Konventionenhandbuch kontrollbasiertes Kontrollsystem

ARIS Risk & Compliance Manager

Version 9.8 - Service Release 1

Juni 2015

Product Documentation

Dieses Dokument gilt für ARIS Risk & Compliance Manager ab Version 9.8. Hierin enthaltene Beschreibungen unterliegen Änderungen und Ergänzungen, die in nachfolgenden Release Notes oder Neuausgaben bekanntgegeben werden.

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 (ARCM) 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.

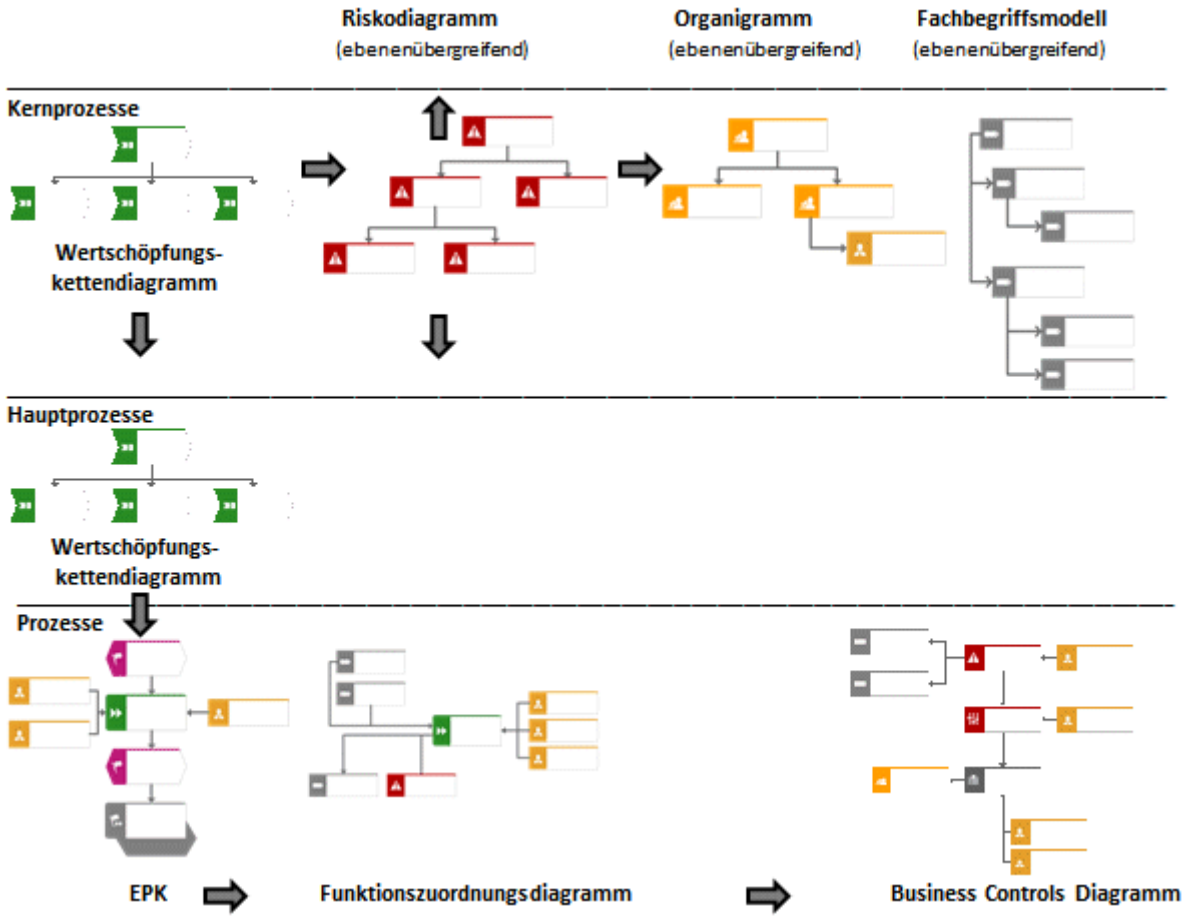

Abbildung 1: Modellierungsebenen und deren Modelltypen

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

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.

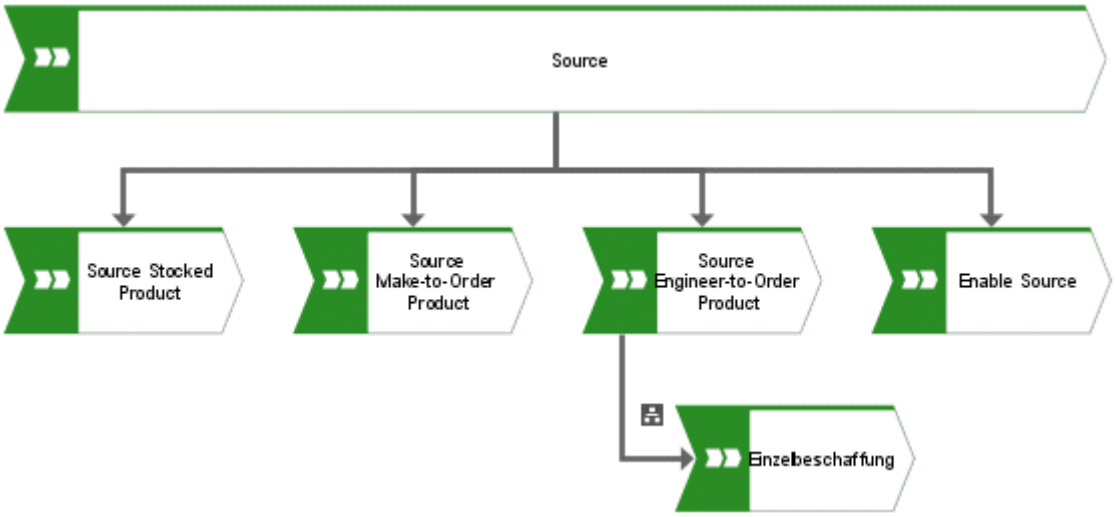

Abbildung 2: Ebene 1 – Wertschöpfungskettendiagramm

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 (ABA) zu Prozesshierarchieelement (ARCM)

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

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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.

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
				HIERARCHY	model_name	Name des Modells (s. o.)
Funktion	Objektverknüpfung	AT_AAM_OBJ_LINK		HIERARCHY	objectlink	
Funktion	GUID des Objekts			HIERARCHY	objectguid	
				HIERARCHY	children	Untergeordnete HE
				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 Ebene 2 - Wertschöpfungskettendiagramm (WKD)

Als Modell der Ebene 2 wird das Wertschöpfungskettendiagramm genutzt. Ebene 2 dient der Darstellung der Hauptprozesse und zur Abbildung des Zusammenhangs der auf Ebene 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 Ebene 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 u. a.) 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.

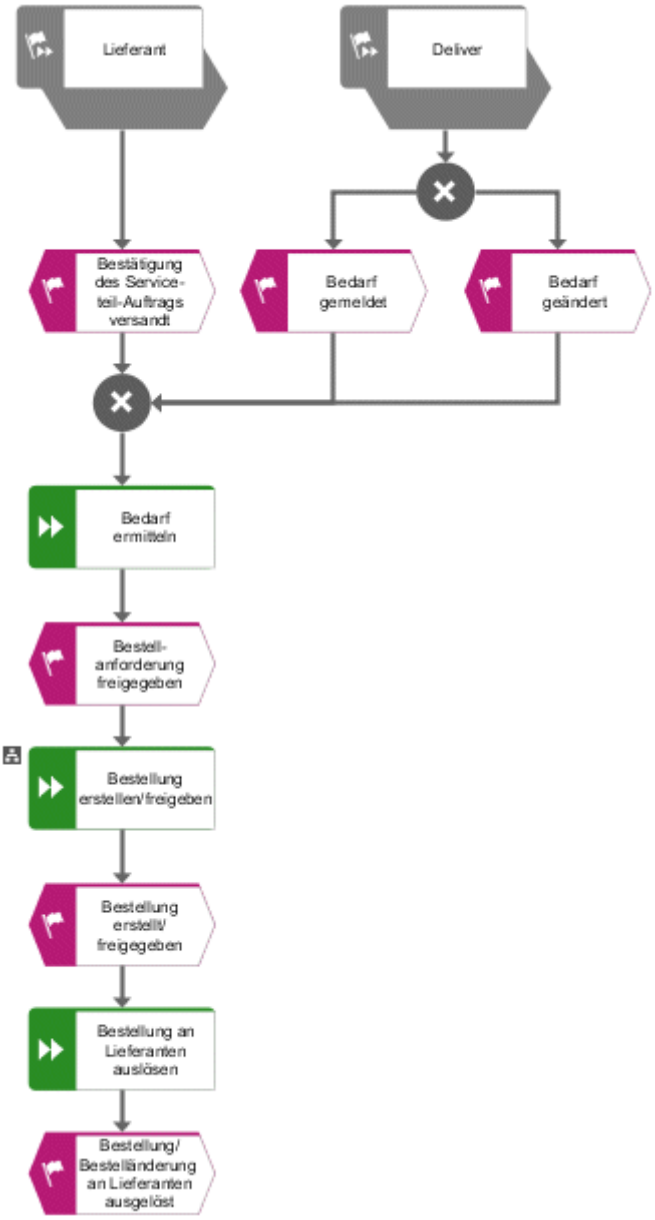

Abbildung 4: Ebene 3 – Ereignisgesteuerte Prozesskette

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

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

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. D. h. jedes Element der Hierarchie darf nur genau ein übergeordnetes Element besitzen.

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.

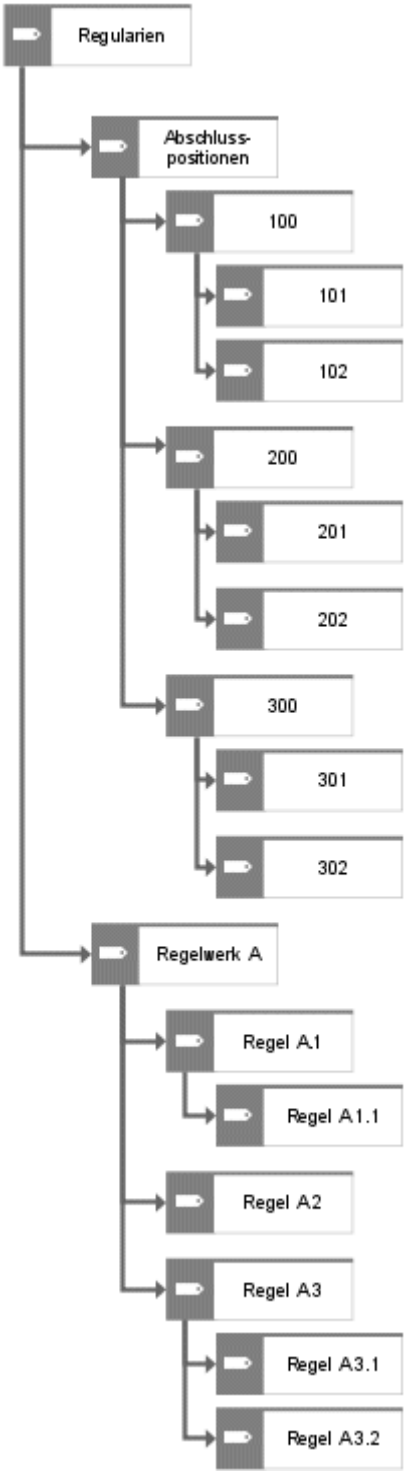

Abbildung 5: Struktur Regularienhierarchie

4.1.3.1.1 Zuordnungen Fachbegriff (ABA) zu Regularienelement (ARCM)

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

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
				HIERARCHY	model_name	Name des Modells (s. o.)
Fachbegriff	Objektverknüpfung	AT_AAM_OBJ_LINK		HIERARCHY	objectlink	
Fachbegriff	GUID des Objekts			HIERARCHY	objectguid	
				HIERARCHY	children	Untergeordnete HE
				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.

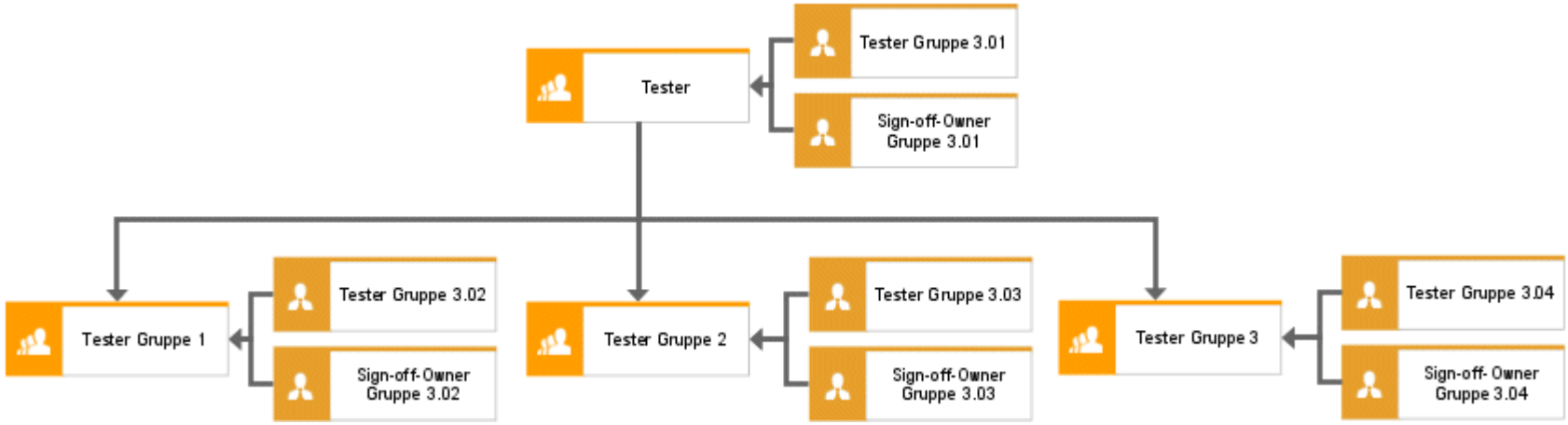

Abbildung 6: Struktur Testerhierarchie

Für jede Organisationseinheit wird somit ein Testerhierarchieelement in ARIS Risk & Compliance Manager angelegt (Ausnahme: Das oberste Hierarchieelement existiert bereits in ARCM). 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 (ABA) zu Testerhierarchieelement (ARCM)

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

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
				HIERARCHY	modelguid	GUID des Modells, in dem eine Ausprägung der Organisations-einheit vorkommt. Es wird das erste verfügbare Organi-gramm 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. Durch die Kante **ist übergeordnet** wird die Hierarchie zwischen den Objekten abgebildet.

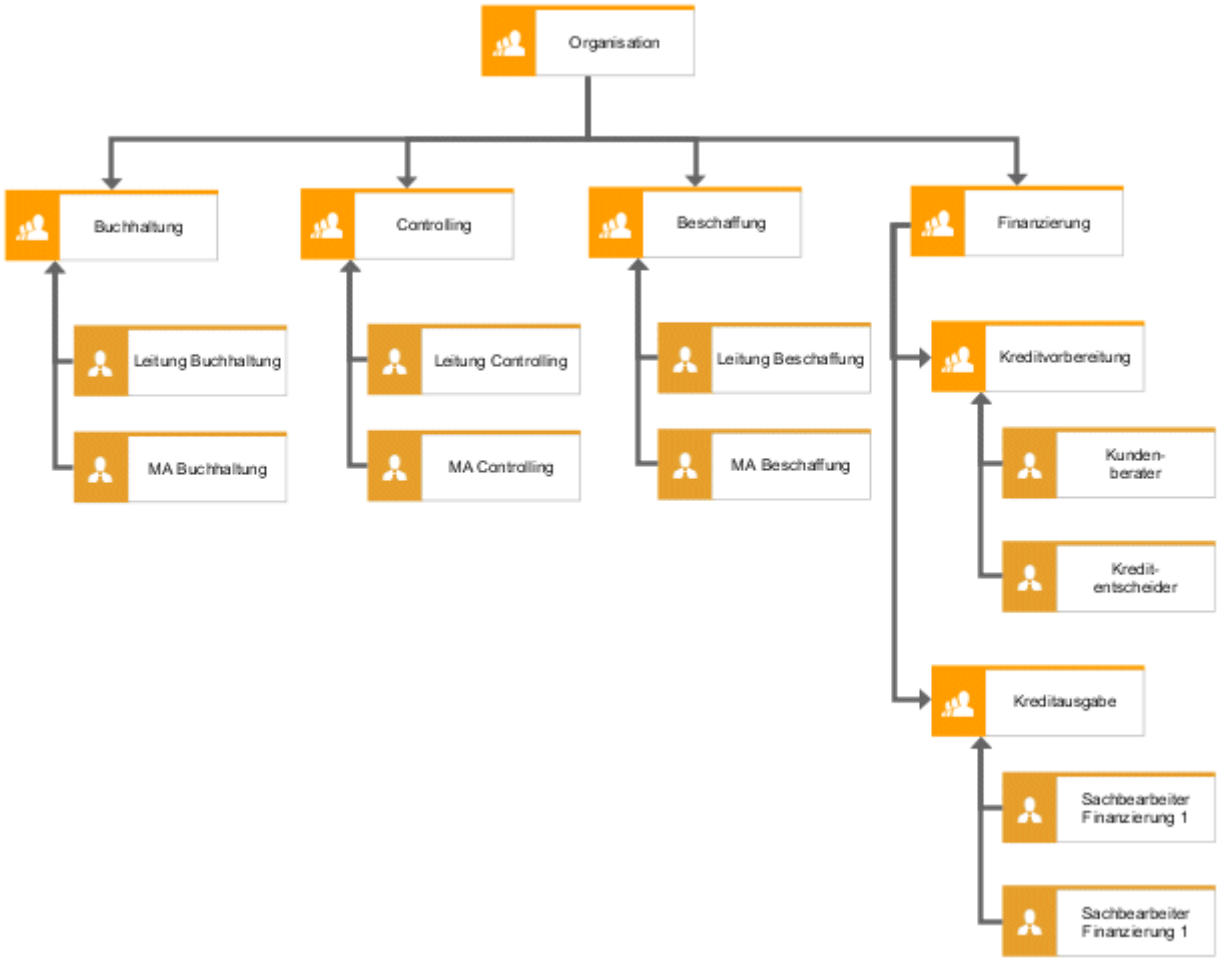

Abbildung 7: Struktur Organisationshierarchie

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 (ABA) zu Organisationshierarchieelement (ARCM)

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

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
				HIERARCHY	modelguid	GUID des Modells, in dem eine Ausprägung der Organisations-einheit vorkommt. Es wird das erste verfügbare Organi-gramm 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 Organisationshierar-chie 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.

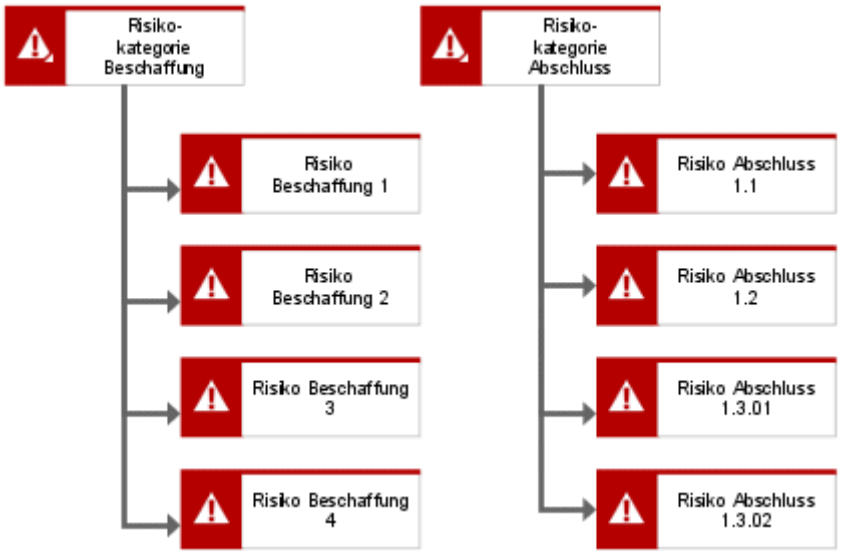

Abbildung 8: Struktur Risikohierarchie

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.

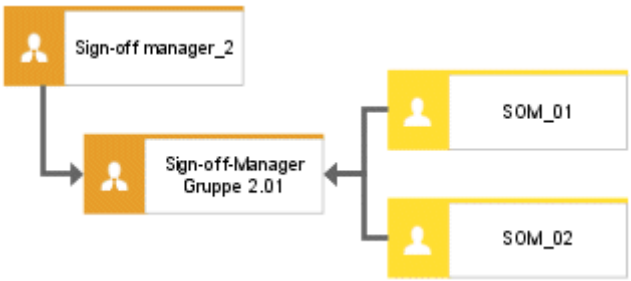

Abbildung 9: Struktur Benutzer/Benutzergruppen

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 die Ebene der zu generierenden Gruppe. <Rolle>_<Ebene>, d. h.: Sign-off manager_2 > Rolle: Sign-off-Manager, Ebene: 2 (bzw. mandantenspezifisch). Für die übergeordnete Rolle (in diesem Fall Sign-off manager_2) wird keine Benutzergruppe in ARIS Risk & Compliance Manager generiert.

Für die verschiedenen Ebenen gilt:

- Ebene 1: mandantenübergreifend

  Bedeutet, dass die Rechte mandantenübergreifend vergeben werden.
- Ebene 2: mandantenspezifisch

  Bedeutet, dass die Rechte für einen bestimmten Mandanten vergeben werden.
- Ebene 3: objektspezifisch

  Bedeutet, dass die Rechte für ein bestimmtes Objekt vergeben werden, z. B. Policy, Risiko oder Kontrolle.

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 der Ebene **2** (also mit mandantenübergreifenden Rechten) generiert. Zudem wird ein Benutzer mit der Benutzerkennung **SOM_01** generiert.

Mapping Rollenname (ARCM) zu Rolle (ABA)

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 (ABA)	Anmerkung
roles.testauditor	Test auditor	Ebene 1, 2 und 3
roles.testauditorexternal	Test auditor external	Ebene 1 und 2
roles.deficiencyauditor.l1	Deficiency auditor (L1)	Ebene 1 und 2
roles.deficiencyauditor.l2	Deficiency auditor (L2)	Ebene 1 und 2
roles.deficiencyauditor.l3	Deficiency auditor (L3)	Ebene 1 und 2
roles.deficiencymanager.l1	Deficiency manager (L1)	Ebene 1 und 2
roles.deficiencymanager.l2	Deficiency manager (L2)	Ebene 1 und 2
roles.deficiencymanager.l3	Deficiency manager (L3)	Ebene 1 und 2
roles.groupusermanager	Users/User groups manager	Ebene 1 und 2
roles.hierarchymanager	Hierarchy manager	Ebene 1 und 2
roles.riskmanager	Risk manager	Ebene 1, 2 und 3
roles.controlmanager	Control manager	Ebene 1, 2 und 3
roles.signoffmanager	Sign-off manager	Nur Ebene 2
roles.signoffreviewer	Sign-off reviewer	Nur Ebene 3
roles.signoffowner	Sign-off owner	Nur Ebene 3
Roles.testmanager	Test manager	Ebene 1 und 2
roles.testreviewer	Test reviewer	Nur Ebene 3
roles.tester	Tester	Nur Ebene 3
roles.issueauditor	Issue auditor	Ebene 1 und 2
roles.issuemanager	Issue manager	Ebene 1 und 2
roles.incidentauditor	Incident auditor	Ebene 1 und 2
roles.incidentmanager	Incident manager	Ebene 1 und 2
roles.incidentreviewer	Incident reviewer	Nur Ebene 3
roles.incidentowner	Incident owner	Nur Ebene 3
roles.lossauditor	Loss auditor	Ebene 1 und 2
roles.lossmanager	Loss manager	Ebene 1 und 2
roles.lossreviewer	Loss reviewer	Nur Ebene 3
roles.lossowner	Loss owner	Nur Ebene 3

4.1.4.1 Zuordnungen Rolle und Person

Zuordnungen Rolle (ABA) zu Benutzergruppe (ARCM)

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

ABA-Attribut	API-Name	ARCM-Attribut	M*	Anmerkung
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 (ABA) zu Benutzer (ARCM)

Bestehende Datenbanken nach alter Modellierungskonvention können mit dem mitgelieferten Report **ARCM user migration.arx** migriert werden. Da die beiden Attribute für Vor- und Nachname aus demselben Attribut abgeleitet werden, sollte das Ergebnis überprüft werden.

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

ABA-Attribut	API-Name	ARCM-Attribut	M*	Anmerkung
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 **Mandanten** wird über den Mandanten ermittelt, in den 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 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.

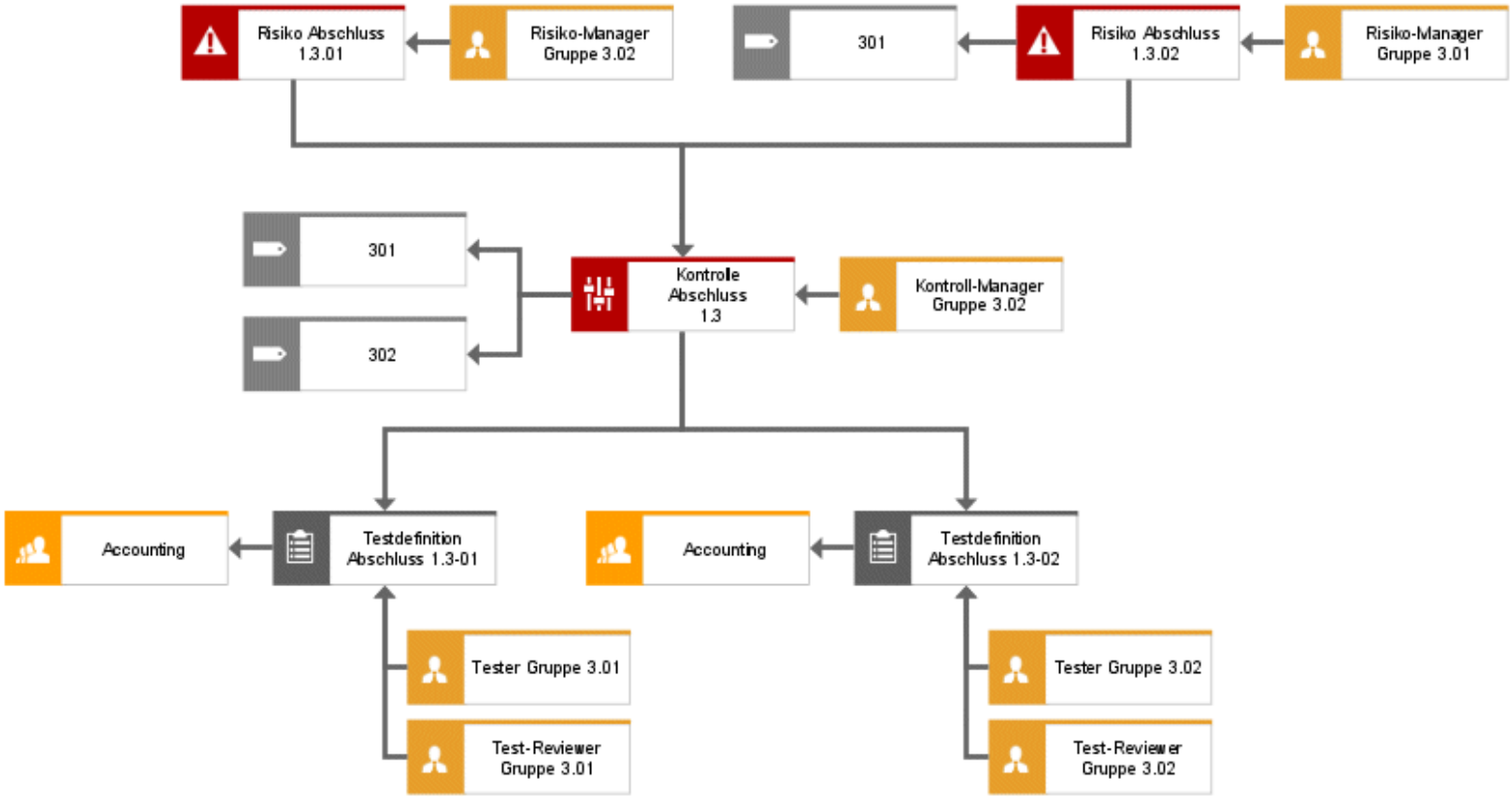

Abbildung 10: Struktur Business Controls Diagram

Die Zuordnung einer Risk-Manager Gruppe und einer Control-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	Anmerkung
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 zum einen die Beziehung zum Tester und zum anderen die Beziehung zum Test-Reviewer hergestellt

4.1.5.1 Kontrolle

Die Kontrolle wird in ARIS mit dem Objekt **Funktion** (OT_FUNC, ST_CONTR) modelliert. Für jede Kontrolle, welche das Attribut **Export-relevant** gesetzt hat, wird eine Kontrolle in ARIS Risk & Compliance Manager angelegt. Eine Kontrolle muss eindeutig definiert sein und darf nicht wiederverwendet werden.

Zuordnung Funktion (Kontrolle) (ABA) zu Control (ARCM)

Für das Objekt Funktion (Kontrolle) gelten folgende Zuordnungen:

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
Kontrolle	Name	AT_NAME	X	control	name	
Kontrolle	Kontroll-ID	AT_AAM_CTRL_ID		control	control_id	
				control	control_owner_group	Wird über die Kante zur Rolle ermittelt und ein entsprechender Link zum Kontroll-Manager in ARCM gespeichert
Kontrolle	Kontrollfrequenz	AT_AAM_CTRL_FREQUENCY	X	control	control_frequency	
Kontrolle	Kontrolldurchführung	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 ARCM gefüllt

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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 ARCM gefüllt
Kontrolle	Kontrollaktivität	AT_AAM_CTRL_ACTIVITY	X	control	controls	
Kontrolle	Kontrollziel	AT_AAM_CTRL_OBJECTIVE		control	control_objective	
Kontrolle	Key-Kontrolle	AT_AAM_KEY_CTRL	X	control	key_control	

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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	X	control	assertions	In Abhängigkeit der Werte, die True sind, wird die Enumeration in ARCM 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 ermittelt und ein entsprechender Link zum Prozess-Hierarchie-element in ARCM gespeichert
				control	testdefinitions	Wird über die Kante zur Testdefinition ermittelt und ein entsprechender Link zur Testdefinition in ARCM gespeichert

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
			X	control	financial_statement	Wird über die Kante zum Fachbegriff ermittelt und ein entsprechender Link zum Regularienhierarchie-element in ARCM gespeichert

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

4.1.5.2 Risiko

Risiken werden in ARIS mit dem Objekt **Risiko** (OT_RISK) modelliert. Für den Export in ARIS Risk & Compliance Manager sind nur die Risiken relevant, die an einer Kontrolle modelliert sind, die export-relevant ist. Eine Wiederverwendung von Risiken ist möglich.

Zuordnungen Risiko (ABA) zu Risiko (ARCM)

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

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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 ARCM gefüllt
Risiko	Beschreibung/ Definition	AT_DESC	X	risk	description	
Risiko	Auswirkung	AT_AAM_IMPACT	X	risk	impact	
Risiko	Wahrscheinlichkeit	AT_AAM_PROBABILITY	X	risk	probability	
Risiko	Risikokatalog 1	AT_AAM_RISK_CATALOG_1		risk	risk_catalog1	

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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 ARCM generiert und mit dem Risiko verlinkt
				risk	controls	Wird über die Kante zur Kontrolle ermittelt und ein entsprechender Link zur Kontrolle in ARCM gespeichert
				risk	risk_owner_group	Wird über die Kante zur Rolle ermittelt und ein entsprechender Link zum Risiko-Manager in ARCM gespeichert

*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 den Import in ARIS Risk & Compliance Manager sind nur die Testdefinitionen relevant, die an einer Kontrolle modelliert sind, welche Export-relevant ist.

Zuordnung Testdefinition (ABA) zu Testdefinition (ARCM)

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

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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 ARCM 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 ARCM gefüllt
Testdefinition	Testumfang	AT_AAM_TEST_SCOPE	X	testdefinition	testextend	

ARIS-Objekt	ARIS-Attribut	API-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
			X	testdefinition	test_owner_group	Wird über die Kante zur Rolle mit der Rolle Tester ermittelt und ein entsprechender Link zum Tester in ARCM gespeichert
Testdefinition	Ereignisgesteuerte Testfälle erlaubt	AT_EVENT_DRIVEN_TESTS_ ALLOWED	X	testdefinition	event_driven_allowed	Bei **true** wird die Test-definition nur für auto-matisierte Kontrolltests herangezogen. Gleich-zeitig muss die Testfre-quenz auf **ereignis-gesteuert** 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-Namen	M*	ARCM-Objekt	ARCM-Attribut	Anmerkung
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	test_reviewer	Wird über die Kante zur Rolle mit der Rolle Test-Reviewer ermittelt und ein entsprechender Link zum Test-Reviewer in ARCM gespeichert
			X	testdefinition	effected_orgunit	Wird über die Kante zum Organisationseinheit bzw. Gruppe, Stelle, Standort ermittelt und ein entsprechender Link zur betroffenen Organisationseinheit in ARCM 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_MOD

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 **Export-relevant** 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 **Export-relevant** gepflegt ist.

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 Ausgangsselektionsmenge der für den Export in ARIS Risk & Compliance Manager relevanten Funktionen wird über die Kante **wird durchgeführt an** zu den export-relevanten Kontrollen ermittelt.

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 Hierarchie der Regularien 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.

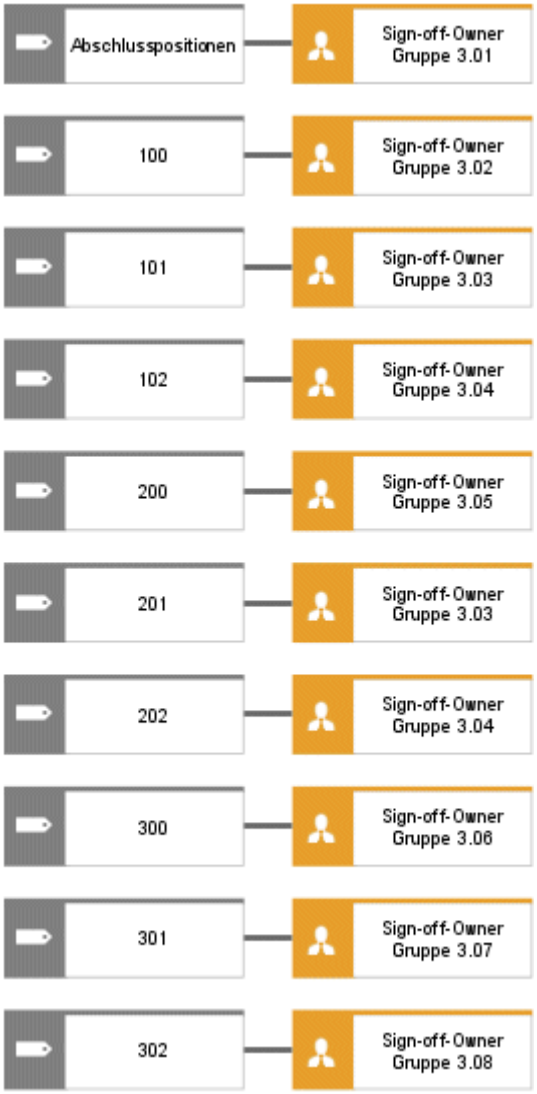

Abbildung 12: Zuordnung Regularien – Sign-Off-Owner-Gruppe

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.

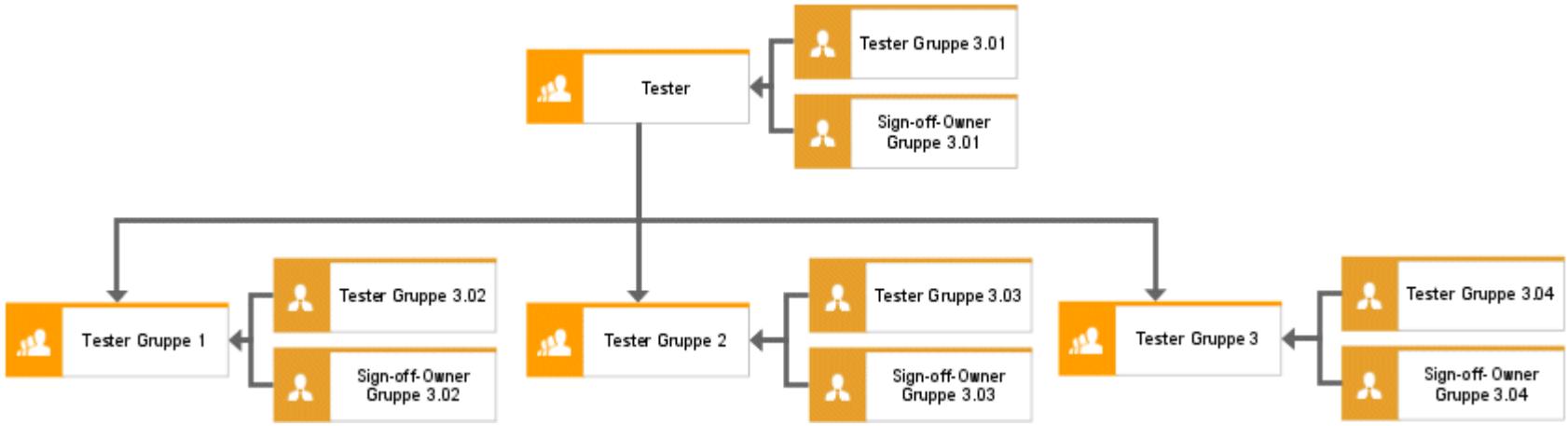

Abbildung 13: Zuordnung Organisationseinheit (Tester) – Sign-Off-Owner-Gruppe

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.

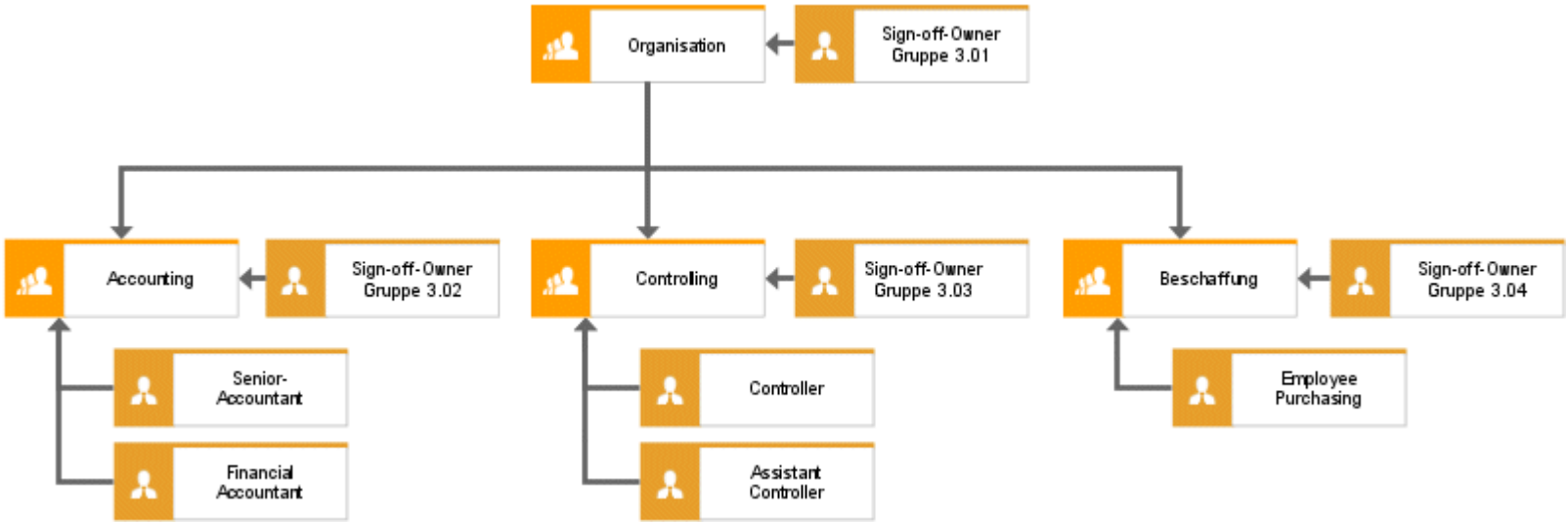

Abbildung 14: Zuordnung Organisationseinheit – Sign-Off-Owner-Gruppe

4.2 Deaktivierung von Objekten und Beziehungen

Die Objekte und Beziehungen in ARIS Risk & Compliance Manager unterliegen einer Versionierung, um eine Nachvollziehbarkeit von Änderungen zu gewährleisten. Objekte und Beziehungen werden in ARIS Risk & Compliance Manager daher nicht gelöscht, sondern deaktiviert. D. h., dass die entsprechenden Datenelemente nicht aus der Datenbank entfernt, sondern nur als deaktiviert gekennzeichnet werden.

Um Objekte/Beziehungen in ARIS Risk & Compliance Manager über einen Import zu deaktivieren, müssen die Objekte/Beziehungen in ARIS Architect entsprechend gekennzeichnet werden. Dies erfolgt über das Attribut **Deaktiviert** (AT_DEACT). Das Attribut kann sowohl für Objekte als auch für Kanten gesetzt werden. Sobald das Attribut gesetzt ist, wird das entsprechende Objekt bzw. die entsprechende Kante beim nächsten Import deaktiviert.

Dies ist natürlich nur der Fall, wenn die Objekte/Beziehungen Teil der Export-Datei von ARIS Architect sind. Nach erfolgreichem Import in ARIS Risk & Compliance Manager können Sie die Objekte/Kanten in ARIS Architect löschen. Wurden Objekten/Beziehungen in ARIS Architect vor einem Deaktivierungsimport gelöscht, können Sie diese manuell in ARIS Risk & Compliance Manager deaktivieren.