ARIS RISK & COMPLIANCE MANAGER

KONTROLLBASIERTES TEST- UND SIGN-OFF-MANAGEMENT

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.

Inhalt

1 Textkonventionen 1

2 Einleitung 2

3 Inhalt des Dokuments 3
3.1 Zielsetzung und Abgrenzung 3

4 ARIS-Konventionen 4
4.1 Identifikation von Kontrollen und Prozessen 4
4.1.1 Prozess- und Kontrollmodellierung auf Level 3 – Ereignisgesteuerte Prozesskette (EPK) 4
4.2 Dokumentation weiterer Hierarchien des Unternehmens 5
4.2.1 Testerhierarchie 6
4.2.1.1 Zuordnung Organisationseinheit (ARIS) zu Testerhierarchieelement (ARCM) 7
4.3 Anlegen von Benutzern und Benutzergruppen 9
4.3.1 Zuordnungen Rolle und Person 11
4.4 Analyse von Kontrollen und Risiken und Ableitung der Tests 13
4.4.1 Kontrolle 15
4.4.2 Risiko 19
4.4.3 Testdefinition 22
4.5 Allgemeine Modellierungsregeln 26
4.5.1 Automatisiertes Testen von Kontrollen 26
4.5.2 Sign-off 26
4.5.2.1 Sign-off über die Prozesshierarchie 26
4.5.2.2 Sign-off über die Regularienhierarchie 27
4.5.2.3 Sign-off über die Testerhierarchie 28
4.5.2.4 Sign-off über die Organisationshierarchie 29

5 Rechtliche Hinweise 30
5.1 Dokumentationsumfang 30
5.2 Datenschutz 31
5.3 Disclaimer 31

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 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.
  ```

2 Einleitung

Die modellhafte Dokumentation von Geschäftsprozessen und Funktionen in ARIS bringt eine Reihe von Vorteilen mit sich (Einheitlichkeit, Komplexitätsreduzierung, Wiederverwendbarkeit, Auswertbarkeit, Integrität usw.). Dies ist jedoch nur möglich, wenn die methodischen und funktionalen Regeln sowie Konventionen bei der Modellierung in ARIS Architect eingehalten werden. Es wird empfohlen, die Konventionen in diesem Handbuch sowie im Handbuch der allgemeinen Konventionen zu befolgen, um eine ordnungsgemäße Pflege der relevanten Objekte in ARIS Architect zu gewährleisten. Nur dann können alle modellierten Daten auch in ARIS Risk & Compliance Manager überführt und weiterverwendet werden.

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 Identifikation von Kontrollen und Prozessen

4.1.1 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. eine Kontrolle mit der Kante **wird durchgeführt an** direkt mit einer Funktion in einer EPK verbunden werden.

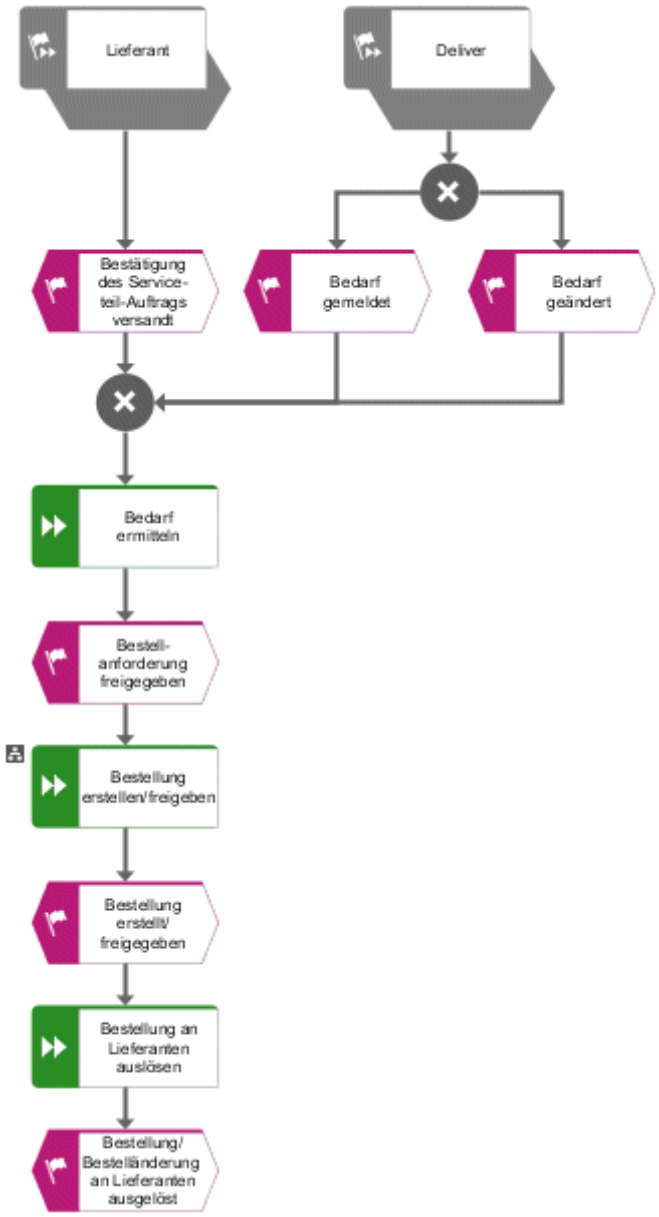

Abbildung 1: Ebene 3 – Ereignisgesteuerte Prozesskette

Folgende Modelltypen können einem Objekttyp in einer EPK hinterlegt werden:

Objekttyp	Hinterlegter Modelltyp
Funktion	EPK
Funktion	Funktionszuordnungsdiagramm
Kontrolle (OT_FUNC, ST_CONTR)	EPK
Kontrolle (OT_FUNC, ST_CONTR)	Business Controls Diagram

LEVEL 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)
- Kontrolle (Objekttyp: OT_FUNC, Symboltyp: ST_CONTR)

4.2 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.

4.2.1 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.

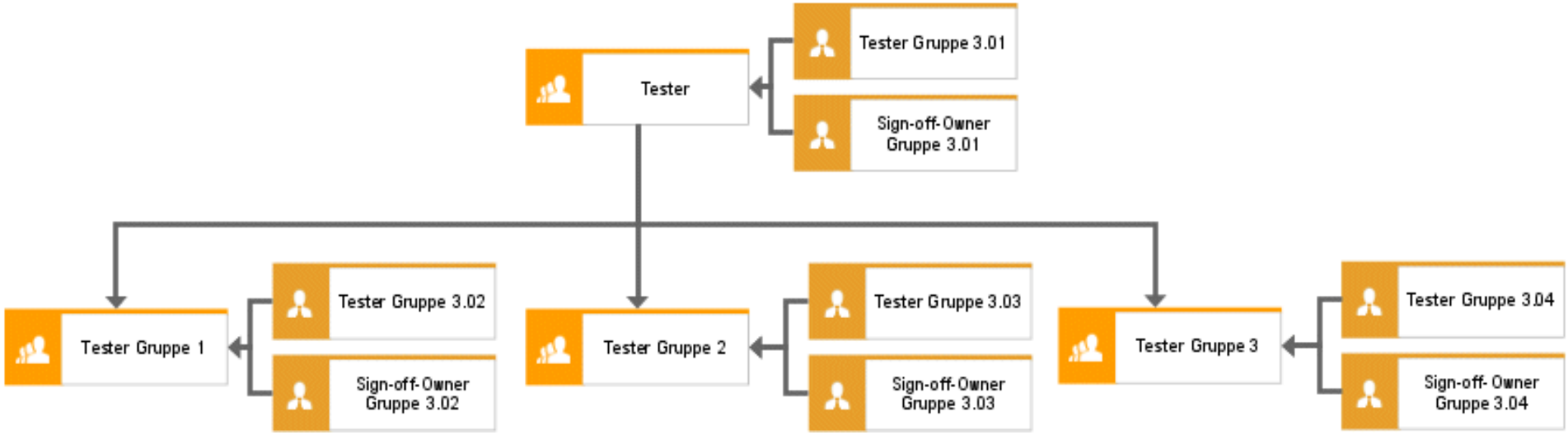

Abbildung 2: Struktur Testerhierarchie

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 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.

4.2.1.1 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		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.

4.3 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.

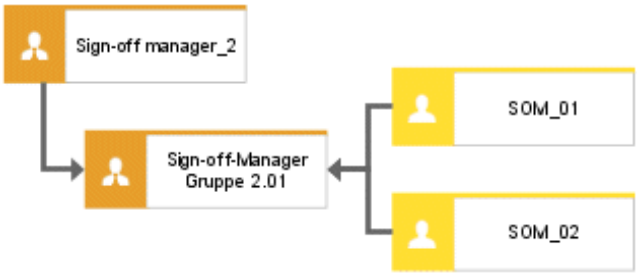

Abbildung 3: Struktur Benutzer/Benutzergruppen

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
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

4.3.1 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.

4.4 Analyse von Kontrollen und Risiken und Ableitung der Tests

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

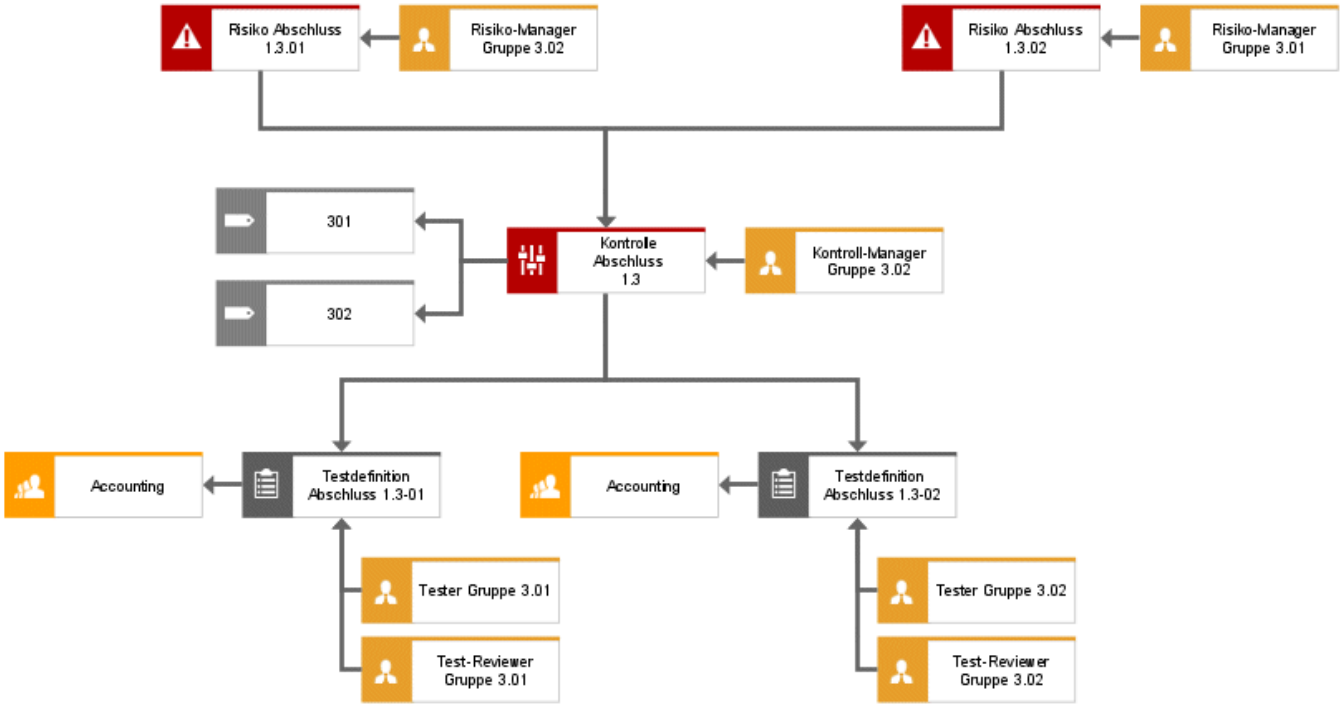

Abbildung 4: Struktur Business Controls Diagram

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
Kontrolle	betrifft	Fachbegriff	über diese Kante wird die Beziehung zu den Regularien 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.
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.
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.

4.4.1 Kontrolle

Die Kontrolle wird in ARIS mit dem Objekt **Funktion** (OT_FUNC) und dem Standardsymbol **Kontrolle** (ST_CONTR) modelliert. Für jede Kontrolle, für die das Attribut **ARCM-Synchronisation** gesetzt ist, wird eine Kontrolle in ARIS Risk & Compliance Manager angelegt. Eine Kontrolle muss eindeutig definiert sein und darf nicht wiederverwendet werden.

ZUORDNUNG 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 ermittelt und ein entsprechender Link zum Kontroll-Manager in ARIS Risk & Compliance Manager gespeichert
Kontrolle	Kontrollfrequenz	AT_AAM_CTRL_FREQUENCY		control	control_frequency	
Kontrolle	Kontrollausführung	AT_AAM_CTRL_EXECUTION_MANUAL AT_AAM_CTRL_EXECUTION_IT		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		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		control	controls	
Kontrolle	Kontrollziel	AT_AAM_CTRL_OBJECTIVE		control	control_objective	
Kontrolle	Key-Kontrolle	AT_AAM_KEY_CTRL		control	key_control	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Kontrolle	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		control	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.
				control	control_function	Wird über die Kante zur Funktion identifiziert. Ein entsprechender Link zum Prozesshierarchieelement in ARIS Risk & Compliance Manager wird gespeichert.

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
				control	testdefinitions	Wird über die Kante zur Testdefinition identifiziert. Ein entsprechender Link zur Testdefinition in ARIS Risk & Compliance Manager wird gespeichert.
			X	control	financial_statement	Wird über die Kante zum Fachbegriff identifiziert. Ein entsprechender Link zum Regularienhierarchieelement in ARIS Risk & Compliance Manager wird gespeichert.

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

4.4.2 Risiko

Risiken werden in ARIS mit dem Objekt **Risiko** (OT_RISK) 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. Eine Wiederverwendung von Risiken ist möglich.

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		risk	risktype	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARIS Risk & Compliance Manager gefüllt.
Risiko	Beschreibung/Definition	AT_DESC		risk	description	
Risiko	Auswirkung	AT_AAM_IMPACT		risk	impact	
Risiko	Wahrscheinlichkeit	AT_AAM_PROBABILITY		risk	probability	
Risiko	Risikokatalog 1	AT_AAM_RISK_CATALOG_1		risk	risk_catalog1	
Risiko	Risikokatalog 2	AT_AAM_RISK_CATALOG_2		risk	risk_catalog2	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Risiko	Titel 1 Titel 2 Titel 3 Titel 4	AT_TITL1- AT_TITL2- AT_TITL3- AT_TITL4-		risk	document: ▪ name ▪ title	Gibt die verlinkten Dokumente aus.
Risiko	Link 1 Link 2 Link 3 Link 4	AT_EXT_1- AT_EXT_2- AT_EXT_3- AT_LINK		risk	document: ▪ Link	Gibt die verlinkten Dokumente aus.
Risiko	ARIS Dokumentablage Titel 1 ARIS Dokumentablage Titel 2 ARIS Dokumentablage Titel 3 ARIS Dokumentablage Titel 4	AT_ADS_TITL1- AT_ADS_TITL2- AT_ADS_TITL3- AT_ADS_TITL4-		risk	document: ▪ name ▪ title	Gibt die verlinkten Dokumente aus.

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
Risiko	ARIS Dokumentablage link 1 ARIS Dokumentablage link 2 ARIS Dokumentablage link 3 ARIS Dokumentablage link 4	AT_ADS_LINK_1 AT_ADS_LINK_2 AT_ADS_LINK_3 AT_ADS_LINK_4		risk	document: ▪ Link	Gibt die verlinkten Dokumente aus.
				risk	controls	Wird über die Kante zur Kontrolle identifiziert. Ein entsprechender Link zur Kontrolle in ARIS Risk & Compliance Manager wird gespeichert.
				risk	manager_group	Wird über die Kante zur Rolle identifiziert. Ein entsprechender Link zum Risiko-Manager in ARIS Risk & Compliance Manager wird gespeichert.

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

4.4.3 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		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		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		testdefinition	testextend	

ARIS-Objekt	ARIS-Attribut	API-Name	M*	ARCM-Objekt	ARCM-Attribut	Anmerkungen
			X	testdefinition	owner_group	Wird über die Kante zur Rolle identifiziert. Ein entsprechender Link zum Tester in ARIS Risk & Compliance Manager wird gespeichert.
Testdefinition	Ereignisgesteuerte Testfälle erlaubt	AT_EVENT_DRIVEN_TESTS_ ALLOWED		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		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.
				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		testdefinition	isfollowup	

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

4.5 Allgemeine Modellierungsregeln

Kontrollen innerhalb der modellierten Business Controls Diagrams müssen eindeutig sein und dürfen in höchstens einem Business Controls Diagram ausgeprägt sein. Sie dürfen nur mit genau einer Funktion und mit mindestens einer Testdefinition verbunden sein.

Ein Risiko darf in höchstens einem Business Controls Diagram ausgeprägt sein. Ein Risiko kann mit mindestens einer Kontrolle verbunden sein, bei der das Attribut **ARCM-Synchronisation** gepflegt ist.

Eine Testdefinition muss innerhalb des modellierten Business Controls Diagram eindeutig sein und darf in höchstens einem dieser Diagramme ausgeprägt sein. Gleichzeitig darf eine Testdefinition nur mit exakt einer Kontrolle verbunden sein, bei der das Attribut **ARCM-Synchronisation** gepflegt ist.

4.5.1 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.

4.5.2 Sign-off

4.5.2.1 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 **wird durchgeführt an** zu den Kontrollen ermittelt, für die das Attribut **ARCM-Synchronisation** gesetzt ist.

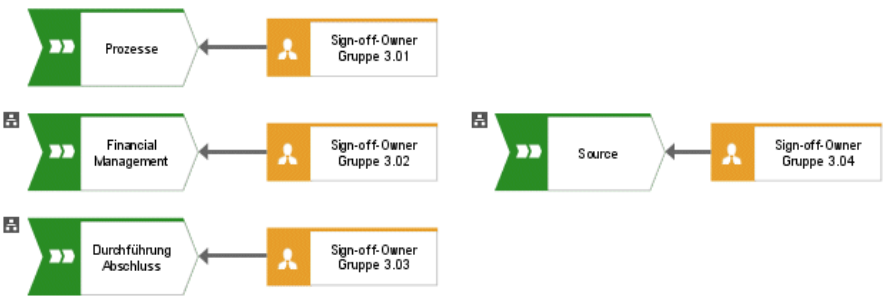

Abbildung 5: Zuordnung Funktion – Sign-Off-Owner-Gruppe

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

4.5.2.2 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.

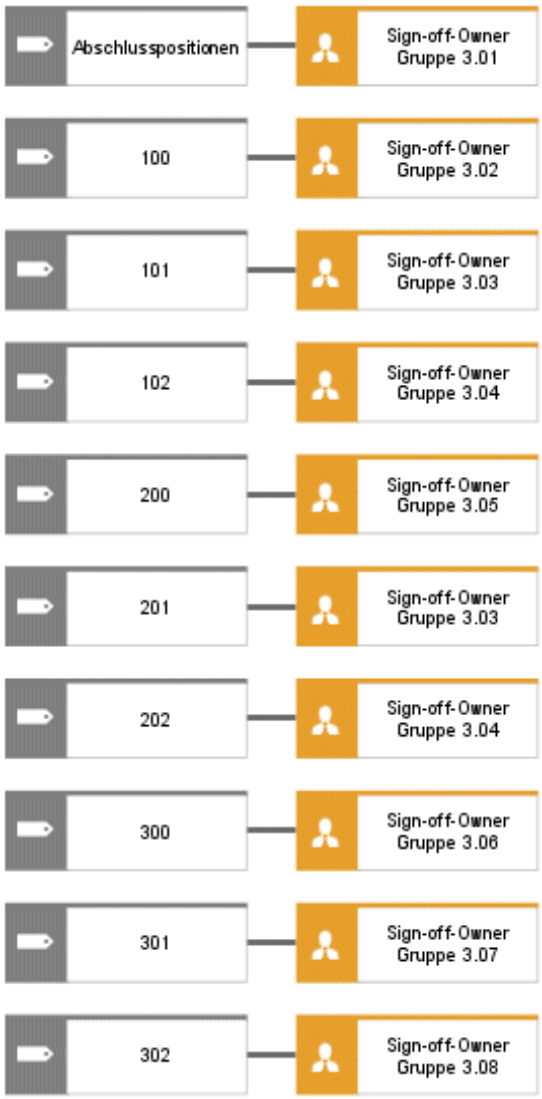

Abbildung 6: Zuordnung Regularien – Sign-Off-Owner-Gruppe

4.5.2.3 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.

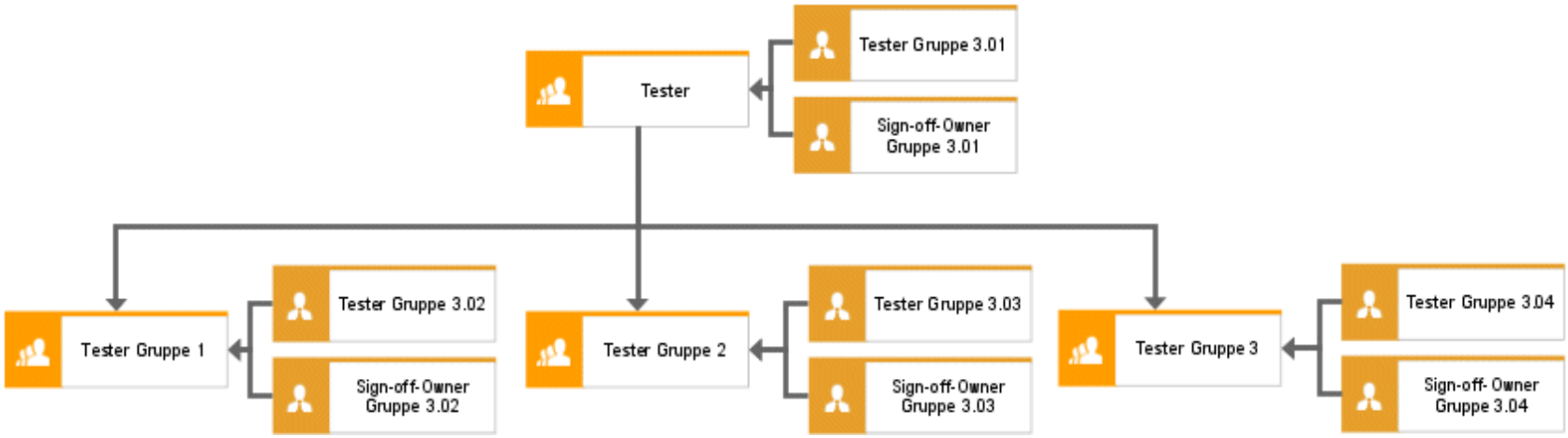

Abbildung 7: Zuordnung Organisationseinheit (Tester) – Sign-Off-Owner-Gruppe

4.5.2.4 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.

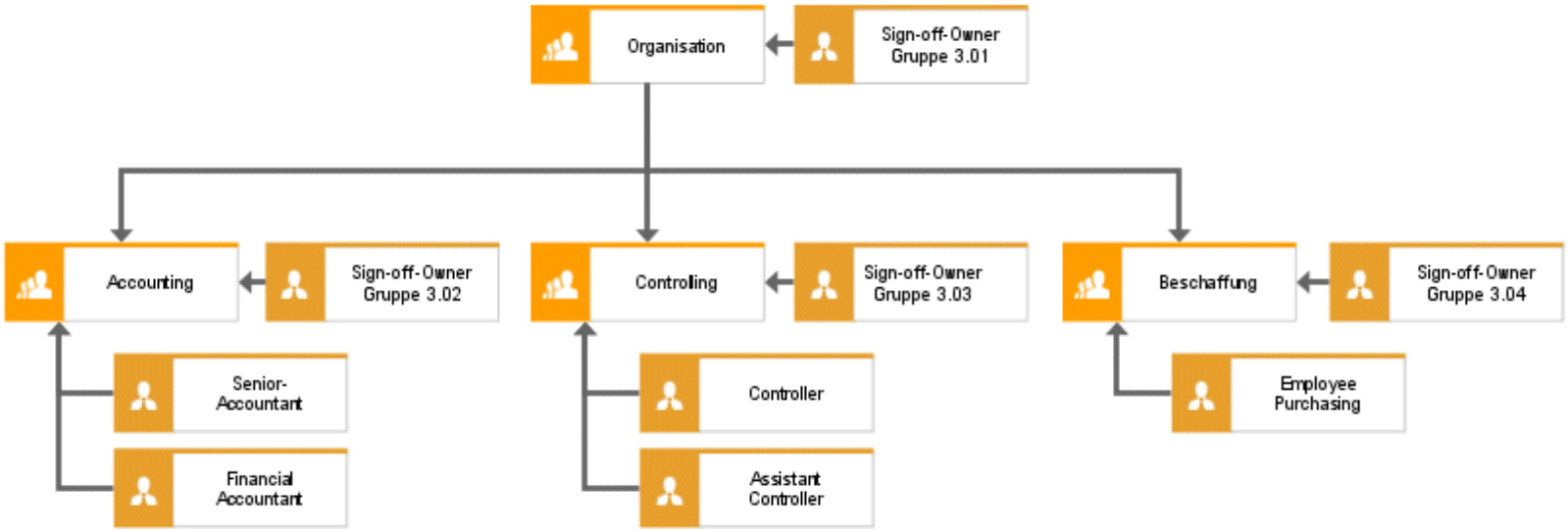

Abbildung 8: Zuordnung Organisationseinheit – Sign-Off-Owner-Gruppe

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.