

Consulta AG

Gesellschaft für Wirtschafts- und Unternehmensberatung

BERDA

Berechtigungsdatenbank

Berechtigungsdatenbank

**Die Lösung für die Governance-
Themen Ihrer IT-Architektur**

Consulta AG

Villa Weber

Postfach 252

CH-8630 Rüti ZH

Tel. +41 55 250 55 55

www.consulta-ag.ch

www.berda.biz

Stephan Illi

lic. oec. HSG

stephan.illi@consulta-ag.ch



1. Einstufung des Themas und Ursachenforschung

IT-Berechtigungen sind ein Thema, für welches die obersten Führungsorgane der Unternehmung die Verantwortung tragen. In der Schweiz ist nebst dem Verwaltungsrat die Revisionsstelle als Organ für die Vermeidung des Missbrauchs im Zusammenhang mit Benutzerberechtigungen verantwortlich, denn sie werden im Rahmen des internen Kontrollsystems (IKS) eingeordnet.

Damit betrifft das Thema alle Bereiche der Governance und Compliance und ist regelmässiger Prüfpunkt der internen und externen Revision.

Ein gutes Berechtigungskonzept ist die Basis einer nachhaltigen Lösung für diese Situation.

1.1 Was ist ein Berechtigungskonzept?

Jede IT-Architektur besteht aus verschiedenen Applikationen (z.B. SAP). Jede dieser Applikationen verwaltet ihre Berechtigungen separat und regelt die Rollenvergabe unterschiedlich. Jeder Stelleninhaber ist Systembenutzer und benötigt deshalb unterschiedliche Berechtigungen bei verschiedenen Applikationen.

Ein gutes Berechtigungskonzept regelt diese Zuständigkeiten (Berechtigungen) sowohl auf fachlicher Seite, als auch auf Applikationsseite (technische Sicht) für sämtliche IT-Systeme der Applikationsarchitektur.

1.2 Ein Berechtigungskonzept bietet Schutz

Ein aktuelles und gelebtes Berechtigungskonzept schützt den Konzern unter anderem vor:

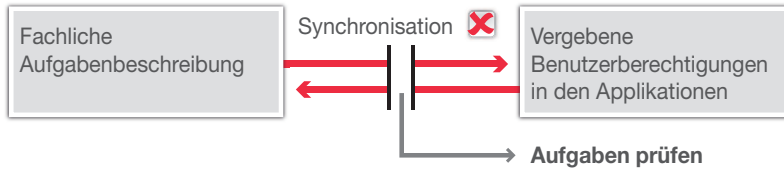
- Betrug
- Datenklau, -missbrauch und deliktischen Modifikationen
- Finanziellen Vermögensverlusten des Eigentümers
- Beanstandungen durch die Revision
- Zeitverlust bei der Fehlersuche in nicht gepflegten Berechtigungen
- Verpassen von regulatorischen, steuer- und handelsrechtlichen Auflagen



Optimalfall



Regelfall



Zustand der Berechtigungen in grösseren IT-Landschaften



1.3 Ursachenforschung

In jeder grösseren IT-Architektur gibt es Unterschiede zwischen den fachlichen Anforderungen an die Zugangsberechtigungen aufgrund der Stellenbeschreibungen der User und den tatsächlich in den IT-Applikationen vergebenen Berechtigungen. Diese Diskrepanz führt oft zu Beanstandungen bei der IKS-Revision.

Berechtigungen müssen nach dem Need-To-Have Prinzip vergeben sein, damit die eben erwähnten deliktischen Handlungen vermieden werden können.

1.4 Ursachen für die Diskrepanzen

- Die Funktionentrennung ist nicht gegeben (z.B. kann eine einzige Person die Aufgaben «Zahllauf erstellen» und «Zahllauf ausführen» durchführen).
- Es besteht keine geltende Namenskonvention bei der Rollenverwaltung. Dies führt dazu, dass eine Übersicht fehlt und für die gleiche Aufgabe zwei unterschiedliche Rollennamen vergeben werden.
- Die Berechtigungen sind nicht nach dem Need-To-Have Prinzip vergeben, da die vom Fach formulierten Anforderungen nicht korrekt von der IT umgesetzt wurden.
- Reorganisationen, und seien sie noch so klein, werden selten konsequent in der Benutzerverwaltung in allen Applikationen nachgeführt.



2. Mögliche Lösungswege

Die folgende Übersicht stellt einige Lösungsmöglichkeiten dar.

Name der Lösung	Vorteile	Nachteile
CheckAUD®	<ul style="list-style-type: none">▪ Automatisiertes Prüfen der vergebenen Rollen	<ul style="list-style-type: none">▪ Reaktives Tool, hilft nicht bei der Vorbeugung
SAP GRC®	<ul style="list-style-type: none">▪ Unterstützt die nachvollziehbare Rollenvergabe	<ul style="list-style-type: none">▪ Nur für SAP Anwendungen möglich▪ Keine Verknüpfung mit fachlichen Aufgaben möglich
Manuelles Prüfen (z.B. per Emails an die Vorgesetzten)	<ul style="list-style-type: none">▪ Ausreichend bei kleineren Architekturen▪ Pragmatisch	<ul style="list-style-type: none">▪ Hohe Fehlerquote, da nicht automatisiert
BERDA der Consulta AG	<ul style="list-style-type: none">▪ Verknüpft fachliche Aufgabenbeschreibungen mit technischen Rollen▪ Passend für alle Applikationen▪ Kostengünstig & pragmatisch▪ Leicht zu aktualisieren	<ul style="list-style-type: none">▪ Keine automatisierte Rollenvergabe, sondern reine Erstellung von Handlungsanweisungen an die Berechtigungsverwaltung

Mögliche Lösungen für die Berechtigungsproblematik



3. Übersicht der Vorgehensweise

Um Ihre IT-Architektur bereit zu machen, den ständig wechselnden Anforderungen zu entsprechen, haben unsere Spezialisten ein bewährtes Vorgehen entwickelt, das durch praxiserprobte Hilfsmittel komplettiert wird.

3.1 Das Vorgehen der Consulta AG

1

Geschäftssystem-analyse

- Strategie & Prozesse verstehen
- Aufbauorganisation analysieren
- IT-Architektur abbilden

2

IT Systeme priorisieren und Konzept erstellen

- Prozessrisiken beurteilen
- IT-Systeme priorisieren
- Berechtigungskonzept erstellen

3

Berechtigungen bereinigen

- Aufgabenbeschreibungen je Rolleninhaber erstellen
- Funktionstrennungskonflikte identifizieren
- Rollen bereinigen
- Berechtigungsvergabe ändern

4

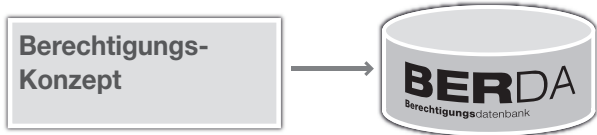
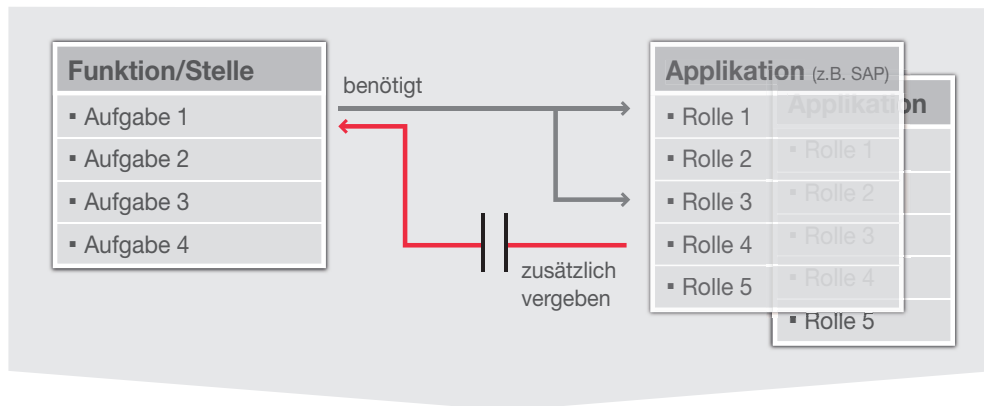
Laufende Aktualisierung sicherstellen

- Strategie & Prozesse aktualisieren und vergleichen
- Berechtigungsvergabe regeln
- Rollenansprüche regeln



3.2 Der Consulta - Lösungsansatz

Dabei verfolgen wir den pragmatischen und ganzheitlichen Lösungsansatz mit unserer eigenentwickelten BERDA (BERechtigungs-DATENbank).



Lösungsansatz BERDA

Dieser für KMUs entwickelte Lösungsansatz begeistert auch Grosskonzerne. Er wurde von uns unter anderem bei einem grossen Schweizer Dienstleistungs-Konzern implementiert und wird von KPMG empfohlen.

3.3 Die Funktionsweise der BERDA



Abgleich der Aufgabenbeschreibungen und der effektiv vergebenen Rollen in der Applikation



Ausgabe der Delta-Reports anhand benutzerdefinierter Masken (nach Abteilung, nach Hierarchieebene, nach Aufgaben, nach User, etc.)



Veränderungen in der Organisation (Mitarbeiter-Eintritt, -Austritt, -Übertritt, fehlende Berechtigungen) können so leicht abgebildet werden und den IT-Beauftragten vor der Revision zur Behebung allfälliger Diskrepanzen mitgeteilt werden



4. Zusammenfassung und Fazit

Ein funktionierendes und leicht zu aktualisierendes Berechtigungskonzept regelt Ihre IT-Governance dauerhaft und einfach und arbeitet komplementär zu den Revisions-Kontroll-Tools wie z.B. Check-Aud®.

Durch den ganzheitlichen Ansatz der BERDA, die Fach und IT involviert und in der Lage ist, die Dynamik Ihrer Organisation aufzufangen, ist dieses Tool die passende Ergänzung für Ihre IT-Architektur.

Das sind Ihre Vorteile:

- Ein pragmatisches Berechtigungskonzept
- Eine in der Praxis erprobte IT-Applikation ohne grossen Wartungsaufwand, mit niedrigen Supportkosten, mit einmaliger Lizenzgebühr, intuitiver Bedienung und absoluter Revisions-tauglichkeit



Stephan Illi

lic. oec. HSG
stephan.illi@consulta-ag.ch
Leiter Unternehmensbera-
tung, Mitglied des Verwal-
tungsrates

Wir freuen uns über Ihre
Kontaktaufnahme – rufen
Sie uns an für ein unver-
bindliches und vertrauliches
Gespräch bei uns in der Villa
Weber in Rüti.

Consulta AG

Villa Weber
Postfach 252
CH-8630 Rüti ZH
Tel. +41 55 250 55 55
www.consulta-ag.ch
www.berda.biz

