

## NOTE AUGUST 2006

---

This is an example for a possible documentation structure including special requirements for HR.

### *Table of content*

1. Target / scope
2. Premise
  - 2.1. Protection of Data being transmitted across state and international borders  
[Non-violation of local and export laws]
3. Function structure
  - 3.1. Explanation of concept
  - 3.2. Integration in SAP system landscape with interfaces
  - 3.3. Description of system and data ownership
  - 3.4. Data classification
  - 3.5. Overview of relevant organizational units
4. Dependency of authorizations
  - 4.1. Segregation of duties
  - 4.2. Dual control principle  
[symmetric with OSS 151207 / asymmetric] – P\_ORGIN,  
P\_ORGXX  
or RPUAUD00 (master data log)
5. Functions
  - 5.1. Basic system adjustments
    - 5.1.1. Profile parameter of the function category login/\* and auth/\*
    - 5.1.2. Globally deactivated authorization objects
    - 5.1.3. Deactivation of individual authorization objects
  - 5.2. Name convention and Use
    - 5.2.1. User groups
      - 5.2.1.1. User of the User group SUPER
      - 5.2.1.2. User of the User group “XXX”
    - 5.2.2. User Name convention
  - 5.2.3. Roles
    - 5.2.3.1. Use of SAP Standard roles
    - 5.2.3.2. Single Roles
    - 5.2.3.3. Composite Roles
    - 5.2.3.4. Inheritance and Derivation [USORG]
  - 5.2.4. Indirect Role assignment
    - 5.2.4.1. Local
    - 5.2.4.2. Global
  - 5.2.5. Profiles
    - 5.2.5.1. Use of the profiles SAP\_ALL, SAP\_NEW, P\_BAS\_ALL
    - 5.2.5.2. Use of SAP standard profiles
  - 5.2.6. Reference users
  - 5.2.7. Central User Administration
6. Working place analysis [Job description - including transaction codes]
  - 6.1. User with the authorization to maintain personnel master data
  - 6.2. User of the business area Financial accounting / Cost center import
  - 6.3. User with display authorization within the personnel administration
  - 6.4. User with critical authorization
  - 6.5. Coordination function for Payroll
7. HR Specials
  - 7.1. Infotypes
    - 7.1.1. Description of used Infotypes
    - 7.1.2. Use of Infotype 0130 [protection of master data from deletion]

- 7.2. Main authorization switches
  - 7.2.1. AUTSW ORGIN
  - 7.2.2. AUTSW ORGXX
  - 7.2.3. AUTSW NNNNN
  - 7.2.4. AUTSW ADAYS
  - 7.2.5. AUTSW PERNR
  - 7.2.6. AUTSW APPRO
  - 7.2.7. AUTSW ORGPD
- 7.3. Context sensitive authorization switches
  - 7.3.1. AUTSW INCON
  - 7.3.2. AUTSW XXCON
  - 7.3.3. AUTSW NNCON
  - 7.3.4. AUTSW DFCON
- 7.4. Structural authorizations
  - 7.4.1. Description
  - 7.4.2. Use
  - 7.4.3. Customizing and assignment [e.g. T77PR, TU77A]
- 7.5. System settings
  - 7.5.1. Table T77S0
- 7.6. P\_ORGIN
  - 7.6.1. [INFTY, SUBTY, AUTHC, PERSA, PERSG, PERSK, VDSK1]  
especially authorization level, organizational key, time limitation responsibility  
– time logic  
ADAYS in table T77S0, indicator for access (T582AVALDT) in T582A
- 7.7. P\_ABAP
  - 7.7.1. “Degree of simplification for authorization check”
  - 7.7.2. Reports to be protected
- 7.8. Log of HR report starts [Table T599R - evaluation with report RPUPROTD]
- 7.9. Use of PFCG\_ORGFIELD\_CREATE [OSS Note 323817]
- 7.10. Calculation Rules
- 7.11. External check DEÜV [Table T5D4S]
- 7.12. Protection of tables REGUH, REGUP in FI – [Table T558A]
- 7.13. Protection of special transactions [S\_TCODE and P\_TCODE]
  - 7.13.1. PU00
  - 7.13.2. PU01
  - 7.13.3. PU03
- 7.14. Integration of evaluation control [e.g. RHUSERREALATIONS]
- 8. User education and training
  - 8.1. Help Desk
  - 8.2. Super User
  - 8.3. User manual
- 9. User administration / role administration
  - 9.1. Structure
  - 9.2. Authorization administration
  - 9.3. Administrator user accounts
  - 9.4. Administration of user master records
    - 9.4.1. Creation
      - 9.4.1.1. Request
      - 9.4.1.2. User type
      - 9.4.1.3. Initial Password / Use of Wizard
      - 9.4.1.4. Approval procedure
      - 9.4.1.5. Archiving of request
      - 9.4.1.6. Guarantee privacy regulation / Data protection
      - 9.4.1.7. Initial Logon
    - 9.4.2. Change of responsibilities
    - 9.4.3. Change and deletion
    - 9.4.4. User master records in the system
  - 9.5. Administration of roles
    - 9.5.1. Principle of menu control
      - 9.5.1.1. Exceptions from the menu control
    - 9.5.2. Changes of roles
      - 9.5.2.1. Documentation of role changes
    - 9.5.3. Creation of roles and profiles

- 9.5.4. Testing of roles
  - 9.5.4.1. Positive Test
  - 9.5.4.2. Negative Test
- 9.5.5. Deletion of roles and profiles
- 9.6. Logon procedure
  - 9.6.1. Regulations for complex passwords
  - 9.6.2. Multiple logon
- 9.7. Control activities within the user administration
  - 9.7.1. Locking and deletion of users
  - 9.7.2. Unlocking of users
- 10. Protection of Special user
  - 10.1. SAP Standard user
    - 10.1.1. User SAP\*
    - 10.1.2. User DDIC
    - 10.1.3. Technical user (TMSADM, SAPCPIC)
  - 10.2. Company specific special user
    - 10.2.1. Emergency user
    - 10.2.2. Support user
    - 10.2.3. Batch-User
    - 10.2.4. ALE-Remote User
  - 10.3. Auditing
    - 10.3.1. Audit Log
      - 10.3.1.1. Configuration (e.g. all dialog user with SAP\_ALL)
      - 10.3.1.2. Evaluation
    - 10.3.2. Security Log
      - 10.3.2.1. Configuration
      - 10.3.2.2. Evaluation
- 11. Table logging
  - 11.1. General information
  - 11.2. Parameter
  - 11.3. Evaluation and check
    - 11.3.1. Display of logged table content
    - 11.3.2. Check of log status for individual tables

- 11.3.3. Other evaluations
  - 11.3.3.1. List of all logged tables
  - 11.3.3.2. List of change history for logged tables
- 11.3.4. Determination and control of size for table DBTABLOG
- 11.4. Archiving / Deletion
- 12. System changeability in the production system
  - 12.1. Security guideline for cross client settings
- 13. Client changeability in the production system
- 14. Special functions
  - 14.1. Restriction of download [S\_GUI, S\_OLE\_CALL]
  - 14.2. Restriction of query and ad-hoc query
  - 14.3. Restriction of printer access and authorizations
  - 14.4. Customizing authorization / Table maintenance
  - 14.5. Maintenance of system parameters
  - 14.6. Reports
    - 14.6.1. Name convention for self created reports
    - 14.6.2. Deletion of self created reports that are not longer needed
    - 14.6.3. Protection of self created reports
      - 14.6.3.1. Authorization group
      - 14.6.3.2. Authority-check in source code
    - 14.6.4. Documentation for self created reports
  - 14.7. Tables
    - 14.7.1. Name convention for self created tables
    - 14.7.2. Logging of self created tables
    - 14.7.3. Protection of self created tables [authorization-group]
    - 14.7.4. Documentation for self created tables
  - 14.8. Transaction codes
    - 14.8.1. Name convention for self created transaction codes
    - 14.8.2. Assignment of authorization-objects within SE93
    - 14.8.3. Maintenance of self created transaction codes SU22/SU24
    - 14.8.4. Documentation for self created transaction codes

- 14.9. Authorization objects
  - 14.9.1. Name convention for self created authorization objects
  - 14.9.2. Integration of self created authorization objects SU22/SU24
  - 14.9.3. Documentation for self created authorization objects
- 14.10. Batch-Input Sessions
  - 14.10.1. Protection of Batch-Input Sessions
  - 14.10.2. Procedure for cancelled Batch-Input Sessions
  - 14.10.3. Deletion of processed Batch-Input Sessions
- 14.11. Jobs
  - 14.11.1. General information [e.g. name convention]
  - 14.11.2. Definition of company specific jobs
  - 14.11.3. Documentation of company specific jobs
  - 14.11.4. Retention requirements for company specific jobs
  - 14.11.5. Scheduling
- 14.12. Customer extensions
- 14.13. Function modules
- 14.14. Transport Management
- 14.15. Cross system authorizations
- 14.16. Basis / Administration
- 14.17. Developer key
  - 14.17.1. Protection of table DEVACCESS
  - 14.17.2. Logging of table DEVACCESS
- 14.18. Development
- 14.19. Protection of individual-related data PA
- 14.20. Access to PA and PE tables
- 14.21. Cross client authorizations
- 14.22. Protection of RFC Connections and Destinations
- 15. Customer system analysis and reporting
- 16. Internal Control Management
- 17. Update of documentation
- 18. Regulations according to the change history