Untangling SAP Security

pwc

Many medium to large organizations today use SAP to help operate their complex business environment. SAP is the largest enterprise resource planning (ERP) system in the world. It is a total business solution which supports several financial and non-financial processes such as sales, distribution, production, financial and management accounting, human resources, inventory and logistics management. SAP's unique authorization concept, as well as its extensive configuration and security settings offer many control options. SAP security configuration however, may not always be applied consistently due to its highly complex nature and the amount of flexibility the application provides.

How can PwC help?

PwC has developed an industry leading tool called ***Automated Controls Evaluator (ACE*)***.

The purpose of this tool is to analyze SAP security settings and identify privileged access and potential segregation of duties issues accurately and efficiently. Our tool comes with a set of pre-defined segregation of duty (SoD) conflict cases. These cases include the required transaction codes, authorization objects and field values necessary to enable meaningful results which are representative of the levels of access any particular user has been granted. False positives are therefore minimized and this greatly reduces the level of effort required to analyze the results.

What does ACE* do?

The tool extracts relevant security and configuration data from the SAP system, analyzes it and generates exception reports by role or by user for management review and follow-up. As the security data interrogation and analysis is performed on an independent computer, there is no impact on the organization's system performance. The tool requires two ACE* ABAPs (Advanced Business Application Programming) files to be run on the production system. The extracted data appears in a format that can only be read by ACE*. The ABAP files introduce no changes to the production systems and settings. Profile or role designs and user allocations are interrogated against SAP administrative objects, critical module transactions and other transaction combinations. SoD conflict test cases can be selected from a set of pre-defined tests inside the global test library or can be custom designed as per client requirements.

The ACE tool facilitates the following types of analysis in SAP:*

Privileged Access Review

ACE* identifies security risks within SAP by analyzing access to the following high risk areas:

- Critical basis transactions;
- User provisioning process;
- Program changes and development;
- Computer operations; and
- SAP tables and programs.

Segregation of Duties Review

ACE* analyzes the potential segregation of duties issues within and across business processes by reviewing the conflicting access at:

- Role and profile level;
- Ability level (group of SAP transactions allowing a user to perform the same business functionality);
- Transaction level; and
- Object and field levels.

In case of an GRC implementation, it supports the evaluation of the ruleset.

Configuration Review

ACE* analyzes key SAP configuration settings which act as automated application controls such as “three-way match” and “release strategy.”

ACE* can be used to assess security and configuration within all business cycles.

Standard SoD conflict cases have been set-up for business cycles in the global test library.

Contact

Andrea Major
Partner
+36 1 461 9364
andrea.major@hu.pwc.com

Angelika Jonás
Manager
+36 1 461 9704
angelika.jonas@hu.pwc.com

pwc