ARIS Risk & Compliance Manager

ADMINISTRATIONSHANDBUCH

Version 10.0 - Service Release 3

Dezember 2017

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

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 ARIS Risk & Compliance Manager

ARIS Risk & Compliance Manager ist eine Web-Anwendung. ARIS Risk & Compliance Manager verwendet Java-Servlets und Java-Server-Pages (JSP), die neben einer Java-Umgebung (JDK) einen Web-Container, d. h. Servlet-Container (Apache-TomEE) als Ablaufumgebung benötigen. Die Daten werden in einem relationalen Datenbanksystem gehalten und durch eine JDBC-Schnittstelle mit der Anwendung ausgetauscht. Zu Testzwecken können Sie ARIS Risk & Compliance Manager mit der Datenbank **Apache Derby** verwenden. Für den Produktivbetrieb benötigen Sie das Datenbanksystem **Oracle** oder **Microsoft®-SQL-Server**.

Falls es eine aktualisierte Version dieses Dokuments gibt, finden Sie diese hier: http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer (http://aris.softwareag.com/ARISDownloadCenter/ADCDocumentationServer)

3 Administration

3.1 Konfiguration des Event-Enabling in ARIS Risk & Compliance Manager

ARIS Risk & Compliance Manager bietet die Möglichkeit, Events von einem Messaging-Provider (Standard ist Universal Messaging) zu abonnieren und daraus in ARIS Risk & Compliance Manager definierte Objekte zu generieren, z. B. Testfälle. Die Steuerung durch Events wird während des Setups oder nachträglich über ARIS Cloud Controller konfiguriert.

Beispiele - Befehle für ARIS Cloud Controller

```
reconfigure arcm_m arcm.config.eventProviderActive="true"
reconfigure arcm_m arcm.config.eventProviderUrl="nsp://localhost:9000"
reconfigure arcm_m arcm.config.eventTypeStoreLocation="
C:/SoftwareAG/common/EventTypeStore"
reconfigure arcm_m arcm.config.eventConfigurationLocation="
C:/SoftwareAG/profiles/SPM/configuration"
reconfigure arcm_m
arcm.config.eventSecurityFilePath="C:/SoftwareAG/common/conf/event/routing/event
-routing-security.xml"
```

BEDEUTUNG DER PARAMETER

- **arcm.config.eventProviderActive**

  Zentrale Angabe zur Aktivierung des Event-Enabling. Ist der Wert false angegeben, wird der Service nicht gestartet. Bei true müssen die weiteren Parameter gültige Werte enthalten.

- **arcm.config.eventProviderUrl**

  Der Parameter muss die gültige URL einer Universal-Messaging-Server-Instanz enthalten, z. B. nsp://localhost:9000.

- **arcm.config.eventTypeStoreLocation**

  Der absolute Pfad zu einem lokal verfügbaren Event-Type-Store ist zu hinterlegen. Liegt die Instanz des Universal- Messaging-Servers auf demselben Host, kann der Store dieser Installation verwendet werden. Beispiel: C:\SoftwareAG\common\EventTypeStore

- **arcm.config.eventConfigurationLocation**

  Der absolute Pfad des Basisverzeichnisses einer spezifischen Event-Routing-Konfiguration wird benötigt. Liegt die Instanz des Universal-Messaging-Servers auf demselben Host, kann das Basiskonfigurationsverzeichnis dieser Installation verwendet werden. Beispiel: C:\SoftwareAG\profiles\SPM\configuration

- **arcm.config.eventSecurityFilePath**

  In diesem Parameter wird der absolute Pfad der Sicherheitskonfigurationsdatei erwartet. Bei identischem Host kann die Datei der Universal-Messaging-Server-Installation referenziert werden. Beispiel: C:\SoftwareAG\common\conf\event\routing\event-routing-security.xml

- **arcm.config.useDurableEventSubscriptions**

  Standardmäßig arbeitet das Event-Enabling mit dauerhaften Abonnements von Messages. Diese Funktionalität kann deaktiviert werden, indem dieser optionale Parameter auf den Wert false gesetzt wird.

UNTERSTÜTZE EVENT TYPEN

Um aus den Events in ARIS Risk & Compliance Manager definierte Objekte zu generieren, werden bestimmte vordefinierte Event-Typen mitgeliefert. Diese müssen in den lokalen Event Type Store und in den Event Type Store des Event-generierenden Systems kopiert werden. Die zugehörigen Dateien für den Event Type Store befinden sich im Hauptverzeichnis des Installationsmediums von ARIS Risk & Compliance Manager im Ordner **Event Type Store**. Der Inhalt dieses Ordners wird dann in das Hauptverzeichnis des jeweiligen Event Type Store kopiert.

Das Verschicken von Events mithilfe der in ARIS Risk & Compliance Manager mitgelieferten Event-Typen ist Bestandteil von Complex Event Processing. Weitere Informationen hierzu entnehmen Sie bitte der Dokumentation von Complex Event Processing.

BETRIEB EINER AUTARKEN INSTALLATION VON ARIS RISK & COMPLIANCE MANAGER

Liegen ARIS Risk & Compliance Manager und Universal-Messaging-Server nicht auf dem gleichen Host, können die benötigten Konfigurationen und Ressourcen nicht direkt referenziert und verwendet werden. In diesem Fall müssen die folgenden Ressourcen aus der Universal-Messaging-Server-Installation auf das Host-System der Installation von ARIS Risk & Compliance Manager kopiert werden. Zu kopierende Verzeichnisstrukturen (minimales Bundle*):

1. <SAG install directory>\common\conf\event\...
2. <SAG install directory>\common\EventTypeStore\...
3. <SAG install directory>\common\lib\...
4. <SAG install directory>\common\runtime\bundles\...
5. <SAG install directory>\profiles\SPM\configuration\event\routing\...

Anschließend können die kopierten Ressourcen wie zuvor beschrieben in der Event-Enabling-Konfiguration von ARIS Risk & Compliance Manager verwendet werden.

* Weiterführende Information zum Betrieb von Universal-Messaging, insbesondere die Konfiguration durch den Software AG Platform-Manager, entnehmen Sie bitte den produktspezifischen Dokumentationen.

Warnung

Um den fehlerfreien Betrieb und die Kompatibilität zu gewährleisten, achten Sie bitte darauf, die Version der kopierten Ressourcen der Installation von ARIS Risk & Compliance Manager immer mit der Version des verwendeten Universal-Messaging-Servers synchron zu halten.

3.2 Importieren von modellierten Benutzer ins User Management

Nach dem Import eines Datenbankexports aus ARIS Architect in ARIS Risk & Compliance Manager, sind alle importierten Benutzer zunächst deaktiviert. Sie können aktiviert werden, indem sie im User Management manuell angelegt und dann mit ARIS Risk & Compliance Manager synchronisiert werden (**Administration** > **Mit User Management synchronisieren**). Der Report **ARCM-Benutzerexport für das User Management** erledigt dies automatisiert, indem alle modellierten Benutzer einer Datenbank (Objekttyp **Person**) exportiert werden. Folgende Attribute eines Benutzers werden exportiert:

- Anmeldung
- Vorname
- Nachname
- E-Mail-Adresse

Der Report ermittelt außerdem, welches Lizenzrecht ein Benutzer benötigt. Dabei gelten folgende Regeln:

- Ist ein Benutzer keiner Benutzergruppe zugeordnet, wird ihm das Lizenzrecht **Contribute** zugeordnet. Benutzer ohne Gruppenzuordnung sind berechtigt, Aufgaben im Issue-Management wahrzunehmen.
- Ist ein Benutzer einer Benutzergruppe mit der Rolle Vorfall-Owner oder Policy-Addressee zugeordnet, wird ihm das Lizenzrecht **Contribute** zugeordnet.
- Bei allen anderen Rollenzuordnungen erhält der Benutzer das Lizenzrecht **Operate**.

3.2.1 Modellierte Benutzer aus ARIS Architect exportieren

Exportieren Sie die modellierten Benutzer aus ARIS Architect.

Voraussetzung

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

Vorgehen

1. Starten Sie **ARIS Architect**.
2. Öffnen Sie die Datenbank, deren modellierte Benutzer Sie für den Import in das User Management exportieren möchten.
3. Klicken Sie mit der rechten Maustaste auf die Hauptgruppe.
4. Klicken Sie auf **Auswerten > Report starten**.
5. Wählen Sie die Kategorie von **ARIS Risk & Compliance Manager**.
6. Wählen Sie den Report **ARCM-Benutzerexport für das User Management**.

7. Klicken Sie auf **Weiter**.
8. Wählen Sie die Ausgabeeinstellungen.
9. Klicken Sie auf **Fertigstellen**.

Eine Textdatei mit den Attributen Anmeldung, Vorname, Nachname sowie E-Mail-Adresse wird exportiert. Es werden die Benutzer angezeigt, die wegen fehlender Attribute vom Export ausgeschlossen wurden. Sie haben so die Möglichkeit, die benötigten Attribute einzutragen und durch erneutes Starten des Reports alle Benutzer zu exportieren.

Sie können die Benutzer jetzt in die User Management importieren. Die Verwaltung der Benutzer erfolgt für alle ARIS-Produkte zentral im User Management. Nicht zu verwechseln mit der Administration in ARIS Risk & Compliance Manager. Die Zuordnung der Benutzer zu Benutzergruppen erfolgt weiterhin in ARIS Risk & Compliance Manager. Detaillierte Informationen zu Export, Import und Synchronisation von Benutzern finden Sie im **ARIS Risk & Compliance Manager-Administrationshandbuch** (**Administration > Importieren von modellierten Benutzern in die User Management**). Detaillierte Informationen zur User Management finden Sie in der Hilfe der User Management.

3.2.2 Modellierte Benutzer ins User Management importieren

Importieren Sie die modellierten Benutzer ins User Management.

Vorgehen

1. Legen Sie das Installationsmedium von ARIS Risk & Compliance Manager in das Laufwerk.
2. Kopieren Sie die Datei **create_user.bat** aus dem Ordner **Content** in den Ordner **<ARCM-Installationsordner>\server\bin\work\work_umcadmin_s\tools\bin**.
3. Kopieren Sie die Textdatei, die Sie zuvor mit dem Report **ARCM-Benutzerexport für das User Management** erstellt haben in den gleichen Ordner.
4. Ersetzen Sie in der Datei **create_user.bat** den Eintrag **set INPUTFILE** mit dem entsprechenden Namen der Exportdatei.
5. Speichern Sie die Änderung.
6. Führen Sie die Datei **create_user.bat** aus. Sie können dabei ein Kennwort für alle importierten Benutzer vergeben. Möchten Sie kein Kennwort vergeben, drücken Sie die Eingabetaste ohne ein Kennwort einzugeben.

Die Benutzer werden ins User Management importiert.

3.2.3 Benutzer mit dem User Management synchronisieren

Sie können die Benutzer in ARIS Risk & Compliance Manager mit den Benutzern im User Management synchronisieren, um die Daten in ARIS Risk & Compliance Manager zu aktualisieren. Die Verwaltung der Benutzer erfolgt für alle ARIS-Produkte zentral im User Management. Nicht zu verwechseln mit der Administration in ARIS Risk & Compliance Manager. Die Zuordnung der Benutzer zu Benutzergruppen erfolgt weiterhin in ARIS Risk & Compliance Manager. Die Benutzergruppen des User Management entsprechen nicht denen in ARIS Risk & Compliance Manager.

Voraussetzung

Sie haben die Rolle **Benutzer-Manager**, **Benutzergruppen-Manager**, **Systemadministrator** oder **Umgebungsadministrator**.

Vorgehen

1. Klicken Sie auf **Administration**.
2. Klicken Sie unter **Funktionen > Mit User Management synchronisieren** auf **Synchronisieren**. Die Benutzerdaten in ARIS Risk & Compliance Manager werden durch die Daten aus dem User Management ersetzt. Dadurch werden Funktions- und Lizenzrechte, Namen, Kennwörter, E-Mail-Adressen usw. aktualisiert sowie Benutzer deaktiviert.

Der Dialog wird geschlossen. **Monitoring > Jobs und Importe/Exporte** wird angezeigt. Der Job wird unter **Wartende Jobs und Importe/Exporte** ausgegeben. Ist er abgeschlossen, wird er unter **Beendete Jobs und Importe/Exporte** aufgelistet. Die importierten Benutzer werden in ARIS Risk & Compliance Manager aktiviert.

3.3 Installation der ARIS Architect-Komponenten

Die Makros und Reporte für ARIS Risk & Compliance Manager sind Bestandteil der ARIS Server-Installation. Die Installation weiterer Komponenten entfällt dadurch.

3.4 Anbindung an einen Verzeichnisdienst (LDAP)

Anders als in den Vorgängerversionen wird LDAP nun nicht mehr direkt mit ARIS Risk & Compliance Manager verbunden. Stattdessen muss die LDAP-Anbindung im User Management konfiguriert werden. Informationen hierzu finden Sie im **ARIS Server-Installations- und -Administrationshandbuch** im Kapitel **Set up ARIS for LDAP server operation**.

3.5 Server von MashZone für die Dashboard-Integration vorbereiten

Sie können die Nutzung von MashZone/MashZone NextGen Business Analytics in ARIS Risk & Compliance Manager aktivieren, um Daten in Dashboards zusammenzuführen, zu kombinieren und anschaulich zu visualisieren. Dafür sind Änderungen an den Servereinstellungen von MashZone erforderlich. Für MashZone NextGen Business Analytics müssen diese Änderungen nicht durchgeführt werden.

Zwei unterschiedliche Instanzen des User Management können nicht parallel auf einem Computer laufen. Daher benötigen MashZone und ARIS Risk & Compliance Manager jeweils eine eigene Instanz. Die Dashboards von MashZone werden daher von einem anderen Server bereitgestellt, als die Oberfläche von ARIS Risk & Compliance Manager, in die sie eingebettet sind.

Die Umleitung von Inhalten aus MashZone zu anderen Systemen, wie ARIS Risk & Compliance Manager, ist zur Sicherheit standardmäßig in MashZone beschränkt auf die Option **SAMEORIGIN**, d. h. der MashZone-Server antwortet nur auf eigene Anfragen. Deshalb muss die Einschränkung **SAMEORIGIN** in der Datei web.xml deaktiviert werden. Detaillierte Informationen zu X-Frame-Optionen finden Sie hier (https://developer.mozilla.org/en-US/docs/Web/HTTP/X-Frame-Options).

Vorgehen

1. Öffnen Sie die Datei **web.xml** (<MashZoneInstallDir>\MashZoneNG\apache-tomee-jaxrs\webapps\mashzone\WEB-INF\web.xml).
2. Fügen Sie die Zeilen:

```
<init-param>
            <param-name>antiClickJackingEnabled</param-name>
            <param-value>false</param-value>
</init-param>
```

   in den folgenden Abschnitt ein. Das Ergebnis sollte nun so aussehen:

```
<filter>
       <filter-name>HTTP Header Security Filter</filter-name>

<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
       <init-param>
              <param-name>antiClickJackingEnabled</param-name>
              <param-value>false</param-value>
       </init-param>
              <init-param>
              <param-name>antiClickJackingOption</param-name>
              <param-value>SAMEORIGIN</param-value>
       </init-param>
       <init-param>
              <param-name>hstsEnabled</param-name>
              <param-value>true</param-value>
       </init-param>
       <init-param>
              <param-name>hstsMaxAgeSeconds</param-name>
              <param-value>604800</param-value>
       </init-param>
</filter>
```

3. Speichern Sie ihre Änderungen.
4. Starten Sie den Server von MashZone erneut.

Der Server von MashZone ist für die Dashboard-Integration vorbereitet.

3.6 Verwendung der SAML2-Authentifizierung für Dashboard-Verbindungen

Die SAML2 Single Sign-On-Authentifizierung wird von MashZone NextGen Business Analytics seit dem 9.12-Release unterstützt. Um diese Authentifizierung für Dashboard-Verbindungen in ARIS Risk & Compliance Manager verwenden zu können, werden zusätzliche Konfigurationen und Einstellungen für die SAML2-Unterstützung in User Management benötigt. Detaillierte Informationen über die SAML2-Konfiguration finden Sie in der User Management-Dokumentation.

3.7 Anbindung an ARIS Publisher

Sie können eine Verbindung von ARIS Risk & Compliance Manager zu ARIS Publisher herstellen, um Objekte und Modelle aus ARIS Publisher in ARIS Risk & Compliance Manager anzuzeigen. Gemäß dem empfohlenen Vorgehen sollten die Stammdaten (Benutzer, Risiken, Kontrollen, usw.) in ARIS Architect modelliert werden. Nach der Modellierung können diese Daten mit dem Export-Report von ARIS Risk & Compliance Manager exportiert und in ARIS Risk & Compliance Manager importiert werden. Zusätzlich ist es möglich die Datenbank von ARIS Architect mit ARIS Publisher zu veröffentlichen. Nach dem Import der Stammdaten in ARIS Risk & Compliance Manager kann über die Umgebungen die Anbindung an ARIS Publisher konfiguriert werden. Dadurch kann z. B. in ARIS Risk & Compliance Manager von einem Risikoformular auf das Objekt im veröffentlichten Modell verlinkt werden, um den Prozess in ARIS Publisher anzuzeigen.

Voraussetzung

ARIS Risk & Compliance Manager und ARIS Publisher verwenden das gleiche User Management zur Verwaltung von Benutzern. Das User Management für alle ARIS-Produkte, nicht zu verwechseln mit der Administration in ARIS Risk & Compliance Manager, dient zur Verwaltung von Benutzern, Benutzergruppen, Funktions- und Lizenzrechten, Lizenzen, Dokumenten und Konfigurationen. Damit ist die einmalige Anmeldung für verschiedene ARIS-Produkte gewährleistet.

Vorgehen

USER MANAGEMENT

1. Öffnen Sie das User Management.
2. Legen Sie im User Management eine Benutzergruppe und einen Benutzer an.
3. Ordnen Sie dem Benutzer diese Benutzergruppe zu.
4. Ordnen Sie der Benutzergruppe das Funktionsrecht **Publisher-Administrator** zu.

ARIS ARCHITECT

1. Starten Sie **ARIS Architect**.
2. Klicken Sie auf **ARIS > Administration**. Die **Administration** wird angezeigt.
3. Melden Sie sich an der Datenbank an, die Sie exportieren möchten.
4. Klicken Sie in der Navigation auf **Benutzer**. Die Benutzer und Benutzergruppen werden angezeigt.
5. Klicken Sie mit der rechten Maustaste auf die zuvor erstelle Benutzergruppe.
6. Klicken Sie auf **Eigenschaften**.
7. Klicken Sie auf **Funktionsrechte**.
8. Aktivieren Sie das Kontrollkästchen für das Recht **Datenbankexport**. (Die produktspezifischen Berechtigungen werden nicht zentral im User Management zugewiesen, sondern im jeweiligen ARIS-Produkt.)
9. Klicken Sie auf **Zugriffsrechte**.
10. Ordnen Sie der Benutzergruppe mindestens das Zugriffsrecht **Lesen** für die Hauptgruppe zu.

11. Klicken Sie auf **Rechte vererben**, um die Rechte auf alle Untergruppen zu übertragen.
12. Klicken Sie auf **OK**.
13. Veröffentlichen Sie die gewünschte Datenbank.
14. Ändern sie nach dem Export den Status auf **Aktiviert**.

ARIS PUBLISHER

1. Öffnen Sie ARIS Architect.
2. Melden Sie sich mit dem Benutzer **root** und dem Kennwort **root** an.
3. Öffnen Sie das Modul **Gruppen**. Die von Ihnen angelegte Benutzergruppe wird angezeigt.
4. Klicken Sie in der Zeile der Gruppe auf **Zuordnen**. Der Dialog wird geöffnet.
5. Ordnen Sie die zuvor im User Management angelegt Gruppe ARIS Publisher zu.
6. Klicken Sie auf **Speichern**.

ARIS PUBLISHER-INTEGRATION IN ARIS RISK & COMPLIANCE MANAGER AKTIVIEREN

Voraussetzung

Sie haben die Rolle **Systemadministrator**.

1. Öffnen Sie ARIS Risk & Compliance Manager.
2. Klicken Sie auf **Administration**.
3. Klicken Sie unter **Systemmanagement** auf **Umgebungen**.
4. Klicken Sie auf den Namen der gewünschten Umgebung.
5. Klicken Sie unter **Einstellungen für die Integration von ARIS Publisher** auf **Ja**.
6. Tragen Sie im Feld **Objektverknüpfung** den ARIS Publisher-Link in folgender Form ein:

   http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>&localeid=1033&ph=<exportID>&objectguid={GUID}
7. Ersetzen Sie die Platzhalter folgendermaßen:
   a. **<BusinessPublisherServer>** = Name oder IP-Adresse des ARIS Publisher Servers.
   b. **<Benutzername>** = Name des Benutzers, der zuvor angelegt wurde.
   c. **<Kennwort>** = Kennwort des Benutzers, der zuvor angelegt wurde.
   d. **<exportID>**
      1. Öffnen Sie ein Modell in ARIS Publisher.
      2. Klicken Sie mit der rechten Maustaste auf ein Objekt.
      3. Klicken Sie auf **Link kopieren**.
      4. Kopieren Sie im angezeigten Link den Parameter **ph** mit seinem Wert und ersetzen Sie damit **<exportID>**.

   Der Platzhalter **{GUID}** muss nicht ersetzt werden. Dieser wird von ARIS Risk & Compliance Manager dynamisch ersetzt.
8. Tragen Sie in das Feld **Modellverknüpfung** den zuvor angelegten Link in der folgenden Form ein und ersetzen Sie den Parameter **objectguid** durch **modelguid**:

http://<BusinessPublisherServer>:19990/businesspublisher/link.do?login=<Benutzername>&password=<Kennwort>localeid=1033&ph=<exportID>&modelguid={GUID}

9. Ersetzen Sie die Platzhalter.
10. Klicken Sie auf **Speichern**.

Die ARIS Publisher-Integration wird aktiviert.

TEST DURCHFÜHREN

1. Melden Sie sich bei ARIS Risk & Compliance Manager mit der Rolle **Test-Manager** an.
2. Öffnen Sie ein Risiko, welches durch den Stammdatenimport generiert wurde.
3. Klicken Sie in der Zeile **Funktion** auf **Objektverknüpfung** und **Modellverknüpfung**.

ARIS Publisher wird in einem neuen Fenster geöffnet. Das entsprechende Objekt oder Modell wird geöffnet, wenn die Anbindung korrekt konfiguriert wurde.

3.8 Runnable über ARIS Cloud Controller sichern und rücksichern

ARIS Risk & Compliance Manager ermöglicht das Generieren und Rücksichern von Datenbankschnappschüssen direkt aus der Web-Anwendung. Die ARIS Cloud Controller (ACC)-Funktionalität zum Sichern und Rücksichern von Mandanten ist zusätzlich zum Generieren von Runnable-Sicherungsdateien verwendbar, die einen Datenbankschnappschuss sowie alle angewandten individuellen Anpassungen enthalten. Nähere Informationen finden Sie im Handbuch von ARIS Cloud Controller, Kapitel **Back up a tenant** und **Restore a tenant**.

3.9 Runnable über ARIS Tenant Management sichern und rücksichern

ARIS Tenant Management erlaubt die Sicherung und Rücksicherung mandantenspezifischer Daten von ARIS Risk & Compliance Manager. Die erzeugten Runnable-Sicherungsdateien enthalten einen Datenbankschnappschuss sowie alle angewandten individuellen Anpassungen. Nähere Informationen finden Sie im **ARIS Tenant Management Handbuch**.

Hinweis: Bei der Rücksicherung mandantenspezifischer Daten über ARIS Tenant Management müssen die Sicherungsdateien dieselben individuellen Anpassungen enthalten wie die angewandten Exemplare von ARIS Risk & Compliance Manager. Ist dies nicht der Fall, sind die individuellen Anpassungen für die entsprechenden Exemplare manuell anzuwenden.

4 Glossar

Global Unique Identifier (GUID)

Eindeutiger, datenbankübergreifender Identifizierer für Elemente von ARIS.

Java Database Connectivity (JDBC)

Schnittstelle, die die Kommunikation zwischen einer Java-Anwendung und einer Datenbank ermöglicht.

Multi-Purpose Internet Mail Extensions-Mapping (MIME-Mapping)

Verbindet eine Dateinamenerweiterung mit dem Typ der Datendatei, z. B. Text, Audio, Bild.

Service-ID von Oracle (SID)

Eindeutige Kennung, die Oracle benötigt, um die Datenbankinstanz zu identifizieren.

Simple Mail Transfer Protocol (SMTP)

Übertragungsprotokoll speziell für den Austausch von Mails. Es legt beispielsweise fest, wie zwei Mailsysteme interagieren und wie die Steuermeldungen zu diesem Zweck aussehen müssen.

5 Disclaimer

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

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

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

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

6 Support von Software AG

IM WEB

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

Klicken Sie auf **https://empower.softwareag.com/** (**https://empower.softwareag.com/**).

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

7 Index