

SAP Solution in Detail

SAP Solutions for Governance, Risk, and Compliance

SAP Access Control

Minimize Access Risk and Prevent Fraud – With SAP® Access Control



Table of Contents

3	Quick Facts	9	A Flexible, Unified Solution for Business Users
4	The Access Governance Balancing Act: Risk Versus Cost		Compliant Identity Management Across Your IT Landscape
	Overview		Real-Time Risk Analysis and Request Management for Non-SAP Software
5	The Solution: SAP Access Control		Reporting Powered by the SAP HANA Platform
	Reduce Access Risk and Fraud		Integrated Platform for Governance, Risk, and Compliance
	Reduce the Cost of Access Management		Find Out More
	Reduce the Cost of Ongoing Compliance Activities		
7	Features and Functions		
	Automated, Real-Time Risk Analysis		
	Streamlined User-Access Management		
	Comprehensive Business Role Management		
	Periodic Access Certification Reviews		
	Closed-Loop, Emergency Access Management		
	Advanced Reports, Dashboards, and Analytics		

Quick Facts

Summary

With the SAP® Access Control application, you can move beyond manual processes for managing access risk. The application enables you to manage segregation of duties (SoD), critical and sensitive access, and superuser access effectively and efficiently. It automates the compliant provisioning of users, periodic user and role certifications, and the maintenance of compliant roles. This allows you to manage access risk on an exception basis and focus on value-adding initiatives.

Business Challenges

- Introduce a unified, enterprise-wide approach to managing access risk
- Increase business and IT collaboration
- Reduce time and cost of audits
- Facilitate streamlined, cost-effective processes for dealing with audit and fraud issues
- Eliminate the need for manual provisioning

Key Features

- **Access-risk analysis** – Accurately identify and remediate SoD and critical access violations in real time
- **User-access management** – Automate access assignments across SAP and non-SAP software while preventing access violations with embedded risk analysis
- **Role management** – Define and maintain compliant roles in business-friendly terms and language
- **Periodic certification of authorizations** – Conduct periodic user-access reviews and ensure SoD mitigations are effective on a regular basis
- **Emergency access management** – Confidently authorize users to perform superuser activities outside their role using “firefighter” login IDs in a controlled, auditable environment

Business Benefits

- **Reduced access risk**, internal fraud, and loss of revenue due to employee error
- **Reduced cost** of enterprise-wide access management
- **Efficient, cost-effective audits** and ongoing compliance activities

For More Information

To find out more about how SAP Access Control and other SAP solutions for governance, risk, and compliance can benefit your business, visit us at www.sap.com/grc.

The Access Governance Balancing Act: Risk Versus Cost

Using manual processes and spreadsheets to manage access risk is not only resource intensive and time consuming; it's costly and can expose you to unnecessary risk. With the SAP® Access Control application, you can automate key processes to detect, remediate, and ultimately **prevent access violations**, streamline user provisioning, and centralize role management. This helps reduce the cost of access management, audit, and ongoing compliance activities and minimize the risk of internal fraud.

OVERVIEW

Most, if not all, organizations have measures in place to adhere to internal policies and external compliance requirements related to managing access risk. By and large, these measures are manual, and the cost and effort required to enforce these policies on a continual basis can be overwhelming. In addition, manual processes are difficult to manage, sustain, and scale. Automated solutions for managing access and access risk are required to address these key business challenges.

Eliminate Inefficient and Costly Manual Processes

Many organizations today have inefficient processes in place in their attempt to maintain ongoing access-risk compliance. They include tools such as e-mail, spreadsheets, and paper files, each of which involves multiple manual steps. Manually transitioning end users to a new assignment or hiring new employees and granting them access can take weeks away from productive work. This approach often leaves out risk analysis altogether. Employees who perform the work of granting and rescinding access to business applications often overlook how the changes may violate segregation-of-duties (SoD)

rules and critical access risk. With no automated workflow, providing a record of changes must be performed manually as well.

Unify the Approach to Managing Access Risk

Today's increasingly complex, ever-changing business environment often results in organizations adopting a fragmented approach to managing access risk. They may consider users and authorizations at the single-system level, but not user access across the enterprise. This leads to an incomplete or false view of risk and the controls put in place to manage that risk.

Even in organizations where the process is partially standardized, very little communication or collaboration occurs between IT and the business, due to little, if any, understanding of the other's domain. While business owners are accountable for managing user-access risk, they do not always understand technical IT terms or how technical authorizations work. IT staff members, on the other hand, do not have the business knowledge to understand the risk to be considered when granting access. As a result, companies ineffectively manage the risk associated with users who have

been granted more access than they need to business applications. Further, in most organizations IT is usually overburdened due to manual user-access management tasks, including role management, role provisioning, and password reset requests.

Prevent Access-Risk Violations

In many organizations, upholding internal SoD policies and managing critical access is more of a detective process than a preventive one. If access-risk analysis is not built into the user and role maintenance processes to prevent access violations, it becomes a separate initiative requiring additional time, money, and resources.

Gain Visibility of User Access and Access Risk

Managing user access and access risk manually makes it nearly impossible to achieve a clear view of access governance. When organizations manually manage thousands of users, roles, and authorizations, they cannot see where users have too much access or access to sensitive data in violation of company policy, which could impact ongoing compliance initiatives. Manual processes for managing emergency or superuser access are just as difficult to administer. Both continue to be a top find in auditing results.

The Solution: SAP Access Control

With SAP Access Control, you can move beyond manual processes for managing access risk. The application lets you manage SoD, critical and sensitive access, and superuser access. It automates the compliant provisioning of users, periodic user and role certifications, and the design and maintenance of compliant roles. Because you manage access risk on an exception basis, you can focus your time and resources on value-adding initiatives.

REDUCE ACCESS RISK AND FRAUD

SAP Access Control delivers risk analysis and remediation functionality that enables businesses to analyze critical access and SoD conflicts based on real-time data. The application identifies potential access risks using a comprehensive rule set based on business process expertise and best-practice experience.

SAP Access Control includes rules for the most common business functions and associated risks, which is requisite for identifying SoD violations and critical access risks. The rules database is compatible with SAP and non-SAP software – including products from Oracle Corporation, PeopleSoft Inc., and JD Edwards, as well as legacy software and applications not classified as enterprise resource planning (ERP) software. This comprehensive approach lets you monitor risk across business applications enterprise-wide to establish a consistent policy and prevent duplication of effort.

Upon identifying SoD and critical access violations, business managers review the issues identified in an initial risk analysis and then take action to remediate these risks. Actionable reporting enables users to mitigate the risk using a customer-defined set of mitigating controls.

Alternatively, requests can be created to modify user access in a way that will remove the risk violation completely.

Simulation functionality is built in to support a preventive approach to managing user access. IT can simulate authorization changes for users and roles before modifying the access, thus reducing access risk and opportunity for internal fraud.

REDUCE THE COST OF ACCESS MANAGEMENT

The revenue and resources required to enforce access-risk management on an ongoing basis can be overwhelming. Even after conducting an initial cleanup, new risks may arise on a daily basis as user assignments and business needs change.

Most organizations have measures in place to address access risk and compliance requirements related to access risk. These measures are usually manual, and the cost and **effort required to enforce access-risk policies manually** can be overwhelming.



SAP Access Control automates access management activities throughout the employee lifecycle. Employees can re-request access using a self-service portal, which streamlines the request process and reduces the IT resources required. Facilitated by the SAP Business Workflow tool, approvers receive an e-mail notification of an employee's request to modify access. The application automatically tests for SoD and critical-access violations, facilitates the removal of SoD or critical-access risks, and enforces the assignment of mitigating controls prior to approval. With this functionality, the application prevents unmitigated access-risk violations from being introduced into the environment. Additionally, a dynamic workflow process provides end-to-end automation for user provisioning. Password self-service features are included, and integration with market-leading identity management applications supports compliant identity management across the enterprise.

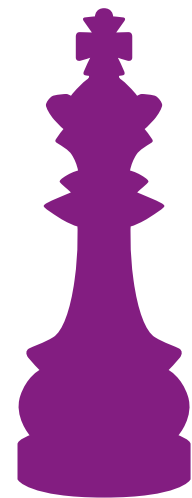
REDUCE THE COST OF ONGOING COMPLIANCE ACTIVITIES

Inefficient compliance processes can be costly and difficult not only to manage but to scale as well. SAP Access Control helps customers reduce the cost of ongoing compliance activities by:

- Maintaining a comprehensive audit trail of user and role management activities
 - Centrally storing all logs and approvals, thereby eliminating the need to search different repositories to prove compliance during an audit
 - Automating compliance reviews of user access, role authorizations, risk violations, and control assignments, saving thousands of hours that manual, error-prone processes require
 - Delivering a closed-loop process for managing emergency access, which continues to be a number-one audit issue
- Automating the process of requesting, approving, and assigning access; monitoring and logging emergency activities; and storing the reviewed activities in a central location
 - Providing continued visibility of the access-risk management process with embedded reports, dashboards, and analytics, as well as custom reporting options

With these features, customers are not only able to reduce audit costs, but they can also reduce the cost of maintaining sustainable compliance on an ongoing basis.

Today's increasingly complex business environment often results in organizations adopting a **fragmented approach to managing access risk**. Companies usually consider the users and authorizations they have at the single-system level – if at all.



Features and Functions

SAP Access Control delivers a broad range of features that enable customers to continuously manage access risk.

AUTOMATED, REAL-TIME RISK ANALYSIS

SAP Access Control enables companies to accurately identify and analyze risk violations in real time, which cannot be accomplished with a manual process. The security model on which the SAP software is based is very detailed, and in many cases customers have violations in their environment that they are not aware of. The application enables customers to see deep into the application security model, making it possible for them to eliminate false positives and make accurate assessments the first time they perform a risk analysis.

But the software doesn't stop there. SAP Access Control is a single solution for automated, real-time risk analysis across your SAP and non-SAP software landscape. The application performs single-system and cross-system risk analysis, giving companies the ability to look at user authorizations holistically across the enterprise.

SAP Access Control is delivered with a comprehensive library of configurable risks and rules based on best-practice experience. Simulation functions allow customers to run what-if scenarios to understand whether changes to authorizations at the user or role level will introduce new risks, and actionable reporting enables you to assign mitigating controls for identified risks directly from reports. The application collects transaction usage data and provides details on when users executed conflicting or critical transactions, with date and time stamps. Customers can enable alert functions to notify process owners when transactions

were executed that violated specific SoD or critical transaction rules.

These features enable you to continuously monitor your business applications for SoD and critical-access conflicts.

STREAMLINED USER-ACCESS MANAGEMENT

SAP Access Control streamlines the access request process and automates access management activities throughout the employee lifecycle with a flexible, rules-driven approach. The access request management functions of SAP Access Control are standardized on the technology of the SAP Business Workflow tool, a technology that customers of the SAP ERP application are familiar with. Automating user-access management tasks – such as the user-access request, risk analysis, and approval process – makes it faster and easier for users to obtain the access that they need while maintaining compliance.

Requests for user access can be drawn from a number of different sources. For each, a what-if simulation can be embedded during the provisioning process to assess the risk impact of role assignments across business applications. Additional features include:

- Integration with HR software, including the SAP ERP Human Capital Management (SAP ERP HCM) solution, which can trigger changes to user assignments based on new hire, transfer, or termination actions in the HR software
- Integration with the SAP NetWeaver® Identity Management component and third-party identity management software through standard Web services
- A self-service portal for business users to request access for themselves or others

The SAP GRC Access Approver mobile app simplifies the approval process even further, allowing requests for user access and emergency access to be addressed from supported mobile devices. Unlike other mobile approval products, SAP GRC Access Approver not only shows the access being requested but the potential risk associated with assignment as well as any mitigating controls that may have been assigned.

These features enable you to enforce the mitigation of risk before the assignment of roles to users.

COMPREHENSIVE BUSINESS ROLE MANAGEMENT

As a single authoritative source for role definition, SAP Access Control supports flexible role-building methodologies. The application translates technical access terms into common business language. This facilitates collaboration between IT and business owners by allowing them to use the same, consistent terms to document role definitions.

The flexible role-building methodology guides you through a step-by-step process of building and maintaining roles. Business roles, which consist of one or more technical roles from one or more software systems, can be maintained and assigned to users.

By incorporating SoD and critical-access rules into the role design process, the application allows you to define compliant roles proactively. The application also offers functionality to perform preventive simulations to show you the impact access changes will have before they are introduced into a production environment. Simulations can be performed at the user or role level to test for access-risk violations.

By automating the role management process, SAP Access Control helps businesses reduce the cost of role maintenance, eliminate errors that can result from manual processes, and enforce best practices.

PERIODIC ACCESS CERTIFICATION REVIEWS

SAP Access Control automates the periodic review of users, roles, and risks in four key areas:

- User-access review – a review of user-to-role assignments based on real-time assignments
- Role certification – a review of the authorizations and content in each role
- Role affirmation – a review of role assignments by role owner
- Access-risk reviews – a complete certification of access risks (SoD and critical access) based on real-time assignments

CLOSED-LOOP, EMERGENCY ACCESS MANAGEMENT

Granting emergency access to SAP ERP leads to one of the most common audit issues SAP customers experience today. You may have additional accounting personnel who need to post payments during the month-end close or IT personnel that

require elevated access to support the business. If system access is too severely restricted, costly and unproductive delays can occur as approval is granted, new access privileges are created, and emergency access is granted.

SAP Access Control enables rapid response with functionality that authorizes users to perform activities outside their role using “firefighter” login IDs with superuser privileges in a controlled, auditable environment.

With a self-service emergency-access request and workflow approval process, the application efficiently creates emergency access for any user and allows companies to quickly resolve this common audit issue, significantly reducing the time required to perform critical tasks.

Once a user has completed the activities using the firefighter ID, a request containing detailed usage information is created and sent to a process owner for review. Any exceptions noted during review between intended and actual usage are also managed via workflow. Escalation procedures can be put in place to ensure all logs are reviewed and approved.

Usage data and a request history are retained for audit and reporting purposes. These features enable customers to confidently manage emergency access and reduce audit costs.

ADVANCED REPORTS, DASHBOARDS, AND ANALYTICS

SAP Access Control delivers automated, prebuilt reporting for comprehensive visibility into access risk. SAP BusinessObjects™ Dashboards software and SAP Crystal Reports® software are embedded in the application, providing real-time visibility to effectively manage access risk in five key areas:

- Access-risk analysis reports reveal users, roles, profiles, and select HR objects that violate SoD or critical-access rules.
- Access request reports show details related to access request status and history, including service-level reporting.
- Role management reports include role-to-role and user-to-role comparison and change history reporting.
- Emergency access reports display detailed and summary usage information based on emergency access privileges, as well as status and history of emergency access log reviews.
- Audit and security reports show usage statistics for transactions executed by users and roles, as well as expired and expiring roles for users.

The application’s open framework also allows for customized reporting with external analytic and reporting solutions.

SAP Access Control **streamlines the access request process** and automates access management activities throughout the employee lifecycle with a flexible, rules-driven approach.



A Flexible, Unified Solution for Business Users

Built on the ABAP® programming language and tightly integrated with SAP ERP, SAP Access Control offers a single solution for managing segregation of duties, critical access, emergency access, request management, role management, and user certifications. The flexible framework enables you to leverage existing technology investments to extend the value of SAP Access Control across the enterprise, reducing your total cost of ownership.

COMPLIANT IDENTITY MANAGEMENT ACROSS YOUR IT LANDSCAPE

SAP Access Control integrates with SAP NetWeaver Identity Management and other third-party identity management applications for compliant identity management across your IT landscapes.

REAL-TIME RISK ANALYSIS AND REQUEST MANAGEMENT FOR NON-SAP SOFTWARE

Our partnership with Greenlight Technologies allows customers to extend real-time risk analysis and request management functions to non-SAP software. Connections to software from Oracle, JD Edwards, and PeopleSoft are delivered with SAP Access Control. Greenlight Technologies extends these same functions to other business applications through its RTA Design Studio software, providing visibility into access risk across the enterprise.

REPORTING POWERED BY THE SAP HANA® PLATFORM

Through the SAP HANA® Analytics Foundation for SAP solutions for GRC and integration with the SAP NetWeaver Business Warehouse application, a virtual data model is exposed to enable custom reporting through SAP BusinessObjects software and other industry-standard tools.

These robust reporting options deliver the transparency that is required by regulators and auditors and give organizations the confidence essential for successful business management. They offer the flexibility to innovate business processes and improve the productivity of managers, thereby significantly lowering the overall cost of compliance.

INTEGRATED PLATFORM FOR GOVERNANCE, RISK, AND COMPLIANCE

SAP Access Control runs on the same platform as the SAP Risk Management application and the SAP Process Control application, delivering an integrated basis for managing an effective governance, risk, and compliance (GRC) program. This harmonization enables shared processes, controls, master data, and more across all risk, controls, policy, and compliance management activities. This unified technology platform reduces your cost of ownership through lower implementation, administrative, and maintenance costs.

FIND OUT MORE

To find out more, contact your SAP representative or visit us on the Web at www.sap.com/grc.



www.sap.com/contactsap

CMP4157 (13/01)

© 2013 SAP AG or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

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.

SAP 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 other countries.

Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices.



The Best-Run Businesses Run SAP™