**Glossar des Access Risk Control Tools**

**Generelle Begrifflichkeiten:**

**ERP-System** (Enterprise Resource Planning): Software-System zur Resourcenplanung eines Unternehmens, zusätzlich Unterstützung des gesamten Geschäftsprozessablaufs

**SAP**: Hersteller des bekanntesten **ERP**-Systems

**SUIM: SAP** User Information System

**ABAP**: Advanced Business Application, proprietäre Sprache von SAP

**OS**: Betriebssystem

**Compliance-Verstoß**: Verstoße gegen die Regelkonformität

**GDPR**: General Data Protection Regulation der EU

**RFC**: Remote Function Call

**SoD**: Funktionstrennungskonflikte

**JCo**: Java Connector für **SAP**

**UML**: Unified Modelling Language, wird in der Informatik zum Modellieren von System verwendet

**API**: Application Programming Interface

**JRE**: Java Runtime Environment

**Mock-Ups**: Visueller Systementwurf

**KMU**: Kleinere Mittelständische Unternehmen

**Design Pattern**: Bewährte Lösungsansätze für gewisse Problemstellungen

**Repository**: Gemeinsames Verzeichnis zur Ablage von Daten

**Positives Berechtigungskonzept**: Vergabe von Berechtigungen durch den Administrator

**ART**: Access Risk Control Tool / Access Risk Tool

**SAP\_ALL**: „Admin“-Berechtigungen bei SAP

**Datenobjekte des ART:**

**AccessPattern**: Berechtigungen, die das eigentlich verbotene Ausführen von bestimmten Aktionen erlauben, besteht entweder aus mehreren Pattern- oder einer ProfileCondition

**PatternCondition**: Enthält mehrere Authorization-Objects

**ProfileCondition**: Enthält ein Profil Profil: Ein Berechtigungsprofil, bspw. SAP\_ALL

**Authorization-Object**: Enthält mehrere Berechtigungsfelder mit jeweils bis zu 4 Attributen

**Whitelist**: Liste von Benutzern, die das Tool nicht abgleichen soll

**Configuration**: Enthält mindestens ein AccessPattern und optional eine Whitelist

**SAP-Configuration**: Verbindungsdaten, um auf ein SAP-System zugreifen zu können

**CriticalAccessQuery**: Enthält die Configuration, die SAP-Configuration und die CriticalAccessEntries einer Abfrage

**CriticalAccessEntry**: Tupel aus Benutzername und AccessPattern, gegen das verstoßen wird

**Benutzerrollen des ART:**

**Configurator**: Berechtigungen zum Erstellen/Löschen/Bearbeiten von SAP-Systemen, Erstellen/Löschen/Bearbeiten von Konfigurationen und Erstellen/Löschen/Bearbeiten von Whitelists bzw. AccessPatterns

**Viewer**: Berechtigung, eine CriticalAccessQuery zu starten, sowie die Ergebnisse älterer CriticalAccessQueries anzusehen und Ergebnisse zu exportieren

**Admin**: Berechtigung zum Erstellen/Löschen/Bearbeiten von Benutzern im ART