative

Users: Initiative Leader

1. Go to the Product Initiatives record.
    a. From the menu bar, click Product Security Development Assessment.
    b. Under Solutions, click Product Security Development Assessment.
    c. Under Applications, click Product Initiatives.
    d. 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  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 by the Data Feed. 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  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 Tasks section on your Task landing screen.
2. Click the **EDIT** button in the top of the record.

3. To Approve the request
   - **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.
   - 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.
   - Make sure the Risk Mitigation Approval field contains Approved in all the Initiative Risk Assessment records.
   - Click on **Approve** button in the top left of the screen.
4. To request additional information from the Initiative Leader:
   - **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.
   - 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.
   - Document the additional information requested in the Risk Mitigation Review Comments field.
   - Click on **Request Additional Information** button at the top left of the screen.
5. To Reject the Initiative:
   - **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.
   - 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.
   - Document the reason for rejecting the request in the Risk Mitigation Review Comments field.
   - 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.
   a. From the menu bar, click Product Security Development Assessment.
   b. Under Solutions, click Product Security Development Assessment.
   c. 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.
   d. From the menu bar, click Product Security Development Assessment.
   e. Under Solutions, click Product Security Development Assessment.
   f. Under Applications, click Product Initiatives.
   Select the initiative record in 'Release Approval' Status.
2. Click the **EDIT** button in the top of the record.
3. To Approve the request
   - Click on **Approve** button in the top left of the screen. The user has a secure way to approve the record with **electronic signatures.**
   - User enters their Archer password for completing the Approve action.
   - Electronic signature is tracked through entries in a History Log field and by having a system generated snapshot automatically attached to an attachment field.
4. To request additional information from the Initiative Leader:
   - Document the additional information requested in the Comments field.
   - Click on **Request Additional Information** button at the top left of the screen.
5. To Reject the Initiative:
   - Document the reason for rejecting the request in the Comments field.
   - 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.
   g. From the menu bar, click Product Security Development Assessment.
   h. Under Solutions, click Product Security Development Assessment.
   i. Under Applications, click Product Initiatives.
   Select the initiative record in 'Release to Ops' Status.
2. Click the **EDIT** button in the top of the record.
3. To Approve the request
   - Click on **Approve** button in the top left of the screen. The user has a secure way to approve the record with **electronic signatures.**

- User enters their Archer password for completing the Approve action.
- Electronic signature is tracked through entries in a History Log field and by having a system generated snapshot automatically attached to an attachment field.

4. To request additional information from the Initiative Leader:
   - Document the additional information requested in the Comments field.
   - Click on **Request Additional Information** button at the top left of the screen.
5. To Reject the Initiative:
   - Document the reason for rejecting the request in the Comments field.
   - 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 on your 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.
   a. From the menu bar, click Product Security Development Assessment.
   b. Under Solutions, click Product Security Development Assessment.
   c. 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.
   a. From the menu bar, click Product Security Development Assessment.
   b. Under Solutions, click Product Security Development Assessment.
   c. Under Applications, click Countermeasures.

   d. click New.
2. Enter Countermeasure Name in the General Information section.
3. Select the Threat Type by clicking  next to the field and making your selection.
4. Select user from the list in the Countermeasure Approver field by clicking  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  and 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.
   a. From the menu bar, click Product Security Development Assessment.
   b. Under Solutions, click Product Security Development Assessment.
   c. 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
   - Select 'Approve' from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   - Click **Save** in the Record Toolbar to save in Countermeasure record.
5. To request additional information from the Initiative Leader:
   - Select 'Needs Additional Information' from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.

- Document the additional information requested in the Comments field.
- Click **Save** in the Record Toolbar to save in Countermeasure record.

6. To Reject the Countermeasure:
   - Select 'Reject' from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   - Document the reason for rejecting the request in the Comments field.
   - Click **Save** in the Record Toolbar to save in Countermeasure record.
7. To Decommission the Countermeasure:
   - Select 'Decommission' from Countermeasure Review field value by clicking the down arrow next to the field and making your selection.
   - Document the reason for Decommissioning the request in the Comments field.
   - Click **Save** in the Record Toolbar to save in Countermeasure record.