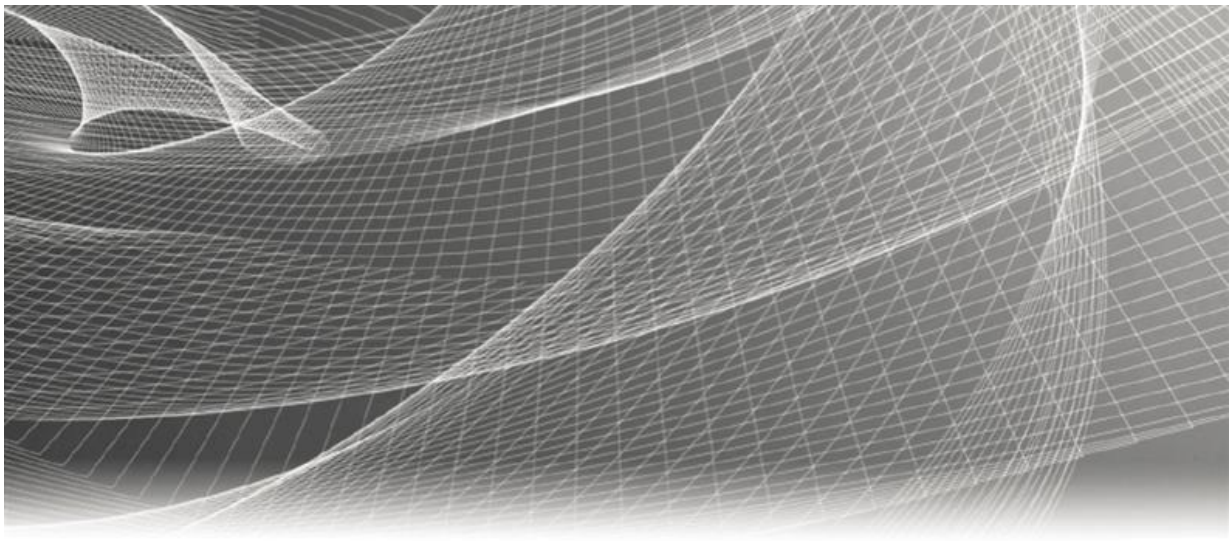


NTT
ISMS Control Assessment App-Pack Implementation Guide

6.6 Patch 4 and 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 Dell are either registered trademarks or trademarks of Dell Corporation ("Dell") 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 towww.emc.com/legal/emc-corporation-trademarks.htm.

License agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on RSA.com. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

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.

For secure sites, Dell recommends that the software be installed onto encrypted storage for secure operations.

For customers in high security zones, Dell recommends that a full application sanitization and reinstallation from backup occur when sensitive or classified information is spilled.

Note on Section 508 Compliance

The RSA Archer® Suite 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 RSA Archer.

The RSA Archer Mobile App can be used with assistive technologies built into iOS. While there remain some gaps in support, RSA is committed to improving the experience of users of these technologies as part of our ongoing product road map for the RSA Archer Mobile App.

Distribution

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

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice. Use of the software described herein does not ensure compliance with any laws, rules, or regulations, including privacy laws that apply to RSA's customer's businesses. Use of this software should not be a substitute for consultation with professional advisors, including legal advisors. No contractual obligations are formed by publication of these documents.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL INC. 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.

February 2020

Table of Contents

Chapter 1: Overview of ISMS Control Assessment

About ISMS Control Assessment

Designing the right processes, organization, and templates during the initial setup of an Information Security Management System (ISMS) are challenges organizations face. Rolling out ISMS in a big organization requires automating frequent manual steps, usability, easy reporting or access permissions to sensitive information.

The NTT ISMS Control Assessment App-Pack helps organizations roll out and operate ISMS by assessing multiple assets throughout the organization, such as applications, locations or business units. This contains a classification and a control assessment step. It augments existing RSA Archer use cases to support an assessment approach as described in the ISO 2700x standards or NIST special publications. Another NTT offering, the NTT ISMS Risk Assessment App-Pack, adds an additional step to the workflow that helps organizations to define, prioritize, and track measures based on risks automatically derived from previous steps.

The App-Pack is designed to provide a multilanguage user interface for end users. This includes both layout aspects (dashboards, field names or values in values lists, sections, and tabs) and content (control names and control statements).

Key Features and Benefits

The NTT ISMS Assessment App-Pack enables the user to:

- Evaluate the maximum impact resulting from a breach of a security objective (confidentiality, integrity, availability) based on a questionnaire or by inheriting from one or multiple assets.
- Assess compliance with relevant controls (filtered by asset category, classification and zone).
- Define and track remediation plans.

With the NTT ISMS Assessment App-Pack, you can:

- Assess assets with a streamlined process as part of the organization’s ISMS.
- Gain insight into compliance violations of internal or external policies.
- Prioritize budget, in conjunction with the NTT ISMS Risk Assessment App-Pack, without the need for a manual risk assessment.
- Improve overall compliance and security.

Prerequisites (and System Requirements)

Components	Recommended Software
ODA License(s)	ISMS Control Assessment requires 5 ODA licenses.
RSA Archer	RSA Archer 6.6 P4 and later
Prerequisite Required Use Cases	RSA Archer Issues Management
Optional Use Cases	RSA Archer IT Risk Management

Compatible Use Cases and Applications

Required Core Applications

The following applications are prerequisites for this offering and are required.

Application	Use Case	Primary Purpose(s) of the Relationship
Remediation Plans	RSA Archer Issues Management	• Define remediation plans to improve compliance. • Track these remediation plans as part of your overall Issues Management use case.
Task Management	NA	• Track tasks as part of your overall Task Management.

Optional Related Core Applications

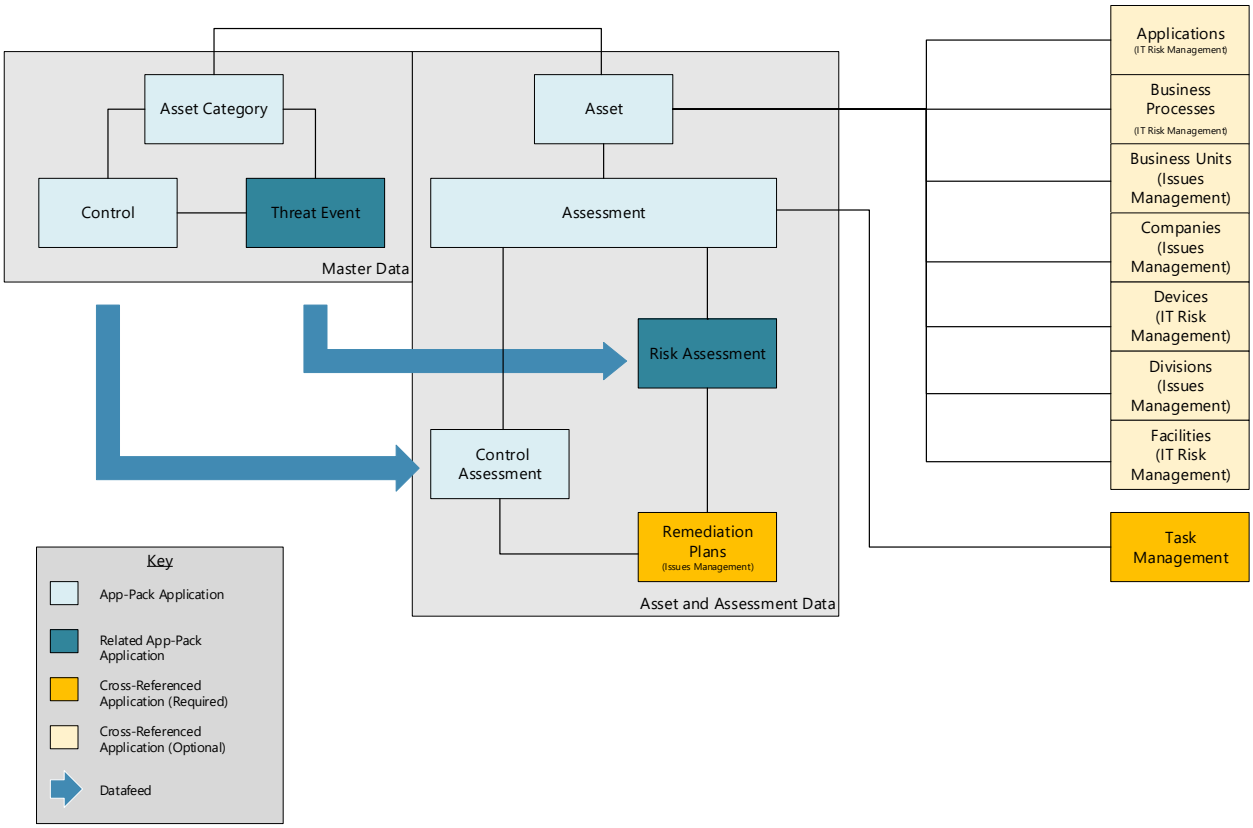
The following applications are optional. This offering can be related to these applications through cross-references. Link your assets to records in these applications (refer to 'Task 8 (Optional): Synchronize Assets' in chapter 4). This is a similar approach as it is used in the Audit Entities application as part of the RSA Archer Audit Management use cases.

Application	Use Case
Applications	RSA Archer IT Risk Management (RSA Archer IT & Security Risk Management)
Business Processes	RSA Archer IT Risk Management (RSA Archer IT & Security Risk Management)
Business Units	RSA Archer Issues Management (RSA Archer Audit Management)
Companies	RSA Archer Issues Management (RSA Archer Audit Management)

Devices	RSA Archer IT Risk Management (RSA Archer IT & Security Risk Management)
Divisions	RSA Archer Issues Management (RSA Archer Audit Management)
Facilities	RSA Archer IT Risk Management (RSA Archer IT & Security Risk Management)

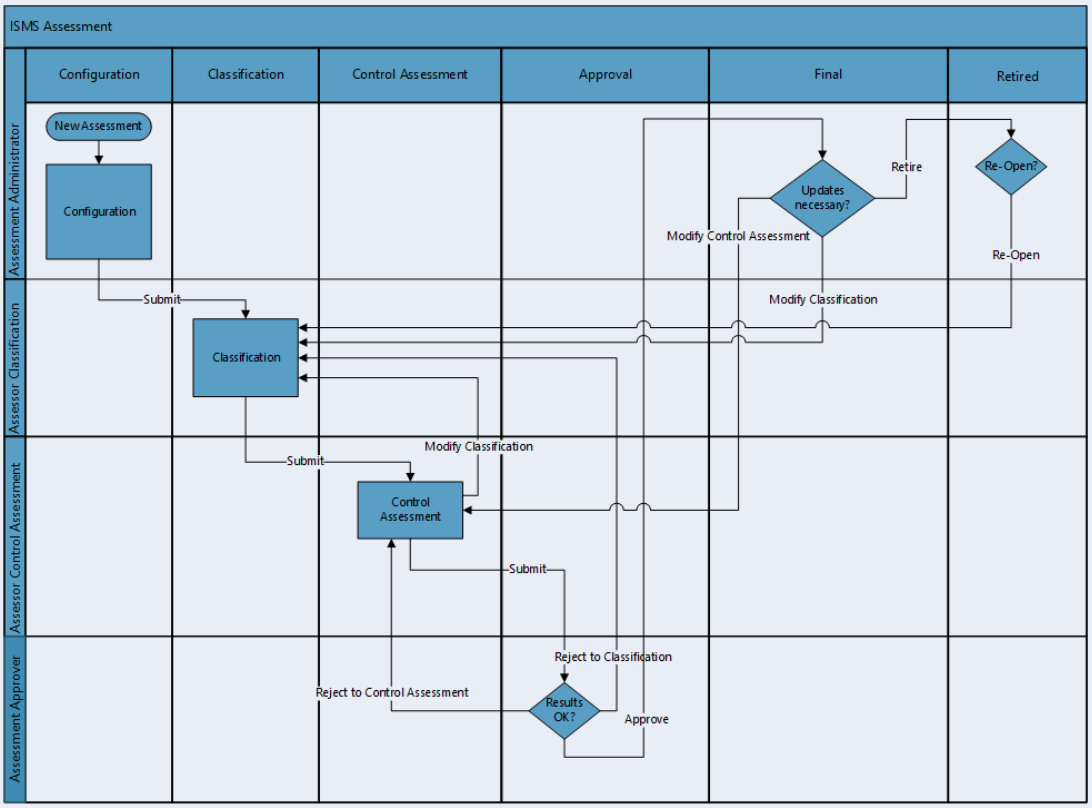
Chapter 2: ISMS Control Assessment Components

Architecture Diagram



Swim Lane Diagram

The following diagram shows the general workflow of the offering.



Applications

Application	Description
Asset	The Asset application is the central repository of ISMS related asset information. It contains basic master data as well as classification information that can be used to inherit an assessment's classification from (see Task 10 (Optional): Add Additional Master Data Applications in chapter 4).
Asset Category	The Asset Category application contains types of assets like Web Application, Database Server, and Office Building. For each asset category, a set of relevant controls can be defined.
Control/Control Category	The levelled application Control/Control Category is the central repository for ISMS-related control information.
Assessment	The Assessment application is the central application of the App-Pack. From a business point of view the workflow contains the following steps: 1. Classification (determine the maximum impact from a breach in security objectives (confidentiality, integrity, availability) and derive a classification). 2. Control assessment (report the implementation status for each relevant control). 3. Approval (review and confirm assessment results).
Control Assessment/Control Category	The levelled Control Assessment/Control Category application contains data copied from the Control/Control Category application. Users enter the implementation status of a control for specific assets.

Related NTT App-Pack Applications

Application	App-Pack	Primary Purpose(s) of the Relationship
Threat Event	NTT ISMS Risk Assessment	The Threat Event application is the central repository for ISMS related threat information.
Risk Assessment		The Risk Assessment application contains data copied from the Threat Event application. Risks (gross, net, residual) are calculated automatically based and users can define Remediation Plans to mitigate risks.

Personas and Access Roles

The following table describes the functions that make up the application's organization roles. Depending on the functional roles of your organization, these functions and responsibilities may vary.

Function	Description
Assessment Administrator	Creates new assessments, selects assets for assessments, grants access to assessors. Is authorized to reopen retired assessments. Group: ISMS Assessment Administrators
Assessment Approver	Reviews and approves assessments Group: ISMS Assessment Approvers
Assessor Control Assessment	Assessor during control assessment step in the workflow. Group: ISMS Assessors
Assessor Classification	Assessor during classification step in the workflow. Group: ISMS Assessors
Asset Administrator	Manages data for assets. Group: ISMS Asset Administrators
Master Data Administrator	Manages data for asset categories, controls and control categories. Group: ISMS Master Date Administrators
Security Manager	Read access to all data. Group: ISMS Security Managers

Access Control Matrix						
Group[1]/Application	Assessment	Asset	Asset Category	Control	Control Assessment	Remediation Plans
Assessment Administrators	CRU	R	R	R	R	
Assessment Approvers	RU	R	R	R	R	R
Assessors	RU	R	R	R	RU	CRU
Asset Administrators		CRU	R			
Master Data Administrators			CRU	CRU		
Security Managers	R	R	R	R	R	R

[1] In Archer, all the groups listed here have a prefix 'ISMS Assmt:' that is not included here.

Additionally, the following technical roles/groups have been defined:

Function	Description
Platform Owners	Operations and support role for the whole RSA Archer Platform.
ISMS Assmt: Module Owners	Operations and Support role for the NTT ISMS Control Assessment App-Pack and the NTT ISMS Risk Assessment App-Pack.
ISMS Assmt: Data Feeds	Technical role for all data feeds.

Note: 'Platform Owners' and 'ISMS Assmt: ISMS Module Owners' groups have been defined according to NTT's best practice approaches for operational roles. Other RSA Archer customers might have other approaches (see Task 4 (if necessary): Adapt Platform Owner and Module Owner Groups in chapter 4).

Chapter 3: Installing ISMS Control Assessment

Installation Overview

Complete the following tasks to install the application.

Step 1: Prepare for the Installation

1. Ensure that your RSA Archer system meets the following requirements:
    - RSA Archer Platform version 6.6 Patch 4.
2. Download the ODA install package from the RSA Archer Exchange on RSA Link: (https://community.rsa.com/community/products/archer- grc/archer-61/downloads).

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: Set up Data Feeds

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

Step 4: Test the Installation

Test the application according to your company standards and procedures, to ensure that the use case works with your existing processes.

Installing the Package

Task 1: Back Up Your Database

There is no Undo function for 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.

Task 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.

Task 3: Map Objects in the Package

Important: This step is required only if you are upgrading to a later version of ISMS Control Assessment.

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.

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 "Mapping Parent/Child Objects" 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.

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.

Task 4: Install the Package

All objects from the source instance are installed in the target instance unless the object cannot be found or is flagged to not be installed in the target instance. 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.

Task 5: Activate Workflow

1. Go to the Manage Applications page.
   a. From the menu bar, click  .
   b. Under Application Builder, click Applications.
2. In the Applications section, select the Assessment 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.

Task 6: 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 Warnings.

Setting Up Data Feeds

Task 1: Create Data Feed User

1. Go to the Manage Users page.
    a. From the menu bar, click  .
    b. Under Access Control, click Users.
2. Click Add New.
3. In the General Information section, enter the name of the user, the username for log on.
    a. First Name: ISMS_A2A_min1
    b. Last Name: ISMS_A2A_min1
    c. User Name: ISMS_A2A_min1
4. in the Account Maintenance section
    a. Enter and confirm a password.
    b. Uncheck 'Force Password Change On Next Sign-In'
    c. If you defined a separate Security Parameter for data feed users, select it.
5. On the Groups Tab, add 'ISMS Assmt: Data Feeds' by clicking on 'Lookup'.

Task 2: Configure Data Feeds

This section refers to the following data feeds:

- ISMS - 0-Min-1 - 010 - Assessment - Update Control Assessment - A2A
- ISMS - 0-Min-1 - 030 - Assessment - Archive - A2A
- ISMS - 0-Min-1 - 040 - Assessment - Update IRPF Helper Fields - A2A

Please refer to the appendix section 'Data Feeds' to learn more about these data feeds.

Repeat the following steps for each data feed:

1. Go to the Manage Data Feeds page.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.

2. Select the data feed from the list.
3. From the General tab in the General Information section, in the Status field, select Active.
4. Click the Transport tab. Update the fields as follows:
    a. Security Section:
        i. In the URL field, type: YourServerName/VirtualDirectoryName/ws/search.asmx
    b. Transport Configuration Section:
        i. In the User Name and Password fields, type the username and password of the user you created in the previous step.
        ii. In the Instance field, type the name of the Platform instance the App-Pack has been installed in.
5. Verify that key field values are not missing from the data feed setup window.
6. Click Save.

Task 3: 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.
    a. From the menu bar, click  .
    b. Under Integration, click Data Feeds.
    c. Select the data feed.
    d. 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.

Please note: The data feeds already contain the schedule configuration set by NTT. Please do not change this configuration without considering any potential consequences.

Chapter 4: Configure the ISMS Control Assessment

Different organizations have different approaches in their ISMS implementation. This results in different requirements for a tool used to support their ISMS rollout and operation. The App-Pack has been built to be as flexible and generic as possible. The following tasks describe typical adaptations to the App-Pack that customers might implement to fully support their specific approaches. The offering includes a four-hour WebEx session with an NTT Lead Consultant about how to implement customer-specific requirements.

Task 1: Grant Access to Remediation Plans

Create a new Record Permission Field 'ISMS Assmt: Inherited Permissions' in the application Remediation Plans. Configure it as follows:

- Permission Model: Inherited/Unrestricted
- Select the following fields from the Control Assessment application:
  - Data Feeds (A-RPF)
  - Security Manager (A-RPF)
  - Assessment Permissions R (I-RPF)

Task 2: Change 'Classification Type' Field Settings

In the Assessment application there is a values list field 'Classification Type' to determine how the classification for the set of assets should be done with the following values:

Value	Description
Manual Assessment	Users select the maximum potential impact for each security objective.
Inherit from Asset	Archer derives the maximum impact from assets.
Assessment with Questionnaire	Users fill out a little questionnaire.

Out-of-the-box this field is not calculated. We recommend changing this to make sure that all assessments have an adequate data quality.

Multiple options include.:

- Select a static value (e.g., *VALUEOF([Classification Type],"Assessment with Questionnaire")*).
- Create an Assessment Type field in the application Assessment to derive the Classification Type from (e.g., 'if assessment type = 'Facility' then Classification Type = 'Manual Assessment'').
- Create an Asset Type field in the application Asset to derive the Classification Type from (e.g., 'if the Asset is an IT Application, use 'Assessment with Questionnaire', if the asset is a facility, use 'Manual Assessment'').
- Promote field to a global values list and create a Classification Type field in the application Asset Category from which to derive the Classification Type.

Note: If the value is 'Inherit from Asset', other mechanisms must be implemented to make sure that the maximum impact is set for each asset. There are also multiple options to do this:

- Configure these fields as required.
- Use additional master data applications (ref. Task 10 (Optional): Add Additional Master Data Applications in chapter 4).

Note: Check the calculation order after the change.

Task 3: Embed JavaScript Libraries

Some custom objects use publicly available JavaScript libraries. To embed the custom objects, do the following:

Copy them to the company files folder (NTT best practice):

1. Copy all the files in the '(3) JS Libraries' folder in your company files directory (e.g. C:\inetpub\wwwroot\archer\company_files).
2. Change the file extension of all files to '.js'.

If copying the files to the server is not possible (for example, because you use a hosted environment), change the custom object code to load the files from a central repository:

Change the custom object code according to the mapping table:

Out-of-the-Box Code	Replace with
<script src="../company_files/raphael.min.js"></script>	<script src="https://cdnjs.cloudflare.com/ajax/libs/raphael/2.2.8/raphael.min.js" integrity="sha256-BgmwZ6j044t3GCQhmJtpiHkUGVYzjapcGWjBH4dVnes=" crossorigin="anonymous"></script>
<script src="../company_files/progressStep.min.js"></script>	<script src="https://cdnjs.cloudflare.com/ajax/libs/progressStep/1.0.3/progressStep.min.js" integrity="sha256-1dgOX5j3o8UIzgSIRJb/f/Ui5AethNu8a2ClYa8pIXc=" crossorigin="anonymous"></script>
<script src="../company_files/popper.min.js"></script>	<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.1/umd/popper.min.js" integrity="sha256-/ijcOLwFf26xEYAjW75FizKVo5tnTYiQddPZoLUHHZ8=" crossorigin="anonymous"></script>
<script src="../company_files/tippy.all.min.js"></script>	<script src="https://cdnjs.cloudflare.com/ajax/libs/tippy.js/3.4.1/tippy.all.min.js" integrity="sha256-iLOTBBYaCzN2utfyApj2yRw3ltH86LwYZrzOz3TTbyg=" crossorigin="anonymous"></script>

In the following custom objects:

Custom Object	Libraries	Applications
Workflow Progress	raphael.min.js progressStep.min.js	Assessment
Translation and Design	popper.min.js tippy.all.min.js	Assessment Asset Asset Category Control/Control Category Control Assessment

If none of the options are acceptable, remove all the custom objects from layout in all applications. All the features are used to improve user experience, none of the features are required for the App-Pack to function.

Task 4 (if necessary): Adapt Platform Owner and Module Owner Groups

NTT built the App-Packed following its Implementation Best Practices. One of these is to define operational and support groups already during implementation. Because most RSA Archer customers have multiple GRC processes (NTT calls them Modules) hosted in one RSA Archer environment, NTT's Best Practice is to define:

- Platform Owner Group and Role (supporting all Modules).
- Module specific Owner Group and Role for each Module (supporting a particular Module).

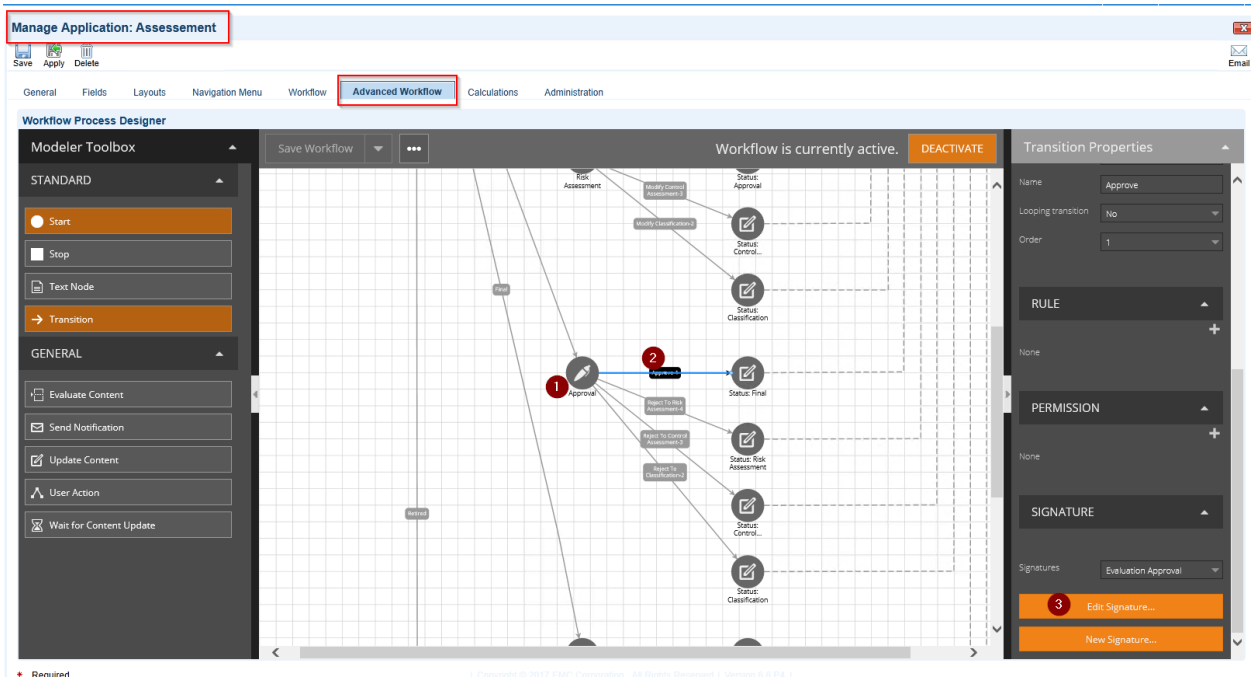
Other RSA Archer customers might have different Best Practices. These Groups and Roles are not necessary for the App-Pack to function. Adapt them according to your Best Practices or remove them.

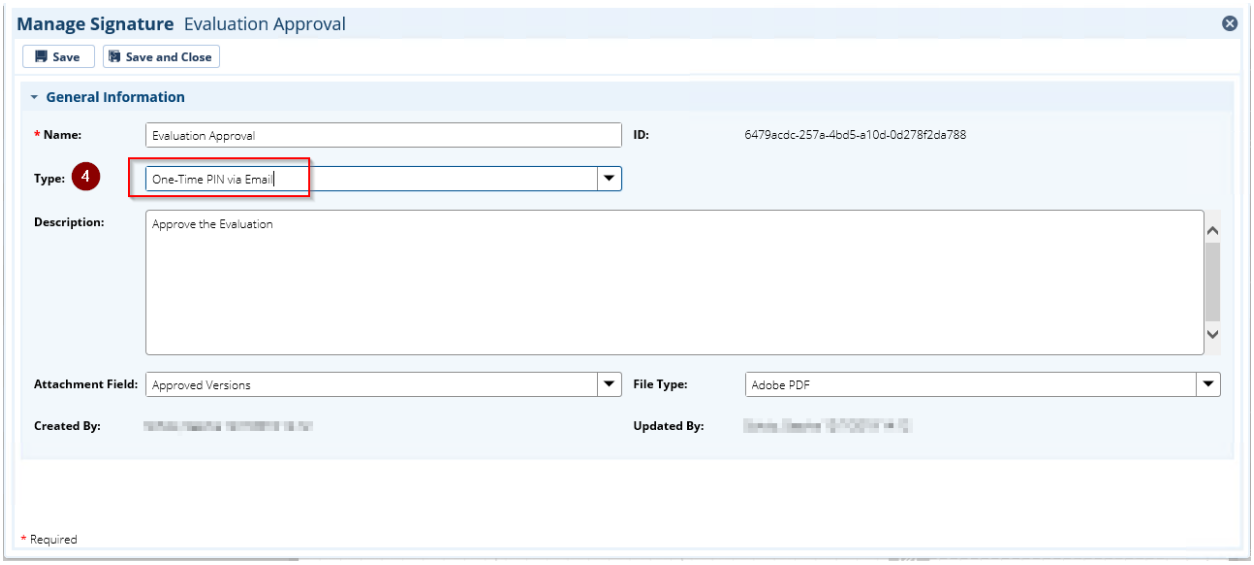
- Replace groups as:
    - Application Owners in all applications
    - Report Administrators in all applications
- Replace groups in Access tab of:
    - All Dashboards
    - The ISMS Assessment Workspace
    - All History Log (Debug) fields

Task 5 (if necessary): Change Signature Type

The Assessment application uses the Advanced Workflow Signature feature to archive data after approval. Out-of-the-box the type is set to 'User Name / Password'. If you use Single-Sign-On authentication, change this to 'One-Time PIN via Email':

1. On the Advanced Workflow Tab in application Assessment, locate the User Action Node 'Approval'.
2. Click on transition 'Approve'.
3. Click the 'Edit Signature' button.
4. Change Type to 'One-Time PIN via Email'.





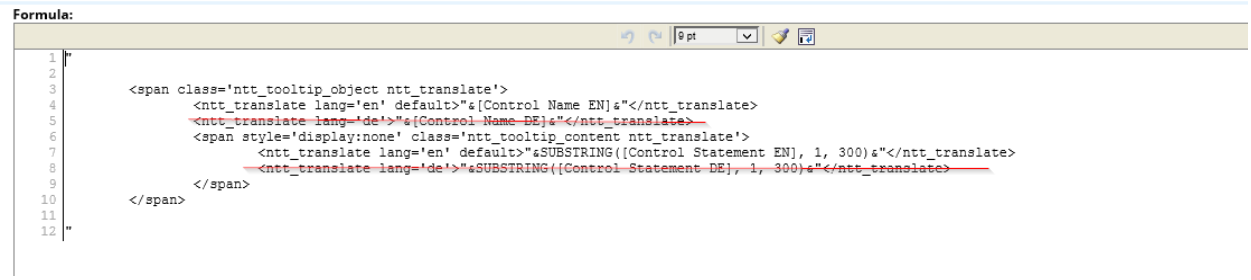
Task 6 (if necessary): Multilanguage

The App-Pack is bilingual (English and German). This includes configuration aspects like fields, sections, tabs, workspaces, or dashboards using the Globalization feature within RSA Archer. Additionally, users can also integrate bilingual content-like controls. The following steps deactivate second language if not needed:

1. Deactivate the following fields (Application/Level/Field) and remove them from Layout:
    a. Control/Control Category/Control Category Name DE
    b. Control Control/Control Name DE
    c. Control/Control/Control Statement DE
    d. Control Assessment/Control Category/Control Category Name DE

e. Control Assessment/Control/Control Name DE
f. Control Assessment/Control/Control Statement DE

2. Remove '<ntt_translate>' tags for the 'German fields' from the following calculated fields (see the following screenshot):
    a. Control/Control Category/Control Category Name
    b. Control/Control/Control Name
    c. Control/Control/Control Statement
    d. Control/Control/Control Summary
    e. Control Assessment/Control Category/Control Category Name
    f. Control Assessment/Control/Control Name
    g. Control Assessment/Control/Control Statement
    h. Control Assessment/Control/Control Summary



3. Remove '<ntt_translate>' tags with lang='de' in field 'Classification With Questionnaire Table' in application Assessment.

Add additional languages by creating new fields and adding them to the Calculated Fields mentioned above.

Task 7 (if necessary): Change Impact and Classification Classes

The App-Pack includes three impact classes and three classification classes for each security objective. Some organizations might use a different set of classes. To support these requirements, change the following configurations:

- Global Values Lists (names, numeric values, translations):
    - ISMS Classification Confidentiality
    - ISMS Classification Integrity
    - ISMS Classification Availability
    - ISMS Impact
- Formula within the following fields in the application Assessment:
    - Classification Confidentiality
    - Classification Integrity
    - Classification Availability
    - Max Impact Confidentiality
    - Max Impact Integrity

- Max Impact Availability

Task 8 (Optional): Synchronize Assets

Many RSA Archer customers use core applications to manage master data for e.g. applications, business units, facilities. To be as flexible as possible NTT chose a similar approach to define assets as RSA did in their RSA Archer Audit Management use cases (application Assets is comparable to the Audit Entity application in the Audit Engagements and Workpapers Use Case).

Many RSA Archer customers use Archer2Archer data feeds to synchronize data in the Audit Entity with data in the corresponding master data applications. This can also be done with the Asset application. Alternatively, a synchronization mechanism can be built directly with an external repository like a CMDB.

Task 9 (Optional): Synchronize Control Procedures

Many RSA Archer customers use the core application 'Control Procedures' to manage their controls. To be as flexible as possible NTT chose to build an ODA to manage controls for the ISMS Assessment App-Pack. Nevertheless, it does not make sense to maintain data in two different applications manually. If you already use the Control Procedures application as your central repository for controls, you can build an Archer2Archer data feed to synchronize these data with the Asset application within the ISMS Assessment App-Pack.

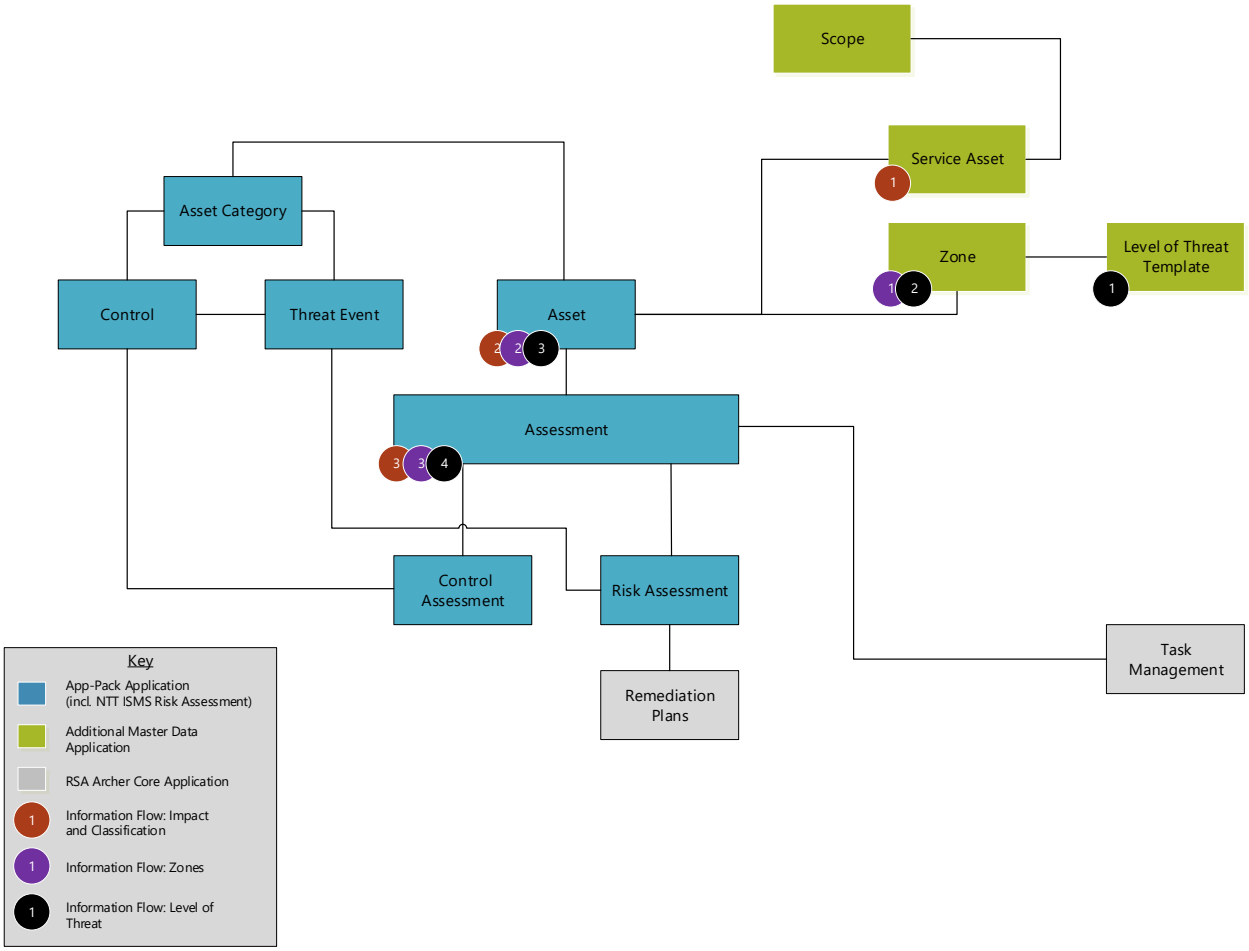
Task 10 (Optional): Add Additional Master Data Applications

The out-of-the-box implementation of the App-Pack contains many fields in the Asset application that act as input for an assessment to filter relevant controls, including the following:

- Zones
- Maximum impact for all security objectives
- Level of threat as input for risk assessment (ISMS Risk Assessment App-Pack)

From a methodology point of view, these are attributes of each asset. In practice these attributes are often derived from other data to reduce effort and improve data quality.

The following architecture diagram outlines a setup a customer uses to fit his specific needs. Since this is a very customer-specific task, your setup may look different:



Additional Application	Purpose
Scope	Record permissions related to some roles are defined here and derived all underlaying data.
Service Asset	Maximum impact is defined on a service asset level and derived to assets and assessments.
Zone	All zones (physical and network) for a scope. The Zones parameter is defined here and then derived to assets and assessments.
Level of Threat Template	Level of Threat (relevant for the NTT ISMS Risk Assessment App-Pack) parameters are defined here and then derived to zones, assets and assessments.

Chapter 5: Using ISMS Control Assessment

Task 1 (Optional): Import Sample Content

As a starting point and to illustrate the basic concepts of the App-Pack NTT provides sample data as part of the offering for the following applications:

- Controls (based on NIST 800-53)
  - Control Categories
  - Controls
- Asset Categories

The following table gives instructions for the import:

File	Target Application	Non-Default Settings
(1) Control - Control Category.csv	Control → Control Category	File Encoding = UTF-8 File Contains HTML Formatting
(2) Control - Control.csv	Control → Control	
(3) Asset Category.csv	Asset Category	

Note: NTT does not guarantee that the mappings provided as part of the sample content are complete or correct for every customer. This sample content is not intended to be used 'as is' in a production environment. NTT assumes that every customer will use their own content or adapt the sample content to fit their specific needs.

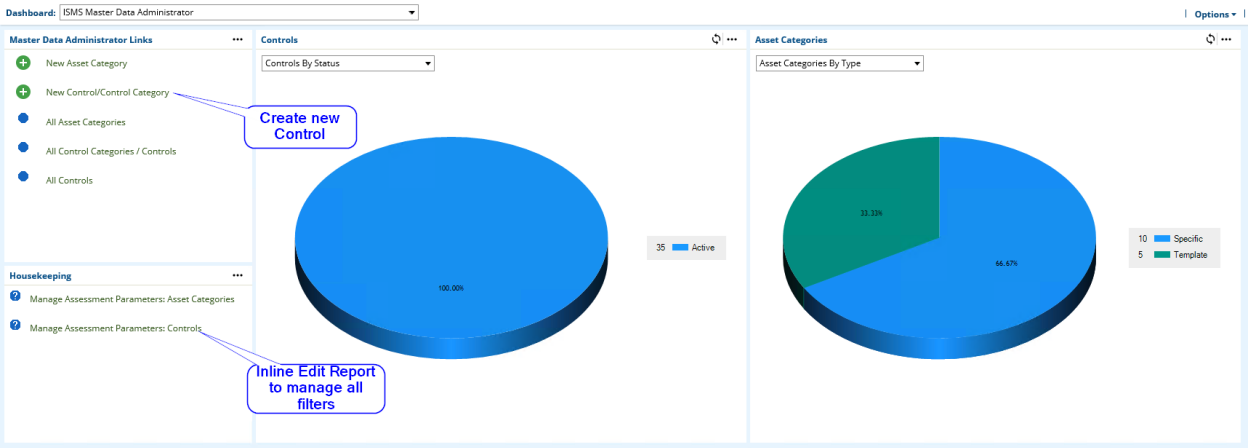
Task 2: Define Controls (Master Data Administrator)

Create the controls and define which controls are relevant (or in scope) for which assets. Three filter mechanisms are available to filter controls:

1. By Asset Category: For each Asset Category only a subset of controls is relevant. Only controls mapped to an Asset Category that is assigned to an Asset can be in scope. Example:
   a. Introducing encryption (Control) does not make sense for an office building (Asset Category).
   b. Having a guard sitting at the entrance (Control) does not make sense for a database server (Asset Category).
2. By Classification: Based on the maximum impact (and derived from that the classification) for each security objective, only a subset of the controls mapped to an Asset Category are relevant for this asset. Example:
   a. Username / Password authentication (Control) is fine for systems managing internal data (Classification), but multi-factor authentication (Control) is required for systems managing confidential data (Classification).
   b. A cluster setup (Control) is required only for systems having a 'High' classification for availability (Classification).
3. By Zone: Based on the Zone an asset resides in, only a subset of the controls mapped to an Asset Category are relevant for this asset. Example:

a. A Web Application Firewall (Control) is only required if the asset is accessible via the Internet (Zone).
b. A CCTV surveillance system (Control) is required for an entrance to a restricted area (Zone).

The Master Data Administrators have access to all these tasks from the ISMS Master Data Administrator dashboard:



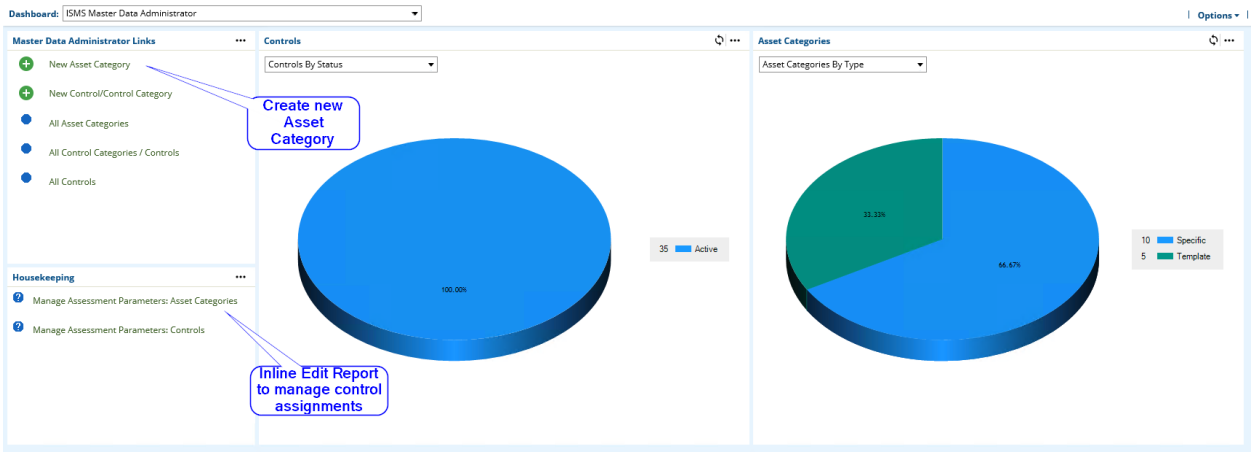
See Task 9 (Optional): Synchronize Control Procedures in Chapter 4.

Task 3: Define Asset Categories (Master Data Administrator)

In addition to Manage Controls, a Master Data Administrator also can define Asset Categories. As described in Task 2: Define Controls (Master Data Administrator), an Asset Category serves as a first filter mechanism to select controls relevant for an Asset. NTT implemented a two-layer approach (field Inheritance Type):

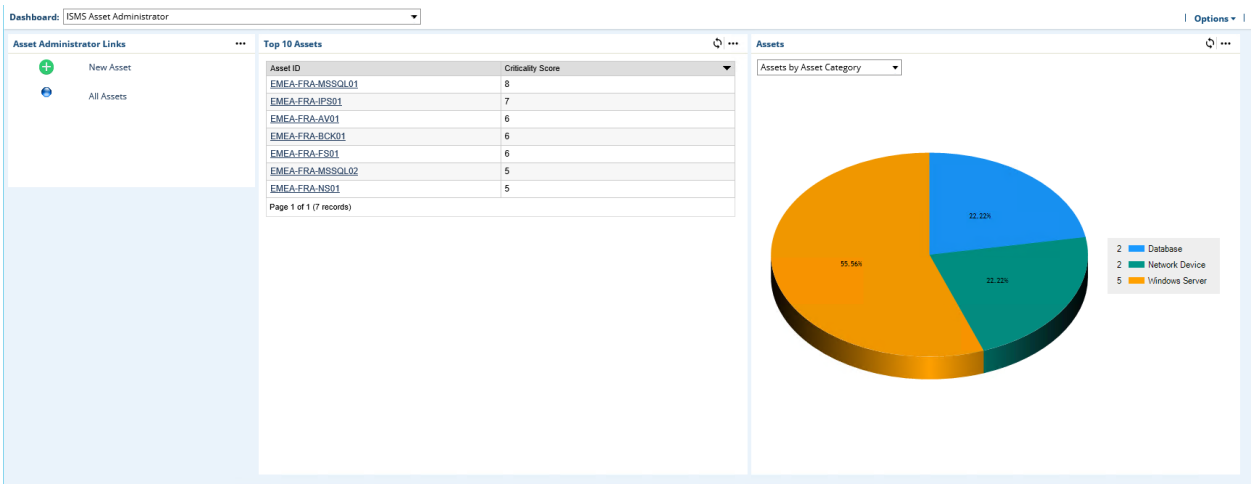
1. Assets can be assigned to specific asset categories.
2. Templates simplify the management of relevant controls as specific categories inherit controls from one or more templates.

The Master Data Administrators have access to all these tasks from the ISMS Master Data Administrator dashboard:



Task 4: Create Assets (Asset Administrator)

An Asset Administrator can create and manage assets from the ISMS Asset Administrator dashboard:

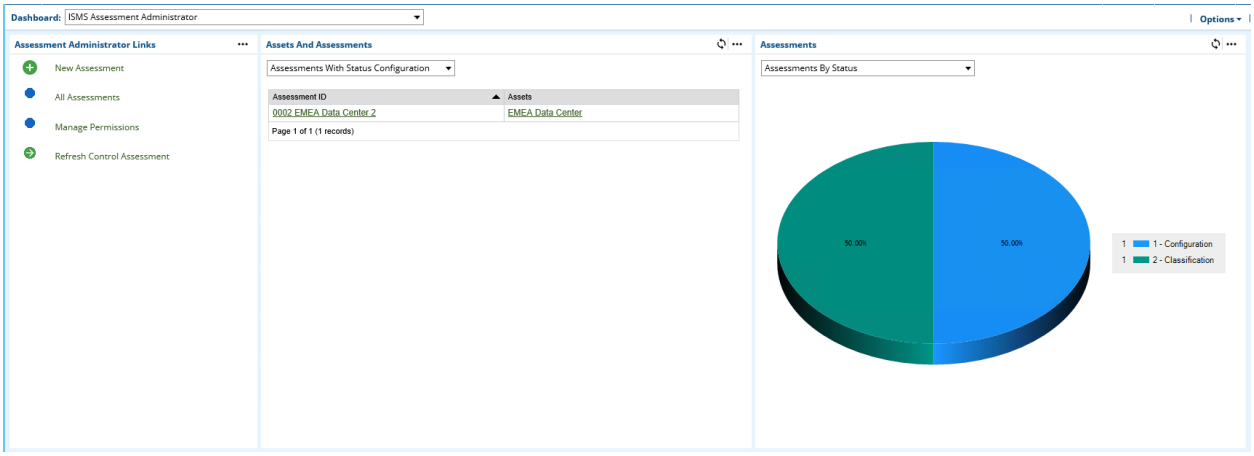


See Task 8 (Optional): Synchronize Assets in Chapter 4.

Task 5: Configure Assessments (Assessment Administrator)

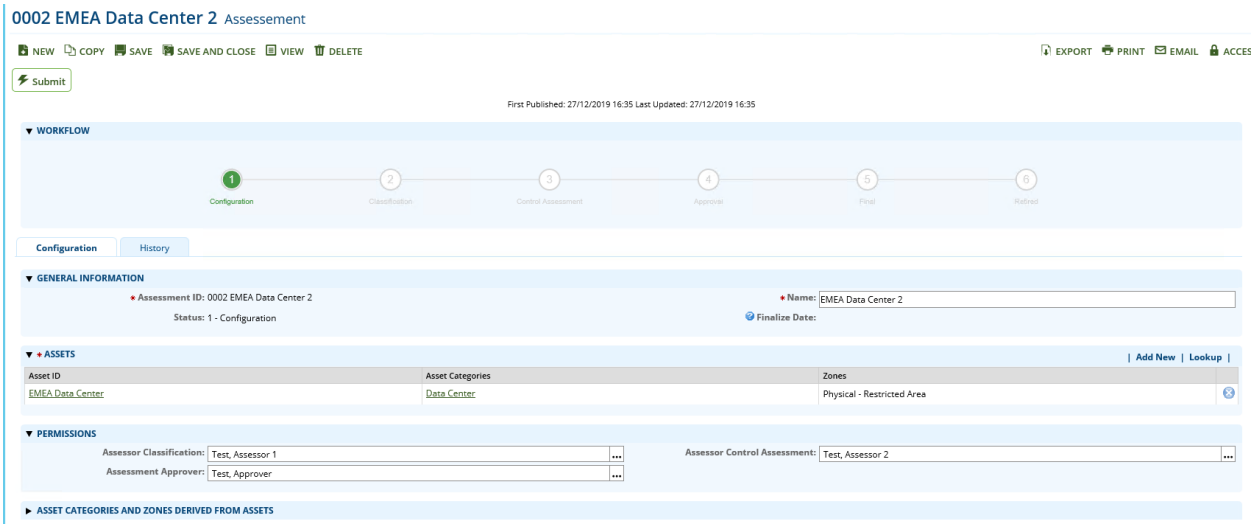
Assessment Administrators create and manage assessments from the ISMS Assessment Administrator dashboard. Assessment Administrators can:

- Assign users to assessment specific roles:
  - Assessor Classification
  - Assessor Control Assessment
  - Assessment Approver
- Assign Assets to Assessments
- Refresh Control Assessment[2]



To finalize the configuration step, click Submit.

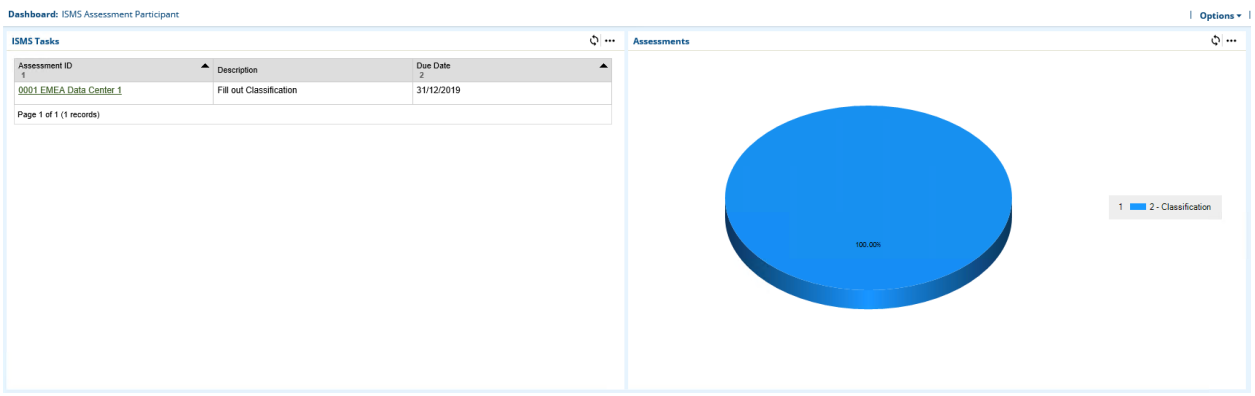
[2] RSA Archer copies master data from the Controls application to the Control Assessment application during the transition between status 'Classification' and 'Control Assessment' (please also refer to Appendix ISMS - 0-Min-1 - 010 - Assessment - Update Control Assessment - A2A). In some cases, it is necessary to refresh the master data by checking the 'Refresh Control Assessment' checkbox located on the Control Assessment tab on the layout. An inline edit report is located the ISMS Assessment Administrator dashboard.



This task refers to the step ‘Configuration’ in the swim lane diagram in Chapter 2.

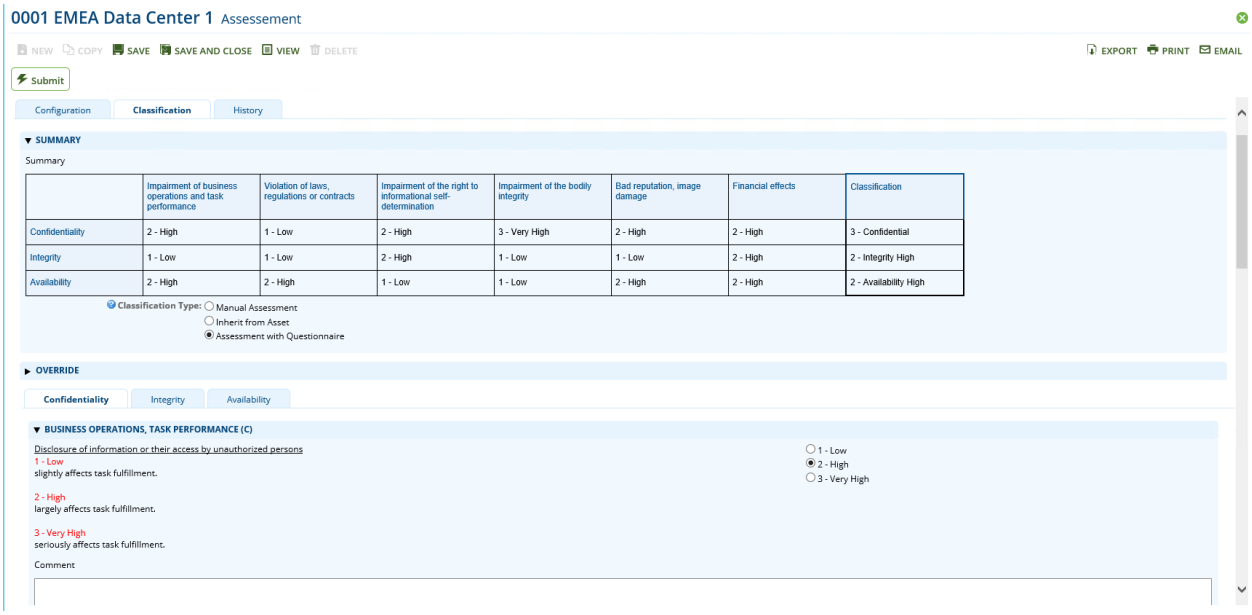
Task 6: Fill Out Assessments (Assessor)

Assessments contain different steps filled out by different personas who all have access to their task from the ISMS Assessment Participant dashboard:



Fill Out Classification (Assessor Classification)

As described in Task 2: Change ‘Classification Type’ Field Settings in Chapter 4, multiple approaches classify assets assigned to an assessment. The following screenshot shows the ‘Assessment with Questionnaire’ approach:

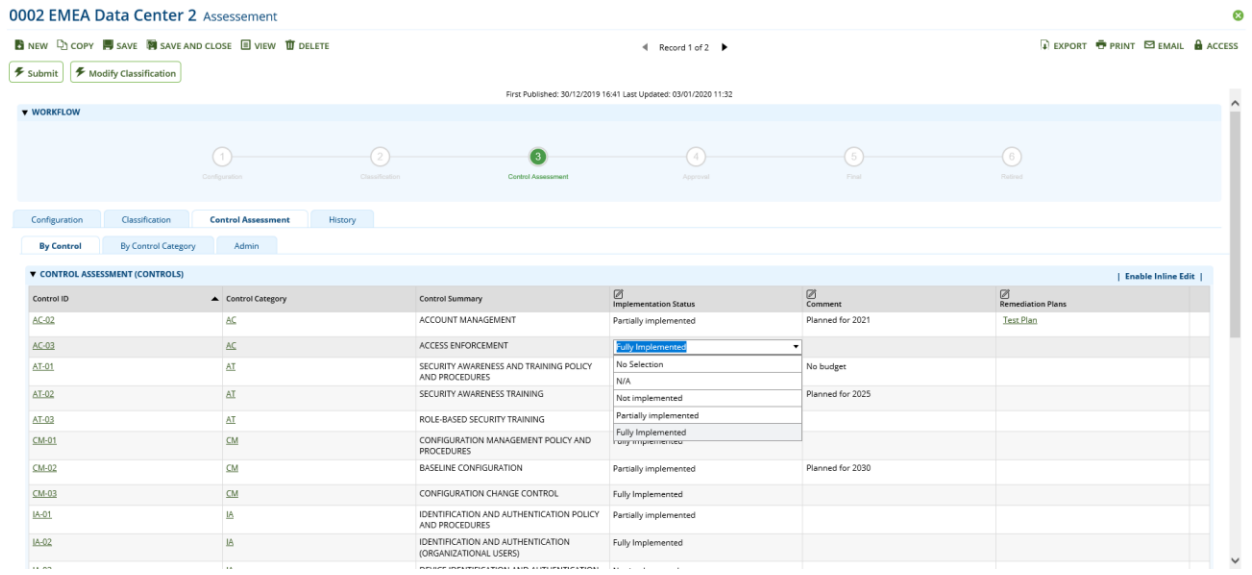


To finalize the classification step, click Submit and the assessment is set to a read-only mode until the data feed ISMS - 0-Min-1 - 010 - Assessment - Update Control Assessment - A2A (Annex) created or updates the Control Assessment records.

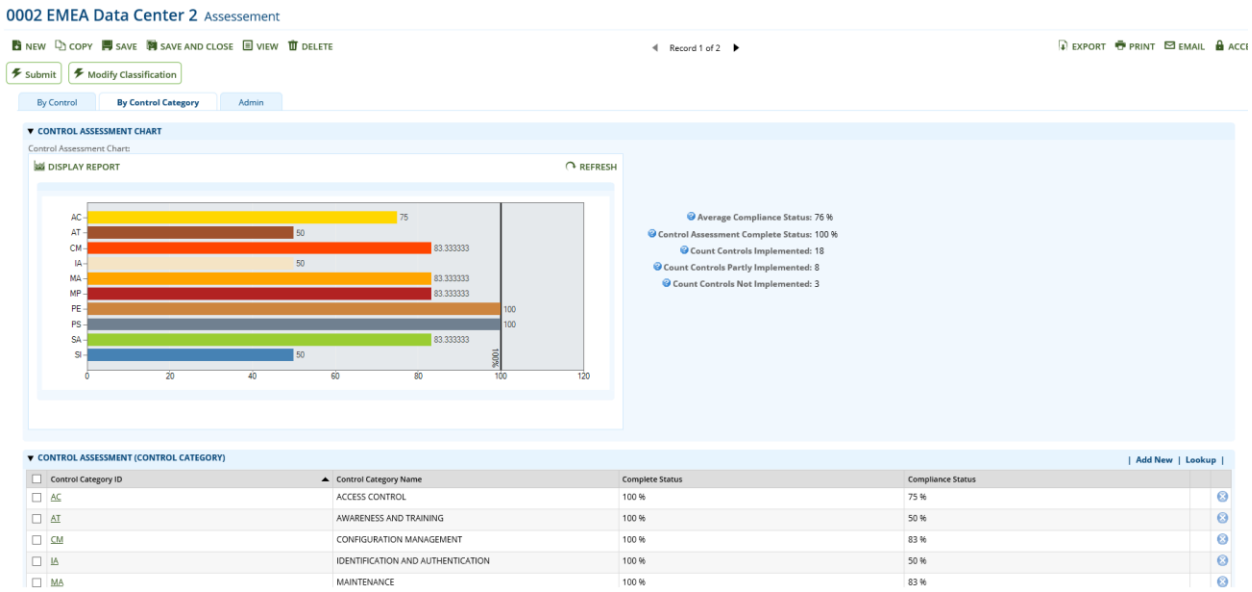
See the 'Classification' step in the swim lane diagram in Chapter 2.

Fill Out Control Assessment (Assessor Control Assessment)

Assessors report the implementation status of all controls in a complete list (Tab 'By Control)':



Or they can open a control category record (tab 'By Control Category') and report back the same type of data for controls mapped to this control category. A chart gives an overview of the implementation status for each category:

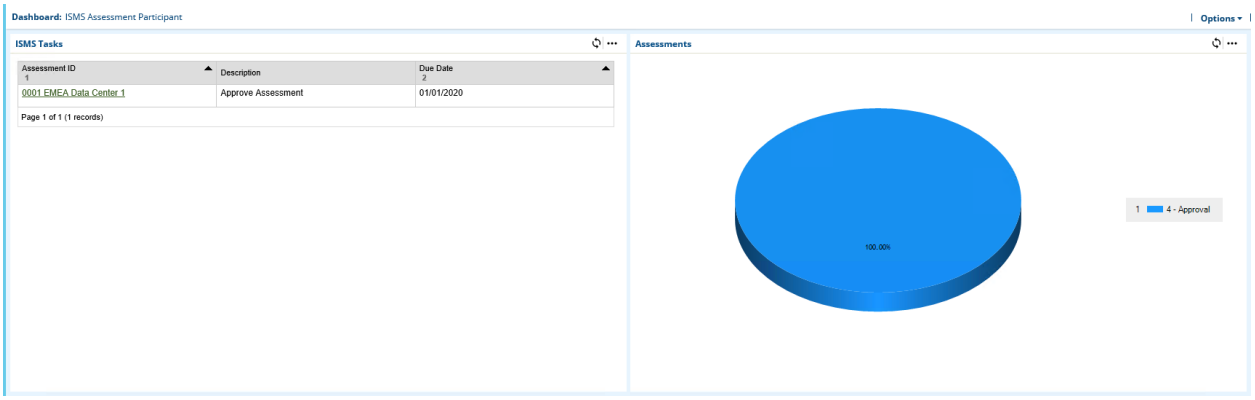


To finalize the Control Assessment step, click Submit.

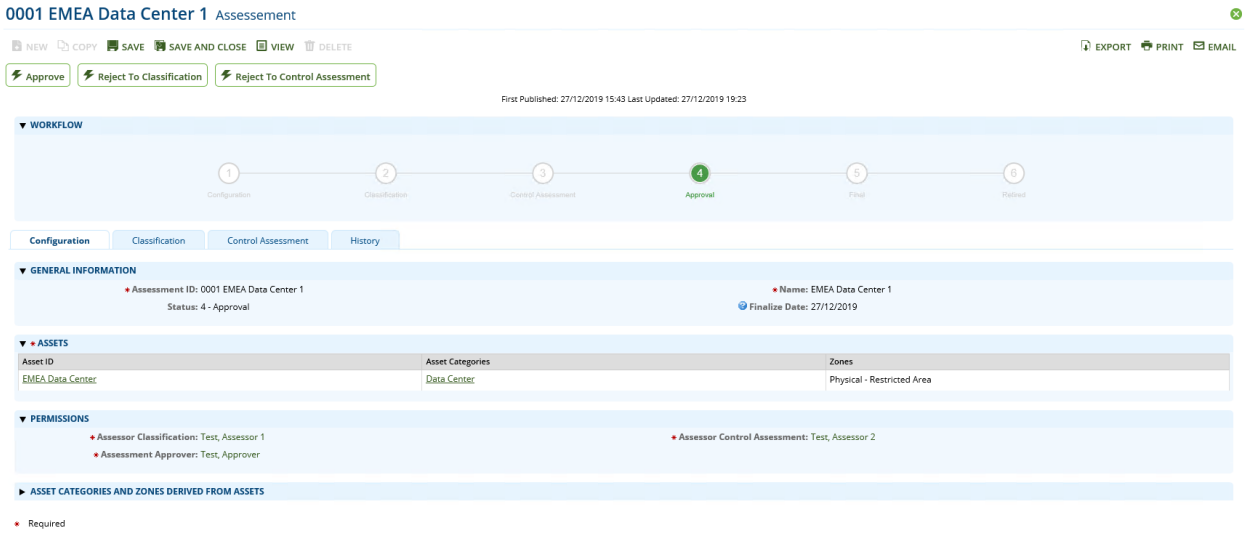
See the 'Control Assessment' step in the swim lane diagram in Chapter 2.

Task 7: Approve Assessments (Assessment Approver)

Assessment approvers have access to the Approval task from the ISMS Assessment Participant dashboard:



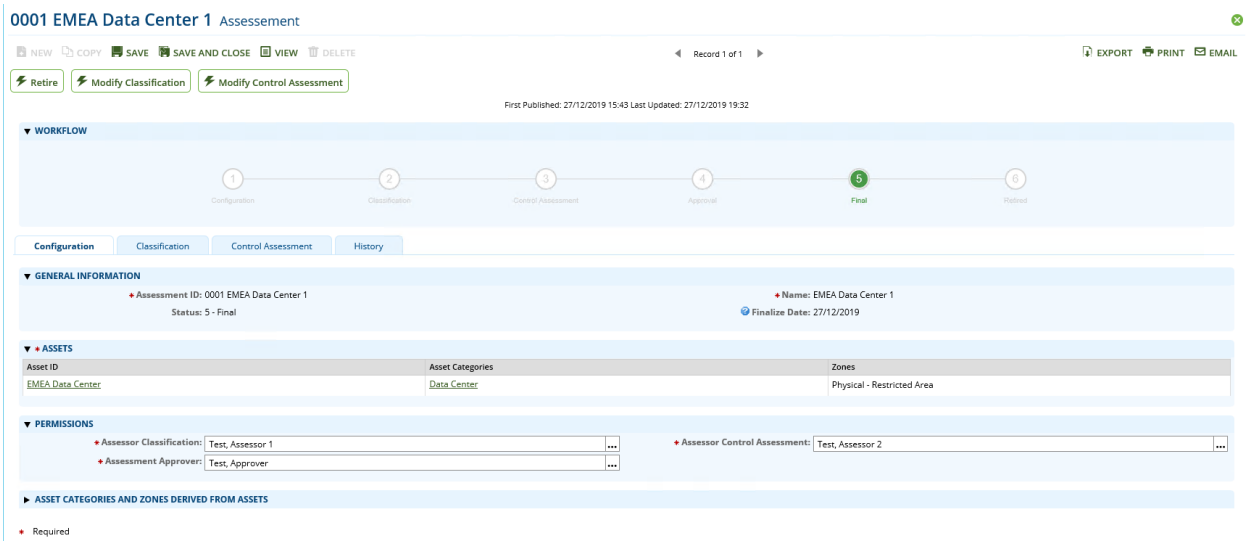
Review all the results and approve or reject the assessment:



This task refers to the step ‘Results OK’ in the swim lane diagram in Chapter 2.

Task 8: Reopen Assessments (Assessment Administrator)

Assessment Administrators can reopen or retire assessments in status ‘Final’ by clicking on one of the buttons shown in the following screenshot.



See the ‘Updates necessary’ step in the swim lane diagram in Chapter 2.

Appendix

Data Feeds

ISMS - 0-Min-1 - 010 - Assessment - Update Control Assessment - A2A

This data feed copies data from the levelled Control application to the leveled Control Assessment application. It is the first data feed running in a convoy of data feeds. It runs once every ten minutes.

The data to be copied to the Control application is obtained by the report ZZ_ISMS - 0-Min-1 - 010 - Assessment - Update Control Assessment - A2A. The report returns data from cross-reference Controls in Scope in application assessment when it is triggered by either the workflow changing to step Control Assessment or by a manual refresh initiated by the user in the Admin sub tab of the Control Assessment tab in the Assessment application.

The xslt stylesheet in the data feed creates an xml document with the control data from the report. A flag value (Assessment_TriggerControlAssessmentUpdateDFAWF) is set 0 to indicate that the data feed has run. A cross-reference to the original record in the Control application is saved.

After the execution of the data feed the user can do the control assessment using the control data from cross-reference Controls in Scope copied by this data feed.

ISMS - 0-Min-1 - 030 - Assessment - Archive - A2A

This data feed copies classification and control assessment data from the Assessment application to corresponding subforms inside the Assessment application. It also copies a selection of this data to fields in the Approved Versions sub tab of the History tab. These fields show the recently approved main assessment data.

The data to be copied to the subforms and the approved version fields is obtained by the report ZZ_ISMS - 0-Min-1 - 030 - Assessment - Archive - A2A. The report returns data from the Assessment application when it is triggered by the workflow changing to step Final.

The xslt stylesheet in the data feed creates an xml document with the archive data from the report. A flag value (Assessment_TriggerArchive) is set 0 to indicate that the data feed has run.

After the execution of the data feed the user can view the archived data.

ISMS - 0-Min-1 - 040 - Assessment - Update IRPF Helper Fields - A2A

This data feed copies users from manual record permission fields inside the Assessment Application to helper permission fields in the same application. These helper permission fields are used to inherit permissions to the Control Assessment application. In this way the users have update and/or read permissions for Control Assessment only during the corresponding workflow step and they have only the minimum required permissions for the Assessment application.

The user and permission data are obtained by the report ZZ_ISMS - 0-Min-1 - 040 - Assessment – Update IRPF Helper Fields - A2A. The report returns the permission data from the Assessment application when it is triggered by a change of the manual record permission fields.

The xslt stylesheet in the data feed creates an xml document with the permission data from the report. A flag value (TriggerPermissionUpdate_Current) is set to indicate that the data feed has run.

After the execution of the data feed the users have the required permissions for the Control Assessment application.

Custom Objects

Workflow Progress

This Custom Object generates a progress diagram to show the status of the assessment workflow process. Each workflow state is shown with the index number and the name. The status is indicated by a green circle and by green text. Depending on the language set in the user's account properties, the name of the current language is used. The custom object uses shared libraries to draw the diagram and is managed by a calculated field (Workflow Helper).

Translation and Design

This Custom Object generate a tooltip for each field that has ntt_translate tags. Depending on the current language of the browser, the ntt_translate tags matching the current language are used to construct the tooltip text. These tags are defined in calculated fields (e.g. 'Control Name' or 'Control Summary' in the application Control / Control)

Inline Edit Auto Save

This Custom Object executes the click function of the 'Save All' element inside Inline Edit Grids.

Refresh Status

This Custom Object shows a Refresh Status link when a Data Feed was triggered. When the user clicks on the link, the current web page in Archer is refreshed and the Refresh Status link is shown again in case the Data Feed has not completed yet. After the Data Feed has completed and a refresh happened on the page the link is not shown anymore.

Applications Using Custom Objects

Application/ Custom Object	Workflow Progress	Translation and Design	Inline Edit Auto Save	Refresh Status
Assessment	☒	☒	☒	☒
Asset	☐	☒	☐	☐
Asset Category	☐	☒	☐	☐
Control/Control Category	☒	☒	☒	☐
Control Assessment	☐	☒	☒	☐