![Software AG]

ARIS

GDPR CONVENTIONS FOR ARIS ACCELERATORS

VERSION 10.0 - SERVICE RELEASE 10

October 2019

Contents

1 Text conventions

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

- Menu items, key combinations, dialogs, file names, entries, etc. are displayed in **bold**.

- User-defined entries are shown as **<bold text in angle brackets>**.

- Example texts that are too long to fit on a single line, such as a long directory path, are wrapped to the next line by using ↵ at the end of the line.

- File extracts are shown in this font format:

  `This paragraph contains a file extract.`

- Warnings have a colored background:

Warning

This paragraph contains a warning.

2   Introduction

To simplify the creation of Data Protection Management information and functionality, as well as to facilitate their reusability, you can model objects in ARIS Architect. These objects are then used by the workflows of ARIS Risk & Compliance Manager. However, this is only possible if you adhere to the methodological and functional rules and conventions for modeling in ARIS Architect. Only then all modeled data can be transferred to ARIS Risk & Compliance Manager and reused there. To be able to properly maintain these objects in ARIS Architect, refer to the **ARCM – General conventions** manual and the respective convention manual for the workflows of ARIS Risk & Compliance Manager.

3   Content of document

The sections below explain the standards for the usage 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

3.2   Prerequisites

To be able to use the following conventions, first import the **GDPR method extension** filter into ARIS Architect. It adds derived and user-defined method constructs (model types, object types, symbols, connection types, attribute type groups, and attribute types) to the ARIS method. These method constructs are required for GDPR regulation. All other accelerators are based on this enhanced ARIS method.

To use the GDPR method extensions, use the **Entire method** filter or add the GDPR method extensions to any existing ARIS GRC filter. The GDPR method extension filter contains only additional enhancements for GDPR which are based on the GRC method. For detailed information on the GRC method, refer to the convention manuals delivered with ARIS Risk & Compliance Manager. For more information on installing ARIS Accelerators for GDPR, refer to the **ARIS accelerators for GDPR Installation Guide**.

4   ARIS conventions
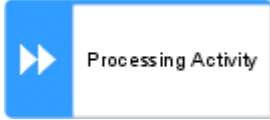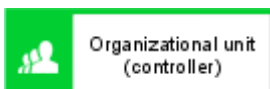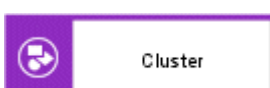
4.1   Create processing activities and relations

The core of the ARIS data privacy features relies on the identification of process functions (processing activities (page 14)), defined by the European General Data Protection Regulation (GDPR (page 14)). Use the **GDPR processing activity** attribute in ARIS to specify whether a process function is a processing activity (**true**) or not (**false**).

Processing activities and associated information are modeled in a **Processing activity description diagram** model (API name: b0205e20-4aa5-11e7-43b7-08002721906d) in ARIS Architect to simplify master data maintenance. This model type is derived from the **Function allocation diagram** model type.

4.1.1 Objects and relationships

You can use the following objects in the **Processing activity description diagram** model within the framework of Data Protection Management:

Object type name	API name	Symbol type name	Symbols	ARCM name
Function	OT_FUNC	Processing activity	Processing Activity	Process (hierarchy element)
Organizational unit	OT_ORG_UNIT	Organizational unit (processor)	Organizational unit (processor)	Organization processor (hierarchy element)
Organizational unit	OT_ORG_UNIT	Organizational unit (controller)	Organizational unit (controller)	Organization controller (hierarchy element)
Cluster/data model	OT_CLST	Cluster	Cluster	Data (hierarchy element)
Risk	OT_RISK	Risk	Risk	Risk
Application system type	OT_APPL_SYS_TYPE	Application system type	Application system type	Application system type (hierarchy element)

You can use the following the following connections:

Object	Connection/API name	Object
Organizational unit (controller)	is technically responsible for (CT_IS_TECH_RESP_1)	Processing activity
Organizational unit (processor)	carries out (CT_EXEC_1)	Processing activity
Risk	occurs at (CT_OCCUR)	Processing activity
Application system type	supports (CT_CAN_SUPP_1)	Processing activity
Processing activity	reads (CT_READ_1), has as output (CT_HAS_OUT)	Cluster

4.1.2 Attributes

4.1.2.1 Processing activities attributes

The following allocations are applicable for the **processing activity**:

ARIS attribute	API name	ARCM attribute	Notes
Name	AT_NAME	name	Mandatory field, limited to 250 characters.
Description	AT_DESC	description	Specifies the purpose of the processing activity.
GDPR processing activity	2b70adc0-4504-11e7-43b7-08002721906d	gdpr_processingActivity	User-defined - Specifies whether or not the function is a processing activity.
Data privacy score	695b1ad0-1df9-11e7-43b7-08002721906d	gdpr_process_privacyScore	User-defined - Specifies an estimated score on a predefined scale, in order to qualify the data privacy of the hierarchy element. Example: The score derived from the Processing Activity Qualification questionnaire.

ARIS attribute	API name	ARCM attribute	Notes
Data sensitivity	332790f0-1dfa-11e7-43b7-08002721906d	gdpr_process_dataSensitivity	User-defined - Indicates whether the data requires special handling. Options (default values): ▪ **Public data** ▪ **Sensitive** ▪ **Very sensitive** ▪ **Highly sensitive** ▪ **Extremely sensitive**
Sign-off relevant	AT_AAM_SIGN_OFF_RELEVANT	signoff	Mark the processing activity as relevant for sign-off. If not specified, the default value in ARIS Risk & Compliance Manager is false.

4.1.2.2 Cluster attributes

The following allocations are applicable for the **cluster**:

ARIS attribute	API name	ARCM attribute	Notes
Name	AT_NAME	name	Mandatory field, limited to 250 characters.
Description	AT_DESC	description	
Restriction level	15eaceb1-096b-11e7-2959-d4bed9888991	gdpr_restrictionLevel	User-defined - Specifies the level of legal usage of the data. Options (default values): ▪ **Unrestricted data** ▪ **Personal data** ▪ **Sensitive personal data** ▪ **Confidential data**
Data privacy score	695b1ad0-1df9-11e7-43b7-08002721906d	gdpr_privacyScore	User-defined - Specifies an estimated score on a predefined scale, in order to qualify the data privacy of the hierarchy element. Example: The score derived from any data element qualification questionnaire.

4.1.2.3   Organizational unit attributes

The following attribute allocations apply to the **Organizational unit** object:

ARIS attribute	API name	ARCM attribute	Notes
Name	AT_NAME	name	Mandatory field, limited to 250 characters.
Description	AT_DESC	description	
Data protection officer	1c2537a1-4072-11e7-43b7-08002721906d	gdpr_protOfficer	User-defined - Displays the name and address of the data protection officer. Must be included in the record of processing activities. Must be listed in the report.
Data protection representative	8f055dc1-407e-11e7-43b7-08002721906d	gdpr_protRepresentative	User-defined - Displays the name and address of the data protection representative. Must be included in the record of processing activities. Must be listed in the report.
Sign-off relevant	AT_AAM_SIGN_OFF_RELEVANT	signoff	Marks the organizational unit as relevant for sign-off. If not specified, the default value in ARIS Risk & Compliance Manager is false.

4.1.2.4 Application system types attributes

The following attribute allocations apply to the **application system type:**

ARIS attribute	API name	ARCM attribute	Notes
Name	AT_NAME	name	Mandatory field, limited to 250 characters.
Description	AT_DESC	description	
Data sensitivity	332790f0-1dfa-11e7-43b7-08002721906d	gdpr_dataSensitivity	User-defined - Indicates whether the data requires special handling. Options (default values): ▪ **Public data** ▪ **Sensitive** ▪ **Very sensitive** ▪ **Highly sensitive** ▪ **Extremely sensitive**
GDPR qualification score	badc1630-2014-11e7-43b7-08002721906d	gdpr_qualificationScore	User-defined - Indicates an estimated score on a predefined scale in order to qualify the hierarchy element. Example: A score derived from any application system qualification questionnaire.
GDPR risk relevance score	da6e5cb1-2014-11e7-43b7-08002721906d	gdpr_riskRelevanceScore	User-defined - Indicates an estimated score on a predefined scale in order to qualify the risk relevance of the hierarchy element. Example: The score derived from the GDPR risk assessment.

ARIS attribute	API name	ARCM attribute	Notes
Data privacy score	695b1ad0-1df9-11e7-43b7-08002721906d	gdpr_privacyScore	User-defined - Specifies an estimated score on a predefined scale, in order to qualify the data privacy of the hierarchy element. Example: The score derived from any application system qualification questionnaire.

4.2   Create processing activity/process hierarchy

To model a business cluster of processing activities, for example, departments or countries in which an organization is represented, use the **Record of processing activities** model (API name: c45962f1-4b87-11e7-43b7-08002721906d) derived from the **Value-added chain diagram** model. Any hierarchy between the processing activities can be represented by the **is process-oriented superior**/**is process-oriented subordinate** (CT_IS_PRCS_ORNT_SUPER) connection.

In ARIS Risk & Compliance Manager, only a tree structure for hierarchies is allowed. Therefore, each processing activity can only have one superior processing activity/function.

4.3   Create cluster/data hierarchy

To model a hierarchy between clusters, use the **IE Data model** or the **eERM** model. The hierarchy between clusters is represented by the **consists of**/**is part of** (CT_CONS_OF_2) connection as a direct connection between two clusters in the IE Data model or as an implicit connection built by assigning an eERM model to the cluster.

In ARIS Risk & Compliance Manager, only a tree structure for hierarchies is allowed. Therefore, each cluster can only have one superior cluster.

5 Glossary

GDPR

The **G**eneral **D**ata **P**rotection **R**egulation (GDPR) protects the rights of individuals' personal data within the European Union. It also regulates the export of personal data outside the EU. GDPR is a regulation by the European Parliament, the Council of the European Union, and the European Commission.

PROCESSING ACTIVITY

A processing activity is any operation which is performed on individuals' personal data, such as collection, recording, disclosure by transmission, and therefore is subject to the General Data Protection Regulation (GDPR (page 14)).

Processing activities and associated information are modeled in **Processing activity description diagram** models and **Record of processing activities** models in ARIS Architect. For detailed information, refer to the **ARIS Risk & Compliance Manager - Data Protection Management** guide.

SINGLE SIGN-ON (SSO)

With **SSO** or **single sign-on** the user only needs to authenticate himself once with his user name and password to access all services, programs and computers without logging in again.

If services, programs, and computers request a new authentication when accessed by the user the authentication is carried out by the underlying SSO mechanism.

6 Legal information

6.1 Documentation scope

The information provided describes the settings and features as they were at the time of publishing. Since documentation and software are subject to different production cycles, the description of settings and features may differ from actual settings and features. Information about discrepancies is provided in the Release Notes that accompany the product. Please read the Release Notes and take the information into account when installing, setting up, and using the product.

If you want to install technical and/or business system functions without using the consulting services provided by Software AG, you require extensive knowledge of the system to be installed, its intended purpose, the target systems, and their various dependencies. Due to the number of platforms and interdependent hardware and software configurations, we can describe only specific installations. It is not possible to document all settings and dependencies.

When you combine various technologies, please observe the manufacturers' instructions, particularly announcements concerning releases on their Internet pages. We cannot guarantee proper functioning and installation of approved third-party systems and do not support them. Always follow the instructions provided in the installation manuals of the relevant manufacturers. If you experience difficulties, please contact the relevant manufacturer.

If you need help installing third-party systems, contact your local Software AG sales organization. Please note that this type of manufacturer-specific or customer-specific customization is not covered by the standard Software AG software maintenance agreement and can be performed only on special request and agreement.

If a description refers to a specific ARIS product, the product is named. If this is not the case, names for ARIS products are used as follows:

Name	Includes
ARIS products	Refers to all products to which the license regulations of Software AG standard software apply.
ARIS Client	Refers to all programs that access shared databases by using ARIS Server.
ARIS Download Client	Refers to an ARIS Client that can be accessed using a browser.

6.2   Data protection

Software AG products provide functionality with respect to processing of personal data according to the EU General Data Protection Regulation (GDPR).

Where applicable, appropriate steps are documented in the respective administration documentation.

6.3   Disclaimer

ARIS products are intended and developed for use by persons. Automated processes, such as the generation of content and the import of objects/artifacts via interfaces, can lead to an outsized amount of data, and their execution may exceed processing capacities and physical limits. For example, processing capacities are exceeded if models and diagrams transcend the size of the modeling area or an extremely high number of processing operations is started simultaneously. Physical limits may be exceeded if the memory available is not sufficient for the execution of operations or the storage of data.

Proper operation of ARIS products requires the availability of a reliable and fast network connection. Networks with insufficient response time will reduce system performance and may cause timeouts.

If your product contains ARIS document storage, the following applies:

ARIS document storage was tested with 40.000 document items. This includes documents, document versions or folders. We recommend monitoring the number and overall size of stored document items and archiving some document items if needed.

If ARIS products are used in a virtual environment, sufficient resources must be available there in order to avoid the risk of overbooking.

The system was tested using scenarios that included 100,000 groups (folders), 100,000 users, and 1,000,000 modeling artifacts. It supports a modeling area of 25 square meters.

If projects or repositories are larger than the maximum size allowed, a powerful functionality is available to break them down into smaller, more manageable parts.

Some restrictions may apply regarding the use of process administration, ARIS Administration, ARIS document storage, and ARIS Process Board, and the generation of executable processes. Process Governance has been tested and approved for 1000 parallel process instances. However, the number may vary depending on process complexity, for example, if custom reports are integrated.

ARIS document storage was tested with 40.000 document items. This includes documents, document versions or folders. We recommend monitoring the number and overall size of stored document items and archiving some document items if needed.