



# **ARIS RISK & COMPLIANCE MANAGER**

## **PRÜFUNG DER SEMANTIK FÜR DEN DATENEXPORT**

VERSION 10.0 - SERVICE RELEASE 6

Oktober 2018

This document applies to ARIS Risk & Compliance Manager Version 10.0 and to all subsequent releases.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Copyright © 2010 - 2018 [Software AG](#), Darmstadt, Germany and/or Software AG USA Inc., Reston, VA, USA, and/or its subsidiaries and/or its affiliates and/or their licensors.

The name Software AG and all Software AG product names are either trademarks or registered trademarks of Software AG and/or Software AG USA Inc. and/or its subsidiaries and/or its affiliates and/or their licensors. Other company and product names mentioned herein may be trademarks of their respective owners.

Detailed information on trademarks and patents owned by Software AG and/or its subsidiaries is located at <http://softwareag.com/licenses>.

Use of this software is subject to adherence to Software AG's licensing conditions and terms. These terms are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

This software may include portions of third-party products. For third-party copyright notices, license terms, additional rights or restrictions, please refer to "License Texts, Copyright Notices and Disclaimers of Third Party Products". For certain specific third-party license restrictions, please refer to section E of the Legal Notices available under "License Terms and Conditions for Use of Software AG Products / Copyright and Trademark Notices of Software AG Products". These documents are part of the product documentation, located at <http://softwareag.com/licenses> and/or in the root installation directory of the licensed product(s).

## Inhalt

1	Textkonventionen.....	1
2	Einleitung.....	2
3	Vorgehen .....	3
3.1	Installation von Reporten zur Prüfung der Semantik .....	3
3.2	Reporte zur Prüfung der Semantik ausführen.....	3
3.2.1	Beispiel für einen Report ohne Fehlermeldungen.....	5
3.2.2	Beispiel für einen Report mit Fehlermeldungen.....	5
4	Wissenswertes .....	6
4.1	Welche zusätzlichen Komponenten benötigen Sie für die Reporte zur Prüfung der Semantik?.....	6
4.2	Welche Reporte zur Prüfung der Semantik gibt es und in welchem Kontext sind sie ausführbar? .....	7
4.3	Welcher Prüfinhalt ist für Auditvorlagen definiert?.....	7
4.4	Welcher Prüfinhalt ist für Kontrollen definiert?.....	9
4.5	Welcher Prüfinhalt ist für Hierarchiestrukturen definiert? .....	11
4.6	Welcher Prüfinhalt ist für Policy-Definitionen definiert?.....	12
4.7	Welcher Prüfinhalt ist für Fragebogenvorlagen definiert?.....	14
4.8	Welcher Prüfinhalt ist für Risiken definiert?.....	16
4.9	Welcher Prüfinhalt ist für Testdefinitionen definiert?.....	17
4.10	Welcher Prüfinhalt ist für Benutzergruppen definiert? .....	19
4.11	Welcher Prüfinhalt ist für Benutzer definiert? .....	19
5	Rechtliche Hinweise.....	20
5.1	Dokumentationsumfang.....	20
5.2	Datenschutz.....	21
5.3	Disclaimer .....	21
6	Index .....	i

# 1 Textkonventionen

Im Text werden Menüelemente, Dateinamen usw. folgendermaßen kenntlich gemacht:

- Menüelemente, Tastenkombinationen, Dialoge, Dateinamen, Eingaben usw. werden **fett** dargestellt.
- Eingaben, über deren Inhalt Sie entscheiden, werden **<fett und in spitzen Klammern>** dargestellt.
- Einzeilige Beispieltexthe werden am Zeilenende durch das Zeichen ↵ getrennt, z. B. ein langer Verzeichnispfad, der aus Platzgründen mehrere Zeilen umfasst.
- Dateiauszüge werden in folgendem Schriftformat dargestellt:

Dieser Absatz enthält einen Dateiauszug.

## 2 Einleitung

Bei der Modellierung in ARIS müssen bestimmte Konventionen eingehalten werden. Wurden die Konventionen nicht berücksichtigt, bricht der Import von Daten aus ARIS nach ARIS Risk & Compliance Manager ab. Mithilfe der Reporte zur Prüfung der Semantik können Sie vor dem Export der Daten prüfen, ob die Richtlinien eingehalten wurden. Sie können die Reporte einzeln ausführen oder per Makro automatisch alle vorhandenen Reporte nacheinander. Als Ergebnis wird ein Protokoll generiert, mithilfe dessen Sie die Modellierungsfehler korrigieren können, sodass ein erfolgreicher Import nach ARIS Risk & Compliance Manager gewährleistet ist. Eine detaillierte Beschreibung von der Konzeption über die Modellierung bis zum Export finden Sie in den Konventionenhandbüchern.

Die nachfolgenden Beschreibungen der Reporte zur Prüfung der Semantik beziehen sich auf die Standarddefinitionen der Konfigurationsdatei **ARCM-Semantics\_Properties.js** und der Reporte.

### RISIKOBASIERTE ODER KONTROLLBASIERTE MODELLIERUNG

Die Modellierung der Daten für ARIS Risk & Compliance Manager kann risikobasiert oder kontrollbasiert erfolgen. Beim risikobasierten Ansatz ist das Risiko das zentrale Objekt, beim kontrollbasierten Ansatz die Kontrolle. Die Entscheidung welcher Ansatz verwendet wird, muss zu Beginn eines Projektes bei der Modellierung in ARIS getroffen werden. Risiko- und kontrollbasierter Ansatz sind exklusiv, d. h. innerhalb einer Installation von ARIS Risk & Compliance Manager kann nur ein Ansatz verwendet werden.

## 3 Vorgehen

### 3.1 Installation von Reporten zur Prüfung der Semantik

Die ARIS Risk & Compliance Manager-Reporte zur Prüfung der Semantik sind standardmäßig in der Kategorie **ARIS Risk & Compliance Manager** verfügbar. Der Masterreport **Einhaltung der ARIS Risk & Compliance Manager-Modellierungskonventionen prüfen** führt alle einzelnen Reporte zur Prüfung der Semantik aus.

### 3.2 Reporte zur Prüfung der Semantik ausführen

Es gibt zwei Möglichkeiten die Reporte (Seite 7) zur Prüfung der Semantik durchzuführen. Sie können die einzelnen Reporte ausführen oder den Masterreport starten, der alle vorhandenen Reporte nacheinander ausführt.

#### EINZELNE REPORTE AUSFÜHREN

Indem Sie einzelne Reporte ausführen, können Sie gezielt einen Objekttyp auf Existenz und Gültigkeit der Pflicht-Attribute prüfen, sowie auf Vorhandensein der erforderlichen Objektbeziehungen.

#### Voraussetzung

- Sie benötigen das Zugriffsrecht **Lesen** für die Gruppen, in denen die Datenbankelemente gespeichert werden.
- Die Elemente wurden gespeichert.
- Sie können auf dieses Skript zugreifen. Der Zugriff auf Skripte kann auf bestimmte Benutzergruppen beschränkt sein.

### Vorgehen

1. Starten Sie ARIS Architect.
2. Klicken Sie auf **ARIS >  Explorer**. Die Registerkarte **Explorer** wird geöffnet.
3. Klicken Sie in der Leistenanzeige auf  **Navigation**, wenn die Leiste **Navigation** noch nicht aktiviert ist.
4. Klicken Sie mit der rechten Maustaste auf das gewünschte Objekt, Modell bzw. die gewünschte Gruppe.
5. Klicken Sie auf **Auswerten > Report starten**. Der **Report-Assistent** wird geöffnet.
6. Wählen Sie die gewünschte **ARIS Risk & Compliance Manager**-Kategorie und den entsprechenden Report zur Prüfung der Semantik (**Semantik [...] prüfen**).
7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Ausgabeeinstellungen.
9. Klicken Sie auf **Fertigstellen**.
10. Wählen Sie den Modellierungsansatz.
11. Klicken Sie auf **OK**.

Der Report wird gestartet. Als Ergebnis wird ein Report als Text-Datei ausgegeben.

### ALLE VORHANDENEN REPORTE AUSFÜHREN

Durch das Starten des Reports **Einhaltung der ARIS Risk & Compliance Manager-Modellierungskonventionen prüfen** werden alle vorhandenen Reporte in der hinterlegten Reihenfolge abgearbeitet.

### Vorgehen

1. Starten Sie ARIS Architect.
2. Klicken Sie auf **ARIS >  Explorer**. Die Registerkarte **Explorer** wird geöffnet.
3. Klicken Sie in der Leistenanzeige auf  **Navigation**, wenn die Leiste **Navigation** noch nicht aktiviert ist.
4. Klicken Sie mit der rechten Maustaste auf die gewünschte Gruppe bzw. Datenbank.
5. Klicken Sie auf **Auswerten > Report starten**. Der **Report-Assistent** wird geöffnet.
6. Wählen Sie die gewünschte **ARIS Risk & Compliance Manager**-Kategorie und den Report **Einhaltung der ARIS Risk & Compliance Manager-Modellierungskonventionen prüfen**.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Ausgabeeinstellungen.
9. Klicken Sie auf **Fertigstellen**.
10. Wählen Sie den Modellierungsansatz.
11. Klicken Sie auf **OK**.

Alle vorhandenen Reporte werden gestartet. Als Ergebnis wird ein Sammelbericht über die Ergebnisse aller Einzelreporte als Text-Datei ausgegeben.

### 3.2.1 Beispiel für einen Report ohne Fehlermeldungen

```
*****  
Fehlerreport der Prüfung der Semantik für Testdefinitionen  
*****
```

Keine Fehler gefunden.

### 3.2.2 Beispiel für einen Report mit Fehlermeldungen

```
*****  
Fehlerreport der Prüfung der Semantik für Hierarchiestrukturen  
*****
```

Hierarchiestruktur der "Regularien" geprüft. Enthält Fehler!

Pflichtattribut(e) nicht definiert!!

```
Fachbegriff - (Unbenannt)  
  Pflichtattribut(e) nicht definiert: AT_NAME  
  Pflichtattribut(e) nicht definiert: AT_AAM_SIGN_OFF_RELEVANT
```

```
Vorhanden in:  
  Gruppe: 1.5 Regularien  
  Modell: Hierarchie Regularien
```

Mehrere Vater-Knoten gefunden!

```
Fachbegriff - (Unbenannt)  
Vorhanden in:  
  Gruppe: 1.5 Regularien  
  Modell: Hierarchie Regularien  
    Vater 1: Fachbegriff  
    Vater 2: Regularien
```



## 4 Wissenswertes

In diesem Abschnitt finden Sie Hintergrundinformationen zu den erläuterten Vorgehensweisen.

### 4.1 Welche zusätzlichen Komponenten benötigen Sie für die Reporte zur Prüfung der Semantik?

Die Logik der Prüfung der Semantik (Seite 3) ist in vier Komponenten aufgeteilt.

#### DIE REPORTE FÜR DIE DURCHFÜHRUNG DER JEWEILIGEN PRÜFUNG

- **Semantik der Hierarchiestrukturen prüfen**
- **Semantik der Risiken prüfen**
- **Semantik der Kontrollen prüfen**
- **Semantik der Testdefinitionen prüfen**
- **Semantik der Benutzer prüfen**
- **Semantik der Benutzergruppen prüfen**
- **Semantik der Fragebogenvorlagen prüfen**
- **Semantik der Auditvorlagen prüfen**

#### DIE JAVASCRIPT DATEIEN FÜR DIE BEREITSTELLUNG DER BASISFUNKTIONALITÄT DER REPORTE

- **arcm-common.js** (Abschnitt **Gemeinsame Dateien**)
- **arcm-mapping.js** (Abschnitt **Gemeinsame Dateien**)
- **aris2arcm-mapping.xml** (Abschnitt **Gemeinsame Dateien**)
- **ARCM-Semantics\_BaseDataFunctions.js**
- **ARCM-Semantics\_BaseReportAndOutputFunctions.js**

#### DIE JAVASCRIPT DATEI FÜR DIE KONFIGURATION DER PRÜFUNGEN

- **ARCM-Semantics\_Properties.js**

#### DER MASTERREPORT FÜR DIE AUSFÜHRUNG ALLER VORHANDENEN REPORTE IN EINEM SCHRITT

Der Report **Einhaltung der ARIS Risk & Compliance**

**Manager-Modellierungskonventionen prüfen** führt alle zugeordneten Reporte aus, bündelt die Ergebnisse und gibt diese aus.

## 4.2 Welche Reporte zur Prüfung der Semantik gibt es und in welchem Kontext sind sie ausführbar?

Sie können die Reporte zur Prüfung der Semantik folgendermaßen ausführen:

Report	Kontext
<b>Semantik der Hierarchiestrukturen prüfen</b>	Gruppe
<b>Semantik der Risiken prüfen</b>	Gruppe
<b>Semantik der Kontrollen prüfen</b>	Gruppe
<b>Semantik der Testdefinitionen prüfen</b>	Gruppe
<b>Semantik der Benutzergruppen prüfen</b>	Gruppe
<b>Semantik der Benutzer prüfen</b>	Gruppe
<b>Semantik der Fragebogenvorlagen prüfen</b>	Gruppe
<b>Semantik der Befragungs-Tasks prüfen</b>	Gruppe
<b>Semantik der Auditvorlagen prüfen</b>	Gruppe
<b>Semantik der Policys prüfen</b>	Gruppe

Makro	Kontext
<b>Einhaltung der ARIS Risk &amp; Compliance Manager-Modellierungskonventionen prüfen</b>	Datenbank, Gruppe

## 4.3 Welcher Prüfinhalt ist für Auditvorlagen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### **Semantik der Auditvorlagen prüfen**

### PRÜFINHALT

Geprüft wird, ob:

- das Attribut **ARCM-Synchronisation** gepflegt ist. Es werden nur Auditvorlagen berücksichtigt, bei denen dieses Attribut aktiviert ist.
- ein Audit jeweils mit genau einer Audit-Owner-Gruppe und genau einer Audit-Reviewer-Gruppe sowie höchstens einer Audit-Auditor-Gruppe verbunden ist.
- ein Auditschritt mit genau einer Auditschritt-Owner-Gruppe verbunden ist.

- höchstens eine Kante vom Typ **ist im Scope von** an einem Hierarchietyp im Modell vorhanden ist.
- ein Auditschritt mit genau einem übergeordneten Auditschritt oder genau einem Audit mit der Kante vom Typ **gehört zu** verbunden ist, um eine eindeutige Baumstruktur zu gewährleisten.
- eine Auditvorlage bzw. Auditschrittvorlage in einem Modell nur einmal vorhanden bzw. ausgeprägt ist.
- das Startdatum der Vorbereitung des Audits vor oder gleich dem Startdatum des Auditzeitraums ist.
- der Auditschrittzeitraum innerhalb dem Auditzeitraum liegt, bzw. ob Start- und Enddatum von Auditschrittzeitraum und Auditzeitraum identisch sind, wobei das Enddatum des Auditzeitraums unter Berücksichtigung des für das Attribut **Freies Wochenende** gepflegten Wertes aus dem Startdatum und der Höchstgesamtzeit errechnet wird.
- die Pflichtattribute für die folgenden Objekte gepflegt sind:
  - **Auditvorlage:**
    - **Name**
    - **Startdatum**
    - **Höchstgesamtzeit**
    - **Beginn der Vorbereitung des Audits**
    - **Startdatum des Kontrollzeitraums**
    - **Enddatum des Kontrollzeitraums**
  - **Auditschrittvorlage:**
    - **Name**
    - **Startdatum**
    - **Höchstgesamtzeit**
    - **Gewünschte Bearbeitungszeit**
- für die Definition des Umfangs (Scope) einer Auditvorlage/Auditschrittvorlage Hierarchietypen, Risikokategorie, Anwendungssystemtyp, Funktion (Prozess), Organisationseinheit oder Fachbegriff im Aufgabenzuordnungsdiagramm mit Hilfe der Kante **ist im Scope von** verbunden sind.
- der Wert der Höchstgesamtzeit und der gewünschten Bearbeitungszeit nicht 0000:00:00:00 ist.
- der Wert der gewünschten Bearbeitungszeit nicht größer ist als der Wert der Höchstgesamtzeit.

## 4.4 Welcher Prüfinhalt ist für Kontrollen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### Semantik der Kontrollen prüfen

### PRÜFINHALT

#### RISIKOBASIERTE MODELLIERUNG

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Name**
- die Kontrolle innerhalb des modellierten Business Controls Diagrams eindeutig ist.
- eine Kontrolle in höchstens einem Business Controls Diagram ausgeprägt ist.
- die Kontrollen jeweils mit exakt einem Risiko verbunden sind, bei dem das Attribut **ARCM-Synchronisation** gesetzt ist (gilt nicht, wenn die Prüfung auf einem Risikodiagramm gestartet wurde, für das das Attribut **ARCM-Synchronisation** gesetzt wurde).
- die Kontrollen jeweils mit maximal einer Kontroll-Manager-Gruppe verbunden sind.

#### KONTROLLBASIERTE MODELLIERUNG

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Name**
- die Kontrolle innerhalb des modellierten Business Controls Diagrams eindeutig ist.
- eine Kontrolle in höchstens einem Business Controls Diagram ausgeprägt ist.
- das Attribut **ARCM-Synchronisation** gepflegt ist. Es werden nur Kontrollen berücksichtigt, bei denen dieses Attribut aktiviert ist.
- die Kontrollen jeweils mit maximal einer Kontroll-Manager-Gruppe verbunden sind.
- die Kontrollen jeweils mit maximal einer Funktion verbunden sind. Zur Generierung der Prozesshierarchie eine Baumstruktur benötigt, keine Netzstruktur.

## RISIKO- UND KONTROLLBASIERTE MODELLIERUNG

Geprüft wird, ob ein Kontrollausführungs-Task mit der Kontrolle verbunden ist. Falls ja, wird geprüft, ob:

- die Pflichtattribute gepflegt sind:
  - **Name** und
  - **Kontrolldokumentations-Frequenz** und
  - **Frist zur Dokumentation der Kontrollausführung in Tagen** und
  - **Startdatum** und
  - **Länge des dokumentierten Zeitraums**
- ein Kontrollausführungs-Task jeweils mit exakt einer Organisationseinheit verbunden ist.
- ein Kontrollausführungs-Task jeweils mit exakt einer Gruppen verbunden ist (es muss genau eine Kontrollausführungs-Owner-Gruppe geben).
- das Attribut **Ereignisgesteuerte Kontrolldokumentation erlaubt** auf **true** gesetzt ist, wenn für die Kontrolldokumentations-Frequenz der Wert **Ereignisgesteuert** festgelegt ist.
- das Startdatum vor dem Enddatum liegt.
- das Kontrollausführungs-Task innerhalb des modellierten Business Controls Diagrams eindeutig ist.
- ein Kontrollausführungs-Task genau eine zugeordnete Kontrolle hat. Eine Kontrolle kann mehrere Kontrollausführungs-Tasks haben, aber ein Kontrollausführungs-Task immer nur genau eine Kontrolle.
- ein Kontrollausführungs-Task in höchstens einem Business Controls Diagram ausgeprägt ist.

## 4.5 Welcher Prüfinhalt ist für Hierarchiestrukturen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### **Semantik der Hierarchiestrukturen prüfen**

### KONTEXT

Gemäß der Standarddefinition werden die Hierarchiestrukturen mit folgenden Modellen für die Prüfung herangezogen:

### PROZESS

#### **EPK, Wertschöpfungskettendiagramm und Funktionszuordnungsdiagramm**

### ORGANISATIONSEINHEIT

- **Organigramm**

### REGULARIEN

- **Fachbegriffsmodell**

#### **Besonderheit für Regulatory-Change-Management**

Geprüft wird, ob:

- das Attribut **Review-relevant** gewählt ist. Falls ja, werden die folgenden Pflichtattribute und Bedingungen geprüft:
  - **Review-Frequenz**
  - **Frist zur Durchführung des Reviews in Tagen**
  - **Startdatum des Reviews**
  - Der Fachbegriff jeweils mit genau einer Hierarchie-Owner-Gruppe verbunden sein.

### TESTER

Für die Testerhierarchie können keine Modelle festgelegt werden. Es werden die gleichen Modelle herangezogen, die für die Organisationseinheit festgelegt wurden.

### ANWENDUNGSSYSTEMTYP

- **Anwendungssystemtypdiagramm**

## RISIKOKATEGORIE

- **Risikodiagramm**

## PRÜFINHALT

Geprüft wird, ob:

- die Pflichtattribute für alle Hierarchiestrukturen gepflegt sind:
  - **Name**
- jedes Element der Hierarchie maximal einen Vater-Knoten hat.
- ein Hierarchieelement jeweils mit höchstens einer Sign-off-Owner-Gruppe verbunden ist (für Anwendungssystemtyp- und Risikokategoriehierarchie nicht relevant)

Zum Aufbau der Hierarchie in ARIS Risk & Compliance Manager sind nur Baumstrukturen zulässig, keine Netzstrukturen.

## BESONDERHEIT FÜR DIE RISIKOBASIERTE MODELLIERUNG

- Geprüft wird, ob bei den zugeordneten Risiken das Attribut **ARCM-Synchronisation** gepflegt ist. Bei den Prozessen werden nur Objekte berücksichtigt, denen ein Risiko zugeordnet ist, für das das Attribut **ARCM-Synchronisation** gesetzt ist.
- Geprüft wird, ob es Überschneidungen zwischen der Testerhierarchie und der Organisationshierarchie gibt. Eine Organisationseinheit darf nicht gleichzeitig der Tester- und der Organisationshierarchie angehören.

## BESONDERHEIT FÜR DIE KONTROLLBASIERTE MODELLIERUNG

Geprüft wird, ob bei den zugeordneten Kontrollen das Attribut **ARCM-Synchronisation** gepflegt ist. Bei den Prozessen werden nur Objekte berücksichtigt, denen eine Kontrolle zugeordnet ist, für die das Attribut **ARCM-Synchronisation** gesetzt ist.

## 4.6 Welcher Prüfinhalt ist für Policy-Definitionen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

## REPORTNAME

### Semantik der Policys prüfen

(Der Objekttypname lautet **Policy** in ARIS und **Policy-Definition** in ARIS Risk & Compliance Manager)

## PRÜFINHALT

Geprüft wird, ob:

- das Attribut **ARCM-Synchronisation** gepflegt ist. Es werden nur Policy-Definitionen berücksichtigt, bei denen dieses Attribut aktiviert ist.
- eine Policy-Definition jeweils mit genau einer Policy-Owner-Gruppe verbunden ist.
- eine Policy-Definition jeweils mit höchstens einer Policy-Auditor-Gruppe verbunden ist.
- mindestens eine Policy-Addressee-Gruppe verbunden ist, falls die Policy vom Typ **Bestätigung erforderlich** ist.
- das Startdatum der Veröffentlichung nach dem Startdatum des Freigabezeitraums (Owner) liegt.
- das Enddatum des Veröffentlichungszeitraums nach dem Startdatum des Veröffentlichungszeitraums liegt.
- das Enddatum des Freigabezeitraums (Owner) nach dem Startdatum des Freigabezeitraums (Owner) liegt.
- das Enddatum des Freigabezeitraums (Approver) nach dem Startdatum des Freigabezeitraums (Approver) liegt.
- der Freigabezeitraum der Approver komplett innerhalb des Freigabezeitraums der Owner liegt.
- die Pflichtattribute für die folgenden Objekte gepflegt sind:
  - **Policy-Definition:**
    - **Name**
    - **Policy-Typ**
    - **Startdatum des Freigabezeitraums (Owner)**
    - **Enddatum des Freigabezeitraums (Owner)**
    - **Enddatum des Veröffentlichungszeitraums**
    - **Startdatum des Freigabezeitraums (Approver)**
    - **Enddatum des Freigabezeitraums (Owner)**
    - **Bestätigungsdauer**, falls die Policy vom Typ **Bestätigung erforderlich** ist
  - **Policy-Prüfungs-Task:**
    - **Review-Frequenz**, falls die Policy als Review-relevant gekennzeichnet wurde.
    - **Ereignisgesteuerte Reviews erlaubt**, falls die Policy als Review-relevant gekennzeichnet wurde.
    - **Frist zur Durchführung in Tagen**, falls die Policy als Review-relevant gekennzeichnet wurde.
    - **Review-Frequenz**, falls die Policy als Review-relevant gekennzeichnet wurde.



## 4.7 Welcher Prüfinhalt ist für Fragebogensvorlagen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### Semantik der Fragebogensvorlagen prüfen

### PRÜFINHALT

Geprüft wird, ob:

- das Attribut **ARCM-Synchronisation** gepflegt ist. Es werden nur Fragebogensvorlagen berücksichtigt, bei denen dieses Attribut aktiviert ist.
- die Pflichtattribute für die folgenden Objekte gepflegt sind:
  - **Fragebogensvorlage:**
    - **Name**
  - **Kapitel:**
    - **Name**
  - **Frage:**
    - **Fragetext** und
    - **Fragetyp:**
      - **Einzelauswahl** oder
      - **Mehrfachauswahl** oder
      - **Text** oder
      - **Numerisch (Ganzzahl)** oder
      - **Numerisch (Fließkommazahl)** oder
      - **Datum** oder
      - **Datumsbereich**

Ist der Fragetyp **Einzelauswahl** oder **Mehrfachauswahl**, müssen entweder ein Antwort-Set oder mindestens eine mögliche Antwort zugeordnet werden (Pflichtfelder).

Haben Sie den Fragetyp **Text**, **Numerisch**, **Datum** oder **Datumsbereich** gewählt, wird das Feld **Bewertung der Antwort durch Befragungs-Reviewer** zum Pflichtfeld. Ist das Attribut **Bewertung der Antwort durch Befragungs-Reviewer** auf **Ja** gesetzt, müssen entweder ein Antwort-Set oder eine mögliche Antwort zugeordnet werden (Pflichtfelder).

Einer Frage können mehrere mögliche Antworten zugeordnet sein oder ein Antwort-Set. Sie können nicht gleichzeitig mögliche Antworten und ein Antwort-Set zuordnen. Die jeweilige Zuordnung muss erst entfernt werden, bevor eine andere hinzugefügt werden kann.

- **Antwort-Set:**
  - **Name**
- **Mögliche Antwort:**
  - **Antwort**
- eine Frage in einem Kapitel nur einmal vorkommt. Es ist jedoch möglich eine Frage in unterschiedlichen Kapiteln zu verwenden.
- einem Antwort-Set immer mindestens eine mögliche Antwort zugeordnet ist.
- alle verbundenen Befragungs-Tasks mit mindestens einer Befragtengruppe und genau einer Befragungs-Reviewer-Gruppe verbunden sind.
- alle verbundenen Befragungs-Tasks mit maximal einer Befragungs-Manager-Gruppe (die Zuordnung ist kein Pflichtfeld) verbunden sind.
- die Pflichtattribute für diese Tasks gepflegt sind:
  - **Frequenz**
  - **Startdatum**
  - **Frist zur Durchführung in Tagen**

## 4.8 Welcher Prüfinhalt ist für Risiken definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### Semantik der Risiken prüfen

### PRÜFINHALT

#### RISIKOBASIERTE MODELLIERUNG

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Name**
- das Attribut **ARCM-Synchronisation** gepflegt ist. Es werden nur Risiken berücksichtigt, bei denen dieses Attribut aktiviert ist.
- ein Risiko jeweils mit höchstens einer Risiko-Manager-Gruppe verbunden ist.
- die Risiken innerhalb der modellierten Business Controls Diagrams eindeutig sind. Ein Risiko kann mehrere Kontrollen haben, aber eine Kontrolle immer nur ein Risiko.
- ein Risiko in höchstens einem Business Controls Diagramm ausgeprägt ist.
- die Risiken jeweils mit maximal einer Funktion verbunden sind. Zur Generierung der Prozesshierarchie wird eine Baumstruktur benötigt, keine Netzstruktur.
- das Attribut **Risiko-Management-relevant** gewählt ist. Falls ja, werden die folgenden Pflichtattribute und Bedingungen geprüft:
  - **Bewertungsfrequenz**
  - **Frist zur Durchführung in Tagen**
  - **Startdatum der Risikobewertungen**
- dem Risiko genau eine Risiko-Owner-Gruppe und eine Risiko-Reviewer-Gruppe zugeordnet ist.

## KONTROLLBASIERTE MODELLIERUNG

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Name**
- jedes Risiko mit mindestens einer Kontrolle verbunden ist, bei der das Attribut **ARCM-Synchronisation** gepflegt ist.
- ein Risiko jeweils mit höchstens einer Risiko-Manager-Gruppe verbunden ist.
- ein Risiko in höchstens einem Business Controls Diagramm ausgeprägt ist.
- das Attribut **Risiko-Management-relevant** gewählt ist. Falls ja, werden die folgenden Pflichtattribute und Bedingungen geprüft:
  - **Bewertungsfrequenz**
  - **Frist zur Durchführung in Tagen**
  - **Startdatum der Risikobewertungen**
- dem Risiko genau eine Risiko-Owner-Gruppe und eine Risiko-Reviewer-Gruppe zugeordnet ist.
- dem Risiko maximal einer Funktion zugeordnet ist.

## 4.9 Welcher Prüfinhalt ist für Testdefinitionen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### **Semantik der Testdefinitionen prüfen**

## PRÜFINHALT

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Name**
  - **Testtyp:**
    - **Test des Designs** und/oder
    - **Test der Effektivität** und
  - **Testfrequenz** und
  - **Frist zur Durchführung in Tagen** (der Wert muss zwischen 1 und 365 liegen) und
  - **Startdatum der Testdefinition** und
  - **Länge des Kontrollzeitraums.**
- die Testdefinitionen innerhalb des modellierten Business Controls Diagrams eindeutig sind.
- eine Testdefinition in höchstens einem Business Controls Diagram ausgeprägt ist.
- die Testdefinitionen jeweils mit exakt einer Testergruppe und einer Reviewergruppe verbunden sind und ob jedes Gruppenmitglied nur einer der beiden Gruppen zugeordnet ist.
- die Testdefinitionen jeweils mit maximal einer Test-Manager-Gruppe (die Gruppenzuordnung ist kein Pflichtfeld) verbunden sind.
- die Testdefinitionen jeweils mit exakt einer Organisationseinheit verbunden sind. Eine Zuordnung zur Organisationshierarchie ist in ARIS Risk & Compliance Manager vorgeschrieben.
- die Testergruppe, die mit der Testdefinition verbunden ist auch mit genau einem Element der Testerhierarchie verbunden ist.
- das Attribut **Ereignisgesteuerte Testfälle erlaubt** auf **true** gesetzt ist, wenn für die Testfrequenz der Wert **Ereignisgesteuert** festgelegt ist.

## BESONDERHEIT FÜR DIE RISIKOBASIERTE MODELLIERUNG

Geprüft wird, ob:

- eine Testdefinition mit exakt einer Kontrolle verbunden ist, die mit einem Risiko verbunden ist, bei dem das Attribut **ARCM-Synchronisation** gepflegt ist.

## BESONDERHEIT FÜR DIE KONTROLLBASIERTE MODELLIERUNG

Geprüft wird, ob:

- eine Testdefinition mit exakt einer Kontrolle verbunden ist, bei der das Attribut **ARCM-Synchronisation** gepflegt ist.

## 4.10 Welcher Prüfinhalt ist für Benutzergruppen definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### Semantik der Benutzergruppen prüfen

### PRÜFINHALT

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Name**
- ein Objekt vom Typ **Rolle** mit mehr als einem Objekt vom Typ **Rolle** verbunden ist. Eine Gruppe kann immer nur genau eine Rolle in ARIS Risk & Compliance Manager haben. Es erfolgt keine Prüfung, ob eine Gruppe mit exakt einer Rolle verbunden ist oder ob eine Benutzergruppe mit der Rolle **Tester** mit exakt einem Hierarchieelement vom Typ **Tester** verbunden ist.

## 4.11 Welcher Prüfinhalt ist für Benutzer definiert?

Diese Beschreibung bezieht sich auf die Standarddefinition der Konfigurationsdatei und der Reporte.

### REPORTNAME

#### Semantik der Benutzer prüfen

### PRÜFINHALT

Geprüft wird, ob:

- die Pflichtattribute gepflegt sind:
  - **Anmeldung** und
  - **Vorname** und
  - **Nachname** und
  - **E-Mail-Adresse**
- die Benutzer-ID nur aus alphanumerischen Zeichen und Punkt (.), Bindestrich (-) oder Unterstrich (\_) besteht.

## 5 Rechtliche Hinweise

### 5.1 Dokumentationsumfang

Die zur Verfügung gestellten Informationen beschreiben die Einstellungen und Funktionalitäten, die zum Zeitpunkt der Veröffentlichung gültig waren. Da Software und Dokumentation verschiedenen Fertigungszyklen unterliegen, kann die Beschreibung von Einstellungen und Funktionalitäten von den tatsächlichen Gegebenheiten abweichen. Informationen über solche Abweichungen finden Sie in den mitgelieferten Release Notes. Bitte lesen und berücksichtigen Sie diese Datei bei Installation, Einrichtung und Verwendung des Produkts.

Wenn Sie das System technisch und/oder fachlich ohne Service-Leistung der Software AG installieren möchten, benötigen Sie umfangreiche Kenntnisse hinsichtlich des zu installierenden Systems, der Zielthematik sowie der Zielsysteme und ihren Abhängigkeiten untereinander. Aufgrund der Vielzahl von Plattformen und sich gegenseitig beeinflussender Hardware- und Softwarekonfigurationen können nur spezifische Installationen beschrieben werden. Es ist nicht möglich, sämtliche Einstellungen und Abhängigkeiten zu dokumentieren.

Beachten Sie bitte gerade bei der Kombination verschiedener Technologien die Hinweise der jeweiligen Hersteller, insbesondere auch aktuelle Verlautbarungen auf deren Internet-Seiten bezüglich Freigaben. Für die Installation und einwandfreie Funktion freigegebener Fremdsysteme können wir keine Gewähr übernehmen und leisten daher keinen Support. Richten Sie sich grundsätzlich nach den Angaben der Installationsanleitungen und Handbücher der jeweiligen Hersteller. Bei Problemen wenden Sie sich bitte an die jeweilige Herstellerfirma.

Falls Sie bei der Installation von Fremdsystemen Hilfe benötigen, wenden Sie sich an Ihre lokale Software AG-Vertriebsorganisation. Beachten Sie bitte, dass solche Hersteller- oder kundenspezifischen Anpassungen nicht dem Standard-Softwarepflege- und Wartungsvertrag der Software AG unterliegen und nur nach gesonderter Anfrage und Abstimmung erfolgen.

Bezieht sich eine Beschreibung auf ein spezifisches ARIS-Produkt, wird dieses genannt. Andernfalls werden die Bezeichnungen für die ARIS-Produkte folgendermaßen verwendet:

Name	Umfasst
ARIS-Produkte	Bezeichnet sämtliche Produkte, für die die Lizenzbedingungen der Software AG-Standard-Software gelten.
ARIS-Clients	Bezeichnet alle Programme, z. B. ARIS Architect, ARIS Designer, die über ARIS Server auf gemeinsam verwendete Datenbanken zugreifen.
ARIS-Download-Clients	Bezeichnet ARIS-Clients, die aus dem Browser gestartet werden können.

## 5.2 Datenschutz

Die Produkte der Software AG stellen Funktionalität zur Verfügung, die für die Verarbeitung persönlicher Daten entsprechend der EU-Datenschutz-Grundverordnung (DSGVO) genutzt werden kann.

Die Beschreibungen zur Nutzung dieser Funktionalität finden Sie in der Administrationsdokumentation des jeweiligen Produkts.

## 5.3 Disclaimer

ARIS-Produkte sind für die Verwendung durch Personen gedacht und entwickelt. Automatische Prozesse wie das Generieren von Inhalt und der Import von Objekten/Artefakten per Schnittstellen können zu einer immensen Datenmenge führen, deren Verarbeitung wiederum Verarbeitungskapazitäten und physische Grenzen überschreiten können. Physikalische Grenzen können dann überschritten werden, wenn der verfügbare Speicherplatz für die Ausführung der Operationen oder die Speicherung der Daten nicht ausreicht.

Der ordnungsgemäße Betrieb von ARIS Risk & Compliance Manager setzt voraus, dass eine zuverlässige und schnelle Netzwerkverbindung vorhanden ist. Ein Netzwerk mit unzureichender Antwortzeit reduziert die Systemperformanz und kann zu Timeouts führen.

Wenn ARIS-Produkte in einer virtuellen Umgebung genutzt werden, müssen ausreichende Ressourcen verfügbar sein, um das Risiko einer Überbuchung zu vermeiden.

Das System wurde im Szenario **Internal control system** mit 400 gleichzeitig angemeldeten Benutzern getestet. Es enthält 2.000.000 Objekte. Um eine ausreichende Performance zu gewährleisten, empfehlen wir mit nicht mehr als 500 parallel angemeldeten Benutzern zu arbeiten. Kundenspezifische Anpassungen, vor allem in Listen und Filtern, wirken sich negativ auf die Performance aus.



## 6 Index

### A

#### ARIS Risk & Compliance Manager-Reporte

- Auditvorlagen • 7
- Beispiel mit Fehlermeldung • 5
- Beispiel ohne Fehlermeldung • 5
- Benutzer • 19
- Benutzergruppen • 19
- Fragebogenvorlagen • 14
- Hierarchiestrukturen • 11
- Kontrollen • 9
- Policy-Definitionen • 12
- Risiken • 16
- Testdefinitionen • 17

Ausführung • 3

### E

Einführung • 2

### I

Installation • 3

### K

Komponenten • 6

Kontext • 7