



SAP®.  
Kompetenz.  
Nutzen.

## Einführung SAP BO Access Control (GRC)

### Unser Kunde

Der börsennotierte Industriekonzern mit Hauptsitz in Paris ist mit rund 190.000 Mitarbeitern und ca. 38 Milliarden Euro Umsatz eines der zehn größten Unternehmen Frankreichs. Er ist weltweit in über 60 Ländern vertreten und zählt zu den ältesten Unternehmen der Welt. Insbesondere bei Bau- und Dämmstoffen, bei Glas, Industriekeramik, bei Verpackungsmaterialien und beim Baustoffhandel hat der Konzern eine führende Rolle; bei einigen Produkten aus diesen Bereichen sogar als Weltmarktführer oder europäischer Marktführer.

### Ausgangssituation

Das europäische SAP ERP-System unseres Kunden ist in der Vergangenheit stark gewachsen, auf ca. 4.000 User in ca. 30 Buchungskreisen. Insbesondere mit dem Einzug neuer Gesellschaften wurde das genutzte Template für Berechtigungen (Stellen, Rollen) aufgeweitet. Mit diesem Wachstum ist auch ein starker Wildwuchs bei den Berechtigungen entstanden: Temporäre Rollen beispielsweise für Trainees oder Azubis, diverse umfangreiche, sich teilweise überschneidende Basisrollen. Die Transparenz bezüglich der vergebenen Berechtigungen ist dadurch verloren gegangen und es gab eine Vielzahl von Verstößen gegen das Funktionstrennungsprinzip (Segregation of Duties, SoD). Dies wurde in Prüfberichten der internen Revision und der Wirtschaftsprüfer wiederholt bemängelt. Auch wurde der Aufwand für die laufende User-/Berechtigungsadministration immer höher. Aus diesen Gründen hat sich der Kunde entschlossen, SAP BO Access Control (GRC) einzuführen, das konzernweit als Compliance-Tool gesetzt ist.

### Die Teilprojekte

#### Risk Analysis and Remediation

Unter Berücksichtigung der Anforderungen der Wirtschaftsprüfer und internen Revision führten die HPC-Berater dieses Tool ein und erarbeiteten folgende Teilaufgaben:

- Definition einer einheitlichen Risiko-Matrix: Festlegen von SoD-Risiken und kritischen Transaktionen im Rahmen von Risiko-Workshops mit den Process Ownern
- Definition von kompensierenden Kontrollen (sog. Mitigation Controls) für nicht zu vermeidende Risikoverstöße
- Konzept für Rollen- und User-Bereinigung
- Abstimmung der Ergebnisse mit der internen Revision und den Wirtschaftsprüfern
- Technische Umsetzung in GRC und Dokumentation



- Training der GRC-Key-User
- Unterstützung der User bei der Bereinigung von Risiko-Verstößen

Hierbei berücksichtigten sie sowohl die gesetzlichen Vorgaben, als auch die Anforderungen des internen Kontrollsystems des Kunden.

### **Teilprojekt**

#### **Superuser Privilege Management**

Die HPC-Berater führten GRC Superuser Privilege Management als Notfall-User-Konzept für SAP Competence Center-Mitarbeiter des Kunden mit umfangreichen Berechtigungen im Produktivsystem ein.

### **Teilprojekt**

#### **Klassisches Berechtigungskonzept**

Neben der eigentlichen SAP BO Access Control-Einführung erarbeiteten die Berater der HPC folgende Aufgaben im Umfeld des klassischen Berechtigungskonzeptes:

- Einführung der Vererbung von Rollen zur Effizienzsteigerung
- Dokumentation der Rollen
- Reengineering des Berechtigungskonzeptes insbesondere im Bereich Controlling
- Reengineering von Rollen im Rahmen der Bereinigung von Risikoverstößen innerhalb von Rollen
- Einführung einer einheitlichen Master-Sprache für alle Rollen

### **Kundenvorteil aus dem Projekt**

- ✓ Effizienzsteigerung in der Berechtigungsverwaltung
- ✓ Erhöhung der Transparenz der vergebenen Berechtigungen durch Echtzeitanalysen
- ✓ Erfüllung der Forderungen der internen Revision und der Wirtschaftsprüfer bezüglich kritischer Berechtigungen und Funktionstrennung.
- ✓ Verlagerung der Verantwortung für die vergebenen Berechtigungen von der IT zum Business.

### **Betroffene Systeme und Software**

- SAP ERP 6.0 mit ca. 4.000 Usern
- SAP BO Access Control 5.3 Risk Analysis and Remediation
- SAP BO Access Control 5.3 Superuser Privilege Management