

Lösung im Detail

SAP GRC Access Control
als Bestandteil der SAP-Lösungen für
Governance, Risk und Compliance

UNTERNEHMENSWEITE ZUGRIFFS- UND BERECHTIGUNGSKONTROLLE

FUNKTIONSTRENNUNGSRISIKEN ER- KENNEN, BESEITIGEN UND VERHINDERN

Die Prüfung, Kontrolle und Organisation des unternehmensweiten Zugriffs- und Berechtigungswesens sowie der Aufbau eines internen Kontrollsystems (IKS) werden durch SAP® GRC Access Control unterstützt. Die Anwendung hilft, gesetzliche Vorschriften wie die 8. EU-Richtlinie zu erfüllen: Risiken in der Zugriffs- und Berechtigungssteuerung von IT-Systemen lassen sich identifizieren und abbauen, präventive Maßnahmen in Geschäftsprozesse integrieren. Unerlaubten Datenzugriffen und kriminellen Missbrauch wird wirksam vorgebeugt. Der Arbeitsaufwand und die Kosten lassen sich spürbar reduzieren.



THE BEST-RUN BUSINESSES RUN SAP™



DATENMISSBRAUCH UND MANIPULATION VORBEUGEN

Mit SAP GRC Access Control können Unternehmen ihr Zugriffs- und Berechtigungswesen zuverlässiger gestalten, gesetzlichen Vorgaben entsprechen und ein wirksames internes Kontrollsystem (IKS) aufbauen. Sie beugen damit unerlaubten Datenzugriffen und kriminellen Machenschaften wirksam vor.

Betrügerische Handlungen, Identitätsmissbrauch sowie Datendiebstähle und -manipulationen verursachen in vielen Unternehmen hohe Schäden. Eine steigende Anzahl gesetzlicher Auflagen soll diesen kriminellen Handlungen entgegenwirken. Strengere Richtlinien für die Corporate Governance und Datenschutzbestimmungen verpflichten Unternehmen, interne Kontrollmechanismen einzuführen und Geschäftsrisiken sorgfältig zu überwachen. Für die Einhaltung aller Vorgaben sind Revisoren und IT-Sicherheitsexperten zuständig. Die Verantwortung trägt letztlich die Geschäftsführung. Die Nichteinhaltung von Auflagen und Bestimmungen kann beträchtliche Bußgelder bis hin zu gerichtlichen Strafen nach sich ziehen.

Auswirkungen auf die Zugriffs- und Berechtigungssteuerung

Gesetzliche Vorschriften wie verschärfte EU-Richtlinien, das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in Deutschland oder der Sarbanes-Oxley Act (SOX) in den USA fordern nachdrücklich, dass Unternehmen über effektive Überwachungsmechanismen verfügen. Nicht selten existieren in Unternehmen unzählige Zugriffsregeln, die system- und prozessübergreifend miteinander verknüpft sind. Damit Geschäftsführung und IT-Abteilung in jeder Situation gesetzeskonforme Entscheidungen treffen können, benötigen sie spezielle Software, um dieses komplexe Beziehungsgeflecht zu verwalten und zu kontrollieren. Es gilt vor allem, Zugriffs-

und Berechtigungsmechanismen zu automatisieren und frühzeitig über potenzielle Berechtigungskonflikte und Risiken informiert zu sein.

Praxisbewährte Lösungen von SAP

SAP®-Lösungen für Governance, Risk und Compliance (GRC – siehe Abbildung 1) helfen Unternehmen im Rahmen eines ganzheitlichen Konzepts, zahlreiche branchenübergreifende und -spezifische Wirtschaftsvorschriften sicher einzuhalten. Ein umfangreiches Rahmenwerk ermöglicht es, GRC-Aktivitäten unternehmensweit zu standardisieren. Gleichzeitig können innovative SAP- und Partnerlösungen problemlos integriert werden. Dadurch werden Kosten spürbar reduziert sowie

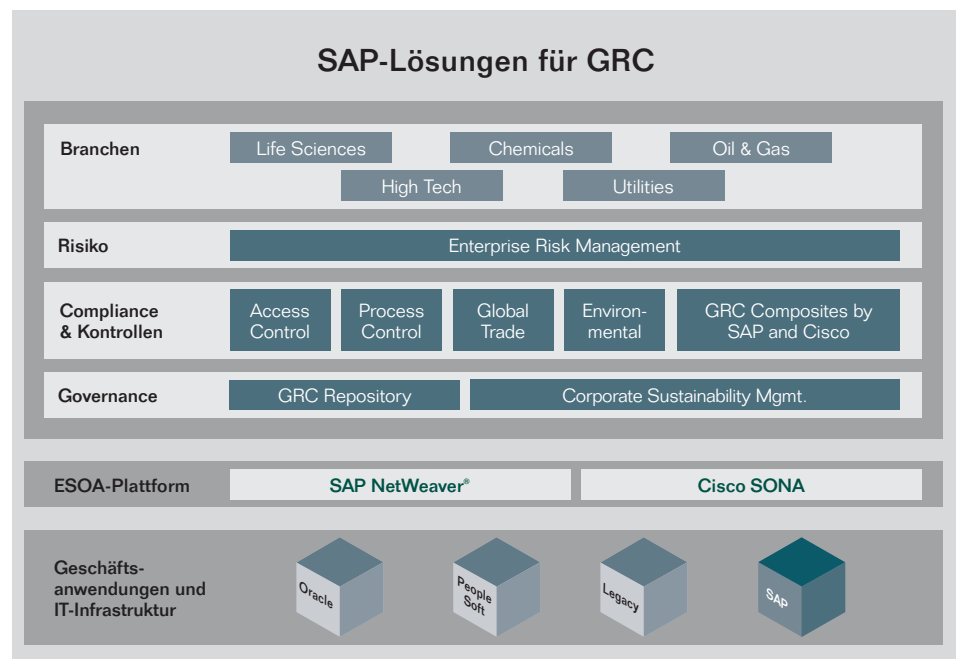


Abbildung 1: SAP GRC Access Control als ein Baustein der SAP-Lösungen für GRC

Sicherheit und Leistungsfähigkeit erhöht. Der ganzheitliche Ansatz eröffnet außerdem deutliche Wettbewerbsvorteile: Gebundene Ressourcen werden freigesetzt, eine deutliche Ausdifferenzierung gegenüber Konkurrenten ist möglich. Hinzu kommt der Investitionsschutz, den eine langfristig angelegte SAP-GRC-Roadmap gewährleistet.

SAP-Lösungen für GRC beinhalten ein umfassendes Portfolio an integrierten Anwendungen. Diese schaffen die Voraussetzung für durchgängige und automatisierte GRC-Prozesse. Das gilt für Bereiche wie Corporate Governance und Unternehmenskontrolle, Risiko-Management, Kontrolltest und Problembeseitigung, Zugriffs- und Berechtigungssteuerung sowie für globalen Handel und Umwelt-, Gesundheits- und Arbeitsschutz.

Sorgfältig aufeinander abgestimmte Funktionalitäten

SAP GRC Access Control ist Bestandteil der SAP-Lösungen für GRC. Als Teil einer integrierten GRC-Strategie versetzt die Anwendung Unternehmen in die Lage, regulatorischen und unternehmerischen Risiken kostengünstig zu begegnen. Mit automatisierten Funktionen trägt die Anwendung dazu bei,

- Zugriffs- und Berechtigungskonflikte schnell zu beseitigen,
- ein kontinuierliches Zugriffs- und Berechtigungsmanagement sicherzustellen und
- Management und Prüfer effizient zu unterstützen.

Mehr als 700 Unternehmen weltweit steuern und überwachen ihr Zugriffs- und Berechtigungswesen bereits durchgängig mit SAP. SAP GRC Access Control (siehe Abbildung 2) bildet eine leistungsstarke, integrierte Komplettlösung für folgende Aufgaben:

- Risikoanalyse und -bereinigung
- Unternehmensweites Rollenmanagement
- Regel- und gesetzeskonforme Berechtigungsvergabe
- Management von Superuser-Berechtigungen
- Regelmäßige Überprüfung der Zugangskontrollen

Risikoanalyse und -bereinigung

SAP GRC Access Control sorgt dafür, dass sämtliche relevanten Bestimmungen in Echtzeit eingehalten werden und damit Überwachungslücken erst gar nicht entstehen.

- **Aktuelle Daten analysieren**
Die Anwendung arbeitet mit permanenten Datenabgriffen in den verschiedenen Systemen. Risiken werden so auf Basis von aktuellen Daten identifiziert. Dadurch lassen sich Konflikte unmittelbar nach ihrem Entstehen erkennen, die Ursache ermitteln und Abhilfe schaffen. Ist das System bereinigt, kann in Simulationen getestet werden, wie sich Änderungen von Berechtigungen oder Benutzerrollen auswirken. So werden Sicherheitsverstöße effektiv verhindert.



SAP GRC Access Control bewertet Risiken auf der Basis von aktuellen Daten, sodass Konflikte in Bezug auf die Funktionstrennung sofort nach ihrem Entstehen erkannt werden.

ZEITAUFWAND UND KOSTEN REDUZIEREN

■ Versteckte Probleme finden

Unternehmen werden dabei unterstützt, Regelverstöße aufzuspüren, die ansonsten möglicherweise unentdeckt blieben. So kann die IT-Abteilung in kürzester Zeit tausende Zeilen individuellen Codes nach verdächtigen Benutzerzugriffen durchsuchen. Manipulationen werden entdeckt, ehe Schäden entstehen.

■ Funktionstrennung sicherstellen

Die Anwendung enthält eine der umfangreichsten Datenbanken von Regeln zur Funktionstrennung. Zudem ermöglicht die Software auch Anwendern ohne spezielle ERP-Kenntnisse, individuelle Regeln anhand gängiger betriebswirtschaftlicher Ausdrücke zu definieren.

■ Risiken konsequent abbauen

SAP GRC Access Control ermittelt Risiken in Verbindung mit der Zugriffs- und Berechtigungssteuerung in SAP-Landschaften sowie Fremdanwendungen, Eigenentwicklungen oder Legacy-Systemen und hilft, diese abzubauen. Unternehmen benötigen demnach für sämtliche Anwendungen und Plattformen ihrer IT-Landschaft nur noch eine Compliance-Lösung.

Unternehmensweites Rollenmanagement

SAP GRC Access Control standardisiert und zentralisiert die Anlage und Administration von Benutzerrollen. Das reduziert die Gefahr von Fehlern

und erleichtert die unternehmensweit einheitliche Durchsetzung bewährter Verfahren. IT-Spezialisten und Anwender aus den Fachabteilungen können mit der Software gleichermaßen bequem wie Kosten sparend Rollen definieren, automatisch Risiken prüfen, Änderungen verfolgen und Wartungsaufgaben durchführen.

■ Auditfähige Rollen definieren

Die Anwendung überträgt die Verantwortlichkeit für die Definition und Pflege der Benutzerrollen von der IT-Abteilung auf ausgewählte Endanwender. Diese können den Handlungs- und Berechtigungsumfang einer Rolle bestimmen sowie Status und Historie der Rolle dokumentieren – ohne umständliche Excel-Tabellen



Abbildung 2: Funktionalitäten von SAP GRC Access Control

oder ähnliches. Die Anwender können Rollen, in denen eine bestimmte Transaktion verwendet wird, oder definierte Rollen mit dem tatsächlichen Rollengebrauch in der SAP-Landschaft vergleichen. Änderungen an Profilen werden da-durch beträchtlich erleichtert. Bevor neue oder geänderte Rollen in das produktive System übernommen werden, werden sie im Rahmen der Risikoanalyse und -bereinigung zuvor auf mögliche Konflikte hinsichtlich der notwendigen Funktionstrennung überprüft.

- Benutzerrollen automatisch anlegen**
 Hat der Anwender den Umfang einer Rolle definiert, kann er sie „per Knopfdruck“ anlegen. Um die Integrität der Rollen zu gewährleisten, hat der Anwender die Möglichkeit, Rol- lendefinitionen mit in SAP-Anwendungen hinterlegten Informationen zu vergleichen. Historische Berichte und Analyseergebnisse werden automa- tisch mit Blick auf spätere Audits erfasst. Rollenverantwortliche können komfortabel die von Auditoren geforderten Dokumente wie Rollen- definitionen oder detaillierte Ände- rungsprotokolle erstellen sowie Testergebnisse dokumentieren.

Regel- und gesetzeskonforme Berechtigungsvergabe

Erteilen oder modifizieren Unternehmen Systemzugriffe, überblicken sie nicht immer alle Auswirkungen auf die gefor- derte Funktionstrennung. SAP GRC

Access Control sorgt während der gesamten Betriebszugehörigkeit eines Mitarbeiters für die ordnungsgemäße Erteilung von Zugriffsrechten. Die Software bietet Funktionen zur Auto- matisierung der Zugriffsvergabe, zur Ermittlung von Konflikten in der Funk- tionstrennung und zur Vereinfachung von Genehmigungsverfahren. Die IT- Abteilung wird spürbar entlastet.

- Abläufe automatisieren**
 SAP GRC Access Control automati- siert selbst komplexeste Genehmi- gungsverfahren. Eine dynamische Workflow-Engine ermittelt auf Basis der Zuständigkeit des Beantragenden und der Art der Anfrage automatisch den geeigneten Genehmigungsweg. Steht der ursprüngliche Adressat nicht zur Verfügung oder antwortet er nicht, leitet die Software das Gesuch automatisch an einen Vertreter weiter. So werden unnötige Verzögerungen vermieden. Falls gewünscht, lassen sich Schleifen zur Risikoanalyse und -eliminierung einbauen.

Abbildung 3: Berech- tigungsanträge mit SAP GRC Access Control einfach und sicher erstellen

The screenshot displays the SAP GRC Access Control interface for a request for approval. The main window shows 'Request No.: 1004' and 'General Information' including user data (Mae Wong) and requestor/manager data (Mae Wong). Below this is a table of role profiles:

System Type	System	Role Profile Name	Type	Role Profile Description	Valid From	Valid To	Owner
SAP	SAP_OR1_800	VIS_FL_AP_DISPLAY_MASTER	AP Display Role	AP Display Role	03/02/2007	12/31/9999	Brian Law (BLAW)
SAP	SAP_OR1_800	VIS_FL_AP_INVOICES	Process Vendor Invoices	Process Vendor Invoices	03/02/2007	12/31/9999	Brian Law (BLAW)
SAP	SAP_OR1_800	VIS_FL_VM_MAINTENANCE	Vendor Maintenance	Vendor Maintenance	03/02/2007	12/31/9999	Perkins (PERKINS)

At the bottom, there are buttons for 'Approve', 'Reject', 'Hold', 'Risk Analysis', 'Select Roles', 'Select PD Profiles', 'Forward Request', and 'Existing Roles'.

- Funktionstrennungskonflikte in Echtzeit erkennen**
 Die Anwendung verhindert Verstöße gegen die Funktionstrennung durch Echtzeitsimulation. Kontrolltätigkeiten werden direkt in die Prozesse des Tagesgeschäfts eingebunden. Unter- nehmen stellen so sicher, dass sie Ver- stöße nicht nur erkennen, sondern gezielt verhindern.
- Genehmigungsprozesse vereinfachen**
 Die Anwendung vereinfacht die Ertei- lung von Zugriffsrechten, indem sie jede Anfrage automatisch um Informati- onen über den Antragsteller aus einem LDAP-Verzeichnis oder einer HR- Datenbank ergänzt. Der zuständige Mitarbeiter erhält per E-Mail den Link zu einer Webseite. Hier kann er den Antrag einsehen und gegebenenfalls genehmigen. SAP GRC Access Control führt daraufhin einen Sicherheits- check durch und aktualisiert die betrof- fenen Benutzerkonten.

Mit SAP GRC Access Control können Business-Manager funktionsabhängige Rollen festlegen und IT-Manager die entsprechenden technischen Berechtigungen definieren.

■ **IT-Abteilung spürbar entlasten**

Anwender können anderen Mitarbeitern den Zugriff auf die von ihnen betreuten Geschäftsprozesse gewähren – ohne spezielles Wissen oder die Hilfe der IT-Abteilung. Sie können einzelne Rollen manuell zuteilen oder den Zugriff komplett in Anlehnung an vorhandene Benutzer mit ähnlichen Rollenprofilen gestalten. Eine weitere Funktion erlaubt Nutzern das selbsttätige Rückstellen von Kennwörtern in einem geschützten Portal. Der Aufwand der IT-Abteilung lässt sich durch diese und andere Maßnahmen um bis zu 50 Prozent reduzieren.

Management von Superuser-Berechtigungen

Auditoren ist der weit reichende Systemzugriff, der in Notfällen so genannten Superusern gewährt wird, ein Dorn im Auge. Was aber können Unternehmen tun, um diesen speziellen Nutzern ein effizientes Arbeiten zu ermöglichen? SAP GRC Access Control ermöglicht es Superusern, Notfallmaßnahmen außerhalb ihrer Rolle in einer kontrollierten und für den Audit transparenten Umgebung durchzuführen. Dort werden alle Aktivitäten lückenlos protokolliert.

■ **Superusern schnell und sicher den Zugriff ermöglichen**

Benötigt ein Anwender Zugriff auf kritische Berechtigungen, erzeugt die Anwendung ein temporäres Benutzerprofil in Form einer ID, mit der er einen umfangreichen, aber kontrollierten Systemzugriff erhält. So kann er ohne weitere Genehmigungsprozedur die Problemlösung in Angriff nehmen.

■ **Aktivitäten zurückverfolgen**

Die SAP-Anwendung beobachtet und protokolliert alle Handlungen eines Superusers – ohne die Protokollfunktionen der betroffenen SAP-Anwendung zu belasten. In detaillierten Berichten können sich Anwender und Auditoren danach ein Bild von den durchgeführten Aktivitäten machen.

Die Protokolle reichen bis zu den Eingaben des Users in einzelne Datenfelder. Die erfassten Daten lassen sich einfach filtern, sortieren und herunterladen. Zudem informiert die Anwendung entsprechende Sicherheitsverantwortliche automatisch über die Inanspruchnahme einer ID. Bei Bedarf lassen sich zu Prüfzwecken detaillierte Protokolle per E-Mail an weitere Personenkreise schicken.

■ **Stets volle Kontrolle**

Mit SAP GRC Access Control haben Sicherheitsverantwortliche die vollständige Kontrolle über die Verwendung von IDs. Sie können Benutzer zuordnen, Zugriffsrechte vergeben, Regeln für den Versand von Benachrichtigungen aufstellen und detaillierte Prüfungen vornehmen.

SAP GRC Access Control gewährleistet eine ordnungsgemäße und schnelle Genehmigung und Erteilung von Zugriffsrechten durch automatisierte Prozesse.

Regelmäßige Überprüfung der Zugangskontrollen

Unternehmensführungen sind angehalten, die Berechtigungen von Usern regelmäßig hinsichtlich der Funktionstrennung zu überprüfen. Das betrifft auch die Bestätigung von Berechtigungen und kompensierende Kontrollen, um die Wirksamkeit der entsprechenden Kontrollen sicherzustellen. Die SAP-Anwendung unterstützt das Management bei der Umsetzung dieser Aufgabe. Gleiches gilt für die Revision. Sie muss sicherstellen, dass Unternehmen sich innerhalb der vorgegebenen Richtlinien bewegen. Deshalb ist es wichtig, nachvollziehen zu können, ob alle Berechtigungen regel- und gesetzeskonform vergeben und alle Funktionstrennungs-Konflikte angemessen kompensiert worden sind. SAP GRC Access Control beweist sich dabei als effektive Hilfe.

Alle Risiken sicher im Griff

Mit SAP GRC Access Control gehen Unternehmen bei der Kontrolle von Risiken in der Zugriffs- und Berechtigungssteuerung, der Einhaltung gesetzlicher Vorschriften und höchster Standards auf Nummer sicher – und reduzieren spürbar ihren manuellen Arbeitsaufwand und Kosten.

Powered by SAP NetWeaver®

SAP-Lösungen basieren auf SAP NetWeaver®. Die Geschäftsprozessplattform führt unterschiedliche Technologiekomponenten zusammen und integriert SAP-Software und Fremdsysteme. Mit SAP NetWeaver sind Unternehmen in der Lage, ihre IT-Systeme schnell an neue Geschäftsprozesse anzupassen. Die Plattform bildet das Fundament für eine konzernweite serviceorientierte IT-Architektur (Enterprise SOA) und ermöglicht es Unternehmen, innerhalb kürzester Zeit neue Geschäftsanwendungen zusammenzustellen oder Verbesserungen an bestehenden Anwendungen vorzunehmen.



Flexible Prozessabbildungen und eine automatisierte hierarchische Rollengenerierung vereinfachen die Anlage und Pflege von Benutzerrollen.

Kurz zusammengefasst

SAP GRC Access Control unterstützt als Schlüsselkomponente der SAP-Lösungen für Governance, Risk und Compliance Unternehmen bei der Überwachung und Steuerung von Zugriffsrechten. Die Lösung beugt Funktionstrennungsrisiken vor, reduziert die Gefahren einer missbräuchlichen Nutzung von Informationen und trägt der Einhaltung internationaler Vorgaben und Auflagen für das Finanz- und Risikomanagement Rechnung.

Herausforderungen

- Zunehmende gesetzliche Auflagen und Anforderungen an eine wirksame Zugriffs- und Berechtigungskontrolle
- Vorbeugung und Schutz vor betrügerischen Handlungen, Identitätsmissbrauch sowie Datendiebstählen und -manipulationen
- Hoher Aufwand für die Evaluierung, den Test und die Administration von Zugriffsregeln und Berechtigungen

Unterstützte Geschäftsprozesse und Softwarefunktionen

- Regel- und gesetzeskonforme Berechtigungsvergabe
- Automatisierung und Vereinfachung damit verbundener Genehmigungsverfahren
- Risikoanalyse und -bereinigung mit permanenten Datenabgriffen
- Echtzeit-Erkennung von Konflikten in der Funktionstrennung auf der Basis eines umfassenden Regelwerks
- Anlage und Administration von Benutzerrollen
- Zuverlässiges und kontrolliertes Management von Superuser-Berechtigungen
- Regelmäßige Überprüfung der Zugangskontrollen

Hauptnutzen

- Unternehmen können mit einem kostengünstigen Zugriffs- und Berechtigungsmanagement regulatorischen und unternehmerischen Auflagen entsprechen und Risiken eingrenzen.
- Automatisierung von Zugriffsvergaben und Genehmigungsprozessen erfolgen auf der Basis durchgängiger Prozesse und reduziert damit spürbar den Arbeitsaufwand.
- Überwachungslücken werden geschlossen.
- Verstöße beim Zugriff auf Produktsysteme können direkt erkannt und verhindert werden.
- Risiken lassen sich auf der Basis von aktuellen Daten zeitnah identifizieren.
- Berechtigungskonflikte hinsichtlich der Funktionstrennung werden frühzeitig sichtbar.
- Regelkonforme Rollen lassen sich einfach definieren und pflegen.
- Die IT-Abteilung wird entlastet.

Weitere Informationen

Sie möchten mehr erfahren? Weitere Informationen finden Sie unter www.sap.de/grc.

50 081 195 (08/01)

© 2008 SAP AG.

Alle Rechte vorbehalten. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign und weitere im Text erwähnte SAP-Produkte und -Dienstleistungen sowie die entsprechenden Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und anderen Ländern weltweit. Alle anderen Namen von Produkten und Dienstleistungen sind Marken der jeweiligen Firmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die vorliegenden Angaben werden von SAP AG und ihren Konzernunternehmen („SAP-Konzern“) bereitgestellt und dienen ausschließlich Informationszwecken. Der SAP-Konzern übernimmt keinerlei Haftung oder Garantie für Fehler oder Unvollständigkeiten in dieser Publikation. Der SAP-Konzern steht lediglich für Produkte und Dienstleistungen nach der Maßgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Aus den in dieser Publikation enthaltenen Informationen ergibt sich keine weiterführende Haftung.