GRC Access Control Implementation Guide for Enterprise Role Management

Applies to

SAP Solutions for Governance, Risk, and Compliance: Access Control (rel. 5.2)

Summary

GRC Access Control identifies and prevents access and authorization risks in cross-enterprise IT systems to prevent fraud and reduce the cost of continuous compliance and control. This paper provides a quick reference guide to understand the main features, business benefits, and implementation best practices of the application's capability for enterprise role management.

Authors: Janet Tran, Ruth Johnson

Company: SAP

Created on: 15 Sep 2007

Revised: 20 Nov 2007

Authors' Bio

Janet Tran and Ruth Johnson are leading experts on GRC Access Control. Prior to joining the Customer Advisory Office for GRC, they gained deep experience in a large number of client implementations.

Table of Contents

Main Features

GRC Access Control allows for better enterprise role management. The features listed here are noteworthy as they extend the capabilities to manage roles found in SAP ERP:

1. Documentation
    a. Role definition – additional role attributes to document the role definition.
    b. Maintain role information after they are generated to keep role information current.
    c. Approval comments with date and time stamps for each role.
    d. Role comparison – ensure role definition and roles generated in SAP systems are in sync. Provides an auditing tool to show any discrepancies between role definitions and actual roles generated in the back-end system.
2. Preventive risk analysis
    a. Performing risk analysis at role design time prior to creating role in SAP Development environment.
3. Approval workflow and role generation
    a. Setting up a workflow for role approval.
    b. Automated role generation into SAP R3 environment.
4. Audit Trails & Reporting
    a. Tracking progress during role implementation.
    b. Monitoring the overall quality of the implementation.
    c. Providing an audit trail for all role modifications.
5. Integration with compliant user provisioning
    a. Role source for user provisioning

Key Benefits

Access Control simplifies the enterprise role management process:

- Provides a single enterprise role repository for role design, testing and maintenance to enforce consistency and standardization.
- Provide role source integration with compliant user provisioning
- Facilitates the role design process with a pre-defined (yet customizable) design methodology and workflow
- Supports the definition and documentation of role information, authorizations and testing results
- When linked to Access Control risk analysis and remediation it enforces the Segregation-of-Duties analysis during role design to prevent risks from entering application systems
- Provides change history for auditing and compliance
- When integrated with Access Control compliant user provisioning it provides workflow approval for control checking and evaluation during role design
- Provides automatic SAP role generation (for SAP WAS(ABAP) target systems only)

Key Stakeholders

Enterprise role management in Access Control focuses on four audiences:

1. Role Design Team – Business Process and Role Owners define what access a given type of user requires to do his or her job
2. Role Approvers – Business Process Owners are able to validate and approve a new or modified role
3. Administrators – Further defines and generates the approved roles based on pre-defined authorizations synch from SAP ERP.
4. Auditors – Detailed reports and audit trail simplify the verification of corporate governance

Best Practices – Implementation Preparation

1. Define and assess current role management process
    a. Determine the strength and weakness in your current role management process:
        i. How do you currently design roles?
        ii. How do you document and store documentation of roles?
        iii. How often do you change your roles?
        iv. How time consuming is the role management process?
        v. What is your organization's current remediation status?
        vi. What is your organization's current process to meet compliance initiative regarding role design and business owner approval?
        vii. How much time is spent in responding to audit requests – internal and external?
    b. Gain knowledge of the system's key features to leverage the application functionality to develop or strengthen your process
        i. Determine how the application can compliment the SAP profile generator (transaction PFCG) functionality and reduce manual effort, disjoint audit trails, etc.
        ii. Determine the level of documentation required for your roles
        iii. Start out with simple process first, then build upon it.
    c. Determine project goal and scope. List specific goals for your organization:
        i. Optimization or consolidation of roles to remove duplication of roles
        ii. Reduce unused transaction codes in roles
        iii. Reducing or remove SOD risk
        iv. Reduce role change requests by x%
        v. Increase business user involvement, awareness, and ownership of compliance issues
        vi. Reduce the complexity of role maintenance
        vii. Increase visibility to audit trails for role change and approval
        viii. etc.
    d. Determine role management methodology
        i. Determine key stakeholders
        ii. Determine role attributes – business process, sub process, functional area, etc. Role Expert makes it easy to define role attributes, mapping roles to your business processes, functional areas, specific locations, etc. Because of this, the following tips may be helpful:

1. The thought process is more important than the mechanics of role design.
2. Carefully define your role attributes before you use the application to ensure integration with compliant user provisioning.
   Note: Role attributes such as business process, sub process, functional area, etc. have to match.
3. Involve the business team (Business Process Owners, etc.) in the design process early and often.
4. Continually look for opportunities to rethink, clarify, and improve business efficiencies.

iii. Determine role naming convention – create naming conventions which automatically suggest role and profile naming standards during the role creation process. Consistent naming conventions are critical to maintain your organization's roles.

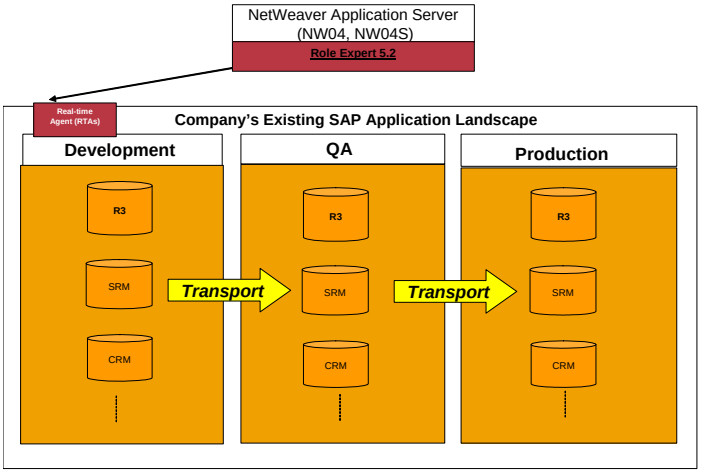
iv. Determine system landscape – the target systems for role generation and risk analysis do not have to be the same. For risk analysis target system, a QA system with quality data (Production like or fresh copy of Production) or Production system is recommended. For role generation target system, Test or Development system is recommended – depending which project phase you're in.

v. Determine approval process – The approval process allows documented collaboration among different stakeholders involved in the role management process. To ensure success, involve the business process owners early and often to generate support and buy-in for the process.

vi. Determine role testing and documentation procedure – document testing details or upload testing documents.

2. Employ phased approach for quick wins and to reduce change management risks:
   a. Phase 1 – Role documentation only (including conversion from existing documentation)
   b. Phase 2 – Pilot implementation with full functionality to a small user group
   c. Phase 3 – Roll out to additional groups
   d. Phase 4 – Additional roll outs as needed
3. Provide appropriate and just in time end user training
4. Develop and communicate enterprise role management procedures to all stakeholders. Just because you have a new system in place, it does not mean you will not need procedures.
5. Recommended change control management
   a. Generate roles in a development environment, with risk analysis pointing to Production or QA systems
   b. Migrate roles via your current change control process DEV to QA
   c. After thorough testing, and risk analysis pointing to production system, again follow your current change control process from to transport roles from QA to Production
   d. Throughout the process, use the application's Role Comparison Feature to ensure that defined roles are in synch with generated roles in target systems.

Best Practice – Change Management



Recommended Implementation Scenarios & Use Cases

AC 5.2 – Only Access Control's enterprise role management is required for the following scenario. Compliant user provisioning is optional for approval workflow.

1. **A documentation solution only (Approval workflow – Optional)**

   a. Use Case – For customers who want to document role definition but do not want to automate role generation via Access Control due to various reasons: 1) Customer uses 'Menu' feature in PFCG and does not want to override existing Menus, 2) Customer continues to use PFCG to maintain roles & authorization data, or 3) Customer wants to separate the role management project into phases with Phase 1 as role documentation only.

   Use case illustration:

   Role design team enters role definition and transaction codes => Security team takes the role, refines transaction codes/objects definition & create role in PFCG => Role Owner approves the role => Role design team test roles and document testing.

   Role Methodology: Definition => Authorization => Approval => Testing

   Note: Roles can be searched by the 'Approval' phase to identify roles which requires action for documentation and/or role maintenance in target systems. Other than role owner notification, no other automatic notification of workflow is available in Access Control 5.2.

   1) Process:

      1. Maintain role definition in enterprise role management (Role design team)

         a. Maintain authorization data for documentation (Role design team enters the transaction codes)

      2. Search for roles which are ready to be created or maintained in 'Approval' phase (Security team)

      3. Manually create/maintain role in Development system via PFCG per authorization data. Additional changes maybe required to complete role authorization data. (Security team)

         Note: *When changes are made directly in PFCG to complete the role, the security user must manually maintain the authorization data changes in enterprise role management.*

      4. Risk analysis is not performed or performed manually in risk analysis and remediation (Access Control).

5. When ready for business/role owner approval, click on 'Approval' button to submit the role to the next stage and/or trigger workflow notification.

***Note:** For full approval workflow and email notification function, configured workflow in compliant user provisioning is required. Role owner must have Approver authorization to be able to approve requests.*

6. Log into Access Control to approve the request for role maintenance. (Role Owner)
7. Perform role testing in source system. (Role design team)
8. Document role testing. (Role design team)

Access Control 5.2 – Usage of compliant user provisioning and risk analysis and remediation is required for the following scenarios:

2. A documentation, approval, and preventative risk analysis solution

a. Use Case – Mainly for customers, who want to document role definition, use workflow approval (where electronic approval maybe required as standard control for their organization), perform preventative risk analysis, maintain authorization data in enterprise role management and generate roles in SAP ERP from Access Control.

Important Note:

1) If customer currently utilizes the 'Menu' feature in PFCG, this solution may not work for them since role generation via Role Expert will override existing Menus previously created in PFCG.

2) If a customer has more complex authorization data maintenance requirements (which can only be maintained directly in PFCG) than the current authorization data function available in Role Expert, then the documentation only Scenario 1 – detailed above – is recommended.

Use case illustration:

Role design team enters role definition and transaction codes => Role design team perform risk analysis at transaction code level => Security team takes the role, refine transaction codes/objects definition, & perform risk analysis => Security team derive roles (if needed) => Role owner approves the role => Role design team test roles and document testing.

Role Methodology: Definition => Authorization => Risk Analysis => Derive Roles (Optional) => Approval => Generation => Testing

Note: Roles can be searched by the 'Derive Role' phase to identify roles which requires actions to further refine authorization data. Other than role owner notification, no other automatic notification of workflow is available in Access Control 5.2.

1) Process:

1. Maintain role definition in Access Control (Role design team)
    a. Maintain authorization data at transaction code level (Role design team enters the transaction codes)
2. Perform risk analysis at transaction code level in enterprise role management (Role design team)
3. Search for roles which are ready to be created or maintained in 'Derive Role' phase (Security team)
4. Refine transaction codes/objects definition & perform risk analysis with enterprise role management (Security team)
5. Derive role(s) in Access Control if needed (Security team)

***Note**: Org Value mapping is required to use 'Derived Roles' If derived roles are not required, the security team will need to 'Save' on the "empty" derive roles screen to have the role move to the next step.*

6. When ready for business/role owner approval, click on ‘Approval’ button to submit the role to the next stage and/or trigger workflow notification (Security team)

Note: *For full approval workflow and email notification function, configured workflow in compliant user provisioning is required. Role owner must have Approver authorization to be able to approve requests.*

7. Log into Access Control to approve the request for role maintenance. (Role owner)
8. Search for roles in ‘Generation’ phase to perform role generation from enterprise role management to target system(s). (Security team)
9. Perform role testing in source system. (Role design team)
10. Document role testing in Access Control’s enterprise role management. (Role design team)

Frequently Asked Questions

1. Can enterprise role management be installed standalone?
    a. Yes, it works as standalone installation. However, without integration to other Access Control capabilities as risk analysis and remediation or compliant user provisioning, it will not be able to perform certain functionalities, such as risk analysis or approval workflow.
2. Is there an upgrade/migration path from release 4.0 to release 5.2?
    a. Yes
3. Which SAP applications are not supported, such as SCM, BW, etc.?
    a. The system supports any SAP applications with SAP_BASIS release 46C, 47/620, 640 and 700. However, automated role generation can only be performed to roles on the ABAP stack of SAP Web Application Server
4. Can we import roles existing outside of Access Control, such as PFCG, legacy systems, or lotus notes?
    a. For roles from SAP systems which have been generated via PFCG, you can import roles with all authorization data by downloading the roles via a provided transaction code, create role information file, and import roles.
5. How does role comparison work?
    a. You can compare multiple roles against one another or you can compare one role in Access Control against one role in the back end system at a time.
6. How do you add transactions to single roles? The authorization data button is not always visible. In which case is it available?
    a. The “Definition” step is a mandatory first step in the process. It is required together with the “Authorization Data” step to utilize the authorization data function. Even if you use enterprise role management for documentation purpose only, make sure to include this step when you configure the process in the configuration tab.
7. How can you delete the authorization objects?
    a. The authorization objects can only be disabled and cannot be deleted. Such functionality is not currently available.
8. How is it possible to enter the remarks which are shown in the change log?
    a. The approval workflow is integrated with Access Control’s compliant user provisioning. When a new role or role change requires approval, enterprise role management passes the change to compliant user provisioning in a change request. The approver logs on, approves the request and enters the approval remarks. The change logs will be communicated as Approver remarks.
9. What are the criteria for the process step definition to be finalized and the next workflow step is reached?
    a. The workflow process terminates at the last step when all criteria for this step are fulfilled.
10. Is it possible to configure "Actions"?
    a. You can’t configure actions; you can only configure steps within the Process.
11. We do not want to use the SAP generated profile name. We need to have the profile specified in Access Control – according to our naming convention standard – to override SAP profiles. How does this work?
    a. The profile name in Access Control will override the SAP profile name in the backend system. If left blank, the SAP generated profile name will be kept in the backend system.

12. Authorization object source – When creating authorization data by bringing in objects via function search and add all transaction codes from a function – does it come from rule architect in the Access Control rule architect or PFCG? Also, when creating authorization data by adding a transaction code directly, where does the auth. object come from?

    a. All authorization objects come from USBOT_C table in the connected SAP ERP target system.

13. Role classification via naming convention – We need to have a field provided for role classification that is at a higher display node than custom field. The 3rd character in our current role name denotes role certain role classification.

    a. This functionality is not current available in this release. The suggested workaround is to use custom fields or use role naming convention.

14. Is there a way to mass import roles?

    a. Yes, the template for mass role import is provided in the Help link.

15. Mass role change on master role and impact on derived role – When a change is made on master role via mass role change function, would the derived roles be automatically changed as well?

    b. Yes, the derived roles will change automatically (per master role changes) once the master role change is made and re-generated.

16. Is the application also available for SAP CRM, BW and or APO?

    a. Currently, you can use enterprise role management to manage documentation and approval for CRM, BW, and APO roles, but the application can automatically generate roles only for SAP ERP systems.

17. Where can I get the template for mass upload of roles?

    a. For manual import from flat files such as spreadsheet, etc., the template can be found in the “Help” link. For the bulk import file from SAP, a template is not needed since the file is generated by our transaction when uploading from SAP ERP/PFCG. Most roles information resident within ERP will be imported from PFCG but if additional role attributes need to be loaded from a file, the templates can also be found in the Help link.

18. When defining roles, how can I enter a range of transaction codes such as MM01 – MM03?

    a. Due to role management best practice, transaction ranges or the usage of wildcards in S_TCODE is not encouraged and currently it’s not on our roadmap to support this function. Currently, transaction codes can only be added one by one.

19. When defining roles, how can I enter an ‘*’ value? For example I might want my role to have all transactions beginning with the letter ‘I’, therefore how can I enter ‘I*’?

    a. Not supported, same reason as in Q8 above. This can be achieved by searching and selecting all the transactions with ‘I*’.

Copyright