Policy Management Conventions Manual

ARIS Risk & Compliance Manager
Version 9.8

April 2015

Contents

1   Introduction

In order to simplify the creation of policy definitions and facilitate reusability you can model objects in ARIS. This is however only possible if the methodological and functional rules and conventions for modeling in ARIS Architect are adhered to. Only then can all modeled data be transferred to ARIS Risk & Compliance Manager (ARCM) and reused there.

2   Text conventions

Menu items, file names, etc. are indicated in texts as follows:

- Menu items, keyboard shortcuts, dialogs, file names, entries, etc. are shown in **bold**.

- Content input that you specify is shown in **<bold and within angle brackets>**.

- Single-line example texts are separated at the end of a line by the character ↵, e.g., a long directory path that comprises multiple lines.

- File extracts are shown in the following font:

    ```
    This paragraph contains a file extract.
    ```

3 Content of document

The sections below explain the standards relating to the use of descriptive views, model types, object types, relationship and connection types, and attributes.

3.1 Objectives and scope

Objective: Specification of modeling guidelines

Not included in this manual: User documentation

4   ARIS conventions

4.1   Create users and user groups

Users and user groups are modeled in an organizational chart in ARIS Architect using the **Person** (OT_PERS) and **Role** (OT_PERS_TYPE) objects.
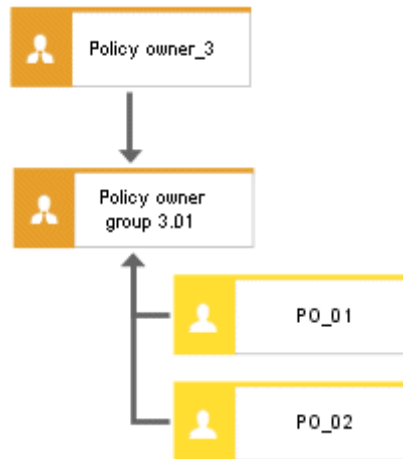
Figure 1: Structure of users/user groups (organizational chart)

The superior role (**Policy owner_3**) determines the role held by the subordinate roles in ARIS Risk & Compliance Manager. Both roles are connected to one another with the **is generalization of** connection. **Policy owner group 3.01** is thus, the generalization of **Policy owner_3**. The name of the superior role defines the role and level of the group to be created. <Role>_<Level>, i. e. Policy owner_3 > Role: Policy owner, Level: 3 (or object-specific). A user group is not generated in ARIS Risk & Compliance Manager for the superior role (**Policy owner_3**).

The following applies for the various levels:

- Level 1: cross-client

  Means that the privileges are assigned across clients.

- Level 2: client-specific

  Means that the privileges are assigned for a particular client.

- Level 3: object-specific

  Means that the privileges are assigned for a particular object, e.g. policy, risk or control.

For the above example, the **Policy owner group 3.01** user group is generated in ARIS Risk & Compliance Manager with the **Policy owner** role and the level 3 (i.e. with object-specific privileges). In addition, the users with the user IDs **PO_01** and **PO_02** are also generated.

Mapping Role name (ARCM) to Role (ABA)

The following allocations are applicable for the user groups in ARIS Risk & Compliance Manager and the naming to be used in ARIS Architect. Further roles are described in the other conventions manuals.

Role (ARCM)	Role (ABA)	Notes
roles.policyauditor	Policy auditor	Levels 1, 2, and 3
roles.policymanager	Policy manager	Levels 1 and 2
roles.policyowner	Policy owner	Level 3 only
roles.policyapprover	Policy approver	Level 3 only
roles.policyaddressee	Policy addressee	Level 3 only

4.1.1   Role to person allocations

Role (ABA) to User group (ARCM) allocations

The following allocations are applicable for the **Role** (user group) object:

ABA attribute	API name	ARCM attribute	M*	Notes
Name	AT_NAME	name	X	The name of a user group is limited to 250 characters.
Description/ Definition	AT_DESC	description	-	
Role	–	role	X	The values for Role and Role level are determined as described above.
Role level	–	rolelevel	X	
Users	–	groupmembers	-	Users are determined by the **performs** connection between the person and the role.

*The **M** column specifies whether the attribute is a mandatory field.

Person (ABA) to User (ARCM) allocations

Existing databases based on old modeling conventions can be migrated using the report **ARCM user migration.arx** supplied. Since the two attributes for first and last name are derived from the same attribute the result needs to be verified.

The following allocations are applicable for the **Person** (user) object:

ABA attribute	API name	ARCM attribute	M*	Notes
Login	AT_LOGIN	Userid	X	The user ID of of a user is limited to 250 characters.
First name	AT_FIRST_NAME	firstname	X	
Last name	AT_LAST_NAME	lastname	X	
		name	-	Is a combination of the last and first name
Description/ Definition	AT_DESC	description	-	
E-mail address	AT_EMAIL_ADDR	email	X	
Telephone number	AT_PHONE_NUM	phone	-	
		clients	-	The **clients** field is determined by the client into which data is imported.
		substitutes	-	The **substitutes** field is only maintained manually.

*The **M** column specifies whether the attribute is a mandatory field.

4.2 Create policy definitions
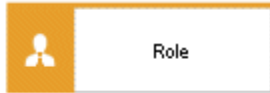
4.2.1 Business controls diagram model

You can model policy definitions in ARIS to simplify master data maintenance. The model **Business controls diagram** (MT_BUSY_CONTR_DGM) is intended for this.

4.2.1.1   Objects and relationships

The following objects can be used in the **Business controls diagram** model within the framework of policy management:

Object type name	Symbol type name	API name	Symbol	ARCM name
Policy	Business policy	OT_POLICY		Policy definition
Role	Role	OT_PERS_TYPE		Policy owner, Policy approver, Policy addressee, Policy auditor (depending on the role selected)
Risk	Risk	OT_RISK		Risk
Application system type	Application system type	OT_APPL_SYS_TYPE		Application system type
Organizational unit	Organizational unit	OT_ORG_UNIT		Organization
Technical term	Technical term	OT_TECH_TRM		Regulations

The following connections may be used:

Object	Connection	Object	Remark
Role	is technically responsible for	Policy	Assigns the user group to the policy definition.
Risk	is reduced by	Policy	Creates the connection between the policy and the risk.
Policy	affects	Organizational unit	Creates the connection between the policy and the affected organizational hierarchy element.
Policy	affects	Technical term	Creates the connection between the policy and the affected regulation hierarchy element.
Policy	affects	Application system type	Creates the connection between the policy and the affected application system type hierarchy element.

4.2.1.2   Attributes

The following allocations are applicable for the **Policy** object:

ABA attribute	API name	ARCM attribute	M*	Notes
Name	AT_NAME	name	X	Limited to 250 characters.
Description	AT_DESC	description		
Policy type	AT_POLICY_TYPE	policy_type	X	Two selection options: ▪ **Confirmation required** (the confirmation process is started after the policy is published) ▪ **Publish only** (the process ends after the policy is published)
Confirmation text	AT_CONFIRMATION_TEXT	confirmation_text	(X)	Only mandatory if **Confirmation required** was selected at policy type.
Confirmation duration in days	AT_CONFIRMATION_DURATION	duration	(X)	Only mandatory if **Confirmation required** was selected at policy type.
Start date of approval period (owner)	AT_START_DATE_APPROVAL_PERIOD_OWNER	startdate		Start of the approval period for the policy owner.
End date of approval period (owner)	AT_END_DATE_APPROVAL_PERIOD_OWNER	enddate	X	End of the approval period for the policy owner.

ABA attribute	API name	ARCM attribute	M*	Notes
Start date of approval period (approver)	AT_START_DATE_APPROVAL_PERIOD_APPROVER	approverstartdate	X	Start of the approval period for the policy approver. The approvals are generated for the approver.
End date of approval period (approver)	AT_END_DATE_APPROVAL_PERIOD_APPROVER	approverenddate	X	End of the approval period for the policy approver.
Start date of publishing period	AT_START_DATE_PUBLISHING_PERIOD	publishingstartdate		Start of the publishing period. If no start date is set the publishing period starts directly after approval by the policy owner.
End date of publishing period	AT_END_DATE_PUBLISHING_PERIOD	publishingenddate	X	End of the publishing period.
Export relevant	AT_AAM_EXPORT_RELEVANT	-		This attribute specifies whether an policy definition should be exported to ARIS Risk & Compliance Manager.
Title 1/Link 1 Title 2/Link 2 Title 3/Link 3 Title 4/Link 4	AT_TITL1/AT_EXT_1 AT_TITL2/AT_EXT_2 AT_TITL3/AT_EXT_3 AT_TITL4/AT_EXT_4	documents		

ABA attribute	API name	ARCM attribute	M*	Notes
ARIS Document Storage link 1 ARIS Document Storage link 2 ARIS Document Storage link 3 ARIS Document Storage link 4	AT_ADS_LINK_1 AT_ADS_LINK_2 AT_ADS_LINK_3 AT_ADS_LINK_4	documents		

*The **M** column specifies whether the attribute is a mandatory field.

Additional attributes (Review attribute group) for the Policy object from ARIS Architect 9.5

ABA attribute	API name	ARCM attribute	M*	Notes
Review-relevant	AT_REVIEW_RELEVANT	reviewRelevant	X	Marks the policy as review-relevant.

ABA attribute	API name	ARCM attribute	M*	Notes
Review activities	AT_REVIEW_ACTIVITY	activities	(X)	Describes the activities to be executed during the review. Becomes a mandatory field if the policy was marked as review-relevant.
Review frequency	AT_REVIEW_FREQUENCY	frequency	(X)	Outputs the interval at which the policy review is to be carried out. Available options are: - One-off - Daily - Weekly - Monthly - Quarterly - Semi-annually - Annually - Every second year - Event-driven Becomes a mandatory field if the policy was marked as review-relevant.
Event-driven review allowed	AT_EVENT_DRIVEN_REVIEW_ALLOWED	event_driven_ allowed	(X)	Outputs whether ad hoc reviews are allowed for policies. Becomes a mandatory field if the policy was marked as review-relevant.

ABA attribute	API name	ARCM attribute	M*	Notes
Time limit for the execution of the review in days	AT_REVIEW_EXECUTION_TIME_LIMIT	duration	(X)	Outputs the number of days that are available to the policy owner to process the review. The review duration is specified by the end date at which the review must be completed. Becomes a mandatory field if the policy was marked as review-relevant.
Start date of policy review	AT_START_DATE_OF_POLICY_REVIEWS	startdate	(X)	Outputs the date from which the first policy review is to be generated. Becomes a mandatory field if the policy was marked as review-relevant.
End date of policy review	AT_END_DATE_OF_POLICY_REVIEWS	enddate		Outputs the date up to which policy reviews are to be generated.
Length of control period	AT_AAM_TESTDEF_CTRL_PERIOD	control_period	(X)	Outputs the period to which the policy review relates. Becomes a mandatory field if the policy was marked as review-relevant.

*The **M** column specifies whether the attribute is a mandatory field.

4.2.2 Process models

To create a connection to the process hierarchy policies can be modeled in the following process models.

Model type number	Model name
12	Value-added chain diagram
13	EPC
14	Function allocation diagram
18	PCD
50	EPC (material flow)
51	PCD (material flow)
134	EPC (column display)
140	EPC (row display)
154	EPC (table display)
173	EPC (horizontal table display)

4.2.2.1 Objects, relationships and attributes

You can use the following objects in process models :

Object type name	Symbol type name	API name	Symbols	ARCM name
Function	(Depending on the process model)	OT_FUNC		Process
Policy	Business policy	OT_POLICY		Policy definition

The following connections may be used:

Object	Connection	Object	Remark
Policy	affects	Function	Creates the connection between the policy and the affected process hierarchy element.

4.2.3 Business rule architecture diagram

To model a hierarchy between policies, you can use the following connection from ARIS Architect 9.5 in the **Business rule architecture diagram** model.

Object	Connection	Object	Remark
Policy	encompasses	Policy	Represents a hierarchy between policies

4.3 Deactivation of objects and relationships

The objects and relationships in ARIS Risk & Compliance Manager are subject to versioning to ensure traceability of changes. Therefore, objects and relationships in ARIS Risk & Compliance Manager are deactivated and not deleted. This means that the corresponding data items are not removed from the database, but rather marked as deactivated.

To deactivate objects/relationships in ARIS Risk & Compliance Manager via an import you must mark them accordingly in ARIS Architect. To do so, you use the attribute **Deactivated** (AT_DEACT). The attribute can be set for both objects and connections. As soon as the attribute is set, the object or connection will be deactivated upon the next import.

Of course, this is only the case if the objects/relationships are included in the ARIS Architect export file. After the successful import into ARIS Risk & Compliance Manager you can delete the objects/connections in ARIS Architect. If objects/relationships were deleted in ARIS Architect before a deactivation import took place you can deactivate them manually in ARIS Risk & Compliance Manager.