SAP Security and the **Provisioning of SAP Access**

soterion

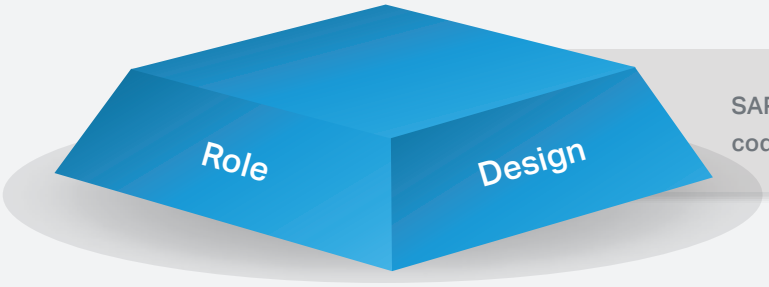
To determine the best SAP access provisioning option for your organisation, it's necessary to examine the evolution of SAP security, access control and identity access management (IAM).

The evolution of SAP security, access control (GRC) and IAM

SAP Role Design

In the early days of SAP (R2), users were assigned SAP access through SAP profiles. This evolved into SAP roles via the Profile Generator (PFCG). To improve the provisioning process and combat SAP authorisation creep, where users inherit inappropriate access over time, SAP introduced the option to assign SAP roles to the HR Organisation Structure. When a user was moved into an HR position in SAP, they automatically inherited the SAP roles linked to the HR position.

SAP Composite Roles were introduced that also enhanced provisioning efficiency. An SAP Composite Role is a data container for a group of single roles. When an SAP user is assigned an SAP Composite Role, they inherit all the single roles contained in the Composite Role.



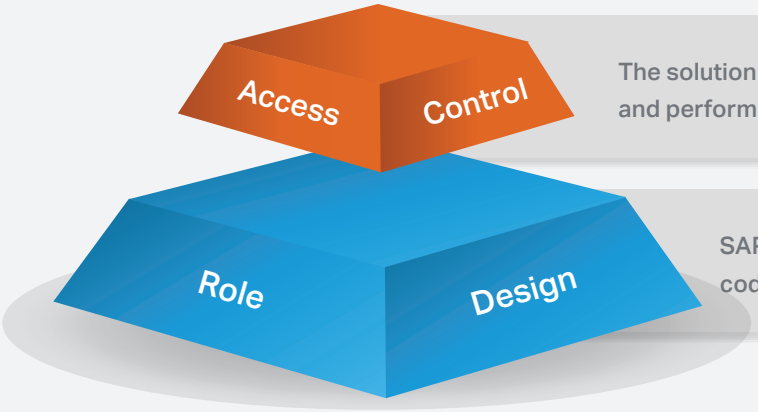
SAP users gain access to SAP functionality (via transaction codes, org levels etc).

However, assigning SAP roles to users without understanding their risk impact led to the birth of access control (GRC) solutions.

Access control solutions

Initially, access control solutions primarily analysed SAP systems for access risk violations and performed access risk 'what-if' simulations on proposed role allocations. As access control solutions evolved, additional functionality was added to perform User Access Reviews and role provisioning. For role provisioning, the concept of a Business Role was introduced. A Business Role is similar to an SAP Composite Role in that it is a data container for a group of roles. When a user is assigned a Business Role, they inherit all the roles associated with that Business Role.

In most access control solutions, a Business Role is more flexible than an SAP Composite Role, enabling partial assignment in many cases. For instance, if an accounts payable clerk only requires 80% of the functionality contained in the ACCOUNTS_PAYABLE_-CLERK Business Role, it can be partially assigned. An SAP Composite Role is less flexible, as once it's assigned, all associated single roles are available to the user. This can make risk remediation (role clean-up) difficult, as the activities of a group of users must be considered. When removing an SAP single role from a Composite Role, all users assigned to the Composite Role will be impacted.

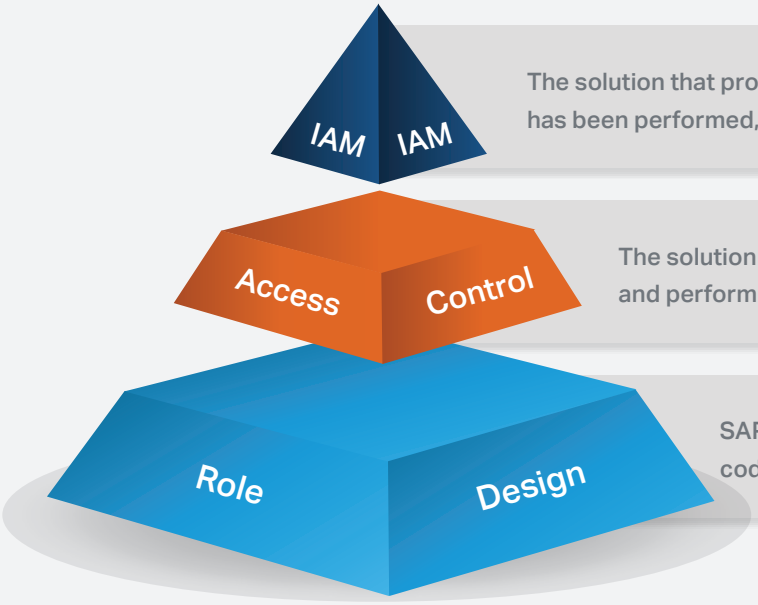


The solution that analyses the role design for access risk violations and perform what-if simulations on proposed role assignments.

SAP users gain access to SAP functionality (via transaction codes, org levels etc).

IAM solutions

IAM solutions were introduced to manage an identity across the IT landscape and facilitate the Joiner-Mover-Leaver process. As IAM solutions could provision access to multiple systems and solutions, many believed this would address all previous provisioning challenges and make onboarding and user provisioning significantly more efficient. IAM solutions also have a Business Role concept, which is more powerful than the access control solution Business Roles. Access control solution Business Roles are limited to roles from the SAP systems, while IAM solution Business Roles cater to roles from multiple systems (SAP and non-SAP).



The solution that provisions all the SAP access after the relevant risk analysis has been performed, reviewed and approved.

The solution that analyses the role design for access risk violations and perform 'what-if' simulations on proposed role assignments.

SAP users gain access to SAP functionality (via transaction codes, org levels etc).

Utopia? Not quite

Seamless integration between access control solutions and IAM solutions has proven challenging in reality, preventing organisations from benefiting from any symbiotic relationship between risk management and provisioning. As a result, organisations are required to choose which of these solutions will perform any of the overlapping tasks or functions.

Below is a list of some of the overlapping functions that can be performed in both the access control and IAM solution:

Overlapping Functionality	Access Control / GRC	Identity Access Management
Business Role concept	**Pros:** Powerful access risk reporting at the business role level. Usage information ensures more effective risk remediation i.e. more appropiate business role **Cons:** Limited to SAP systems	**Pros:** Provision SAP and non-SAP access, resulting in greater provisioning efficiencies. **Cons:** Less powerful access risk reporting at the business role level. Limited usage information makes risk remediation a challenge with buiness roles providing in-appropiate access to the users
Access Risk Analysis	**Pros:** Detailed access risk capabilities at SAP authorisation object / field level **Cons:** Limited to SAP systems	**Pros:** Cross-system access risk capability **Cons:** Risk analysis at the SAP role level is not sufficient for the SAP market
'What-If' Simulations	**Pros:** 'What-If' simulations for SAP systems performed at detailed level and results presented with risk and usage information resulting in more informed decision making by reviewers **Cons:** Limited to SAP systems	**Pros:** Simulations can be performed across non-SAP systems **Cons:** Risk analysis (simulations) not perfomed at the detailed (auth object field) level required for effective control in SAP
Workflow approvals and Role Provisioning	**Pros:** Can cater for complex workflow requirements as standard functionality Cons: Limited to SAP systems	**Pros:** Provisioning to SAP and non-SAP systems **Cons:** Limited out-the-box workflow capabilities and / or require a lot of effort to configure
User Access Reviews	**Pros:** Reviews presented with risk and usage information resulting in more informed decision making by reviewers **Cons:** Limited to SAP systems	**Pros:** User Access reviews are wider than just the SAP systems **Cons:** Limited risk and usage information relating to SAP systems

Choosing the right solution for each function is crucial to achieving an organisation's desired business objectives. Each solution has its own set of advantages and disadvantages, depending on factors such as the business objectives, the type of systems and applications, and the number of solutions in scope.

For organisations with a large SAP footprint, managing access risk is important, and balancing provisioning efficiencies with effective access control is essential. If an IAM solution is chosen to perform overlapping activities, the desired level of access risk management may not be achieved. For these organisations, using the access control solution for provisioning SAP access may achieve the desired result.

If an organisation has a small SAP footprint and does not require detailed SAP access risk analysis, an IAM solution may suffice.

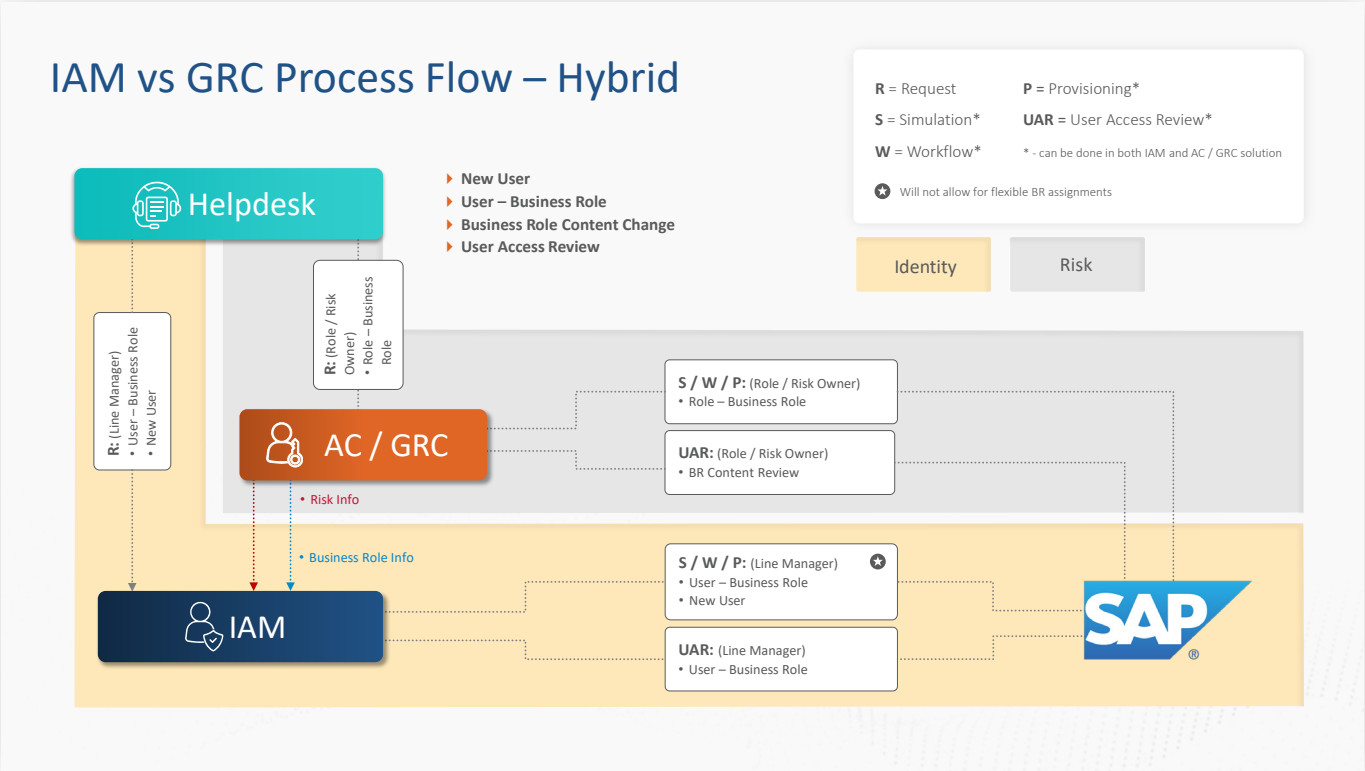
The choice of solution depends on the organisation's needs.

Is a hybrid model the way to go?

To balance provisioning efficiencies with effective access risk management, a hybrid model can be considered.

For those organisations who have a large SAP footprint and / or place a lot of importance on effective access risk management, an access control solution can be used for all overlapping activities for the SAP systems, while an IAM solution can be used for all non-SAP systems.

Another option is to use the access control solution for the design of the Business Roles and then replicate them in the IAM solution for provisioning. By defining Business Roles in the access control solution, historical usage data and access risk information can be used to create appropriate Business Roles for the group of users assigned.



While a hybrid model has its downsides, such as requiring certain business users to perform their activities in two different systems, it can enable the organisation to address its requirements for effective SAP access risk management while improving the efficiencies of SAP user provisioning to an acceptable level.

Conclusion

All approaches have their pros and cons, and there is no one-size-fits-all solution. When making a decision, it's crucial to consider your organisation's needs, business objectives, SAP footprint, and risk management priorities.

To make the best decision, it's important for the SAP security and cyber teams to work together, discussing and debating each use case to select the optimal solution for the organisation.

A hybrid model may be the lesser of all evils and provide the best balance between provisioning efficiencies and effective access risk management.