# *Messung der Rollenqualität*

**Role Based Access Control (RBAC) liegt im Trend. Unternehmen führen RBAC ein oder arbeiten bereits mit einer rollenbasierten Administration. Nun stellen sich verstärkt Fragen nach der Qualität der Rollen. Dieser Artikel beschäftigt sich mit den Fragen, wie Rollenqualität erreicht, gemessen und bewahrt werden kann.**

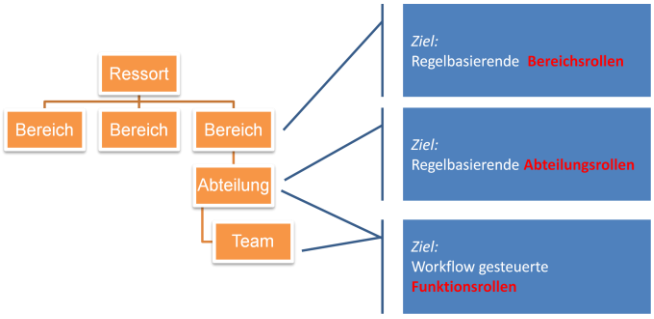
## Definition Rollenqualität

Was heisst Rollen-Qualität? Im Wesentlichen geht es darum, dass eine Rolle sämtliche zur Ausübung einer bestimmten Tätigkeit (Funktion) erforderlichen, Berechtigungen beinhaltet. Wichtig dabei ist es, den Anwendungszweck (Scope) einer Rolle so zu definieren, dass sie klar einem Prozess resp. einer Tätigkeit/Aufgabe oder Funktion zugeordnet werden kann. Ebenso müssen Compliance Vorgaben, wie z.B. Segregation of Duties (SoD) bei der Bildung der Rolle berücksichtigt werden.

## Erreichen der Rollenqualität

Um die geforderte Qualität in den Rollen zu erreichen, ist ein strukturiertes, methodisches Vorgehen vorausgesetzt. Im ersten Schritt muss bestimmt werden, wie das Rollenmodell aussehen soll.

*Beispiel eines Rollenmodells:*




Bei der Umsetzung (Identifikation und Modellierung) der Rollen garantiert ein schrittweises Vorgehen die benötigte Rollenqualität. In der Praxis kann dieses Vorgehen folgendermassen aussehen:

1. Prozessanalyse und Rollenidentifikation
2. Fachliche Beschreibung der Rolle (Scoping)
3. Identifikation von Vorgaben (z.B. SoD)
4. Festlegen der benötigten Zugriffe (z.B. durch Role Mining)
5. Validierung / Test / Bereinigung
6. Transition / Überführung in Produktion

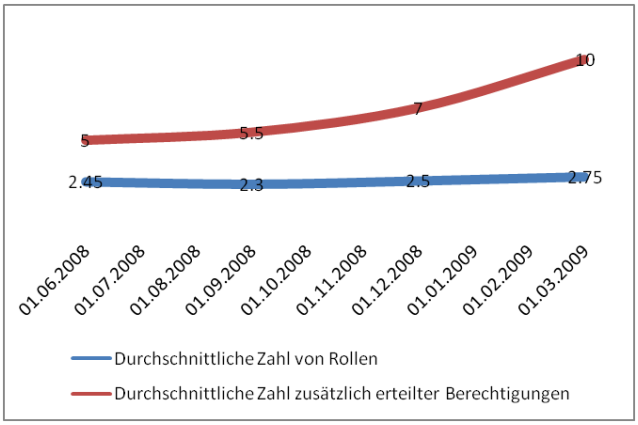
Entscheidet man sich für einen Bottom-Up Ansatz für das Festlegen der benötigen Berechtigungen einer Rolle, helfen Role-Engineering Tools wie **rol**mine®, welche den Prozess der Rollenbildung unterstützen. Ebenso sind auch Datenqualität- und Aktualität, Kenntnisse über die Berechtigungen sowie Organisations- und Prozessverständnis notwendig, um eine ausreichende Rollenqualität zu erreichen.

## Messen der Rollenqualität

Die Qualität bestehender Rollen und somit eines gesamten Rollen-Katalogs lässt sich aus unterschiedlichen Gesichtspunkten beurteilen. Für die Beurteilung müssen Unternehmen mit der Einführung der Rollen klare Messwerte festlegen. So lassen sich abnehmende Qualität und erforderlicher Handlungsbedarf frühzeitig erkennen.

### *Mitarbeiterbezogene Kriterien*

- Durchschnittliche Zahl an zusätzlich vergebenen Berechtigungen
- Durchschnittliche Zahl zugeteilter Rollen




Bei den mitarbeiterbezogene Kriterien definiert nicht primär das Einhalten eines im Voraus festgelegten, absoluten Durchschnittswerts die Qualität, sondern der Entwicklungs-Trend.

Zeichnet sich ab, dass die Zahl der zusätzlich vergebenen Einzelrechte pro Mitarbeiter (oder insgesamt) steigt, ist dies ein Indiz dafür, dass die Rollen geprüft und überarbeitet werden sollten. Es ist zu vermuten, dass die Rollen nicht alle, zur Ausübung einer Tätigkeit benötigten Berechtigungen beinhalten. Eine steigende Zahl von Rollen pro Mitarbeiter lässt darauf schliessen, dass im Unternehmen eher neue Rollen gebildet als Erweiterungen bestehender Rollen geprüft werden. Oder aber, dass bei veränderten Tätigkeiten eins Mitarbeiters neue Rollen zwar zugeteilt, nicht mehr benötigte Rollen aber nicht entzogen werden.

***Katalogbezogene Kriterien***

- Gesamtzahl der Rollen
- Anzahl Berechtigungen pro Rolle
- Anzahl Mitarbeiter pro Rolle
- Anzahl von Ausnahmeregeln (pro Rolle / über den gesamten Katalog)
- Anzahl von Verstössen

Häufig stellt sich die Frage, wie viele Rollen für ein Unternehmen optimal sind. Zu viele Rollen sind unübersichtlich und erhöhen den Administrationsaufwand. Gibt es zu wenige (klare Rollen) wird die Vergabe von Einzelberechtigungen gefördert oder das Risiko zu unrecht vergebender Berechtigungen/Rollen erhöht. Dieser Umstand wird als Rollenparadox bezeichnet. Zwar reduziert sich der Aufwand für die Administration der Rollen, jedoch steigt die Zahl der Ausnahmen, deren Überprüfung wieder zu erheblichem Mehraufwand führt.

Je mehr Berechtigungen einer Rolle zugewiesen (und im Idealfall auch automatisch provisioniert werden können), desto geringer sind die manuellen Eingriffe in der Berechtigungsadministration. Damit reduzieren sich der Aufwand für die Berechtigungsvergabe und -Kontrolle aber auch die Fehlerhäufigkeit bei der Berechtigungszuteilung.

Die Abgrenzung der Rollen zueinander hat starken Einfluss auf die Anzahl Mitarbeiter, welche einer Rolle zugewiesen werden können. Eine zu enge Abgrenzung führt dazu, dass viele Rollen nur für wenige Mitarbeiter anwendbar sind und insgesamt eine hohe Zahl von Rollen benötigt wird. Dies führt zu erhöhten Kosten in der Rollen-Administration.

Gibt es zu den definierten Rollen eine grosse Zahl von Ausnahmeregeln (oder –Bewilligungen), ist dies weiter ein Indiz für, dass der Scope der einzelnen Rollen nicht eindeutig ist oder sich die Rollen untereinander zu wenig abgrenzen. In diesem Fall genügt das Rollenmodell den betrieblichen Anforderungen nicht und eine Überarbeitung der Rollenstrukturen muss geprüft werden.

Zur Messung der Katalog-Qualität sind zu den genannten KPI's SOLL Werte zu definieren. Mit der periodischen Überprüfung ist es möglich, Trends zur Qualität des Rollenkatalogs zu erfassen und geeignete Massnahmen einzuleiten.

***Rollenspezifische Qualitätsmerkmale***

- Anzahl Rollen-Änderungen (Changes)
- Zahl der Rollen-Zuteilungen
- Zahl der Rückweisungen

Zentral für die Qualität der Rolle ist die Richtigkeit und Aktualität der Rolle. Veränderungen in den Zielsystemen erfordern auch Anpassungen in der Rolle. Daneben gibt es aber auch Anpassungen, auf Grund fehlender Berechtigungen oder unnötig enthaltenen Rechten. Jede Änderung an einer Rolle führt zu administrativem Aufwand, weshalb es wichtig ist, Rollen so zu definieren, dass sie möglichst vollständig und stabil sind. Eine hohe Change-Häufigkeit pro Rolle und übergeordnet auch über den gesamten Rollenkatalog ist Indiz für ein zu instabiles Umfeld und es ist zu prüfen, wie die Berechtigungsstrukturen in den einzelnen Zielsystemen stabilisiert werden können.

Die Bildung einer Rolle macht nur dann Sinn, wenn diese auch genutzt wird. Die Messung der Zahl von Rollenzuteilungen macht Sinn, lässt sich aber nur in Kombination mit der organisatorischen Entwicklung (Anzahl Eintritte / Wechsel / Austritte) im Anwendungsbereich der Rolle aufschlussreich interpretieren.

Zur Verbesserung von Rollenbeschreibungen (Scope, Anwendung / Inhalt) hilft eine die Auswertung nach der Anzahl von Rückweisungen. Wird die Vergabe einer Rolle besonders oft abgelehnt, ist der Grund in der Regel bei unklaren resp. unzureichenden Beschreibungen zu suchen.

Die Frage, ob eine Rolle von guter Qualität ist, wird unterschiedlich beantwortet.

## Bewahren der Rollenqualität

Einmalig ein qualitativ hochwertiges Rollenmodell zu entwickeln ist eine Sache. Die erreichte Qualität der einzelnen Rollen und somit des gesamten Rollen-Katalogs zu wahren, ist eine andere Sache. Die Qualität der Rollen ist vergänglich. Nur eine durchdachte Rollenadministration hilft, den Stand der Rollen aktuell zu halten.

Eine unzureichende Qualität kann dazu führen, dass grundlegende Ziele, die mit der Einführung eines rollenbasierenden Zugriffsmanagements verfehlt werden.

Damit die Qualität der Rollen nachhaltig gesichert wird, müssen im Unternehmen Prozesse und Verantwortlichkeiten für das Role Life Cycle Management etabliert werden. Dazu gehört insbesondere ein funktionierender Change Management Prozess für Rollen. Hier liegt die Schwierigkeit, Änderungsbedarf an Rollen frühzeitig zu erkennen. Bedingung für eine funktionierende Früherkennung ist es, die Einflussfaktoren für Changes zu verfolgen (z.B. Organisationsänderungen, Einführung neuer Applikationen, Anpassungen an bestehenden Berechtigungen in bestehenden Applikationen…).

Rollen sind nicht im Besitz der IT. Damit die Rollen den betrieblichen Anforderungen gerecht werden, müssen die Fachbereiche in die Pflicht genommen werden. Dies erfolgt in der Praxis dadurch, dass der Rollenowner aus dem Fachbereich kommt und für die einzelne Rolle verantwortlich ist. Über die Rollenowner erfolgt auch die Überprüfung der Rolle im Rahmen des von Validierung / Re-Validierungsprozessen. Ebenso sind verantwortlich für die Attestierung im den Workflows für die Rollenzuweisung.