



Compliant user provisioning: an alternative approach

By Phil Shipley

Many companies are facing the ever-increasing burden of negative audit findings with respect to SAP systems and access provisioning processes. For these companies, SAP GRC Access Control is often the first option that comes to mind when looking for a solution to these problems. This, however, is only part of the solution.

SAP customers who run SAP HR and an Enterprise Portal have the option of upgrading to ERP 6.0 Enhancement Pack 4 for HR and activating the add-on packages for HR Administrative Services and HCM Processes and Forms.

These two packages, when combined with the complementary business packages of Manager Self Service and HR Administrative Services on the Enterprise Portal, can offer the customer an opportunity to build a completely bespoke access provisioning solution. This solution is based upon standard and SAP-supported ABAP and Java Webdynpro technologies.

This combination of SAP products will still provide similar compliance assurances as GRC, but with greater flexibility with respect to the following:

- modelling customer-specific business processes;
- providing comprehensive approval and audit trails; and
- seamlessly integrating into a position-based security model.

One benefit of taking this approach is that the resulting tool set is not limited to only user access

provisioning requests. Only a minimal number of processes need to be built in order to go live with this concept. The processes covered by the solution can then be extended to cover a broad range of manager-initiated HR-related requests, creating much greater value for the users from the implementation.

User access provisioning is the process or mechanism for giving a user access to use a business's SAP applications. It encompasses providing a user's access to perform their job, applying changes when the user changes jobs, ensuring that the user only ever has enough access to fulfil their existing role and de-provisioning the access upon termination of employment.

To be able to call this process compliant, it must be demonstrated that the users do not have authorisation to perform fraudulent activities in the SAP environment, including activities and processes that may go across separate SAP systems such as ERP, CRM and SRM. Compliance also by definition infers the ability to monitor, control and report that compliance is being enforced. Compliance does not only mean acting in accordance with regulation such as the *Sarbanes Oxley Act* and ensuring risks are controlled or removed, but also conforming with your organisation's specific application security design, policy and standards and ensuring there has been no deviation from this.

When auditors perform tests on a SAP system, they are often looking

for gaps in the provisioning process. This includes looking at what access users have, whether it contains any risks, how the access was approved, how this access was provisioned to the user and whether it still aligns with the documented design. Customers therefore need to be able to provide evidence that:

- SAP application access allocated to users is risk-free or mitigating controls are in place;
- The access design is documented and has only changed with approval;
- The access allocated to users is aligned with the intended design, that is, users do not have roles beyond what the job requires;
- Processes are in place to ensure compliance, that is, can they identify and remediate compliance issues?

This solution is capable of meeting audit needs and solving the many challenges involved in building a compliant user provisioning process. To do this, the solution includes the following:

- Position Based Security (PBS) with Central User Administration (CUA);
- HR Org Management (HR-OM) and if required, HR ALE Distribution with CRM /SRM BP Integration;
- Manager Self Service (MSS) utilising HCM Processes and Forms (Adobe);
- HR Administrative Services;
- Governance, Risk and Compliance (GRC)
 - o Super User Privilege Management (SPM)

o Risk Analysis and Remediation (RAR).

In the above diagram (roll over button), a high-level map of the solution components is shown:

1. The main interface is the Enterprise Portal. Managers and administrators can perform all provisioning related processes from here. Adobe Forms provide request and approval audit trails of all provisioning activity.


2. The source HR chart is established in ERP. This is where the CUA must reside in order to read the role and system assignments off the HR chart via distributed composite roles and position-based security.

3. The org chart, users and roles are distributed via HR ALE and the CUA to any other SAP application. Business Partner Integration can also be included.

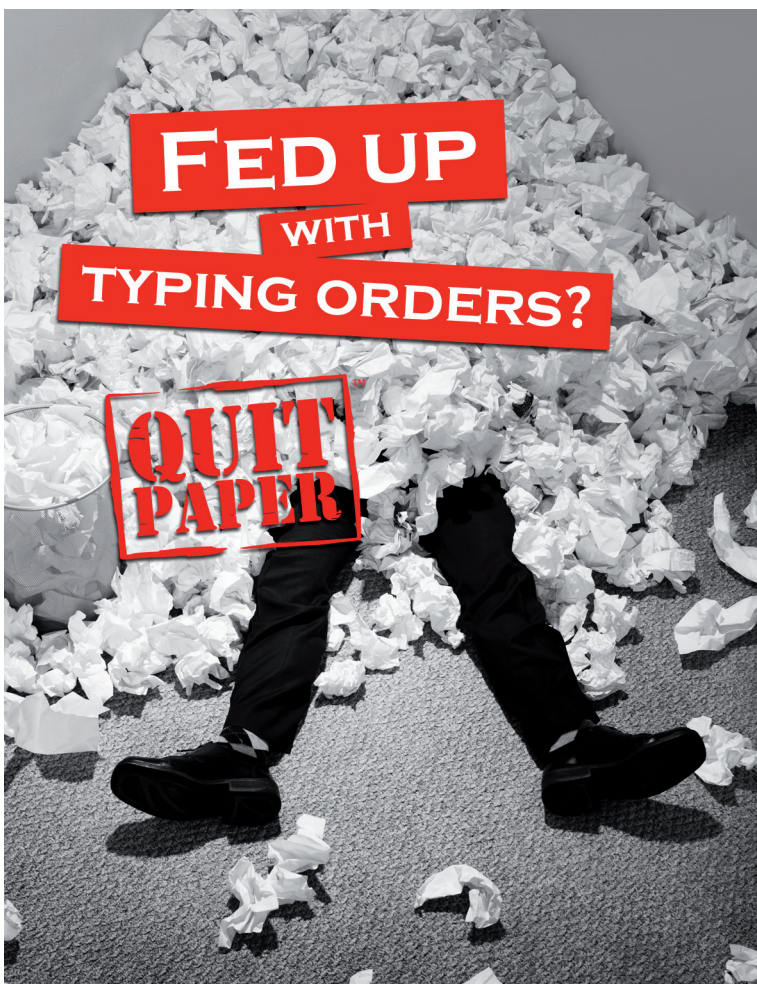
4. GRC RAR runs over the top of this process, providing monitoring and control over SoD risks within and across SAP backend systems.

5. GRC SPM is optional, but easily implemented. It is used by support users to support production clients as a way of granting super user access in a controlled and auditable manner.

A key point to make about position-based security is that once the set of roles per position is deemed compliant, any holder of the position will also be compliant. By not allowing changes to the role assignments without an approved

change in the design, you will ensure your end-users are always compliant. This is where this concept truly becomes effective. Managers are empowered to move their own people and affect their access rights, but regardless of where they are moved, they are not creating risks because all positions are already compliant. 

Phil Shipley is a senior consultant with Zer01 Group. With over 10 years SAP experience, Phil is a highly respected SAP security professional. Zer01 is an SAP specialist consultancy focused on providing integrated SAP solutions for Governance, Risk and Compliance (GRC) for customers across all industries. For more information on Zer01 or this article, please consult www.zer01group.com or Robert Pedler, CEO, at [Robert.pedler@zer01group.com](mailto:pedler@zer01group.com).



Fax to Order: Are you still typing your sales orders into SAP?

Download this **White Paper** and find out how to improve your fax to order process:

- **Boost productivity** to process more orders with fewer resources
- Cut order processing costs **by up to 70%**
- Speeding order fulfilment and virtually **eliminating errors**
- **Monitoring and prioritising** sales order processing
- Making orders readily **accessible in the SAP application** (no more paper archiving!)



Click here and get
the White Paper now >