Deloitte.

Role Management

Enable your application security and reach the next maturity level

Nowadays more and more transactions are performed electronically. The related risks grow as these transactions become increasingly interesting for different individuals. Such a paperless world and the interconnectedness of the business processes present unique and substantial security challenges, but also opportunities.

Appropriate business process controls and thus effective Role Management and Access Controls should be designed and implemented in a way to safeguard the basic information security principles which are best summarized by the CIA triad: confidentiality, integrity and availability.

Typical issues encountered in the Role Management are:

- Roles contain Segregation of Duties (SoD) conflicts and give too broad access resulting in a single actor performing key business process control activities
- Complex roles make the SoD remediation difficult & costly
- The authorization concept is not transparent and therefore not understandable for business people
- Too much effort is spent to user & authorization maintenance
- Ineffective control of the user access management process
- Unstructured role change management process

Giving you the solution

A well-designed and a transparent authorization concept is a definitive method to mitigate the emerging business risks. A role structure in line with business processes & organization will generate ownership of the business stakeholders over the access to process activities & data across business applications – limiting risks of intentional fraud or unintentional error across the organization. Flexible & dedicated roles facilitate the maintenance of the role concept, maintaining ease of use and security compliancy.

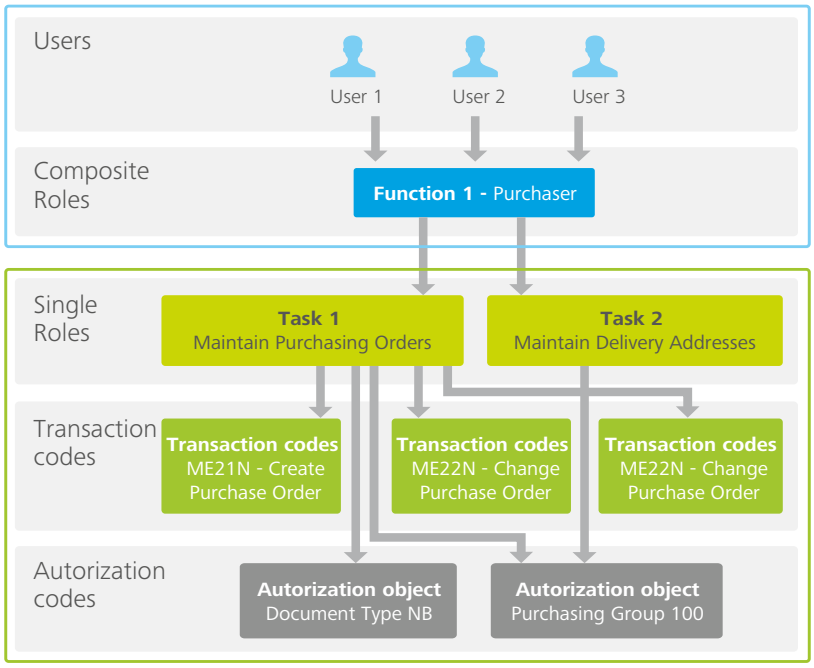

Figure 1: Deloitte's two-layer concept model

A transparent and modular authorization model also allows easier monitoring and audit. More specifically, the high granularity and rigidity of pre-designed tasks makes it very easy to report on the extent of user's access rights. If a change (extension or reduction) of access rights is needed for a given function (job-role), the security administrator's efforts are limited. This model is visualised in Figure 1.

Our approach to designing authorizations in ERP systems is based on the two layer function-task concept, following a rigid and proven logic that combines the technical flexibility with ease-of-use for the business. The key characteristics of a sound authorization concept include:

Transparency

The transparency of a role model defines comprehensibility.

Scalability

Scalability defines how easily the role model could be extended.

Maintainability

Maintainability defines the maintenance cost.

Deloitte has the skilled specialists, experience and tools to deliver a sound SAP Authorization concept to your organization:

- We provide a generic role catalogue to be tailored to your company's structure.
- We provide extensive expertise on the technical set-up of SAP security models.
- Our combined expertise in SAP processes, Audit, Risk & Control ensure our access management solutions are sustainable and fit the Company's strategy & objectives.

We follow a 4-step process:

Step 1 – Planning & Preparation

First, we work with you to identify and specify the security objectives of your company. They will be documented in the Security Baseline document and a Role Change Management process will be defined.

Step 2 – Design & Realization

During this stage the business requirements are further refined and translated into technical specifications ensuring clear and consistent design. In this step we also build the planned enhancements in line with the business requirements and the business performs extensive testing.

Step 3 – Final preparation

During the Final preparation the authorization concept is transported to the Production environment(s) and the technical documentation is finalized. The knowledge transfer and handover are essential to ensure a smooth transition.

Step 4 – Go-Live & Hypercare

After the Go-Live our team of experts will closely cooperate with and support your security team to guarantee a quick resolution should any issues arise.

Control your environment, maximize the risk visibility and rely on accurate data to run your business and support your strategic decisions.

Contacts

For more information, please contact:

Erik Luysterborg
+32 2 800 23 36
eluysterborg@deloitte.com

Pieter Lenaerts
+32 2 800 27 26
plenaerts@deloitte.com

For further information, visit our website at www.deloitte.com

2782