July 2014, HAPPIEST MINDS TECHNOLOGIES

Continuous Compliance in SAP Environments

Author

Shirish Thadla

SHARING. MINDFUL. INTEGRITY. LEARNING. EXCELLENCE. SOCIAL RESPONSIBILITY.

You can remediate this situation by easily finding these noncompliant situations through a targeted query.

All values entered through the organizational panel are stored in Table AGR_1252. If an organizational field is manually changed, this value is stored in Table AGR_1251 instead of Table AGR_1252. To find these values, you can perform the query on Table AGR_1251.

Identify Manually Added Authorizations in a Role's **Authorization Tree**

You can find a role's authorizations that don't seem to be related to any transaction codes or that have been manually created. It's important that all authorizations present in a role's authorization tree are logically related to the transaction codes granted with the role itself. Otherwise, you risk losing control of your security concept. Each manual authorization added into the authorization tree is not linked to the transaction in the role menu. That means when you remove a transaction from the role menu, the manual authorization objects present in the authorization tree will not automatically be removed.

Finding Non-standard or Manual Authorizations

If you want to retrieve all manually inserted authorizations, you can do so through Transaction SE16 by browsing Table AGR_1251 (Authorization Data for the Activity Group).

Ensuring Users are assigned only to the Roles and Transactions they Use

You can determine whether a user has too many roles assigned to him by exporting statistical data to a spreadsheet. It's normal to find roles with hundreds (or even thousands) of transactions defined in a role's menu. If you ask your business users to tell you which transactions they need, they will probably ask for all available transactions. However, security guidelines indicate that each user should only be authorized for the minimum transactions he needs (the principle of least privilege).

While Transaction ST03N (workload and performance statistics) is mainly used to verify an instance's performance, it's a fantastic resource for security managers as well. If you want to extract all Transaction ST03N data, you can use a specific function module. Using Transaction SE37 (ABAP function modules), you can execute a function called SWNC_GET_WORKLOAD_STATISTIC.

Indirect Role Assignment to Simplify User Maintenance and Reporting

You can use the HR organizational structure (HR-OM) to distribute authorizations to users. The classical approach to assigning a role to a user is direct assignment via Transactions SU01 (user maintenance) or PFCG (role maintenance). However, there's a more powerful scenario you can consider: indirect assignment of roles to users using an organizational structure as a bridge between users and roles. With this scenario, it will be much easier to share security documentation with business contacts who technically own the data and users but often have very limited technical knowledge.

© 2014 Happiest Minds Technologies Pvt. Ltd. All Rights Reserved

One of the most difficult decisions a user manager has to make is how to delegate duties among business contacts. This is because they speak a different language— security and authorization managers are often very technical, whereas business references are not necessarily SAP experts. For instance, when you make a pivot table from data stored in Table AGR_USERS to document the link between the roles and users, the result will be similar to the one shown in the figure below (with roles in the rows and users in the columns). Business contacts will find it very difficult to match this output with their organization.

chette di riga	ACAVALLERI	AFAZIO	AGOMBA	APAPA	CCORONATO	FBERETTA	FCOLOMBO	FF_USER	FMORLEO	FPASTORE	FSOFIA	GCANNATA	GGABRIELE	ISANTANOCITA	JALBAMONTE	MABBA'	MARRIGONI	MPIROTTA	MTRESOLDI	NCAVALLERI	NPARRAVICINI	PALBESANO	PPERABONI	RMARELLI	RPULICI	TEST_200	TEST_IAM_04	VNAVA
BC:T_001_V															1		1		1									1
BC:T_999_V								1																				
CO:C_XX_0001																1							1	1				
CO:T_001_M																1							1	1				
CO:T_005_M																1							1	1				
CO:T_016_V																1							1	1				
FI:C_MD_MANAGER										1																		
FI:C_XX_0001			1		1	1								1														
FI:T_001_E		1																										
FI:T_001_M		1																										
FI:T_001_V		1																										
FI:T_002_E		1																										
FI:T_002_M		1																										
FI:T_002_V		1																										
FI:T_005_M										1																		
FI:T_007_M										1																		
FI:T_007_V			1		1	1								1		1							1	1				
FI:T_019_M										1																		

Instead of using a direct assignment (of roles to users), you can take advantage of the HR-OM component. You can assign the role (AG object) and users (US object) to the position (S object).

Identify Business Owners

By understanding each type of owner that's present in a business, you can easily determine which person manages what data or responsibility to ensure proper governance. Defining the owners of a company is not very clear, especially during periodical revalidations (users and roles). Often, an owner receives a document to be validated and he has difficulties because the goal and the responsibilities are not well defined.

In security processes, many different areas are involved. For each area, one or more owners have to be identified.

Divide the authorization processes for owners into (at least) two main areas:

- User processes
- Role processes

happiest minds
The Mindful IT Company
Born Digital . Born Agile

© 2014 Happiest Minds Technologies Pvt. Ltd. All Rights Reserved

The typical situation where it's not clear how to proceed occurs when a user asks for a new transaction. The requested transaction could be added to a role not yet assigned to the user, or a new role (containing the transaction) could be assigned to the user. In recent years, the Segregation of Duties (SoD) logic has added a new level of complexity. When a new request causes an SoD conflict, a new set of owners are involved.

Unfortunately, when the responsibilities aren't well addressed, the security team becomes responsible for all mistakes and misunderstandings. A proposal containing details of responsibilities held by different owners follow:

Business area owner

Responsible for the users in his area or department. Every user must be assigned to a responsible person who will manage each change of the user's data.

Business process owner

Responsible for defining the sequence of all activities that are mandatory in his processes. The decisions made by a business process owner should be valid across all company departments. For each business process, there is one process owner.

Data owner

Responsible for the most important information of the process: the data. Each data owner must assure that the data are correctly created and maintained. Every time a data is involved, data owners must validate the request.

Role owner

Responsible for the content (transactions and authorizations) of roles. He must communicate with data owners and process owners to guarantee the final integrity for each role's change.

SoD rules owner

Responsible for physically maintaining the set of rules necessary to perform risk analysis.

SoD risk owner

Responsible for defining a risk in terms of content and level of severity (critical, high, medium, low).

SoD mitigation control owner

Responsible for mitigation actions.

Many other people can also be relevant to maintain a high level of governance such as internal controllers, business process analysts, and so on. All security and authorization

© 2014 Happiest Minds Technologies Pvt. Ltd. All Rights Reserved

processes should be well designed and written with a clear indication of the owners' involvement and responsibilities. When all owners have been identified, it's important to formally communicate this fact in the company to avoid misunderstanding.

Outcome

Though the above procedure is time consuming and requires manual effort, the organization can be assured of achieving:

- Minimizing Access Risk and Preventing Fraud
- Enabling a Secure, Global Supply Chain

The above procedure can be automated by implementing/integrating the SAP GRC application within the landscape which not only reduce the efforts, cost but also brings in a continuous automated monitoring control framework.

Appendix

Most important User Tables

Table	Description	How it helps
USR01	Transaction SU01 DEFAULT Tab data	Verifies the default data tab of users
USR02	User login data, date of creation, last logon, user status	Finds users not assigned to any user group
USR05	Parameter ID and value for each user	Provides the list of parameter IDs which can be restored in case of an accidental deletion
USR07	Last failed authorization check	Enables you to enquire on last failed authorization checks
ADR6	Email addresses	Extracts the mail address
TPARA	User master data Parameter ID tables	Finds a Parameter ID

happiest minds
The Mindful IT Company
Born Digital . Born Agile

© 2014 Happiest Minds Technologies Pvt. Ltd. All Rights Reserved

Most important Role Tables

Table	Description	How it helps
AGR_1016	List of all generated profiles linked to a role	Provides the role's name by looking at the profile
AGR_1250	List of all authorization objects inserted into a role (without authorization value detail)	Provides all authorization objects inserted into a role without authorization object value detail
AGR_1251	List of all authorization objects inserted into a role (with authorization value detail)	Provides information on whether a critical authorization object is inactive in all roles except certain ones
AGR_1252	List of organizational values inserted into a role	Provides the allowed organizational data domain where a role can work
AGR_AGRS	List of all simple roles in a composite role	Provides how many simple roles are inserted in a composite role
AGR_DEFINE	List of all roles defined in a system	Provides a list of all roles defined in the system
AGR_FAVOS	Personal Profile Generator roles favourites	Lists the favourite roles for a user in transaction PFCG
AGR_FLAGS	Role Attributes	Contains several flag attributes, including whether a role is collective and what the role master language is
AGR_NUM_2	Last number of generated profile	Tells the last number of the generated profile
AGR_TCODES	List of all transactions inserted into a role menu	Tells in which role menus Transaction MM03 is inserted
AGR_TEXTS	List of all descriptions of a role	Tells how many language descriptions a role has
AGR_USERS	List of all users assigned to a role	Tells how many users are assigned to a role

happiest minds
The Mindful IT Company
Born Digital . Born Agile

© 2014 Happiest Minds Technologies Pvt. Ltd. All Rights Reserved