SAP Solution in Detail
SAP NetWeaver

SAP NetWeaver Identity Management

Business-Driven, Compliant Identity Management

The Best-Run Businesses Run SAP™

Table of Contents

3 **Quick Facts**

4 **Business Challenges**

Identity Management for the User Lifecycle

5 **The Solution**

Supporting a Heterogeneous IT Landscape

Providing Business-Driven Identity Management

Identity Federation and Single Sign-On

8 **Features and Functions**

10 **The Benefits**

For More Information

Quick Facts

Summary
Identity management is becoming a key challenge, as organizations must ensure that users have the right access to applications in a timely manner and that data is secure. The SAP NetWeaver® Identity Management component addresses this challenge by helping you align identity management with your organization's key business processes.

Business Challenges
- Reduce operational costs in complex system landscapes
- Manage access to applications
- Comply with local and global regulations

Key Features
- **Business-driven, compliant identity management** – Align identity management with business processes running in SAP® applications; fulfill compliance requirements by integrating SAP NetWeaver Identity Management with the SAP Access Control application
- **Provisioning, workflow, and approvals** – Assign and maintain user access rights across multiple systems; provision employees and business partners; audit all changes
- **Password management** – Provide password self-service functionality and password synchronization across all connected target systems
- **Roles and entitlements** – Align roles with business processes rather than technical directory structures
- **Reporting and auditing** – Produce reports based on current access and past events
- **Identity federation** – Enable cross-enterprise identity management and single sign-on in on-premise and on-demand environments

Business Benefits
- **Lower costs and increased productivity** due to tight integration with your business processes across heterogeneous systems
- **Compliance with regulatory requirements** for auditability of access to applications, minimizing segregation-of-duties risks

For More Information
Call your SAP representative today, or visit us on the Web at www.sap.com/platform/netweaver/components/IDM/index.epx.

Business Challenges

Managing Costs, Process Change, and Compliance

With the SAP NetWeaver® Identity Management component, you can integrate identity management with the business processes within and beyond your enterprise. Identity federation facilitates joint authentication and single-sign-on solutions for secure identity management across company boundaries. This approach helps overcome the challenges involved in managing users in heterogeneous IT landscapes – system complexity, constantly evolving user tasks, and mandates for tracking who had access to which applications when.

Identity management solutions address several key business challenges.

High operational costs and risks – Complex system landscapes require that your IT department maintain multiple sources of identity data, entering data for each user as well as assigning permissions in multiple systems. Having to provision users in multiple systems translates into delays in making new employees productive. It also presents risks when employees who have changed roles or have left the organization continue to have access longer than they should. Paper-based approval processes further complicate this process, and users are dependent on help desk staff for password resets and changes in access or permissions.

Changing business consumption models – In today's complex business environment, organizations are increasingly interconnected. Business processes are extended across corporate boundaries with participants from multiple organizations, including partners and customers. As new consumption models are introduced in this context in response to competitive pressures, managing access to the applications by participants from within as well as across enterprise boundaries becomes a challenge.

Increasing compliance requirements – One of the key factors driving the adoption of identity management solutions in the past few years is compliance requirements. Laws such as the Sarbanes-Oxley Act, Gramm-Leach-Bliley Act (for financial institutions), and Health Insurance Portability and Accountability Act require that your organization be able to state with certainty who had access to what system resources and when. Identity management solutions help you achieve compliance, provide needed audit trails, and prevent unauthorized access.

IDENTITY MANAGEMENT FOR THE USER LIFECYCLE

A comprehensive identity management solution covers the entire lifecycle of a user, from the onboarding process of a new employee to the termination of an employment contract. If you don't have an identity management solution, the work required to provision and manage user access in a compliant and auditable way is labor intensive, repetitious, and error prone.

This problem is compounded when you consider the typical user lifecycle within an organization. When an employee is hired, your organization gives him or her certain permissions in a variety of systems. Later, the employee may receive a promotion or change roles and so receive new, additional permissions. Furthermore, you may need to grant other temporary privileges for some year-end activity or while an employee is covering for a colleague on vacation. Thus, an employee typically tends to accrue privileges over time and often continues to have access that is no longer required for the current role. This is, of course, a security risk. But it is also a potential compliance violation. Adding a new role might cause conflicting authorizations for the user. Consider this example: A purchasing manager is authorized to issue orders to external vendors – for example, to buy office supplies. To step in for a colleague who's on sick leave, this purchasing manager temporarily needs the authorization to create vendors in the system. The employee could now misuse his roles, create a new (fictitious) vendor, and issue an order. To minimize the risk that comes from such segregation-of-duties violations, a compliance check must be performed for all role assignments that apply to critical business processes, such as enterprise resource planning (ERP) system roles. Finally, when the employee leaves your company, the access that this user has may still not be revoked, perhaps even years later, which presents obvious and ongoing security risks to your organization.

At each stage, you need to give the user access to the right set of applications according to his or her current role. SAP NetWeaver Identity Management helps you manage this process centrally, across SAP® solutions as well as heterogeneous, non-SAP applications.

The Solution
How SAP NetWeaver Identity Management Can Help

SAP NetWeaver Identity Management can help your organization grant and manage user access to heterogeneous applications securely and efficiently, in alignment with your business processes and in accordance with audit and compliance requirements.

The solution provides a central mechanism for provisioning users and assigning the appropriate business roles. It also supports related processes such as password management, self-service, and approvals workflow. SAP NetWeaver Identity Management supports user provisioning by offering:

- One central place to manage users in SAP and non-SAP applications regardless of the individual data stores (for example, changing a phone number or e-mail address automatically updates all relevant systems)
- Tight integration with your company's business processes
- Centralized reporting functionality to address the pressing need for compliance and auditability using the SAP NetWeaver Business Warehouse application, mapping of one user to identities in all systems, and fully auditable user access across the entire IT landscape
- Password-reset and lost-password management functionality for end users, alleviating help desk workload and reducing operational costs
- Built-in identity federation functionality for cross-company identity management processes and single sign-on
- Integration with the SAP NetWeaver Single Sign-On application to support end-to-end single sign-on and encryption in distributed environments, including all SAP GUIs as well as Web-based front ends

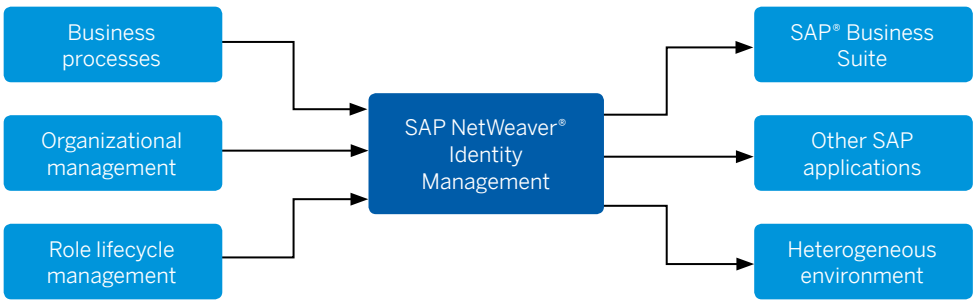
SUPPORTING A HETEROGENEOUS IT LANDSCAPE

SAP NetWeaver Identity Management enables you to streamline provisioning of users into all applications – SAP and third-party – as well as operating systems, file systems, and databases via a comprehensive, constantly expanding connector framework (see Figure 1). The integration is based on open communication standards to enable the integration of virtually all applications, including Microsoft Active Directory, Microsoft Exchange, IBM Lotus Notes, and many others. The integration of SAP NetWeaver Business Warehouse allows for highly customized, differentiated, state-of-the-art reporting.

PROVIDING BUSINESS-DRIVEN IDENTITY MANAGEMENT

Identity management solutions evolved from the need for IT organizations to efficiently manage users across multiple applications. These solutions were essentially IT efficiency tools that streamlined the process of user management by providing a central mechanism to enable these processes. As organizations achieve these efficiencies and realize the value of these solutions, it is becoming apparent that you can accrue greater benefits. You can gain these benefits by aligning the user management functionalities more closely with the business processes that these users access.

Figure 1: Support for Heterogeneous Landscapes in SAP NetWeaver Identity Management



SAP NetWeaver Identity Management is integrated with SAP Business Suite software. This comprehensive support for user provisioning is driven by the business processes implemented by the various applications of SAP Business Suite. For example, integration with the SAP ERP Human Capital Management solution automates identity management processes on the basis of employee creation and status change events triggered by HR business processes, as shown in Figure 2.

However, integration is not limited to employee processes. Identity management processes for business partners and students are also supported, such as the automated creation of users and corresponding business partners in the SAP Customer Relationship Management and SAP Supplier Relationship Management applications.

SAP NetWeaver Identity Management offers a convenient but powerful role concept (see Figure 3). Business roles, which are defined as part of a business process, can be assigned to users. These business roles consist of one or more technical roles, which are system specific and represent access information or technical authorizations. These include authorization roles such as those for SAP software systems that are based on the ABAP® programming language or groups for Microsoft's Active Directory. By focusing on business processes and business roles, SAP NetWeaver Identity Management lets you start with business requirements and encapsulate the complexity of managing technical roles and access. When you assign a business role to a user, all technical roles for that business role and any role below it in the hierarchy are assigned to the user. In addition, workflow and provisioning is automatically triggered.

Figure 2: Integration of HR Processes with SAP NetWeaver Identity Management

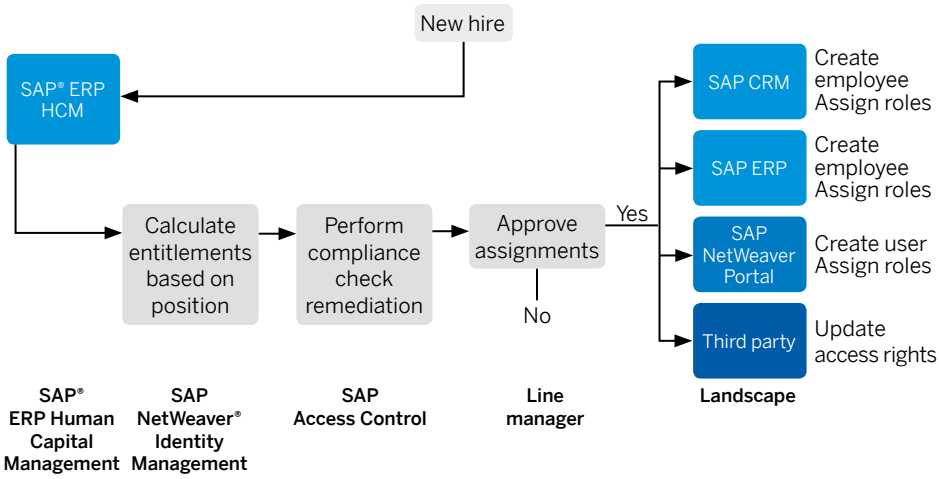
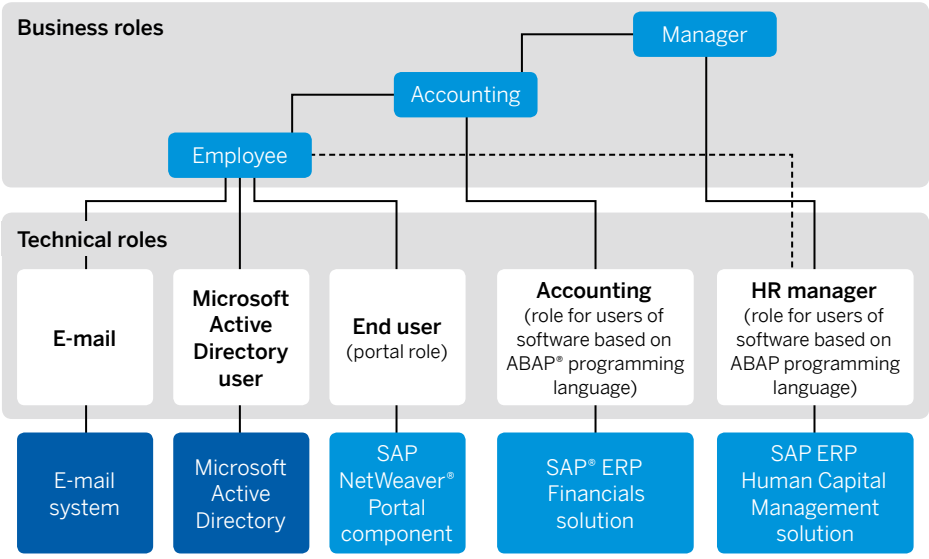


Figure 3: Business Roles and Technical Roles



By complementing your identity management functionality with a solution for governance, risk, and compliance that manages access control, you can enable compliant identity management (see Figure 4). In other words, you can ensure that roles and authorizations assigned to a user do not contain conflicting rights. You're not only securing the identity management process but also making it completely compliant and auditable. SAP NetWeaver Identity Management offers compliant user provisioning and full reporting and audit functionalities. By integrating SAP NetWeaver Identity Management with SAP solutions for governance, risk, and compliance (GRC), you can prevent segregation-of-duties violations that can occur when roles with conflicting permissions are assigned to a user and put mitigating controls in place. Your organization can get clean, stay clean, and stay in control of access to all applications in the system landscape, from SAP Business Suite to third-party applications.

IDENTITY FEDERATION AND SINGLE SIGN-ON

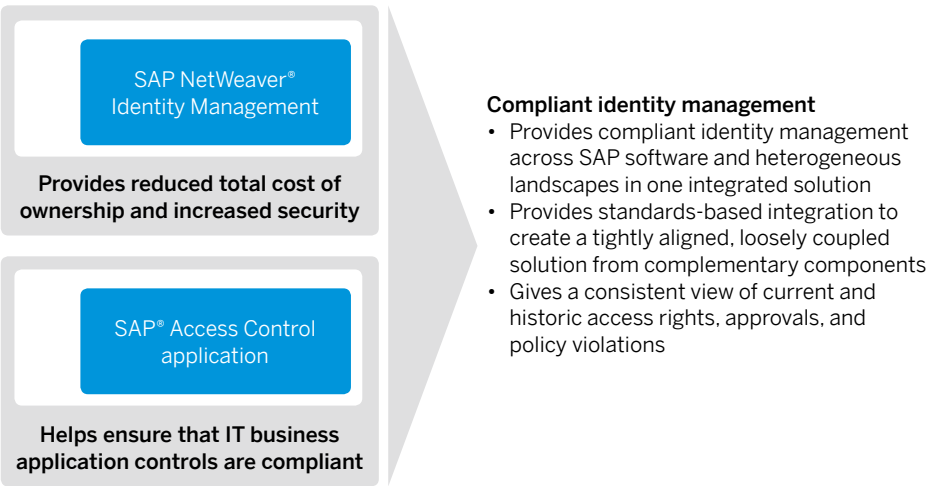
As business processes are no longer confined to corporate boundaries, and IT applications are increasingly moving from on-premise to on-demand or cloud processes, identity management is becoming an extremely important factor in a company's security strategy. The concept of identity federation describes the process of authenticating a user across multiple IT systems and organizations. An airline passenger, for example, could be a car rental customer as well. If the airline and the rental car provider have entered into a federation agreement, which means that they have agreed to mutually trust each other's authentication of their customers, customers must only authenticate themselves once. Their authenticated identity can then be transferred from the airline's system to the rental car provider's system or vice versa.

Federation is enabled through the use of open industry standards, such as the Security Assertion Markup Language (SAML). SAP NetWeaver Identity Management contains the complete set of functionality needed to set up a fully integrated and secure identity federation process. Both an identity provider that issues SAML assertion tickets, which can be used for authentication in a browser-based federation process, and a security token service for Web service environments are included in the identity management solution.

Integration with SAP NetWeaver Single Sign-On offers comprehensive single sign-on and encryption across organizational and technical boundaries. SAP NetWeaver Single Sign-On provides state-of-the art technologies for integrating heterogeneous system landscapes into one single-sign-on process, stretching from SAP GUI front ends to Web-based applications. It protects your communication channels with sophisticated, standards-based encryption technologies and at the same time adds convenience in day-to-day business operations.

The new ID service enables single sign-on across the SAP software landscape, as well as centralized user information management – taking a fragmented process and turning it into a streamlined user experience. This on-demand deployment bridges the gap between customers' on-premise applications, on-demand applications from SAP, and third-party on-demand applications by verifying user identities, granting authentication, and enabling secure single sign-on across the software landscape.

Figure 4: How Business-Driven Compliant Identity Management Works

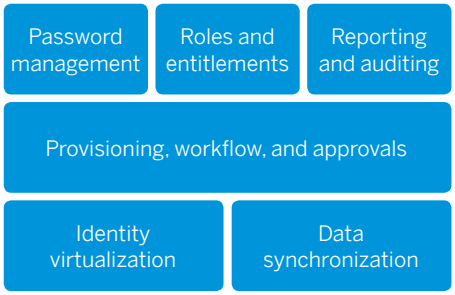


Features and Functions

What You Can Do with SAP NetWeaver Identity Management

SAP NetWeaver Identity Management consists of two main components – the identity center and the virtual directory server – that combine to deliver the functions shown in Figure 5.

Figure 5: Components of SAP NetWeaver Identity Management



The main functions of SAP NetWeaver Identity Management include:

Business-driven identity management processes – Tightly integrated into your SAP Business Suite applications, SAP NetWeaver Identity Management offers a one-step approach to user administration for your entire SAP and non-SAP software landscape.

Reporting and auditing – Critical for compliance, extensive auditing functionality enables you to produce reports based on current access and past events. If questions come up, reports can conclusively state whether the person in question had entitlements to particular applications and associated features and functions. You can transparently maintain all changes to data, user access rights, and administrative permissions. Tight integration with the SAP Access Control application, an SAP solution for GRC, allows for the effective mitigation of segregation-of-duties risks and a fully compliant user-provisioning process.

Provisioning, workflow, and approvals – Business rules and policies drive assignment and maintenance of user access rights across multiple systems. You can quickly provision employees as well as business partners, and all changes and approvals are fully auditable.

Identity virtualization – SAP NetWeaver Identity Management provides an integrated, unified view of the virtual identity of users, as well as identity services to let you leverage identity information and access rights across networks.

Password management and employee self-service – The software supports self-service password reset and password synchronization across all connected target systems, as well as the ability to perform self-service updates of personal information. These functions reduce the cost incurred by your help desk in servicing password resets.

Roles and entitlements – Roles align with business processes rather than technical directory structures. Users are assigned roles and given certain privileges, called entitlements, that enable access to various systems.

Identity federation – Standards-based support for identity federation processes helps ensure convenient and secure interenterprise identity management. Integration with SAP NetWeaver Single Sign-On enables comprehensive, standards-based single sign-on and encryption of communication channels across the enterprise. The ID service facilitates secure single sign-on in cloud environments.

SAP NetWeaver Identity Management can help your organization grant and manage user access to heterogeneous applications securely and efficiently.

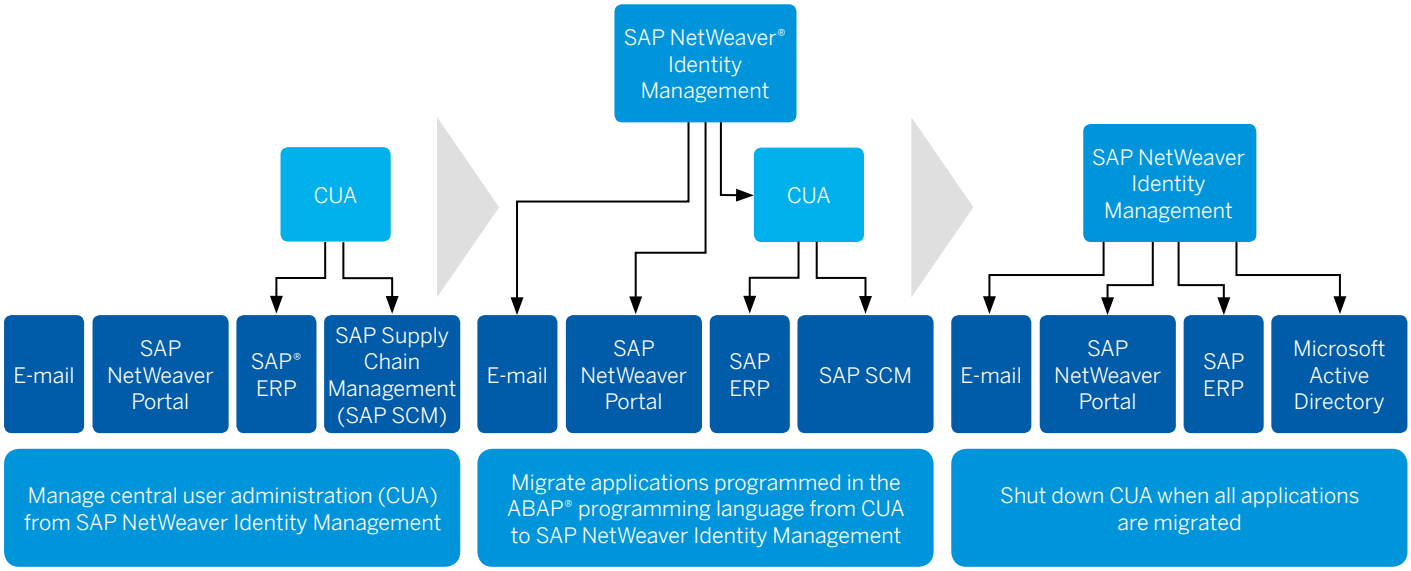
MIGRATING FROM CUA TO SAP NetWeaver® IDENTITY MANAGEMENT

Do you use the central user administration (CUA) tool to manage users across multiple SAP® software systems that are based on the ABAP® programming language? Moving to the SAP NetWeaver® Identity Management component from CUA provides the following advantages:

- Supports all relevant systems, including SAP and third-party software
- Supports sophisticated business-roles definition and management
- Provides self-service password resets, removing the biggest headache for help desk staff
- Enables workflow-based requests for approvals, automating user provisioning in multiple back-end systems
- Supports standards such as Lightweight Directory Access Protocol (LDAP), Service Provisioning Markup Language (SPML), and Directory Service Markup Language (DSML)

Furthermore, migration from CUA is intuitive. As shown in Figure 6, you install SAP NetWeaver Identity Management on top of CUA. Start connecting applications programmed in ABAP to SAP NetWeaver Identity Management and disconnecting them from CUA. After you disconnect the last application from CUA, the migration is complete.

Figure 6: Migration from CUA to SAP NetWeaver Identity Management



The Benefits

Taking Identity Management to the Next Level

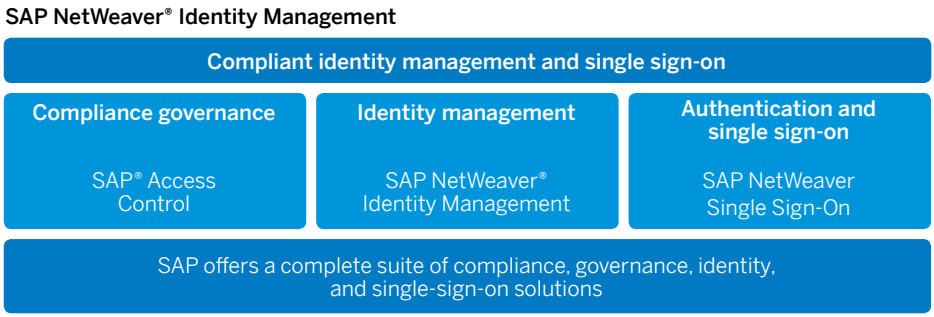
SAP NetWeaver Identity Management takes identity management from the technical level to the business level. This business-oriented solution lifts identity management by focusing on managing the lifecycle of employees, partners, and customers rather than on technical account management; it moves the management responsibility from IT administrators to business process owners.

With identity federation and single-sign-on functionality, SAP NetWeaver Identity Management helps you take identity management to the next level and secure on-demand and cloud applications. Tight integration with SAP NetWeaver Single Sign-On enables a smooth user experience, enhancing security across your system landscape.

As organizations continue to allow more and more employees, customers, and business partners access to information and processes across their system landscapes, the need for advanced and flexible single sign-on across the enterprise becomes increasingly important. Leading organizations are also seeking to standardize and centralize security management to improve the overall security of their applications and to decrease costs. These factors reveal the need for centralized authentication, authorization, auditing, and single-sign-on experience across all applications. SAP NetWeaver Single Sign-On provides support for many authentication systems including passwords, tokens, X.509 certificates, and smart cards. (See Figure 7.)

The new ID service allows for secure single sign-on in cloud environments. It covers the processes for managing identities and their lifecycles within the SAP cloud. Customers can set up one SAP identity per user and leverage single sign-on when browsing SAP Web sites, using on-demand software from SAP, or accessing third-party on-demand applications. This saves time and resources by enabling users to update their profiles only once and requiring just one password to log on to various on-demand solutions from SAP.

Figure 7: Support for Compliance, Identity Management, and Single Sign-On



By integrating SAP NetWeaver Identity Management with SAP solutions for governance, risk, and compliance, you can prevent segregation-of-duties violations and put in place mitigating controls.

SAP NetWeaver Identity Management also lets you emphasize compliance by providing full audit and reporting functionalities and integrating with SAP solutions for GRC in preventing segregation-of-duties violations. Most important, SAP NetWeaver Identity Management supports SAP software as well as the full heterogeneous landscape, including Lightweight Directory Access Protocol (LDAP) directories, third-party business applications, operating systems, e-mail systems, and databases. You can integrate SAP NetWeaver Identity Management across the entire system landscape and beyond, into the larger business network. By lowering total cost of ownership and increasing operational efficiency, SAP NetWeaver Identity Management helps meet your organization's objectives of lower cost, higher productivity, compliance, and auditability.

FOR MORE INFORMATION

For more information about how SAP NetWeaver Identity Management can help your organization, call your SAP representative today or visit us on the Web at www.sap.com/platform/netweaver/components/IDM/index.epx.

SAP NetWeaver Identity Management takes identity management from the technical level to the business level. It moves the management responsibility from IT administrators to business process owners.

www.sap.com/contactsap

CMP3796 (12/10) ©2012 SAP AG. 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™