Business-Driven, Compliant
Identity Management
By integrating SAP Identity Management with SAP solutions for governance, risk, and compliance, you can prevent SoD violations and put in place mitigating controls.
Quick Facts

Summary
Identity management is becoming a significant challenge for organizations today. You must ensure that your users have the right access to a multitude of applications in a timely manner, that the data is secure, and that access to corporate assets is compliant with corporate policies as well as legal regulations. The SAP® Identity Management component helps you align identity management with your organization’s key business processes.

Objectives
• Reduce operational costs in complex system landscapes
• Manage access to applications
• Comply with local and global regulations

Solution
• Business-driven, compliant identity management with business processes running in cloud and on-premise solutions from SAP
• User access rights assigned and maintained across multiple systems
• Password self-service functionality and synchronization
• Roles aligned with business processes rather than technical directory structures
• Reports based on current access and past events

Benefits
• Lower costs and increased productivity due to tight integration with your business processes
• One central location for identity data storage, eliminating redundancies
• Compliance with regulatory requirements, minimizing segregation-of-duties risks

Learn more
For more information, please visit http://scn.sap.com/community/idm.

SAP Identity Management can help your organization grant and manage user access to heterogeneous applications securely and efficiently.
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, enforce segregation-of-duties (SoD) policies, provide needed audit trails, and prevent unauthorized access.

With the SAP® Identity Management component, you can integrate identity management with the business processes within and beyond your enterprise. 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 FOR THE USER LIFECYCLE

A comprehensive identity management solution covers the entire lifecycle of a user, from the on-boarding 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 or her roles, create a new (fictitious) vendor, and issue an order. To minimize the risk that comes from such SoD 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 Identity Management helps you manage this process centrally, across SAP solutions as well as heterogeneous, non-SAP applications.

SAP Identity Management takes identity management from the technical level to the business level, moving management responsibility from IT administrators to business process owners.
How SAP Identity Management Can Help

SAP 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 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 SAP Lumira® software or the SAP 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
• Integration with the SAP 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
• Built-in connectivity with SuccessFactors® Employee Central, a user management component from SuccessFactors, an SAP company, for smooth compatibility and integration of on-premise and cloud identity management processes

Integration between SAP Identity Management and SAP Single Sign-On offers comprehensive single sign-on and encryption across organizational and technical boundaries.
SUPPORTING A HETEROGENEOUS IT LANDSCAPE

SAP Identity Management enables you to streamline provisioning of users into all applications – SAP and third party, cloud and on premise – as well as operating systems, file systems, and databases through 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 Lumira and SAP Business Warehouse allows for highly customized and differentiated state-of-the-art reporting.

Figure 1: Support for Heterogeneous Landscapes in SAP Identity Management
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 your organization achieves these efficiencies and realizes 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.

SAP 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.

Integrated connectivity with SuccessFactors Employee Central allows for an equally tight integration of user data coming into on-premise applications from the cloud, or vice versa (see Figure 2).

Figure 2: Integration of HR Processes with SAP Identity Management

Kim Perkins joins the company as a marketing specialist. From the first day with her new company, she is able to log on to all relevant systems, including access to employee self-services and the SAP® Customer Relationship Management (SAP CRM) application to track the marketing activities she is responsible for.

1. Prehire phase
   HR ensures that all necessary employee data for Kim is available, such as position and entry date.

2. HR operations
   Event-based extraction of personnel data

3. SAP ERP HCM
   SuccessFactors Employee Central

4. Kim’s manager approves the assignment.

5. First day at work
   Role and authorization information is provisioned to relevant target systems.

SAP Identity Management component

SAP ERP HCM = SAP ERP Human Capital Management

SAP ERP HCM
User created ("employee")

SAP ERP
Business partner created
User created ("marketing professional")

SAP CRM
User created
Access to employee self-services
Access to SAP CRM

SAP Enterprise Portal
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 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 Active Directory. By focusing on business processes and business roles, SAP 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 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 audit-able. SAP Identity Management offers compliant user provisioning and full reporting and audit functionalities. By integrating SAP Identity Management with the SAP Access Control application, for governance, risk, and compliance (GRC) management, you can prevent SoD 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.

**SINGLE SIGN-ON FOR ON-PREMISE AND CLOUD APPLICATIONS**

Integration with SAP Single Sign-On offers comprehensive single sign-on and encryption across organizational and technical boundaries. SAP 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.

Integration of SAP Identity Management with the SAP Cloud Identity offering helps you provide cloud-based business users with simple, secure access to your SAP and third-party applications in the cloud that support critical processes such as human resource management, finance, and procurement. This comprehensive cloud service for identity lifecycle management provides state-of-the-art authentication mechanisms, secure single sign-on functionality, and on-premise integration.

---

**Figure 4: How Business-Driven Compliant Identity Management Works**

- **SAP® Identity Management**
  - Provides reduced total cost of ownership and increased security

- **SAP Access Control**
  - Helps ensure that IT business application controls are compliant

**Compliant identity management**
- Provides compliant identity management across SAP software and heterogeneous landscapes in one integrated solution
- Provides standards-based integration to create a tightly aligned, loosely coupled solution from complementary components
- Gives a consistent view of current and historic access rights, approvals, and policy violations
Features and Functions: What You Can Do with SAP Identity Management

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

The main functions of SAP Identity Management are included in the following text.

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

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 SAP Access Control allows for the effective mitigation of SoD 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 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.

Single sign-on – Integration with SAP Single Sign-On and SAP Cloud Identity enable comprehensive, standards-based single sign-on and encryption of communication channels across and beyond the enterprise.
The Benefits: Taking Identity Management to the Next Level

SAP 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. Tight integration with SAP Single Sign-On and SAP Cloud Identity software enable a smooth user experience, enhancing security across your on-premise and cloud 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 Single Sign-On provides support for many authentication systems including passwords, tokens, X.509 certificates, and smart cards (see Figure 6). SAP Cloud Identity allows for secure single sign-on in cloud environments. It covers the processes for managing identities and their lifecycles within the SAP Cloud portfolio. 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.

SAP Identity Management also lets you emphasize compliance by providing full audit and reporting functionalities and integrating with SAP solutions for GRC in preventing SoD violations.

Figure 6: Support for Compliance, Identity Management, and Single Sign-On

<table>
<thead>
<tr>
<th>Identity and access management</th>
<th>Authentication and single sign-on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity, governance, and administration</td>
<td>• Single sign-on</td>
</tr>
<tr>
<td>• Managing identity lifecycle</td>
<td>• Secure network communication</td>
</tr>
<tr>
<td>• Segregation of duties</td>
<td>• Central access policies</td>
</tr>
<tr>
<td>• Emergency access</td>
<td>• Two-factor authentication</td>
</tr>
<tr>
<td>• Role management</td>
<td></td>
</tr>
<tr>
<td>• Reporting</td>
<td></td>
</tr>
</tbody>
</table>
Most important, SAP 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 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 Identity Management helps meet your organization’s objectives of lower cost, higher productivity, compliance, and auditability.

FIND OUT MORE
For more information about how SAP Identity Management can help your organization, call your SAP representative today or visit us on the Web at [http://scn.sap.com/community/idm](http://scn.sap.com/community/idm).