| **Access Risk Analysis – ARA**  **Analyzing Risks associated with Access** |
| --- |
| Risk: when an Employee in a Company is assigned with Task/Tasks that could provide him/her with an opportunity to commit fraud  Employee -> Company -> Task/Tasks -> Opportunity -> Fraud  Tasks are assigned to the employee in form of Roles, which are made up of Actions/Tcodes, which in turn are made up Permissions/Authorizations |
| Workshops with BP Owners and other relevant personnel would have to be conducted to gather information about the Risks associated with the following:  Roles -> Actions/Transaction Codes -> Permissions/Authorizations  Role1                Action1  Action2             Permission1   Permission2  Role2                Action3  Action4             Permission3   Permission4 |
| Based on the information gathered we need to define the Risks      . Action1= Conflicting Action   .Action2= Conflicting Action.   Action3= Critical Action    .Permission1= Critical Permission  Function1= Action1   .Function2= Action2   .Function3=Action3   .Function4= Permission1  Risk 1= Function1+Function2 . Risk 2= Function3  Rule is a condition: If Function1+Function2 is given to a user Then it is a Risk  Therefore Rule1 is generated against Function1, Function2 and Risk1  \*Example: Action1= XK99: Vendor Mass Maintenance .Action2= ME2L: Maintain Purchase Order – Purchasing  Risk= Create a fictitious vendor and initiate purchases to that vendor |
| Run a Risk Analysis against all the Risks defined |
| Based on the Analysis, Remediate the Risks by executing cleanup process by Re-designing/defining the roles.  This can be done through Simulation to check if the defined Risks will be eliminated if  the cleanup is executed. |
| In certain unavoidable circumstances Remediation isn’t an option, so the solution is to Mitigate the Risk                           Mitigation     | Prevention | Detection | | --- | --- | | Super User Access | Mitigation Control  Audits  Alerts |   So when you create a Mitigation Control:  You specify the Risk Ids and the OU they are associated with->  The Risk Ids will look up the Function they are associated with->  Functions will look up the Actions (T-codes) they are associated with. Assign an Owner and Controller to the MC and  tie all of this up to an end user/role/profile who is assigned with a role/roles, which could pose a threat. |
| To Ensure all the hard work done so far does not go for a waste, run  SOD review, Audit Trails and Risk Analysis on a periodic basis |

| **SOD Management Process** |
| --- |
| The entire process described above is termed as ‘SOD Management Process’.    **Segregation of Duties (SoD)** is an internal control within a Company implemented to prevent or decrease the risk of errors or regulatory irregularities and ensure corrective action is taken. Ideally, no one individual must have the authority of:  Creation .Modification .Reviewing .Deletion  SoD ensures no single user has access to separate phases of these business transactions. This is done by Dividing, Distributing and Allocating key tasks amongst various individuals thereby eliminating or at least reducing the possibility of errors and fraud. All of this is carried out in three separate phases:    Phase 1  Risk Recognition  Rule Building & Validation    Phase 2  Risk Analysis  Remediation  Mitigation    Phase 3  Continuous Compliance |

***\*Credit for the following SOD Management Process flow goes to:***[***Alessandro***](http://scn.sap.com/people/alessandr0)***&***[***Colleen***](http://scn.sap.com/people/m.lee)

| **Steps** | **Description** |
| --- | --- |
| [/wp-content/uploads/2014/08/step1_530217.png](javascript:void(0);) | Gather a list of applicable SOD conflicts that allow fraud or generate significant errors. The outcome of this step is that your business has determined what is an unacceptable risk that they want to report on and manage via remediation or mitigation.  Helpful documents:  [Risk Lifecycle](https://blogs.sap.com/?p=102548) |
| [/wp-content/uploads/2014/08/step2_530218.png](javascript:void(0);) | Build the rule set based on the recognized risks from step 1. The outcome of this step is the technical rule set to analyze the user and/or role assignments.  Helpful documents:  [Business Risks / Rule Set](http://scn.sap.com/docs/DOC-54434)  [Rule set – Rules & Rule Types](http://scn.sap.com/docs/DOC-54530) |
| [/wp-content/uploads/2014/08/step3_530237.png](javascript:void(0);) | Analyze the SoD output. This can be performed with the help of SAP GRC Access Control. In case of manual analysis, for each user, analyze if he/she has the access to perform any of the conflicting functions defined in step 1. The outcome is basically to provide the business insight to alternatives for correcting or eliminating discovered risks.  Helpful documents:  [Online vs. Offline Risk Analysis](http://scn.sap.com/docs/DOC-56653) |
| [/wp-content/uploads/2014/08/step4_530238.png](javascript:void(0);) | In this step, evaluate if the conflicting tasks can be performed by an alternate person. If so, role changes and/or user reassignments can be performed to segregate duties properly. The outcome must be a very low number of remaining risks that need mitigation.  Helpful documents:  [Remediating Access Control SoD Risks](http://scn.sap.com/docs/DOC-57447) |
| [/wp-content/uploads/2014/08/step5_530239.png](javascript:void(0);) | If it would not be possible to remediate the existing conflicts, consider formulating an appropriate control to mitigate the risk. This would typically entail working with the business to setup additional monitoring procedures that ensure to compensate the risk. The outcome must be no remaining risks.  Helpful documents:  [Internal Controls – a step towards strong controls](http://scn.sap.com/docs/DOC-56548)  [Defining Mitigating Controls / Compensating Controls](http://scn.sap.com/docs/DOC-53355)  [Creation of Mitigation Controls in GRC 10.0](http://scn.sap.com/docs/DOC-51292)  [Mitigating Control Lifecycle](https://blogs.sap.com/?p=102547) |
| [/wp-content/uploads/2014/08/step6_530240.png](javascript:void(0);) | Finally, establish a new continuous process wherein every access request is reviewed against the SoD conflict matrix prior to provisioning on the system. Also make sure that all role changes must be analyzed and remediated before implementing. The outcome, and also final result, your system remains clean.  Helpful documents:  [Approve/Reject Own Requests](http://scn.sap.com/docs/DOC-55401)  [Risk Terminator on SAP Wiki](http://wiki.scn.sap.com/wiki/download/attachments/51962/Risk%20Terminator%20Documents%20on%20SCN.pdf) |
| **Configuration in a Nutshell** | |
| Now that we’ve covered the what and the why part we have to get our hands dirty and physically create them. If you have access to a Server, after following SAP documentation for ‘From Post-Installation to First Risk Analysis’ and ‘Enhanced Access Risk Analysis’, try executing the following tasks:     1. Create test users using SU01 2. Create test roles with Critical/Conflicting Actions using PFCG 3. Assign role/roles to test users including roles for Risk Owner , Mitigation Controller 4. Create Access Control Owners in NWBC 5. Activate/Check following BC Sets using ‘SCPR20’    * GRAC\_RA\_RULESET\_COMMON    * GRAC\_RA\_RULESET\_SAP\_R3    * GRAC\_RA\_RULESET\_SAP\_HR (Optional) 6. Check Configuration Parameters of Risk Analysis: SPRO -> IMG -> GRC -> Access Control -> Maintain Configuration Settings    * Risk Analysis    * Function Maintenance    * Mitigation Maintenance    * Change Log 7. Create/Check Business Process and Sub Process: SPRO -> IMG -> GRC -> Access Control -> Maintain Business Process and Sub processes    * This will come in handy when creating Functions and Risks 8. Create Organizations: SPRO -> IMG -> GRC -> Shared Master Data -> create a Root Organization Hierarchy    * You cannot create a Mitigation Control without this 9. Add Owners to the created Organization in NWBC: Setup -> Organizations 10. Run following Sync Jobs:  SPRO -> IMG -> GRC -> Access Control -> Synchronization Jobs     * Authorization Sync     * Repository Object Sync 11. Create the following in NWBC     * Functions     * Access Risks     * Mitigation Control 12. Run a Risk Analysis against the Risks at Role level and after the cleanup at User level 13. Remediate using Simulation and see if it works 14. Mitigate Risks against User/Role/Profile 15. Create Alerts: SPRO -> IMG -> GRC -> Access Control -> ARA -> Generate Alerts 16. Setup Batch Risk Analysis on a periodic basis:  SPRO -> IMG -> GRC -> Access Control -> ARA -> Batch Risk Analysis 17. Setup SOD/UAR Review | |