

Liebe Leserin, lieber Leser,

das zurückliegende Jahr war für HPC wirtschaftlich ein erfolgreiches. Damit das so bleibt, arbeiten wir mit aller Konzentration an unseren heutigen Kompetenzen weiter und bauen darüber hinaus Governance, Risk & Compliance (GRC) aus. HPC wird zum Beispiel ab dem zweiten Quartal 2008 am Ramp-Up des neuen Releases SAP Process Control 2.5 teilnehmen und dort in direkter Zusammenarbeit mit der SAP AG Projekte durchführen. Die Bedeutung von GRC nimmt aber nicht nur bei HPC, sondern auch am Markt zu.

Ein anschauliches Beispiel für die Gefahren der Nichteinhaltung von Compliance lieferte vor wenigen Wochen die französische Bank Société Générale. Offensichtlich haben Mängel im internen Kontrollwesen zu einem der größten Bankenskandale der vergangenen Jahre geführt.

Doch nicht nur für Großkonzerne bleibt das Thema wichtig. Auch kleinere Unternehmen profitieren gerade hinsichtlich des Vertrauens der Kunden, wenn die Sicherheit der eigenen Systeme und Daten u.a. mit Hilfe sauberer Berechtigungskonzepte gewährleistet ist.

HPC ist Ihr SAP Special Expertise Partner für GRC und GTS, wenn es um die Erstellung und Umsetzung einer firmenweiten Compliance-Strategie geht. Unser GRC-Competence Center verfügt über umfassende Erfahrungen und das richtige Know-how.

Aber auch in unseren weiteren Kernkompetenzen wie Logistic Execution, Mobility, ERP-Beratung und -Einführung sowie Business Intelligence sind wir natürlich weiterhin hoch aktiv und stets für Sie da.

Ihre HPC NEWS Redaktion

Dunja Werner

Kontakt: Marketing@HPC.de

Inhalt

- **Saubere Berechtigungsvergabe ebnet den Weg: Warum Berechtigungen als Compliance-Basis so wichtig sind**
- **Risiken entdecken, beheben, verhindern: SAP® GRC Risk Analysis & Remediation**
- **HPC Quick Five: Optimierung der Berechtigungsverwaltung**
- **HPC in der Praxis: Neue Lagerlösung für mehr Transparenz**
- **Kooperation mit PTS-Group ausgeweitet: Strategische Partnerschaft**
- **Glossar: Segregation of Duty**
- **Glossar: Objekte, Berechtigungen, Rollen**

Saubere Berechtigungsvergabe ebnet den Weg

Warum Berechtigungen als Compliance-Basis so wichtig sind

Auch die längste Reise beginnt mit einem ersten kleinen Schritt. Sicher hatte Mao Tse Tung mit diesem Spruch anderes im Sinn. Dennoch scheint es häufig ein endloser Weg zu sein, das eigene Unternehmen so auszurichten, dass es allen Regeln folgt, die Sicherheit den gesetzten Maßstäben gerecht wird und gleichzeitig ein überschaubares und regulierbares IT-Wesen besteht.

Der erste – allerdings gar nicht so kleine - Schritt dorthin ist es, den Zugang zum System, zu Daten und Informationen so zu organisieren, dass wirklich nur diejenigen Anwender Zugang erhalten, die es entsprechend ihrer Aufgabe auch sollten. Wenn die Zugangsvergabe richtig geordnet ist, hat ein Unternehmen schon einen ganz wichtigen Grundstein zur integrierten und ganzheitlichen Compliance gelegt.

Die Grundlage für die Einhaltung von Richtlinien bezüglich Zugriffen auf SAP-Daten jeglicher Art ist das SAP-Berechtigungswesen.

SAP-Berechtigungen machen ein SAP-System überhaupt erst nutzbar. Die Möglichkeiten zur Steuerung der erlaubten Zugriffe sind enorm. Ca. 2.600 Berechtigungsobjekte sorgen für eine hohe Flexibilität, bedingen aber auch eine hohe technische Komplexität. Daher sind SAP-Berechtigungen oftmals ein IT-Thema, obwohl die Daten- und Prozessverantwortung für die produktiven Systeme in der Fachabteilung liegen.

Um ein sicheres, praxisnahes und administrierbares Konzept zu gewährleisten müssen aber alle Beteiligten am selben Strang ziehen. Nur durch diese gemeinsame Anstrengung, die in eine integrierte Compliance-Strategie münden sollte, kann das gewünschte Ziel erreicht werden.

Die IT ist lediglich Dienstleister für die technische Umsetzung dessen, was die Fachabteilung bezüglich deren Geschäftsprozessen vorgibt.

Bei der Konzeption des Berechtigungskonzeptes ist z.B. zu berücksichtigen, dass die Rollen nicht personalisiert, sondern arbeitsplatz- oder aufgabenspezifisch definiert werden. Grundlegend und selbstverständlich ist ein eindeutiges Namenskonzept, das Transparenz und somit Effizienz schafft. Weiterhin ist für ein organisationsübergreifendes SAP-System ein Rollen-Template-Ansatz zu empfehlen und die Einhaltung von Gewaltentrennungs-Richtlinien, sowie die Vermeidung von kritischen Berechtigungen in permanenten Benutzerstämmen zu berücksichtigen.

Aber gerade die Einhaltung von Gewaltentrennung und der Balance-Akt zwischen Betriebs-sicherung (z.B. kritische Berechtigungen wie Mandantenpflege, Verbucher-Administration) und Vermeidung von Risiken ist in regelmäßigen Abständen der Prüfung von Auditoren unterworfen. Außerdem entspricht gerade die Umsetzung dieser Themen den Anforderungen eines jeden Managements.

Nichts kann also auf dem Weg einer Compliance-Strategie eine gründliche Konzeption ersetzen. Nur wenn alle beteiligten Personen und Systeme einbezogen werden, kann eine von Grund auf einheitliche und durchgängige Lösung erzielt werden, deren Vorteile dann nicht nur bei Audits, sondern im alltäglichen Arbeiten zum Tragen kommen.

Aufgrund der fachlichen und technischen Komplexität dieser Aufgabenstellung und deren Umsetzung werden SAP-Berechtigungs-Konzepte oft stiefmütterlich behandelt. „Hauptsache, wir können arbeiten!“ welcher ambitionierte Berechtigungsverwalter hat dies nicht schon gehört?

Aber: das SAP-Berechtigungswesen ist mit entsprechender Erfahrung durchaus in den Griff zu bekommen! Mit einer gravierenden Einschränkung: Ein zufriedenstellendes Risikolevel – also die Art und Anzahl der in den Rollen und insbesondere Rollen-Kombinationen vorliegenden Risiken – kann mit SAP-Standard-Funktionen kaum erreicht werden. Die Erhaltung eines einmal erreichten Risikolevels ist eine hohe Herausforderung an Skill und Ressourcen.

SAP® GRC Access Control bietet eine in die bestehenden Geschäftsprozesse integrierte Lösung, mit der Berechtigungen und Benutzer effizient und nachhaltig risikominimiert verwaltet werden können. Die Fachabteilungen werden mit dieser Lösung in die Lage versetzt, ihre Verantwortung für Compliance wahrzunehmen.

SAP® Access Control ist eine Komplettlösung für folgende Aufgaben:

- Risk Analysis and Remediation - für die Risiko-Minimierung von Rollen und Benutzern, sowie die nachhaltige Risiko-Vermeidung.
- Superuser Privilege Management – für eine effiziente und auditsichere Notfall-User-Lösung.
- Compliant User Provisioning – für eine praxisnahe Benutzer-Administration inkl. nachhaltiger Vermeidung von Gewaltentrennungskonflikten.
- Enterprise Role Management – für einen sicheren Rollen-Änderungs-Prozess.

Mehr über den Einstieg in's Access Management [mit dem HPC Quick Check](#)

Kontakt:
Bianca Becker
06201 / 94 95 0

Bianca.Becker@HPC.de

Risiken entdecken, beheben, verhindern

SAP® GRC Risk Analysis & Remediation (ehem. Compliance Calibrator)

Mit SAP® GRC Risk Analysis and Remediation werden Rollen- und Benutzeränderungen in Echtzeit auf kritische Berechtigungen und Verstöße gegen die Funktionstrennung überprüft und somit vermieden. Dem Management und den Auditoren werden übersichtliche Berichte zur Information über den aktuellen Zustand des Berechtigungskonzeptes bezüglich vorliegender Risiken zur

Verfügung gestellt.

Mit SAP® GRC Risk Analysis & Remediation wird ein umfangreiches Risiko-Regelwerk ausgeliefert. Es umfasst aktuell rund 200 Risiken, die sich aus den Kombinationsmöglichkeiten von mehreren tausend SAP-Standardtransaktionen ableiten. Auf dieser Basis wird das unternehmensindividuelle Regelwerk definiert, die größte Hemmschwelle zur Definition von Risiken ist somit schon genommen.

Werden im SAP-Berechtigungskonzept einem Anwender beispielsweise Rollen mit Berechtigungen zur Sachkontenpflege, Rechnungseingang und Zahlungsausgang zugewiesen, wird von Risk Analysis & Remediation anhand des hinterlegten Regelwerks ein potenzielles Risiko identifiziert gemeldet. Wenn ein Gewaltentrennungsverstoß beispielsweise aus personellen Gründen nicht zu vermeiden ist, können entsprechende kompensierende Kontrollprozesse hinterlegt werden. Deren Durchführung wird wiederum von SAP® GRC Risk Analysis & Remediation überwacht und ggf. eskaliert.

SAP® GRC Access Control ermöglicht somit auch dem Fachbereich, die Risiken im Berechtigungskonzept einzuschätzen.

Kontakt:

Bianca Becker
06201 / 94 95 0
Bianca.Becker@HPC.de

HPC Quick Five

Optimierung der Berechtigungsverwaltung

HPC bietet Ihnen Unterstützung bei der Ermittlung einer Optimierungs-Strategie, sowie bei der Neuaufstellung Ihrer bestehenden SAP®-Berechtigungslösungen. Unsere Standard-Beratungspakete umfassen z.B. eine Bestandsaufnahme (Pre-Audit), die Einführung einer zentralen Benutzerverwaltung, die Umstellung von Profilen auf Rollen, die Konzeption zur Einbindung von Eigenentwicklungen oder auch ein neues Namenskonzept. Alle Schritte sind einzeln buchbar und bieten bei überschaubaren Investitionen einen enormen Gewinn hinsichtlich der Compliance.

Natürlich haben wir auch Erfahrung im Re-Design von bestehenden Berechtigungskonzepten, Neueinführungen und Upgrades. Sprechen Sie uns einfach an!

Unser Angebot als [PDF-Download](#).

Kontakt:
Dunja Werner
06201 / 94 95 0
Marketing@HPC.de

HPC in der Praxis

Neue Lagerlösung für mehr Transparenz

Für einen Hersteller von schnelllaufenden Dieselmotoren spielen Ersatzteile eine große Rolle. Deren Herstellung, Verfügbarkeit und Lagerung sind ein wichtiger Bestandteil einer schlanken Produktion und effizienter Prozesse.

HPC implementiert bei MTU Friedrichshafen eine neue Lagerabwicklung mit Trennung von Ersatz- und Serienteilen. Damit werden nachfolgende Vorteile verbunden:

- Zentrale Beschaffung aus dem Seriensystem
- Nutzung von Einkaufsmengenvorteilen
- Getrennt wirtschaftliche Steuerung der Serien- bzw. Ersatzteilproduktion

Die neue Ersatzteillösung basiert auf einem Systemverbund SAP® ERP 6.0 mit SAP® eWM und SAP® R/3. In SAP® ERP 6.0 werden alle Ersatzteilprozesse wie Beschaffung, Disposition und Vertrieb abgebildet. Das SAP® extended Warehouse zur Ersatzteillagerabwicklung ist über Schnittstellen an SAP® ERP 6.0 gekoppelt. Die zentrale Beschaffung von Serien- und Ersatzteilen wird über das Seriensystem SAP® R/3 abgewickelt.

Unsere Berater haben in diesem Projekt von rund 15 Monaten Dauer bestehende Prozesse analysiert, neue Prozesse in Blueprints aufgesetzt, einen Prototypen entworfen und schließlich umgesetzt. Die Produktivsetzung ist im 2. Quartal 2008 geplant.

Den Kunden erwartet nun eine höhere Transparenz im Ersatzteillager sowie einen Gewinn an Effizienz und höherer Produktivität bei gleichzeitig sinkenden Lagerhaltungskosten.

Kontakt:
Roland Hofmann
06201 / 94 95 0
Vertrieb@HPC.de

Kooperation mit PTS-Group ausgeweitet

Strategische Partnerschaft

Die PTS-Group aus Bremen und die HPC AG haben ihre Zusammenarbeit ausgebaut. Die beiden Unternehmen arbeiten bereits seit längerem in der Beratung zusammen. Die Bremer sind ein Fullservice-Provider und unterhalten drei Rechenzentren in Deutschland.

Durch die erweiterte Kooperation mit PTS vergrößert sich nun die Angebotspalette von HPC um Hosting und Application Management, während die Bremer künftig auf die Beratungskompetenz von HPC zurückgreifen können. Auf diese Weise können auch Kunden mit umfangreicheren Anforderungen aus einer Hand betreut werden.

Kontakt:
Dunja Werner
06201 / 94 95 0
Marketing@HPC.de

Glossar

Segregation of Duty – SoD

Die Segregation of Duty bedeutet zu deutsch Funktions- oder Gewaltentrennung. Dabei handelt es sich um die Aufteilung verschiedener Schritte eines Geschäftsprozesses auf mehrere Personen, so dass keine Interessenskonflikte aus verschiedenen Funktionen ein und derselben Person entstehen können. Wer beispielsweise einen Auftrag vergibt, darf nicht gleichzeitig diese Auftragsvergabe auf ihre Richtigkeit überprüfen. Ziel ist es, die Anhäufung von Kompetenzen zu vermeiden, welche zusammen ein mögliches Risiko zur Durchführung von kriminellen Handlungen bietet und daher häufig Gegenstand von Prüfungen ist. Diese Regel ist von grundsätzlicher Natur und geht auf Gesetze zurück wie HGB, GoBS und den [Sarbanes-Oxley Act](#).

Wirksame Offenlegungskontrollen sind festzulegen, einzuführen und zu überwachen. Schwächen, Fehler und Täuschungen müssen veröffentlicht werden. Die Offenlegungsverpflichtung gilt übrigens auch für nicht bilanzwirksame Transaktionen.

Objekte, Berechtigungen, Rollen

Berechtigungsobjekte ermöglichen es, komplexe Berechtigungen zu definieren. Ein Berechtigungsobjekt umfasst bis zu zehn Berechtigungsfelder, die in einer UND-Verknüpfung geprüft werden. Dabei wird ermittelt, ob ein Benutzer eine bestimmte Aktion ausführen darf. Um die Berechtigungsprüfung erfolgreich zu durchlaufen, muss der Benutzer die Prüfung für jedes im Objekt enthaltene Feld bestehen. Zur besseren Übersichtlichkeit sind Objekte in Objektklassen gegliedert.

Eine Berechtigung ist die Ausprägung eines Berechtigungsobjektes mit bestimmten zugelassenen Feldwerten und -kombinationen. Es werden ein oder mehrere Werte für jedes Berechtigungsfeld definiert, das im Berechtigungsobjekt enthalten ist. Berechtigungen werden in Profilen zusammengefasst und sind erst in ihrer Kombination funktionstüchtig.

Rollen basieren idealerweise auf Arbeitsplatzbeschreibungen und erlauben einem Benutzer seine Aufgaben im Tagesgeschäft durchzuführen. Hilfreich zu deren Erstellung sind daher neben den Arbeitsablaufbeschreibungen auch die Stellenbeschreibungen der Personalabteilung. Rollen werden mit dem Profil- oder Rollengenerator angelegt. Dieser unterstützt die korrekte Objektausprägung (Definition von Berechtigung), das heißt, dass Berechtigungsvorschläge anhand der der Rolle zugewiesenen Transaktionscodes erstellt werden. Es können sogenannte Template-Rollen angelegt werden, deren enthaltene Funktionen in Tochterrollen vererbt werden, die sich lediglich in der Ausprägung der Organisationseinheiten unterscheiden.

Die für eine Transaktion notwendige Objektausprägung (Berechtigung) muss bei der manuellen Profilpflege im Trial&Error-Verfahren ermittelt werden. Bei der Verwendung von Rollen dient das Profil nur als "technische Hülle" für die Berechtigung. Es wird daher dringend empfohlen, keine manuelle Profilpflege durchzuführen, sondern den Profil- oder Rollengenerator zu verwenden.

Kontakt

HPC AG
Marketing & PR
Dunja Werner
Multring 28
69469 Weinheim
Tel.: 06201 / 94 95 0
Fax: 06201 / 94 95 95
Mail: Marketing@HPC.de

Hat Ihnen unser Newsletter gefallen und Sie kennen jemanden, der sich auch für die Inhalte interessieren könnte? Dann empfehlen Sie uns doch einfach weiter!

NEWS, ANREGUNGEN, KRITIK, LOB

Wenn Sie Neuigkeiten haben, die wir im Newsletter über ihre Branche veröffentlichen sollen, wenn Sie Anregungen haben, Kritik oder Lob äußern wollen, mailen Sie uns einfach

Kontakt: Marketing@HPC.de

© 2008. Für den Inhalt des Newsletters ist die HPC AG verantwortlich.