

Basisrolle für Überprüfungen durch Betriebsrat und Datenschutzbeauftragten

Z_AUDITOR_BR_DSB_BAS

(Version 1.0 – 11.2.2010)

Inhalt:

1. Einleitung
2. Besonderheiten, Merkwürdigkeiten
3. Bekannte Probleme
4. Nicht realisierbare Funktionen
5. Menü der Rolle
6. Berechtigungen

Änderungen an der Dokumentation:

18.05.2010: Aufnahme von Inhaltsverzeichnis und Änderungsprotokoll Hinweis auf die neue Version von RPDINF01 Hinweis zu Folgetransaktionen
--

1. Einleitung

Die Frage nach einer angemessenen SAP-Rolle für Überprüfungen durch den Betriebsrat oder den Datenschutzbeauftragten stellt sich immer wieder. SAP liefert mit dem Audit Info System (AIS) eine Reihe von Rollen für Revisionszwecke, die jedoch zum Teil sehr weitgehend und daher häufig nicht geeignet sind. Insbesondere enthalten sie z.T. kritische Änderungsberechtigungen.

Die Frage nach angemessenen Rollen für SAP-Datenschutzprüfungen wurde im Fachbereich Informatik der Universität Hamburg in einer Diplomarbeit behandelt. Dabei sind sechs neue Rollen entstanden, die als Grundlage für die Prüfberechtigungen von Datenschutzbeauftragten, Betriebs- und Personalräten dienen können. (siehe www.forbit.de/SAPAudit)

FORBIT hat daraus eine neue Rolle entwickelt,

- die nur die wesentlichen Transaktionen und Berechtigung enthält, die für Systemprüfungen durch Betriebsrat oder Datenschutzbeauftragten erforderlich sind,
- keine Änderungen im System zulässt, also auf reine Anzeigefunktionen beschränkt ist und
- keinen Zugriff auf personenbezogene Daten erlaubt, mit Ausnahme von Benutzerdaten.

Außerdem wurde die Rolle an den aktuellen Releasestand (6.0) angepasst. Sie enthält u.a. Funktionen zu

- Allgemeinen Systemprüfungen (Mandanten, System, Parameter, Systemänderbarkeit, Schnittstellen)
- Entwicklung/Customizing (ABAP Programme, Transaktionen, Erweiterungskonzept)
- Tabellen (Inhalte, Berechtigung, Protokollierung)
- Security Audit Log
- Benutzer und Berechtigungen
- HR-Personalwirtschaft (benutzte Infotypen, Protokollierung Reportstarts)
- „Dateiregister zu personenbezogenen Daten“ (die von SAP bereitgestellten Varianten der Funktion Verwedungsnachweis von Domänen (Report RSCRDOMA). Zu Nutzen und Grenzen siehe SAP ERP Datenschutzeleitfaden.)

Dabei wurden Funktionen, die nur mit sehr speziellem technischen Wissen sinnvoll genutzt werden können, weggelassen.

Wir können keine Gewähr dafür übernehmen, dass es vollständig gelungen ist, alle Änderungsberechtigungen oder Zugriffsmöglichkeiten auf personenbezogene Daten aus der Rolle zu entfernen. Die Rolle sollten vor Benutzung den üblichen Sicherheitsprüfungen unterzogen werden. Die Benutzung geschieht auf eigene Gefahr.

Diese Rolle wurde von der FORBIT GmbH erstellt und kann von Unternehmen für eigene Zwecke kostenlos benutzt werden. Weitere Rechte (z.B. Veröffentlichung, kommerzielle Nutzung) vorbehalten.

Die Rolle kann unter www.forbit.de/SAPAudit heruntergeladen und per upload im SAP-ERP System installiert werden.

Diese Rolle wurde für SAP ERP ECC 6.0 getestet.

Hinweise, Verbesserungsvorschläge und Fehlermeldungen zu dieser Rolle bitte an mott@forbit.de.

2. Besonderheiten, Merkwürdigkeiten:

RSCSAUTH Pflege/Restore Berechtigungsgruppen

Um die Zuordnung von Reports zu Berechtigungsgruppen prüfen zu können, wurde diese Transaktion aufgenommen. Es sieht so aus, als wenn man mit dieser Funktion Änderung durchführen könnte, aber die Anzeigen sind irreführend. Man kann zwar neue Berechtigungsgruppen in die Tabelle eintragen, wenn man die Änderungen sichert, erhält man erst eine Fehlermeldung, dann aber eine Bestätigung, trotzdem wird nichts geändert, was man mit neuerlichem Aufruf der Funktion kontrollieren kann.

SE16, SE16N, SE17 Data Browser, Tabellenanzeige

Eine Funktion zum Anzeigen von Tabelleinhalten wird für verschiedene Prüfungsaufgaben gebraucht. Insbesondere gibt es einige interessante Systemtabellen, für die keine andere Anzeigemöglichkeit besteht. Es wurde hier nur die Transaktion SE16N zur Verfügung gestellt, weil sie von vornherein auf die Anzeige beschränkt ist und die Ausgabe im SAP List Viewer (ALV) vorsieht. Damit ist auch die mit SE16 verbundene Schwierigkeit, dass u.U. nicht alle Felder angezeigt werden, weil die Ausgabebreite nicht angepasst wurde, umgangen. Leider ist bei SE16N die Eingabe der Auswahlparameter etwas hakelig. Bei Bedarf kann SE16 oder SE17 zusätzlich oder statt dessen berechtigt werden.

Tabellen mit Anwendungsdaten, insbesondere personenbezogenen Daten, sollen über diese Funktion nicht zugänglich sein. Es wurden die folgenden Tabellenklassen berechtigt:

AQPR	Query Protokoll.
BS	Steuerung SAP
PC	RP:Steuerung Anwender
PS	RP:Steuerung SAP
SS	RS:Steuerung SAP
SUSR	Benutzerstamm
SVIM	erw. Tabellenpflege

Zur Klasse SC siehe unten.

SUIM Benutzerinformationssystem

Alle Funktionen von SUIM sind mit den in der Rolle enthaltenen Menüpunkten ausführbar, allerdings wurde die Struktur des Menüs etwas vereinfacht. Auf die Aufnahme der Transaktion SUIM selbst in das Menü wurde verzichtet. Wer jedoch die Funktion kennt und weiter benutzen möchte, sollte die Möglichkeit dazu haben; daher wurde die Transaktion zusätzlich berechtigt.

3. Bekannte Probleme

HRAUTH Berechtigungs - Workbench

RHAUTH erlaubt den Aufruf des Reports RHBAUS00, der dazu dient, die Indizes für strukturelle Berechtigungsprofile neu zu generieren. Dieser Report zeigt nur Wirkung, wenn zur Performance-Verbesserung die Tabelle T77UU (Benutzerdaten im SAP-Memory) gepflegt wird (Customizingaktivität *Benutzerdaten im SAP-Memory speichern*).

In diesem Fall wird der Report in der Regel ohnehin täglich als Batch-Job gestartet, so dass ein Start zwischendurch unkritisch wäre. Ein Missbrauch ist nur denkbar, wenn der Benutzer gleichzeitig das Org-Management manipulieren kann. Auch in diesem Fall bedarf es detaillierter Kenntnisse, um

Missbrauch zu treiben. Falls T77UU benutzt wird und Manipulationen möglich erscheinen, sollte die Transaktion HRAUTH aus der Rolle gelöscht werden.

S_ALR_87101324 Infotypen und Subtypen (Report RPDINF01)

In der neuen Version des Reports (vgl. Hinweis 1276561 vom 15.04.2010) existiert das Problem nicht mehr. Entsprechende Korrektur durchführen. Für frühere Versionen gilt:

Bei der Anwendung der Transaktion (Report RPDINF01) können personenbezogene Informationen offenbart werden, wenn man im Auswahldialog nur eine Personalnummer angibt. Dann wird angezeigt, ob zu dieser Personalnummer Datensätze eines Infotyps existieren. Man erhält also ggf. die Information, dass für eine Personalnummer Datensätze zu Behinderung oder Pfändung vorhanden sind. Auch wenn man den Inhalt des Datensatzes nicht sehen kann, gibt die Information über die Existenz eines Datensatzes schon einen Hinweis, der kritisch sein kann.

Da diese Funktion andererseits eine der wichtigsten Kontrollen der benutzen Infotypen darstellt, wurde sie dennoch in die Rolle aufgenommen.

Abhilfe: Erzeugen einer Variante des Reports, in der das Feld Personalnummer mit einem passenden Personalnummernbereich vorbelegt ist, und Einbindung der Variante statt des Originalreports.

4. Nicht realisierbare Funktionen

Im Folgenden sind Funktionen aufgeführt, die eigentlich in einer allgemeinen Prüfrolle sinnvoll wären, die aber zu weitgehende Berechtigungen beinhalten, weil die enthaltenen Berechtigungsprüfungen Mängel oder Fehler enthalten, und die daher weggelassen werden mussten:

SE84 Repository Infosystem (oder SE80)

Die Transaktion ist eigentlich ein hilfreiches Universalanzeigewerkzeug für alle Objekte (Tabellen, Programme, Transaktionen usw.) des System. Bei der Anzeige von Programmen ist jedoch eine Funktion zum Ausführen des betrachteten Programms dabei (Direkt - F8), die ohne jede weitere Berechtigungsprüfung jedes Programm erstmal startet. Nicht einmal das Berechtigungsobjekt S_PPROGRAMM wird geprüft, wie man es in Analogie zu SA38 erwarten könnte! Man kann hoffen, dass die weitere Ausführung des Programms dann an der im Programm eingebauten Berechtigungsprüfung scheitert, aber da kann man nicht sicher sein (bei Kundenprogrammen ist es u. U. fraglich, ob die Authority Checks richtig oder überhaupt eingebaut wurden, und auch bei SAP Programmen kann man sich auf ausreichende Berechtigungsprüfungen nicht unbedingt verlassen). Daher müssen wir auf diese Funktion leider verzichten.

SQ01, SQ02, SQ03, SQ10 Query

Die Transaktionen, die man zum Ansehen von Queries, Infosets, Query-Benutzergruppen braucht, beinhalten leider alle auch Änderungsberechtigungen bzw. die Möglichkeit zum Ausführen der Query. Möglichkeiten zur Begrenzung auf reine Anzeigefunktion mittels der Berechtigungsobjekte haben wir nicht gefunden.

Abhilfe: Tabellenanzeige mit SE16N für die Tabellen, in denen Queries verwaltet werden, u.a.:

- AQQCAT und AQLCAT (Query-Katalog) enthalten Benutzergruppe, Queryname, Infoset (Global oder Lokal) – AQGTQ und AQLTQ enthalten die Texte (Bezeichnungen, Langnamen) der Queries
- AQGDBBS (Infosets je Gruppe) und

- AQGDBBN (Benutzer je Gruppe)

Oder: Einbinden der Reports RSAQDEL0, RSAQUSGR, RSAQSHSG mit passenden Varianten – liefert allerdings nur Ergebnisse für den lokalen Bereich.

Tabellenklasse SC (RS:Steuerung Anwender)

Ein Zugriff auf die Tabelle HRP1001, die den Infotyp 1001 (Verknüpfungen) des Organisationsmanagements enthält, ermöglicht u.a. einen Zugriff auf alle Verknüpfungen von einer Person (Objekttyp P) zu anderen Objekten (Planstelle, Qualifikationen, Veranstaltungen...) im Org-Management! Um ein Zugriff auf diese personenbezogenen Informationen zu unterbinden, wird die zu HRP1001 gehörige Tabellenklasse SC nicht berechtigt. Leider gehören viele (1765) andere Tabellen zu dieser Klasse, z.B. die Tabellen für Infotyp 1016 und 1017, die, wenn sie benutzt werden, einer Kontrolle zugänglich sein sollten. Der mögliche Zugriff auf u.U. sensible personenbezogene Daten wurde als schwerwiegender erachtet, daher ist diese Tabellenklasse nicht berechtigt.

Abhilfe: eigene Tabellenklasse für HRP1001 schaffen.

RBDAUD01 ALE Audit

ermöglicht es, ohne weitere Berechnungsprüfung die Inhalte von IDocs, und damit ggf. personenbezogene Daten zu sehen. Daher weggelassen.

TU02 Systemparameter, Übersicht mit Historie

listet die Systemparameter und die Historie (Änderungen) auf. Die Transaktion enthält auch die Möglichkeit, die Daten zu einem Server zu löschen („Delete Server“!), dabei scheint es keine weitere Berechtigungsprüfung zu geben. Daher wurde die Transaktion weggelassen.

Abhilfe: Wenn man bei einer Kontrolle wirklich einmal in die Situation kommen sollte, dass die Änderungen an den Systemparametern nachvollzogen werden müssen, sollte man einen Systemadministrator hinzuziehen.

RSWBO040 Objekte in Aufträgen/Aufgaben suchen

Erlaubt über den Menüpunkt „Springen“ den Aufruf von SE03 mit sehr weitgehenden Möglichkeiten. Ob dabei alle Änderungsmöglichkeiten wirklich durch die Berechtigungsprüfung abgefangen werden, wäre zu prüfen. Vorsichtshalber weggelassen.

Bemerkung zu Folgetransaktionen

Über die Transaktion SE97 kann man steuern, ob innerhalb einer Transaktion beim Aufruf einer Folgetransaktionen eine zusätzliche Berechtigungsprüfung durchgeführt wird.

Wenn man bei Transaktionen, die hier aufgenommen wurden, Probleme mit Folgetransaktionen hat, kann man sie auf diesem Weg lösen.

Auch könnte man hier weggelassene Transaktionen zusätzlich in die Rolle aufnehmen, wenn man zuvor den Aufruf problematischer Folgetransaktionen durch diese Funktion verhindert hat.

In beiden Fällen ist jedoch zu prüfen, ob es dadurch zu Wechselwirkungen bei anderen Rollen kommt, bei deren Design von der Standardeinstellung ausgegangen wurde. Gegebenenfalls müssen weitere Rollen nachgepflegt werden.

5. Menü der Rolle

Menü der Rolle: Z_AUDITOR_BR_DSB_BAS

```

|-- Eigene Daten
| |
| |----SU3 Benutzer eigene Daten pflegen
| |----SU53 Auswertung der Berechtigungsprüfung
| |----SU56 Benutzerpuffer analysieren
|
|-- Weiterführende Informationen
| |
| |-- S A P
| | |
| | |----URL SAP Homepage (deutsch)
| | |----URL SAP Service Marketplace
| | |----URL SAP Help Portal
| | |----URL SAP Technical Resources
| |
| |-- SAP User Groups (Revision)
| | |
| | |----URL SAP Arbeitskreis Wirtschaftsprüfung und Revision
| | |----URL DSAG Deutsche SAP® Anwendergruppe e.V
| | |----URL DSAG AG Datenschutz im AK Revision/Risikomanagement
| |
| --- Leitfäden
| |
| |----URL DSAG Datenschutzleitfaden + Prüfleitfaden SAP-ERP
| |----URL SAP R/3-Sicherheitsleitfaden (Anmeldung erforderlich)
| |----URL SAP: Ältere Datenschutzleitfäden
|
|-- Allgemeine Systemprüfungen
| |
| |-- Mandanten
| | |
| | |----SCC4 Mandantenverwaltung
| |
| |-- System
| | |
| | |----HIER Interne Pflege Anwendungsbereiche
| | |----SM51 Liste der SAP-Systeme
| |
| |-- Parameter
| | |
| | |----RZ11 Systemparameter mit Doku
| | |----RSPFPAR Profileparameter anzeigen
| |
| |-- Systemänderbarkeit
| | |
| | |----RSWBO004 Systemänderbarkeit setzen (nur Anzeige!)
| |
| --- Kommunikationsarten von R/3
| |
| |-- RFC / SAP Remote Function Call
| | |
| | |----SM59 RFC-Destinations (Anzeige)
| |

```

```

|   --- ALE Verteilungsmodell
|   |
|   |-----BD64 Verteilungsmodellpflege
|-- Entwicklung/Customizing
|   |
|-- ABAP Programme
|   |
|   |-----RSABTPGP Reportberechtigungsgruppen anzeigen
|   |-----RSCSAUTH Pflege/Restore Berechtigungsgruppen
|   |
|-- Transaktionen
|   |
|   |-----RSAUDITC_BCE Gesperrte Transaktionen
|-- Erweiterungskonzept
|   |
|   |-----CUSTMON1 Objekte im Kundennamensraum
|-- Repository/Tabellen
|   |
|-- Tabelleninformationen
|   |
|   |-----SE16N Allgemeine Tabellenanzeige
|   |-----SE11 R/3-Data-Dictionary
|   |
|-- Tabellenberechtigung
|   |
|   |-----SM30V_BRG Liste der Berechtigungsgruppen
|   |-----SM30V_DDAT Zuordnung der Berechtigungsgruppen zu Tabellen/Views
|   |-----SAPSCRIPT AIS-Doku
|   |
|   |-----S_ALR_87101219 Tabellenprotokollierung (und andere Infos)
|-- Tabellenaufzeichnungen
|   |
|   |-----RSPFPAR_TABLEREC Systemparameter
|   |-----RDDPRCHK_AUDIT Tabellen mit/ohne Tabellenprotokollierung
|   |-----SE13 Techn. Tabelleneinstellungen
|   |-----RSTBHIST Tabellenhistorie
|   |-----RFTBPROT_BCE_AUDIT Auswertung Tabellenhistorie (RSTBPROT/RSVTPROT)
|   |-----SAPSCRIPT AIS-Doku
|-- Security Audit Log
|   |
|   |-----SM19 Konfiguration Security Audit
|   |-----SM20 Auswertung Security-Audit-Log
|-- Benutzer und Berechtigungen
|   |
|-- Authentisierung
|   |
|   |-----RSPFPAR_LOGIN Anmeldeeregeln Parameter
|   |-----RSPFPAR_SAPSTAR Profilparameter zum Sonderbenutzer SAP*
|   |-----SE16USR40 Unerlaubte Kennwörter
|   |
|-- Infosystem Benutzer & Berechtigungen
|   |
|   |-----SU01D Benutzeranzeige
|   |-- Benutzerübersicht
|   |
|   |

```

```
| | | |----RSUSR003 Kennworte der Standardbenutzer prüfen
| | | |----RSUSR200 Liste der Benutzer nach Anmeldedatum
| | | |----RSUSR200 Benutzer nach Anmeldedatum und Kennwortänderung
| | | |----S_BCE_68001402 Benutzer mit Falschanmeldungen
| | | |----RFAUDI06_BCE Anzahl der Benutzerstammsätze
| | | |----RSUSR007 Benutzer mit unvollständiger Adresse
| | | |----RSUSR200 Benutzer nach Anmeldedatum
| | | |----RSUSR200_INITPASS Benutzer mit Initialkennwort
| | | |----RSUSR200_UNUSED30 Seit 30 Tagen nicht angemeldet
| | | |----RSUSR200_PWDCHG180 Seit 180 Tagen Kennwort nicht geändert
| | |
| | | |-- Infosystem: Benutzer, Rollen, Profile, Berecht., Ber.Objekte, Transakt.
| | | |
| | | |----S_BCE_68001400 Benutzer nach komplexen Selektionskriterien
| | | |----S_BCE_68001425 Rollen nach komplexen Selektionskriterien
| | | |----S_BCE_68001409 Profile nach komplexen Selektionskriterien
| | | |----S_BCE_68001417 Berechtigungen nach komplexen Suchkriterien
| | | |----S_BCE_68001413 Berechtigungsobjekte nach komplexen Suchkriterien
| | | |----S_BCE_68001429 ausführbare Transaktionen ( alle Selektionsmöglichkeiten )
| | |
| | | |-- Benutzer mit kritischen Berechtigungen
| | | |
| | | |----S_BCE_68002111 mit kritischen Berechtigungen (neue Version)
| | |
| | | |-- Vergleiche
| | | |
| | | |----S_BCE_68001430 Vergleiche von Benutzern
| | | |----S_BCE_68001777 Vergleiche von Rollen
| | | |----S_BCE_68001431 Vergleiche von Profilen
| | | |----S_BCE_68001432 Vergleiche von Berechtigungen
| | |
| | | |-- Verwendungsnachweis
| | | |
| | | | |-- Profile
| | | | |
| | | | |----S_BCE_68001395 in Benutzern
| | | | |----S_BCE_68001421 in Rollen
| | | | |----S_BCE_68001404 in Sammelprofilen
| | | |
| | | | |-- Berechtigungen
| | | | |
| | | | |----S_BCE_68001396 in Benutzern
| | | | |----S_BCE_68001405 in Profilen
| | | |
| | | | |-- Berechtigungswerte
| | | | |
| | | | |----S_BCE_68001397 in Benutzern
| | | | |----S_BCE_68001423 in Rollen
| | | | |----S_BCE_68001406 in Profilen
| | | | |----S_BCE_68001415 in Berechtigungen
| | | |
| | | | --- Berechtigungsobjekte
| | | | |
| | | | |----RFAUDI20_BCE Verwendungsnachweis: Berechtigungsobjekt->Transaktion/Progr.
| | | | |----S_BCE_68002030 in Programmen
| | | |
| | | |-- Änderungsbelege
| | | |
| | | |----S_BCE_68001439 für Benutzer
| | | |----RSSCD100_PFCG_USER für Rollenzuordnung
```

```

| | | |----RSSCD100_PFCG für Rollen
| | | |----S_BCE_68001440 für Profile
| | | |----S_BCE_68001441 für Berechtigungen
| | |
| | | |-- Strukturelle Berechtigungen
| | | |
| | | |----S_ALR_87101321 Berechtigte Objekte je Benutzer/Prof
| | |
| | | |----HRAUTH Berechtigungs - Workbench
| | |
| | | --- Rollenverwaltung
| | | |
| | | |----RSPFPAR_PROFGEN Systemparameter
| | | |----PFCG Rollenverwaltung
| | | |----SU22 Berechtigungsvorschlagswerte für Profilgenerator (SAP-Vorschläge)
| | | |----SU24 Berechtigungsvorschlagswerte für Profilgenerator (Kundendaten)
| | | |----AUTH_DISPLAY_OBJECTS Anzeige aktiver Berechtigungsobjekte
| | |
| | | |-- HR-Personalwirtschaft
| | | |
| | | | |-- Personaladministration
| | | | |
| | | | |----S_ALR_87101323 Anzeige der Infotypen gemaess Datadi
| | | | |----S_ALR_87101324 Infotypen und -Subtypen
| | | |
| | | | |-- Personalplanung
| | | | |
| | | | |----S_ALR_87101320 Infotypdefinitionen anzeigen
| | | | |----S_PH0_48000120 Datenbankstatistik Personalplanung
| | | |
| | | | --- HR-Protokollierung
| | | | |
| | | | | |-- HR Änderungsprotokollierung
| | | | | |
| | | | | |----SM30_V_T585A Belegrelevante Infotypen
| | | | | |----SM30_V_T585B Feldgruppendifinition
| | | | | |----SM30_V_T585C Feldgruppeneigenschaften
| | | | |
| | | | | --- Protokollierung Reportstarts
| | | | | |
| | | | | |----SM30_V_T599R HR Reportattribute
| | | | | |----S_ALR_87014082 Protokoll der Reportstarts
| | | |
| | | | --- Dateiregister zu personenbezogenen Daten
| | | | |
| | | | |----S_ALR_87101308 Verwendungsnachweis von Domänen zu nicht-leeren DB-Tabellen
| | | | |----S_ALR_87101309 Dateiregister für Mitarbeiterdaten
| | | | |----S_ALR_87101310 Dateiregister für Bewerberdaten
| | | | |----S_ALR_87101311 Dateiregister für Lieferantendaten
| | | | |----S_ALR_87101312 Dateiregister für Kundendaten
| | | | |----S_ALR_87101313 Dateiregister für Partnerdaten
| | | | |----S_ALR_87101314 Dateiregister für Sachbearbeiterdaten
| | | | |----S_ALR_87101315 Dateiregister für Verkäufergruppensdaten
| | | | |----S_ALR_87101316 Dateiregister für Patientendaten
| | | | |----S_ALR_87101317 Dateiregister für R/3 Benutzer
| | | | |----S_ALR_87101318 Ausgabe Felddokumentation mit erlaubten Werten

```

6. Berechtigungen

Profil zur Rolle Z_AUDITOR_BR_DSB_BAS					
Objekt	Feld	Wert			Kommentar
B_ALE_MODL			ALE: Verteilungsmodellpflege		
	ACTVT			Aktivität	SU22 Vorschlag für BD64
		3		Anzeigen	
	CUSTOMODEL			Modellsicht des ALE-Modells	
		*			
P_TCODE			HR: Transaktionscode		
	TCD			Transaktionscode	
		PFCG			SU22 Vorschlag für PFCG
		SU01D			SU22 Vorschlag für SU01D
S_ADDRESS1			Business Address Services: Adreßtyp1 (Organisationsadressen)		
	ACTVT			Aktivität	SU22 Vorschlag für SU01D
		3		Anzeigen	
	ADGRP			Adreßgruppe (Schlüssel) (Business Address Services)	
		BC01			
S_ADMI_FCD			Systemberechtigungen		
	S_ADMI_FCD			Systemadministrationsfunktion	
		AUDD		Basis Audit Anzeigeberechtigung	Nötig für SM20
S_C_FUNCT			C-Aufrufe in ABAP-Programmen		
	ACTVT			Aktivität	SU22 Vorschlag für SM19
		16		Ausführen	
	CFUNCNAME			Name einer CALL-baren C-Routine	
		AUDIT_GET_INFO			
		AUDIT_SET_INFO			
		C_GET_CPU_ID			
		C_GET_SYSTEM_NUMBER			
		C_SAPGPARAM			
	PROGRAM			Programmname mit Suchhilfe	
		SAPLSECU			
		SAPMSM19			
	ACTVT			Aktivität	SU22 Vorschlag für SM20
		16		Ausführen	
	CFUNCNAME			Name einer CALL-baren C-Routine	
		C_DIR_READ_FINISH			
		C_DIR_READ_NEXT			
		C_DIR_READ_START			
		C_GET_CPU_ID			
		C_GET_SYSTEM_NUMBER			
		C_RSTRB_READ_BUFFERED			
		C_SAPGPARAM			
	PROGRAM			Programmname mit Suchhilfe	
		SAPLSECU			
		SAPLSLO6			
		SAPMSM20			
S_DEVELOP			ABAP Workbench		
	ACTVT			Aktivität	
		3		Anzeigen	
	DEVCLASS			Paket	
		*			
	OBJNAME			Objektname	
		*			
	OBJTYPE			Objekttyp	
		*			
	P_GROUP			Berechtigungsgr.ABAP/4-Programm	
		*			

S_GUI			Berechtigung für GUI-Aktivitäten	
	ACTVT		Aktivität	
		61	Exportieren	
S_PROGRAM			ABAP: Programmablaufprüfungen	
	P_ACTION		Benutzeraktion ABAP/4 Programm	
		SUBMIT	Ausführen ABAP Programm	
	P_GROUP		Berechtigungsgr.ABAP/4-Programm	
		SAP_ALL		notwendig für TA RSCSAUTH, In der Berechtigungsgruppe mit dem merkwürdigen Namen SAP_ALL sind jedoch nur 2 Programme.
S_RFC			Berechtigungsprüfung beim RFC-Zugriff	
	ACTVT		Aktivität	
		16	Ausführen	SU22 Vorschlag für SM20, wird benötigt, wenn die Daten auf verschiedenen Systemen gespeichert sind.
	RFC_NAME		Name des zu schützenden RFC-Objekts	
		SECU		
		SLO2		
		SLO6		
	RFC_TYPE		Typ des zu schützenden RFC-Objekts	
		FUGR	Funktionsgruppe	
S_RFC_ADM			Administration für RFC-Destination	
	ACTVT		Aktivität	
		3	Anzeigen	
	ICF_VALUE		Internet Communication Framework-Werte	
		*		
	RFCDEST		logische Destination (Wird bei Funktionsaufruf angegeben)	
		*		
	RFCTYPE		Art des Eintrags in RFCDES	
		*		
S_TABU_CLI			Tabellenpflege mandantenunabhängiger Tabellen	
	CLIIDMAINT		Kennzeichen für mandantenunabhängige Pflege	
		''		
S_TABU_DIS			Tabellenpflege (über Standardtools wie zB SM30)	
	ACTVT		Aktivität	
		3	Anzeigen	
	DICBERCLS		Berechtigungsgruppe	
		AQPR	Query Protokoll.	
		BS	Steuerung SAP	
		PC	RP:Steuerung Anwender	
		PS	RP:Steuerung SAP	
		SS	RS:Steuerung SAP	
		SUSR	Benutzerstamm	
		SVIM	erw. Tabellenpflege	für SM30V_DDAT nötig
S_TCODE			Transaktionscode-Prüfung bei Transaktionsstart	
	TCD		Transaktionscode	Transaktion des Menüs
		AUTH_DISPLAY_OBJECTS		
		BD64		
		CUSTOMON1		
		HIER		
		HRAUTH		
		PFCG		
		RDDPRCHK_AUDIT		
		RFAUDI06_BCE		

	RFAUDI20_BCE			
	RFTBPROT_BCE_AUDIT			
	RSABTPGP			
	RSAUDITC_BCE			
	RSCSAUTH			
	RSPFFPAR			
	RSPFFPAR_LOGIN			
	RSPFFPAR_PROFGEN			
	RSPFFPAR_SAPSTAR			
	RSPFFPAR_TABLEREC			
	RSSCD100_PFCG			
	RSSCD100_PFCG_USER			
	RSTBHIST			
	RSUSR003			
	RSUSR007			
	RSUSR200			
	RSUSR200_INITPASS			
	RSUSR200_PWDCHG180			
	RSUSR200_UNUSED30			
	RSWBO004			
	RZ11			
	SCC4			
	SE11			
	SE13			
	SE16N			
	SE16USR40			
	SM19			
	SM20			
	SM30V_BRG			
	SM30V_DDAT			
	SM30_V_T585A			
	SM30_V_T585B			
	SM30_V_T585C			
	SM30_V_T599R			
	SM51			
	SM59			
	SU01D			
	SU22			
	SU24			
	SU3			
	SU53			
	SU56			
	S_ALR_87014082			
	S_ALR_87101219			
	S_ALR_87101308			
	S_ALR_87101309			
	S_ALR_87101310			
	S_ALR_87101311			
	S_ALR_87101312			
	S_ALR_87101313			
	S_ALR_87101314			
	S_ALR_87101315			
	S_ALR_87101316			
	S_ALR_87101317			
	S_ALR_87101318			
	S_ALR_87101320			
	S_ALR_87101321			
	S_ALR_87101323			
	S_ALR_87101324			
	S_BCE_68001395			
	S_BCE_68001396			
	S_BCE_68001397			
	S_BCE_68001400			
	S_BCE_68001402			

		S_BCE_68001404			
		S_BCE_68001405			
		S_BCE_68001406			
		S_BCE_68001409			
		S_BCE_68001413			
		S_BCE_68001415			
		S_BCE_68001417			
		S_BCE_68001421			
		S_BCE_68001423			
		S_BCE_68001425			
		S_BCE_68001429			
		S_BCE_68001430			
		S_BCE_68001431			
		S_BCE_68001432			
		S_BCE_68001439			
		S_BCE_68001440			
		S_BCE_68001441			
		S_BCE_68001777			
		S_BCE_68002030			
		S_BCE_68002111			
		S_PH0_48000120			
	TCD			Transaktionscode	Manuell zugefügte Transaktionen
		SU_VCUSRVARCOM_DISP			für S_BCE_68002111 (Benutzer mit kritischen Berechtigungen) nötig, um die Varianten ansehen zu können
		SU_VCUSRVAR_DISP			Nicht im Menü, aber wer die TA kennt, soll sie ausführen können.
		SUIM			
S_TRANSPRT				Transport Organizer	
	ACTVT			Aktivität	Erforderlich für CUSTMON1
		3		Anzeigen	
	TTYPE			Auftragstyp (Change & Transport System)	
		''			
S_USER_ADM				Administrationsfunktionen für Benutzer/Berechtigungsverwaltg.	
	S_ADM_AREA			Administrationsbereiche zum Berechtigungsobjekt S_USER_ADM	
		CHKSTDPWD			SU22 Vorschlag für RSUSR03
S_USER_AGR				Berechtigungswesen: Prüfung für Rollen	
	ACTVT			Aktivität	
		3		Anzeigen	
		8		Änderungsbelege anzeigen	
	ACT_GROUP			Name der Rolle	
		*			
S_USER_AUT				Benutzerstammpflege: Berechtigungen	
	ACTVT			Aktivität	
		3		Anzeigen	
		8		Änderungsbelege anzeigen	
	AUTH			Berechtigungsname in Benutzerstammpflege	
		*			
	OBJECT			Berechtigungsobjekt	
		*			
S_USER_GRP				Benutzerstammpflege: Benutzergruppen	
	ACTVT			Aktivität	
		3		Anzeigen	
		8		Änderungsbelege anzeigen	
	CLASS			Benutzergruppe in Benutzerstammpflege	
		*			

