



SAP-Lösungen für Governance, Risk und Compliance unterstützen die Prüfung, Kontrolle und Organisation des unternehmensweiten Zugriffs- und Berechtigungswesens. Die Software hilft, gesetzliche Vorschriften wie den Sarbanes-Oxley Act (SOX) 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.

SAP Technical Brief

SAP-Lösungen für Gouvernance, Risk und Compliance

UNTERNEHMENSWEIT WIRKSAME ZUGRIFFS- UND BERECHTIGUNGSKONTROLLE

Risiken in der Zugriffs- und Berechtigungssteuerung unternehmensweit erkennen, beseitigen und verhindern

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 der Sarbanes-Oxley Act in den USA, der Combined Code und der Turnbull Report in Großbritannien sowie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) in Deutschland 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) helfen Unternehmen im Rahmen eines ganzheitlichen Konzepts, zahlreiche branchenübergreifende und -spezifische Wirtschaftsvorschriften sicher einzuhalten. Integrierte Anwendungen sorgen für eine ordnungsgemäße Zugriffs- und Berechtigungssteuerung. Sie tragen auch zur Eindämmung von Kosten bei. Möglich machen das Funktionen, die Risikofaktoren im gesamten Unternehmen automatisiert identifizieren, beseitigen und dauerhaft bekämpfen. Daraus resultieren Kostenvorteile sowie mehr Sicherheit und Leistungsfähigkeit.

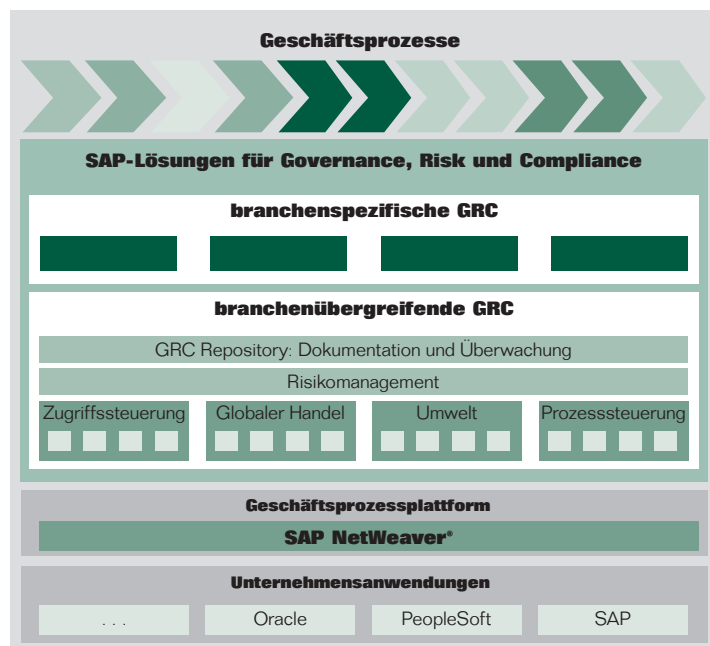


Abbildung 1: Anwendungen zur Zugriffssteuerung: automatische unternehmensweite Kontrolle innerhalb des GRC-Konzepts von SAP

Der ganzheitliche Ansatz eröffnet außerdem Wettbewerbsvorteile: Bisher im Compliance-Management gebundene Ressourcen werden freigesetzt, eine deutliche Ausdifferenzierung gegenüber Konkurrenten ist möglich.

Sorgfältig aufeinander abgestimmte Anwendungen

Mehr als 400 Unternehmen weltweit überwachen die Compliance ihres Zugriffs- und Berechtigungswesen bereits durchgängig mit SAP-Anwendungen. Die aufeinander abgestimmten Anwendungen Virsa Compliance Calibrator, Virsa Role Expert, Virsa FireFighter for SAP und Virsa Access Enforcer (siehe Abbildung 2) bilden eine leistungsstarke Komplettlösung für folgende Aufgaben:

■ Risikoidentifikation

Selbst ungewöhnliche Missbrauchsrisiken in Zugriffsrechten werden in SAP- und Fremdsystemen aufgedeckt. Kunden sind gegen alle möglichen Gefahren geschützt – auch gegen Verstöße hinsichtlich der Funktionstrennung und unzulässige Transaktionen.

■ Risikoabbau und -minderung

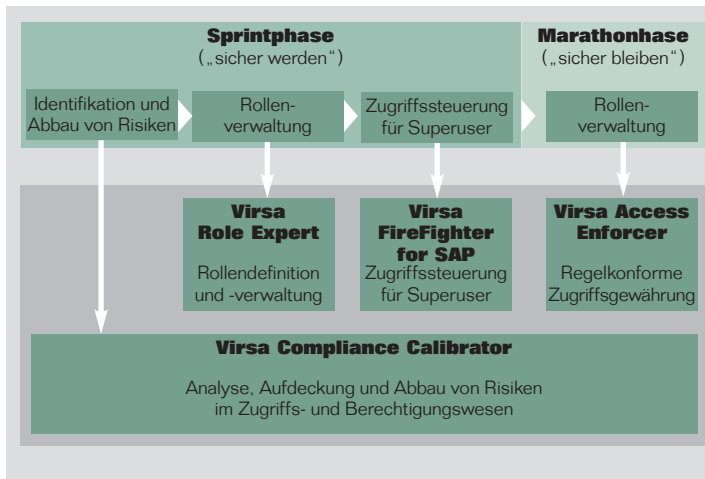
Risiken des Zugriffs- und Berechtigungsmissbrauchs werden mittels automatisierter Workflows und Funktionen wirksam und kostenorientiert behoben und verringert, die Zusammenarbeit zwischen IT-Verantwortlichen und Endanwendern nachhaltig unterstützt.

■ Reporting und Analyse

Umfangreiche Berichte und rollenspezifische Dashboards machen den Erfolg von Compliance-Maßnahmen für das Management messbar. Dieses kann so frühzeitig korrigierende Maßnahmen ergreifen.

■ Risikoprävention

Sind Zugriffs- und Berechtigungsrisiken eingegrenzt, sorgt die Anwendung proaktiv dafür, dass sich keine neuen Risiken in das Produktivsystem einschleichen. In Echtzeit können Anwender das System – ohne jegliche Unterstützung der IT-Abteilung – auf Risiken prüfen. Durch die Automatisierung der Benutzerverwaltung wird Risikoprävention zu einem kontinuierlichen Prozess.



Virsa Compliance Calibrator

Virsa Compliance Calibrator sorgt dafür, dass rund um die Uhr alle Bestimmungen eingehalten werden. Die Software ist in kürzester Zeit einsatzbereit.

■ Aktuelle Daten analysieren

Virsa Compliance Calibrator arbeitet mit permanenten Datenabgriffen in den verschiedenen Systemen. Risiken werden so auf Basis von aktuellen Daten bewertet. Dadurch lassen sich Konflikte unmittelbar nach ihrem Entstehen erkennen, die Ursache ermitteln und Abhilfe schaffen. Ist das System bereit, kann in Simulationen getestet werden, wie sich Änderungen an Berechtigungen oder Benutzerrollen auswirken. So werden Sicherheitsverstöße effektiv verhindert.

■ Versteckte Probleme finden

Virsa Compliance Calibrator hilft Unternehmen, Regelverstöße aufzuspüren, die ansonsten möglicherweise bis zu einem Audit unentdeckt blieben. So kann die IT-Abteilung beispielsweise 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 in SAP-Landschaften. Zudem ermöglicht es die Software auch Anwendern ohne spezielle ERP-Kenntnisse, individuelle Regeln anhand gängiger betriebswirtschaftlicher Ausdrücke zu definieren.

■ Risiken konsequent abbauen

Virsa Compliance Calibrator 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.

Virsa Role Expert

Virsa Role Expert standardisiert und zentralisiert die Anlage von Benutzerrollen. Das reduziert die Gefahr von Fehlern und erleichtert die unternehmensweit einheitliche Durchsetzung bewährter Verfahren. IT-Spezialisten und technische Laien können mit der Software gleichermaßen bequem wie kostensparend Rollen definieren, automatisch Risiken prüfen, Änderungen verfolgen und Wartungsaufgaben durchführen.

■ Auditfähige Rollen definieren

Virsa Role Expert 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 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 dadurch beträchtlich erleichtert. Bevor neue oder ge-

änderte Rollen in das produktive System übernommen werden, prüft Virsa Compliance Calibrator sie zuvor auf mögliche Konflikte hinsichtlich der notwendigen Funktionstrennung.

■ Benutzerrollen automatisch anlegen

Hat der Anwender den Umfang einer Rolle definiert, kann er sie „per Knopfdruck“ anlegen. Die Nutzung des Profilgenerators der SAP-Software macht ein manuelles Zusammenführen von Daten überflüssig. Um die Integrität der Rollen zu gewährleisten, hat der Anwender die Möglichkeit, Rollendefinitionen mit in SAP-Anwendungen hinterlegten Informationen zu vergleichen. Historische Berichte und Analyseergebnisse werden von Virsa Role Expert automatisch mit Blick auf spätere Audits erfasst. Rollenverantwortliche können komfortabel die von Auditoren geforderten Dokumente wie Rollendefinitionen oder detaillierte Änderungsprotokolle erstellen sowie Testergebnisse kontrollieren.

Virsa FireFighter for SAP

Auditoren ist der weitreichende 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? Virsa FireFighter for SAP 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 Zugriff ermöglichen

Benötigt ein Anwender Hilfe durch einen IT-Superuser, erzeugt die Anwendung ein temporäres Benutzerprofil, eine so genannte FireFighter-ID, mit dem er einen umfangreichen, aber kontrollierten Systemzugriff erhält. So kann er sich ohne weitere Genehmigungsprozedur an die Problemlösung machen.

■ Aktivitäten zurückverfolgen

Virsa FireFighter for SAP 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 FireFighter-ID. Bei Bedarf lassen sich zu Prüfzwecken detaillierte Protokolle per E-Mail an weitere Personenkreise schicken.

■ Stets volle Kontrolle

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

Virsa Access Enforcer

Erteilen oder modifizieren Unternehmen Systemzugriffe, überblicken sie nicht immer alle Auswirkungen auf die rechtlich geforderte Funktionstrennung. Virsa Access Enforcer sorgt während der gesamten Betriebszugehörigkeit eines Mitarbeiters

The screenshot shows the 'Virsa Access Enforcer' interface. At the top, there are tabs for 'Inform', 'Administration', and 'Configuration'. The main area is titled 'Request No: 4010'. Below this, there are sections for 'General Information', 'User Data', and 'Requestor and Manager Data'. The 'User Data' section includes fields for User (Wong/Mey), E-Mail (emenduser@virsa-systems.com), Telephone ((510) 851-5550), Location (United States Headquarter), Employee Type (Regular), Request Type (New), and Priority (High). The 'Requestor and Manager Data' section includes fields for Requestor (Wong/Mey), E-Mail (emenduser@virsa-systems.com), Manager (Fox/Wilson), and E-Mail (emuser@virsa-systems.com). Below these sections, there is a table with columns for 'System', 'Role/Profile Name', 'Type', 'Role/Profile Description', 'Valid From', 'Valid To', and 'Owner'. The table contains two rows: one for 'ERP' with 'Z AP PAYABLE' and 'Vendor Invoice Processor', and another for 'ERP' with 'Z AP SUPERVISOR' and 'Accounts Payable Supervisor'. At the bottom, there are buttons for 'Approve', 'Reject', 'Hold', 'Risk Analysis', 'Select Roles', and 'Select PD Profiles'.

Abbildung 3: Berechtigungsanträge mit Virsa Access Enforcer einfach und sicher erstellen

für die ordnungsgemäße Erteilung von Zugriffsrechten. Die Software bietet Funktionen zur Automatisierung der Zugriffsvergabe, zur Ermittlung von Konflikten in der Funktionstrennung und zur Vereinfachung von Genehmigungsverfahren. Die IT-Abteilung wird spürbar entlastet.

■ Abläufe automatisieren

Virsa Access Enforcer automatisiert selbst komplexeste Genehmigungsverfahren. 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 nicht, leitet die Software das Gesuch an einen Vertreter weiter. So werden unnötige Verzögerungen vermieden. Falls gewünscht, lassen sich Schleifen zur Risikoanalyse und –eliminierung einbauen.

■ Funktionstrennungskonflikte in Echtzeit erkennen

Virsa Access Enforcer verhindert Verstöße gegen die Funktionstrennung durch Echtzeitsimulation der Daten in einem Produktivsystem sowie Tests der gesamten SAP-Softwarelandschaft. Kontrolltätigkeiten werden direkt in die Prozesse des Tagesgeschäfts eingebunden. Unternehmen stellen so sicher, dass sie Verstöße nicht nur erkennen, sondern gezielt verhindern.

■ Genehmigungsprozesse vereinfachen

Die Anwendung vereinfacht die Erteilung von Zugriffsrechten, indem sie jede Anfrage automatisch um Informationen 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. Virsa Access Enforcer führt daraufhin einen Sicherheitscheck durch und aktualisiert die betroffenen Benutzerkonten.

■ IT-Abteilung spürbar entlasten

Mit Virsa Access Enforcer können Anwender 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.

Alle Risiken sicher im Griff

Mit SAP-Lösungen für Governance, Risk und Compliance 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. Weitere Informationen finden Sie unter www.sap.de/grc

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.

www.sap.com/contactsap

THE BEST-RUN BUSINESSES RUN SAP™



50 081 195 (06/09)

© 2006 by SAP AG. All rights reserved. SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary. Printed on environmentally friendly paper.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.