ARIS Risk & Compliance Manager

KONVENTIONEN RISIKOBASIERTES TEST- UND SIGN-OFF-MANAGEMENT

Version 10.0 - Service Release 5

Juli 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.

Inhalt

1 Einführung

Die modellhafte Dokumentation von Geschäftsprozessen und Funktionen in ARIS bringt eine Reihe von Vorteilen mit sich (Einheitlichkeit, Komplexitätsreduzierung, Wiederverwendbarkeit, Auswertbarkeit, Integrität usw.).

Dies ist nur möglich, wenn die methodischen und funktionalen Regeln sowie Konventionen bei der Modellierung in ARIS Architect eingehalten werden. Nur dann können alle modellierten Daten auch in ARIS Risk & Compliance Manager überführt und weiterverwendet werden.

2 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 Beispieltexte 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.`

3 Inhalt des Dokuments

In den folgenden Kapiteln werden die Standards bezüglich der Verwendung von Beschreibungssichten, Modelltypen, Objekttypen, Beziehungs- bzw. Kantentypen sowie Attributen erläutert.

3.1 Zielsetzung und Abgrenzung

Ziel: Festlegung von Modellierungsrichtlinien

Nicht Inhalt dieses Handbuchs: Anwenderdokumentation

4 ARIS-Konventionen

4.1 Modellierungsebenen und Modelltypen

4.1.1 Übersicht über die Modellierungsebenen und deren Modelltypen

In der nachfolgenden Abbildung werden die Prozessmodellierungsebenen und die darin zur Verwendung vorgeschlagenen Prozessmodelltypen dargestellt.

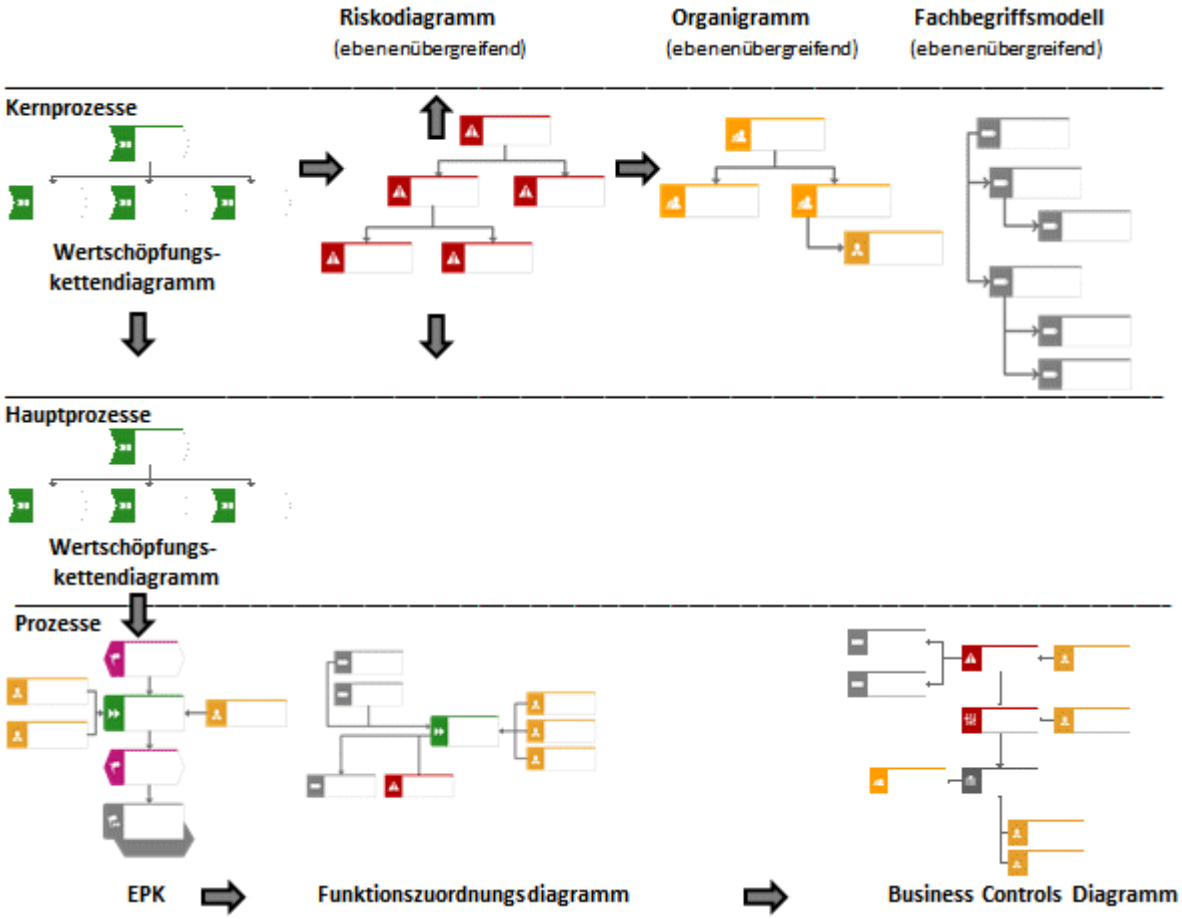

Abbildung 1: Modellierungsebenen und deren Modelltypen

4.1.2 Identifikation von Kontrollen und Prozessen

4.1.2.1 Prozessmodelle

Folgende Prozessmodelle können zum Aufbau der Prozesslandschaft/Prozesshierarchie benutzt werden.

Modellname	Modelltypnummer
Wertschöpfungskettendiagramm	12
EPK	13
Funktionszuordnungsdiagramm	14
VKD	18
EPK (Materialfluss)	50
VKD (Materialfluss)	51
EPK (Spaltendarstellung)	134
EKP (Zeilendarstellung)	140
EPK (Tabellendarstellung)	154
EPK (Tabellendarstellung horizontal)	173
Enterprise BPMN collaboration diagram	272
Enterprise BPMN process diagram	273

In den folgenden Kapiteln wird eine mögliche Modellierung der Prozesslandschaft vorgeschlagen.

4.1.2.2 Prozessmodellierung auf Ebene 1 – Wertschöpfungskettendiagramm (WKD)

Ebene 1 enthält als zentrales Modell das Übersichtsprozessmodell. Es wird mit Hilfe des Modelltyps **Wertschöpfungskettendiagramm** modelliert. Dieser Übersichtskernprozess dient als Einstiegsmodell.

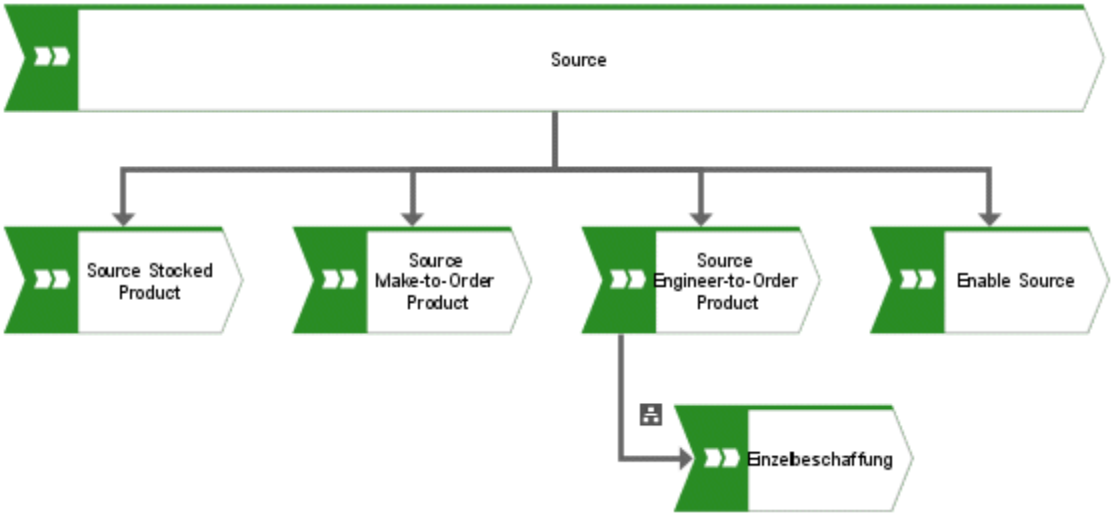

Abbildung 2: Ebene 1 – Wertschöpfungskettendiagramm

Der dazu verwendete Objekttyp ist die **Funktion** (OT_FUNC). Die Hierarchie zwischen den Objekten wird über die Kante **ist prozessorientiert übergeordnet** bzw. **ist prozessorientiert untergeordnet** abgebildet. In ARIS Risk & Compliance Manager ist nur eine Baumstruktur der Hierarchien erlaubt. Daher kann jede Funktion nur genau eine übergeordnete Funktion besitzen. Folgende Modelltypen können einem Objekttyp in einer WKD hinterlegt werden:

Objekttyp	Hinterlegter Modelltyp
Funktion [Wertschöpfungskette]	WKD
Funktion [Wertschöpfungskette]	Funktionszuordnungsdiagramm

Für jede relevante Funktion wird somit in ARIS Risk & Compliance Manager ein Hierarchieelement angelegt. Ausnahme: Das oberste Hierarchieelement existiert bereits in ARIS Risk & Compliance Manager.

4.1.2.2.1 Zuordnungen Funktion (ARIS) zu Prozesshierarchieelement (ARCM)

Für das Objekt **Funktion** gelten folgende Zuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Funktion	Name	AT_NAME	X	HIERARCHY	name	
				HIERARCHY	isroot	Ist nur für das oberste Hierarchieelement **true**.
				HIERARCHY	hnumber	Ist für die Prozesshierarchie nicht relevant.
				HIERARCHY	type	Prozesshierarchie (Value 4)
Funktion	Beschreibung/Definition	AT_DESC		HIERARCHY	description	
			X	HIERARCHY	status	Status ist **true** (für aktiv)
Funktion	Sign-off-relevant	AT_AAM_SIGN_OFF_RELEVANT	X	HIERARCHY	signoff	
Funktion	Modellverknüpfung	AT_AAM_MOD_LINK		HIERARCHY	modellink	
				HIERARCHY	modelguid	GUID des Modells, in dem eine Ausprägung der Funktion vorkommt. Es wird das erste verfügbare Prozessmodell (EPK, WKD usw.) gewählt.
				HIERARCHY	model_name	Name des Modells (s. o.)

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Funktion	Objektverknüpfung	AT_AAM_OBJ_LINK		HIERARCHY	objectlink	
Funktion	GUID des Objekts			HIERARCHY	objectguid	
				HIERARCHY	children	Untergeordnetes Hierarchieelement
				HIERARCHY	so_owner	Zugeordnete Sign-off-Owner Gruppe
				HIERARCHY	tester	Ist für diesen Hierarchietyp nicht relevant.

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.2.3 Prozessmodellierung auf Level 2 - Wertschöpfungskettendiagramm (WKD)

Als Modell des Levels 2 wird das Wertschöpfungskettendiagramm genutzt. Level 2 dient der Darstellung der Hauptprozesse und zur Abbildung des Zusammenhangs der auf Level 3 befindlichen Teilprozesse.

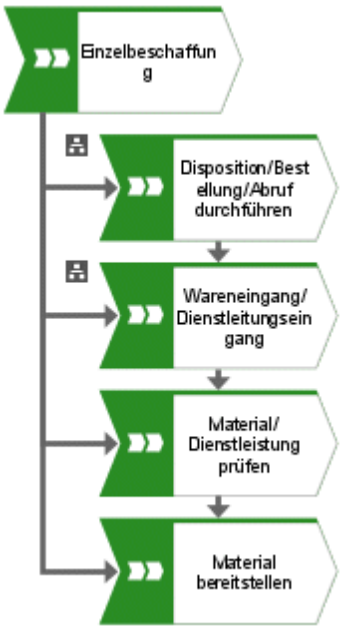

Abbildung 3: Ebene 2 – Wertschöpfungskettendiagramm

Es gelten die gleichen Konventionen wie für die als Wertschöpfungskette modellierten Kernprozesse.

Folgende Modelltypen können einem Objekttyp in der WKD hinterlegt werden:

Objekttyp	Hinterlegter Modelltyp
Funktion	EPK
Funktion	Funktionszuordnungsdiagramm

4.1.2.4 Prozess- und Kontrollmodellierung auf Level 3 – Ereignisgesteuerte Prozesskette (EPK)

Mit einer EPK können Prozesse eines Unternehmens beschrieben werden. Im Mittelpunkt steht dabei der zeitlich-logische Ablauf der durchzuführenden Tätigkeiten. Dazu wird eine Abfolge von Funktionen und resultierenden Ereignissen verwendet. Diese schlanken Prozesse können durch zusätzliche Objekte (Organisationseinheiten, Stellen (Rollen), Anwendungssysteme etc.) mit erweitertem Informationsgehalt versehen werden. So kann z. B. ein Risiko mit der Kante **tritt auf an** direkt mit einer Funktion in einer EPK verbunden werden.

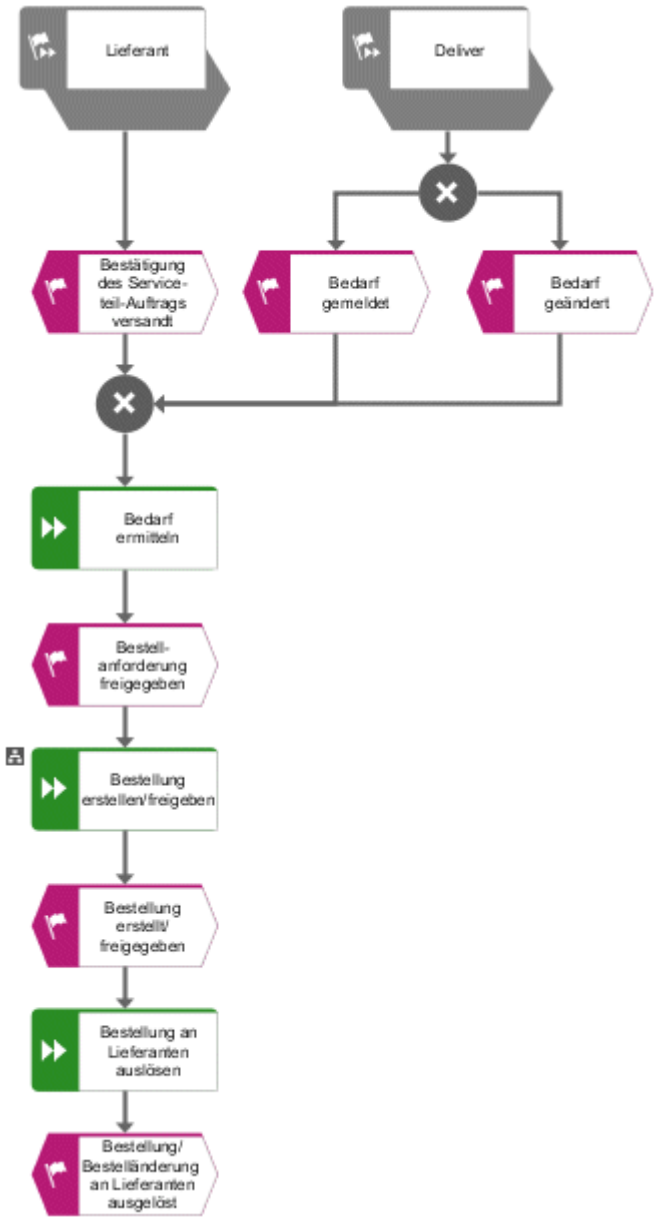

Abbildung 4: Ebene 3 – Ereignisgesteuerte Prozesskette

Folgende Modelltypen können einem Objekttyp in einer EPK hinterlegt werden:

Objekttyp	Hinterlegter Modelltyp
Funktion	EPK
Funktion	Funktionszuordnungsdiagramm
Risiko	EPK
Risiko	Business Controls Diagram

EBENE 3 – FUNKTIONSZUORDNUNGSDIAGRAMM (FZD)

Die EPKs können auch als schlanke EPKs modelliert werden, das bedeutet ohne Organisationseinheiten, Stellen und Anwendungssysteme. Die Beziehungen dieser zusätzlichen Objekte zu einer Funktion werden dann in einem Funktionszuordnungsdiagramm modelliert, das der Funktion hinterlegt wird. Die Objekt- und Symboltypen des Funktionszuordnungsdiagramms sind diejenigen, welche aus der schlanken eine erweiterte EPK machen. Dies sind im Einzelnen:

- Funktion
- Stelle
- Organisationseinheit
- Typ Organisationseinheit
- Gruppe
- Rolle
- Person intern
- Anwendungssystem
- Anwendungssystemtyp
- Informationsträger (Datei, Dokument)
- Risiko

4.1.3 Dokumentation weiterer Hierarchien des Unternehmens

Für alle Hierarchien, die in ARIS Risk & Compliance Manager überführt werden sollen, ist nur eine Baumstruktur erlaubt. Dies bedeutet, dass jedes Element der Hierarchie nur genau ein übergeordnetes Element besitzen darf.

4.1.3.1 Regularienhierarchie

Die Regularienhierarchie wird in ARIS im Fachbegriffsmodell mit dem Objekt **Fachbegriff** (OT_TECH_TRM) modelliert. Durch das Attribut **Regularien** können Regularien eindeutig identifiziert werden (API-Name: AT_AAM_ANNUAL_ACCOUNTS_ITEM). Die Hierarchie zwischen den Objekten wird über die Kante **hat** abgebildet.

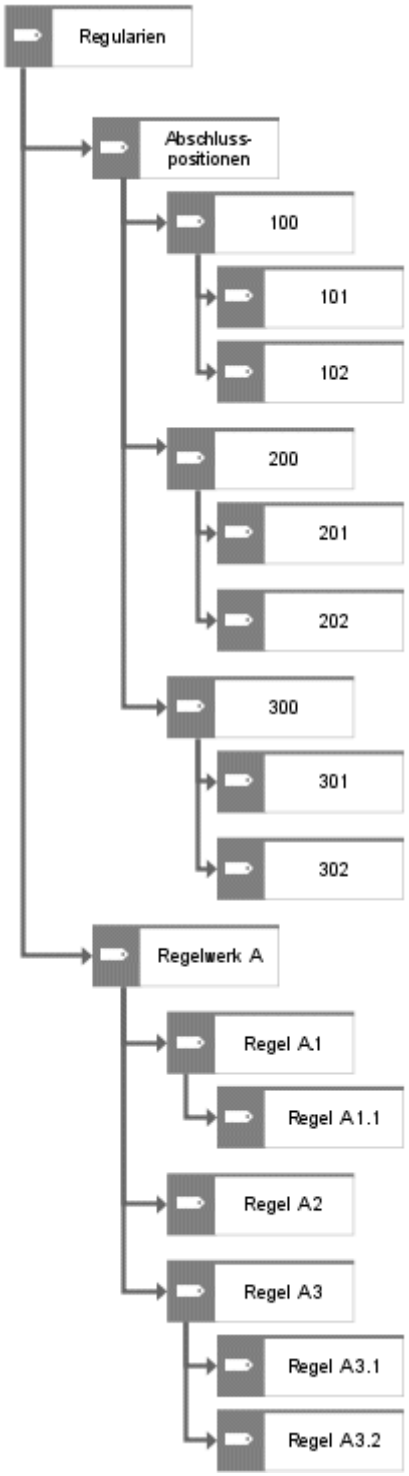

Abbildung 5: Struktur Regularienhierarchie

4.1.3.1.1 Zuordnungen Fachbegriff (ARIS) zu Regularienelement (ARCM)

Für das Objekt **Fachbegriff** gelten folgende Attributzuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Fachbegriff	Name	AT_NAME	X	HIERARCHY	name	
				HIERARCHY	isroot	Ist nur für das oberste Hierarchieelement **true**.
Fachbegriff	Kurzbezeichnung	AT_SHORT_DESC		HIERARCHY	hnumber	
				HIERARCHY	type	Regularienhierarchie (Value = 2)
Fachbegriff	Beschreibung/Definition	AT_DESC		HIERARCHY	description	
			X	HIERARCHY	status	Status ist **true** (für aktiv)
Fachbegriff	Sign-off-relevant	AT_AAM_SIGN_OFF_RELEVANT	X	HIERARCHY	signoff	
Fachbegriff	Modellverknüpfung	AT_AAM_MOD_LINK		HIERARCHY	modellink	
				HIERARCHY	modelguid	GUID des Modells, in dem eine Ausprägung des Fachbegriffs vorkommt. Es wird das erste verfügbare Fachbegriffsmodell gewählt.

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
				HIERARCHY	model_name	Name des Modells (s. o.)
Fachbegriff	Objektverknüpfung	AT_AAM_OBJ_LINK		HIERARCHY	objectlink	
Fachbegriff	GUID des Objekts			HIERARCHY	objectguid	
				HIERARCHY	children	Untergeordnetes Hierarchieelement
				HIERARCHY	so_owner	Zugeordnete Sign-off-Owner Gruppe
				HIERARCHY	tester	Ist für diesen Hierarchietyp nicht relevant.

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.3.2 Testerhierarchie

Die Testerhierarchie wird in ARIS im Organigramm mit dem Objekt **Organisationseinheit** (OT_ORG_UNIT) modelliert. Die Hierarchie zwischen den Objekten wird über die Kante **ist übergeordnet** abgebildet.

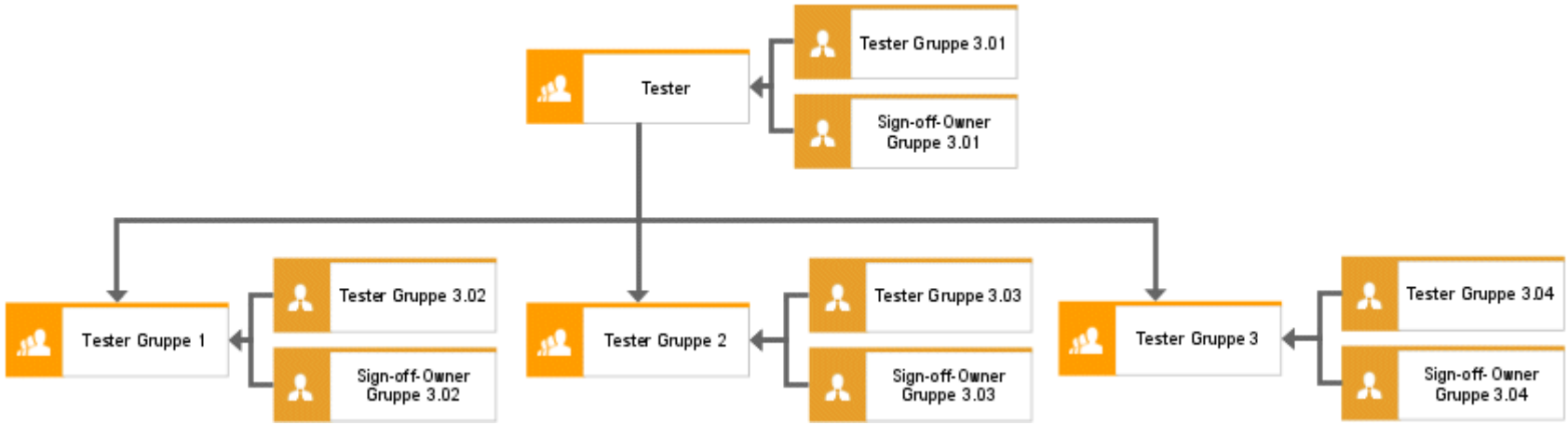

Abbildung 6: Struktur Testerhierarchie

Für jede Organisationseinheit wird somit ein Testerhierarchieelement in ARIS Risk & Compliance Manager angelegt (Ausnahme: Das oberste Hierarchieelement existiert bereits in ARIS Risk & Compliance Manager). Derzeit kann jedem Hierarchieelement nur eine Benutzergruppe (Seite 22) zugeordnet werden.

Für das obige Beispiel werden somit in ARIS Risk & Compliance Manager die Testerhierarchieelemente **Tester**, **Tester group 1**, **Tester group 2** und **Tester group 3** neu angelegt. **Tester** ist dabei den anderen Hierarchieelementen übergeordnet.

4.1.3.2.1 Zuordnung Organisationseinheit (ARIS) zu Testerhierarchieelement (ARCM)

Für das Objekt **Organisationseinheit** gelten folgende Attributzuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Organisationseinheit	Name	AT_NAME	X	HIERARCHY	name	
				HIERARCHY	isroot	Ist nur für das oberste Hierarchieelement **true**.
				HIERARCHY	hnumber	Ist für die Testerhierarchie nicht relevant.
				HIERARCHY	type	Testerhierarchie (Value = 1)
Organisationseinheit	Beschreibung/Definition	AT_DESC		HIERARCHY	description	
			X	HIERARCHY	status	Status ist **true** (für aktiv)
Organisationseinheit	Sign-off-relevant	AT_AAM_SIGN_OFF_RELEVANT	X	HIERARCHY	signoff	
Organisationseinheit	Modellverknüpfung	AT_AAM_MOD_LINK		HIERARCHY	modellink	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
				HIERARCHY	modelguid	GUID des Modells, in dem eine Ausprägung der Organi-sationseinheit vorkommt. Es wird das erste verfügbare Organigramm gewählt.
				HIERARCHY	model_name	Name des Modells (s. o.)
Organisationseinheit	Objektverknüpfung	AT_AAM_OBJ_LINK		HIERARCHY	objectlink	
Organisationseinheit	GUID des Objekts			HIERARCHY	objectguid	
				HIERARCHY	children	Untergeordnete Hierachieeinheit
				HIERARCHY	so_owner	Zugeordnete Sign-off-Owner Gruppe
				HIERARCHY	tester	Zugeordnete Testergruppen

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.3.3 Organisationshierarchie

Die Organisationshierarchie wird in ARIS im Organigramm mit dem Objekt **Organisationseinheit** (OT_ORG_UNIT) modelliert. Zudem sind die Objekte **Gruppe** (OT_GRP), **Stelle** (OT_POS) und **Standort** (OT_LOC) erlaubt. Die Hierarchie zwischen den Objekten wird über die Kante **ist übergeordnet** abgebildet.

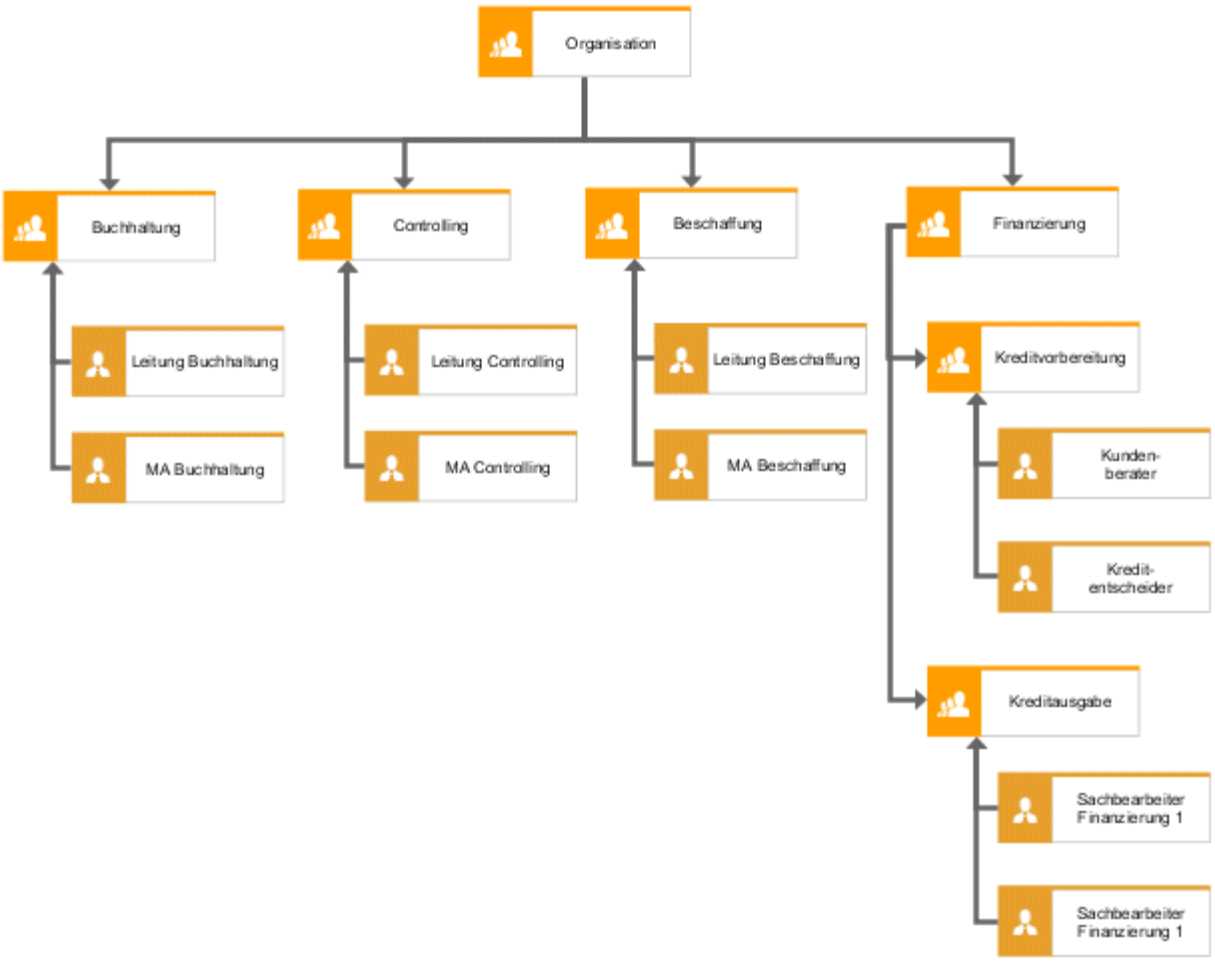

Abbildung 7: Struktur Organisationshierarchie

Für jede Organisationseinheit wird somit ein Organisationshierarchieelement angelegt. Ausnahme: Das oberste Hierarchieelement existiert bereits in ARIS Risk & Compliance Manager.

Für das obige Beispiel werden somit in ARIS Risk & Compliance Manager die Organisationshierarchieelemente **Organisation**, **Buchhaltung**, **Controlling** und **Beschaffung** angelegt. **Organisation** ist dabei den anderen Hierarchieelementen übergeordnet.

4.1.3.3.1 Zuordnung Organisationseinheit (ARIS) zu Organisationshierarchieelement (ARCM)

Für das Objekt **Organisationseinheit** gelten folgende Attributzuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Organisationseinheit	Name	AT_NAME	X	HIERARCHY	name	
				HIERARCHY	isroot	Ist nur für das oberste Hierarchieelement **true**.
				HIERARCHY	hnumber	Ist für die Organisationshierarchie nicht relevant.
				HIERARCHY	type	Organisationshierarchie (Value = 3)
Organisationseinheit	Beschreibung/Definition	AT_DESC		HIERARCHY	description	
			X	HIERARCHY	status	Status ist **true** (für aktiv)
Organisationseinheit	Sign-off-relevant	AT_AAM_SIGN_OFF_RELEVANT	X	HIERARCHY	signoff	
Organisationseinheit	Modellverknüpfung	AT_AAM_MOD_LINK		HIERARCHY	modellink	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
				HIERARCHY	modelguid	GUID des Modells, in dem eine Ausprägung der Organi-sationseinheit vorkommt. Es wird das erste verfügbare Organigramm gewählt.
				HIERARCHY	model_name	Name des Modells (s. o.)
Organisationseinheit	Objektverknüpfung	AT_AAM_OBJ_LINK		HIERARCHY	objectlink	
Organisationseinheit	GUID des Objekts			HIERARCHY	objectguid	
				HIERARCHY	children	Untergeordnete Hierarchieelemente
				HIERARCHY	so_owner	Zugeordnete Sign-off-Owner Gruppe
				HIERARCHY	tester	Ist für die Organisationshier archie nicht relevant.

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.3.4 Risikohierarchie (optional)

Die Risikohierarchie wird in ARIS im Risikodiagramm modelliert. Hier kann eine Kategorisierung der Risiken (OT_RISK) vorgenommen werden. Es können dabei Risiken Kategorien (OT_RISK_CATEGORY) und die Kategorien wiederum weiteren Kategorien mit Hilfe der Beziehung **umfasst** bzw. **enthält** untergeordnet werden. Dies dient der Strukturierung wird aber nur in Verbindung mit der Komponente **Operational Risk Management** überführt.

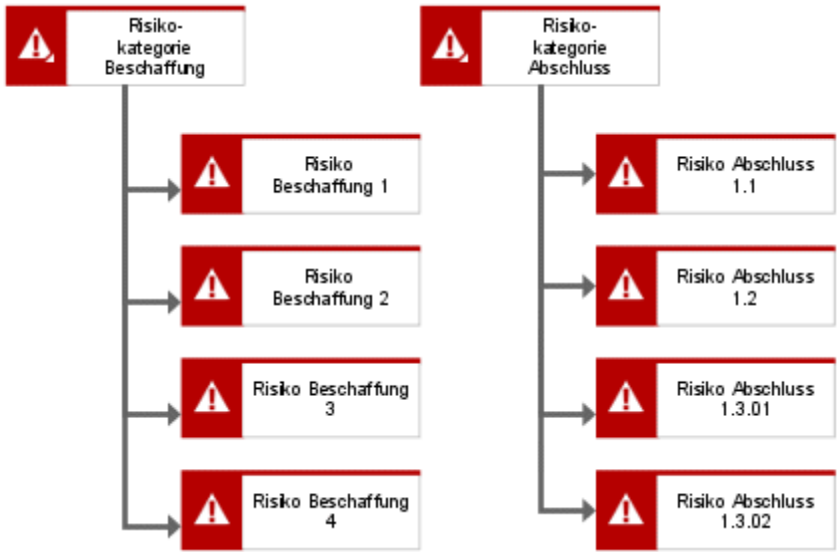

Abbildung 8: Struktur Risikohierarchie

4.1.4 Anlegen von Benutzern und Benutzergruppen

Benutzer und Benutzergruppen werden in ARIS Architect im Organigramm mit den Objekten **Person** (OT_PERS) und **Rolle** (OT_PERS_TYPE) modelliert.

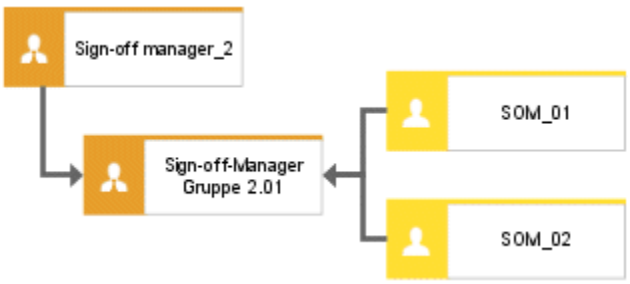

Abbildung 9: Struktur Benutzer/Benutzergruppen

Die übergeordnete Rolle **Sign-off manager_2** bestimmt dabei die Rolle, die die untergeordneten Rollen in ARIS Risk & Compliance Manager innehaben. Die beiden Rollen sind über die Kante **ist Verallgemeinerung von** miteinander verbunden. **Sign-off-Manager Gruppe 2.01** ist somit Verallgemeinerung von **Sign-off manager_2**. Der Name der übergeordneten Rolle definiert die Rolle und den Level der zu generierenden Gruppe. <Rolle>_<Level>, d. h.: Sign-off manager_2 > Rolle: Sign-off manager, Level: 2 (bzw. umgebungsspezifisch). Für die übergeordnete Rolle (in diesem Fall Sign-off manager_2) wird keine Benutzergruppe in ARIS Risk & Compliance Manager generiert.

Für die verschiedenen Rollenlevel gilt

- Rollenlevel 1: umgebungsübergreifend

  Die Rechte, die der Benutzergruppe auf Basis ihrer Rolle zugewiesen werden, gelten für alle Umgebungen, die der Benutzergruppe zugeordnet sind.

- Rollenlevel 2: umgebungsspezifisch

  Die Rechte, die der Benutzergruppe auf Basis ihrer Rolle zugewiesen werden, gelten für die Umgebung, in der die Benutzergruppe angelegt wurde.

- Rollenlevel 3: objektspezifisch

  Die Rechte, die der Benutzergruppe auf Basis ihrer Rolle zugewiesen werden, gelten für die entsprechenden Objekte der aktuellen Umgebung, in der die Benutzergruppe angelegt wurde.

Für das obige Beispiel wird somit in ARIS Risk & Compliance Manager die Benutzergruppe **Sign-off-Manager Gruppe 2.01** mit der Rolle **Sign-off-Manager** und dem Level **2** (also mit umgebungsübergreifenden Rechten) generiert. Zudem wird ein Benutzer mit der Benutzerkennung **SOM_01** generiert.

MAPPING ROLLENNAME (ARCM) ZU ROLLE (ARIS)

Für die Benutzergruppen in ARIS Risk & Compliance Manager und der zu verwendenden Benennung in ARIS Architect gelten folgende Zuordnungen. Weitere Rollen finden Sie in den anderen Konventionenhandbüchern.

Rolle (ARCM)	Rolle (ARIS)	Rollenlevel
roles.testauditor	Test auditor	Level 1, 2 und 3
roles.testauditorexternal	Test auditor external	Level 1 und 2
roles.deficiencyauditor.l1	Deficiency-Auditor (L1)	Level 1 und 2
roles.deficiencyauditor.l2	Deficiency auditor (L2)	Level 1 und 2
roles.deficiencyauditor.l3	Deficiency auditor (L3)	Level 1 und 2
roles.deficiencymanager.l1	Deficiency-Manager (L1)	Level 1, 2 und 3
roles.deficiencymanager.l2	Deficiency manager (L2)	Level 1, 2 und 3
roles.deficiencymanager.l3	Deficiency manager (L3)	Level 1, 2 und 3
roles.groupusermanager	Users/User groups manager	Level 1 und 2
roles.hierarchymanager	Hierarchy manager	Level 1 und 2
roles.riskmanager	Risk manager	Level 1, 2 und 3
roles.controlmanager	Control manager	Level 1, 2 und 3
roles.signoffmanager	Sign-off manager	Level 2 und 3
roles.signoffreviewer	Sign-off reviewer	Nur Level 3
roles.signoffowner	Sign-off owner	Nur Level 3

Rolle (ARCM)	Rolle (ARIS)	Rollenlevel
Roles.testmanager	Test manager	Level 1, 2 und 3
roles.testreviewer	Test reviewer	Nur Level 3
roles.tester	Tester	Nur Level 3
roles.issueauditor	Issue auditor	Level 1 und 2
roles.issuemanager	Issue manager	Level 1 und 2
roles.incidentauditor	Incident auditor	Level 1 und 2
roles.incidentmanager	Incident manager	Level 1 und 2
roles.incidentreviewer	Incident reviewer	Nur Level 3
roles.incidentowner	Incident owner	Nur Level 3
roles.lossauditor	Loss auditor	Level 1 und 2
roles.lossmanager	Loss manager	Level 1 und 2
roles.lossreviewer	Loss reviewer	Nur Level 3
roles.lossowner	Loss owner	Nur Level 3

4.1.4.1 Zuordnungen Rolle und Person

ZUORDNUNGEN ROLLE (ARIS) ZU BENUTZERGRUPPE (ARCM)

Für das Objekt **Rolle** (Benutzergruppe) gelten folgende Zuordnungen:

ARIS-Attribut	API-Name	ARCM-Attribut	M*	Anmerkungen
Name	AT_NAME	name	X	Der Name einer Benutzergruppe ist auf 250 Zeichen beschränkt.
Beschreibung/ Definition	AT_DESC	description	-	
Rolle	–	role	X	Die Werte für Rolle und Rollenlevel werden wie weiter oben beschrieben ermittelt.
Rollenlevel	–	rolelevel	X	
Benutzer	–	groupmembers	-	Die Benutzer werden über die Kante **nimmt wahr** zwischen Person und Rolle ermittelt.

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

ZUORDNUNGEN PERSON (ARIS) ZU BENUTZER (ARCM)

Für das Objekt **Person** (Benutzer) gelten folgende Zuordnungen:

ARIS-Attribut	API-Name	ARCM-Attribut	M*	Anmerkungen
Anmeldung	AT_LOGIN	Userid	X	Die Benutzer-ID eines Benutzers ist auf 250 Zeichen beschränkt.
Vorname	AT_FIRST_NAME	firstname	X	
Nachname	AT_LAST_NAME	lastname	X	
		name	-	Wird aus Nach- und Vorname zusammengesetzt.
Beschreibung/ Definition	AT_DESC	description	-	
E-Mail-Adresse	AT_EMAIL_ADDR	email	X	
Telefonnummer	AT_PHONE_NUM	phone	-	
		clients	-	Das Feld **Umgebungen** wird über die Umgebung bestimmt, in die importiert wird.
		substitutes	-	Das Feld **Vertretungen** wird nur manuell gepflegt.

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.5 Analyse der Risiken und Ableitung der Kontrollen und Tests

Für die in den Prozessen identifizierten Risiken können im Business Controls Diagram Kontrollen und Testdefinitionen inklusive der Verantwortlichkeiten definiert werden. Zudem können die Auswirkungen auf die Hierarchien des Unternehmens dokumentiert werden, z. B. welches Risiko welche Bilanzposition betrifft.

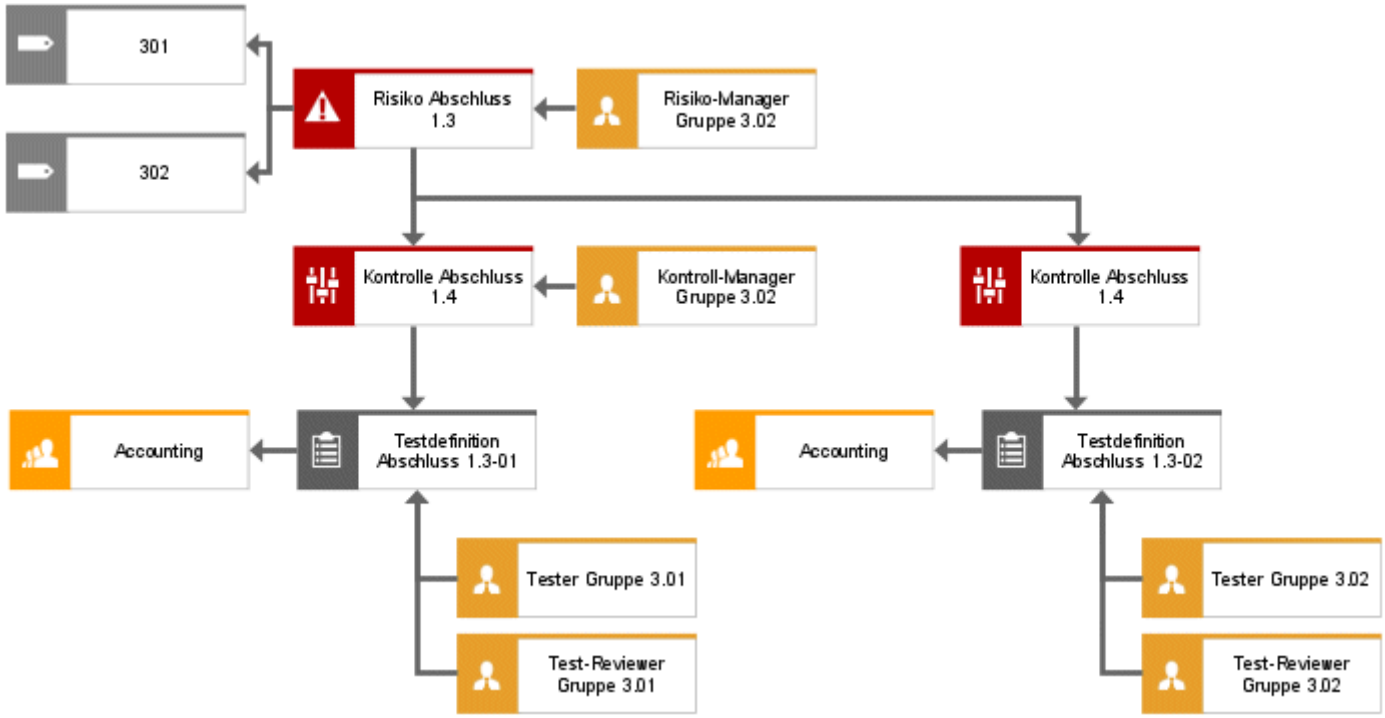

Abbildung 10: Struktur Business Controls Diagram

Die Zuordnung einer Risiko-Manager Gruppe, einer Test-Manager-Gruppe und einer Kontroll-Manager Gruppe ist optional.

BEZIEHUNGEN DES RISIKO-OBJEKTS UND DER DAMIT VERBUNDENEN OBJEKTE

Zwischen den Objekten des Business Control Diagrams sind folgende Kanten relevant:

Objekt	Kante	Objekt	Anmerkungen
Risiko	betrifft	Fachbegriff	über diese Kante wird die Beziehung zu den Regularien hergestellt.
Risiko	Ist fachlich verantwortlich für	Rolle	über diese Kante wird die Beziehung zum Risiko-Manager hergestellt.
Risiko	is reduced by	Kontrolle	über diese Kante wird die Beziehung zur Kontrolle hergestellt.
Kontrolle	wird überwacht durch	Testdefinition	über diese Kante wird die Beziehung zur Testdefinition hergestellt.
Kontrolle	ist fachlich verantwortlich für	Rolle	über diese Kante wird die Beziehung zum Kontroll-Manager hergestellt.
Testdefinition	betrifft	Organisationseinheit	über diese Kante wird die Beziehung zur betroffenen Organisationseinheit hergestellt.
Testdefinition	ist zugeordnet	Rolle	über diese Kante wird die Beziehung zum Tester, zum Test-Reviewer und zum Test-Manager hergestellt.

4.1.5.1 Risiko

Das Risiko wird in ARIS Architect mit dem Objekt **Risiko** (OT_RISK) modelliert. Für jedes Risiko, welches das Attribut **ARCM-Synchronisation** gesetzt hat, wird ein Risiko in ARIS Risk & Compliance Manager angelegt.

ZUORDNUNG RISIKO (ARIS) ZU RISIKO (ARCM)

Für das Objekt Risiko gelten folgende Zuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Risiko	Name	AT_NAME	X	RISK	name	
Risiko	Risiko-ID	AT_AAM_RISK_ID		RISK	risk_id	
Risiko	Risikotypen	AT_AAM_RISK_TYPE_FINANCIAL_REPORT AT_AAM_RISK_TYPE_COMPLIANCE AT_AAM_RISK_TYPE_OPERATIONS AT_AAM_RISK_TYPE_STRATEGIC	X	RISK	risktype	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt.
Risiko	Beschreibung/Definition	AT_DESC	X	RISK	description	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
			X	RISK	risk_function	Wird über die Kante zur Funktion identifiziert. Ein entsprechender Link zum Prozesshierarchieelement in ARIS Risk & Compliance Manager wird gespeichert.
			X	RISK	financial_statement	Wird über die Kante zum Fachbegriff identifiziert. Ein entsprechender Link zum Regularienhierarchieelement in ARIS Risk & Compliance Manager wird gespeichert.
Risiko	Auswirkung	AT_AAM_IMPACT	X	RISK	impact	
Risiko	Wahrscheinlichkeit	AT_AAM_PROBABILITY	X	RISK	probability	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Risiko	Risikokatalog 1	AT_AAM_RISK_CATALOG_1		RISK	risk_catalog1	
Risiko	Risikokatalog 2	AT_AAM_RISK_CATALOG_2		RISK	risk_catalog2	
Risiko	Titel 1 und Verknüpfung 1 bis Titel 4 und Verknüpfung 4	AT_TITL1 und AT_EXT_1 usw.		RISK	documents	Aus dem Titel und der Verknüpfung wird jeweils ein Dokument (O_10) in ARIS Risk & Compliance Manager generiert und mit dem Risiko verlinkt.
				RISK	controls	Wird über die Kante zur Kontrolle identifiziert. Ein entsprechender Link zur Kontrolle in ARIS Risk & Compliance Manager wird gespeichert.

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
				RISK	manager_group	Wird über die Kante zur Rolle identifiziert. Ein entsprechender Link zum Risiko-Manager in ARIS Risk & Compliance Manager wird gespeichert.
Risiko	Assertions	AT_AAM_ASSERTIONS_EXIST_OCCURRENCE AT_AAM_ASSERTIONS_COMPLETENESS AT_AAM_ASSERTIONS_RIGHTS_OBLIGATIONS AT_AAM_ASSERTIONS_VALUATION_ALLOCATION AT_AAM_ASSERTIONS_PRESENTATION_DISCLOSURE AT_AAM_ASSERTIONS_NA	X	RISK	assertions	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt. Es besteht eine Abhängigkeit der Werte. Die ersten 5 Werte können nicht in Kombination mit dem letzten Eintrag vorkommen.

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.5.2 Kontrolle

Die Kontrolle wird in ARIS mit dem Objekt **Funktion** (OT_FUNC) und dem Standardsymbol **Kontrolle** (ST_CONTR) modelliert. Für den Export in ARIS Risk & Compliance Manager sind nur die Kontrollen relevant, die an einem Risiko des Typs **ARCM-Synchronisation** modelliert ist.

FUNKTION (KONTROLLE) (ARIS) ZU CONTROL (ARCM)

Für das Objekt **Funktion (Kontrolle)** gelten folgende Zuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Kontrolle	Name	AT_NAME	X	CONTROL	name	
Kontrolle	Kontroll-ID	AT_AAM_CTRL_ID		CONTROL	control_id	
				CONTROL	manager_ group	Wird über die Kante zur Rolle identifiziert. Ein entsprechender Link zum Kontroll-Manager in ARIS Risk & Compliance Manager wird gespeichert.
Kontrolle	Kontrollfrequenz	AT_AAM_CTRL_FREQUENCY	X	CONTROL	control_frequency	
Kontrolle	Kontrollausführung	AT_AAM_CTRL_EXECUTION_ MANUAL AT_AAM_CTRL_EXECUTION_IT	X	CONTROL	control_execution	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt.

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Kontrolle	Wirkung der Kontrolle	AT_AAM_CTRL_EFFECT	X	CONTROL	control_effect	
Kontrolle	COSO-Komponente	AT_AAM_COSO_COMPONENT_CRTL_ENVIRONMENT AT_AAM_COSO_COMPONENT_RISK_ASSESSMENT AT_AAM_COSO_COMPONENT_CTRL_ACTIVITIES AT_AAM_COSO_COMPONENT_INFO_COMMUNICATION AT_AAM_COSO_COMPONENT_MONITORING		CONTROL	control_type	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt.
Kontrolle	Kontrollaktivität	AT_AAM_CTRL_ACTIVITY	X	CONTROL	controls	
				CONTROL	testdefinitions	Wird über die Kante zur Testdefinition identifiziert. Ein entsprechender Link zur Testdefinition in ARIS Risk & Compliance Manager wird gespeichert.
Kontrolle	Kontrollziel	AT_AAM_CTRL_OBJECTIVE		CONTROL	control_objective	
Kontrolle	Key-Kontrolle	AT_AAM_KEY_CTRL	X	CONTROL	key_control	

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.5.3 Testdefinition

Die Testdefinition wird in ARIS mit dem Objekt **Testdefinition** (OT_TEST_DEFINITION) modelliert. Für die Synchronisation mit ARIS Risk & Compliance Manager sind nur diejenigen Risiken relevant, die an einer Kontrolle modelliert werden, für die das Attribut **ARCM-Synchronisation** gesetzt ist.

ZUORDNUNG TESTDEFINITION (ARIS) ZU TESTDEFINITION ARCM)

Für das Objekt **Testdefinition** gelten folgende Zuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Testdefinition	Name	AT_NAME	X	testdefinition	name	
Testdefinition	Testaktivität	AT_AAM_TEST_ACTIVITY	X	testdefinition	testingsteps	
Testdefinition	Art des Tests	AT_AAM_TEST_NATURE_INQUIRY AT_AAM_TEST_NATURE_OBSERVATION AT_AAM_TEST_NATURE_EXAMINATION AT_AAM_TEST_NATURE_REPERFORMANCE	X	testdefinition	test_nature	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt.
Testdefinition	Testtyp	AT_AAM_TEST_TYPE_DESIGN AT_AAM_TEST_TYPE_EFFECTIVENESS	X	testdefinition	test_type	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt.
Testdefinition	Testumfang	AT_AAM_TEST_SCOPE	X	testdefinition	testextend	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
			X	testdefinition	owner_group	Wird über die Kante zur Rolle mit Hilfe der Rolle Tester identifiziert. Ein entsprechender Link zum Tester in ARIS Risk & Compliance Manager wird gespeichert.
Testdefinition	Ereignisgesteuerte Testfälle erlaubt	AT_EVENT_DRIVEN_TESTS_ ALLOWED	X	testdefinition	event_driven_allowed	Bei **true** wird die Test-definition nur für automatisierte Kontrolltests herangezogen. Gleich-zeitig muss die Testfrequenz auf **ereignisgesteuert** gesetzt sein.
Testdefinition	Testfrequenz	AT_AAM_TEST_FREQUENCY	X	testdefinition	testfrequency	
Testdefinition	Frist zur Durchführung in Tagen	AT_AAM_TEST_DURATION	X	testdefinition	testduration	
Testdefinition	Startdatum der Testdefinition	AT_AAM_TESTDEF_START_ DATE	X	testdefinition	testdefinition_startdate	
Testdefinition	Enddatum der Testdefinition	AT_AAM_TESTDEF_END_ DATE		testdefinition	testdefinition_enddate	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Testdefinition	Länge des Kontrollzeitraums	AT_AAM_TESTDEF_CTRL_PERIOD	X	testdefinition	control_period	
Testdefinition	Offset in Tagen	AT_AAM_TESTDEF_OFFSET	X	testdefinition	offset	
			X	testdefinition	reviewer_group	Wird über die Kante zur Rolle mit Hilfe der Rolle Test-Reviewer identifiziert. Ein entsprechender Link zum Test-Reviewer in ARIS Risk & Compliance Manager wird gespeichert.
			X	testdefinition	manager_group	Wird über die Kante zur Rolle mit Hilfe der Rolle Test-Manager identifiziert. Ein entsprechender Link zum Test-Manager in ARIS Risk & Compliance Manager wird gespeichert.

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
			X	testdefinition	effected_orgunit	Wird über die Kante zu Organisationseinheit, Gruppe, Stelle oder Standort identifiziert. Ein entsprechender Link zur betreffenden Organisationseinheit in ARIS Risk & Compliance Manager wird gespeichert.
Testdefinition	Wiedervorlage erlaubt	AT_AAM_TESTDEF_ FOLLOWUP	X	testdefinition	isfollowup	

*Die Spalte **M** gibt an, ob das Attribut ein Pflichtfeld ist.

4.1.5.4 Allgemeine Modellierungsregeln

Risiken innerhalb der modellierten Business Controls Diagrams müssen eindeutig sein. Ein Risiko kann mehrere Kontrollen haben, aber eine Kontrolle immer nur ein Risiko. Ein Risiko darf in höchstens einem Business Controls Diagram ausgeprägt und jeweils nur mit einer Funktion verbunden sein.

Die Kontrolle innerhalb des modellierten Business Controls Diagram muss eindeutig und darf in höchstens einem Business Controls Diagram ausgeprägt sein. Kontrollen können jeweils mit exakt einem Risiko verbunden sein, bei dem das Attribut **ARCM-Synchronisation** gepflegt ist. Die Kontrolle kann mit mindestens einer Testdefinition verbunden sein.

Die Testdefinition innerhalb des modellierten Business Controls Diagram muss eindeutig sein und darf in höchstens einem Business Controls Diagram ausgeprägt sein. Eine Testdefinition darf mit exakt einer Kontrolle verbunden sein, die mit einem Risiko verbunden ist, bei dem das Attribut **ARCM-Synchronisation** gepflegt ist und die Kontrollen jeweils mit mindestens einer Testdefinition verbunden sind.

4.1.5.5 Automatisiertes Testen von Kontrollen

Um automatisierte Kontrolltests per Event-Enabling durchzuführen, muss das Attribut **Ereignisgesteuerte Testfälle erlaubt** auf **true** gesetzt werden. Automatisierte Tests von Kontrollen können dann ad hoc durchgeführt werden, z. B. angesteuert durch ein externes Ereignis.

Zusätzlich muss für das Attribut **Testfrequenz** der Attributwert **Ereignisgesteuert** gewählt werden, um zu vermeiden, dass vom System unterjährige Testfälle generiert werden. Diese Frequenz wird nur für die Verarbeitung von Ad-hoc Tests verwendet.

4.1.6 Sign-off

4.1.6.1 Sign-off über die Prozesshierarchie

Für den Sign-off wird in einem Wertschöpfungskettendiagramm die Beziehung zwischen der Funktion und der Sign-off-Owner-Gruppe (Rolle) modelliert. Ein Beispiel ist in der folgenden Abbildung dargestellt.

Die ursprüngliche Auswahl der für die Synchronisation relevanten Funktionen wird über die Kante **tritt auf an** zu den Kontrollen ermittelt, für die das Attribut **ARCM-Synchronisation** gesetzt ist.

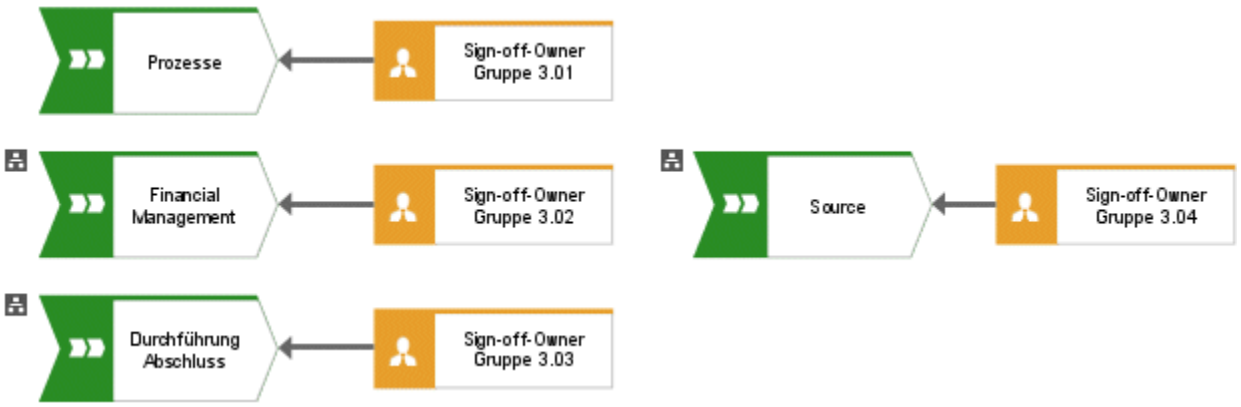

Abbildung 11: Zuordnung Funktion – Sign-Off-Owner-Gruppe

Über die Kante **entscheidet über** wird eine Verbindung zwischen einer Sign-off-Owner Gruppe (Benutzergruppe) und einem Prozesshierarchieelement hergestellt.

4.1.6.2 Sign-off über die Regularienhierarchie

Für den Sign-off über die Regularienhierarchie wird in einem Funktionszuordnungsdiagramm die Beziehung zwischen den Regularien und der Sign-off-Owner-Gruppe modelliert. Über die Kante **ist Eigner von** wird eine Verbindung zwischen der Benutzergruppe und einem Hierarchieelement hergestellt.

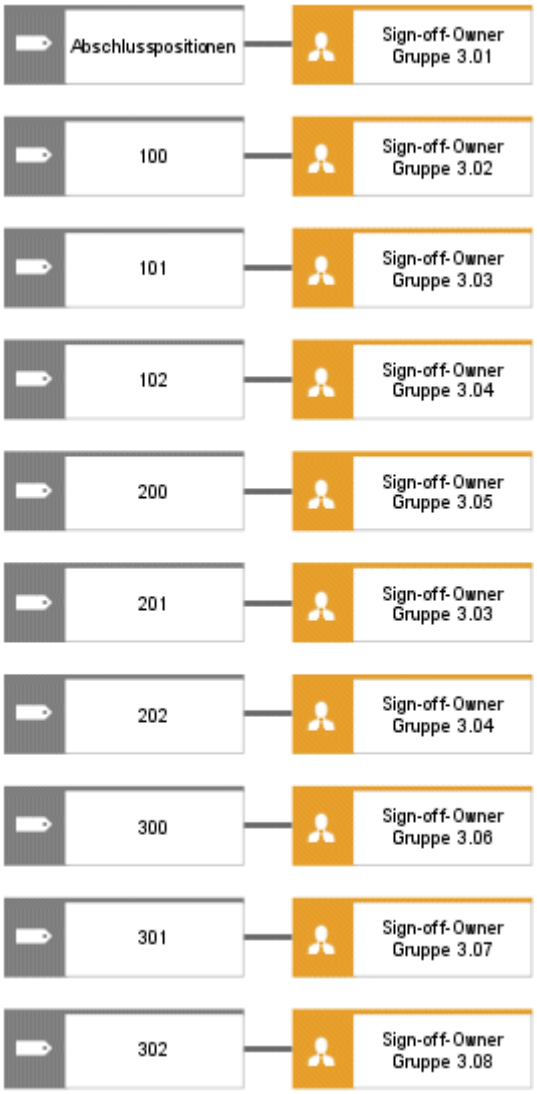

Abbildung 12: Zuordnung Regularien – Sign-Off-Owner-Gruppe

4.1.6.3 Sign-off über die Testerhierarchie

Für den Sign-off über die Testerhierarchie wird in dem Organigramm der Testerhierarchie die Beziehung zwischen der Organisationseinheit und der Sign-off-Owner-Gruppe modelliert. Über die Kante **gehört zu** wird die Verbindung zwischen der Benutzergruppe und dem Hierarchieelement hergestellt.

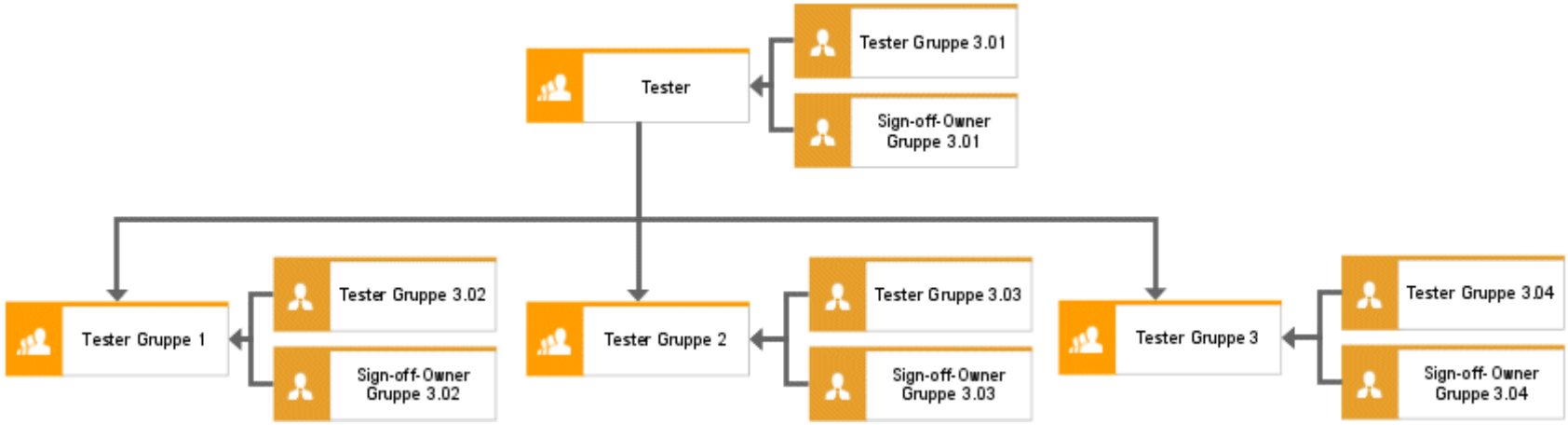

Abbildung 13: Zuordnung Organisationseinheit (Tester) – Sign-Off-Owner-Gruppe

4.1.6.4 Sign-off über die Organisationshierarchie

Für den Sign-off wird in dem Organigramm der Unternehmensorganisation die Beziehung zwischen den Organisationseinheiten und den Sign-off-Owner-Gruppen modelliert. Über die Kante **gehört zu** wird die Verbindung zwischen der Benutzergruppe und dem Hierarchieelement hergestellt.

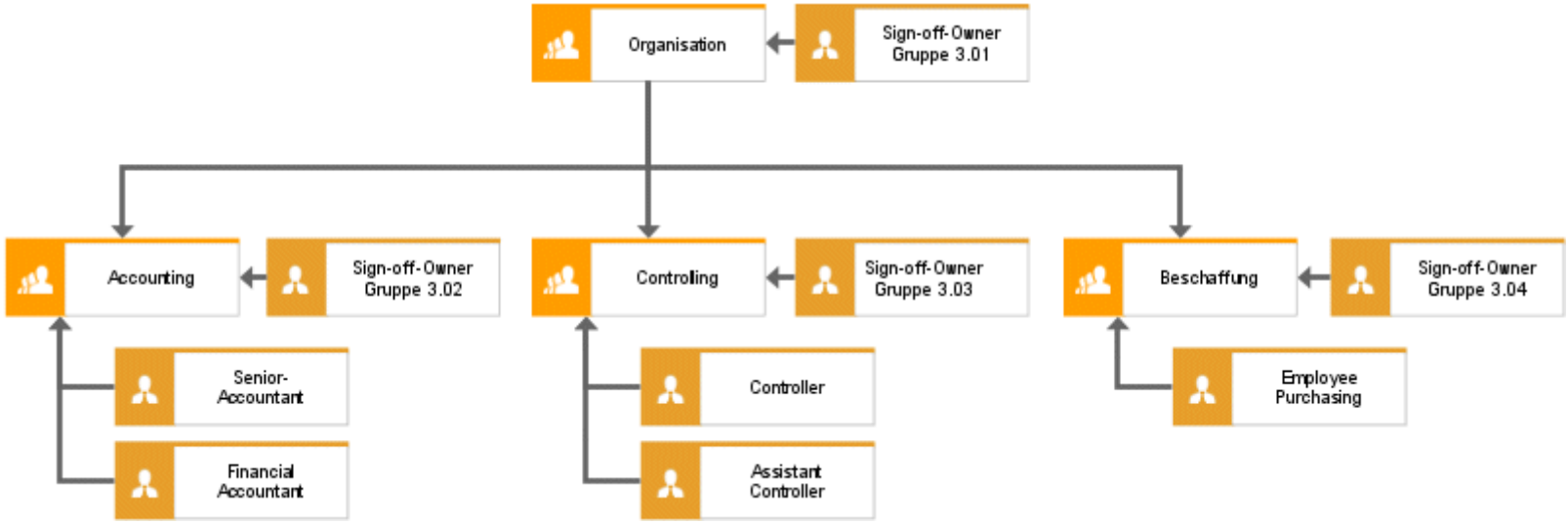

Abbildung 14: Zuordnung Organisationseinheit – Sign-Off-Owner-Gruppe

5 Support

IM WEB

Öffnen Sie **Empower (https://empower.softwareag.com/),** um Support zu erhalten.

Mit einem gültigen Support-Vertrag haben Sie Zugriff auf die Lösungsdatenbank.

Bei Fragen zu speziellen Installationen, die Sie nicht selbst ausführen können, wenden Sie sich an Ihre lokale Software AG-Vertriebsorganisation.

TELEFONISCH

Mit einem gültigen Support-Vertrag erreichen Sie den Global Support ARIS unter:

+800 ARISHELP

Dabei steht das "+" für das jeweilige Präfix, um in diesem Land eine internationale Verbindung anzuwählen.

Beispiel für die Anwahl innerhalb Deutschlands mit direkter Amtsleitung: 00 800 2747 4357

Sollte diese Nummer von Ihrem Telefonanbieter nicht unterstützt werden, lesen Sie die Informationen zu Empower https://empower.softwareag.com/public_directory.asp.

6 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.