Compliant Provisioning
SAP GRC Goes Identity Management
Disclaimer

This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.
Identity and Access Management Imperative

<table>
<thead>
<tr>
<th>Compliance with IAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP NetWeaver Identity Management</td>
</tr>
<tr>
<td>SAP GRC Access Control</td>
</tr>
<tr>
<td>SAP IAM Proposition</td>
</tr>
<tr>
<td>IAM Scenarios and Qualification</td>
</tr>
<tr>
<td>IdM &amp; GRC Technical Integration</td>
</tr>
</tbody>
</table>
The IAM Imperative

Identities are at the core of every business, affecting how organizations securely interact and build trusted relationships with customers, partners, and employees.

Effective management of users’ identities, credentials and access rights is no longer considered a differentiator – it’s a business imperative.
What Is Identity Management?

- Integrated system of business processes, policies and technologies
- Enables organizations to facilitate and control their users’ access to critical online applications and resources
- Protects confidential personal and business information from unauthorized users
[Burton Group] positions the acquisition as a battle between SAP and Oracle to push their respective application platforms.

[Other blogs] believe that SAP is making this move to become an organization’s de facto infrastructure by way of controlling the organizations IdM.

In March, 2007 Oracle announced its GRC Suite which includes technologies acquired from Stellent, Inc. The rivalry between these vendors has begun to resemble a game of Battleship. SAP’s acquisition of MaXware representing a return fire on Oracle’s various IdM acquisitions.

...SAP’s entrance to the identity management market does however change the dynamic beyond the existing rivalry with Oracle. The acquisition will have a direct impact on the identity management market.

By acquiring MaXware, SAP seeks to improve its identity and access management capabilities, rather than to compete against established IAM suite vendors. This move underscores a new approach to a maturing IAM market.

...MaXware will provide the company with many (though not all) of the component technologies expected of an identity management suite provider.
IAM Business Drivers

### Regulatory Compliance
- Sarbanes-Oxley
- SEC
- GAAP (third-party audit)

### Business Need
- External users’ access
- Employee personalization
- Outsourcing

### Risk Management
- Reporting
- Terminations
- Policy-based compliance
- Audit management

### Cost Containment
- Cost reduction/avoidance
- Common architecture
- Productivity savings

### Operational Efficiency
- Improved SLAs
- Employee personalization
- Enhanced user experience

Source: Burton Group
Identity Crisis
Today's environment is complex and disorganized

- Many systems and instances
- Each user has many identities
- Identities and access permissions change
- Difficult to manage, expensive to maintain
- Poor access and productivity
- Limited process integration
- Security and compliance issues
Trends

By 2008, investments in identity management solutions will increase 60% to address regulatory requirements (0.8 probability) (Gartner 4/06)

By 2008, investments in user-provisioning (UP) solutions will increase 60% to address regulatory compliance (0.8 probability) (Gartner 4/06) Regulatory Compliance was the No 1 driver for UP implementations in the past 18 months (as of 4/2006)

User Provisioning products will continue to be used to manage and report on internal user access through 2010 (0.8 probability)

Currently, ~ 1,200 UP implementations worldwide, the majority of which in large enterprises (HC>5000) (Gartner estimate)

Enterprise Role Management is considered the future of compliant user provisioning (i.e. address the problem at the root).

IdM is ERP for Security Administration
Current Approach - The Cost of the Status Quo

Risk of Non-Compliance

- with key regulations around the world

Cost of Compliance

- Time, labor and cost required to produce reports required for regulatory compliance

Cost of a manual user provisioning process ("Just call IT") incl. cost of manual and error-prone approval and provisioning process

Insufficient protection of sensitive information

- Accidental and deliberate errors can cost up 5% of annual revenue!

Productivity losses

- Effectiveness and efficiency in on-boarding new employees

Source: 1 Association of Certified Fraud Examiners, 2006 Report to the Nation on Occupational Fraud and Abuse
Identity and Access Management Imperative

Compliance with IAM

SAP NetWeaver Identity Management

SAP GRC Access Control

SAP IAM Proposition

IAM Scenarios and Qualification

IdM & GRC Technical Integration
IAM Audit and Compliance Problem

Challenges:
- Prove, enforce, monitor
- Who accessed what?
- Comply with regulations

Costly to:
- Report & maintain secure access control infrastructure
- Audit manually
- Fail

Other problems:
- Incomplete and distributed I&A data
- NOT a one-time shot
- Little automation
- Immature IT tools

Strategic Planning Assumption: By 2008, investments in identity management solutions will increase 60% to address regulatory compliance requirements (0.8 probability).
Key Pain Points

- How do you ensure that your ERP and financial systems stay clean of segregation-of-duties violations?

- How do you analyze new user requests and role changes to ensure that they are not creating new SoD violations?

- How do you automate the provisioning process?

- What is the role of your IT security teams and business process owners in the provisioning process?

- Optional: How easily can your compliance applications integrate with your identity management and provisioning systems?
Identity and Access Management Imperative

Compliance with IAM

SAP NetWeaver Identity Management

SAP GRC Access Control

SAP IAM Proposition

IAM Scenarios and Qualification

IdM & GRC Technical Integration
Identity Management “Big Picture”

- Users
- Administrators
- Operations
- Auditors

Workflow
- Role Management
- Segregation of Duty
- Approval

Policy
- Monitoring
- Risks/Controls/Remediation
- Attribute Management

Audit & Reporting

Connectivity

Enterprise Applications

IT Infrastructure

SAP
PeopleSoft
Oracle
AD
Exchange
Notes
The SAP Advantage
An integrated solution for business and IT

- Integrated approach supports a comprehensive enterprise SOA strategy built on SAP’s open platform
- Seamlessly links IDs with business roles, for smoother process integration
- Powerful synchronization and virtualization, plus integration with core processes and information in HR system
- The only tightly integrated GRC and IdM offering in the market today
SAP Introduces Business-Driven Identity Management

Provisioning, synchronization and process integration

- Provision access by role
- Open integration
- Synchronization
- Reporting and audit
- Easy administration
- Self-service for users
- SOA
Identity and Access Management Imperative

Compliance with IAM

SAP NetWeaver Identity Management

**SAP GRC Access Control**

SAP IAM Proposition

IAM Scenarios and Qualification

IdM & GRC Technical Integration
SAP GRC Access Control
Sustainable prevention of segregation of duties violations

**Minimal Time to Compliance**
(Get Clean)

- Risk Analysis and Remediation
  Rapid, cost-effective and comprehensive initial clean-up

- Enterprise Role Management
  Enforce SoD compliance at design time

- Compliant User Provisioning
  Prevent SoD violations at run time

- Superuser Privilege Management
  Close #1 audit issue with temporary emergency access

**Continuous Access Management**
(Stay Clean)

**Effective Management Oversight and Audit**
(Stay in Control)

- Periodic Access Review and Audit
  Focus on remaining challenges during recurring audits

Risk analysis, remediation and prevention services

Cross-enterprise library of best practice segregation of duties rules
Real-time compliance stops security and controls violations before they occur

- **Significantly reduce the cost of compliance**
- **Reduce risk** with preventive cross-enterprise controls
- **Reduce time to compliance** through automation
- **Ready-to-run** with most comprehensive rules set

36% reduction of costs managing authorization risk
- Customer survey, 5/2005
Compliant User Provisioning
Problem: Inefficient and un-auditable user provisioning

Current approach

Access request → e-mail
Manager approval
Role owner
Manager approval
spreadsheets, paper forms
IT security
Manual provisioning

Compliant provisioning

HR event → Request generated
100% automated

Employee hired/retired → Risk analysis
Path workflow—based on request type and user attributes
Segregation of Duties Analysis
Workflow
Remediation Mitigation Approval
Workflow
Automated provisioning
100% automated

SAP, Oracle, PeopleSoft
SAP GRC Enterprise Role Management
SAP Solutions for GRC: Access Control

Enables Enterprise Role Definition and Maintenance in a Single Location

- Reduce cost of role maintenance
- Smooth compliance and avoid authorization risk
- Eliminate errors and enforce best practices
- Audit ready traceability and security checks

Centralized Role Management

Enterprise Rules → Enterprise Role Mgmt → Audit Log

Across Applications

SAP → ORACLE → PeopleSoft → ...

Compliant Enterprise Roles

Role → Role → Role → Role → Role → Role

28% time savings in role management
SAP GRC SuperUser Privilege Management
SAP Solutions for GRC: Access Control

Enables Compliance-focused Emergency Access for SAP

- Close #1 open audit issue
- Avoid business obstructions with faster emergency response
- Reduce audit time
- Reduce time to perform critical tasks

“Superusers and auditors love it”

- Pre-assigned firefight IDs
- Access restrictions
- Validity dates
- Field-level changes tracked in audit log
Identity and Access Management Imperative

Compliance with IAM

SAP NetWeaver Identity Management

SAP GRC Access Control

SAP IAM Proposition

IAM Scenarios and Qualification

IdM & GRC Technical Integration
Business-Driven Identity Management

SAP addresses compliance issues across the organization

Operations

- Business Controls
- SAP GRC Access Control
  - Risk analysis
  - Audit and compliance
  - Privilege management for business transactions

Development

- Systems Access
- SAP NetWeaver Identity Management
  - User provisioning
  - Identity synchronization and virtualization
  - Privilege management for applications and resources

SAP will offer an integrated solution
IdM adds value to GRC in a joint solution by extending its reach outside of business applications and directory servers and into a broader heterogeneous environment.

IdM provides additional functionality, centered on aspects of the Identity lifecycle, e.g. self-service password reset and de-provisioning.

<table>
<thead>
<tr>
<th>IdM Qualification</th>
<th>GRC Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key driver to reduce the burdens associated with user accounts and privileges across multiple target resources.</td>
<td>Key driver being to implement automated Segregation of Duty controls on business application privileges for compliance.</td>
</tr>
<tr>
<td>Improves the quality of service for users through measures such as self-service password reset.</td>
<td>Requirement for fine-grained authorization specifically within business applications.</td>
</tr>
<tr>
<td>Real-time detection of changes on target resources and synchronization of identity data across multiple target resources.</td>
<td>Requirement for in-depth, automated analysis of the risks presented by changes to a user’s ERP privileges before they are committed.</td>
</tr>
</tbody>
</table>

The combination of SAP GRC and Identity Management provides a solution that satisfies the requirements of the CFO to ensure that IT business application controls are compliant, while providing the economies required by the CIO.
<table>
<thead>
<tr>
<th>Identity and Access Management Imperative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance with IAM</td>
</tr>
<tr>
<td>SAP NetWeaver Identity Management</td>
</tr>
<tr>
<td>SAP GRC Access Control</td>
</tr>
<tr>
<td>SAP IAM Proposition</td>
</tr>
<tr>
<td>IAM Scenarios and Qualification</td>
</tr>
<tr>
<td>IdM &amp; GRC Technical Integration</td>
</tr>
</tbody>
</table>
Stand-Alone
Customer Motivation: Segregation of Duties and/or SAP Focus

SAP GRC Access Control

Oversight
- Management
- Audit

Risk Analysis
- Risk Analysis and Remediation

User Provisioning
- Add/Modify User Role & Permissions

Compliant User Provisioning

End-user requesting access

Inform end-user

Risk Analysis Request → Mitigation Workflow → Provision into Application
Stand-Alone
Customer Motivation: Segregation of Duties and/or SAP Focus

- Customer focus on compliance and SoD
- Provisioning into ERP systems or manual
- Optimized for SAP environments
- No integration work (IdM <-> AC) necessary
- Rapid deployment
- Limited provisioning resources (AD, DB, flat file)
Integrated with a 3rd Party IDM Solution

Customer Motivation: IT - Identity and Access Driven

Oversight

Management
Audit

Risk Analysis

User Provisioning

Risk Analysis and Remediation
Add/Modify User Role & Permissions

Compliant User Provisioning

Risk Analysis Request
Mitigation Workflow
Provision into Application

SAP GRC Access Control

Identity Management Software

Request for ERP Access/Role
Status Update

End-user requesting access

Inform end-user

Key
- Identity Management Software
- SAP GRC Access Control

© SAP AG 2007, SAP TechEd '07 / SIM202 / 30
Integrated with a 3rd Party IDM Solution
Customer Motivation: IT - Identity and Access Driven

- Large IdM install base (more than 5000 successful projects)
- IdM vendor’s compliance solution is weak
  - No rule set out of the box
  - Customize IdM products to become compliant
  - No granular security
- Integration experience (adapters, agents)
  - Joint development effort
  - Experience in integration
- SAP integration certification to provide all web service functionality, including bi-directional capabilities
- Customer home-grown application integration
Access control to provide web services to connect IdM and GRC
Access control to exchange data and information and to enable compliant user provisioning
- IdM limited account or role control and lack of SoD knowledge
- IdM systems were designed to gather and aggregate data from disparate sources. When organizations build too much intelligence into the IdM policy engine, that engine becomes impossible to maintain

Customer choice – Depending on the project/customer driver (IT or Business) can both applications provide certain capabilities

Unified user authentication/authorization for SAP systems

Full support for compliant user provisioning in heterogeneous landscape
Identity and Access Management Imperative

Compliance with IAM

SAP NetWeaver Identity Management

SAP GRC Access Control

SAP IAM Proposition

IAM Scenarios and Qualification

IdM & GRC Technical Integration
SAP GRC Access Control Web Services – Scenario 1

1. Requestor Login
2. Request Access to Enterprise System
3. Provisioning Workflow
4. SAP?
5. Perform Risk Analysis
6. Provision SAP

1. Select Application
2. Select Roles

Yes
No

Provision Non-SAP System

IDM
GRC Web service
SAP GRC Access Control Web Services – Scenario 2

1. Requestor Login
2. Request Access to Enterprise System
3. Provisioning Workflow
4. ERP?
5. Provision Non-ERP System
6. Request Status
7. Audit Trail
8. Exit Service

GRC
IDM
GRC Web service
IDM Web Service

© SAP AG 2007, SAP TechEd '07 / SIM202 / 35
SAP GRC Access Control Web Services

1. Select Applications

This is a bi-directional web service. When the service is called by IDM, it returns a list of application resources configured within GRC to IDM. Whereas, when GRC calls this service, it returns a list of applications configured within IDM to GRC.

2. Search Roles

This service enables the user to search for roles before submitting a request to GRC. Additional filtration capabilities are also provided to narrow down the search as a part of this web service.

– Role Details - Detail information of the selected role can be obtained by calling this service.

3a. Request Submission to GRC

The requestor can submit a request to GRC using this service, for compliant provisioning.

– Search Master Data - This service provides the user the ability to lookup for master data required to submit the request. (Example: Functional Area, Priority, Custom Fields, and Request Types etc.)

3b. Request Submission to IDM

This web service is called by GRC to submit a request to IDM.

Following are two scenarios when the service will be called.

– When a user is created or changed in an SAP HR system, a new request will be submitted to IDM to create or remove users and their privileges.

Example: An event occurs in SAP HR, such as the hiring of a new employee.

This event will initiate a request to enable the user to have some basic privileges to perform the job function for which he/she is hired for.

The request might consist of both ERP and Non-ERP applications. This will trigger a request being submitted to the IDM system for non-ERP system, while GRC processes the request for the ERP systems in the request.

The audit logs, and request status can be consolidated into one by calling the ‘Audit Logs’ and ‘Request Status’ web service.

– When a user requests non-ERP system from the GRC end user form, GRC calls this service to submit a request to IDM.

4. Risk Analysis

The service enables the user to perform Segregation of Duty (SoD) analysis, and returns the possible violations.
5. **Provisioning**

The provisioning service is called to provision users and roles into various ERP applications.

6. **Audit Logs (including provisioning logs)**

This is a *bi-directional* web service. The Audit log web service will return a comprehensive detail list of audit history. It enables GRC to retrieve the audit Logs from IDM (for non-ERP provisioning), as well as provide the audit history of user provisioning to IDM.

7. **Request Status**

This is a *bi-directional* service.
This service returns the status, and detail request information for the selected request.

8. **Exit Web service**

This service is called once the request is processed completely within GRC. It notifies IDM about the closing of a request.
Further Information

SAP Public Web:
- SAP Developer Network (SDN): [www.sdn.sap.com](http://www.sdn.sap.com)
- SAP GRC: [www.sap.com/grc](http://www.sap.com/grc)

Related SAP Education and Certification Opportunities

Related Workshops/Lectures at SAP TechEd 2007
- Session ID: **SIM206** SAP NetWeaver Identity Management in Action
- Session ID: **SIM150** Manage and Prevent User-Access and Authorization Risk Across the Enterprise with SAP GRC
- Session ID: **SIM203** Implementing SAP GRC Access Control Globally and Take Identity Management to the Next Level
- Session ID: **SIM212** ASUG Influence Update: Security and Identity Management Roadmap Session
The SAP NetWeaver, Development Subscription offers a cost effective total solution for developers to build applications for the SAP NetWeaver platform.

Subscription gives you one year access to ...

- SAP NetWeaver platform software, patches, and updates
- Development license for SAP NetWeaver to evaluate, develop and test
- Standard software maintenance
- Online sessions from SAP TechEd
- Access to SAP Enterprise Services Workplace for testing
- Premium presence in forums

Purchase the SAP NetWeaver, Development Subscription today at the TechEd Community Clubhouse, or online at https://www.sdn.sap.com/irj/sdn/subscriptions

Show us you are a subscriber and get a reward!